Das Clavister

cOS Core Kochbuch

Nur die leckersten Rezepte

von Peter Nilsson
Herausgegeben durch
Clavister AB Schweden

Gedruckt in Schweden

Deutsche Erstauflage, 2017

ISBN: **978-91-982968-3-9**

Clavister AB
Sjögatan 6J
SE-89160 Örnsköldsvik
Schweden

www.clavister.com

cookbook@clavister.com

Danksagungen

Ein großes Dankeschön für ihre Ermutigung und Unterstützung dabei, dieses Buch fertigzustellen, geht an die folgenden Personen: Colin Mummery, Neal Sutherland, Kimmo Klemola, Tobias Rhén, Torbjörn Fahlen, Jaap van Duijn und Edgard Dias Batista. Für die deutsche Übersetzung ein großes Dankeschön an Ulf Dunkel.

Über den Autor

Peter Nilsson ist Senior Support Engineer bei Clavister AB und hat mehr als zehn Jahre Erfahrung darin, Unternehmen zu helfen, Netzwerk-Sicherheitslösungen mithilfe von Clavister-Produkten zu installieren. Er lebt in Örnsköldsvik, Schweden.

Inhalt

Kapitel 1: Grundlagen

Die Absicht dieses Buches ist, Neulinge an das cOS-Core-Netzwerk-Betriebssystem heranzuführen. cOS-Core ist die Software, die die wichtigste Clavister-Produktpalette zukunftsfähiger Firewalls steuert. cOS-Core bietet eine breite Palette von Funktionen, mit denen ein Netzwerkadministrator den Datenverkehr, der eine Clavister-Firewall passiert, kontrollieren, begrenzen und beobachten kann. Dieser Datenfluss kann in beliebigen, sowohl öffentlichen als auch privaten Netzwerken stattfinden und die Daten können zwischen Clients und Servern fließen, ebenfalls öffentlich oder privat.

cOS-Core läuft nicht als Software auf einem anderen Betriebssystem, wie z.B. Linux. Stattdessen läuft es direkt auf seiner Hardware-Plattform und ist deshalb selbst ein echtes Betriebssystem. Weil kein darunter liegendes Wirtsbetriebssystem nötig ist, ist cOS-Core hochperformant und benötigt wenig Speicher, weswegen es maßgeschneidert für Umgebungen mit Hardware-Ressourcenbeschränkungen ist. cOS-Core kann sowohl auf Clavister-Hardware als auch unter einem Hypervisor in einer virtuellen Umgebung laufen.

Dieses Kapitel beschreibt die grundsätzlichen Prinzipien von cOS-Core, was IP-Regeln, Verwaltung, Routing, Routing-Grundsätze und andere Funktionen angeht. Wenn Sie sich mit diesen Prinzipien schon auskennen, können Sie zum nächsten Kapitel weiterblättern.

Das separate *Clavister-cOS-Core-Verwaltungshandbuch* beschreibt jede Funktion ausführlich mit allen Details. Dieses Kochbuch konzentriert sich mehr auf Lösungen und Szenarien, statt in aller Ausführlichkeit zu erklären, was genau jede Einstellung macht. Wir empfehlen, dieses Kochbuch zusammen mit dem Clavister-cOS-Core-Verwaltungshandbuch zu nutzen, um das Verständnis von cOS-Core zu vertiefen. Das Verwaltungshandbuch ist knapp tausend Seiten dick und wird bei jeder Veröffentlichung von cOS-Core als Teil der PDF-Dateidokumentation mitgeliefert. Sie können es auch auf der Firmenwebsite von Clavister herunterladen (www.clavister.com).

1.1. Das Objekte-Konzept

Dieser Abschnitt beschreibt das Konzept und die Nutzung von cOS-Core-*Objekten*. Ebenso behandelt er allgemein die Verwendung der *Internet-Oberfläche* (WebUI), mit dem Sie cOS-Core verwalten (jeder Webbrowser kann verwendet werden, um sich zur Verwaltung mit dem cOS-Core zu verbinden). Sie erfahren, wann Sie es verwenden, wann Sie es besser nicht verwenden und warum es wichtig ist, von Anfang an strukturiert zur arbeiten.

Objekte können in allen Aspekten einer cOS-Core-Einstellung benutzt werden. Wir können z.B. ein IP-Objekt namens „Meine_IP" erzeugen und ihm als IP-Adresse z.B. 192.168.1.1 zuweisen. Dann können wir diesen Objektnamen an anderen Stellen verwenden, z.B. mit IP-Regeln, Schnittstellen oder Benutzerauthentifizierung.

Das Verwenden von Adressbuch-Objekten bietet einige wichtige Vorteile:

- Es verbessert das Verständnis der Konfiguration, indem wir bedeutungsvolle, symbolische Namen verwenden.
- Das Verwenden von Adress-Objektnamen, statt nummerische Adressen einzugeben, verringert Fehler.
- Wenn ein Adressbuch-Objekt geändert werden muss, werden alle Funktionen und Eigenschaften, die dieses Objekt benutzen, automatisch aktualisiert.

Je weiter wir im Buch fortschreiten, desto detaillierter gehen wir darauf ein, wie Sie die verschiedenen Objekte nutzen.

Adressbuch mit anderen Objekten nutzen

Sie können viele Objektarten der cOS-Core-Konfiguration erzeugen. Um zunächst bei den Grundzügen zu bleiben, werden wir jetzt nur IP-Adressobjekte im Adressbuch und Dienst-Objekte besprechen. Andere Objektarten werden im späteren Verlauf in anderen Rezepten erklärt.

Abbildung 1.1.1 ist ein Bildschirmfoto aus der Verwaltungsoberfläche (WebUI), das den ersten Teil des *Objekte*-Menüs zeigt.

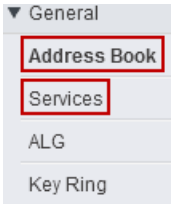


Abbildung 1.1.1 Objekte-Menü im WebUI

Wenn wir z.B. eine IP-Regel erzeugen, haben wir die Möglichkeit, eine nummerische IP-Adresse oder ein Netzwerk von Hand einzugeben, oder wir können ein benanntes Objekt verwenden, das sich schon im Adressbuch befindet.

Es wird dringend empfohlen, Adressen aus dem Adressbuch für IP-Regeln, Routing- und andere Objektarten zu verwenden. Wenn wir direkt nummerische IP-Adressen und Netzwerke eingeben, ist die Konfiguration schwerer zu lesen und zu strukturieren. Zum Beispiel verwenden die IP- Regeln im nachfolgend gezeigten WebUI- Bildschirmfoto nummerische IP-Adressen statt Adressbuch-Objekte.

	Name	Log	Src If	Src Net	Dest If	Dest Net	Service
1	▶ Test_Rule_1	✔	Lan	192.168.50.0/24	Dmz	172.16.10.0/24	all_services
2	▶ Test_Rule_2	✔	Lan	192.168.51.0/24	Dmz	172.16.20.0/24	all_services

Abbildung 1.1.2 IP-Regeln ohne Adressbuch-Objekte

Unsere IP-Regeln, oder auch alle anderen Teile der Konfiguration, lassen sich besser strukturieren und lesen, wenn wir Adressbuch-Objekte verwenden. Das wird nachfolgend verdeutlicht, wo die IP-Regeln von oben jetzt statt nummerischer Werte Adressbuch-Objekte verwenden.

	Name	Log	Src If	Src Net	Dest If	Dest Net	Service
1	▶ Test_Rule_1	✔	Lan	Lannet	Dmz	Dmznet	all_services
2	▶ Test_Rule_2	✔	Lan	Stockholm_Net	Dmz	Stockholm_ServerNet	all_services

Abbildung 1.1.3 IP-Regeln mit Adressbuch-Objekten

Dennoch ist es immer möglich, den Mauszeiger auf ein Adressbuch-Objekt zu halten, um einen Hilfstext angezeigt zu bekommen, der die nummerische IP-Adresse oder die Gruppenzugehörigkeit zeigt.

Das Wichtigste hier ist, dass das Ändern eines Adressbuch-Objekts automatisch alle Referenzen zu dem Objekt mit ändert.

Dienste

Ein Dienst-Objekt ist eine Referenz zu einem bestimmten IP-Protokoll mit dazugehörigen Parametern. Eine Dienst-Definition basiert normalerweise auf einem der hauptsächlichen Transportprotokolle wie z.B. TCP oder UDP, das mit einer bestimmten Quelle und/oder Ziel-Portnummer(n) verbunden ist. Der HTTP-Dienst z.B. ist so definiert, dass er das TCP-Protokoll mit dem verbundenen Ziel-Port 80 und einem beliebigen Quell-Port verwendet.

Das nachfolgende Bildschirmfoto zeigt die grundsätzlichen Eigenschaften eines Dienst-Objekts im cOS-Core.

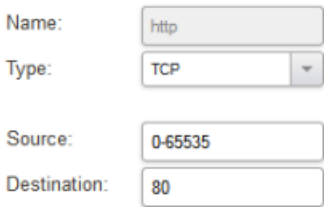


Abbildung 1.1.4 Dienst-Objekt-Eigenschaften

Dienst-Objekte sind jedoch nicht nur auf das TCP- oder UDP-Protokoll beschränkt. Sie können ebenso ICMP-Nachrichten enthalten als auch benutzer-definierbare IP-Protokolle.

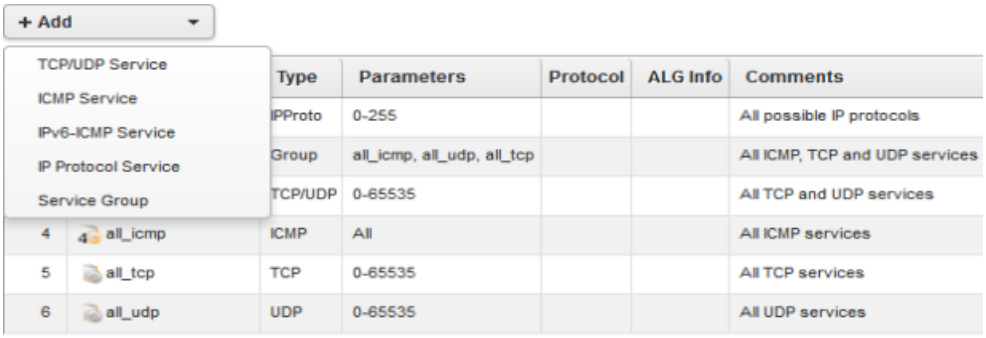


Abbildung 1.1.5 Dienst-Objektarten

1.2. Einführung in IP-Regeln

Eine grundlegende Funktion vom cOS-Core findet sich in den IP-Regeln (die manchmal auch Sicherheitsrichtlinien genannt werden). Dieser Abschnitt beschreibt, was eine IP-Regel ist, wie man sie verwendet, und gibt einige Tipps.

Unterschiede zwischen einer IP-Regel und einer IP-Richtlinie

Es gibt zwei Arten von Datenverkehr-Regeln: IP-Regeln (IP Rules) und IP-Richtlinien (IP Policies). Im nachfolgenden WebUI-Bildschirmfoto wird gezeigt, wie beide Arten hinzugefügt werden.

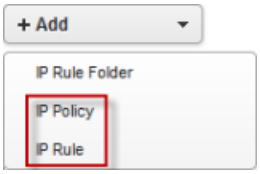


Abbildung 1.2.1 Eine neue IP-Richtlinie oder IP-Regel hinzufügen

IP-Regeln und IP-Richtlinien sind zwei Regelarten, die das Gleiche tun. Der Zweck von IP-Richtlinien ist es, Anwendern beim Anlegen von Regeln zu helfen, indem die benötigte Anzahl von Regeln und Schritten verringert und automatisch Regeln hinzugefügt werden, wenn nötig (abhängig von der Art der Aktion und der verwendeten Netzwerke).

In diesem Buch legen wir alle Beispiele, Beschreibungen und Abbildungen immer auf der Basis von IP-Regeln statt auf IP-Richtlinien aus, weil wir so viel detaillierter die Regeln-Funktionalität des cOS-Cores beschreiben können.

IP-Regel-Aktionen

Wenn Sie eine IP-Regel erzeugen, können verschiedene Aktionen ausgewählt werden, wie im nächsten Bildschirmfoto gezeigt.

Name	Description
Drop	Drop the packet silently
Reject	Drop the packet and respond with an ICMP error or TCP reset
Allow	Stateful connection creation
NAT	Dynamic Address Translation (hide)
Forward fast	Stateless packet forwarding
SAT	Static Address Translation
SLB SAT	Server Load Balancing using Static Address Translation
Multiplex SAT	Multiplex Static Address Translation
Goto	Go to another rule set
Return	Return to the previous rule set

Abbildung 1.2.2 IP-Regel-Aktionen

Eine Aktion legt fest, wie der cOS-Core die fragliche IP-Regel behandeln soll. Soll sie die Quell- IP oder das Netzwerk des Clients verbergen, indem sie Netzwerk- Adress-übersetzung (NAT, Network Address Translation) verwendet? Oder soll es vielleicht den Datenverkehr abstellen, ohne den Client zu benachrichtigen (Verwerfen)?

Die meistgebrauchte IP-Regel ist die nachfolgende:

- **Zulassen**

  Eine Erlauben-Aktion bedeutet, dass wir den Datenverkehr von einer definierten Quell-Schnittstelle und einem Quell-Netzwerk zur Ziel-Schnittstelle und zum Ziel-Netzwerk zulassen, ohne die Quell-IP des sich verbindenden Clients maskieren.

- **NAT** (Netzwerk-Adressübersetzung, Network Address Translation)

  Eine NAT-Aktion bedeutet, dass wir den Datenverkehr von einer definierten Quell-Schnittstelle und einem Quell-Netzwerk zur Ziel-Schnittstelle und zum Ziel-Netzwerk zulassen, aber die Quell-IP des Datenverkehrs dabei maskieren. Diese Aktion wird üblicherweise verwendet, wenn Clients mit privaten IP-Adressen ins Internet gehen wollen, so dass ihre Quell-IP-Adressen geändert werden müssen, bevor sie den cOS-Core verlassen.

- **SAT** (Statische Adressübersetzung, Static Address Translation)

  Eine SAT-Aktion bedeutet, dass wir den Datenverkehr von einer definierten Quell-Schnittstelle und einem Quell-Netzwerk zu der Ziel-Schnittstelle (oder dem Ziel-Netzwerk, aber meistens wird es nur für einzelne IPs genutzt) zulassen, aber dabei die

Ziel-IP in etwas anderes übersetzen. Dies wird manchmal auch *Port-Weitergabe (Port Forwarding)* genannt. Eine SAT-Regel benötigt immer eine dazugehörige Erlauben-, NAT- oder FwdFast-Regel, um den Datenverkehrsfluss zu erlauben. (Im weiteren Verlauf des Buches werden wir dies noch weiter vertiefen.) Diese Art von Regel wird normalerweise benutzt, um Zugang von außen auf interne Ressourcen zu gewähren, wie z.B. einen Webserver.

- **Verwerfen** und **Ablehnen**

  Eine Verwerfen-Aktion verwirft das Datenpaket von der definierten Quell-Schnittstelle und dem Quell-Netzwerk auf dem Weg zur Ziel-Schnittstelle und dem Ziel-Netzwerk, ohne dem Client mitzuteilen, dass das Datenpaket verworfen wurde. Eine Ablehnen-Aktion kann verwendet werden, wenn der Client informiert werden sollte, dass ein Ziel-Dienst nicht erreichbar ist. Aus der Sicherheitsperspektive gesehen empfiehlt es sich, „Ablehnen" statt „Verwerfen" zu nutzen, weil es normalerweise besser ist, überhaupt nichts zu sagen, statt dem Client mitzuteilen, dass da eventuell irgendwas los war.

- **FwdFast** (Beschleunigt, Forward Fast)

  Im Vergleich zu allen anderen Aktionen ist dies eine sogenannte „statuslose Aktion". Das bedeutet, dass der cOS-Core den Datenverkehr zulässt, aber weder einen Verbindungsstatus zwischen Quelle und Ziel erzeugt noch beobachtet. Da der cOS-Core den Verbindungsstatus für die Beschleunigt-Aktion nicht beobachtet, werden Datenpakete ebenfalls nicht wie üblich überprüft, wie z.B. TCP-Sequenznummern, Verbindungsstatus usw. Diese Regel wird hauptsächlich dann genutzt, wenn irgendwas im Netzwerk nicht richtig funktioniert, aber eine auf jeden Fall funktionierende Regel benötigt. „Beschleunigt" benötigt normalerweise zwei Regeln, um zu funktionieren, und zwar je eine Beschleunigt-Regel in jeder Richtung, da ja eben weder Verbindung noch Status kontrolliert werden.

  Anders, als ihr Name andeutet, ist eine Beschleunigt-Regel nicht schneller als andere Regelarten, weil sie für jedes Datenpaket eine Regel-Suche durch cOS-Core benötigt, was mehr System-Ressourcen benötigt als eine Regel mit Statuskontrolle, wie z.B. eine Erlauben-Regel.

Im weiteren Verlauf des Buches werden wir auch andere Regel-Aktionen erläutern.

1.3. Einführung in Routing

IP-Routing ist eine der grundlegendsten Funktionen des cOS-Cores. Jedes IP-Datenpaket, das durch eine Clavister-Firewall der nächsten Generation fließt, wird an irgendeinem Punkt im Laufe der Zeit von mindestens einer Routing-Entscheidung betroffen sein. Korrekt eingestellte Routen sind entscheidend dafür, dass das System wie erwartet funktioniert.

Eine *Route* legt fest, wo ein Netzwerk sich befindet. Schauen wir uns die einfachste Definition einer Route an, in der eine Schnittstelle und ein Netzwerk gewählt wurden, wie im nachfolgenden Bildschirmfoto dargestellt.

Abbildung 1.3.1 Eine einfache Route

Hinweis

Es wird nicht empfohlen, eine Netzwerk-Adresse direkt einzugeben, aber in diesem Beispiel tun wir es trotzdem, damit das Beispiel leichter zu verstehen ist. Normalerweise würde ein Adressbuch-Objekt benutzt.

Im vorigen Bildschirmfoto teilen wir dem cOS-Core mit, dass wir die LAN-Schnittstelle nutzen müssen, um Hosts im Netzwerk 192.168.50.0/24 zu finden. Wenn Sie Routen festlegen, tun Sie das so, als ob der cOS-Core Ihnen die folgende Frage stellt: „Ich möchte Netzwerk XXXX erreichen. Hinter welcher Schnittstelle kann ich es finden?“

1.4. Zwei wichtige cOS-Core-Prinzipien

Prinzip 1: Regel-Reihenfolge

Mit Regeln meinen wir IP-Regeln, Regeln für Benutzerauthentifizierung, für Remote-Verwaltung, Piping-Regeln und so weiter. Grundsätzlich also alles mit Bezug auf einstellbare Regeln, das festlegt, wie eine Funktion oder Eigenschaft sein soll. Das Hauptprinzip solcher Regeln ist, dass sie von oben nach unten gelesen und befolgt werden. Das bedeutet, dass der cOS-Core die entsprechende Regelliste durchgeht, bis es eine passende Regel findet. Wenn eine Regel gefunden wurde, hört die Suche auf.

Dadurch ist es sehr wichtig, dass unsere Regeln in der richtigen Reihenfolge angelegt sind. Um ein einfaches IP-Regel-Beispiel zu machen, haben wir zwei Regeln, die wie folgt aussehen:

	Name	L...	Src If	Src Net ▲	Dest If	Dest Net	Service
1	■ DropAll	✔	any	all-nets	any	all-nets	all_services
2	▶ NAT_Dns	✔	Lan	Lannet	Wan	all-nets	dns-all

Abbildung 1.4.1 Problematische IP-Regel-Reihenfolge

In diesem Fall haben wir eine AllesVerwerfen-Regel an Regelposition #1 und eine neue Regel an Position #2, die DNS-Anfragen von der LAN-Schnittstelle und dem LAN-Netzwerk zulässt. Die zweite Regel #2 in diesem Szenario wird niemals erreicht werden, weil die Regel davor zuerst zutrifft und den Datenverkehr verwirft. Nachdem eine passende Regel gefunden wurde, werden keine weiteren Regeln beachtet.

Indem wir die neue DNS-Regel über die AllesVerwerfen-Regel schieben, wie im nächsten Bildschirmfoto gezeigt, beheben wir das Problem.

▲	Name	L...	Src If	Src Net	Dest If	Dest Net	Service
1	▶ NAT_Dns	✔	Lan	Lannet	Wan	all-nets	dns-all
2	■ DropAll	✔	any	all-nets	any	all-nets	all_services

Abbildung 1.4.2 Richtige IP-Regel-Reihenfolge

Probleme in IP-Regelsätzen entdecken

Das Verständnis, wie die Regeln gelesen werden, ist sehr wichtig, weil es ansonsten dazu führen kann, dass wir unser Netzwerk unbeabsichtigt sowohl für hereinkommende als auch für hinausgehende Verbindungen öffnen. Wenn wir uns die AllesVerwerfen-Regel im nächsten Bildschirmfoto ansehen und sie von links nach rechts lesen, sehen wir, dass folgende Treffer auftreten:

	Name	L...	Src If	Src Net ▲	Dest If	Dest Net	Service
1	■ DropAll	✔	any	all-nets	any	all-nets	all_services
2	▶ NAT_Dns	✔	Lan	Lannet	Wan	all-nets	dns-all

Abbildung 1.4.3 Problematische IP-Regel-Reihenfolge

- Die Quell-Schnittstelle ist eingestellt als **Irgendwas**. Treffer? Ja.
- Das Quell-Netzwerk ist eingestellt als **alle-Netze**. Treffer? Ja.
- Die Ziel-Schnittstelle ist eingestellt als **Irgendwas**. Treffer? Ja.
- Das Ziel-Netzwerk ist eingestellt als **alle-Netze**. Treffer? Ja.
- Der Netzwerk-Dienst ist eingestellt als **alle_Dienste**. Treffer? Ja.

Also wurden alle Kriterien für einen Regel-Treffer erfüllt und die Regel wird angewendet, in diesem Falle also den Datenverkehr verwerfen. cOS-Core wird nicht nach weiteren Regel-Treffern suchen, weil er gefunden hat, was er gesucht hat, anhand der Definition, wo der Datenverkehr empfangen wurde, wohin er ging und welcher Port (oder welches Protokoll) dafür genutzt wurde.

Prinzip 2: Routing

Wenn eine Routingtabelle ausgewertet wird, ist die Reihenfolge der Routen nicht wichtig. Stattdessen werden alle Routen in der entsprechenden Routingtabelle ausgewertet und die „kleinste" Route wird verwendet. Um „kleinste" zu verstehen, nehmen wir an, wir hätten die folgenden zwei Routen:

1. *Schnittstelle=LAN Netzwerk=10.10.10.0/24*
2. *Schnittstelle=DMZ Netzwerk=10.10.10.0/16*

Die erste Route wird als kleiner angenommen und kann daher den ersten Treffer ergeben.

Ein sehr häufiger Protokoll-Eintrag in Bezug auf Routing-Probleme ist ein Protokoll-Ereignis, das den Text „Default_Access_Rule“ (Standard_Zugangsregel) enthält. Das tritt dann im obigen Szenario auf, wenn Datenverkehr von der IP-Adresse 10.10.10.10 an der DMZ-Schnittstelle empfangen wird, weil das LAN-Netzwerk (/24) kleiner als das DMZ-Netzwerk (/16) und das kleinere Netzwerk vorrangig ist.

Wenn Datenverkehr an einer Schnittstelle ankommt, an der der cOS-Core ihn nicht erwartet, wird der Datenverkehr ebenfalls verworfen und eine Protokoll-Ereignisnachricht „Default_Access_Rule“ erzeugt.

Route-Metrik verwenden

Die *Route-Metrik* kann benutzt werden, um dem cOS-Core mitzuteilen, welche Route er verwenden soll, falls es mehrere identische Routen gibt. Der Metrikwert wird als ein Parameter einer Route eingestellt.

1. *Schnittstelle=Wan1 Netzwerk=alle-Netze Gateway=ISP1-GW Metrik=50*
2. *Schnittstelle=Wan2 Netzwerk=alle-Netze Gateway=ISP2-GW Metrik=100*

In diesem Beispiel sind die Schnittstellen unterschiedlich, aber das Netzwerk ist identisch. Indem wir der vorrangigen Route für die Schnittstelle Wan1 einen niedrigeren Metrikwert zuweisen, teilen wir dem cOS-Core mit, dass es im Falle eines Netzwerk-Konflikts diese Route anstelle der Wan2-Schnittstelle-Route nehmen soll.

Hinweis

Eine identische Route mit der gleichen Metrik kann ganz normal vorkommen, wenn sie in Verbindung mit Server-Lastverteilung genutzt wird. Server-Lastverteilung wird in einem späteren Kapitel besprochen.

Identische Routen mit der gleichen Metrik

Ein anderes übliches Szenario, das auftreten kann, ist eine Situation, in der sowohl die Route als auch die Metrik identisch sind, wie in diesem Beispiel:

1. *Schnittstelle=Wan1 Netzwerk=alle-Netze Gateway=ISP1-GW Metrik=100*
2. *Schnittstelle=Wan2 Netzwerk=alle-Netze Gateway=ISP2-GW Metrik=100*

In diesem Beispiel wird der cOS-Core nicht in der Lage sein, zu entscheiden, welche der beiden Routen er nehmen soll. Ihre Netzwerk-Größe ist identisch und die Metriken sind ebenfalls gleich. Der Administrator möchte, dass der cOS- Core Wan1 als vorrangige Internetprovider- Schnittstelle benutzt, und es könnte sein, dass diese bestimmte Einstellung Monate lang problemlos funktioniert, bis sie ganz plötzlich nicht mehr weiterläuft.

Der Grund dafür ist, dass der cOS-Core, weil er nicht in der Lage ist, zu entscheiden, welche Route er nutzen soll, zufällig eine der beiden nutzt. Nach einem System-Neustart kann es eine andere Route wählen, so dass wir fälschlicherweise annehmen könnten, alles funktioniert prima und alles sei korrekt eingestellt.

Damit wir dieses Problem richtig angehen können, müssen wir entweder die Metrik der primären oder der sekundären Route ändern. Falls wir möchten, dass Wan1 (in diesem Szenario) die vorrangige Schnittstelle in Richtung Internetprovider ist, müssen wir ihre Metrik so einstellen, dass sie niedriger als die der Wan2-Schnittstelle-Route ist, so wie hier:

1. *Schnittstelle=Wan1 Netzwerk=alle-Netze Gateway=ISP1-GW Metrik=50*
2. *Schnittstelle=Wan2 Netzwerk=alle-Netze Gateway=ISP2-GW Metrik=100*

1.5. Kommentargruppen benutzen

Es wird dringend empfohlen, Kommentargruppen zu benutzen, um Objekte und Regeln unterscheiden zu können. Wenn Sie Gruppen mit verschiedenen Farben und Gruppierungen nutzen, hilft dies ungemein, größere Konfigurationen zu lesen. Wir empfehlen, das Adressbuch, Regeln, Routen und so weiter in Gruppen zu strukturieren, und zwar schon so früh wie möglich.

Um eine neue Kommentargruppe hinzuzufügen, wählen Sie das erste Objekt, das Teil der neuen Gruppe sein soll, machen Sie einen Rechtsklick und wählen Sie **Neue Gruppe**. Das Beispiel im nächsten Bildschirmfoto zeigt, wie dies im Adressbuch gemacht wurde.

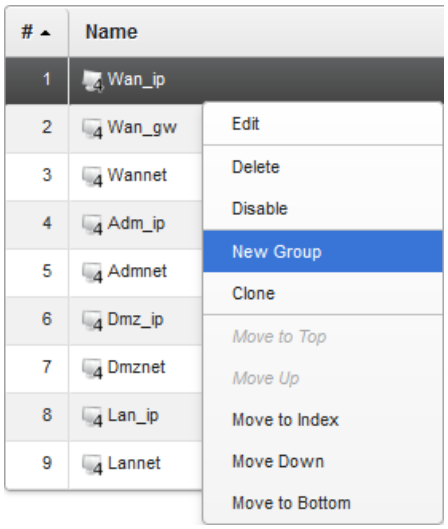


Abbildung 1.5.1 Neue Kommentargruppe hinzufügen

Bevor Sie Kommentargruppen hinzufügen, kann es sein, dass das Adressbuch etwa so wie im nachfolgenden Bildschirmfoto aussieht.

#	Name	Address
1	Wan_ip	203.0.113.10
2	Wan_gw	203.0.113.1
3	Wannet	203.0.113.0/24
4	Adm_ip	192.168.98.14
5	Admnet	192.168.98.0/24
6	Dmz_ip	192.168.99.1
7	Dmznet	192.168.99.0/24
8	Lan_ip	192.168.100.1
9	Lannet	192.168.100.0/24

Abbildung 1.5.2 Adressbuch ohne Strukturierung durch Kommentargruppen

Wenn für alle Objekte, die Teil einer Gruppe sind, eine bestimmte Farbe festgelegt wird, ist es viel leichter, das Adressbuch zu lesen.

#	Name	Address
WAN Interface Objects		
1	Wan_ip	203.0.113.10
2	Wan_gw	203.0.113.1
3	Wannet	203.0.113.0/24
ADM Interface Objects		
4	Adm_ip	192.168.98.14
5	Admnet	192.168.98.0/24
DMZ Interface Objects		
6	Dmz_ip	192.168.99.1
7	Dmznet	192.168.99.0/24
Lan Interface Objects		
8	Lan_ip	192.168.100.1
9	Lannet	192.168.100.0/24

Abbildung 1.5.3 Adressbuch mit Strukturierung durch Kommentargruppen

Kapitel 2: Grundeinstellung

Dieses Kapitel beschreibt, wie Sie die Grundkonfiguration des cOS-Cores ausführen, um Internetzugang zu erhalten und grundsätzliche Routing- und IP-Regeln einrichten.

Das Ziel dieses Kapitels ist, in die Konfiguration des cOS-Cores einzusteigen und mit der Internet-Oberfläche (WebUI) und verschiedenen anderen Aspekten der grundsätzlichen Einstellungsmöglichkeiten vertraut zu werden, wie z.B. Regeln für Remote-Verwaltung, Lizensierung, Firmware-Aktualisierungen, das Erlauben hinausgehender Verbindungen und mehr.

Die Clavister-Firewall der nächsten Generation, die hier verwendet wird, hat vier physische Schnittstellen, die die logischen Namen WAN, LAN, DMZ und ADM haben.

Netzwerk-Diagrammsymbole

Wenn wir die Rezepte in diesem Buch durcharbeiten, werden wir Netzwerk-Diagramme betrachten, die das jeweilige Szenario versinnbildlichen, das wir besprechen.

Die Netzwerk-Diagramme verwenden jeweils dieselben Symbole die nachfolgend in *Abbildung 2.1* gezeigt werden, jeweils mit einer kurzen Beschreibung, wofür sie stehen.

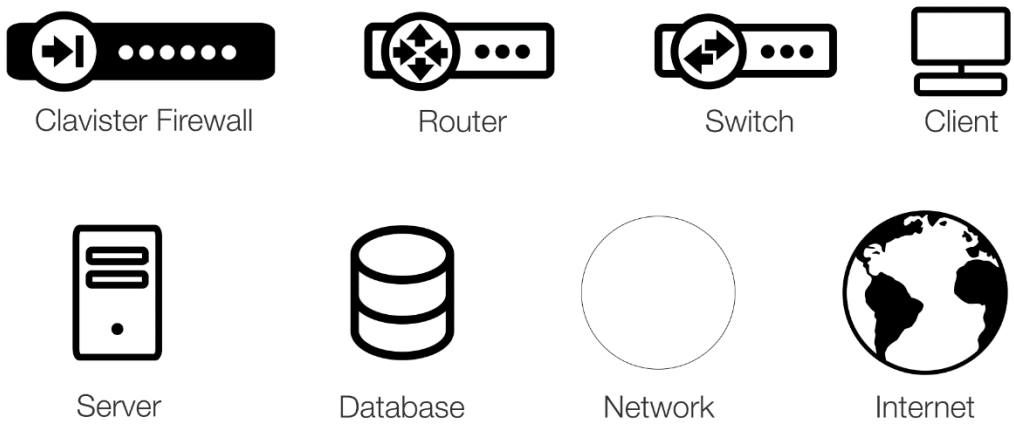


Abbildung 2.1 Kochbuch-Diagrammsymbole

Rezept 2.1. Einfache Installation, Lizensierung, Sicherheitskopien und Firmware-Aktualisierungen

Ziele

Das Ziel dieses Rezepts ist, Verwaltungszugang zur Clavister-Firewall der nächsten Generation zu erhalten, um die Regeln für Remote-Verwaltung zu überprüfen, eine Lizenz in der Firewall zu installieren und eine Firmware-Aktualisierung durchzuführen.

Detailbesprechung

Wenn Sie das System zum ersten Mal hochfahren, stellt der cOS-Core automatisch einen Verwaltungszugang auf einer voreingestellten einzelnen Ethernet-Schnittstelle bereit und weist dieser die private IPv4-Adresse 192.168.1.1 zu. Die erste Schnittstelle wird normalerweise für die Verbindung zur Verwaltung-Workstation benutzt.

Diese Verwaltungsschnittstelle ist in der vollständigen Schnittstellenliste mit **if1** beschriftet, die nachfolgend in *Tabelle 2.1.1* gezeigt wird.

Schnittstellenname	IP-Adresse
Core	127.0.0.1
if1	192.168.1.1
if2	127.0.1.1
if3	127.0.2.1
if4	127.0.3.1

Tabelle 2.1.1 Die standardmäßige Verwaltungsschnittstelle

Sie können eine Verbindung zum cOS-Core mit einer der folgenden Methoden herstellen:

- Netzwerkverbindung mit dem WebUI über HTTP (TCP Port 80).
- Netzwerkverbindung mit dem WebUI über verschlüsseltes HTTPS (TCP Port 443).
- Netzwerkverbindung mit der Kommandozeile des cOS-Cores über SSH (TCP Port 22).
- Direkte Verbindung zur Kommandozeile des cOS-Cores über den Konsole-Port der Firewall.

Hinweis

Die Konfiguration von Zentralverwaltung und -Zugang werden in diesem Buch weder besprochen noch genutzt.

Standard-Verwaltung-IP und -Netzwerk mittels Kommandozeile ändern

Die standardmäßige IP-Adresse und das Netzwerk, wie in der Verwaltungsschnittstelle eingestellt, entsprechen nicht immer dem, was der Administrator möchte. Wenn der sich verbindende Client nicht Mitglied des 192.168.1.0/24-Netzwerks ist und sich mit der ersten Schnittstelle verbindet, sind weder WebUI- noch SSH-Zugang möglich, bis dies geändert wurde.

Der einzige Weg, dies zu ändern, führt über die Kommandozeile auf der lokalen Konsole. Wir werden hier die Verwendung und Funktionalität der Kommandozeile nicht weiter vertiefen, weil sich der Großteil des Buches auf das WebUI bezieht.

Weil diese Frage häufig auftaucht, werden wir nachfolgend die beiden grundsätzlichen Kommandozeile-Befehle aufführen, die Sie benötigen, um die standardmäßige IP-Adresse und das Netzwerk in der Verwaltungsschnittstelle zu ändern, sowie die Regeln für Remote-Verwaltung zu aktualisieren, um Zugang von unserem neuen Netzwerk zu erlauben.

```
Gerät:/> set Interface Ethernet if1 IP=192.168.98.14 Net-
work=192.168.98.0/24
```

```
 Gerät:/> set RemoteManagement RemoteMgmtHTTP rmgmt_http Net-
work=192.168.98.0/24 Interface=if1
```

Weitere Informationen über die Kommandozeile finden Sie im Referenzhandbuch „cOS-Core-Kommandozeile“.

Verbindung zum WebUI

Um eine Verbindung zum WebUI herzustellen, öffnen Sie einen Browser wie Firefox, Chrome oder Opera und geben Sie die IP-Adresse der Verwaltungsschnittstelle ein. In unserem Setup wird dies 192.168.98.14 sein, wie im nächsten Bildschirmfoto gezeigt.

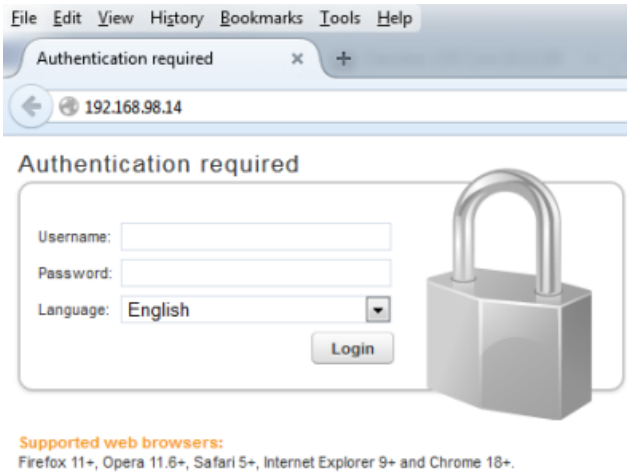


Abbildung 2.1.2 Der Login-Dialog des cOS-Cores

Die voreingestellte Angabe sowohl für Login und Passwort einer neuen Installation ist „**admin**“.

Regeln für Remote-Verwaltung

Sobald wir Zugang zum WebUI haben, empfiehlt es sich, die aktuellen Verwaltung-Zugangsregeln zu überprüfen. Diese Regeln kontrollieren die Zugangslevels zu WebUI, SSH und InControl und legen fest, von welchen Schnittstellen und Netzwerken Clients sich verbinden dürfen, um den COS-Core zu verwalten.

Die Regeln für Remote-Verwaltung finden Sie im WebUI unter **System > Remote-Verwaltung**.

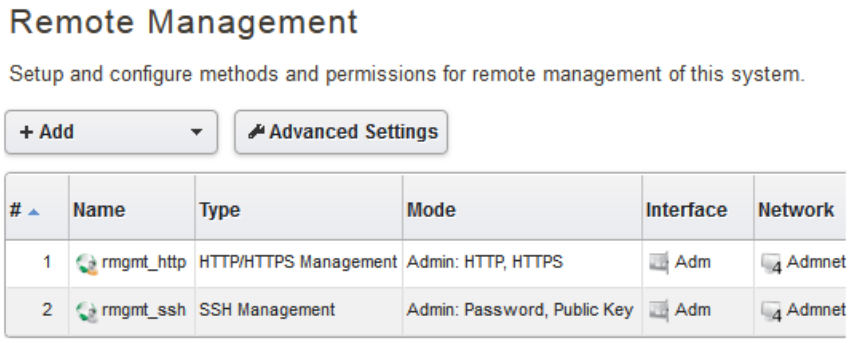


Abbildung 2.1.3 Regeln für Remote-Verwaltung

In den weiter oben gezeigten Regeln haben wir den Verwaltungszugang mithilfe von HTTP, HTTPS (Regel **1**) und SSH (Regel **2**) von der ADM-Schnittstelle und dem Admnet-Netzwerk eingestellt, der 192.168.98.0/24 im Adressbuch entspricht. Mit diesen Regeln für Remote-Verwaltung haben wir jetzt begrenzten Zugang; der einzige Weg, um sich zu verbinden und das Verwaltung-WebUI zu erreichen (und SSH zu benutzen) ist momentan, Teil des Admnet-Netzwerks zu sein und sich hinter der ADM-Schnittstelle zu befinden.

Wenn wir versuchen, uns von einer anderen Schnittstelle oder einem anderen Netzwerk mit dem WebUI zu verbinden, wird der Zugang verweigert. Dem Client wird keine Login-Eingabe angeboten, weil der cOS-Core aktiv die Verbindung verwirft, ohne dem Client irgendeine Rückmeldung zu geben, da der Benutzer keinen Zugang zur Remote-Verwaltung hat.

Verwaltungszugang weiter beschränken

In vielen Szenarios wird die Firewall an Schlüsselpositionen im Netzwerk platziert, so dass es wichtig ist, sicherzustellen, dass kein unautorisierter Zugang erlaubt wird. Um die Sicherheit weiter zu erhöhen, werden wir zwei Dinge tun:

1. HTTP-Verwaltungszugang abschalten

2. HTTPS-Port auf irgendetwas anderes ändern.

HTTP ist unverschlüsselter Datenverkehr, was bedeutet, dass das Passwort leicht erhalten werden kann, indem man die Datenpakete zwischen dem Verwaltungs-PC und der Clavister-Firewall erfasst. Es gibt keinen Grund, unverschlüsselte Kommunikation zwischen dem Verwaltung-Client und der Firewall zu erlauben.

Den standardmäßigen HTTPS-Verwaltungsport 443 auf irgendetwas anderes zu ändern, ist zudem eine gute Idee, um von den Standard-Ports abzuweichen, selbst wenn der Datenverkehr verschlüsselt ist.

Um die HTTP-Verwaltung abzuschalten, öffnen wir die Regel für Remote-Verwaltung namens „rmgmt_http" und entfernen den Haken bei HTTP, wie im nachfolgenden Bildschirmfoto gezeigt.

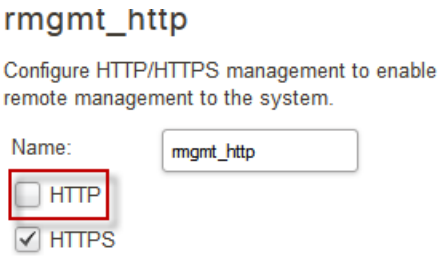


Abbildung 2.1.4 HTTP/HTTPS-Optionen

Um den HTTPS-Port zu ändern, gehen Sie zu **System > Remote-Verwaltung > Erweiterte Einstellungen** und ändern Sie den HTTPS-Port in den gewünschten Port, wie nachfolgend gezeigt. In diesem Kapitel lassen wir den Port 443 wie voreingestellt.

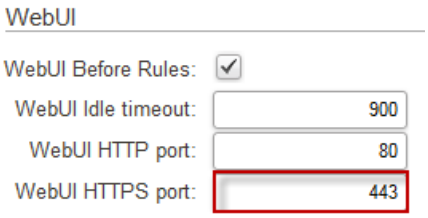


Abbildung 2.1.5 HTTPS-Port ändern

Demo-Modus und cOS-Core-Lizenzen

Wenn ein Clavister-Firewall der nächsten Generation hochfährt, hat es keine Lizenz (falls sie nicht vorher installiert wurde). Ohne Lizenz läuft der cOS-Core für zwei Stunden im Demo-Modus. Im Demo-Modus kann die Firewall zum Testen und Ausprobieren genutzt werden, aber einige Eigenschaften haben eingeschränkte Funktionalität. Obwohl die meisten Rezepte und Lösungen aus diesem Buch sogar ohne Lizenz eingestellt werden könnten, gehen wir davon aus, dass eine gültige Lizenz installiert worden ist.

Sobald der zweistündige Demo-Modus abgelaufen ist, wird die Firewall gesperrt und erfordert einen Neustart, um weitere zwei Stunden genutzt werden zu können.

Der Zweck einer Lizenz ist, festzulegen, welche Fähigkeiten und Einschränkungen der cOS-Core hat. Solche Fähigkeiten umfassen solche Parameter wie die erlaubte Anzahl der VPN-Tunnel und die Höchstanzahl der Routingtabellen.

Es gibt verschiedene Wege, eine Lizenz zu installieren:

1. Automatische Aktivierung über das WebUI.
2. Manuelle Aktivierung und Hochladen über das WebUI.
3. Manuelle Aktivierung und Hochladen über die Kommandozeile.
4. Manuelle Aktivierung und Hochladen über InControl.

In dieser Übung werden wir Methode **2** benutzen, weil die automatische Aktivierung in virtuellen Umgebungen wie VMware™ nicht möglich ist und es unser Ziel ist, in diesem Buch plattformunabhängig zu sein.

Lizenzregistrierung und Hochladen

Um eine Lizenz zu registrieren, brauchen Sie Zugang zu www.clavister.com und müssen sich entweder mit einem existierenden Konto einloggen oder, falls Sie Neukunde sind, ein neues Konto anlegen.

Sobald Sie ein Konto haben und eingeloggt sind, gehen Sie zum Lizenz-Abschnitt Ihres Kontos und geben die erforderlichen Daten wie den Lizenzschlüssel oder das Dienst-Etikett ein, je nachdem, welche Art von Lizenz Sie haben. Ältere Clavister-Firewalls nutzen einen Lizenzschlüssel und eine MAC-Adresse zum Registrieren, während neuere Firewalls eine Kombination aus Dienst-Etikett und Hardware-Seriennummer zur Registrierung nutzen.

Sobald alle Schritte zur Registrierung einer Lizenz vollständig sind, können wir die Lizenzdatei herunterladen. Die Lizenzdatei hat das Format „<lizenz-schluessel>.lic“.

Es gibt zwei WebUI-Orte, an denen wir eine Lizenzdatei zum cOS-Core hochladen können:

- **Status > Wartung > Lizenz**
- **Status > Wartung > Upgrade**

Suchen Sie auf der Festplatte nach dem Speicherort Ihrer heruntergeladenen Lizenzdatei und klicken Sie [Lizenz hochladen]. Sobald die Lizenz hochgeladen ist, werden zwei Optionen angeboten:

- cOS-Core beenden und neustarten (empfohlen).
- Beenden und *Neueinstellung* ausführen.

Eine Neueinstellung ist ähnlich dem Neustart, wenn eine geänderte Konfiguration bereitgestellt wird. Es ist ein Warmstart, der wesentlich schneller als ein vollständiger Neustart des cOS-Cores abläuft. Der Grund, warum ein Neustart empfohlen wird, ist, dass Speicher für bestimmte Parameter (z.B. VPN-Tunnel) nur nach einem Neustart zugewiesen wird. Für eine ordnungsgemäße Funktionalität wird daher ein Neustart empfohlen.

Rezept 2.2. Einstellung und System-Sicherheitskopien herunterladen

Ziele

Konfiguration-Sicherheitskopien sind sehr wichtig für jeden Systemadministrator. In der Lage zu sein, ein vollständiges Abbild der Konfiguration zu erstellen, kann sehr nützlich sein und ebenfalls dazu verwendet werden, eine Konfiguration von einer Clavister-Firewall zu einer anderen zu übertragen. Dieses Rezept beschäftigt sich mit diesen Aufgaben.

Detailbesprechung

Es wird dringend empfohlen, in regelmäßigen Abständen Sicherheitskopien der Konfiguration und des Systems zu machen. Die Sicherheitskopie-Funktion im cOS-Core finden Sie unter **Status > Wartung > Sicherheitskopie & Wiederherstellung** im WebUI.

Es gibt zwei Arten von Sicherheitskopien, die erstellt werden können:

- Konfiguration-Sicherheitskopie.
- System-Sicherheitskopie.

Eine *Konfiguration-Sicherheitskopie* besteht nur aus der cOS-Core-Konfiguration; der cOS-Core selbst ist nicht enthalten. Eine *System-Sicherheitskopie* besteht aus der Konfiguration, dem cOS-Core-Lader und der ausführbaren cOS-Core-Firmware. Es ist sehr nützlich, eine vollständige System-Sicherheitskopie zu haben, bevor wir uns an Firmware-Aktualisierungen versuchen, weil wir dann leicht und rasch den vorherigen cOS-Core-Status wiederherstellen können, falls nötig.

Falls wir eine cOS-Konfiguration nach einem Hardware-Austausch auf einer neuen Clavister-Firewall klonen wollen, ist es wichtig, sich zu erinnern, dass die Lizenzdatei niemals in irgendwelchen Sicherheitskopie-Dateien enthalten ist.

cOS-Core-Aktualisierung durchführen

Es ist wichtig, den cOS-Core immer mit der letzten Patch- oder Release-Version aktuell zu halten, um unser Netzwerk sicher zu halten, weil Clavister fortwährend den cOS-Core verbessert und aktualisiert.

Es ist gut möglich, dass die auf der neuen Clavister-Hardware vorinstallierte cOS-Coreversion bereits eine Aktualisierung benötigt. Aufgrund der sensiblen Natur dessen, wo der cOS-Core in einem Netzwerk installiert ist (üblicherweise an einem zentralen Punkt), gibt es keine automatische Aktualisierung des cOS-Cores. Alle Aktualisierungen müssen von Hand durch den Administrator durchgeführt werden.

Neue Firmware-Aktualisierungen und -Versionen werden nach dem Registrieren und Einloggen von der Clavister-Firmenwebsite heruntergeladen. Sobald Sie sich in Ihr Nutzerkonto eingeloggt haben, wählen Sie die neue cOS-Coreversion, die Sie installieren wollen, und laden Sie die passende Datei herunter, die zu Ihrer Hardware passt. Upgrade-Dateien haben das Dateisuffix *.UPG*.

Firmware-Upgrades werden durchgeführt, indem Sie im WebUI **System > Wartung > Upgrade** aufrufen, wie nachfolgend gezeigt.

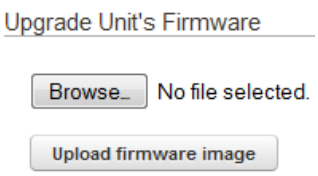


Abbildung 2.2.1 Firmware hochladen

Wichtig

Bevor Sie irgendeine Firmware-Aktualisierung durchführen, wird dringend empfohlen, zunächst eine vollständige System-Sicherheitskopie anzufertigen. Jede neue cOS-Coreversion wird immer ausführlichen Tests unterzogen, um Probleme zu vermeiden, aber es kann neue Eigenschaften und Funktionen geben, die im Verhalten der Firewall Unterschiede zeigen.

Bevor Sie ein cOS-Core-Upgrade durchführen, stellen Sie sicher, dass Sie die Anmerkungen zu der neuen Version gelesen haben. Es können sich Änderungen ergeben haben, die Ihre besondere Aufmerksamkeit verlangen, nachdem das Upgrade durchgeführt wurde.

Weil eine vollständige System-Sicherheitskopie sowohl Konfigurations- als auch Firmware-Dateien enthält, ist sie die schnellste Möglichkeit, den vorherigen Status der Firewall wiederherzustellen.

Rezept 2.3. Internet-Zugang für Administratoren

Ziele

Der Zweck dieses Rezepts ist es, dem Administrator aus dem Verwaltung-(admnet)-Netzwerk Internet-Zugang zu gewähren. Dieser Zugang wird in der nachfolgenden *Abbildung*

2.3.1 illustriert.

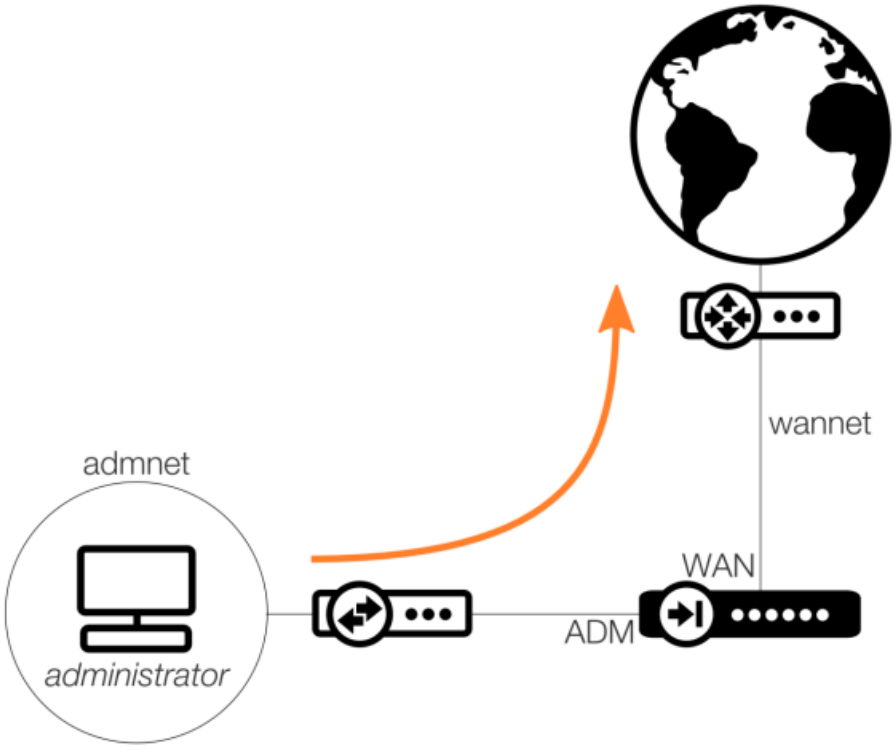


Abbildung 2.3.1 ADM-zu-WAN-Netzwerk-Schema mit Datenverkehr-Richtungspfeil

Detailbesprechung

Zuerst müssen wir festlegen, welche IP und welches Netzwerk wir für unsere verschiedenen Schnittstellen verwenden wollen.

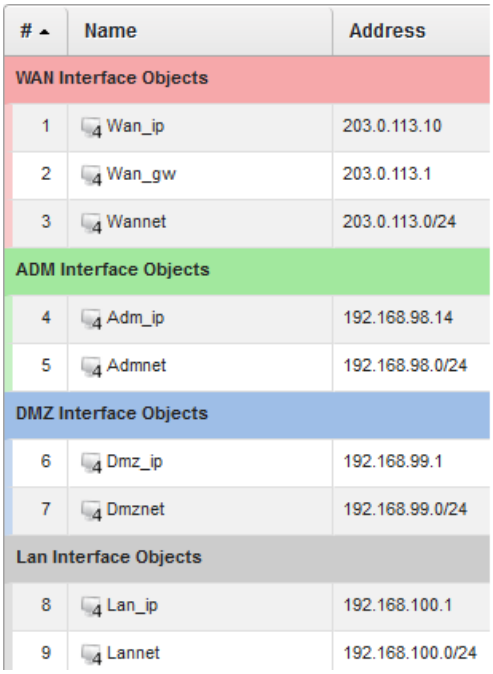
In unserem Beispiel verwenden wir die folgenden Netzwerke für die verschiedenen Schnittstellen:

- **WAN** – 203.0.113.0/24
- **ADM** – 192.168.98.0.0/24
- **DMZ** – 192.168.99.0/24
- **LAN** – 192.168.100.0/24

Es ist üblich, die IP-Adresse zu wählen, die von der Schnittstelle selbst verwendet wird, und entweder die erste oder die letzte IP im Netzwerk-IP-Bereich zu nutzen (hauptsächlich, weil Clients hinter dem cOS-Core sie als ihr standardmäßiges Gateway nutzen werden).

Der Administrator hat nicht viel Kontrolle über die von seinem Internetdienstanbieter zugewiesenen IP-Adressen, und zudem kann es Situationen im eigenen internen Netzwerk geben, die uns zwingen, eine andere als die erste oder letzte IP-Adresse zu verwenden.

Im nachfolgenden Bildschirmfoto haben wir IP- und Netzwerk-Objekte erzeugt, die wir in den verschiedenen Schnittstellen nutzen werden. Auf diese verwendeten Objekte werden wir uns im weiteren Verlauf dieses Kapitels in Beschreibungen und Netzwerk-Schemata beziehen.



#	Name	Address
WAN Interface Objects		
1	Wan_ip	203.0.113.10
2	Wan_gw	203.0.113.1
3	Wannet	203.0.113.0/24
ADM Interface Objects		
4	Adm_ip	192.168.98.14
5	Admnet	192.168.98.0/24
DMZ Interface Objects		
6	Dmz_ip	192.168.99.1
7	Dmznet	192.168.99.0/24
Lan Interface Objects		
8	Lan_ip	192.168.100.1
9	Lannet	192.168.100.0/24

Abbildung 2.3.2 Adressbuch-Objekt-Zusammenfassung

Sobald alle benötigten Objekte und Netzwerke angelegt sind, gehen wir zum Abschnitt „Schnittstellen“ im WebUI und stellen sicher, dass alle Objekte der richtigen Schnittstelle zugewiesen sind, wie im nachfolgenden Bildschirmfoto dargestellt.

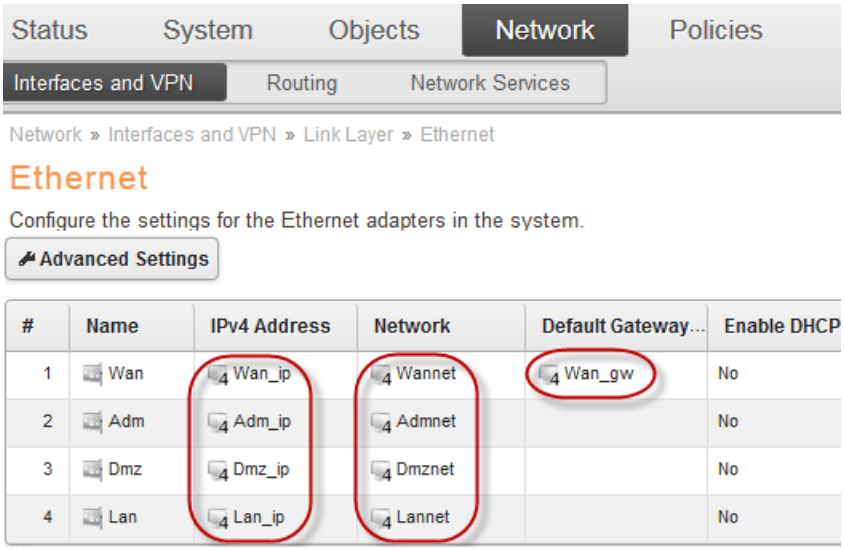


Abbildung 2.3.3 Schnittstelle-Objekt-Zuteilung

Bitte beachten Sie beim vorher Gesagten, dass es nur ein Objekt gibt, das als Standard-Gateway eingestellt wurde. Dies ist die Gateway-Adresse unseres Internetdienstanbieters (ISP, Internet Service Provider).

Sobald jedes Objekt der/den entsprechenden Schnittstelle(n) hinzugefügt ist, werfen wir einen raschen Blick auf die Routingtabelle. Auf der Grundlage unserer aktuellen Konfiguration sollte die Routingtabelle **main** wie im nachfolgenden Bildschirmfoto aussehen.

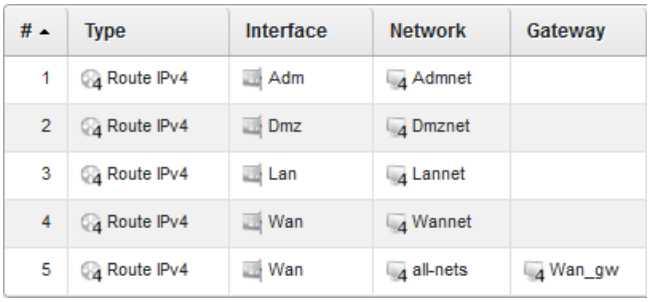


Abbildung 2.3.4 Routingtabelle-Zusammenfassung

Hinweis

Abhängig von der Anzahl der Schnittstellen und der Hardware-Plattform würde diese Routingtabelle natürlich anders aussehen.

Zwei Methoden, Routen hinzuzufügen

Es gibt zwei Wege, der Routingtabelle Routen hinzuzufügen. Ein Weg ist, die automatische Erzeugung von Routen in jeder Schnittstelle zu aktivieren, wie im nachfolgenden Bildschirmfoto gezeigt. Diese Optionen sind standardmäßig angehakt.

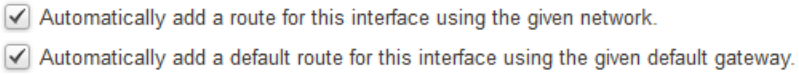


Abbildung 2.3.5 Optionen zu automatischen Erzeugung von Routen

Das bedeutet, wenn wir ein Netzwerkobjekt oder ein Gateway zu einem Objekt wie einer Ethernet-Schnittstelle hinzufügen, wird automatisch eine Route erzeugt und hinzugefügt.

Die andere Methode ist, in der Routingtabelle von Hand eine Route zu erzeugen. Einer der Nachteile beim Verwenden der automatisch erzeugten Routen ist, dass wir für diese Routen keine Kommentargruppen erzeugen können. Daher kann es sinnvoll sein, die Haken bei den obigen Optionen zu entfernen und die Routen von Hand zu erzeugen, damit wir Kommentargruppen nutzen können. In diesem Kapitel lassen wir die Optionen aber aktiviert, weil wir keine weiteren Änderungen an der Routingtabelle vornehmen werden.

IP-Regeln

Jetzt müssen wir den wichtigsten Teil des Rezepts herstellen, die IP-Regeln.

Abbildung 2.3.6 Vorrangiger Ort der IP-Regeln

Normalerweise gäbe es ein paar automatisch erzeugte IP-Regeln (wobei es davon abhängt, welche cOS-Coreversion wir nutzen, wie viele und wie sie konfiguriert sind). In diesem Buch gehen wir davon aus, dass der IP-Regelsatz leer ist und wir ihn von Grund auf neu erzeugen.

Um es nicht zu kompliziert zu machen, werden wir eine sehr großzügige IP-Regel anlegen, die allen Nutzern hinter der ADM-(Administratoren)-Schnittstelle erlaubt, sich mit beliebigen IPs an der externen WAN-Schnittstelle über irgendeinen Port und irgendein Protokoll zu verbinden.

Es wäre vernünftig, den Administratoren vorübergehend vollen externen Zugang zu geben, damit sie ins Internet gehen können, um Software-Aktualisierungen und andere Programme herunterladen können, die zur Vorbereitung benötigt werden, um das interne Netzwerk aufbauen und einstellen zu können. Wir sprechen von „vorübergehend", weil dieser Zugang im weiteren Verlauf mehr und mehr eingeschränkt werden wird.

Die IP-Regel, die wir jetzt erzeugen, hat die im nachfolgenden Bildschirmfoto gezeigten Eigenschaften.

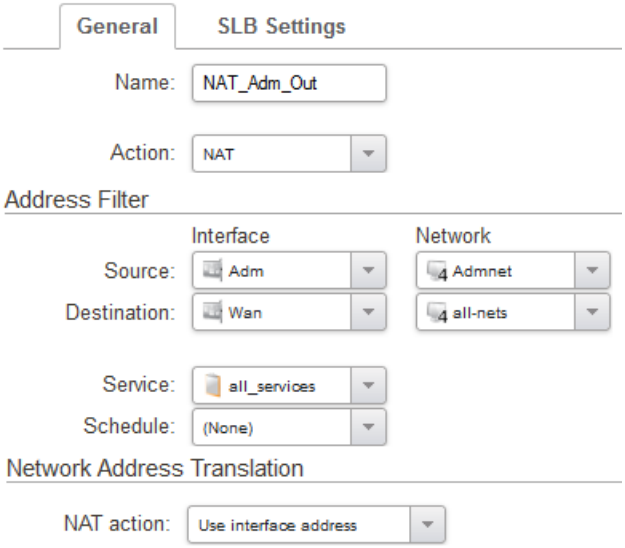


Abbildung 2.3.7 IP-Regel-Eigenschaften

Im weiteren Verlauf werden wir hauptsächlich die IP-Regel-Zusammenfassung verwenden, um IP-Regeln und ihre Eigenschaften zu beschreiben, sofern nicht spezielle Optionen genutzt werden. Die Regel-Zusammenfassung für die obige Regel sieht aus wie im nachfolgenden Bildschirmfoto.

Name	L...	Src If	Src Net	Dest If	Dest Net	Service	Address Translation
▶ NAT_Adm_Out	✔	Adm	Admnet	Wan	all-nets	all_services	SRC:NAT

Abbildung 2.3.8 Übersicht der IP-Regel-Zusammenfassung

Die Regel, die wir erzeugt haben, gewährt jedem vollen Zugang ohne jede Beschränkung, sobald er sich irgendwie mit der ADM-Schnittstelle verbunden hat; alle Ports und Protokolle sind erlaubt.

Es gibt eine weitere Regel, die wir gern erzeugen würden, bevor wir zum Ende dieses besonderen Rezepts kommen. Eine Regel namens „AllesVerwerfen“ mit den Eigenschaften, wie im nachfolgenden Bildschirmfoto gezeigt.

	Name	L...	Src If	Src Net	Dest If	Dest Net	Service	Address Translation
1	▶ NAT_Adm_Out	✔	Adm	Admnet	Wan	all-nets	all_services	SRC:NAT
2	■ DropAll	✔	any	all-nets	any	all-nets	all_services	

Abbildung 2.3.9 Die „AllesVerwerfen"-Regel

Unser AllesVerwerfen hat keinerlei Einschränkungen. Die Aktion ist so eingestellt, dass sie Verwerfen nutzt, Quell- und Ziel-Schnittstelle sind beliebig, Quell- und Ziel-Netzwerk sind alle Netze und die Dienst-Art ist „alle_dienste“. Das bedeutet alles auf allen Schnittstellen und Ports/Protokollen. Alles, was nicht von der ADM-Schnittstelle und dem ADM-Netz eingeleitet wird, wird von dieser Regel verworfen.

Warum sollte man eine AllesVerwerfen-Regel benutzen?

Ohne die AllesVerwerfen-Regel würde Datenverkehr, der nicht unserer neu erzeugten Regel entspricht, durchfallen bis zum letzten Eintrag des IP-Regelsatzes. Wenn dann immer noch nichts zu einem Treffer führt, wird der Datenverkehr durch eine versteckte, standardmäßige Verwerfen-Regel namens „Standard_Regel“ verworfen. Diese Regel ist identisch zu unserer AllesVerwerfen-Regel, aber der Vorteil, eine explizite AllesVerwerfen-Regel zu haben, ist, dass wir sie bewusster einsetzen können, ihr einen eindeutigen Namen geben, ihre Protokoll-Kategorie (falls nötig) ändern und außerdem Kommentargruppen nutzen können, um klarzustellen, das alles, was diese Regel erreicht, verworfen werden wird, wie nachfolgend dargestellt.

#	Name	L...	Src If	Src Net	Dest If	Dest Net	Service	Address Translation
Rules for the ADM interface.								
1	▶ NAT_Adm_Out	✔	Adm	Admnet	Wan	all-nets	all_services	SRC:NAT
Anything below this rule will be dropped!								
2	■ DropAll	✔	any	all-nets	any	all-nets	all_services	

Abbildung 2.3.10 Eine „AllesVerwerfen"-Regel mit Kommentargruppen

Die AllesVerwerfen-Regel ist nicht zwingend erforderlich, sie ist optional.

Wir empfehlen nochmals dringend, so früh wie möglich schon Kommentargruppen zu nutzen, um unsere IP-Regelsätze leichter lesbar und verständlicher zu machen. Momentan ist es noch leicht lesbar, aber wenn Sie erstmal hunderte oder sogar tausende Regeln und Objekte haben, wird es immer schwieriger.

Administratoren können jetzt das Internet auf allen von ihnen gewählten Quell- und Ziel-Ports oder -Protokollen erreichen.

Rezept 2.4. Die LAN-Schnittstelle für externen und internen Zugang einstellen

Ziele

Der Zweck dieses Rezepts ist, LAN-Nutzern Zugang zum Internet zu geben und außerdem Server hinter der DMZ-Schnittstelle erreichen zu können. Mit „LAN-Nutzer" meinen wir einen Nutzer, die sich hinter der LAN-Schnittstelle befinden. Diese Person kann ebenfalls *Client*, *Student* oder *Mitarbeiter* genannt werden. Die Mehrzahl der Leute, die das Netzwerk nutzen, wird sich hinter der LAN-Schnittstelle befinden, wie nachfolgend in *Abbildung 2.4.1* gezeigt.

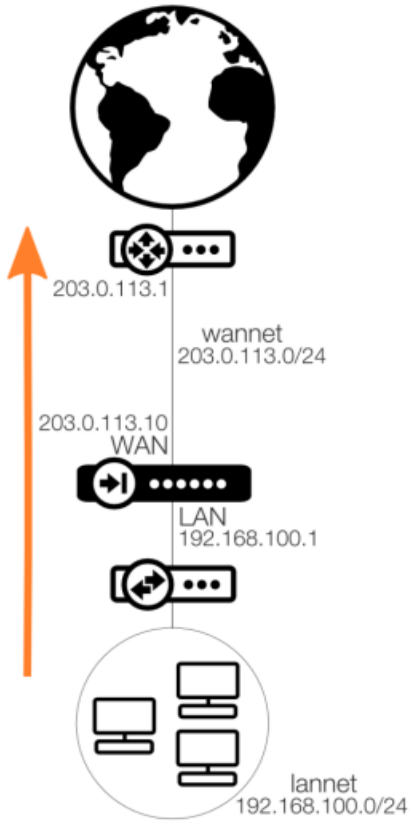


Abbildung 2.4.1 LAN-zu-WAN-Netzwerkzugang

Detailbesprechung

Weil alle grundsätzlichen Netzwerke und IPs schon definiert sind, müssen wir nur noch ein paar weitere IP-Regeln erzeugen. Es werden keine zusätzlichen Routen oder Änderungen an bestehenden Routen benötigt.

Wir beginnen, unseren Nutzern hinter der LAN-Schnittstelle Internetzugang zu geben, indem wir eine IP-Regel wie die nachfolgend gezeigte erzeugen.

#	Name	L...	Src If	Src Net	Dest If	Dest Net	Service	Address Translation
Rules for the Lan interface								
1	▶ NAT_Lan_Out	✔	Lan	Lannet	Wan	all-nets	all_services	SRC:NAT

Abbildung 2.4.2 Eine NAT-IP-Regel für die LAN-Schnittstelle

Und das ist schon alles. Diese IP-Regel nutzt die Aktion NAT, weil wir von einem privaten Netzwerk zu irgendetwas im Internet gehen. Durch das Erzeugen dieser IP-Regel geben

wir unseren Nutzern hinter der LAN-Schnittstelle Zugang zum Internet, indem sie die externe WAN-Schnittstelle auf irgendeinem Port und mit irgendeinem Protokoll benutzt. Wir stellen ein, dass die Ziel-Schnittstelle WAN sein soll, weil wir die Anzahl der Ziel-Schnittstellen, auf die diese IP-Regel reagieren soll, begrenzen wollen. Diese Regel reagiert jetzt nur, wenn die Ziel-Schnittstelle die externe WAN-Schnittstelle ist (mit anderen Worten, für Internet-Datenverkehr).

Hinweis

Bitte vergessen Sie nicht, jede neu erzeugte IP-Regel oberhalb der AllesVerwerfen-Regel zu platzieren, weil die Reihenfolge der IP-Regeln sehr wichtig ist.

Obwohl es so funktioniert, ist es allerdings nicht empfohlen, die IP-Regel so einzustellen, doch viele Administratoren machen es trotzdem so. Wir werden erklären, warum dies keine gute Idee ist. Der Hauptgrund ist Sicherheit. Indem wir den Dienst „alle_dienste“ nutzen, begrenzen wir den externen Zugang überhaupt nicht. Benutzer sind so in der Lage, jede Anwendung und jedes Programm zu nutzen, um damit das Internet zu erreichen. Auch Exploits, Malware, Keyloggers, Bots usw. Alles, was den Computer eines Clients infizieren könnte, hat so vollständigen Zugang zu allem Möglichen.

Selbst wenn viele dieser Art von Programmen die üblichen Ports wie 80 oder 443 nutzen könnten, gibt es keinen Grund, den Zugang zum Internet so vollständig zu öffnen. Ja, es ist sehr leicht, das so einzustellen, aber weder sicher noch empfohlen.

Wir empfehlen, zu überprüfen, was genau von der LAN-Schnittstelle in Richtung Internet eingeleitet werden kann. Wenn wir die absoluten Grundlagen ansehen, ist es sinnvoll, die folgenden Dienste zu erlauben: HTTP, HTTPS und DNS, wie im nachfolgenden Bildschirmfoto gezeigt.

#	Name	L...	Src If	Src Net	Dest If	Dest Net	Service	Address Translation
Rules for the Lan interface								
1	▶ NAT_Lan_HTTP	✔	Lan	Lannet	Wan	all-nets	http	SRC:NAT
2	▶ NAT_Lan_HTTPS	✔	Lan	Lannet	Wan	all-nets	https	SRC:NAT
3	▶ NAT_Lan_DNS	✔	Lan	Lannet	Wan	all-nets	dns-all	SRC:NAT

Abbildung 2.4.3 NAT-IP-Regeln für bestimmte Dienste

Es ist möglich, im Adressbuch eine Dienst-Gruppe anzulegen und „http", „https“ und „dns-all“ dieser Gruppe hinzuzufügen. Dann brauchen wir nur eine IP-Regel für alle drei Dienste. Es ist eine Frage des persönlichen Geschmacks, welche Methode Sie verwenden. In diesem Buch werden wir aus Gründen der Einfachheit für jeden Dienst eine IP-Regel erzeugen.

DHCP-Server auf der LAN-Schnittstelle einstellen

Wir haben jetzt Regeln für grundsätzlichen Internet-Zugang. Aber weil wir diese Regeln beschränkt haben, um nur zu reagieren, wenn die Ziel-Schnittstelle extern ist (WAN), passen die Regeln nicht, wenn wir versuchen, etwas intern zu erreichen, zum Beispiel die DMZ. Dies wird nachfolgend in *Abbildung 2.4.4* dargestellt.

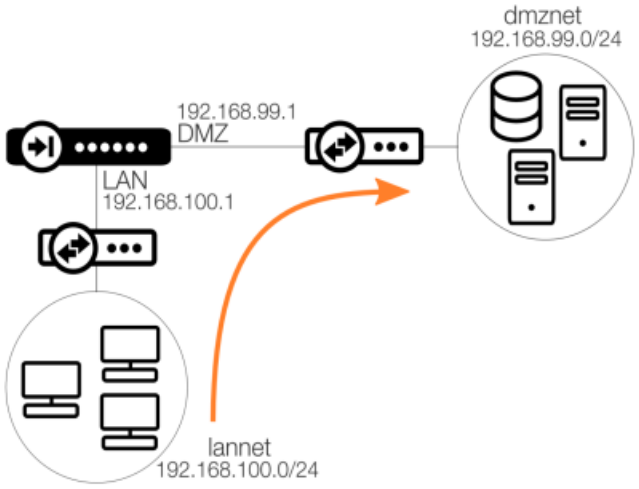
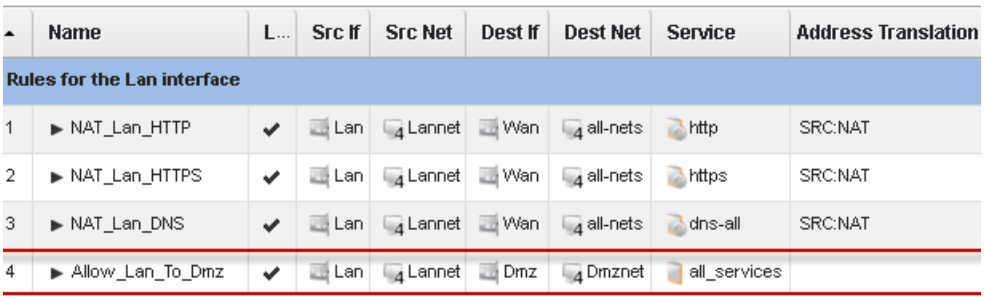


Abbildung 2.4.4 Datenverkehr von LAN zu DMZ mit Datenverkehr-Richtungspfeil

Wir könnten unsere bestehenden Regeln abändern, um auch Zugang zur DMZ-Schnittstelle zu gestatten, aber es ist besser, neue Regeln für den Zugang zwischen mehreren Schnittstellen zu erzeugen. Hier sind einige Gründe, warum dies eine gute Idee ist:

- Besserer Überblick über die Funktionalität der Regeln.
- Geringere Möglichkeit, versehentlich Zugang zu eingeschränkten Ressourcen zu bekommen.
- Leichter anpassbare Funktionalität.

Damit wir Nutzern erlauben können, Verbindungen vom LAN zum DMZ-Netzwerk zu starten, brauchen wir eine IP-Regel, die wie Regel **4** im nachfolgenden Bildschirmfoto aussieht.



	Name	L...	Src If	Src Net	Dest If	Dest Net	Service	Address Translation
Rules for the Lan interface								
1	▶ NAT_Lan_HTTP	✔	Lan	Lannet	Wan	all-nets	http	SRC:NAT
2	▶ NAT_Lan_HTTPS	✔	Lan	Lannet	Wan	all-nets	https	SRC:NAT
3	▶ NAT_Lan_DNS	✔	Lan	Lannet	Wan	all-nets	dns-all	SRC:NAT
4	▶ Allow_Lan_To_Dmz	✔	Lan	Lannet	Dmz	Dmznet	all_services	

Abbildung 2.4.5 LAN-zu-DMZ-IP-Regel

Bitte beachten Sie, dass Regel **4** im obigen Regelsatz keine Adressübersetzung-Regel (NAT oder SAT) ist. Der Grund dafür ist, dass es für Kommunikation zwischen zwei internen privaten Netzwerken nicht notwendig ist, die Sender-IP der Quelle zu maskieren. Es liegt jedoch beim Administrator, zu entscheiden, welche Art von Regel-Aktionen und Diensten er benutzen will und welche Anforderungen es in seinem Netzwerk-Design überhaupt gibt.

Warum sollte man *alle_dienste* in der Regel für DMZ benutzen?

Dies ist eine Geschmacksfrage und es liegt beim Administrator, zu entscheiden, wie viele Zugänge zwischen den internen Netzwerken erlaubt sein sollen.

Viele würden innerhalb ihrer eigenen Netzwerke vollständige Kommunikation zwischen erlauben. Einige Administratoren benutzen sogar FwdFast für diese Kommunikation. Es wird jedoch empfohlen, Regeln mit Statuskontrolle zu nutzen, wann immer möglich (FwdFast-Regeln haben keine Statuskontrolle).

Sollten Nutzer hinter der LAN-Schnittstelle überhaupt Zugang zur DMZ haben?

Die Chance, durch Schadsoftware infiziert zu werden, ist für Geräte im LAN größer als für einen Server in der DMZ. Daher wird empfohlen, den Zugang zur DMZ zu so weit wie möglich zu beschränken.

Gibt es einen Grund für einen normalen Nutzer, direkten Zugang zu den Servern in der DMZ zu bekommen?

Das hängt immer davon ab, wie das Netzwerk gestaltet ist und welche Art von Anwendungen und Inhalten in der DMZ benutzt werden. Statt dem gesamten LAN-Netzwerk über alle Ports und Protokolle Zugang zur DMZ zu erlauben, wäre es besser, nur bestimmten Computern begrenzten Zugang zur DMZ zu gewähren. Ein Weg hierfür ist, Netzwerk-Objektgruppen zu nutzen.

Es ist noch besser, den Zugang noch weiter zu begrenzen und nur bestimmten Diensten wie z.B. HTTP, DNS usw. zu erlauben. Jeder Zugang zwischen zwei Schnittstellen, der alle Ports oder Protokolle oder das gesamte Netzwerk erlaubt, ist ein mögliches Sicherheitsrisiko.

Netzwerk-Objektgruppen für angepassten Zugang zur DMZ anlegen und benutzen

In der nachfolgenden *Abbildung 2.4.6* sehen Sie drei Client-PCs mit statischen IP-Adressen, die über die LAN-Schnittstelle Zugang zur DMZ bekommen sollen. Wir wollen von unserer vorigen Regel wegkommen, die dem gesamten Netzwerk hinter der LAN-Schnittstelle erlaubt, die DMZ zu erreichen.

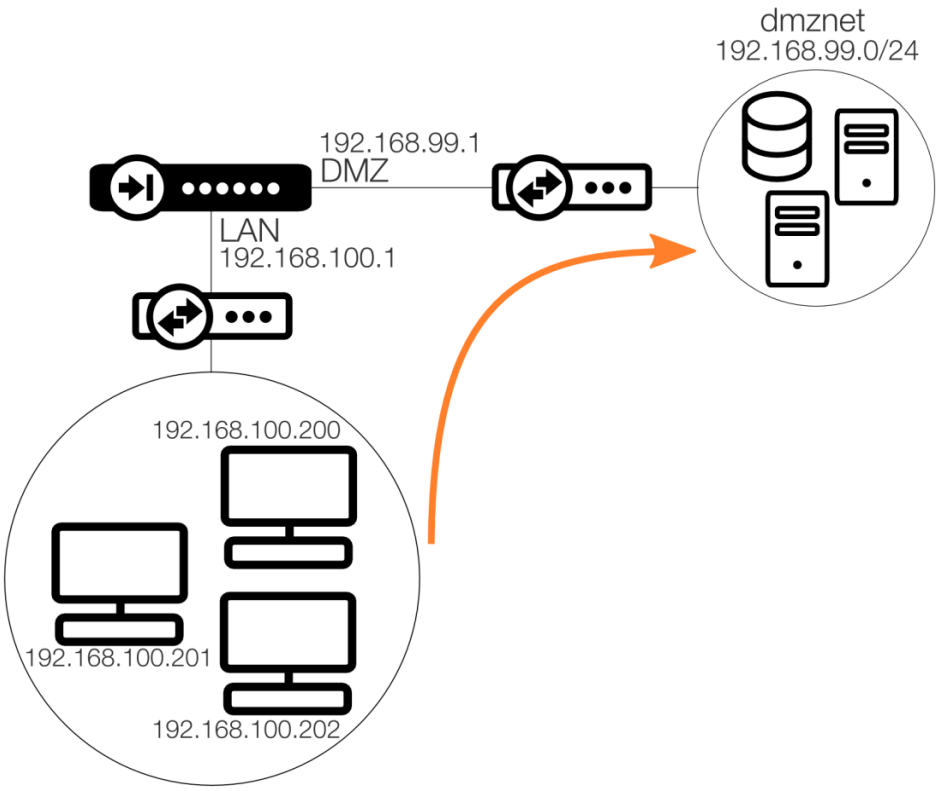


Abbildung 2.4.6 Zugang von Geräten im LAN zum DMZ-Netzwerk

Die obige Abbildung zeigt drei bestimmte Computer hinter der LAN-Schnittstelle, die Zugang zu den Servern hinter der DMZ-Schnittstelle erhalten werden. Der orange Pfeil zeigt die Richtung, in der der Datenverkehr fließen soll.

Um dies zu erreichen, erzeugen wir drei neue Adressobjekte, die die IP-Adressen der Geräte hinter der LAN-Schnittstelle enthalten. Diesen Geräten werden wir Zugang zur DMZ geben und ihnen statische IP-Adressen zuweisen.

# ▲	Name	Address
6	Lan_PC_1	192.168.100.200
7	Lan_PC_2	192.168.100.201
8	Lan_PC_3	192.168.100.202

Abbildung 2.4.7 LAN-Gerätobjekte mit entsprechenden Adressen

Als nächstes erzeugen wir eine Adressgruppe, die unsere gerade erzeugten Netzwerkobjekte enthält, wie nachfolgend gezeigt.

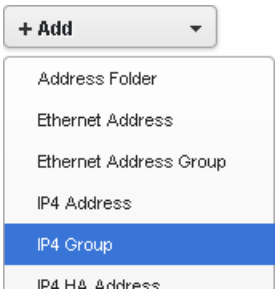


Abbildung 2.4.8 Ein Netzwerk-Gruppenobjekt hinzufügen, das unsere drei Geräte im LAN enthält

Dann geben wir der Gruppe einen passenden Namen und fügen dieser Gruppe unsere Objekte hinzu, wie nachfolgend gezeigt.

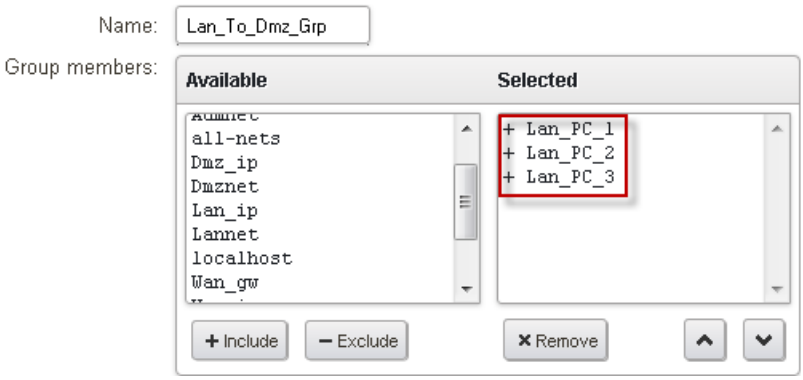


Abbildung 2.4.9 Netzwerkobjekte einem Gruppenobjekt hinzufügen

Sobald das Gruppenobjekt vollständig ist, ändern wir unsere LAN-nach-DMZ-Regel, so dass sie unser gerade erzeugtes Gruppenobjekt statt des gesamten LAN-Netzwerkobjekts (192.168.100.0/24) nutzt. Dies wird im nachfolgenden Bildschirmfoto dargestellt.

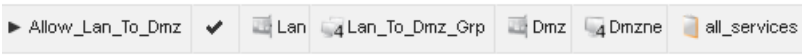


Abbildung 2.4.10 Eine Gruppe mit einer IP-Regel nutzen

Der Effekt dieser Änderung ist, dass nur die drei PCs hinter der LAN-Schnittstelle Zugang zum DMZ-Netzwerk haben. Wenn irgendjemand anderes versucht, aus dem restlichen LAN-Netzwerk die DMZ zu erreichen, wird der Verbindungsversuch verworfen.

Momentan erlauben wir diesen Geräten alle Ports und Protokolle im gesamten DMZ-Netzwerk, aber das kann ebenfalls geändert werden. Wir können den Zugang so begrenzen, dass nur bestimmte Ports und außerdem nur eine oder mehrere bestimmte IP-Adressen

im Zielnetzwerk erlaubt werden, und zwar auf ähnliche Weise, wie wir das beim Verbinden der Client-PCs gemacht haben.

Als Beispiel wollen wir eine wirklich sichere Regel für den Zugang vom LAN zur DMZ mithilfe der folgenden Regel einstellen.

Abbildung 2.4.11 Beispiel einer sicheren Regel, um Zugang zur DMZ zu geben

Jetzt haben wir ein neues Adressbuch-Objekt namens „Dmz_Server_1" erzeugt, das eine einzelne IP-Adresse eines Servers in der DMZ darstellt. Diese Regel nutzen wir als Ziel-Netzwerk für die IP-Regel und begrenzen damit die nutzbaren Ports auf einen einzigen: HTTP-Port 80. Dies ist wirklich sicher und bietet nur noch eine geringe Chance, diesen Server unautorisiert zu erreichen.

Dies sind erst einige der grundsätzlichen Möglichkeiten, die wir mit der Clavister-Firewall haben. Wir könnten zudem noch beliebig viele Ebenen zur Prüfung und Authentifizierung einfügen, um den Zugang noch weiter zu beschränken. Wir könnten ein Benutzer-Passwort verlangen, den Zugang nur zu bestimmten Zeiten oder Wochentagen zulassen, eine verschlüsselte VPN-Verbindung verlangen (VPN = Virtuelles Privates Netzwerk), festlegen, welche MAC-Adressen der Clients erlaubt sind, einschränken, welche Anwendungen den festgelegten Port benutzen dürfen und vieles mehr.

Letztendlich liegt es beim Administrator, zu entscheiden, wie er die Kommunikation zwischen den verschiedenen Netzwerken und Schnittstellen beschränkt, aber der cOS-Core bietet hierzu alle benötigten Werkzeuge.

Tipp

Zum Erzeugen neuer Regeln gibt es eine sehr praktische Funktion namens „Klonen". Wenn wir eine neue Regel (oder einen Dienst, ein Adressbuch-Objekt usw.) einstellen, ist es durchaus wahrscheinlich, dass schon eine ähnliche Regel existiert, die wir mit wenigen Parameter-Änderungen anpassen können.

In solchen Situationen können wir eine bestehende Regel rechtsklicken und „Klonen" auswählen, um diese bestimmte Regel zu klonen und ihr anschließend einen neuen Namen zu geben und die Parameter anzupassen. Dies wird im nachfolgenden Bildschirmfoto dargestellt.

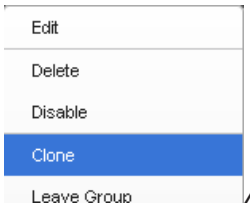


Abbildung 2.4.12 Klonen von Regeln/Objekten

*Bitte beachten Sie, dass ein geklontes Objekt immer **am Ende** der aktuellen Objekte-Liste hinzugefügt wird.*

Rezept 2.5. DMZ einstellen und Zugang zu einem internen Webserver erlauben

Ziele

Der Zweck dieses Rezepts ist es, den Servern und anderen Computern, die sich in der DMZ befinden, Internet-Zugang zu erlauben.

Es kann durchaus sinnvoll sein, Computern in der DMZ zumindest irgendeinen externen Zugang zu geben, damit sie solche Sachen wie Systemaktualisierungen oder neue Anti-Virus-Signaturen herunterladen können.

Abbildung 2.5.1 zeigt eine Übersicht von Netzwerken, die wir in diesem Rezept verwenden, wobei der orange Pfeil die Datenverkehr-Richtung anzeigt, die uns interessiert.

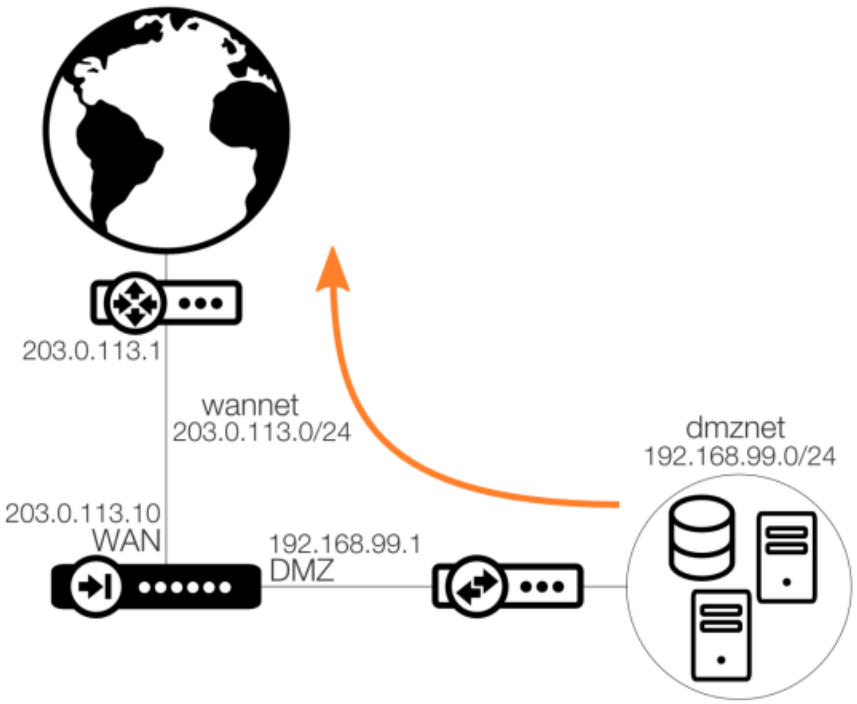


Abbildung 2.5.1 DMZ-zu-WAN-Netzwerk mit Datenverkehr-Richtungspfeil

Wir werden außerdem Regeln erzeugen, die Nutzer im Internet benötigen, um in der Lage zu sein, einen Webserver zu erreichen, der sich hinter der DMZ-Schnittstelle befindet.

Detailbesprechung

Alle grundsätzlichen Netzwerke und IPs wurden schon in früheren Rezepten definiert. Wir müssen nur noch ein paar zusätzliche IP-Regeln erzeugen. Es werden keine zusätzlichen Routen oder Änderungen an bestehenden Routen benötigt.

Der Hauptunterschied ist hier, dass die Regeln jetzt Datenverkehr von der DMZ-Schnittstelle anstelle des LANs erlauben.

Das nachfolgende Bildschirmfoto zeigt die Regeln, die wir erzeugt haben, um den Servern in der DMZ zu erlauben, sich mithilfe der HTTP-, HTTPS- und DNS-Protokolle mit dem Internet zu verbinden.

#	Name	L...	Src If	Src Net	Dest If	Dest Ne...	Service	Address Translation
Rules for the Dmz interface								
1	▶ NAT_Dmz_HTTP	✔	Dmz	Dmznet	Wan	all-nets	http	SRC:NAT
2	▶ NAT_Dmz_HTTPS	✔	Dmz	Dmznet	Wan	all-nets	https	SRC:NAT
3	▶ NAT_Dmz_DNS	✔	Dmz	Dmznet	Wan	all-nets	dns-all	SRC:NAT

Abbildung 2.5.2 DMZ-nach-WAN-IP-Regeln, die Servern in der DMZ erlauben, das Internet via HTTP, HTTP und DNS zu erreichen

Regeln für den externen Zugang zu einem internen Server in der DMZ einstellen

Unser Ziel hier ist es, Clients im Internet Zugang zu einem Webserver zu erlauben, der sich in der DMZ befindet.

Bisher haben wir nur Regeln für Verbindungen erzeugt, die von internen Netzwerken eingeleitet wurden, die sich an der LAN-Schnittstelle befanden. Jetzt werden wir Regeln erzeugen, die uns ermöglichen, vom Internet aus einen Webserver an der DMZ-Schnittstelle zu erreichen.

Das nachfolgende Diagramm zeigt, was wir erreichen wollen, wobei der orange Pfeil die Datenverkehr-Richtung anzeigt, die wir nutzen wollen.

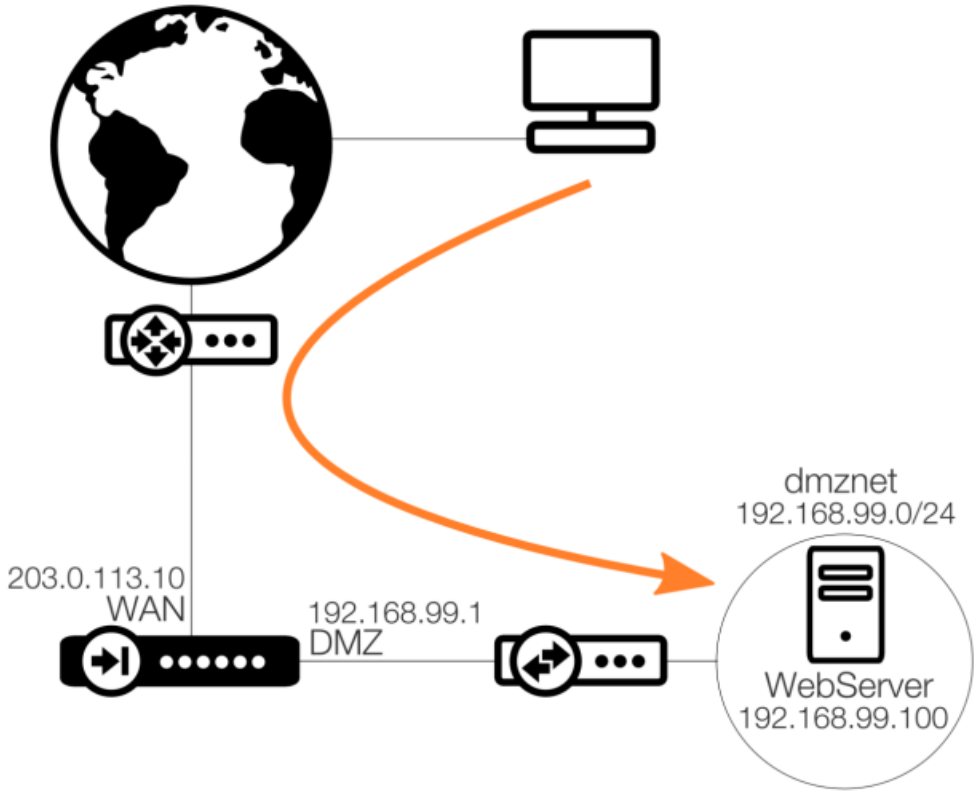


Abbildung 2.5.3 Internen Webserver in der DMZ von einem Client im Internet aus erreichen

Um dies zu erreichen, werden wir eine neue Regelaktion namens SAT (Static Address Translation, Statische Adressübersetzung) nutzen. Die Regeln, die wir bisher genutzt haben, waren NAT (Network Address Translation, Netzwerk-Adressübersetzung) und Erlauben-Regeln, die keine Adressübersetzung bieten.

Hinweis

Einige Netzwerkgeräte-Lieferanten benutzen den Begriff „Port-Weitergabe (port forwarding)", wenn sie sich auf SAT beziehen. Beide Begriffe beziehen sich auf dieselbe Funktionalität.

Im Unterschied zu NAT-Regeln braucht SAT mindestens zwei IP-Regeln, um eingestellt zu werden. Erzeugen Sie zunächst eine SAT-Regel, die die Adressübersetzung ausführt, und dann eine zweite Regel, die den aktuellen Datenverkehr weitergibt. Die zweite Regel kann eine Erlauben- oder NAT-Regel (oder sogar FwdFast oder, in komplexeren und ungewöhnlichen Szenarios) eine andere SAT-Regel sein.

Um weiterhin strukturiert vorzugehen, erzeugen wir ein neues IP-Adressobjekt im Adressbuch und nennen es „Webserver", mit den Eigenschaften wie im nachfolgenden Bildschirmfoto gezeigt.

Abbildung 2.5.4 Die IP-Adresse des Webservers

Um das obige Server-Objekt als Ziel-Server für die Adressübersetzung zu nutzen, müssen wir als nächstes eine SAT-Regel wie die im nachfolgenden Bildschirmfoto gezeigte erzeugen.

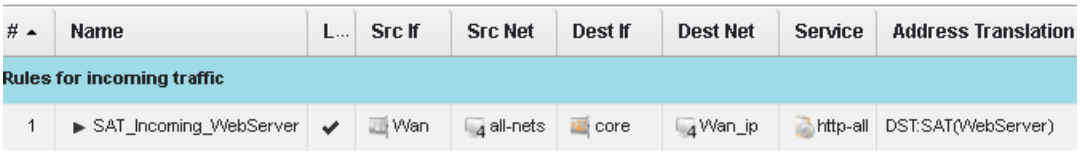


Abbildung 2.5.5 SAT-Regel-Definition

Den Core als Ziel-Schnittstelle benutzen

Ein Punkt, der in der obigen Definition unbedingt hervorgehoben und berücksichtigt werden muss, ist die Ziel-Schnittstelle. Hier haben wir den Core als Ziel-Schnittstelle gewählt, aber was genau ist die Core-Schnittstelle?

Wenn Sie *Core* als Ziel-Schnittstelle festlegen, zeigt dies an, dass der cOS-Core selbst auf Datenverkehr antworten muss, der an dieser Schnittstelle ankommt. Die *Core*-Schnittstelle wird beispielsweise benutzt, wenn der cOS-Core auf eine „Ping"-Anfrage von ICMP antwortet oder wenn er als PPTP- oder L2TP-Server fungiert.

Indem wir die Ziel-Schnittstelle einer Route als *Core* festlegen, weiß der cOS-Core, dass er selbst das letztendliche Ziel des Datenverkehrs ist. Es gibt ein paar Ausnahmen dieser Regel, aber wir werden hier nicht weiter darauf eingehen, um an diesem Punkt nicht unnötige Verwirrung zu stiften.

In unserem aktuellen Setup sind alle IP-Adressen auf allen physischen Schnittstellen so eingestellt, dass sie automatisch *vom Core geroutet* werden. Das bedeutet, dass die IP-Adressen 192.168.98.14, 192.168.99.1, 192.168.100.1 und 203.0.113.10 und letztlich auch die Localhost-IP 127.0.0.1 allesamt Routen haben, deren Routen-Schnittstelle auf *Core* eingestellt ist.

Das IP-Adressobjekt, das wir für den Webserver (192.168.99.100) erzeugt haben, ist daher keine Core-geroutete IP.

Die WAN-IP als Zielnetzwerk nutzen

Wie zuvor gezeigt nutzen wir ein Quellinterface des WANs und ein Zielnetzwerk von Wan_ip. Dies kann eventuell irritieren, da die Quelle und das Ziel anscheinend identisch sind. Wir müssen die Richtung des Datenverkehrs im Blick behalten, sowie, wie die Regel vom cOS-Core interpretiert wird.

Aus der Sicht eines Clients wollen sich die Clients einfach nur mit unserem Webserver an einer bestimmten IP-Adresse verbinden. In diesem Fall ist das die Adresse Wan_ip. Aus der Sicht des cOS-Cores müssen wir eine Regel erzeugen, die den vom Client gewünschten Datenverkehr zu unserem internen Server erlaubt.

Listen wir einmal auf, was passiert:

- **Src if:** Wenn der Datenverkehr vom Client gesendet wird, kommt er an der Internet-Schnittstelle WAN an. Die Quell-Schnittstelle der Regel muss dann WAN (oder Irgendwas, aber das ist wesentlich unsicherer) sein, weil dies die Schnittstelle ist, an der der Datenverkehr ankommt.

- **Src net:** Wir kennen die Quell-IP des Clients nicht. Es kann tausende, wenn nicht sogar Millionen verschiedener Quell-IPs geben, die sich mit unserem Webserver verbinden wollen. Wir haben aus diesem Grund „alle-netze“ als Quell-Netzwerk gewählt, was sämtliche IPv4-IPv4-Adressen bedeutet.

- **Dest if:** Die Ziel-Schnittstelle ist die Schnittstelle, zu der „Wan_ip“ geroutet wird, weil diese IP der Core-Schnittstelle gehört und weil, wie zuvor erläutert, die Ziel-Schnittstelle der Core sein muss (es könnte auch „Irgendwas“ sein, aber das ist unsicher).

- **Dest net:** Dies ist die IP-Adresse, mit der der Client sich verbinden will; grundsätzlich ist sie das Ende der Reise für diese Client-Anfrage. In unserem Beispiel ist es die öffentliche IP-Adresse des „Webservers", hier also Wan_ip.

Die zweite IP-Regel erzeugen

An diesem Punkt haben wir also eine SAT-IP-Regel erzeugt, aber wie schon erwähnt ist das nur die Hälfte dessen, was benötigt wird. Die andere Hälfte ist entweder eine Erlauben- oder NAT-IP-Regel, die dem Datenverkehr erlaubt, zu passieren. Weil der Quell-Datenverkehr in diesem Falle aus dem Internet empfangen wird, wollen wir die Sender-IP-Adressen nicht vor dem Webserver maskieren (hauptsächlich für Protokollierungszwecke und außerdem, um sehen zu können, woher die eingehenden Verbindungen stammen).

Nachdem wir die zweite Erlauben-Regel hinzugefügt haben, sehen die IP-Regeln aus wie folgt:

#	Name	L...	Src I...	Src Net	Dest If	Dest Net	Service	Address Translation
Rules for incoming traffic								
1	▶ SAT_Incoming_WebServer	✔	Wan	all-nets	core	Wan_ip	http-all	DST:SAT(WebServer)
2	▶ Allow_Incoming_WebServer	✔	Wan	all-nets	core	Wan_ip	http-all	

Abbildung 2.5.6 Vollständige Eingangs-Adressübersetzung mit SAT- und Erlauben-Regeln

In diesem Fall kann die weiter vorher in diesem Buch erwähnte „Klonen"-Funktion sehr nützlich sein. Klonen Sie einfach die SAT-Regel, ändern Sie ihre Erlauben-Regel und platzieren Sie sie unterhalb der SAT-Regel. Die Regel-Sortierung ist abermals wichtig, weil wir die Adressübersetzung- Aktion zuerst durchführen müssen, bevor wir den Datenverkehrsfluss erlauben.

Ab jetzt sind Clients im Internet in der Lage, den Webserver hinter der DMZ-Schnittstelle zu erreichen, indem sie sich mit der externen öffentlichen IP-Adresse der Clavister-Firewall (203.0.113.10) verbinden. Im Hintergrund jedoch wird die Zieladresse übersetzt, um sich mit dem internen Webserver (192.168.99.100) zu verbinden, der sich hinter der DMZ-Schnittstelle befindet.

Rezept 2.6. DMZ-Webserver vom internen (LAN-N-)Netzwerk erreichen

Ziele

Der Zweck dieses Rezepts ist es, unsere IP-Regeln so einzustellen, dass Benutzer hinter der LAN-Schnittstelle (und Teile des LAN-Netzes) in der Lage sind, sich mit der Firmen-Website und dem Server in der DMZ zu verbinden, indem sie sich mit der externen Schnittstelle verbinden, wie nachfolgend in *Abbildung 2.6.1* gezeigt.

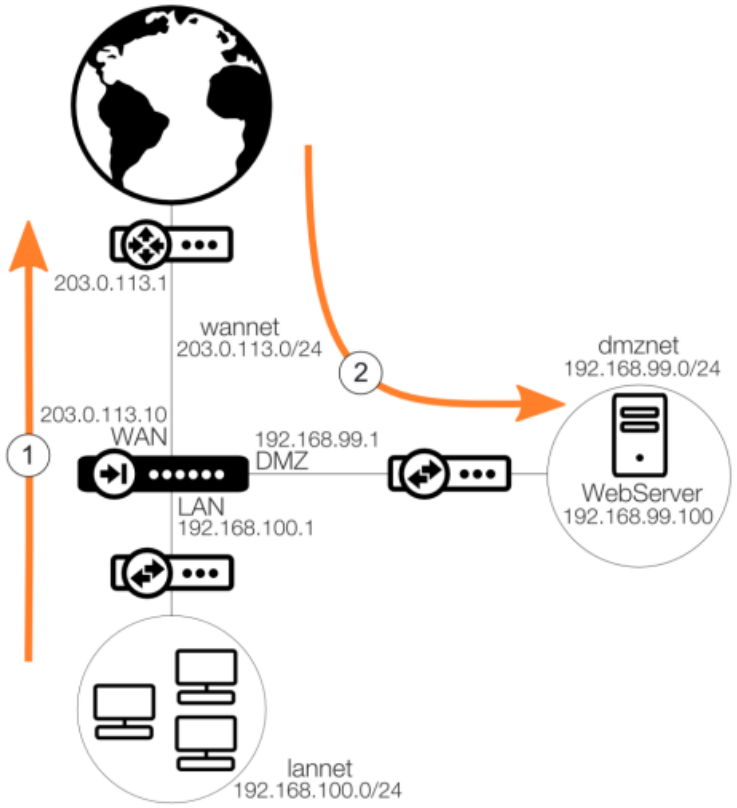


Abbildung 2.6.1 DMZ-Webserververbindung von LAN-Client über öffentliche IP

Detailbesprechung

Zuvor haben wir den Zugang zur DMZ-Schnittstelle von der LAN-Schnittstelle mithilfe einer normalen Erlauben-Regel eingestellt. Das funktioniert prima, wenn der sich ver-

bindende Client die private IP-Adresse des Webservers kennt und sich dann direkt mit ihm verbindet.

Das ist allerdings eine sehr ungewöhnliche Situation. Wenn wir eine Firmen-Website haben, rufen wir sie nicht auf, indem wir ihre private IP-Adresse wie z.B. 192.168.99.100 aufrufen. Stattdessen geben wir den Namen der Website ein, wie z.B. *www.clavister.com*.

Bis wir einen internen DNS-Server so eingestellt haben, dass er uns die private IP-Adresse der Website zurückgibt, müssen wir noch ein paar Änderungen an unseren Eingangs-IP-Regeln vornehmen. Nach den vorangegangenen Rezepten sieht unsere Eingangsregel momentan so aus wie die nachfolgend gezeigte.

#	Name	L...	Src If	Src Net	Dest If	Dest Net	Service	Address Translation
Rules for incoming traffic								
1	▶ SAT_Incoming_WebServer	✔	Wan	all-nets	core	Wan_ip	http-all	DST:SAT(WebServer)
2	▶ Allow_Incoming_WebServer	✔	Wan	all-nets	core	Wan_ip	http-all	

Abbildung 2.6.2 Eingangsregeln zur DMZ vom Internet

Das Problem ist, dass weder Regel **1** noch Regel **2** ansprechen, wenn wir eine Verbindung aus der Quell-Schnittstelle LAN einleiten. Diese Regeln reagieren nur, wenn der Datenverkehr an der WAN-Schnittstelle ankommt.

Um dieses Problem zu lösen, erzeugen wir eine Schnittstellengruppe, die LAN und WAN enthält.

Schnittstellengruppen finden Sie im WebUI, indem Sie **Netzwerk > Schnittstellen** aufrufen und dann **VPN > Verschiedenes > Schnittstellengruppen** wählen.

Dies ist im nächsten Bildschirmfoto vom WebUI gezeigt.

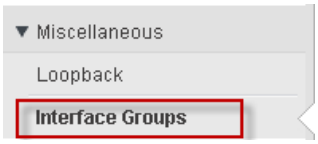


Abbildung 2.6.3 Schnittstellengruppen

Fügen Sie als nächsten Schritt LAN und WAN zu unserer Schnittstellengruppe hinzu, wie nachfolgend gezeigt.

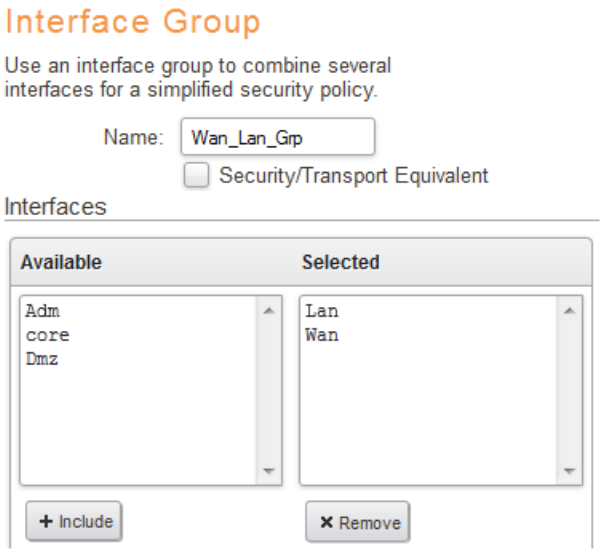


Abbildung 2.6.4 Schnittstellengruppe erzeugen

Nun fügen Sie diese Schnittstellengruppe als Quell-Schnittstelle unseren beiden IP-Regeln hinzu, wie im nächsten Bildschirmfoto gezeigt.

#	Name	L...	Src If	Src Net	Dest If	Dest Net	Service	Address Translation
Rules for incoming traffic								
1	► SAT_Incoming_WebServer	✔	Wan_Lan_Grp	all-nets	core	Wan_ip	http-all	DST:SAT(WebServer)
2	► Allow_Incoming_WebServer	✔	Wan_Lan_Grp	all-nets	core	Wan_ip	http-all	

Abbildung 2.6.5 Geänderte Eingangsregeln, die ebenfalls auf die LAN-Schnittstelle reagieren

Jetzt sind wir in der Lage, uns mit der Firmen-Website zu verbinden, egal, ob wir uns im Internet oder hinter der LAN-Schnittstelle befinden.

Hinweis

Selbst wenn wir die ADM-Schnittstelle in diesem Beispiel nicht dieser Gruppe hinzugefügt haben, ist es eine gute Idee, dies doch zu tun, damit Administratoren die gleichen Zugriffsrechte haben.

Dies ist nicht der einzige Weg, um dieses spezielle Szenario zu bewältigen. Wir können ebenfalls neue SAT-/Erlauben-Regeln erzeugen, die ganz ausschließlich nur auf die LAN-Schnittstelle hören. Oder wir können sowohl die SAT-Regel als auch die Ausgangsregel für die LAN-Schnittstelle so ändern, dass sie die Core-Schnittstelle enthalten. cOS-Core ist sehr flexibel und es gibt in den meisten Fällen verschiedene Wege, um ein Ziel zu erreichen.

Rezept 2.7. Webserver von der gleichen Schnittstelle des Webservers aus erreichen

Ziele

Es gibt ein häufig auftretendes Einstellungsszenario, das dann auftritt, wenn man sich mit der Firmen-Website verbindet und sich der Client und der Server beide hinter der gleichen Schnittstelle im gleichen Netzwerk befinden.

Dieses Rezept behandelt dieses Problem und wie man es lösen kann. Die nachfolgende *Abbildung 2.7.1* stellt die Situation dar, in der ein Client sich an der DMZ-Schnittstelle befindet und Zugang zum Webserver haben will, der sich in der DMZ befindet, indem er sich mit einem FQDN (Fully Qualified Domain Name, vollständig qualifizierter Domänenname) verbindet. Ein Beispiel eines FQDN ist *myserver.example.com*.

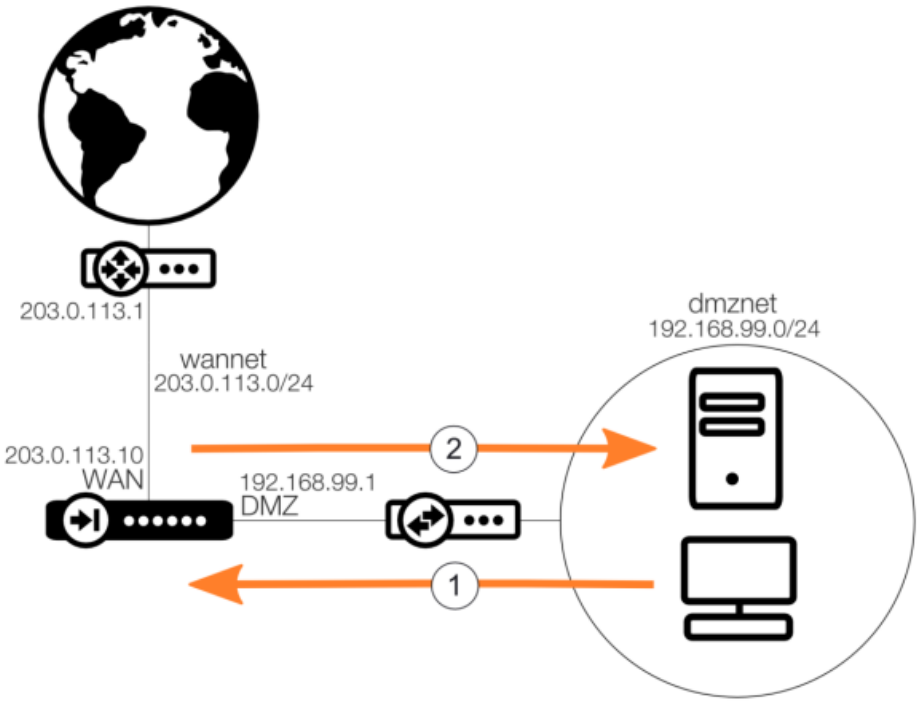


Abbildung 2.7.1 Eine Verbindung von der DMZ zu einem Server im DMZ einleiten

Detailbesprechung

Die sich verbindenden Clients möchten die Firmen-Website erreichen, indem deren Webadresse (wie z.B. www.clavister.com) eingegeben wird. Dies wiederum ergibt eine öffentliche IP, die durch den zuvor beschriebene Regelsatz behandelt werden muss (*Rezept 2.7. Webserver von der gleichen Schnittstelle des Webservers aus erreichen*).

In diesem aktuellen Konfigurationsbeispiel haben wir keine Regeln, die diese spezielle Situation behandeln. Unser Regelsatz sieht momentan so aus wie der nachfolgende für die die Eingang-Regeln zum Server in der DMZ:

#	Name	L...	Src If	Src Net	Dest If	Dest Net	Service	Address Translation
Rules for incoming traffic								
1	▶ SAT_Incoming_WebServer	✔	Wan_Lan_Grp	all-nets	core	Wan_ip	http-all	DST:SAT(WebServer)
2	▶ Allow_Incoming_WebServe	✔	Wan_Lan_Grp	all-nets	core	Wan_ip	http-all	

Abbildung 2.7.2 Der IP-Regelsatz für eingehenden Datenverkehr

Auf der Basis der Quell-Schnittstellengruppe, die wir im IP-Regelsatz nutzen, erlauben wir Datenverkehr sowohl von LAN als auch von WAN kommend. Wenn wir in diesem

Szenario Datenverkehr von der DMZ-Schnittstelle einleiten, bedeutet das, dass keine dieser Regeln angesprochen wird.

Eine einfache Lösung wäre, die DMZ unserem bestehenden Schnittstellengruppen-Objekt hinzuzufügen, wie nachfolgend gezeigt.

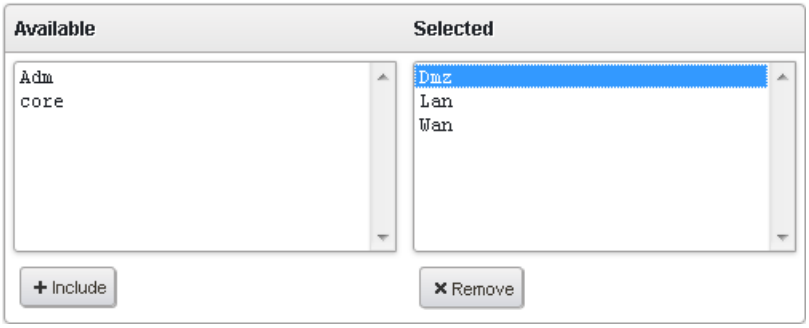


Abbildung 2.7.3 DMZ zur Schnittstellengruppe hinzufügen

Das Problem

Nachdem wir diese Änderungen angewendet haben, sind wir nicht mehr in der Lage, den Webserver von der DMZ zu erreichen.

Der Grund ist ein Problem mit der Datenpaket-Richtung, wie nachfolgend illustriert.

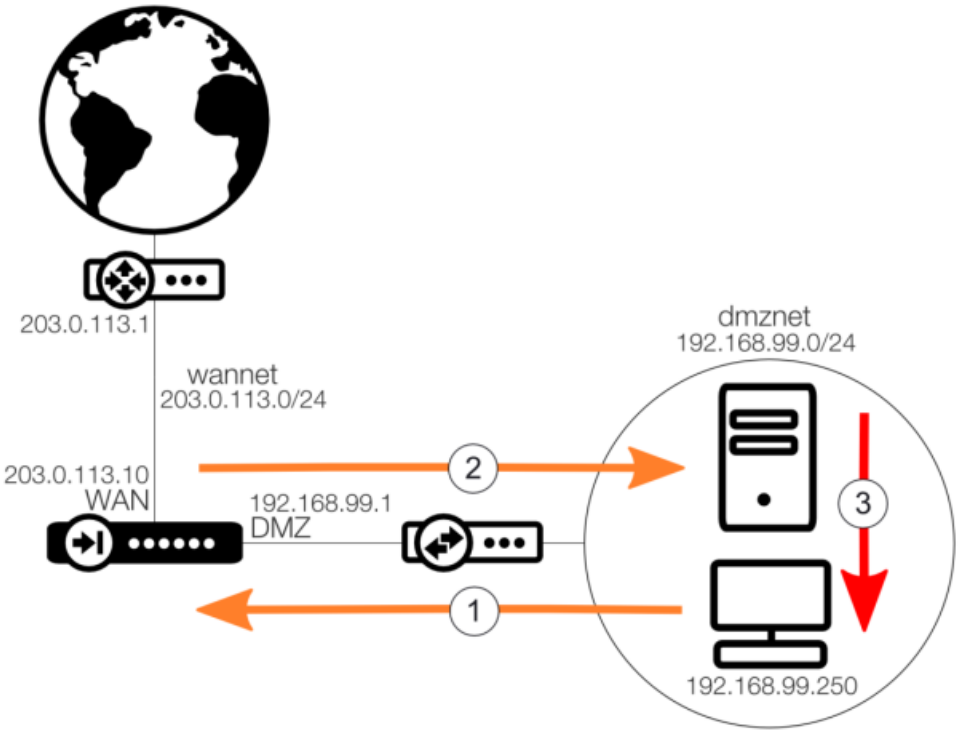


Abbildung 2.7.4 Das Datenpaket-Richtungsproblem

Die Ereignisse werden wie folgt fließen:

- Ein Client verbindet sich mit der öffentlichen IP-Adresse, indem er den öffentlichen FQDN-Namen des Webservers eingibt (**1**).
- IP Regel #1 und #2 reagieren und leiten die Client-Anfrage an den Server in der DMZ weiter (**2**).
- Der Server in der DMZ bekommt eine Anfrage von der IP 192.168.99.250, die Teil des eigenen Netzwerkbereichs des Webservers ist (192.168.99.0/24).
- Weil die IP zum eigenen IP-Bereich des Servers gehört, wird er die Antwort direkt an den sich verbindenden Client senden (**3**).

- Der sich verbindende Client erhält eine Antwort von einer privaten IP-Adresse, während er auf eine Antwort von einer öffentlichen Adresse erwartet, wie sie über den DNS-Nameserver aufgelöst wurde.
- Der Client wird dadurch verwirrt, weil er eine Antwort von einer unerwarteten IP-Adresse erhält, und er verwirft das Datenpaket. Der Verbindungsversuch schlägt fehl.

Um dieses Problem mit einem anderen Beispiel noch weiter zu verdeutlichen: Wenn ein Client eine Anfrage an die IP 203.0.113.50 schickt, erwartet er eine Antwort von derselben IP. Wenn er stattdessen eine Antwort von 192.168.99.100 erhält, wird er einfach dieses Datenpaket wegwerfen und weiter auf eine Antwort von 203.0.113.50 warten.

Die Lösung

Die Lösung ist, die wahre Quell-IP des Clients gegenüber dem Server zu verbergen und dem Webserver einzureden, er solle der Firewall antworten statt direkt dem Client.

Dies bewerkstelligen wir, indem wir eine NAT-Regel zwischen der SAT- und der Erlauben-Regel platzieren, wie nachfolgend gezeigt.

#	Name	L...	Src If	Src Net	Dest If	Dest Net	Service	Address Translation
Rules for incoming traffic								
1	► SAT_Incoming_WebServer	✔	WanLanDmz_Grp	all-nets	core	Wan_ip	http-all	DST:SAT(WebServer)
2	► NAT_Incoming_Dmz	✔	Dmz	Dmznet	core	Wan_ip	http-all	SRC:NAT
3	► Allow_Incoming_WebServe	✔	WanLanDmz_Grp	all-nets	core	Wan_ip	http-all	

Abbildung 2.7.5 DMZ-NAT-Regel-Lösung

Dies bedeutet, dass, wenn der DMZ-Client sich verbindet, die Regeln #1 und #2 anstelle von #1 und #3 reagieren. Die Reihenfolge der Regeln ist hier sehr wichtig, weil wir wollen, dass Regel #2 vor #3 reagiert, da wir ansonsten wieder das gleiche Problem hätten.

Falls dies schwierig zu verstehen ist, lassen Sie es uns nochmal anders erklären.

Unsere erste Regel übersetzt eingehende Verbindungen zur externen Wan_ip (203.0.113.50), um die private IP (192.168.99.100) des Webservers in der DMZ zu erhalten.

Die SAT-Regel führt nur die Adressübersetzung durch; sie lässt den aktuellen Datenverkehr nicht zu. Sobald die SAT-Regel angesprochen wurde, fährt der cOS-Core fort, eine passende Erlauben-, NAT- oder FwdFast-Regel zu finden.

Wenn wir von einem Host im Internet kommen (sagen wir 203.0.113.5), spricht dies zuerst unsere SAT-Regel an, aber weil 203.0.113.5 kein Teil unseres DMZ-Netzwerks ist, wird es nicht Regel Nummer 2 ansprechen. Stattdessen wird Regel Nummer 3 reagieren, weil dies eine IP-Adresse ist, die hinter der externen Internet-Schnittstelle existiert (also geroutet wurde).

Wenn wir etwas von einem Host in der DMZ (sagen wir 192.168.99.250) empfangen, wird das zuerst unsere SAT-Regel ansprechen und weil in diesem Fall die IP 192.168.99.250, mit der wir ankommen, Teil des DMZ-Netzwerks ist, reagiert Regel Nummer 2.

Wenn wir von einem Host in der DMZ (sagen wir 192.168.99.250) ankommen, wird das zuerst unsere SAT-Regel ansprechen und weil in diesem Fall die IP 192.168.99.250, mit der wir ankommen, Teil des DMZ-Netzwerks ist, reagiert Regel Nummer 2.

Diese NAT-Regel wird die wahre IP-Adresse des Clients maskieren, so dass das Datenpaket, wenn es beim Webserver ankommt, die IP der DMZ-Schnittstelle (192.168.99.1) als Absender hat. Der Webserver wird an diese Adresse antworten und so wird die gesamte Konversation zwischen dem sich verbindenden Client und dem Webserver durch den cOS-Core geschickt, was die Kommunikationsverbindung zwischen dem Client und dem Server aufrecht erhält. Der Client erhält eine Antwort von der IP, zu der er die Anfrage geschickt hat, wie nachfolgend gezeigt.

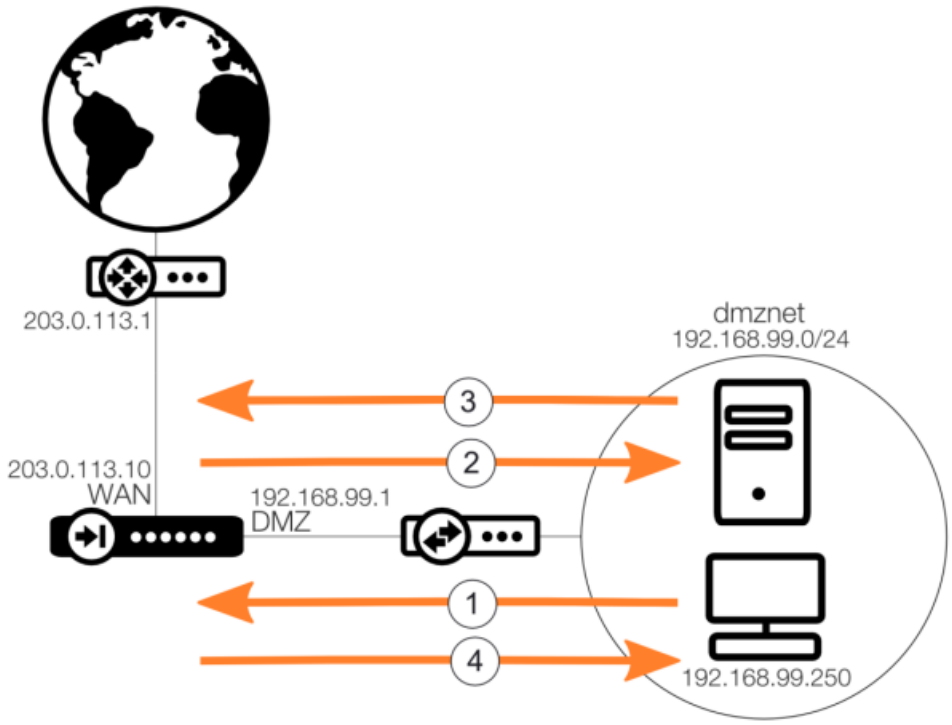


Abbildung 2.7.6 Datenverkehrpaket fließt, wenn NAT verwendet wird

Jetzt ist der Fluss der Ereignisse wie folgt:

- Der Client verbindet sich mit der öffentlichen IP-Adresse, indem er den öffentlichen FQDN-Namen des Webservers eingibt (**1**).
- IP Regel #1 und #2 reagieren und leiten die Client-Anfrage an den Server in der DMZ weiter (**2**).
- Der Server in der DMZ bekommt eine Anfrage von der IP 192.168.99.1, die Teil des eigenen Netzwerkbereichs des Webservers ist (192.168.99.0/24).
- Der Webserver (192.168.99.100) sendet eine Antwort an 192.168.99.1 (**3**), eine IP, die dem cOS-Core selbst gehört. Der Server antwortet dem Client nicht direkt, was das vorherige Problem vermeidet.
- Der cOS-Core kontrolliert die Verbindungen, so dass, sobald die Antwort vom Server kommt, der cOS-Core schon weiß, wohin er die Antwort senden oder weiterleiten muss.

- Der verbindende Client bekommt eine Antwort von der IP, der er die Anfrage geschickt hat, und der Nutzer kann auf den Webserver zugreifen (**4**).

Hinweis

Der cOS-Core ist sehr flexibel. Dies ist nur eine von mehreren möglichen Lösungen für dieses Szenario. Wir könnten zum Beispiel verschiedene Schnittstellengruppen anlegen, um die DMZ von der Erlauben- IP- Regelgruppe auszuschließen und die standardmäßige Ausgangsregel für die DMZ stattdessen ansprechen lassen. Oder wir könnten ein komplett neues Set mit IP-Regeln erstellen, die nur für die DMZ und dieses spezifische Szenario ansprechen. Und es gibt noch weitere Lösungen.

Rezept 2.8. Administrator-Zugang erweitern und IP-Regeln weiter strukturieren

Ziele

Dieses Rezept beschäftigt sich im Detail damit, wie man IP-Regeln ändert oder zum aktuellen IP-Regelsatz hinzufügt, um dem Administrator so viel Zugang zu den Clients, Servern und anderen Geräten im Netzwerk wie möglich zu gewähren, wie nachfolgend gezeigt in *Abbildung 2.8.1*.

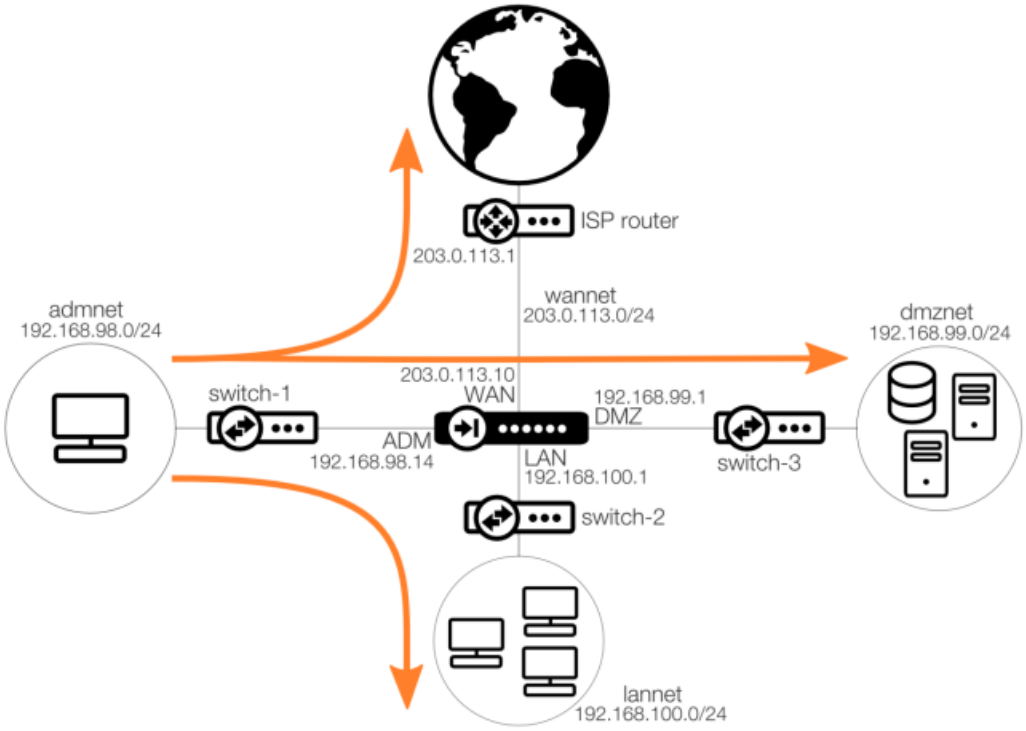


Abbildung 2.8.1 Das vollständige Basis-Netzwerk

Detailbesprechung

Sämtliche Kommunikation zwischen den verschiedenen Netzwerken läuft durch den cOS-Core. Wir müssen sicherstellen, dass der Administrator alle Zugangslevels hat, die er braucht, um das Netzwerk verwalten zu können. Dies schließt Zugang zu Webservern, Client-PCs und allen Schaltern und Routern im Netzwerk ein.

Auf der Basis der vorangegangenen Rezepte sieht die aktuelle Regel für Administrator-Zugang so aus wie die im nachfolgenden Bildschirmfoto gezeigte.

Name	L...	Src If	Src Net	Dest If	Dest Net	Service	Address Translation
▶ NAT_Adm_Out	✔	Adm	Admnet	Wan	all-nets	all_services	SRC:NAT

Abbildung 2.8.2 Die IP-Regel für den Administrator

Diese IP-Regel bedeutet, dass der Administrator im Moment nur Internetzugang hat, aber sich ansonsten mit nichts anderem verbinden kann, weder in den LAN-Zonen noch in der DMZ.

Administratoren brauchen normalerweise vollständigen Zugang zu allem an jedem Port und in jedem Protokoll, so dass wir eine zweite Regel hinzufügen müssen, die Zugang zu allen internen Ressourcen, sowohl den aktuellen als auch zukünftigen, gewährt. Diese Regel ist nachfolgend abgebildet.

Rules for the ADM interface.								
11	▶ NAT_Adm_Out	✔	Adm	Admnet	Wan	all-nets	all_services	SRC:NAT
12	▶ Adm_Internal_Access	✔	Adm	Admnet	any	all-nets	all_services	

Abbildung 2.8.3 Administrator-Zugang zu den internen Ressourcen hinzufügen

Diese neue Regel hat keinerlei Beschränkungen bei der Ziel-Schnittstelle oder dem Netzwerk. Sie erlaubt vollständigen Zugang zu allem von der ADM-Schnittstelle aus.

Beachten Sie außerdem, dass die neue Regel keine Adressübersetzung nutzt. Es gibt keinen dringenden Grund, bei interner Kommunikation Adressübersetzung anzuwenden, solange wir kein Szenario haben wie das, das im vorangegangenen Rezept beschrieben wurde.

Natürlich wird es immer Ausnahmen und besondere Umstände geben, die eine NAT-Regel oder sogar FwdFast-Regeln erfordern, aber es ist nicht der Anspruch dieses Buches, alle möglichen Szenarien zu besprechen.

Hinweis

Der Administrator-Schnittstelle und dem -Netzwerk vollständigen Zugang zu allen Schnittstellen und allen Netzwerken zu geben, kann als Sicherheitsrisiko angesehen werden. In diesem Stadium bräuchte man nur einen PC im Administrator-Netzwerk zu platzieren und er hätte vollständigen Zugang zu allen Netzwerk-Ressourcen, was einen Netzwerk-Scan extrem einfach machen würde.

Es liegt beim Administrator, zu entscheiden, wie weit er den Zugang zu den Netzwerken von den verschiedenen Schnittstellen einschränkt. Es gibt viele Sicherheitsmechanismen und Wege, um den cOS-Core so zu konfigurieren, dass die Auswirkung unautorisierten Zugangs verringert werden kann. Viele davon werden wir im weiteren Verlauf des Buches besprechen.

Administrator-Zugang zur DMZ erweitern

Wie auch andere Schnittstellen haben wir die ADM-Schnittstelle noch nicht zu unserer Schnittstellengruppe hinzugefügt, die für eingehende Verbindungen zum Webserver genutzt wird. Nachdem wir die ADM-Schnittstelle unserer Schnittstellengruppe hinzugefügt haben, sieht sie aus wie im nächsten Bildschirmfoto gezeigt.

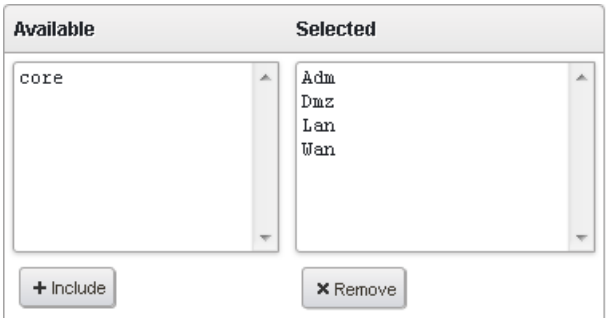


Abbildung 2.8.4 ADM-Schnittstelle zu einer Schnittstellengruppe hinzufügen

Wir haben jetzt der Schnittstellengruppe alle Schnittstellen außer der Core-Schnittstelle hinzugefügt. Gibt es noch irgendeinen Grund, hier Schnittstellengruppen zu nutzen?

Die Antwort ist „Nein". Es gibt keinen wirklichen Vor- oder Nachteil, in diesem besonderen Szenario eine Schnittstellengruppe zu nutzen. Statt die Schnittstellengruppe im IP-Regelsatz zu nutzen, könnten wir auch „Irgendwas" als Schnittstelle nutzen.

Nach dem entsprechenden Anpassen unserer IP-Regeln sieht die endgültige Version des Regelsatzes, das wir in diesem Kapitel erstellt haben, nun wie folgt aus.

#	Name	L...	Src If	Src Net	Dest If	Dest Net	Service	Address Translation
Rules for incoming traffic								
1	▶ SAT_Incoming_WebServer	✔	any	all-nets	core	Wan_ip	http-all	DST:SAT(WebServer)
2	▶ NAT_Incoming_Dmz	✔	Dmz	Dmznet	core	Wan_ip	http-all	SRC:NAT
3	▶ Allow_Incoming_WebServe	✔	any	all-nets	core	Wan_ip	http-all	
Rules for the Dmz interface								
4	▶ NAT_Dmz_HTTP	✔	Dmz	Dmznet	Wan	all-nets	http	SRC:NAT
5	▶ NAT_Dmz_HTTPS	✔	Dmz	Dmznet	Wan	all-nets	https	SRC:NAT
6	▶ NAT_Dmz_DNS	✔	Dmz	Dmznet	Wan	all-nets	dns-all	SRC:NAT
Rules for the Lan interface								
7	▶ NAT_Lan_HTTP	✔	Lan	Lannet	Wan	all-nets	http	SRC:NAT
8	▶ NAT_Lan_HTTPS	✔	Lan	Lannet	Wan	all-nets	https	SRC:NAT
9	▶ NAT_Lan_DNS	✔	Lan	Lannet	Wan	all-nets	dns-all	SRC:NAT
10	▶ Allow_Lan_To_Dmz	✔	Lan	Lan_To_Dmz_Grp	Dmz	Dmznet	all_services	
Rules for the ADM interface.								
11	▶ NAT_Adm_Out	✔	Adm	Admnet	Wan	all-nets	all_services	SRC:NAT
12	▶ Adm_Internal_Access	✔	Adm	Admnet	any	all-nets	all_services	
Anything below this rule will be dropped!								
13	■ DropAll	✔	any	all-nets	any	all-nets	all_services	

Abbildung 2.8.5 Der endgültige IP-Regelsatz des Kapitels

Frage: *Warum soll man dann überhaupt Schnittstellengruppen nutzen? Wo ist der Vorteil?*

Antwort: In diesem Szenario hatten wir eine Situation, in der alle Netzwerke Zugang zu einer bestimmten Ressource benötigten, aber das ist kein gewöhnliches Szenario.

Die meisten Szenario benötigen nur Zugang von einem oder zwei Schnittstellen. Je mehr wir den Zugang zu einer bestimmten Ressource begrenzen, desto besser. „Irgendwas" oder „alle-Netze" als Schnittstelle oder Netzwerk einzustellen, sollte mit besonderer Vorsicht geschehen.

In diesem Setup hatten wir nur vier Schnittstellen, aber was ist, wenn wir 20 Schnittstellen oder ein Szenario haben, wo eine große Anzahl an VLANs genutzt wird, die die Anzahl der Schnittstellen auf über tausend ansteigen lässt? Es ist immer besser, den geringstmöglichen Zugang in IP-Regeln festzulegen. Dies nicht zu tun, kann „Löcher" entstehen lassen, durch die die Regeln unbeabsichtigten Zugang zu Schnittstellen und Netzwerken erlauben.

Rezept 2.9. DMZ-Zugang von der LAN-Schnittstelle

Ziele

Dieses Rezept bespricht, wie man einen DHCP-Server (Dynamic Host Configuration Protocol, Dynamisches Host-Konfigurationsprotokoll) an der LAN-Schnittstelle einstellt.

DHCP-Server sind in jedem Netzwerk äußerst nützlich, egal, wie viele Nutzer es hat. Sie können automatisch IP-Adressen und Netzwerk-Definitionen an Clients ausgeben. Direkte Eingriffe vom Administrator mithilfe statischer IP- und Netzwerk-Einstellungen ist unnötig. DHCP hilft außerdem, zu vermeiden, dass dieselbe IP aus Versehen mehr als einmal vergeben wird. Doppelt vergebene IP-Adressen können in einem Netzwerk zu IP-Konflikten führen, die viele Probleme verursachen können und schwer aufzufinden sind.

Die nachfolgende Abbildung 2.9.1 zeigt die LAN-Schnittstelle mit einer Vielzahl verbundener Clients, die IP-Adressen brauchen, die ihnen mithilfe von DHCP zugewiesen werden.

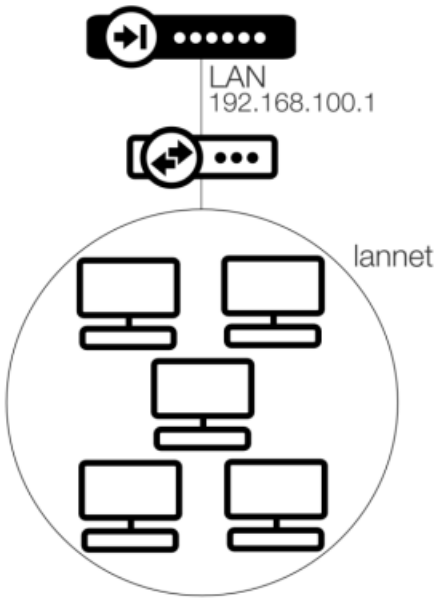


Abbildung 2.9.1 Viele Client-PCs hinter der LAN-Schnittstelle

Detailbesprechung

Um DHCP-Server im WebUI hinzuzufügen und einzustellen, gehen Sie zu **Netzwerk > Netzwerk-Dienste > DHCP > DHCP-Server**, wie im nachfolgenden WebUI-Bildschirmfoto gezeigt.

Abbildung 2.9.2 DHCP-Server

Wenn wir den DHCP-Server anlegen, müssen wir entscheiden, wie viele IP-Adressen der Adresspool enthalten soll.

Die Netzwerkgröße der LAN-Schnittstelle ist ein /24-Netzwerk, so dass wir insgesamt 254 Adressen nutzen können. 192.168.100.1 wird schon vom cOS-Core selbst genutzt, so dass diese Adresse immer ausgeschlossen sein muss. Abhängig von der Anzahl der Nutzer im Netzwerk wird empfohlen, mit den oberen Bereichen des Netzwerk-Umfangs zu beginnen, um Konflikte mit irgendwelchen statisch gesetzten IP-Adressen zu vermeiden, die üblicherweise im unteren Bereich festgelegt werden.

Daher werden wir den Netzwerkbereich von 192.168.100.100 bis 192.168.254 definieren, so dass wir insgesamt 154 verbundene Clients ohne die statisch festgelegten Clients haben können. Die wesentlichen DHCP-Server-Optionen werden im nächsten Bildschirmfoto dargestellt.

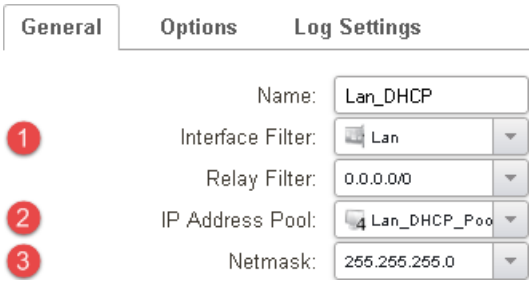


Abbildung 2.9.3 Allgemeine Einstellungen des DHCP-Servers

Zuerst legen wir fest, dass der Schnittstellenfilter (**1**) LAN sein soll. Dies ist die Schnittstelle, an der der DHCP-Server auf eingehende DHCP-Anfragen wartet.

Zweitens werden wir das zuvor definierte IP-Pool-Netzwerkobjekt für den IP-Adressenpool (**2**) verwenden. Zu guter Letzt müssen wir eine Netzmaske definieren (**3**). Weil wir

eine Netzwerkgröße von /24 haben, lassen wir die Netzmaske auf dem Standardwert 255.255.255.0. Dies muss von Hand eingestellt werden, wenn die Netzwerkgröße nicht der standardmäßigen /24 entspricht, weil die Berechnung der Netzmaske nicht automatisch erfolgt.

Als nächstes wechseln wir zum **Optionen**-Tab. Es gibt zwei weitere Optionen, die wir festlegen müssen, damit der DHCP-Server vollständig funktioniert; sie werden im nächsten Bildschirmfoto gezeigt.

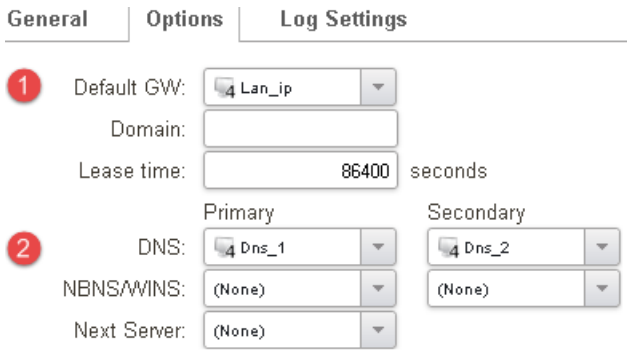


Abbildung 2.9.4 DHCP-Server-Optionen

Die erste Option ist das standardmäßige Gateway (**1**). Das ist das normalerweise genutzte Gateway, das die Clients nutzen sollen, wenn sie ein IP-Nutzungsangebot vom cOS-Core bekommen. Weil die Clients sich hinter der LAN-Schnittstelle befinden und wir wollen, dass sie den cOS-Core nutzen, um das Internet zu erreichen, wählen wir hierfür die Lan_ip-Schnittstelle.

Als nächstes müssen wir einen primären (**2**) und wahlweise einen sekundären DNS-Server festlegen. Das ist nötig, damit Clients DNS-Anfragen machen können, ohne von Hand auf jedem Client einen DNS-Server einrichten zu müssen.

Erzeugen Sie mithilfe der Informationen Ihres Internetdienstanbieters zwei neue Netzwerkobjekte im Adressbuch des cOS-Cores für den primären und den sekundären DNS-Server, und nutzen Sie diese beiden Objekte mit dem DHCP-Server.

Nachdem wir diese Einstellungsänderungen angewendet haben, haben wir einen vollständig funktionierenden DHCP-Server.

Hinweis

Der DHCP-Server hat viele Optionen, die wir noch nicht besprochen haben, wie z.B. den Relaisfilter, die Domäne und Nutzungszeiten. Der Grund dafür ist, dass wir erst einmal die Grundeinstellungen machen. Die Optionen und Einstellungen, die wir hier besprochen haben, sind die absoluten Minimalanforderungen, um einen DHCP-Server für die häufigsten Situationen einzurichten und ans Laufen zu bekommen.

Rezept 2.10. Hinter der DMZ-Schnittstelle einen Protokoll-Empfänger hinzufügen

Ziele

Dieses Rezept erklärt, wie man einrichtet, dass der cOS-Core Versandprotokolle an einen Ziel-Protokollempfänger versendet. Der cOS-Core erzeugt fortwährend Protokollereignis-Nachrichten, die aufzeichnen, was im Netzwerk geschieht. Nachrichten können alles Mögliche sein, von DHCP-Server-Ereignissen bis zu Client-Verbindungen, die erstellt werden, wenn man eine Webseite im Internet aufruft.

Es wird dringend empfohlen, einen Protokollempfänger einzurichten und bei Problemen in die erhaltenen Protokollereignisse zu schauen oder einen Überblick über die Netzwerk-Nutzung zu haben. Die nachfolgende *Abbildung 2.10.1* zeigt einen Protokollempfänger hinter der DMZ-Schnittstelle.

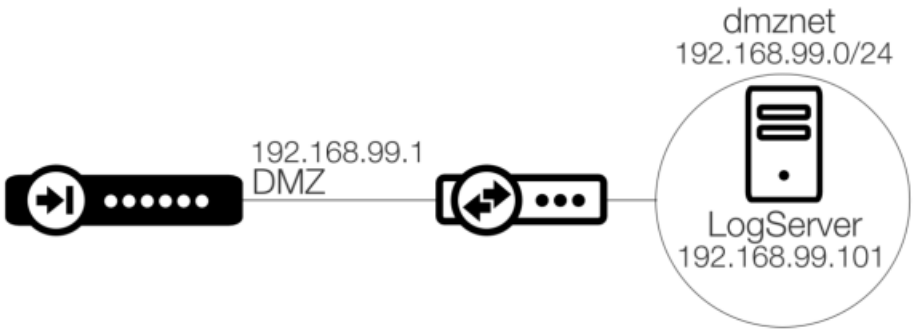


Abbildung 2.10.1 Systemprotokoll-Server hinter der DMZ-Schnittstelle

Detailbesprechung

Die Ereignis-Nachrichten, die der cOS-Core erzeugt, können an verschiedene Arten von Protokollempfängern geschickt werden. Um Nachrichten zu empfangen, ist es nötig, einen oder mehrere Ereignisempfänger-Objekte im cOS-Core einzurichten, die festlegen, welche Ereignisse aufgezeichnet und wohin sie gesendet werden sollen. Es ist nur selten notwendig, die standardmäßigen Protokollereignis-Einstellungen beim Protokollempfänger zu ändern, weil die Standardeinstellungen schon fast alle Situationen abdecken.

Ein Protokollempfänger kann entweder MemLog (memory log receiver, Speicher-Protokollempfänger), SysLog, ein InControl-Protokollempfänger oder ein SNMP-Ereignisempfänger (Simple Network Management Protocol, Einfaches Netzwerkverwaltung-Protokoll) (für Ausfälle) sein, wie im nachfolgenden Menü gezeigt.

Um einen Protokollempfänger einzurichten und/oder hinzuzufügen, gehen Sie im WebUI zu **System > Gerät > Protokoll- und Ereignisempfänger**.

Abbildung 2.10.2 Einen Protokollempfänger hinzufügen

Hinweis

Es kann immer nur einen Speicher-Protokollempfänger geben. Wenn schon einer vorhanden ist, wird keine Möglichkeit angezeigt, einen anderen hinzuzufügen.

Die verschiedenen Arten von Protokollempfängern sind:

- **Speicher-Protokollempfänger**

  Der cOS-Core hat seinen eigenen Protokollierungsmechanismus, der auch MemLog bezeichnet wird. Dieser behält eine begrenzte Anzahl an Protokollereignis-Nachrichten im Speicher und bietet durch das Web-Interface die Möglichkeit, die jüngsten Protokollnachrichten direkt anzuschauen. Weil diese nur im Speicher gehalten werden, werden sie rasch überschrieben, sobald neue Protokolleinträge generiert werden. Das Speicherprotokoll wird außerdem gelöscht, wenn das System neu startet.

- **System-Protokollempfänger**

  Das Systemprotokoll (Syslog) ist der tatsächliche Protokollnachrichten-Standard, um Ereignisse von Netzwerk-Geräten zu protokollieren.

- **InControl-Protokollempfänger**

  Das separat erhältliche Produkt „Clavister Zentralverwaltung“ ist in der Lage, Protokollereignis-Nachrichten von einer oder von vielen Clavister-Firewalls der nächsten Generation zu empfangen und zu analysieren. Ereignisnachrichten, die zum InControl- Protokollempfänger gesendet werden, nutzen ein eigenes Ereignisnachrichtenformat von Clavister zum Protokollieren, genannt FWLog. Dieses Format kann sehr viele Details transportieren und ist geeignet, die Analyse großer Mengen an Protokolldaten zu analysieren.

- **SNMP-Fallen**

  Ein SNMP2c-Ereignisempfänger kann so eingestellt werden, dass er SNMP-Fallen-Protokollnachrichten sammelt. Diese Empfänger werden üblicherweise benutzt, um

kritische Warnmeldungen von Netzwerk-Geräten zu sammeln und darauf zu antworten.

Einen SysLog-Empfänger hinzufügen

Als Beispiel werden wir einen SysLog-Empfänger hinzufügen, der sich hinter der DMZ-Schnittstelle befindet. Für eine Grundeinstellung brauchen wir im cOS-Core nur ein Netzwerk-Objekt mit der IP des Protokollempfänger-Servers (in diesem Fall 192.168.99.101) anzulegen und dann dieses IP-Adressobjekt in der SysLog-Empfängereinstellung auszuwählen, wie nachfolgend gezeigt.

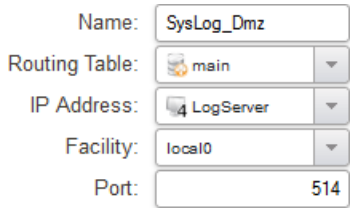


Abbildung 2.10.3 Einen Syslog-Empfänger einstellen

Sobald die Konfiguration angewendet ist, beginnt der cOS-Core damit, alle generierten Protokollereignisse an den Protokollempfänger zu senden. Es ist zudem möglich, einige Protokollkategorien und Protokoll-IDs, die an die Protokollempfänger gesendet werden, auszuschließen, falls sie für den Administrator nicht von Bedeutung sind. Beachten Sie jedoch, dass einige Protokollereignisse benötigt werden, um Berichte wie z.B. die für Bandbreitennutzung zusammenzustellen. Wenn kritische Protokolleinträge nicht enthalten sind, wird der Bericht unvollständig sein oder überhaupt keine gewünschten der Daten darstellen.

Die standardmäßige Einstellung im cOS-Core begrenzt die Maximalanzahl der Protokolle, die pro Sekunde verschickt werden können, auf 2.000, aber sie kann erhöht werden, wenn notwendig.

Damit schließen wir das Kapitel zur Grundeinstellung.

Kapitel 3: Die Universität

3.1. Einleitung

Willkommen auf dem Campus der Clavister-Universität. In diesem Kapitel werden wir eine Situation betrachten, in der wir ein Universitätsnetzwerk von Grund auf entwerfen. Dabei werden wir von einer Grundeinstellung zu einem erweiterten Netzwerk übergehen und mehr Funktionalität für Fortgeschrittene einbauen, wie z.B. Webinhalt-Filter, Virenschutz, Anwendungskontrolle, Bandbreitenverwaltung und weiteres.

Ab diesem Kapitel und weitergehend gehen wir davon aus, dass Sie mit der Clavister-Art, Regeln einzustellen, mit Routingprinzipien und so weiter vertraut sind.

Einige der einfachen IP-Regeln, Verwaltungszugang und Routen wurden bereits weiter vorn in diesem Buch eingerichtet. Falls Sie die beiden vorigen Kapitel nicht gelesen haben, empfehlen wir, dies jetzt nachzuholen, falls Sie noch gar keine Erfahrung mit Clavister und dem cOS-Core haben.

Wir beginnen mit einer Übersicht dessen, was wir aufbauen wollen. Die Grundidee ist, dass alle Studierenden auf dem Campus und in ihrem Wohnheim Internetzugang haben soll, indem sie WLAN oder eine normale Ethernet-Verbindung nutzen.

Abbildung 3.1.1 Der Universitäts-Campus

Im Verlauf dieses Kapitels werden wir Beschränkungen für Bandbreiten und dafür, was Studierende im Internet besuchen dürfen, einbauen, indem wir Webseiten-Klassifizierung einführen.

Das Netzwerk wird ähnlich wie im vorigen Kapitel aufgebaut, indem wir mit einem einfachen Netzwerk beginnen und der Konfiguration nach und nach mehr Funktionalität, Eigenschaften und Komplexität hinzufügen. Die Rezepte können alle für sich benutzt werden, aber es kann sein, dass sie sich auf das Universitätsnetzwerk und seine Einstellungen beziehen.

3.2. Das Netzwerk einrichten

Bevor wir anfangen, die verschiedenen Rezepte einzurichten, müssen wir einen Überblick des Netzwerks besprechen. Wir brauchen einige einleitende Netzwerk-Definitionen und Netzwerk-Objekte für das Grundsetup, ähnlich wie im vorigen Kapitel besprochen.

Ein Überblick über das Campus-Netzwerk ist in der nachfolgenden *Abbildung 3.2.1* dargestellt.

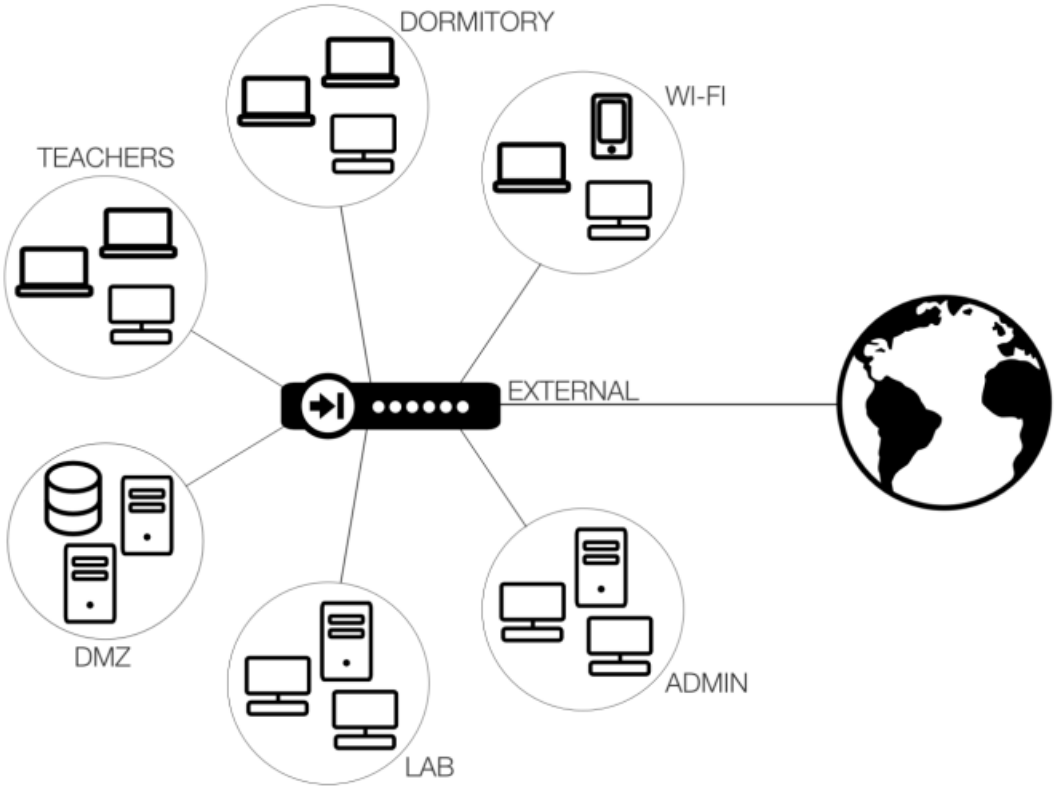


Abbildung 3.2.1 Übersicht des Campus-Netzwerks der Universität

Für diese Installation haben wir eine Clavister-Firewall der nächsten Generation mit acht physischen Ethernet-Schnittstellen gewählt.

Für den Moment beginnen wir mit den in der nachfolgenden *Tabelle 3.2.2* gelisteten einleitenden Adressbuch-Definitionen für diese Schnittstellen.

Schnittstellenname	Netzwerk
EXTERN	203.0.113.0/24
WLAN	10.10.0.0/16

Schnittstellenname	Netzwerk
WOHNHEIM	10.20.0.0/16
DOZENTEN	172.16.0.0/24
DMZ	172.16.10.0/24
H1	172.16.20.0/24
LABOR	192.168.0.0/24
ADMIN	192.168.254.0/24

Tabelle 3.2.2 Adressbuch-Definitionen

Wir haben IP-Adresse und Netzwerke an allen Schnittstellen eingestellt, auch wenn diese z.T. noch gar nicht genutzt wurden. Wenn wir den cOS-Core zum ersten Mal einstellen, hat jede Schnittstelle (außer der Verwaltungsschnittstelle) eine IP-Adresse und ein Netzwerk im Localhost-IP-Bereich 127.x.x.x.

Wie in den obigen Adressen gezeigt, haben wir das Netzwerk an den Schnittstellen WLAN und WOHNHEIM als Netzwerke mit /16-Größe statt der üblicheren /24-Größe festgelegt. Der Grund dafür ist, dass wir jede Menge IP-Adressen an diesen Schnittstellen brauchen werden.

Indem wir die Netzwerkgröße auf /16 erweitern, haben wir Zugang zu mehr als 65.000 Adressen im Vergleich zu den üblichen 254 eines Netzwerks mit /24-Größe. Wir erwarten, dass wir an diesen Schnittstellen eine Vielzahl Nutzer und Geräte haben werden.

Aber was ist mit der LABOR-Schnittstelle? Wenn wir hunderte oder sogar tausende Studierende haben, die zu einem bestimmten Anlass alle die Labor-Umgebung nutzen, reichen 254 Adressen dann aus?

Nein, werden sie nicht, aber wir werden diese Situation noch in einem späteren Kapitel behandeln, indem wir einen anderen Ansatz mit VLANs und Virtuellem Routing nutzen.

Tipp

Indem wir eindeutige Netzwerke und IP-Adressen an jeder Schnittstelle festlegen, machen wir uns die spätere Fehlersuche bei Problemen im Netzwerk wesentlich einfacher.

Wenn Sie ein bestimmtes Netzwerk sehen, das dort nicht sein sollte, wissen Sie augenblicklich, wo dieses Netzwerk geroutet wird und wo sie folgerichtig in der Konfiguration oder bei den angeschlossenen Switches und Routern nachsehen müssen.

Wenn Sie stattdessen viele Anfragen von 127.0.0.1 sehen, ist es wesentlich schwieriger, mögliche Probleme zu beheben.

Wie schon im ersten Kapitel erwähnt, empfehlen wir dringend, dass Sie möglichst oft in Ihrer Konfiguration Kommentargruppen nutzen.

Wenn Sie mit vielen Objekten, Schnittstellen und Routen hantieren, ist es viel einfacher, einen Überblick in der Konfiguration zu behalten, wenn alles gut dokumentiert ist.

Ein Beispiel, wie Sie Kommentargruppen im Adressbuch des cOS-Cores nutzen, wird im nachfolgenden WebUI-Bildschirmfoto gezeigt.

# ▲	Name	Address
Networks related to internet and the external interface		
1	External_Gateway	203.0.113.1
2	External_ip	203.0.113.10
3	External_net	203.0.113.0/24
Networks and hosts related to the Wi-Fi interface.		
4	Wi-Fi_ip	10.10.0.1
5	Wi-Fi_net	10.10.0.0/16
Networks and hosts related to the Dormitory interface.		
6	Dormitory_ip	10.20.0.1
7	Dormitory_net	10.20.0.0/16

Abbildung 3.2.3 Kommentargruppen nutzen

Der beabsichtigte Zweck jeder Schnittstelle unserer Clavister-Firewall ist in der nachfolgenden *Tabelle 3.2.4* zusammengefasst.

Schnittstellenname	Nutzung
WLAN	Campus-WLAN-Zugang. Alle wollen Zugang zum WLAN-Netzwerk haben, solange sie Teil der Universität sind.
WOHNHEIM	Die physische Ethernet-Verbindung zu jeder Studierendenwohnung geht durch diese Schnittstelle. Weniger eingeschränkt als das WLAN-Netzwerk.
DOZENTEN	Die physischen Ethernet-Verbindungen zu jedem Dozenten-Computer in den Dozentenbüros und zu den Klassenzimmern gehen durch diese Schnittstelle. Weniger eingeschränkt als die WOHNHEIM- und WLAN-Schnittstellen.
DMZ	Die Entmilitarisierte Zone (DMZ) der Universität. Standort aller Webserver, FTP-Server, Speichergeräte usw., mit eingeschränktem Zugang für alle außer den Administratoren.
H1	Reservierte Schnittstelle zur Nutzung bei Hochverfügbarkeit
LABOR	Spezielles Labor-Netzwerk mit unbeschränktem Zugang zum Internet. Extrem unterteilt durch VLAN, um zu vermeiden, dass unterschiedliche Labor-Bereiche sich in andere einmischen.
ADMIN	Die physische Ethernet-Verbindung für die Administratoren geht durch diese Schnittstelle. Unbegrenzter Zugang zu allen Bereichen des Universitätsnetzwerks.

Tabelle 3.2.4 Schnittstellennutzung

Momentan eingestellte Schnittstellen-IP-Regeln

Jede Schnittstelle hat momentan zwei eingestellte IP-Regeln, von denen eine DNS-Anfragen zu den DNS-Servern am DMZ-Standort und die andere HTTP und HTTPS ins Internet erlaubt. Jeder interner Zugang wird momentan verweigert. Ausgenommen sind die Administratoren, die vollständigen Zugang sowohl zu internen als auch zu externen Netzwerken haben.

Ein kleines Beispiel des IP-Regelsatzes wird im nächsten Bildschirmfoto des WebUI gezeigt.

#	Name	L...	Src If	Src Net	Dest If	Dest Net	Service	Address Translation
Rules related to administrator interface and network.								
1	▶ Admin_Internet_Access	✔	Admin	Admin_net	External	all-nets	all_services	SRC:NAT
2	▶ Admin_Full_Internal_Access	✔	Admin	Admin_net	any	all-nets	all_services	
Rules related to Wi-Fi interface and network								
3	▶ Wi-Fi_DNS	✔	Wi-Fi	Wi-Fi_net	Dmz	Dmz_DNS_SrvGrp	dns-all	
4	▶ Wi-Fi_HTTP_All	✔	Wi-Fi	Wi-Fi_net	External	all-nets	http-all	SRC:NAT
Rules related to Dmz interface and network								
5	▶ Dmz_DNS	✔	Dmz	Dmz_net	External	all-nets	dns-all	SRC:NAT
6	▶ Dmz_HTTP_All	✔	Dmz	Dmz_net	External	all-nets	http-all	SRC:NAT

Abbildung 3.2.5 Momentane Regeln für die ADMIN und WLAN-Schnittstellen

Aufmerksame Leser mögen darauf hinweisen, dass die DNS-Regel für die DMZ anders aussieht. Das ist so, weil wir die DNS-Server an dieser Stelle benötigen, damit sie andere DNS-Server im Internet erreichen können, um externe DNS-Datensätze holen und speichern zu können. Ansonsten wären Nutzer, die die DNS-Server in der DMZ nutzen, nicht in der Lage, externe Adressen im Internet aufzulösen.

Andere Server an der DMZ-Schnittstelle, die die DNS-Server der DMZ nutzen, brauchen keine weiteren speziellen Regeln. Dieser Datenverkehr gelangt nicht durch die Firewall, weil sie sich im gleichen lokalen Netzwerksegment befinden und diese Anfragen einfach durch den lokalen Switch gehen.

Das hängt natürlich von den Netzwerk-Bedingungen ab, so dass die Anforderungen an die Regel unterschiedlich sein können.

Rezept 3.3. DHCP einstellen

Ziele

Dieses Rezept bespricht die Einstellung von DHCP-Servern (Dynamic Host Configuration Protocol), die überwiegend an den Schnittstellen der Universität genutzt werden. DHCP-

Server wurden in aller Kürze in *Rezept 2.9 vorgestellt. DMZ-Zugang an der LAN-Schnittstelle hinzufügen In diesem Rezept werden wir DHCP- Server in unserer Universitätsumgebung einrichten und nutzen.*

Abbildung 3.3.1 Wenn viele Nutzer eine IP-Adresse brauchen, wird DHCP benötigt

Detailbesprechung

DHCP-Server werden eingesetzt, um verbundenen Clients automatisch IP-Adressen zuzuweisen, ohne dass man die Adresse, das Gateway oder DNS-Server von Hand einstellen muss. Das ist in vielen Szenarios notwendig aufgrund der vielen Arbeit, die man ansonsten damit hätte, jeden Client von Hand zu konfigurieren.

Das trifft natürlich für eine Universität ganz besonders zu, die tausende von PCs, Servern, Telefonen und anderen Geräten haben kann, die alle eine eigene IP-Adresse brauchen.

Um einen DHCP-Server zu konfigurieren, müssen wir mindestens drei Adressbuch-Objekte erzeugen:

1. Ein IP-Adressen-Pool ist ein Bereich von IP-Adressen, die DHCP den Clients zuweisen kann.

2. Eine Gateway-Adresse. Sie wird von den Clients als ihr standardmäßiges Gateway benutzt, sobald sie ein IP-Nutzungsangebot vom DHCP-Server bekommen.

3. Eine oder mehrere DNS-Server-IP-Adressen. Sie werden gleichzeitig mit der Client-IP-Adresse und der Gateway-Adresse an die Clients ausgegeben und sagen ihnen, welche(n) Server sie für DNS-Anfragen ansprechen sollten.

DHCP-Objekte konfigurieren

Wir definieren die folgenden DHCP-Pools für die verschiedenen Schnittstellen und Netzwerke, wie nachfolgend in *Tabelle 3.3.2* gezeigt.

Name	Schnittstelle	DHCP-Pool
WLAN-DHCP-Pool	WLAN	10.10.128.0/17
WOHNHEIM-DHCP-Pool	WOHNHEIM	10.20.128.0/17
DOZENTEN-DHCP-Pool	DOZENTEN	172.16.0.21-172.16.0.254
DMZ-DHCP-Pool	DMZ	172.16.10.201-172.16.10.254
LABOR-DHCP-Pool	LABOR	192.168.0.101-192.168.0.254
ADMIN-DHCP-Pool	ADMIN	192.168.254.128/25

Tabelle 3.3.2 DHCP-IP-Pools, verschiedenen Schnittstellen zugewiesen

Lassen Sie uns nun anschauen, warum wir diese Poolobjekte so definiert haben.

Unsere Entscheidungen gründen alle darauf, welche Art Schnittstelle sie betreffen und was wir hinter dieser Schnittstelle erwarten. Beginnen wir damit, den WLAN- und WOHNHEIM-DHCP-Pool zu betrachten: Wir haben das ganze /16-Netzwerk in zwei Hälften aufgeteilt und die obere Netzwerkhälfte dem DHCP-Pool zugewiesen, was mehr als 32.000 Adressen entspricht. Wir könnten natürlich auch das gesamte /16 nutzen, aber grundsätzlich besteht kein Grund, einen so großen IP-Pool zu haben. Daher lassen wir mehr als ausreichend Platz für zukünftige Netzwerkänderungen, so dass der IP-Pool leicht erweitert

werden kann, um einen größeren Teil des /16-Netzwerks zu umfassen, wenn der Bedarf an IPs steigt.

Der Dozenten-IP-Pool enthält 234 IP-Adressen. Für den Fall, dass wir eine Erweiterung brauchen oder weil wir eventuell einigen Nutzern statische IP-Adressen zuweisen, lassen wir die ersten 20 aus.

Dasselbe gilt für die DMZ-Schnittstelle, aber hier haben wir unterschiedliche Anforderungen an das Netzwerk. Das DMZ-Netzwerk wird viele Server enthalten und die Mehrzahl dieser Server wird statische IP-Adressen haben. Daher ist es immer noch richtig, einen DHCP-Server an der DMZ-Schnittstelle zu haben, aber sein IP-Pool wird deutlich kleiner sein, in diesem Fall nur 53 IP-Adressen.

Ebenso ist es beim Labor-Netzwerk. Weil wir hinter dieser Schnittstelle jede Menge Tests erwarten, haben wir eine ähnlich kleine Größe für dessen DHCP-Server-Adresspool festgelegt.

Schließlich noch die ADMIN-Schnittstelle. Hier erwarten wir eine Mischung aus statischen und dynamischen IP-Zuweisungen, weshalb wir das Netzwerk einfach mithilfe einer /25-Netzmaske aufteilen.

Das Gateway und DNS-Objekte

Das Gateway-Adressobjekt existiert in den meisten Fällen schon, wenn wir an diesem Punkt angekommen sind. Wenn wir einen Nutzer hinter dem WLAN-Netzwerk haben, wird das standardmäßige Gateway für ihn die IP-Adresse sein, die von der WLAN-Schnittstelle genutzt wird. Und in unserer Universität haben wird dieses Objekt bereits früher definiert.

Für DNS erzeugen wir zwei Adressbuch-Objekte, die auf die DNS-Server verweisen, die unsere Clients nutzen sollen, sobald sie ein Nutzungsangebot vom DHCP-Server bekommen. Unsere beiden Universität-DNS-Server befinden sich hinter der DMZ-Schnittstelle.

Den DHCP-Server einrichten

Jetzt, wo die benötigten Objekte definiert und erklärt sind, werden wir den DHCP-Server selbst hinzufügen und einstellen. Das machen Sie unter **Netzwerk > Netzwerk-Dienste > DHCP-Server** im WebUI, wie nachfolgend gezeigt.

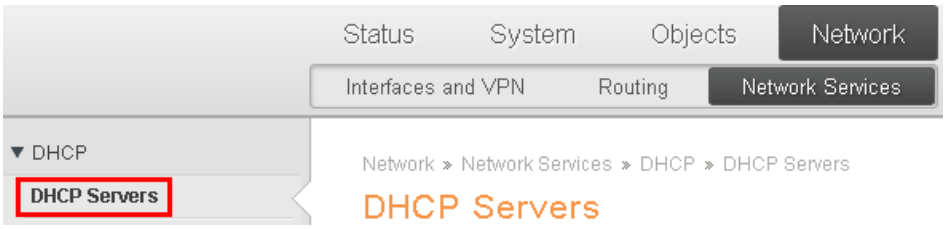


Abbildung 3.3.3 Einen DHCP-Server im WebUI definieren

Wenn der DHCP-Server angelegt ist, müssen wir einige der Standardoptionen und -Einstellungen festlegen. Diese werden im nächsten Bildschirmfoto vom WebUI des cOS-Cores gezeigt.

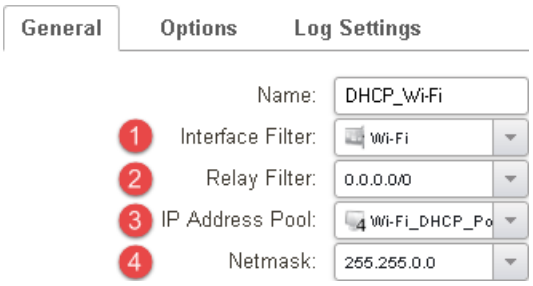


Abbildung 3.3.4 Allgemeine DHCP-Server-Optionen einstellen

Zunächst müssen wird (abgesehen vom Namen) wählen, an welcher Schnittstelle der DHCP-Server lauschen soll (**1**). In diesem Beispiel werden wir die WLAN-Schnittstelle nutzen.

Als nächstes kommt der Relais-Filter (**2**). Der kann dafür genutzt werden, DHCP-Anfragen entweder nur von der lokalen Schnittstelle oder von einem bestimmten DHCP-Weiterleiter zuzulassen. Weil wir an der WLAN-Schnittstelle alles zulassen wollen, lassen wir hier den Standardwert 0.0.0.0/0 (mit anderen Worten: alle-netze).

Die nächste Option (**3**) legt die IP-Adresse fest, die an den anfragenden Client ausgegeben werden sollte. Hier nutzen wir das WLAN-Pool-Objekt, das wir vorher angelegt hatten.

Als letztes kommt die Netzmaske (**4**), die an den anfragenden Client mit dem IP-Nutzungsangebot weitergeleitet wird.

Stellen Sie sicher, dass die Netzmaske richtig eingestellt ist, abhängig vom genutzten Netzwerk. Der voreingestellte Netzmaske-Wert ist 255.255.255.0, was einem C-Klasse-Netzwerk entspricht, aber im Fall der Netzwerke WLAN und WOHNHEIM soll es ein B-Klasse-Netzwerk sein, so dass die Netzmaske 255.255.0.0 lautet.

Hinweis

Der Netzmaske-Wert im DHCP-Server ist unabhängig von der Größe des DHCP-Pools. Er beruht auf der Netzwerkgröße.

Als nächstes werden wir den **Optionen**-Tab auswählen, wie im nächsten Bildschirmfoto gezeigt.

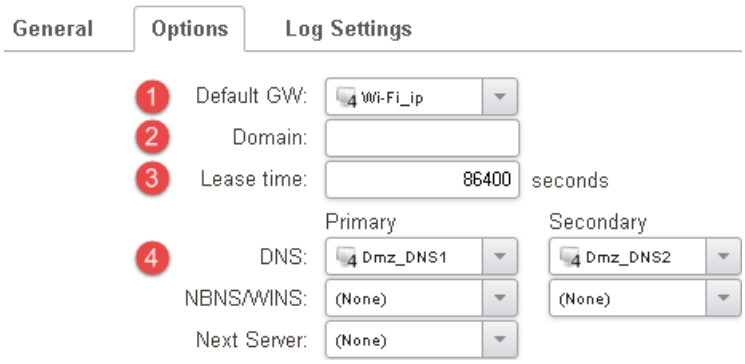


Abbildung 3.3.5 Andere DHCP-Server-Optionen festlegen

Hier ist die IP-Adresse der WLAN-Schnittstelle der Clavister-Firewall das standardmäßige Gateway (**1**). Jeder Client, der eine IP vom DHCP-Server erhält, wird sie automatisch als standardmäßiges Gateway für Netzwerke außerhalb seines eigenen Netzwerksegments nutzen, was in diesem besonderen Fall alles sein wird, was nicht Teil des WLAN-Netzwerks 10.10.0.0/16 ist.

Die Domäne-Option (**2**) ist der Domäne-Name, der für die Domänen-Endung genutzt wird. Das Konzept eines Domäne-Namens ist, dass der Client weiß, zu welcher Domäne er gehört; wenn Sie also z.B. nur das Wort „test" im Webbrowser eingeben, wird dieser versuchen, sich mit „test.domaene.firma" zu verbinden, weil er den Domäne-Namen schon kennt. Im Moment lassen wir diese Option leer, aber sobald die Universitätsdomäne eingerichtet ist und läuft, werden wir hier mit Sicherheit noch einen Wert eingeben.

Die Nutzungszeit (**3**) ist die Zeit in Sekunden, für die eine DHCP-Nutzung zur Verfügung steht. Nach dieser Zeit muss der DHCP-Client die Nutzung erneuern. Wir lassen diese Einstellung auf ihrem Standardwert von 86.400 Sekunden (24 Stunden).

Danach definieren wir DNS-Server (**4**), die sich in unserer DMZ befinden.

Zum Schluss ein kurzer Hinweis, der die Optionen NBNS/WINS und „Nächster Server“ erklären:

- **NBNS/WINS** ist die IP der „Windows Internet Name Service"-Server (WINS, Windows-Internetnamen-Dienst), die in Microsoft-Umgebungen genutzt werden, die die NetBIOS-Nameserver (NBNS) nutzen, um IP-Adressen NetBIOS-Namen zuzuweisen.
- **Nächster Server** legt die IP-Adresse des nächsten Servers im Bootvorgang fest. Das ist üblicherweise ein TFTP-Server.

Keine der beiden obigen Optionen wird in diesem Buch verwendet.

Jetzt haben wir einen vollständig funktionierenden DHCP-Server und können jetzt damit fortfahren, den anderen Schnittstellen und Netzwerken DHCP-Server hinzuzufügen, wie im nachfolgenden Bildschirmfoto gezeigt.

	Name	Interface	Relayer Filter...	IP Address Pool	Netmask	Enable logging
1	DHCP_Wi-Fi	Wi-Fi	0.0.0.0/0	Wi-Fi_DHCP_Pool	255.255.0.0	Yes
2	DHCP_Dormitory	Dormitory	0.0.0.0/0	Dorm_DHCP_Pool	255.255.0.0	Yes
3	DHCP_Lab	Lab	0.0.0.0/0	Lab_DHCP_Pool	255.255.255.0	Yes
4	DHCP_Dmz	Dmz	0.0.0.0/0	Dmz_DHCP_Pool	255.255.255.0	Yes
5	DHCP_Teachers	Teachers	0.0.0.0/0	Teachers_DHCP_Pool	255.255.255.0	Yes
6	DHCP_Admin	Admin	0.0.0.0/0	Admin_DHCP_Pool	255.255.255.0	Yes

Abbildung 3.3.6 DHCP-Server-Zusammenfassung

Nochmals: Vergessen Sie nicht, die *Klonen*-Option zu nutzen, um ähnliche Objekte rascher zu erzeugen.

Hinweis

Beim Bearbeiten der Einstellungen des DHCP-Servers im WebUI gibt es etwas, das zu Irritationen führen kann.

Wenn wir einen schon angelegten DHCP-Server öffnen, werden uns ***Static Host****- und* ***Eigene Optionen*** *angezeigt. Damit Sie die richtige Ansicht zum Bearbeiten sehen, klicken Sie bitte auf den Button* ***Dieses Objekt bearbeiten****, wie nachfolgend gezeigt.*

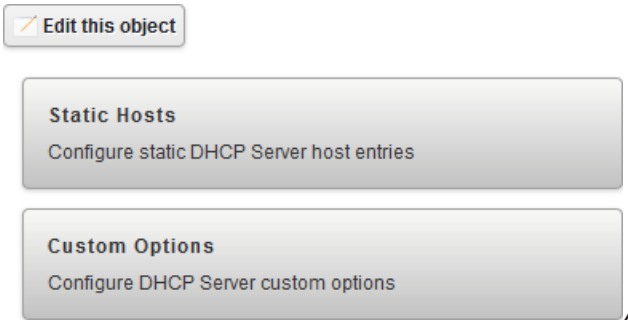


Abbildung 3.3.7 DHCP richtig bearbeiten

Rezept 3.4. Einen Hochverfügbarkeit-Cluster einstellen

Ziele

In unserem Universitätsbeispiel steht das Clavister-Firewall der nächsten Generation als zentraler Punkt im Netzwerk. Falls die Firewall aus dem einen oder anderen Grund ein Problem hat, werden große Teile des Netzwerks ausfallen. Damit dies nicht passiert, werden wir einen Hochverfügbarkeit-Cluster einbauen (HA-Cluster, alias High Availability Cluster), um dem Netzwerk zusätzliche Redundanz zu geben.

In diesem Rezept werden wir beschreiben, was ein Cluster ist, sowie die Einzelheiten der verschiedenen Cluster-Einstellungen, und wie HA konfiguriert wird.

Detailbesprechung

Der Zweck eines HA-Clusters

Die Hochverfügbarkeit des cOS-Cores (HA) gibt Installationen der Clavister-Firewall der nächsten Generation eine Fehlertoleranz-Möglichkeit. HA funktioniert so, dass eine weitere Clavister-Firewall als Absicherungs-"Slave" (Sklave) einer „Master"-Firewall (Herr) hinzugefügt wird. Master und Slave werden miteinander verbunden und bilden so einen logischen HA-Cluster. In einem Cluster ist immer eine Einheit aktiv, während die andere Einheit inaktiv und in Bereitschaft ist.

Grundsätzlich ist der Cluster-Slave inaktiv und beobachtet nur die Aktivitäten des Masters. Wenn der Slave feststellt, dass der Master nicht mehr arbeitet, tritt die HA-Ausfallsicherung (Failover) in Kraft, der Slave wird aktiv und übernimmt die Verantwortung für den gesamten Datenverkehr.

Wenn der Master später wieder funktionsfähig wird, wird der Slave weiter aktiv bleiben und der Master wird den Slave beobachten und nur dann wieder übernehmen, wenn der Slave ausfallen sollte. Dies wird manchmal auch als „aktiv-passive Implementierung von Fehlertoleranz" bezeichnet.

Einen Cluster zu nutzen, hat den wesentlichen Vorteil, dass sogar dann, wenn eine der Firewalls im Cluster ein Problem feststellt, das Netzwerk nicht als Ganzes betroffen ist. Die physische Konfiguration eines Clusters erfordert zusätzliche Hardware, um diese Redundanz bieten zu können.

Die nachfolgende Abbildung 3.4.1 zeigt eine einfache Konfiguration, die ein einzelnes Gerät mit nur zwei Schnittstellen nutzt, eine für interne Clients und eine andere für den externen Internetzugang durch einen Router.

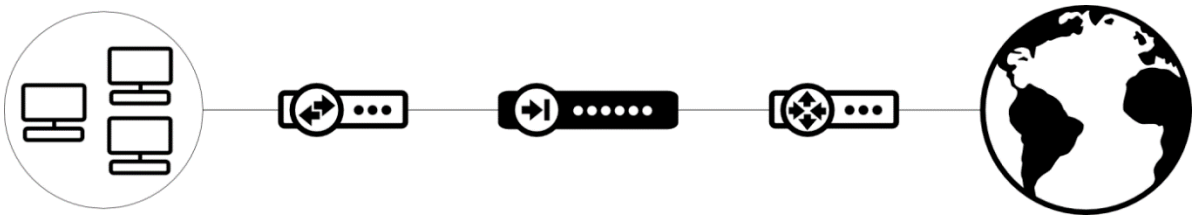


Abbildung 3.4.1 Konfiguration eines Einzelgeräts

Für einen HA-Cluster ist die obige Konfiguration etwas anders. Wie nachfolgend in *Abbildung 3.4.2* gezeigt, müssen sowohl Master- als auch Slave-Geräte am gleichen Switch

angeschlossen sein, weil beide Einheiten alle Netzwerk-Aspekte erreichen können müssen, unabhängig davon, welcher Knoten gerade der aktive ist.

Dies trifft für die externe Schnittstelle ebenfalls zu, obwohl es davon abhängt, welche Art von Router es ist. Wenn der Router selbst einen Switch oder mehrere Ports hat, ist es nicht nötig, vor den Router noch einen Switch zu setzen (dennoch ist es das üblichste Szenario). Die gepunktete Linie in *Abbildung 3.4.2* zeigt die direkte Verbindung zwischen den Cluster-Knoten der Schnittstelle H1 an, die als Synchronisierungsschnittstelle gestaltet wurde.

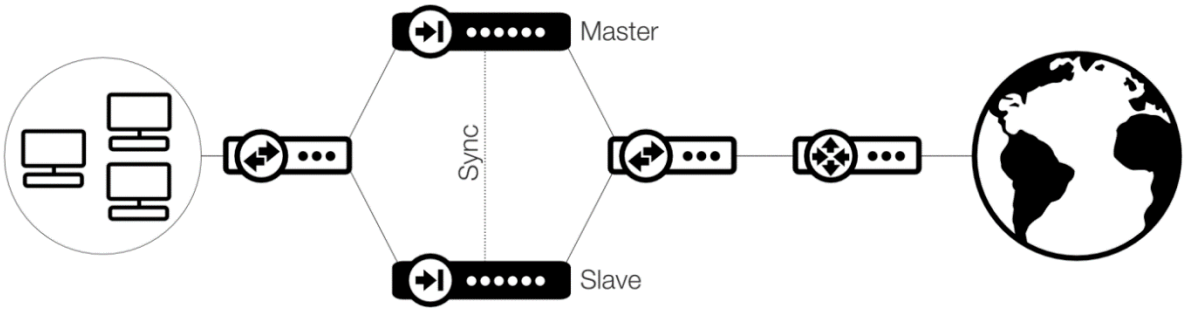


Abbildung 3.4.2 HA-Cluster-Konfiguration

Hinweis

Bitte behalten Sie im Hinterkopf, dass die Master-Einheit eines cOS-Core-Clusters nicht immer dasselbe ist wie die aktive Einheit in einem Cluster.

Bevor wir den Cluster selbst anlegen, müssen wir ein paar neue Adressbuch-Objekte vorbereiten. Ein Einzelgerät hat nur eine IP-Adresse pro Schnittstelle, aber ein Cluster hat drei. Eine IP wird als *Geteilte IP* genutzt, während die anderen beiden die individuellen IPs der beiden Cluster-Knoten sind.

Die *Geteilte IP* einer Schnittstelle meint die IP-Adresse, die von beiden Cluster-Knoten genutzt wird.

Weitergehende Informationen über geteilte IPs und ARP

Sowohl Master als auch Slave kennen die geteilte IP-Adresse. ARP-Anfragen für die geteilte IP-Adresse oder irgendeine andere IP-Adresse, die über den ARP-Konfigurationsabschnitt oder durch Proxy ARP veröffentlicht wird, werden vom aktiven

Knoten beantwortet. Die Hardware-Adresse der geteilten IP-Adresse und anderer veröffentlichter Adressen haben keinen Bezug zu aktuellen Hardware-Adressen der Schnittstellen.

Stattdessen wird vom cOS-Core die MAC-Adresse aus der Cluster-ID in der Form 11-00-00-C1-4A-nn konstruiert, wobei „nn" von einer Kombination der eingestellten Cluster-ID und dem Hartware-Bus/-Slot/-Port der Schnittstelle abgeleitet wird. Die Cluster-ID muss für jeden cOS-Core-Cluster eines Netzwerks eindeutig sein.

Weil die geteilte IP-Adresse immer dieselbe MAC-Adresse hat, gibt es keine Latenzzeit beim Aktualisieren der ARP-Caches für Geräte, die mit dem gleichen LAN wie der Cluster verbunden sind, wenn die Ausfallsicherung eintritt. Wenn ein Cluster-Mitglied feststellt, dass sein Gegenüber nicht mehr funktioniert, sendet es freie ARP-Anfragen mit der geteilten Hardware-Adresse als Senderadresse an alle Schnittstellen.

Dadurch können Switches innerhalb von Millisekunden umlernen, wohin sie Datenpaket senden sollen, die für die geteilte Adresse bestimmt sind. Die einzige Verzögerung, die also bei der Ausfallsicherung auftritt, ist das Erkennen, ob die aktive Einheit nicht mehr läuft. ARP-Anfragen werden ebenfalls in regelmäßigen Abständen gesendet, um sicherzustellen, dass die Switches nicht vergessen, wohin sie Datenpakete senden sollen, die für die geteilte MAC-Adresse bestimmt sind.

HA-Cluster-Setup einstellen

Wie zuvor erwähnt benötigen wir drei IP-Adressen, eine für jede Cluster-Schnittstelle. Die Geteilte IP-Adresse haben wir bereits angelegt, weil wir alle Schnittstellen-IP-Adressen als geteilt benutzen werden. Was wir noch brauchen, sind die individuellen IP-Adressen, die normalerweise für jede Schnittstelle als Master_IP und Slave_IP bezeichnet werden.

Diese Objekte haben einen speziellen Typ, der im Adressbuch angelegt werden kann, wie nachfolgend gezeigt.

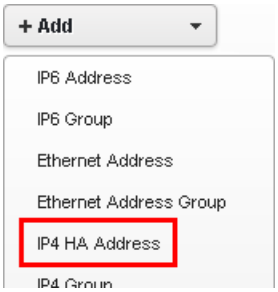


Abbildung 3.4.3 IPv4HA-Clusterobjekte anlegen

Bevor wir diese besonderen Objekte anlegen, müssen wir zunächst zwei neue normale IP-Adressen für jede der im Cluster benutzten Schnittstellen erzeugen, wie nachfolgend gezeigt.

Abbildung 3.4.4 IP-Adressbuchobjekte für Master und Slave erzeugen

Es ist übliche Praxis beim Anlegen eines Clusters, die ersten drei (oder die letzten drei) Adressen im Netzwerkbereich für die Nutzung durch den Cluster zu reservieren. Wie in der vorangegangenen Abbildung gezeigt, legen wir die IP-Adresse .2 für den Master und .3 für den Slave fest.

Nicht alle Schnittstellen brauchen drei IP-Adressen

Die individuellen HA-Adressen dienen hauptsächlich dem Administrator. Die beiden wichtigsten Funktionen, für die die individuellen Adressen genutzt werden, sind:

- **Verwaltung**

  Die Verwaltung muss in Richtung der individuellen Adresse gemacht werden, weil die Geteilte IP eine „virtuelle IP“ ist, die sich beide Cluster-Knoten teilen.

- **Generierung von Protokollereignis-Nachrichten**

  Wenn Protokollnachrichten vom cOS-Core an einen Protokollempfänger gesendet werden, muss er eine eindeutige IP-Adresse als Sender haben. Wir können nicht die geteilte IP-Adresse nutzen, weil wir dann keine Möglichkeit haben, herauszufinden, ob der Master oder der Slave sie gesendet hat.

Ein Problem beim Benutzen von Clustern ist die Notwendigkeit, drei öffentliche IP-Adressen zu haben, weil das nicht immer möglich ist. Dies ist keine Bedingung, solange wir nicht planen, das Gerät vom Internet aus zu verwalten und/oder Protokollnachrichten direkt an einen Host im Internet zu schicken.

Wir müssen nur eine öffentliche IP als die geteilte Adresse festlegen und können dann das automatisch erzeugte Adressbuch-Objekt namens „Localhost“ als Master-/Slave-IP nutzen. Das trifft auch auf alle anderen Schnittstellen zu.

Das standardmäßige „Localhost"-Objekt enthält die Adressen 127.0.0.1 und 127.0.02. Obwohl wir diese Objekte sogar als HA-Objekte für alle Schnittstellen (außer Verwaltung)

nutzen können, ist es empfohlen, trotzdem individuelle Adressen festzulegen. Wenn wir bei der Fehlersuche Datenpakete sehen, die von 127.0.0.1 kommen, ist das schwierig zuzuordnen, wenn diese Adresse verschiedensten Schnittstellen zugewiesen ist.

HA-Clusterobjekte den Schnittstellen zuweisen

In der Konfiguration des Universitätsbeispiels werden wir drei Adressen für alle Schnittstellen benennen. Die Objekte, die wir zuvor erzeugt haben, werden jetzt IPv4HA-Objekten im Adressbuch zugewiesen, wie im nächsten Bildschirmfoto gezeigt.

Abbildung 3.4.5 IPv4-Objekte mit einem IPv4HA-Objekt nutzen

Wir wiederholen diesen Vorgang für alle Schnittstellen außer der externen Schnittstelle, weil wir weder Bedarf haben, den Cluster vom Internet aus zu verwalten noch Protokolle irgendwohin ins Internet zu senden. Verwaltung und Protokolle werden intern behandelt.

Sobald alle Objekte und HA-Objekte erzeugt sind, müssen wir sie jeder Schnittstelle zuweisen. Dieser Vorgang kann erledigt werden, bevor der Cluster selbst angelegt ist. Um dies zu tun, rufen wir im WebUI den Ethernet-Abschnitt auf, wie im nachfolgenden Bildschirmfoto gezeigt.

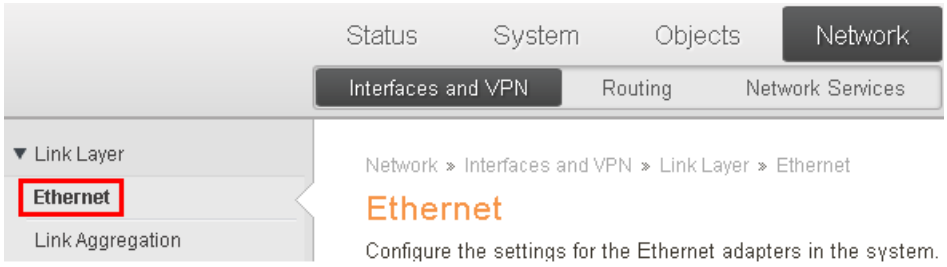


Abbildung 3.4.6 Der Ethernet-Abschnitt im WebUI

Wir öffnen eine der Schnittstellen und wählen dann den Erweitert-Tab und suchen den Abschnitt der privaten IP-Adresse, wie im nächsten WebUI-Bildschirmfoto gezeigt.

Abbildung 3.4.7 Für jede Schnittstelle eine private IP-Adresse festlegen

Dann setzen wir die korrekte private IP-Adresse für jede Schnittstelle, indem wir die zuvor erzeugten IPv4HA-Objekte nutzen; für die externe Schnittstelle wählen wir das Standardobjekt „localhost“.

Den HA-Assistenten starten

Jetzt ist alles vorbereitet, um die Konfiguration in einen Cluster zu verwandeln. Um dies fertigzustellen, gehen wir zum Abschnitt „Hochverfügbarkeit“ im WebUI, wie im nachfolgenden Bildschirmfoto gezeigt.

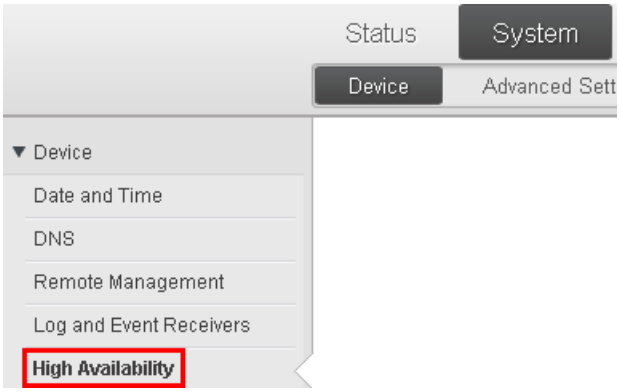


Abbildung 3.4.8 Der HA-Bereich im WebUI

Als nächstes wollen wir den Hochverfügbarkeit-Cluster-Assistenten starten, wie nachfolgend gezeigt.

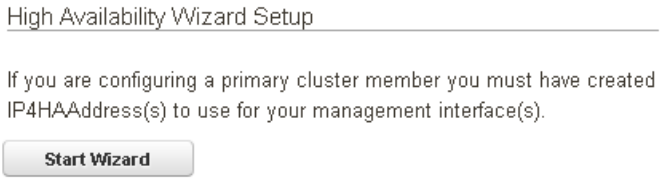


Abbildung 3.4.9 Den HA-Assistenten starten

Der Assistent erwartet, dass wir schon IPv4-HA-Objekte erzeugt haben, bevor wir ihn starten. Weil wir das bereits zuvor getan haben, können wir fortfahren, den HA-Assistenten zu nutzen, und das wird im nächsten Bildschirmfoto gezeigt.

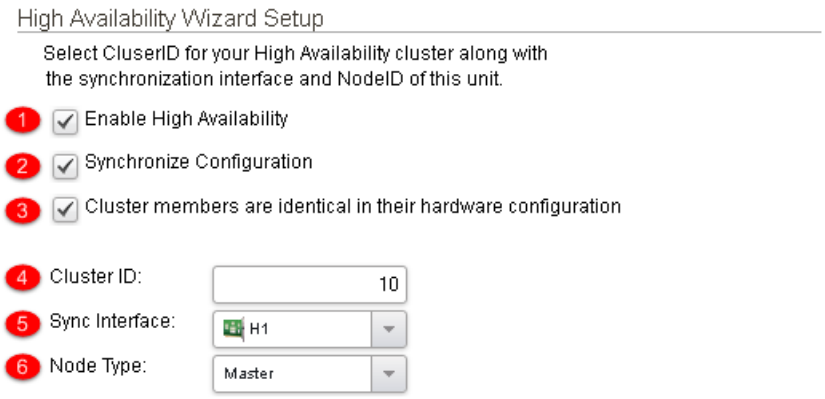


Abbildung 3.4.10 Das erste Setup mithilfe des HA-Assistenten

HA-Assistent-Einstellungen

Nachfolgend sehen Sie eine Beschreibung der Einstellungen, die im obigen Assistent-Bildschirmfoto gezeigt wurden:

1. Dies aktiviert den Cluster selbst.

2. **Konfiguration synchronisieren** bedeutet, dass eine Konfiguration, die auf den Master oder den Slave angewendet wurde, automatisch auf dem anderen Knoten synchronisiert wird. Wenn Sie den Haken dieser Option entfernen, heißt das, dass Sie entweder alle Änderungen in den Konfigurationen der Knoten selbst vornehmen müssen oder dass Sie Clavister InControl nutzen wollen, um die Konfiguration zu synchronisieren.

3. Dies bestätigt, dass die Cluster-Hardware identisch und standardmäßig aktiviert ist. Dies ist eine veraltete Einstellung, die nicht länger benutzt wird, weil alle Cluster heutzutage identische Hardware haben müssen.

4. Hier legen Sie die Cluster-ID fest. Wenn dies nicht der einzige Cluster in einem Netzwerk ist, muss die ID geändert werden, so dass sie eindeutig ist (Der Standardwert ist 0). Die ID wird außerdem verwendet, um die virtuelle MAC-Adresse zu generieren, die von den geteilten Schnittstellen-IPs verwendet wird. Weil wir nicht wissen, ob wir in Zukunft noch weitere Cluster hinzufügen werden, ist es ratsam, von der

standardmäßigen Null-ID wegzukommen. In diesem Fall wird die ID 10 genutzt. Die Cluster-ID kann zwischen 0 und 63 liegen.

5. Wir können wählen, welche Schnittstelle wir als die Synchronisierungsschnittstelle nutzen wollen. In einem Cluster müssen Master und Slave direkt miteinander über eine Synchronisierungsverbindung verbunden sein, die dem cOS-Core als die *Sync*-Schnittstelle bekannt ist. Eine der normalen Schnittstellen beim Master und beim Slave werden für diesen Zweck verwendet und werden mit einem Crosskabel miteinander verbunden.

   Der Cluster synchronisiert solche Daten wie Verbindungen, IPsec-Tunnelstatus, Route-Status und mehr. Das macht er, um so geringe Störungen wie möglich im Datenverkehr zu verursachen, falls/wenn im Cluster ein Aufgabenwechsel geschieht. Zum Beispiel würde dann, wenn eine Konfiguration angewendet wird, mindestens ein Aufgabenwechsel im Cluster durchgeführt. Wenn alles synchronisiert und aktuell ist, würden normale Nutzer überhaupt nichts davon mitbekommen.
6. Dies legt fest, welche Art Knoten diese Einheit ist. Es gibt zwei Optionen, Master oder Slave. Die erste im Cluster eingestellte Einheit wird normalerweise als der Master bezeichnet.

Den Cluster für den Master fertigstellen

Im letzten Schritt des HA-Assistent-Setups für den Master sehen Sie eine Zusammenfassung aller Schnittstellen, geteilter und privater IPs, wie nachfolgend gezeigt. Alle Änderungen in letzter Minute können Sie hier durchführen, bevor Sie den Cluster bereitstellen und aktivieren.

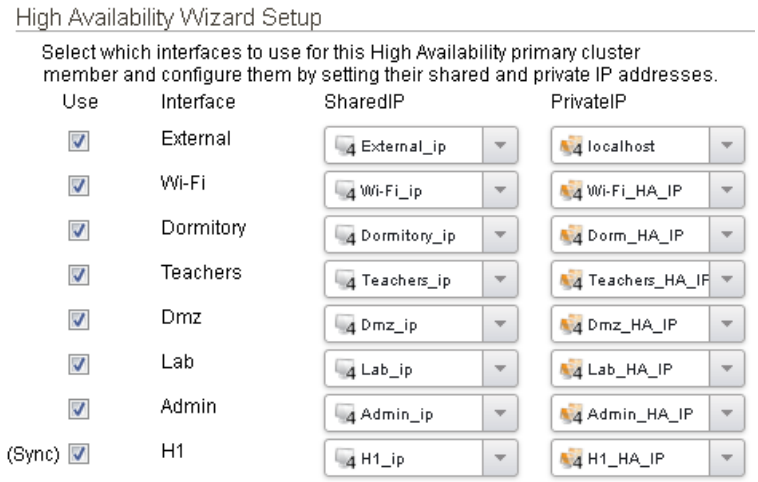


Abbildung 3.4.11 Zusammenfassung der geteilten und privaten IPs an jeder Schnittstelle

Sobald die Konfiguration angewendet ist, ist der Cluster zu 50 % fertig. Er ist jetzt ein Cluster ohne einen Partner-Knoten. Der Partner-Knoten wird der Slave sein.

Den Slave einstellen

Nachdem der Master konfiguriert ist und läuft, müssen wir den Slave-Knoten hinzufügen. Der Vorgang, den Slave hinzuzufügen, ist etwas anders, aber viel leichter, als den Master hinzuzufügen.

Dazu rufen wir im WebUI die Slave-Einheit auf, wählen dort den Hochverfügbarkeit-WebUI-Abschnitt und starten den HA-Assistenten erneut. Hier müssen wir drei Einstellungen ändern, die im nächsten Bildschirmfoto gezeigt werden.

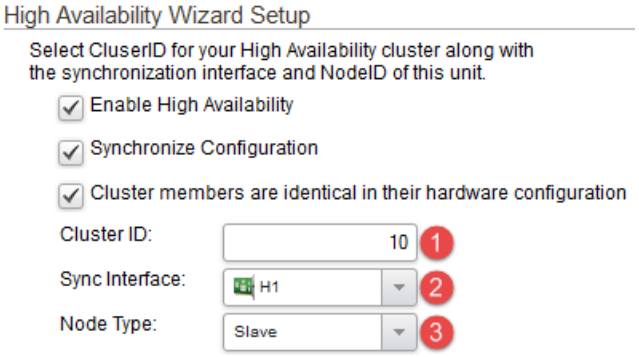


Abbildung 3.4.12 Die drei zu ändernden Slave-Einstellungen

Die Einstellungen wurden wie folgt geändert:

1. Wir müssen die Cluster-ID so einstellen, dass sie mit der der Master-Einheit identisch ist.

2. Die Synchronisierungsschnittstelle legen wir so fest, dass sie ebenfalls identisch mit der der Master-Einheit ist.

3. Dann ändern wir den Knotentyp von Master zu Slave.

Das bedeutet, wenn wir mit dem nächsten Schritt des HA-Assistenten fortfahren, wird der Slave versuchen, den Master zu kontaktieren und die HA-Konfiguration von ihm zu holen. Dazu ist es nötig, dass die Synchronisierungsschnittstelle und die Cluster-ID auf die gleiche Weise eingestellt sind, weil ansonsten die Master-Einheit alle Verbindungsversuche vom Slave ablehnen wird.

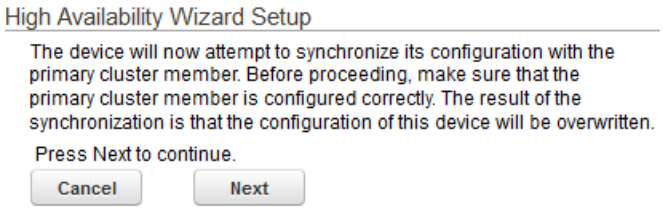


Abbildung 3.4.13 Der HA-Assistent für den Slave-Knoten

Der letzte Schritt ist, die Schnittstellen-Transformationen zu prüfen. Weil die Hardware identisch ist, wählen wir einfach die gleichen Schnittstellen-Transformationen wie beim Master.

Sobald die Konfiguration angewendet ist, ist der HA-Cluster bereitgestellt und läuft.

Prüfen, ob der Cluster funktioniert

Um zu prüfen, ob der Cluster wie erwartet funktioniert, können wir zwei Tests durchführen:

- Wenden Sie eine kleine Änderung der Konfiguration auf einen der Cluster-Knoten an und prüfen Sie dann, ob die Änderung beim anderen Cluster-Knoten ebenfalls ankommt.

- Öffnen Sie die Kommandozeile eines der Cluster-Knoten und starten Sie eines der folgenden Kommandozeile-Kommandos (abhängig davon, ob es der aktive oder inaktive Knoten ist).

  Beim aktiven Knoten:

  ```
  Gerät:/> HA –deactivate
  ```

  Oder beim inaktiven Knoten:

  ```
  Gerät:/> HA –activate
  ```

Wenn der Cluster so arbeitet, wie er soll, sollten beide Cluster-Knoten ihren Aktiv-/Inaktiv-Status umschalten. Der aktive Knoten sollte inaktiv werden und umgekehrt.

Hinweis

In dem seltenen Fall, dass beim Testen die Synchronisierung der Konfiguration nicht funktioniert, versuchen Sie, beide Cluster-Knoten neu zu starten. Dies sollte nur einmalig durchzuführen sein.

Ein alternativer Weg, den Slave hinzuzufügen

Ein anderer Weg, den Cluster-Slave einzustellen, ist, eine Sicherheitskopie der Master-Konfiguration zu nehmen und sie dann auf dem Slave wiederherzustellen, ohne sie zu aktivieren.

Bevor die Konfiguration aktiviert wird, ändern wir den Knotentyp von Master zu Slave, dann wenden wir die Konfiguration an, wie in der letzten Abbildung oben gezeigt.

Rezept 3.5. Webzugang durch Webinhalt-Filter beschränken

Ziele

Der Zweck dieses Rezepts ist es, Beschränkungen festzulegen, welche Art von Webkategorien durch die Clavister-Firewall erlaubt sind. Mit Kategorien meinen wir hier sowas wie Nachrichten, Spieleseiten, Firmenseiten, Inhalte für Erwachsene, Chaträume und so weiter. Wir wollen zum Beispiel den Studierenden unserer Universität nicht erlauben, Seiten mit FSK-18-Inhalten zu besuchen, wie in der nachfolgenden *Abbildung 3.5.1* dargestellt.

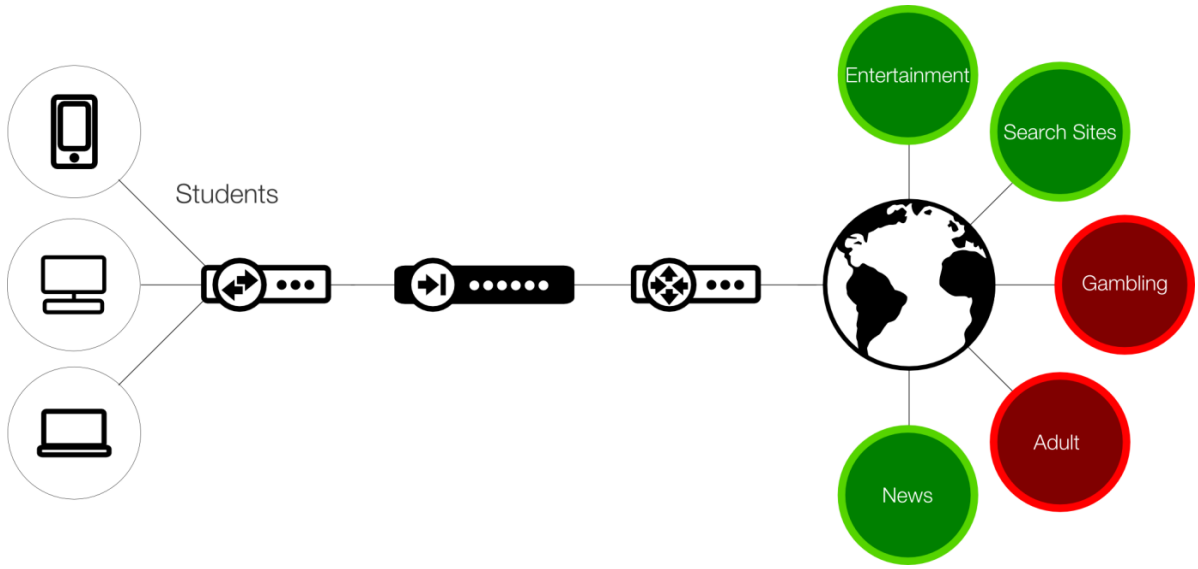


Abbildung 3.5.1 Webkategorien für Studierende blockieren

Hinweis

Obwohl sich der Hauptteil dieses Kapitels auf die Verwendung eines HA-Clusters bezieht, werden wir jetzt Netzwerk-Schemata verwenden, die den Cluster nicht zeigen, um die Darstellung zu vereinfachen (und um zu große Schemata zu vermeiden).

Detailbesprechung

Ein Anwendungslevel-Gateway (ALG, Application Layer Gateway) nutzen

Um Webinhalt-Filter einzubauen (WCF, Web Content Filtering), werden wir ein Konfigurationsobjekt namens „Application Layer Gateway“ (ALG, Anwendungslevel-Gateway) nutzen. Ein ALG fungiert als Mediator, wenn man übliche Internetanwendungen außerhalb des geschützten Netzwerks nutzt. Zum Beispiel für den Webzugang, für Dateiübertragungen und Multimedia-Übertragungen.

ALGs bieten höhere Sicherheit als normale Datenpaket-Filter, weil die ALGs in der Lage sind, sämtlichen Datenverkehr für ein bestimmtes Protokoll zu prüfen und Prüfungen auf höheren Ebenen des TCP/IP-Stacks durchzuführen.

Ein ALG konfigurieren

Um ein ALG zu erzeugen, gehen wir im WebUI zum Abschnitt „Objekte > ALG", wie im nachfolgenden Bildschirmfoto gezeigt.

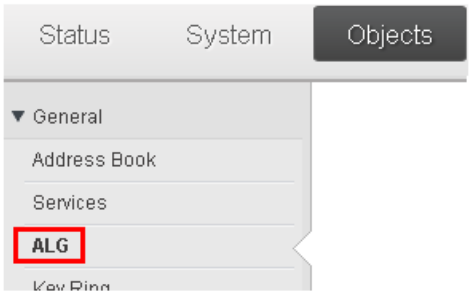


Abbildung 3.5.2 Position der ALG-Funktionen

Es gibt viele verschieden Arten von ALGs, aber in diesem Rezept werden wir ein HTTP-ALG erzeugen und verwenden. Wie dies ausgewählt wird, wird im nachfolgenden Bildschirmfoto dargestellt.

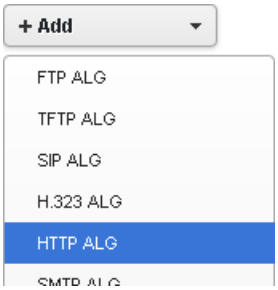


Abbildung 3.5.3 Ein neues ALG erzeugen

Wir werden keine der vorkonfigurierten ALGs benutzen, weil wir eines von Grund auf neu erzeugen wollen.

Sobald das ALG angelegt wurde, sehen wir eine Vielzahl von Einstellungen. Das HTTP-ALG ist das am häufigsten genutzte ALG und hat daher die meisten Eigenschaften und Funktionen. Wir werden sie alle durchgehen und kurz beschreiben, was jede Einstellung macht. Die Einstellungen sind im nachfolgenden Bildschirmfoto dargestellt.

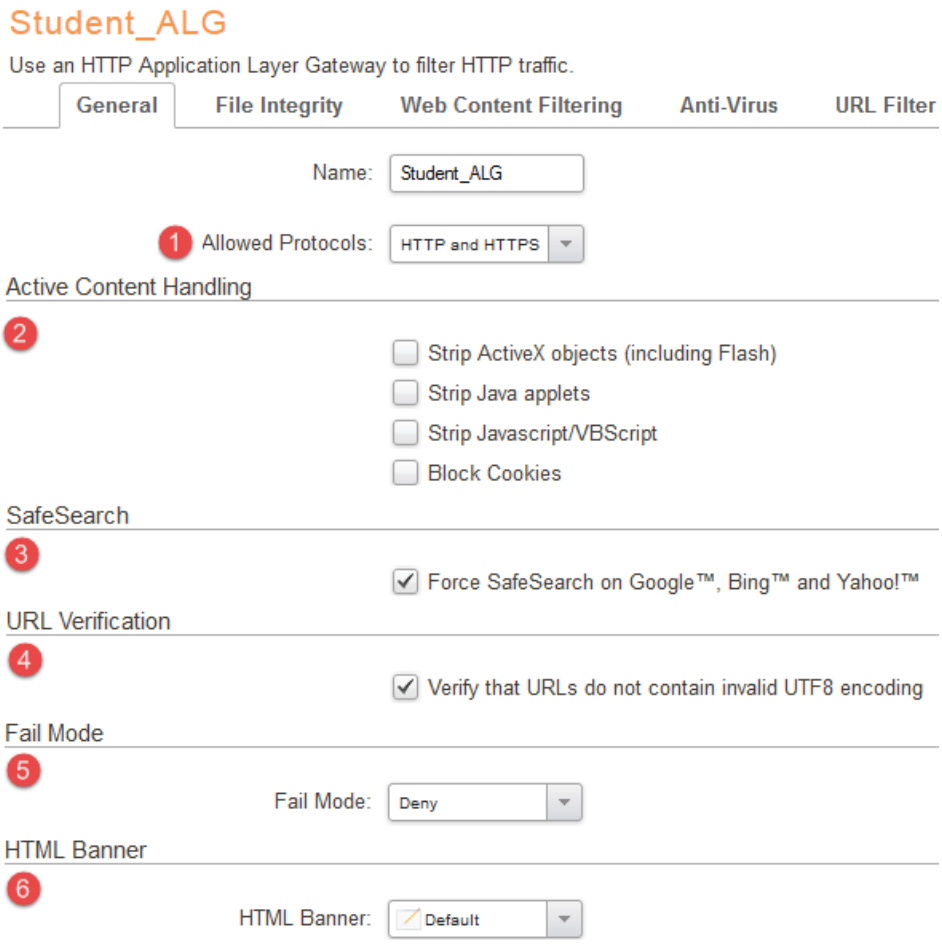


Abbildung 3.5.4 HTTP-ALG-Einstellungen

Allgemeine Einstellungen für das HTTP-ALG

Die oben gezeigten allgemeinen Einstellungen sind wie folgt:

1. Hier legen Sie fest, welche Art Protokolle Sie für dieses ALG zur Nutzung erlauben wollen. Wir haben die Wahl, HTTP, HTTPS oder „HTTPS und HTTPS“ zu nutzen. In diesem Fall wollen wir, dass unser Webinhalt-Filter sowohl HTTP als auch HTTPS nutzt.

Bitte beachten Sie, dass HTTPS Einschränkungen mit sich bringt. Weil HTTPs-Daten verschlüsselt sind, kann das ALG bei HTTPS-Verbindungen nur WCF und URL-Filter verwenden.

2. Wir können bestimmte Komponenten aus HTTP-Daten herausfiltern. Weil der Internet-Datenverkehr heutzutage alle diese Komponenten intensiv benutzt, werden diese Optionen heute kaum noch aktiviert. In unserem Szenario werden wir sie ebenfalls nicht aktivieren.

3. Dann können wir die Option „SafeSearch" einschalten, um zu erzwingen, dass alle Websuchen, die Clients mit den Suchmaschinen von Google™, Microsoft Bing™ oder Yahoo™ durchführen, die SafeSearch-Funktion im Streng-Modus benutzen. SafeSearch funktioniert als automatischer Filter für FSK-18- und möglicherweise beleidigende Inhalte, so dass wir diese Einstellung einschalten.

4. Hier wird festgelegt, dass die verwendeten URLS mithilfe des UTF-8-Standards korrekt formatiert sind. Diese Einstellung aktivieren wir auch.

5. Damit wird bestimmt, wie wir damit umgehen wollen, wenn wir nicht feststellen können, welcher Art eine Datei ist. Ist eine Datei zum Beispiel ein ZIP-Archiv? Eine ausführbare EXE-Datei? Wenn wir nicht in der Lage sind, festzustellen, worum es sich handelt, können wir wählen, wie damit umgegangen werden soll. In unserem Fall blockieren wir alle solchen Dateien.

6. Dies kontrolliert, ob wir irgendwelche selbstgemachten Blockade-Seiten nutzen wollen. Eine Blockade-Seite ist eine Sammlung verschiedener HTML-Dateien für verschiedene Situationen, die auftreten können, wenn/falls WCF Probleme feststellt/blockiert/ablehnt und dem Nutzer eine bestimmte Seite gezeigt werden soll.

   Einige Nutzer wollen ihre eigenen Fehler-/Blockade-Seiten erzeugen, was durch das Anlegen selbstgemachter Blockade-Dateien und ihre Verwendung am ALG möglich ist. Wir werden die standardmäßigen Blockade-Dateien in unserem Setup verwenden.

Datei-Integrität, Webinhalt-Filter, Virenschutz und URL-Filter

Andere Tabs in der ALG-Einstellungsseite sind Datei-Integrität, Webinhalt-Filter (WCF), Virenschutz und URL-Filter. Diese werden im nachfolgenden Bildschirmfoto dargestellt.

Abbildung 3.5.5 HTTP-ALG-Einstellungen-Tab

Weil wir uns auf Webinhalt-Filter konzentrieren wollen, werden wir nur kurz anreißen, wofür die anderen Tabs sind.

- **Datei-Integrität**

  Dieser Tab enthält Einstellungen, die einige Aspekte für Dateien kontrollieren, die durch das ALG hindurch heruntergeladen wurden. Zum Beispiel können wir die maximale Dateigröße festlegen, bestimmte Datei-Suffixe (wie z.B. .zip, .exe usw.) erlauben oder verbieten und den MIME-Typ der Datei prüfen lassen. MIME-Prüfung bedeutet, dass wir zu prüfen versuchen, ob eine .zip-Datei tatsächlich ein ZIP-Archiv und nicht irgendwas anderes mit dem Suffix .zip ist.

- **Webinhalt-Filter (WCF)**

  Darum geht es in diesem Rezept und daher werden wir diesen Tab in Kürze in diesem Abschnitt detailliert beschreiben.

- **Virenschutz**

  Dieser Tab enthält Einstellungen, die sich auf Virenschutz beziehen, wie das Ein-/Ausschalten des Virenschutzes, welche Dateiarten vom Scan ausgeschlossen werden sollen, maximale Kompressionsrate für Archivdateien und wie vorgegangen werden soll, wenn wir eine Datei entdecken, die nicht gescannt werden kann, weil sie verschlüsselt ist.

- **URL-Filter**

  Dieser Tab enthält Optionen, um bestimmte URLs auf eine Whitelist oder Blacklist zu setzen. Es kann sehr nützlich sein, Webinhalt-Filter für bestimmte Seiten aus dem einen oder anderen Grund zu überschreiben. Das nächste Bildschirmfoto zeigt ein Beispiel, wie zwei URL-Filter eingestellt werden können.

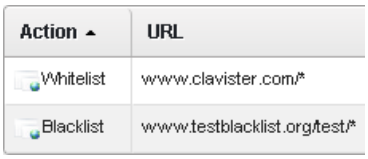


Abbildung 3.5.6 URL-Filter benutzen

Manchmal kann es erwünscht sein, eine Seite zu erlauben, obwohl sie zu einer blockierten Kategorie gehört. Wir können die Whitelist des URL-Filters nutzen, um die Blockade zu überschreiben. Das gleiche trifft zu, wenn Sie irgendetwas Bestimmtes überschreiben wollen, das auf der Blacklist landen sollte, nicht aber die gesamte entsprechende Website.

Erklärung der Webinhalt-Filter-Einstellungen

Jetzt haben wir den Webinhalt-Filter-Tab erreicht, der im nachfolgenden Bildschirmfoto gezeigt wird.

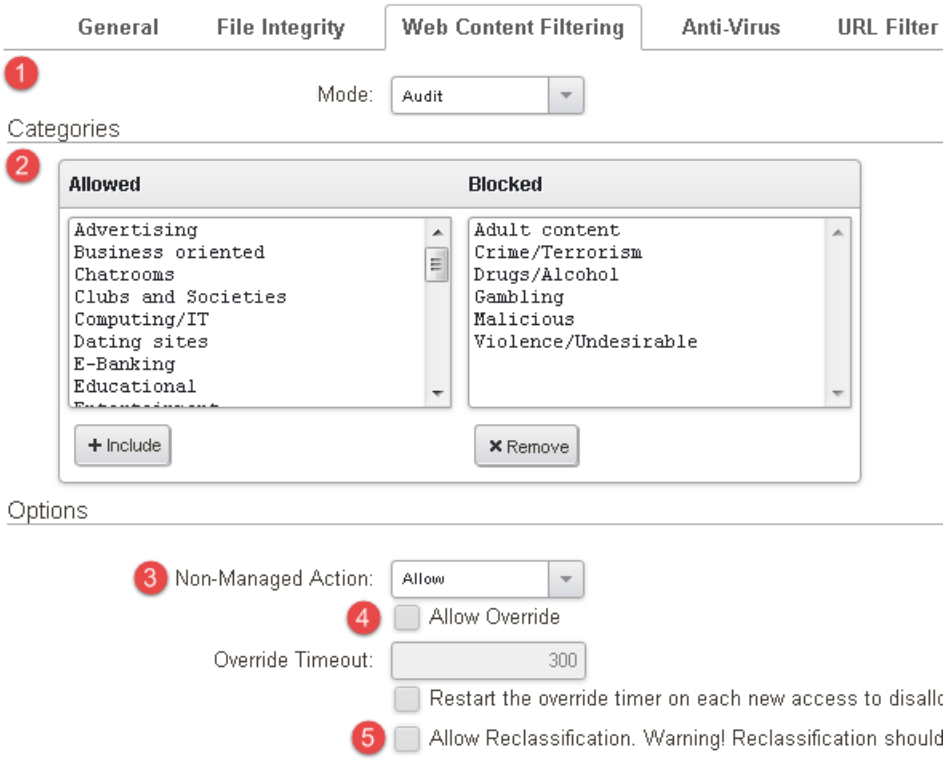


Abbildung 3.5.7 Der Webinhalt-Filter-Tab

Hier stellen wir ein, wie wir den Webinhalt-Filter verwenden wollen, welche Kategorien wir erlauben und verbieten wollen, und noch mehr.

Die Einstellungen sind folgende:

1. Diese Einstellung kontrolliert, in welchem Modus Sie Webinhalt-Filter einsetzen wollen. Die Optionen sind Deaktiviert, Audit und Aktiviert. Weil wir in unserer Installation Webinhalt-Filter noch nicht aktiviert haben, setzen wir ihn in den Audit-Modus. Der Grund dafür ist, dass das Datenverkehr-Muster jeder Installation einzigartig ist. Indem wir den Webinhalt-Filter zuerst in den Audit-Modus setzen, kann der Administrator sehen, welche Nutzer für welche Art der Nutzung blockiert würden, wenn wir von Audit auf Verweigern umschalten. Wie lange man im Audit-Modus bleibt, ist Sache des Administrators, aber ein oder zwei Tage sind meistens ausreichend.

2. Dies legt fest, welche Kategorien wir erlauben sollten und welche Kategorien blockiert werden sollten.

3. Dies ist eine wichtige Einstellung, die kontrolliert, wie der cOS-Core mit Situationen umgehen soll, wenn eine Webseite keine Klassifizierung hat. Soll sie erlaubt oder verweigert werden? Im Problemfall gibt es immer die Option, Webseiten auf die Whitelist zu nehmen, wenn der Administrator nicht möchte, dass der Webinhalt-Filter den Zugang zu ihnen verhindert.

4. Dies bestimmt, ob wir Nutzern gestatten sollten, Einschränkungen zu überschreiben, wenn sie eine blockierte Kategorie aufrufen. Das bedeutet, dass der Nutzer die Möglichkeit erhält, die eingeschränkte Webseite zu öffnen, statt grundsätzlich blockiert zu werden, aber der Verbindungsversuch wird protokolliert. Wir empfehlen, diese Option nicht zu aktivieren, außer für Testzwecke.

5. Hier legen Sie fest, ob Sie eine Änderung der Seiten-Klassifizierung gestatten wollen. Das bedeutet, wenn eine Seite die Klassifikation „Nachrichten“ hat, können Sie sie als etwas anderes klassifizieren, z.B. als „Suchmaschinen-Website“. Dies sollte nur selten erlaubt werden, weil es vorrangig zwei Dinge macht:

    - Der URL-Cache für diese Seiten-Klassifizierung im cOS-Core wird vorübergehend überschrieben, um die gewählte Klassifizierung zu nutzen.
    - Es wird eine Benachrichtigung an die Webinhalt-Filter-Datenbanken gesendet, dass diese Seite eventuell neu klassifiziert werden muss.

    Nur dem Administrator sollte erlaubt sein, Seiten neu zu klassifizieren.

Hinweis

Aufmerksame Leser mögen anmerken, dass Werbung nicht zu den blockierten Kategorien gehört. Der Grund dafür ist, dass viele Webseiten auf Werbung angewiesen sind und dass viele Webseiten so eingestellt sind, dass sie die gewünschten Inhalte erst zeigen, wenn die geschaltete Werbung geladen wurde, was nicht geht, wenn wir die Werbung blockieren. Es bleibt dem Administrator überlassen, zu entscheiden, was erlaubt und was blockiert werden soll. Die Protokolle enthalten Informationen darüber, was erlaubt und blockiert ist, so dass diesbezügliche Probleme rasch untersucht werden können.

Für Fortgeschrittene: Details über die Webinhalt-Filter-Funktionsweise

Um weiter zu erklären, wie Webinhalt-Filtern funktioniert, werden wir das in der nachfolgenden *Abbildung 3.5.8* gezeigte Diagramm verwenden.

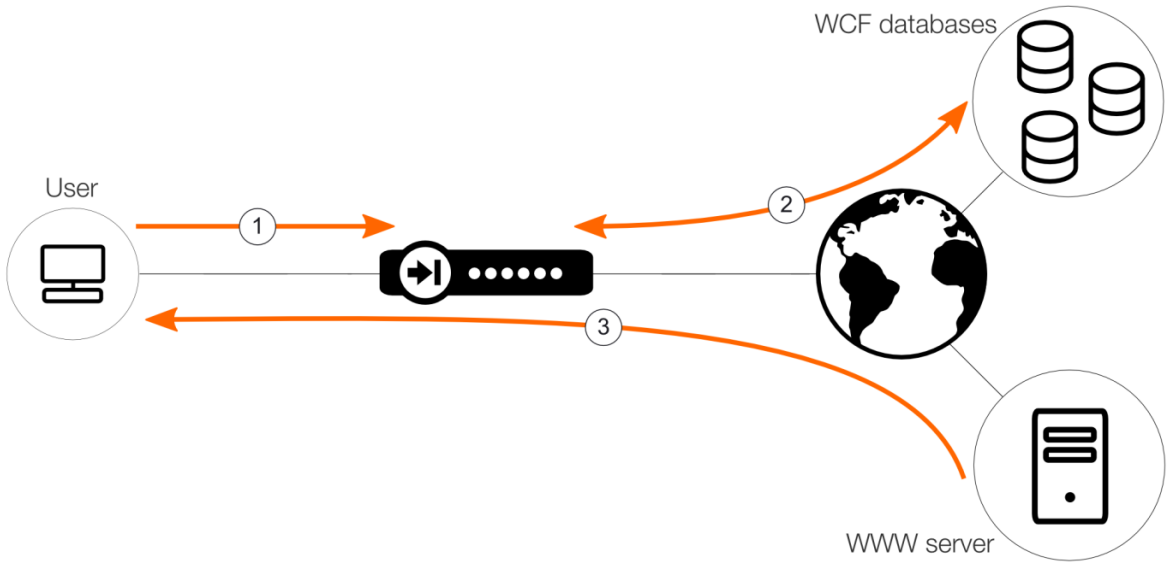


Abbildung 3.5.8 Webinhalt-Filter-Funktionsweise

Der Ablauf des Filterns ist wie folgt:

- Wenn ein Nutzer (**1**) Zugang zu einer Website anfragt, befragt der cOS-Core die dynamischen Webinhaltfilter-Datenbanken (**2**), um die Kategorie-Klassifizierung der

entsprechenden Website zu ermitteln.

- Auf der Basis der momentan eingestellten Filterregeln kann dann Zugang zu dem URL erlaubt oder verweigert werden.
- Wenn der Zugang erlaubt ist, wird die Kommunikation zwischen dem Nutzer und dem Ziel-Webserver hergestellt (**3**).
- Wenn der Zugang verweigert wird, wird dem Nutzer eine Webseite gezeigt, die erklärt, dass die angefragte Website blockiert ist.

Unterschiedliches Verhalten beim Verweigern von HTTPS-Webseiten

Wenn HTTPS genutzt wird, ist es nicht möglich, dem Nutzer eine Webseite zu zeigen, die ihm mitteilt, dass die Website nicht erreichbar ist, während er versucht, eine Website mit eingeschränkter Kategorie-Klassifizierung zu erreichen.

Das liegt daran, dass der Datenverkehr verschlüsselt ist. cOS-Core kann hier nur den Datenstrom unterbrechen und die aktive Verbindung schließen.

Das hat den Effekt, dass der Nutzer entweder irgendeine Fehlerseite zu sehen bekommt oder dass der Seitenaufbau stoppt. Ein Beispiel einer solchen Nachricht wird nachfolgend gezeigt.

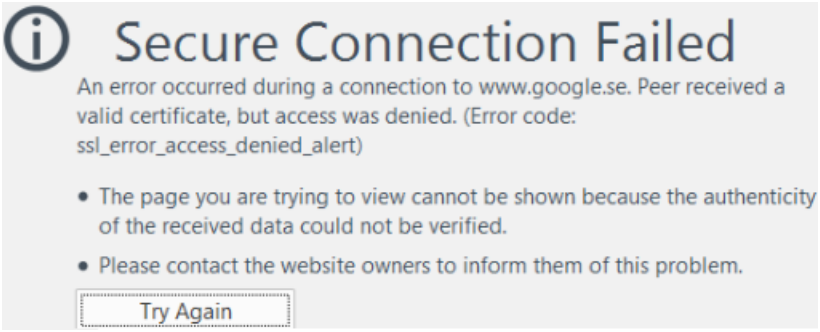


Abbildung 3.5.9 Typische HTTPS-Browser-Fehlermeldung nach Ladefehler

Das bedeutet, dass Nutzer den Administrator kontaktieren können, um sich zu beschweren, dass eine Seite nicht funktioniert, die in Wirklichkeit zu einer blockierten Kategorie gehört.

Webinhalt-Filter-Konfiguration fortsetzen

Nachdem wir in den vorigen Schritten unser ALG fertig konfiguriert haben, müssen wir es jetzt einem Dienst-Objekt zuweisen. Dazu gehen wir im WebUI zu **Objekte > Dienste** und erzeugen ein neues TCP/UDP-Dienst-Objekt, wie im nachfolgenden Bildschirmfoto gezeigt.

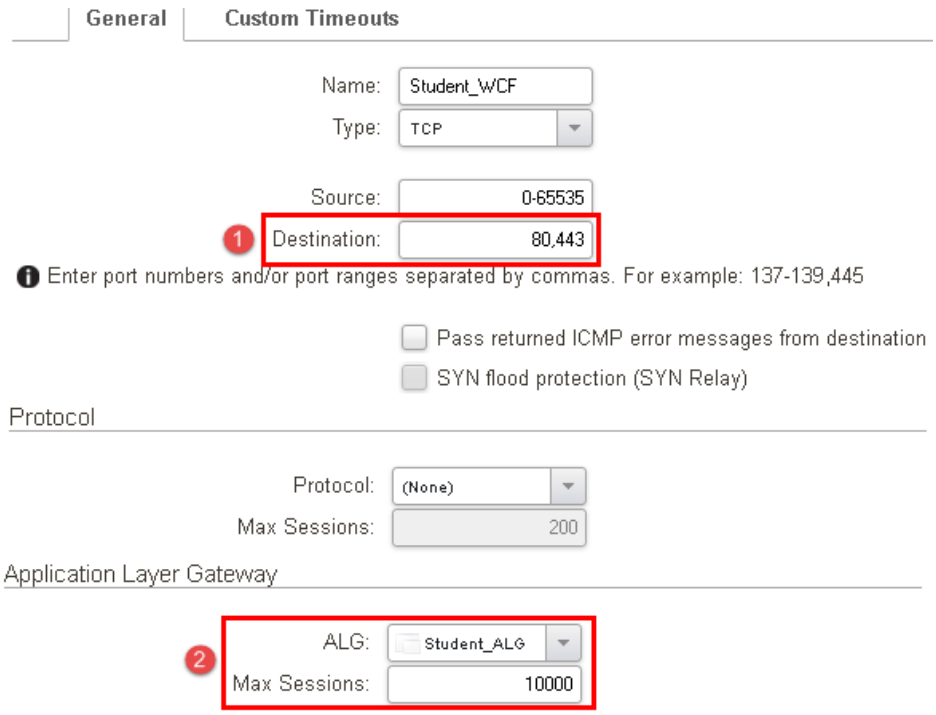


Abbildung 3.5.10 Ein ALG mit einem Dienst-Objekt nutzen

Weil unser ALG auf HTTP und HTTPS verwendet wird, wählen wir in der Zielport-Definition Port 80 und 443, durch ein Komma getrennt (**1**).

Als Nächstes wählen wir im Application-Layer-Gateway-Menü unser zuvor erzeugtes ALG aus (**2**). Zuletzt haben wir noch die Option für „Sitzungen maximal".

Weil dies eine Universität ist, können wir davon ausgehen, dass unsere Nutzer eine Vielzahl Sitzungen nutzen werden. Den passenden Wert für „Sitzungen maximal" kann kniffelig sein, aber **eine gute Faustregel ist, pro Nutzer 20 Sitzungen anzunehmen**. Falls wir also 5.000 Nutzer haben, sollte die Anzahl Sitzungen in diesem Dienst auf 100.000 gesetzt werden.

Jetzt haben wir sowohl das ALG als auch den Dienst eingerichtet. Der letzte Schritt ist, unseren neu erzeugten Dienst mit einer IP-Regel zu nutzen. Im Moment sind unsere IP-Regeln, wie im nachfolgenden Bildschirmfoto gezeigt.

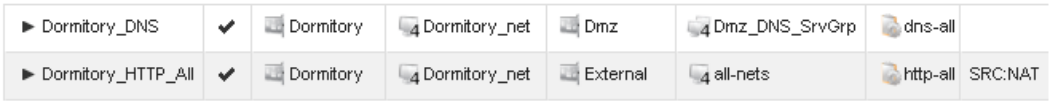


Abbildung 3.5.11 Eingestellte IP-Regeln für das Wohnheim

Wir haben bereits eine Regel, die HTTP und HTTPS erlaubt, so dass wir einfach diese Regel abändern, damit sie unseren neu erzeugten Dienst nutzt. Die fertige Regel hat ALG aktiviert und wird nachfolgend gezeigt.

Abbildung 3.5.12 HTTP/HTTPS-IP-Regel nutzt das Webinhalt-Filter-ALG

Über die Webinhalt-Filter-Datenbanken

Das dynamische Webinhalt-Filtern des cOS-Cores ermöglicht es, das Blockieren von Webseiten zu automatisieren, so dass es nicht nötig ist, im Voraus von Hand festzulegen, welche URLs blockiert oder erlaubt werden sollen.

Stattdessen hat der cOS-Core Zugriff auf externe Datenbanken, die Unmengen von Website-URL-Adressen enthalten, die bereits in Kategorien wie z.B. Einkaufen, Nachrichten, Sport, FSK 18 und so weiter klassifiziert sind.

Diese externen Datenbanken werden ständig mit kategorisierten URLs aktualisiert, während gleichzeitig ungültig gewordene URLs wieder entfernt werden. Der Umfang der URLS in den Datenbanken ist global und deckt Websites in vielen verschiedenen Sprachen auf Servern in vielen verschiedenen Ländern ab.

Webinhalt-Filtern merkt sich URLs

Um das Suchen für den Webinhalt-Filter so schnell wie möglich zu machen, hält der cOS-Core die zuletzt besuchten URLS in einem lokalen Cache im Speicher bereit. Das Caching kann höchst effizient sein, weil eine festgelegte Benutzergruppe wie die Studierenden einer Universität oftmals eine Gruppe ähnlicher Websites aufsuchen.

Rezept 3.6. Unterschiedliche Webzugang-Rechte anhand der Schnittstelle gewähren

Ziele

Der Zweck dieses Rezepts ist, zu beschreiben, wie wir verschiedenen Nutzern unterschiedliche Webzugang-Rechte geben können, abhängig davon, hinter welcher Schnittstelle der Nutzer sich befindet.

Wir werden mehrere Anwendungsebene-Gateways (ALGs) erzeugen, die alle unterschiedlich eingestellt werden und mithilfe von Webinhalt-Filtern Zugang oder Beschränkungen für bestimmte Kategorien geben.

Detailbesprechung

Zusätzliche ALGs erzeugen

Nach dem Einbau von Webinhalt-Filtern wie in *Rezept 3.5 beschrieben. Wenn wir Webzugang mit Webinhalt-Filtern beschränken*, gibt es Einschränkungen in einigen der unerwünschten Webkategorien für unsere Studierenden. Wir wollen jetzt ebenso einige Einschränkungen für unsere Dozenten und WLAN-Nutzer einbauen.

Dabei wollen wir zusätzliche Einschränkungen einrichten, indem wir mehr blockierte Kategorien hinzufügen. Wir blockieren zum Beispiel entfernte Desktops, Chaträume und so weiter.

Letztendlich liegt es beim Administrator und der Universität, eine Richtlinie festzulegen, was erlaubt werden soll und was nicht.

Wenn wir unsere vorrangigen Universität-Beispielgruppen ansehen, die da sind: Studierende/Wohnheim, Dozenten und WLAN, wäre es umsichtig, ihnen Zugang zu verschiedenen Kategorien zu gewähren.

Ein Dozent zum Beispiel sollte weniger Einschränkungen als ein Studierender haben, weil es Aufgaben, Projekte und andere Sachen geben könnte, die es erfordern, dass der Dozent zusätzlichen Zugang zu diesen Ressourcen hat, ohne dass er jedes Mal zum Netzwerk-Administrator laufen muss. Wir werden speziellen Zugang durch Überschreiben weiter unten besprechen.

Die nachfolgende Tabelle 3.6.1 zeigt ein Beispiel, wie wir verschiedene Kategorien für verschiedene Schnittstelle und Gruppen einstellen können.

Schnittstelle	Optionen	Blockierte Kategorie
DOZENTEN	Überschreiben	Erwachsene Blockierliste der Regierung Schädlich Gewalt/Unerwünschtes
STUDIERENDE/WOHNHEIM	SafeSearch	Erwachsene Kriminelles/Terrorismus Drogen/Alkohol Spiele Blockierliste der Regierung Schädlich Fernzugriff/Entfernte Desktops Badekleidung/Dessous Gewalt/Unerwünschtes
WLAN	SafeSearch	Erwachsene Chaträume Kriminelles/Terrorismus Drogen/Alkohol Spiele Blockierliste der Regierung Schädlich Musik-Download Fernzugriff/Entfernte Desktops Badekleidung/Dessous Gewalt/Unerwünschtes

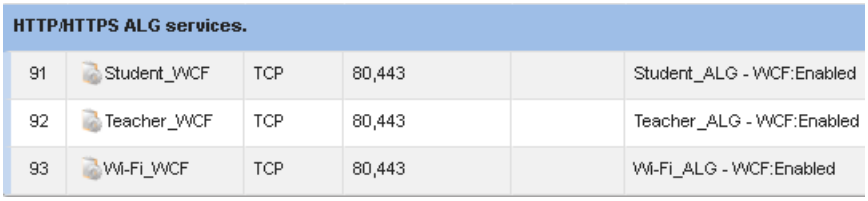
Tabelle 3.6.1 Blockierte Kategorien für verschiedene Gruppen

Um unseren angepassten Zugang zu erstellen, müssen wir weitere ALGs anlegen, um sie in unserem IP-Regelsatz zu verwenden.

Rufen Sie sich die drei Schritte ins Gedächtnis, um ein ALG zu erzeugen und in unserem IP-Regelsatz zu nutzen:

1. Erzeugen Sie ein ALG-Objekt.
2. Weisen Sie das ALG-Objekt einem Dienst-Objekt zu.
3. Weisen Sie das Dienst-Objekt einer IP-Regel zu.

Nachdem wir alle unsere angepassten ALGs erzeugt haben, weisen wir jedes dieser ALGs seinen eigenen Diensten zu, wie im nächsten Bildschirmfoto gezeigt.



HTTP/HTTPS ALG services.					
91	Student_WCF	TCP	80,443		Student_ALG - WCF:Enabled
92	Teacher_WCF	TCP	80,443		Teacher_ALG - WCF:Enabled
93	Wi-Fi_WCF	TCP	80,443		Wi-Fi_ALG - WCF:Enabled

Abbildung 3.6.2 Dienste-Zusammenfassung für die Schnittstellen-Gruppen

DMZ- und ADMIN-Zugangsrechte

Einigen Leserinnen und Lesern mag auffallen, dass wir noch keinerlei ALG-Regeln für die DMZ, Administratoren oder das Labor hinzugefügt haben.

Die DMZ enthält die Server für eingehende Verbindungen zur Universitäts-Website, Domänen-Controller, Speichergeräte, Sicherheitskopie-Systeme, Mailserver und so weiter. Sie werden hauptsächlich vom Administrator kontrolliert, mit sehr begrenzten externen Zugangsmöglichkeiten. Es gibt kaum einen Bedarf für das ALG hinter dieser Schnittstelle, aber letztendlich liegt es beim Administrator, zu entscheiden, welche Dienste er nutzt und welche Art von Zugangslevel erlaubt sein sollte.

Momentan haben die Administratoren unbeschränkten Zugang zum Internet ohne irgendwelche Einschränkungen, weder für Kategorien noch für Ports oder Protokolle. Aber sind Administratoren unfehlbar? Selbst wenn sie das Netzwerk verwalten, gibt es keinen direkten Grund, sie NICHT ebenfalls einzuschränken. Wenn für die Administratoren der Bedarf entsteht, zusätzliche Ports/Protokolle zu nutzen, können sie leicht den IP-Regelsatz des cOS-Cores anpassen, um diesem Bedarf nachzukommen.

Das ist ein Grund, warum Hacker auf Administrator-Konten abzielen, weil diese umfassende Netzwerk-Zugangsprivilegien haben.

Momentan haben wir den externen Zugang für unsere Universität-Administratoren so geändert, dass er nur DNS und HTTP/HTTPS ohne ein ALG nutzen kann. Sie haben immer noch vollständigen Zugang zu allen internen Ressourcen, Netzwerken und Schnittstellen.

Individuelle ALG- und Dienst-Objekte mit IP-Regeln nutzen

Jetzt müssen wir nur noch unsere neu erzeugten Dienst-Objekte in unseren IP-Regeln nutzen. Wie das gemacht wird, wird in den nachfolgenden beiden Regeln gezeigt.

Abbildung 3.6.3 ALG-Dienst-Objekte nutzen

Wir müssen für jede Schnittstellen- und Netzwerk-Kombination IP-Regeln erzeugen und dann das richtige Dienst-Objekt nutzen, um jeder Schnittstelle und jedem Netzwerk den richtigen Webinhalt-Filter-Zugangslevel zu geben. Das „Studierende_WCF"-Dienst-Objekt zum Beispiel muss in den Netzwerken verwendet werden, mit denen unsere Studierenden verbunden sind, was im obigen Beispiel Wohnheim und Wohnheim_net sind.

Wenn dies für alle betroffenen Schnittstellen und Netzwerke erledigt ist, haben wir effektiv verschiedene Zugangsrechte für Studierende, Dozenten und WLAN-Nutzer festgelegt, abhängig davon, mit welchem Netzwerk sie verbunden sind.

Wir werden unserem Universität-Netzwerk noch mehr Sicherheit und Funktionalität hinzufügen, was wir in anderen Rezepten im weiteren Verlauf des Buches besprechen werden. Das Labor-Netzwerk ist allerdings ein anderer Fall, und wir werden uns das Labor-Netzwerk später im Detail ansehen.

Rezept 3.7. Virenschutz einstellen

Ziele

Der Zweck dieses Rezepts ist es, die Sicherheit des Universität-Netzwerks weiter zu verstärken. In diesem Rezept werden wir besprechen, wie mithilfe der zuvor erzeugten ALGs Virenschutz-Scanner aktivieren.

Die Virenschutz-Funktionalität im cOS-Core schützt vor beliebigem Schadcode, der in Dateien enthalten ist, die durch eine Clavister-Firewall der nächsten Generation zu Clients heruntergeladen werden. Das Folgende kann nach Viren gescannt werden:

- Alle Dateien, die durch die Clavister-Firewall heruntergeladen werden. Beispielsweise Dateien, die durch HTTP- oder FTP-Übertragung oder als E-Mail-Anhang via SMTP heruntergeladen wurden.
- Skripte in Webseiten, die via HTTP geliefert werden.
- URLS in Webseiten, die via HTTP geliefert werden.

Die Virenschutz-Scanner-Funktionalität kann für Datei-Downloads aktiviert werden, die mit den folgenden ALGS verbunden sind:

- HTTP-ALG
- FTP-ALG
- POP3-ALG
- SMTP-ALG

Hinweis

Wir werden hier nur die Virenschutz-Anwendung mit der HTTP-ALG vertiefen. Virenschutz kann ebenfalls in den SMTP-, POP3- oder FTP-ALGs aktiviert werden, aber das werden wir nicht weiter behandeln. Die allgemeinen Optionen und die Funktionalität sind für alle ALGs ähnlich, die Virenschutz unterstützen.

Detailbesprechung

Virenschutz-Scanner in einem ALG aktivieren

Um Virenschutz in einem ALG zu aktivieren, rufen wir eines unserer zuvor erzeugten HTTP-ALG-Objekte auf. In diesem Fall wählen wir das für die Studierenden verwendete ALG, das im nachfolgenden WebUI-Bildschirmfoto gezeigt wird.

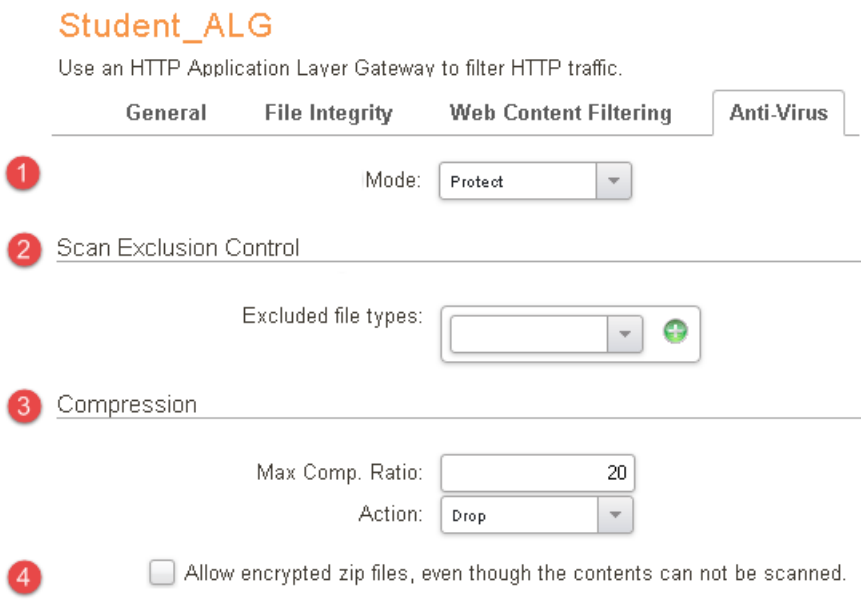


Abbildung 3.7.1 Virenschutz-Optionen im HTTP-ALG

Wenn wir den Virenschutz aktivieren, haben wir zunächst die Wahl, festzulegen, in welchem Modus (**1**) er ausgeführt werden soll. Wir haben drei Optionen: Deaktiviert, Audit und Schützen. **Audit** bedeutet, dass der Virenschutz den Datenverkehr nur scannt. Wenn er einen Virus oder eine andere Bedrohung entdeckt, wird er ein Protokollereignis erzeugen, aber nicht in den Datenverkehr eingreifen. Das kann sehr nützlich sein, wenn wir nur den Status eines Netzwerks prüfen wollen, ohne aktiv irgendwelche Handlungen aufgrund fehlerhaften Verhaltens auszuführen.

Im **Schützen**-Modus verhindern wir aktiv, dass eine Datei heruntergeladen wird. Der Virenschutz-Core ist datenstrombasiert, was bedeutet, dass wir die Datei kontinuierlich scannen, während sie heruntergeladen wird, und wenn ein Virus oder anderer schädlicher Inhalt entdeckt wird, fügt er eine Nachricht in den Datenstrom ein und verwirft die Verbindung.

Scan-Ausschlusskontrolle (**2**) bedeutet die Fähigkeit zu wählen, ob eine bestimmte Dateiart vom Virenschutz-Scan ausgeschlossen werden soll. Dateien vom Scannen auszuschließen, sollte mit Bedacht gemacht werden.

Wenn komprimierte Dateien gescannt werden (**3**), muss der cOS-Core sie dekomprimieren (entpacken), um den Dateiinhalt zu prüfen. Einige Dateiarten können sehr hohe Kompressionsraten haben, so dass die komprimierte Datei nur einen Bruchteil der ursprünglichen, unkomprimierten Dateigröße hat.

Das heißt, dass ein vergleichsweise kleiner komprimierter Dateianhang in eine viel größere Datei entpackt werden muss, was die cOS-Core-Ressourcen stark belasten und den Durchsatz merklich verlangsamen kann.

Um diese Situation zu vermeiden, sollte der Administrator ein **Kompressionsrate-Limit** festlegen. Wenn das Limit dieser Rate z.B. auf 10 gesetzt ist, heißt das, wenn die unkomprimierte Datei 10-mal größer als die komprimierte Datei ist, soll die gewählte **Aktion** ausgeführt werden. Die **Aktion** kann eine der folgenden sein:

- **Erlauben** - Die Datei wird ohne Virenscan durchgeleitet.
- **Normal** - Die Datei wird ganz normal nach Viren durchsucht.
- **Verwerfen** - Die Datei wird verworfen.

Die letzte Option (**4**) legt fest, was zu tun ist, wenn wir Dateien haben, die passwortgeschützt oder verschlüsselt sind. Das Standardverhalten ist, dass wir solche Dateien nicht zulassen sollten, weil wir sie nicht scannen können. Es ist jedoch nicht so ungewöhnlich, z.B. ZIP-Archive mit einem Passwort zu schützen. Daher liegt es beim Administrator, festzulegen, ob er solchen Dateien gestatten oder verweigern sollte, durch die Firewall zu kommen.

Im Szenario unseres Universität-Beispiels werden wir erlauben, dass passwortgeschützte Dateien ins Dozenten-Netzwerk gesendet, aber für jedes andere Netzwerk verweigert werden.

Wichtig: Eine Datei kann als heruntergeladen erscheinen, selbst wenn ein Virus gefunden wurde

Wenn wir über Virenschutz reden, ist ein wichtiger Aspekt, den Sie sich merken sollten, dass wir selbst dann, wenn wir einen Datei-Download des Nutzers abbrechen können, nicht immer den Nutzer auf eine Seite umleiten können, die ihm „Virus gefunden" mitteilt. Was wir jedoch tun können, ist, die Datei absichtlich zu beschädigen, indem wir den Download abbrechen und die Nachricht „Virus gefunden" am Ende der Datei einfügen, sobald ein Virus entdeckt wurde.

Falls sich daher ein Nutzer beschwert, dass eine heruntergeladene Datei nicht funktioniert, kann es sein, dass in dieser besonderen Datei ein Virus gefunden wurde. Prüfen Sie dann entweder die vom cOS-Core generierten Virenschutz-Protokolle oder versuchen Sie, die beschädigte Datei in einem Hex-Editor oder einem ähnlichen Programm zu öffnen, und schauen Sie sich das Ende der Datei an, um zu sehen, ob es den Hinweis „Virus gefunden" enthält.

Schließen Sie daher nicht einfach diese Dateiart aus, weil ein Nutzer ein Problem mit einer Datei hat; es kann sein, dass mit dieser Datei absichtlich etwas angestellt wurde.

Nachfolgend sehen Sie anhand eines Beispiels, was vom cOS-Core z.B. in eine HTML-Datei eingefügt werden könnte:

```
<html>
 <head>
 <title>Virus gefunden</title>
 </head>
 <body>
 <h1>Es wurde ein Virus entdeckt</h1>
 <b>Der Rest dieser Datei wird blockiert</b>
 Infizierte Datei: eicar_com.zip<
```

Falls der Virus auf einer Webseite entdeckt wurde, würde der Nutzer eine einfache Seite mit der obigen Nachricht sehen. Falls jedoch eine Datei heruntergeladen wurde, ist das nicht möglich, so dass stattdessen die Datei absichtlich vom cOS-Core beschädigt wird.

Der Virenschutz des cOS-Cores sollte nicht andere Virenschutz-Programme ersetzen

Es ist sehr wichtig, sich bewusst zu machen, dass der Virenschutz-Scanner des cOS-Cores niemals Virenschutz-Programme, die lokal auf einem Client-PC installiert ist, vollständig ersetzen sollte. Der cOS-Core führt keine so detaillierten Dateiscans und -Prüfungen aus, wie sie lokal installierte Virenschutz-Programme leisten können, weil der cOS-Core nur die Netzwerk-Kommunikation prüfen kann.

Der Virenschutz-Scanner des cOS-Cores sollte die erste Verteidigungslinie, aber nicht die letzte sein.

Ein Hinweis zu Virenschutz-Scans und HTTPS

Bei HTTPS ist der Datenverkehr verschlüsselt, so dass das HTTP-ALG nur zwei Aktionen bei HTTPS-Datenverkehr ausführen kann:

- URL-Filter
- Webinhalt-Filter.

Das sollte bedacht werden, wenn der Dienst, der mit dem ALG genutzt wird, HTTPS einschließt.

Virenschutz-Richtlinie für die Universität

In *Rezept 3.5. Webzugang durch Webinhalt-Filter beschränken* und *Rezept 3.6. Wo wir gerade wir auf der Basis der Schnittstellen verschiedene Web-Zugangsberechtigungen gewährt haben*, haben wir auch erwähnt, dass wir das ALG nicht für Administratoren und die DMZ aktiviert haben, damit sie so wenig Einschränkungen wie möglich beim Zugang haben.

Gibt es jedoch überhaupt keinen guten Grund, zumindest auch Virenschutz für die Admins und DMZ-Server zu aktivieren? Durch das Erzeugen mehrerer ALGs und Dienste sind wir in der Lage, eigene Zugangslevel zu nutzen, so dass wir damit fortfahren sollten, all unseren aktivierten Schnittstellen zusätzliche Zugangslevel hinzuzufügen, einschließlich ADMIN und DMZ.

Für die Administratoren erzeugen wir ein ALG, das weitestgehend unbeschränkt ist. Wir verwenden weder SafeSearch noch prüfen wir das URL-Encoding und wir schalten Webinhalt-Filter aus. Als einzige Eigenschaft aktivieren wir Virenschutz. Wir erlauben also das Weiterleiten verschlüsselter Dateien durch das ALG. Die wichtigste Funktion, die wir hier nutzen wollen, ist Virenschutz.

Weil wir hier über Administratoren sprechen - es wird immer Situationen geben, wo diese Funktion aus dem einen oder anderen Grund überschrieben werden muss. In einem späteren Kapitel werden wir im Detail über das Überschreiben von Zugangslevels und Benutzerauthentifizierung sprechen.

Für die DMZ richten wir ein ALG ein, dass ebenfalls für die DMZ angepasst ist. Wir aktivieren SafeSearch nicht, aber wir erzwingen die URL-Prüfung. Wir aktivieren Webinhalt-Filter und erlauben nur eine sehr begrenzte Anzahl an Kategorien, wie nachfolgend gezeigt.

Abbildung 3.7.2 Webinhalt-Filterkategorien für das DMZ-Netzwerk

Schließlich aktivieren wir noch Virenschutz für unsere DMZ-ALG. Wir erlauben verschlüsselten Dateien nicht, hier hindurchzukommen, so dass diese Option abgeschaltet wird.

Rezept 3.8. Netzwerk-Stabilisierung mit der FTP-ALG

Ziele

Der Zweck dieses Rezepts ist, im Detail zu besprechen, wie Sie das Dateiübertragungsprotokoll (FTP, File Transfer Protokoll) und das Anwendungsebene-Gateway (ALG, Application Layer Gateway) einstellen und wie das ALG genutzt werden kann, um die Anzahl der Ports deutlich zu verringern, die von und zu einem Server offen sein müssen, entweder im lokalen Netzwerk oder draußen im Internet.

Detailbesprechung

FTP benutzt zwei Kommunikationskanäle, einen für Kontrollkommandos und einen für die Übertragung der konkreten Dateien. Wenn eine FTP-Sitzung geöffnet wird, stellt der FTP-Client eine TCP-Verbindung (den Kontrollkanal) auf Port 21 (standardmäßig) zum FTP-Server her. Was danach geschieht, hängt davon ab, welcher FTP-Modus genutzt wird.

FTP arbeitet in zwei Modi: **Aktiv** und **Passiv**. Diese Modi legen die Rolle des Servers beim Öffnen der Datenkanäle zwischen Client und Server fest.

- **Aktiv-Modus**

  Im Aktiv-Modus sendet der FTP-Client ein Kommando an den FTP-Server, das anzeigt, mit welcher IP-Adresse und an welchem Port der Server sich verbinden soll.

Der FTP-Server richtet dann aufgrund der empfangenen Adressinformation den Datenkanal zurück zum FTP-Client ein.

- **Passiv-Modus**

  Im Passiv-Modus wird der Datenkanal vom FTP-Client zum FTP-Server geöffnet, genau wie der Kommandokanal. Dies ist der häufig empfohlene Standardmodus für FTP-Clients.

FTP-Sicherheitsaspekte

Sowohl Aktiv- als auch Passiv-Modus der FTP-Operationen stellen den cOS-Core vor Schwierigkeiten. Stellen wir uns ein Szenario vor, in dem sich ein FTP-Client im internen Netzwerk durch die Clavister-Firewall mit einem FTP-Server im Internet verbindet. Die IP-Regel ist dann so eingestellt, dass sie Netzwerk-Datenverkehr vom FTP-Client zu Port 21 am FTP-Server erlaubt.

Wenn der **Aktiv-Modus** genutzt wird, weiß der cOS-Core nicht, dass der FTP-Server eine neue Verbindung zurück zum FTP-Client aufbauen wird. Daher wird die eingehende Verbindung für den Datenkanal verworfen, weil es keine festgelegten Eingang-Regeln gibt, die diese Verbindung erlauben.

Die für den Datenkanal verwendete Portnummer ist dynamisch, so dass der einzige Weg der ist, Datenverkehr von allen Ports des FTP-Servers zu allen Ports des FTP-Clients zu erlauben. Mehr als 64.000 Eingangs-Ports zu öffnen, ist keine Alternative (Clients vermeiden normalerweise die reservierten Ports 0 bis 1024).

Wenn der **Passiv-Modus** genutzt wird, muss die Firewall Verbindungen vom FTP-Server nicht extra erlauben. Andererseits weiß der cOS-Core immer noch nicht, welchen Port der FTP-Client für den Datenkanal zu nutzen versucht. Das bedeutet, dass er den Datenverkehr von allen Ports des FTP-Clients zu allen Ports des FTP-Servers erlauben muss. Obwohl dies nicht ganz so unsicher wie im Fall des Aktiv-Modus ist, stellt es immer noch ein Sicherheitsproblem dar, dass wir gegebenenfalls mehr als 64.000 Ausgangs-Ports öffnen müssen.

Die cOS-Core-ALG-Lösung

Indem wir die FTP-ALG nutzen, löst der cOS-Core dieses Problem, da er sowohl den Kommando- als auch den Datenkanal prüft. Dadurch weiß der cOS-Core, welche(n) Port(s) Server und Client nutzen werden, so dass er die benötigten Ports zwischen Client und Server

(oder andersherum) öffnen kann, ohne 64.000 Ports in Eingangs- oder Ausgangs-Richtung öffnen zu müssen.

Das FTP-ALG prüft sowohl Kommando- als auch Datenkanal und verwirft den Datenverkehr augenblicklich, falls das Kommando oder durch das ALG gesendete Daten nicht als FTP erkannt werden. Das ALG stellt so effektiv sicher, dass alle eingehenden/ausgehenden Verbindungen durch das ALG gültig sind.

Vorteile des FTP-ALG-Hybridmodus

Eine wichtige Eigenschaft der FTP-ALG des cOS-Cores ist seine Fähigkeit, automatisch spontan zwischen Aktiv- und Passiv-Modus zu wechseln, so dass FTP-Verbindungsmodi kombiniert werden können. Auf der einen Seite der Firewall kann der Passiv-Modus genutzt werden, während der Aktiv-Modus auf der anderen genutzt werden kann. Diese Art der FTP-ALG-Verwendung wird manchmal als *Hybridmodus* bezeichnet. Der Vorteil des Hybridmodus kann wie folgt zusammengefasst werden:

- Der FTP-Client kann so eingestellt werden, dass er den Passiv-Modus nutzt (der empfohlene Modus für Clients).
- Der FTP-Server kann so eingestellt werden, den Aktiv-Modus zu nutzen (der empfohlene Modus für Server).
- Wenn eine FTP-Sitzung gestartet wird, empfängt die Clavister-Firewall der nächsten Generation vom FTP-Client automatisch und transparent den passiven Datenkanal sowie den aktiven Datenkanal vom Server und verbindet sie richtig miteinander. Das ist in der nachfolgenden *Abbildung 3.8.1* illustriert.

Abbildung 3.8.1 Umschaltung durch FTP-ALG-Hybridmodus

Durch diese Umsetzung arbeiten im Ergebnis sowohl der FTP-Client als auch der FTP-Server in ihrem jeweils sichersten Modus. Die Umschaltung funktioniert auch andersherum, wenn also der FTP-Client den Aktiv-Modus und der FTP-Server den Passiv-Modus nutzt.

Das FTP-ALG kann nicht für verschlüsselten FTP-Datenverkehr genutzt werden

Wenn Sie das FTP-ALG nutzen, ist es wichtig, sich zu erinnern, dass es keinen verschlüsselten FTP-Datenverkehr wie z.B. SFTP oder FTPS unterstützt.

Ohne das FTP-ALG bedeutet das Zulassen von verschlüsseltem FTP-Datenverkehr, dass womöglich eine große Anzahl Eingangs-Ports geöffnet werden. Wenn der Bedarf für verschlüsseltes FTP aufkommt, wird empfohlen, den Server und Client so einzustellen, dass sie nur einen bestimmten Portbereich benutzen, um so zu versuchen, die Anzahl geöffneter Ports niedrig zu halten.

Das FTP-ALG und die verschiedenen Modus-Varianten

Ein großer Vorteil von FTP ist, dass es ein sehr altes Protokoll ist und sich daher seit seiner Einführung kaum etwas geändert hat. In allen cOS-Core-Standardkonfigurationen gibt es vier voreingestellte ALGs und ALG-Dienste. Ihre Eigenschaften und am häufigsten genutzten Funktionen sind in der nachfolgenden *Tabelle 3.8.2* aufgelistet.

Name	Erlaubte Client-Modi	Erlaubte Server-Modi
FTP-Eingang	Aktiv/Passiv	Aktiv
FTP-Ausgang	Passiv	Aktiv/Passiv
FTP-Durchgang	Aktiv/Passiv	Aktiv/Passiv
FTP-Intern	Passiv	Aktiv

Tabelle 3.8.2 Eigenschaften der standardmäßig voreingestellten FTP-ALGs

Obwohl dies alles mögliche Kombinationen sind, ist es nicht nötig, dass sie alle entsprechende Funktionen haben, was davon abhängt, wie Client und Server konfiguriert sind und welchen Modus sie nutzen. Eine Zusammenfassung der verschiedenen ALGs und welche Kombination abhängig von den Client-/Server-Einstellungen funktioniert, finden Sie in der nachfolgenden *Tabelle 3.8.3*.

#	Verwendetes ALG	Client-Einstellung	ALG-Client-Seite	ALG-Server-Seite	Server-Modus
1	Durchgang	Aktiv	Aktiv	Nur Aktiv anbieten	Aktiv
2	Durchgang	Passiv	Passiv	Erst Passiv anbieten, dann	Passiv

#	Verwendetes ALG	Client-Einstellung	ALG-Client-Seite	ALG-Server-Seite	Server-Modus
				Aktiv	
3	Eingang	Aktiv	Aktiv	Nur Aktiv anbieten	Aktiv
4	Eingang	Passiv	Passiv	Nur Aktiv anbieten	Aktiv
5	Ausgang	Aktiv	Aktiv	-	Aktiv
6	Ausgang	Passiv	Passiv	Erst Passiv anbieten, dann Aktiv	Passiv
7	Intern	Aktiv	Aktiv	-	-
8	Intern	Passiv	Passiv	Nur Aktiv anbieten	Aktiv

Tabelle 3.8.1 Blockierte Kategorien für verschiedene Gruppen

Die obige Tabelle mag schwierig zu verstehen sein, so dass wir ein paar Beispiele hinzufügen, in denen die verschiedenen ALGs genutzt werden. Ein sehr wichtiger Aspekt, auf den wir achten müssen, wenn wir ein FTP-ALG verwenden, ist, dass es zwei Verbindungen erzeugt. Die erste ist eine Verbindung vom FTP-Client zum ALG, dann vom ALG zum FTP-Server, so dass es sich ähnlich einem Proxy verhält. In der obigen Tabelle ist das mit „ALG-Client-Seite“ und „ALG-Server-Seite“ bezeichnet.

Beispiel 1: Der FTP-Client-Nutzer entscheidet, welcher Modus an den FTP-Server gesendet werden soll

- Wir wollen, dass das FTP-ALG sowohl Passiv- als auch Aktiv-Modus auf Client- und Server-Seite akzeptiert. Das FTP-Durchgang-ALG erlaubt diese Kombination.
- Das ALG gibt den Modus, mit dem der Client sich verbinden will, an den Server weiter.
- Das kann dann nützlich sein, wenn der Administrator dem FTP-Client-Nutzer die Möglichkeit geben will, zu wählen, welchen Modus er nutzen will. In dieser Kombination werden keine Hybridmodi genutzt.

Beispiel 2: Einen FTP-Server in unserer DMZ absichern

- Wir wollen, dass der Server im Aktiv-Modus läuft, weil er dann der Initiator des Datenkanals ist. Es ist sicherer, eine Ausgangsverbindung zu öffnen, als auf viele eingehende Ports zu lauschen.
- Das bedeutet, wir wollen, dass das ALG dem Server den Aktiv-Modus vorschlägt, wie es das FTP-Eingang-ALG macht (**#3** und **#4**, das *Eingang*-ALG in der obigen Tabelle).
- Wenn wir jetzt den Clients nur den Aktiv-Modus gestatten würden, würden sie viele Ports öffnen müssen, und wenn NAT benutzt wird, müssten wir Port-Weitergabe zum Client nutzen, weil die Server-Seite die Verbindung einleiten würde.
- Um beide soeben beschriebenen Probleme zu lösen, müssen wir den Clients erlauben, den Passiv-Modus zu nutzen, so dass sie der Initiator des Datenkanals sind. Das FTP-Eingang-ALG erlaubt diese Kombination.
- Wenn der Client Passiv-Modus vorzieht und unser Server den Aktiv-Modus nutzt, können wir eine Situation bekommen, in der die Modi nicht zueinander passen. Das ALG kümmert sich darum, indem es den Hybridmodus nutzt, um die Datenkanäle zu verbinden (wie schon zuvor erwähnt).
- Wenn der Client den Passiv-Modus nutzt, müssen immer noch viele Ports im cOS-Core geöffnet werden. Das ALG kontrolliert dann durch den Kommandokanal, welche(r) Port(s) genutzt werden soll(en), und erlaubt Datenverkehr nur von dem bestimmten Client zu diesem Port/diesen Ports. Das ist die hauptsächliche Stärke des FTP-ALGs, weil es nicht mehr nötig ist, alle Ports zwischen 1.025 und 65.535 zu öffnen, damit FTP funktioniert.

Beispiel 3: Nutzer absichern, die FTP-Clients benutzen, um sich mit Servern im Internet zu verbinden

- Wir wollen, dass die Clients im Passiv-Modus laufen, weil wir wollen, dass der Client den Datenkanal initiiert. Wir wollen keine Lausch-Ports in der Firewall oder beim Client öffnen.
- Das bedeutet, dass das ALG auf der Client-Seite nur Passiv-Modus (**#6**) akzeptiert, wie es das FTP-Ausgang-ALG macht. Wenn der Client versucht, den Aktiv-Modus zu nutzen, wird die Verbindung nicht hergestellt (#5).

- Das ALG bietet einem außerhalb liegenden Server den Passiv-Modus an, aber wenn der Server dies Angebot ausschlägt, bietet das ALG stattdessen den Aktiv-Modus an und läuft dann im Hybridmodus.

Beispiel 4: FTP-Server und Client sind hinter der Firewall

- Der Client muss Passiv-Modus und der Server muss Aktiv-Modus nutzen. Hier wird empfohlen, das FTP-Intern-ALG zu nutzen (**#8**).
- Weil sowohl Server als auch Clients hier unter unserer Kontrolle sind, und weil wir sie auf diese besondere Weise eingerichtet habe, funktioniert dieses stramme Setup.

Zusätzliche-FTP-ALG-Optionen

In allen Standardkonfigurationen gibt es automatisch generierte FTP-ALGs und Dienst-Objekte. In unserem Beispiel werden wir diese Objekte wiederverwenden. Diese automatisch generierten Objekte sind bearbeitbar (außer dem Namen). Neben den verschiedenen Modi, die wir zuvor beschrieben haben, gibt es einige weitere Einstellungen, die der Administrator entweder ändern will oder zumindest kennen sollte, wie nachfolgend gezeigt.

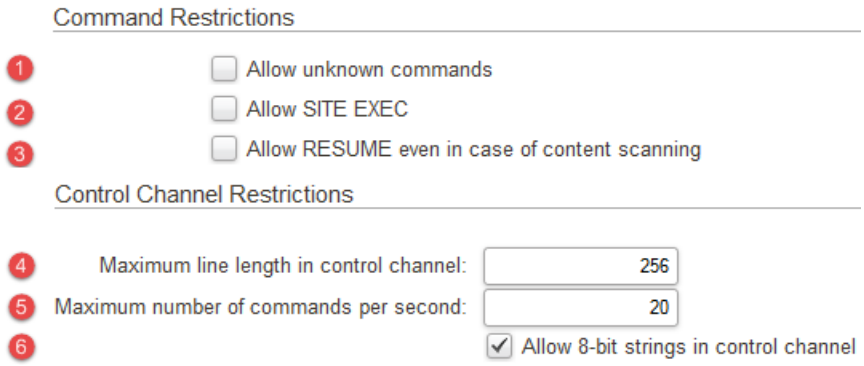


Abbildung 3.8.4 Kommando- und Kontrollkanal-Optionen im FTP-ALG

Unbekannte Kommandos zulassen (**1**) - Damit können FTP-Kommandos erlaubt werden, die nicht zum Standard-FTP-Kommando-Set (definiert in RFC 959) gehören.

SITE EXEC zulassen (**2**) - Einige alte FTP-Server-Versionen unterstützen dieses Kommando, das Zugang zum Server selbst gestattet. Es wird empfohlen, diese Option ausgeschaltet zu lassen, so dass das ALG es blockiert.

RESUME zulassen (**3**) - Das Resume-Kommando (Fortfahren) kann ausgeführt werden, selbst wenn der Inhaltscan die Verbindung beendet hat. Es könnte zum Beispiel blockiert

worden sein, weil wir nicht zulassen, dass .exe-Dateien mit FTP übertragen werden. Es wird empfohlen, diese Option ausgeschaltet zu lassen.

Maximale Zeilenlänge im Kontrollkanal (**4**) - Hiermit beschränken Sie die Länge der Kommandozeile, die ein Client an den Server senden kann. Es ist möglich, mithilfe sehr langer Kontrollkanal-Kommandos eine Art von Angriff gegen den Server zu starten, indem ein Pufferüberlauf verursacht wird. Diese Einschränkung bekämpft diese Bedrohung. Der Standardwert ist 256.

Wenn auf dem Server sehr lange Datei- oder Verzeichnis-Namen verwendet werden, kann es nötig sein, dieses Limit anzuheben. Je niedriger das Limit, desto höher die Sicherheit.

Die Option **Kommandos pro Sekunde** (**5**) kann genutzt werden, um automatisierten Attacken gegen den FTP-Server vorzubeugen. Der Standard ist 20 Kommandos pro Sekunde.

Die Option **8-bit-Zeichenfolgen im Kontrollkanal zulassen** (**6**) legt fest, ob 8-bit-Zeichen im Kontrollkanal erlaubt sind. Das Zulassen von 8-bit-Zeichen macht die Verwendung von Dateinamen mit internationalen Zeichen möglich. Das sind zum Beispiel Akzent- oder Umlautzeichen wie *ääö*.

In unserem Installationsbeispiel werden wir nur einen Punkt im FTP-Eingang und FTP-Ausgang-Objekt ändern, und zwar werden wir den Virenschutz-Scanner aktivieren, wie im nachfolgenden Bildschirmfoto gezeigt.

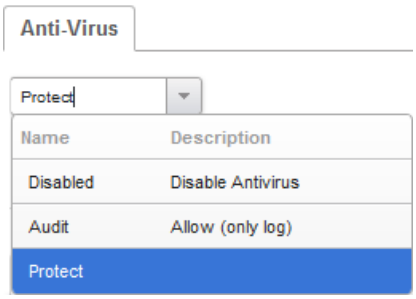


Abbildung 3.8.5 Virenschutz im FTP-ALG als Schutzmodus einstellen

IP-Regeln für ausgehenden Datenverkehr erzeugen

Ähnlich der weiter oben besprochenen HTTP-ALG-Konfiguration wird das FTP-ALG mit der gleichen Reihenfolge der Ereignisse eingestellt, wenn wir ein ALG erzeugen und einer IP-Regel hinzufügen.

1. Erzeugen Sie ein FTP-ALG-Objekt.
2. Erzeugen Sie ein Dienst-Objekt für den Zielport (z.B. Port 21).
3. Weisen Sie das FTP-ALG-Objekt dem Dienst-Objekt zu.
4. Nutzen Sie das Dienst-Objekt mit IP-Regeln.

Wenn die benötigten Dienst-Objekte erzeugt sind, können wir direkt zu unseren IP-Regeln gehen und die IP-Regeln für ausgehenden Datenverkehr für unsere verschiedenen Clients erzeugen, die den FTP-Ausgang-Dienst (sowie das ALG) nutzen, sowie den FTP-Eingang-Dienst für unsere FTP-Server in der DMZ.

Hinweis

Mit „ausgehender Datenverkehr" meinen wir Datenverkehr, der von irgendeinem internen Netzwerk hinaus in Richtung Internet initiiert wird.

Wir erzeugen eine FTP-Ausgang-IP-Regel für alle unsere internen Clients. Das wird im nächsten Bildschirmfoto gezeigt.

Abbildung 3.8.6 FTP-Ausgang-Dienst für das WLAN-Netzwerk

Für unsere Administratoren benötigen wir eine zusätzliche FTP-Regel, weil sie den/die FTP-Server erreichen können müssen, indem sie sich direkt mit der DMZ verbinden. Diese zusätzliche Regel wird im nächsten Bildschirmfoto gezeigt. Weil sie in Richtung eines internen Netzwerks geht, müssen wir keine Adressübersetzung für den Quell-Datenverkehr anwenden. Wir verwenden beispielsweise NAT.

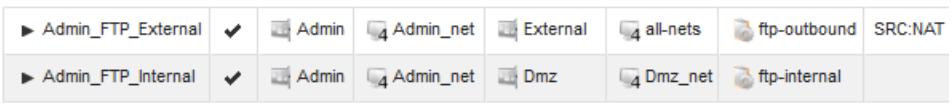


Abbildung 3.8.7 FTP-Ausgang-Dienst für das WLAN-Netzwerk.

IP-Regeln für eingehenden Datenverkehr werden erzeugt.

Wo wir jetzt die ausgehenden IP-Regeln erzeugt haben, brauchen wir eine IP-Regel, die eingehenden Datenverkehr vom Internet in Richtung unseres FTP-Servers in der DMZ zulässt. Das wird in *Abbildung 3.8.8* dargestellt.

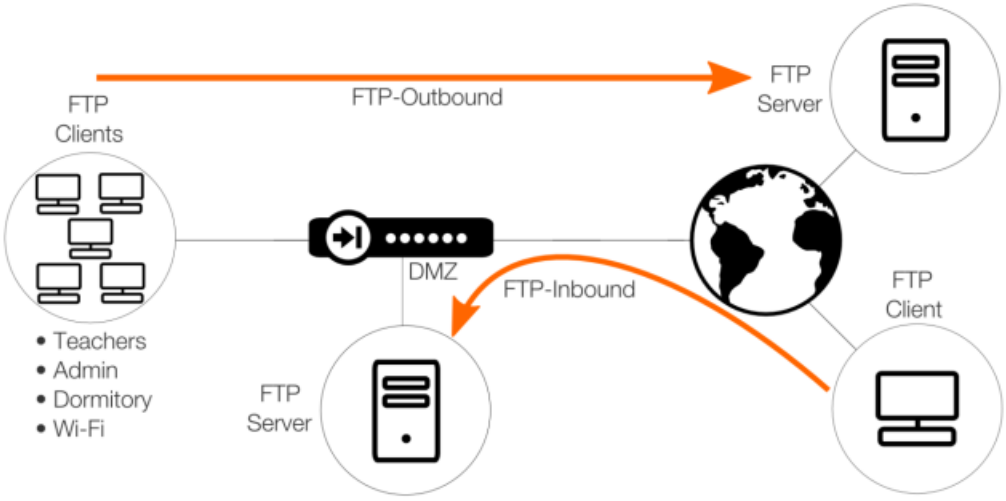


Abbildung 3.8.8 FTP-Ausgang für externe und FTP-Eingang für eingehende Verbindungen

Weil das benötigte ALG und Dienst-Objekt schon erzeugt/angepasst sind, rufen wir unseren IP-Regelsatz auf und erzeugen zunächst eine Regel mit der **Aktion** SAT (Statische Adressübersetzung, Static Address Translation) und mit den nachfolgend gezeigten Eigenschaften.

Abbildung 3.8.9 FTP-Ausgang für externe und FTP-Eingang für eingehende Verbindungen

Wie Sie sehen können, sind die Eigenschaften dieser Regel deutlich anders als die unserer vorangegangenen Regeln. Das liegt daran, dass die Reihenfolge des Datenverkehrs umgedreht wurde. Statt den Datenverkehr vom inneren Netzwerk aus zu initiieren, haben wir jetzt eine Situation, in der wir Nutzer im Internet haben, die unsere FTP-Server in der DMZ erreichen wollen.

Um dies zu erreichen, müssen wir eine Regel erzeugen, die Datenverkehr aus dem Internet behandelt. Weil *EXTERN* der Name unserer externen Internet-Schnittstelle ist, wird dies die Quell-Schnittstelle (**1**). Wir kennen die IPs all der Clients, die sich aus dem Internet mit uns

verbinden, nicht, so dass wir das Quell-Netzwerk auf *alle-netze* (**2**) setzen müssen. Das kann natürlich durch das Verwenden einer einzelnen IP, Gruppe oder eines einzelnen Netzwerks eingeschränkt werden, falls eingeschränkter Zugang bevorzugt wird, aber in unserem Beispiel haben wir einen öffentlichen FTP-Server, der von jedermann erreicht werden kann, so dass wir das Quell-Netzwerk auf *alle-netze* setzen.

Die Ziel-Schnittstelle ist der Core (**3**), weil das Ziel-Netzwerk (**4**) die von der EXTERN-Schnittstelle verwendete, geteilte IP-Adresse ist, mit der sich die Clients zu verbinden versuchen. Standardmäßig wird diese IP-Adresse vom Core geroutet.

Hinweis

Die Core-Schnittstelle ist detaillierter in Kapitel 2: Grundlagen beschrieben.

Als letztes haben wir die Adressübersetzung-Information. In diesem Fall haben wir DST-Übersetzung (= Destination, Ziel), verglichen mit unseren vorangegangenen NAT-Regeln. Das wird nachfolgend gezeigt.

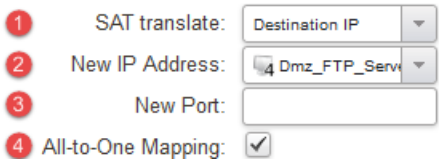


Abbildung 3.8.10 Die SAT-IP-Regel für eingehenden FTP-Datenverkehr

Standardmäßig wird eine SAT-Übersetzung so eingestellt, die Ziel-IP zu sein (**1**). Es ist auch möglich, eine Quellübersetzung zu machen, aber das wird selten gemacht, wenn stattdessen NAT verwendet werden kann. Es gibt ein paar Szenarios, in denen ein Quell-SAT nützlich sein kann, aber das wird in einem späteren Kapitel behandelt.

Die neue IP-Adresse (**2**) wird der FTP-Server mit einer privaten IP-Adresse innerhalb der DMZ sein. Weil wir den Zielport (**3**) nicht ändern, werden wir diese besondere Option leer lassen. Das bedeutet, dass der Originalport benutzt wird (in unserem Fall FTP-Port 21).

Dann gibt es noch eine Option namens All-to-One Mapping (**4**). Diese Option wird hauptsächlich benutzt, wenn wir mehrere Ziel-Netzwerke zu einer bestimmten IP oder einem bestimmten Server übersetzen wollen.

Wir haben diese Option aktiviert, um sicherzustellen, dass die Ziel-Übersetzung von einer bestimmten IP zu einer anderen bestimmten IP erfolgt. Wir aktivieren sie zudem, um eine ziemlich oft auftretende Situation zu vermeiden, in der ein Administrator das Ziel-Netzwerk in einer SAT-Regel als Gruppe, Bereich oder Netzwerk festlegen muss. Dann würde die SAT-Übersetzung eine übertragene Adressübersetzung durchführen, die wir aber auch erst in einem späteren Kapitel behandeln werden.

Hinweis

Wir bezeichnen jeden Datenverkehr, der vom Internet in Richtung unseres cOS-Cores kommt, als eingehenden Datenverkehr.

Eine SAT-Regel benötigt eine zweite passende Regel

Anders als NAT braucht SAT mehr als eine einzige IP-Regel als Einstellung. Zunächst muss eine SAT-Regel, die auf den Ziel-Datenverkehr reagiert, erzeugt werden, um die gewünschte Übersetzung festzulegen.

Wenn der cOS-Core eine passende SAT-Regel gefunden hat, wird er jedoch keine IP-Regelsatz-Anfragen beenden. Stattdessen wird die Suche nach einer passenden Erlauben-, NAT- oder FwdFast-Regel fortgesetzt. Nur wenn der cOS-Core eine solche zweite passende Regel findet, wird die SAT-Regel auf den Datenverkehr angewendet.

Die SAT-Regel legt nur die Übersetzung fest, die stattfinden soll. Die zweite zugewiesene IP-Regel schließlich erlaubt den Datenverkehr-Fluss.

Die zweite Regel reagiert auf die unübersetzte IP-Adresse

Wenn Sie IP-Regeln für SAT erzeugen, ist ein wichtiges Prinzip zu beachten, nämlich, dass die zweite Regel, z.B. eine Erlauben-Regel, auf die originale, unübersetzte IP-Adresse reagieren muss (entweder eine Quell- oder Ziel-IP, abhängig von der Art der SAT-Regel).

Ein häufiger Fehler ist, eine zweite IP-Regel zu erzeugen, die auf die neue, übersetzte IP-Adresse anspricht. Wenn zum Beispiel eine SAT-Regel die Ziel-IPv4-Adresse von 192.168.0.1 nach 172.16.0.1 übersetzt, muss die zweite verbundene Regel dem Datenverkehr gestatten, zum Ziel 192.168.0.1 zu gelangen, und nicht zu 172.16.0.1.

Erst wenn die zweite Regel darauf abzielt, den Datenverkehr zu erlauben, wird der cOS-Core die Route für die übersetzte Zieladresse nachsehen, um herauszufinden, von welcher Schnittstelle der Datenverkehr gesendet werden soll.

Ein einfacher Weg, sicherzustellen, dass die zweite passende Regel richtig reagiert, ist, die *Klonen*-Funktion auf die SAT-Regel anzuwenden, dann das geklonte Objekt unterhalb der SAT-Regel zu platzieren und anschließend seine Aktion in Erlauben, NAT oder FwdFast zu ändern, abhängig von den Bedürfnissen.

In unserem Fall werden wir die Erlauben-Aktion nutzen und sie unterhalt der SAT-Regel platzieren, wie nachfolgend gezeigt.

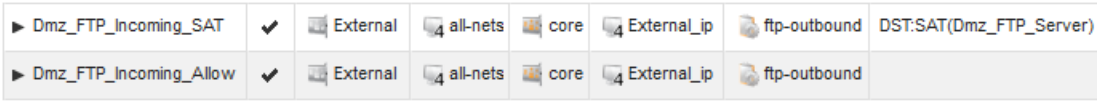


Abbildung 3.8.11 SAT und Erlauben-IP-Regeln für eingehenden FTP-Datenverkehr

Nutzer können sich jetzt mit der externen IP des cOS-Cores an Port 21 verbinden, um Zugang zum öffentlichen FTP-Server der Universität zu bekommen.

Rezept 3.9. Öffentlicher FTP-Serverzugang

Ziele

Der Zweck dieses Rezepts ist, zu beschreiben, wie man mit einer Situation umgeht, die viele Administratoren kennen.

Im vorangegangen Rezept haben wir die Verwendung und Konfiguration von FTP-Clients und -Servern besprochen. Dieses Rezept wird die gleichen IP-Regeln als Grundlage benutzen, um zu beschreiben, wie wir zwei mögliche Probleme lösen können.

Die Regeln, die wir im Moment für FTP und HTTP erzeugt haben, haben die folgenden beiden Hauptprobleme:

- Es ist nicht möglich, sich von einer anderen als der EXTERN-Schnittstelle mit dem FTP-Server der Universität zu verbinden.

- Die IP-Regeln für ausgehendes HTTP sprechen nur an, wenn die Nutzer Internet-Adressen hinter der externen Schnittstelle erreichen wollen. Wenn ein Nutzer sich mit dem FTP-Server (oder einer Webseite) der Universität verbinden will, wird das nicht funktionieren, da die Ziel-Schnittstelle nicht die EXTERN-Schnittstelle ist, sondern die Core-Schnittstelle.

Hinweis

Dieses Rezept nutzt das vorige Rezept als Grundlage, aber die Lösung kann leicht angepasst werden, um für irgendwelche anderen ähnlichen Eigenschaften/Regelsätzen verwendet zu werden, wie in Kapitel 2: Grundlagen im Rezept beschrieben, das sich mit einem Webserver in der DMZ beschäftigt.

Detailbesprechung

Um dieses Problem zu lösen, werden wir ein neues IP-Regeln-Set anlegen, das diese spezielle Situation behandelt. Unsere eingestellten FTP-Regeln sehen momentan so aus wie in der nachfolgenden *Tabelle 3.9.1* gezeigt.

Name	Aktion	Quelle Schnittstelle	Quelle Netz	Ziel Schnittstelle	Ziel Schnittstelle	Dienst
Dmz_FTP_Eingang_SAT	SAT	Extern	alle-Netze	Core	Extern_ip	FTP-Eingang
Dmz_FTP_Eingang_Zulassen	Zulassen	Extern	alle-Netze	Core	Extern_ip	FTP-Eingang
WLAN_FTP_Extern	Wir verwenden beispielsweise NAT.	WLAN	WLAN_net	Extern	alle-Netze	FTP-Ausgang

Tabelle 3.9.1 FTP-IP-Regeln für die EXTERN- und WLAN-Schnittstellen

Wenn wir versuchen, uns von einem Host im WLAN-Netzwerk in Richtung „Extern_ip“ zu verbinden, wird unsere SAT-Regel niemals ansprechen, aufgrund der in **1** und **2** am Anfang dieses Rezepts aufgeführten Gründe.

Hinweis

Das Einstellen von Eingang-Datenverkehr-Regeln mithilfe von SAT wird am Ende von Rezept 3.8 besprochen. Netzwerk-Stabilisierung mit der FTP-ALG

Ein Beispiel für problematischen Datenpaket-Fluss

Ein Nutzer hinter dem WLAN-Netzwerk möchte den FTP-Server erreichen, der sich an der öffentlichen IP der Universität befindet; er versucht sich mit der „Extern_ip“ zu verbinden.

Seine Quell-Schnittstelle wird WLAN sein, so dass wir nun sehen können, dass unsere Eingang-SAT-FTP-Regel nicht ansprechen wird, weil sie nur dafür eingestellt ist, zu reagieren, wenn die Quell-Schnittstelle „EXTERN“ ist.

Die Ausgang-NAT-Regel wird ebenfalls nicht ansprechen, weil die Ziel-Schnittstelle, zu der „Extern_ip“ geroutet wird, nicht EXTERN, sondern der Core ist.

Sogar wenn die NAT-Regel reagieren würde, nutzt unsere Ausgang-NAT-Regel immer noch ein anderes ALG, was niemals funktionieren würde, weil die SAT- und die passende Erlauben-Regel dieselbe ALG-Instanz nutzen müssen.

Das Endergebnis wäre in jedem Fall gleich. Der Datenverkehr wird verworfen, weil keine IP-Regel passt.

Zwei mögliche Lösungen

Dieses Problem hat mehrere Lösungen. Es gibt keinen optimalen weg, dies zu lösen, weil es beim Administrator liegt, zu entscheiden, wie seine Regeln eingestellt werden sollten.

1. Erzeugen Sie eine neue SAT-/NAT-Kombination, die speziell auf jedes interne Netzwerk anspricht.

2. Ändern Sie die bestehenden Regeln ab, um die beteiligten Quell- und Ziel-Schnittstellen zu berücksichtigen.

Hinweis

Wenn Sie ALGs verwenden, muss dasselbe ALG verwendet werden. Wir können nicht für die SAT-Regel und die mit ihr verbundene Erlauben- oder NAT-Regel unterschiedliche ALGs verwenden.

Beide der obigen Lösungen haben ihre Vor- und Nachteile:

Lösung 1 hat den Vorteil, dass die Regeln leichter zu lesen und zu verstehen sind. Der Nachteil ist, dass mehrere Regeln erzeugt werden müssen, um die verschiedenen Szenario und Schnittstellen abzudecken.

Lösung 2 hat den Vorteil, dass der Regelsatz recht schlank bleibt, weil wir nicht so viele IP-Regeln hinzufügen müssen. Der Nachteil hier ist, dass die Konfiguration komplizierter zu lesen und zu verstehen ist. Es ist zum Beispiel nicht immer offensichtlich, zu wissen, dass IP-Regel #1 mit IP-Regel #43 verbunden ist.

Wir werden in diesem Kapitel **Lösung 1** verwenden. Dafür werden wir eine Kombination von zwei Regeln für alle internen Schnittstelle und Netzwerke erzeugen, die in der Lage sein soll, den öffentlichen FTP-Server zu erreichen. Ein Beispiel einer unserer Zwei-Regeln-Kombinationen ist nachfolgend gezeigt.

▶ Wi-Fi_FTP_Incoming_SAT	✔	Wi-Fi	Wi-Fi_net	core	External_ip	ftp-inbound	DST:SAT(Dmz_FTP_Server)
▶ Wi-Fi_FTP_Incoming_Allow	✔	Wi-Fi	Wi-Fi_net	core	External_ip	ftp-inbound	

Abbildung 3.9.2 ALG-Dienst-Objekte verwenden.

Hinweis

Es sollte dick unterstrichen werden, wie wichtig es ist, die richtige Reihenfolge der Regeln zu beachten.

In unserem letzten Konfigurationsbeispiel haben wir SAT-Regeln benutzt. Es wird empfohlen, SAT-Regeln weit oben im Regelsatz zu platzieren, weil sie in einer bestimmten Reihenfolge ansprechen müssen. Die übliche SAT-Regel-Reihenfolge ist „SAT, dann Erlauben", aber wenn die Reihenfolge zu „Erlauben, dann SAT" umgedreht ist, wird der Datenverkehr-Fluss fehlschlagen.

Wenn wir in einem Beispiel die falsche Erlauben-/SAT-Regel-Reihenfolge nutzen, würde die Erlauben-Regel noch immer ansprechen und den Datenverkehr z.B. zur Core-Schnittstelle-IP zulassen. Weil jedoch keine SAT-Regel da ist, die den Datenverkehr zum internen Server umleitet, wird der cOS-Core den Datenverkehr verwerfen und eine Protokollnachricht mit dem Text „Unbehandelt lokal" generieren.

Rezept 3.10. Server-Lastverteilung einstellen

Ziele

Der Zweck dieses Rezepts ist, zu besprechen und zu lernen, wie man eine IP-Regel für Server-Lastverteilung (SLB, Server Load Balancing) einstellt, damit sie die große Anzahl an Anfragen handhaben kann, die in unserem Universität-Beispiel für die Website erwartet werden kann.

Die Universität-Website ist sehr populär. Es gibt Diskussionsforen, Nachrichtenseiten, tägliche Aktualisierungen der Stundenpläne, Back-End-Systeme für Schulprojekte und vieles mehr. Wir erwarten, dass für unsere Website eine große Anzahl Anfragen ankommt. Um die Last handhaben zu können, werden wir eine SLB-IP-Regel einbauen, die den Datenverkehr zwischen drei Servern in der DMZ verteilt, die jeweils Spiegelserver der anderen Server sind.

Die Vorteile davon, die Datenverkehr-Last auf mehrere Server aufzuteilen, sind nicht nur, dass die Geschwindigkeit von Anwendungen verbessert werden kann, sondern auch die Skalierbarkeit durch erleichterte Implementierung eines Server-Clusters (manchmal auch als Serverfarm bezeichnet), der mehr Anfragen handhaben kann, als ein einzelner Server es vermag.

Das Grundprinzip der SLB-Funktionalität ist, Anfragen anzunehmen, die beispielsweise an der EXTERN-Schnittstelle-IP (Extern_ip) ankommen und sie dann an einen Server zu senden, abhängig von einem Verteilalgorithmus (der Algorithmus wird in der IP-Regel ausgewählt).

Eine Darstellung dessen, was wir erreichen wollen, wird als nächstes in *Abbildung 3.10.1* gezeigt.

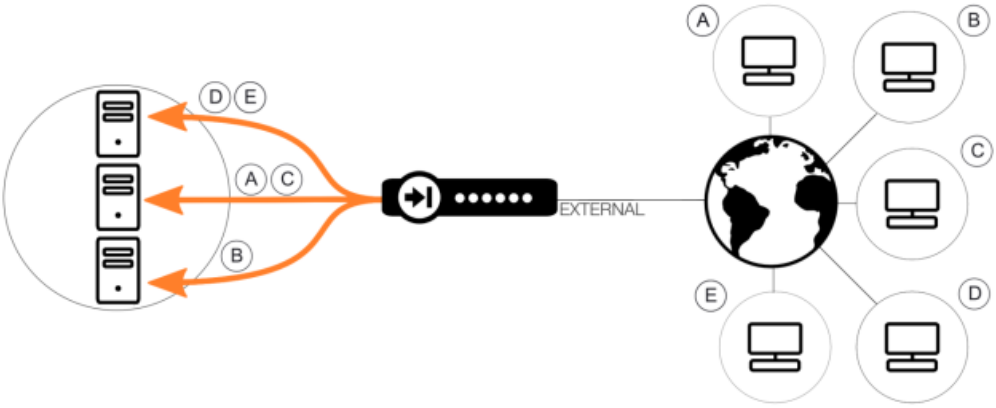


Abbildung 3.10.1 Server-Lastverteilung

Wir haben mehrere Clients im Internet (**A** bis **E**), die sich mit der öffentlichen Website der Universität verbinden wollen. Wenn ein Client an der externen Schnittstelle ankommt, werden wir eine SLB-Regel verwenden, um den Datenverkehr aufzugreifen und die Client-Anfragen auf die drei Webserver zu verteilen (die sich in der DMZ befinden).

Abhängig vom gewählten Verteilalgorithmus müssen die Clients nicht immer in einer bestimmten Reihenfolge auf den Servern landen (**A** muss nicht bei Server *A* landen, **B** muss nicht bei Server *B*) landen.

Detailbesprechung

Vor dem Einstellen der SLB

Bevor wir unsere SLB-Regel erzeugen, müssen wir Adressbuch-Objekte für unsere drei Webserver (in der DMZ) anlegen, wie nachfolgend gezeigt.

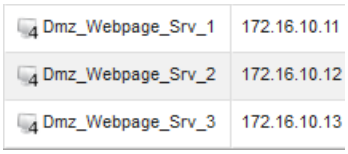


Abbildung 3.10.2 Adressbuch-Objekte für drei Server

Als nächstes erzeugen wir die SLB-IP-Regel selbst. Sie wird auf dieselbe Weise erzeugt wie eine Eingang-FTP-IP-Regel, die in einem der vorangegangenen Rezepte besprochen wurde. Der einzige Unterschied ist, dass wir „SLB SAT" als Aktion wählen.

Die grundsätzlichen Regel-Eigenschaften werden nachfolgend in *Tabelle 3.10.3* gelistet.

Name	Aktion	Quelle Schnittstelle	Quelle Netz	Ziel Schnittstelle	Ziel Schnittstelle	Dienst
Ext_HTTP_ Eingang_SLB	SLB-SAT	Extern	alle-Netze	Core	Extern_ip	http-alle
Ext_HTTP_ Eingang_Zulas-sen	Zulassen	EXTERN	alle-Netze	Core	Extern_ip	http-alle

Tabelle 3.10.3 FTP-IP-Regeln für die EXTERN- und WLAN-Schnittstellen

Für SLB-Regeln müssen wir den SLB-Einstellungen-Tab öffnen (wie nachfolgend gezeigt), um festzulegen, dass unsere neue SLB-IP-Regel die Lastverteilung-Konfiguration vervollständigt, wie im nachfolgenden Bildschirmfoto gezeigt.

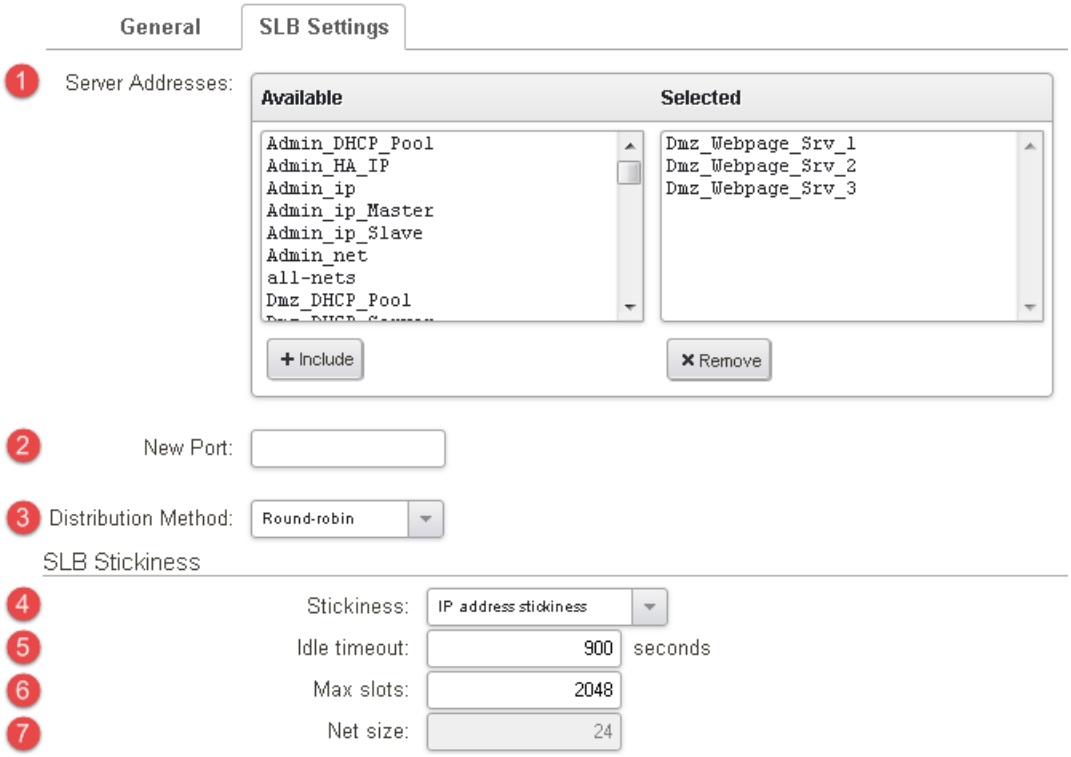


Abbildung 3.10.4 SLB-IP-Regel-Einstellungen

Die erste Option, die wir wählen müssen, sind die Server-Adressen. Hier wählen wir unsere zuvor erzeugten Server-Objekte aus dem Adressbuch (**1**). Das bedeutet, dass Nutzer, die sich mit unserer öffentlichen IPv4-Adresse 203.0.113.10 verbinden, nach der Adressübersetzung bei einer Server-IP-Adresse wie 172.16.10.11, .12 oder .13 landen.

Weil wir kein Interesse daran haben, den Zielport im Innern zu ändern, lassen wir die Option **Neuer Port** (**2**) leer. Nutzer, die an Port 80 ankommen, werden zum gleichen Port im Innern weitergeleitet, nur die Server-IP-Adresse ändert sich.

Es gibt verschiedene Möglichkeiten, festzustellen, wie eine Last in einem Server-Cluster verteilt wird. cOS-Core-SLB unterstützt die folgenden beiden Algorithmen für die **Verteil-Methode** (**3**):

- **Rundlauf-Verfahren** – Der Algorithmus verteilt neu ankommende Verbindungen auf einer Rotationsbasis an eine Serverliste.

- **Verbindungsrate** – Dieser Algorithmus leitet eine Verbindung an den Server weiter, der in einer vorgegebenen Zeitspanne die geringste Anzahl neuer Verbindung hatte.

Es gibt hier keine richtige oder falsche Entscheidung, letztendlich entscheidet der Administrator auf der Basis seiner Anforderungen, welche Methode er verwenden will. Wir werden in diesem Beispiel das Rundlauf-Verfahren benutzen.

Permanenz (**4**) ist etwas, das wir aktivieren sollten. Damit wird gesteuert, wie wir mit mehrfachen Anfragen umgehen wollen, die von derselben Quell-IP (oder Quell-Netzwerk) kommt. Es wird von Vorteil sein, wenn wir versuchen, dass Anfragen, die von derselben Quell-IP stammen, an den gleichen Lastverteilung-Server im Innern gesendet werden. Die Optionen sind Keine, IP oder Netzwerk.

Wir wählen IP, obwohl sogar IP-Permanenz problematisch sein kann, wenn es viele Anfragen von derselben Quell-IP gibt (zum Beispiel, wenn viele Nutzer sich hinter NAT befinden). Wir wollen die Last einzelner Server in der Serverfarm nicht übertreiben, wenn wir es vermeiden können.

Leerlaufzeitüberschreitung (**5**) - Wenn eine Verbindung hergestellt ist, wird die Quell-IP-Adresse für die Verbindung in einer Tabelle gemerkt. Jeder Tabelleneintrag wird als ein *Slot* bezeichnet. Wenn er angelegt ist, bleibt der Eintrag nur für die im Leerlaufzeitüberschreitung-Feld angegebene Anzahl Sekunden gültig. Wenn eine neue Verbindung hergestellt wird, wird die Tabelle nach derselben Quell- IP durchsucht, vorausgesetzt, der Tabellen-Eintrag ist noch nicht abgelaufen. Wurde ein Treffer gefunden, stellt die Permanenz sicher, dass die neue Verbindung an den gleichen Server wie vorherige Verbindungen von derselben Quell-IP gehen.

Der Standardwert für diese Einstellung sind 10 Sekunden, aber wir haben ihn auf 900 (15 Minuten) hochgesetzt, weil wir sicherstellen wollen, dass ein Nutzer so oft wie möglich auf demselben Server landet.

Slots max. (**6**) - Dieser Parameter stellt fest, wie viele Slots in der Permanenz-Tabelle existieren. Wenn die Tabelle sich füllt, wird der älteste Eintrag verworfen, um Platz für einen neuen Eintrag zu machen, selbst wenn er noch gültig war (also die Leerlaufzeitüberschreitung noch nicht erreicht war). Die Folge einer vollen Tabelle kann sein, dass die Permanenz für alle verworfenen Quell-IP-Adressen verlorengeht.

Der Administrator sollte daher versuchen, sicherzustellen, dass der Parameter „Slots max." auf einen Wert eingestellt ist, der für die erwartete Anzahl an Verbindungen, die Permanenz benötigen, ausreicht. Auch wenn wir den Standardwert noch nicht geändert

haben, kann es nötig sein, ihn später nochmal anzuschauen, je nachdem, wie die Anzahl eindeutiger Nutzer ist und ob sie mehrfache Verbindungen zur Serverfarm erzeugen.

Weitere Server-Lastverteilung-Einstellungen

Das nachfolgende Bildschirmfoto zeigt weitere Einstellungen für SLB.

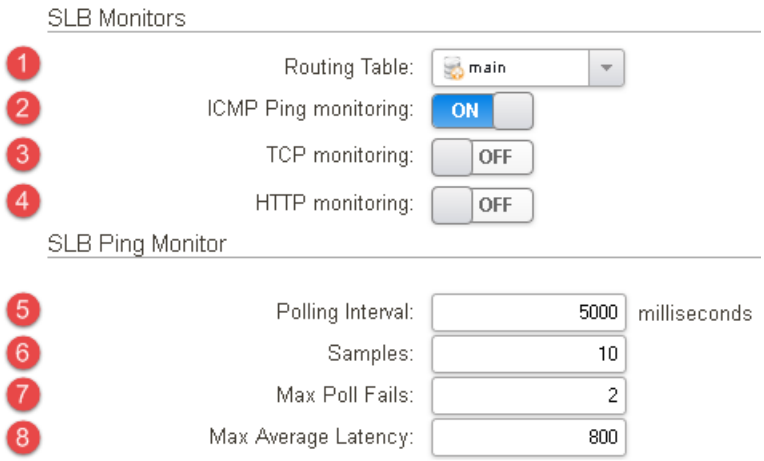


Abbildung 3.10.5 Weitere SLB-IP-Regel-Einstellungen

Die Option **Routingtabelle** (**1**) kontrolliert, welche Routingtabelle vom Monitor genutzt werden soll, um die Ziel-Hosts zu suchen. Weil wir in diesem Kapitel keine Routing-Richtlinie oder virtuelles Routing verwenden, lassen wir den Standardwert *Haupt*.

Bei Serverfarmen wird dringend empfohlen, mindestens eine Überwachungsfunktion einzuschalten. Weil die Server gespiegelt sind, ist es nicht sofort eine Katastrophe, wenn ein Server aus welchem Grund auch immer ausfällt. Wir müssen jedoch in der Lage sein, festzustellen, dass er ausgefallen ist, und dafür ist die Überwachung da. Falls wir keine andere Überwachung haben und ein Server ausfällt, haben wir eine Situation, in der grob geschätzt ein Drittel aller Anfragen für unsere Website fehlschlagen.

Es sind drei verschiedene Arten der Überwachung verfügbar:

- **ICMP** - Eine ICMP-"Ping"-Nachricht wird an den Server gesendet.
- **TCP** - Es wird eine TCP-Verbindung mit dem Server aufgebaut und dann unterbrochen.
- **HTTP** - Es wird eine HTTP-Anfrage an einen bestimmte URL gesendet.

Hinweis

Abhängig davon, welche Art von Überwachungsmethode wir wählen, sind die Überwachungsoptionen unterschiedlich.

In unserem Beispiel werden wir die ICMP-Überwachungsmethode benutzen, um die Sache nicht zu kompliziert zu machen. Für den ICMP-Ping haben wir die folgenden Überwachungsoptionen:

- **Anfrage-Intervall** (**5**) - Diese Option legt fest, wie oft der cOS-Core eine Anfrage an den/die Server senden soll, um zu prüfen, ob sie noch laufen oder nicht. Der Standardwert sind 5.000 Millisekunden.
- **Versuche** (**6**) - Hier legen wir fest, wie viele Versuche an den/die Server gesendet werden sollen. Der Standardwert ist 10.
- **Anfrage-Fehlschläge max.** (**7**) - Diese Option legt fest, wie viele Anfrage-Fehlschläge im Versuche-Umfang erlaubt sein sollen, bevor wir den/die Server als ausgefallen ansehen. Der Standardwert ist 2.
- **Durchschnittliche Latenzzeit max.** (**8**) - Diese Option kontrolliert die maximale Latenzzeit, die wir für die Antwort zulassen wollen, bevor wir entscheiden, dass die Anfrage fehlgeschlagen ist. Der Standardwert sind 800 Millisekunden.

Überwachungsbeispiele

Nehmen wir ein paar Beispiele an, die die oben angesprochenen Standardeinstellungen nutzen, um zu sehen, wie Überwachung funktioniert. Um es einfach zu halten, nutzen wir nur einen Server als Referenz.

Beispiel 1: Der cOS-Core hat einen Abfrage-Auftrag mit 10 Versuchen an einen der Server abgeschlossen. Alle Antworten kamen innerhalb von 100 Millisekunden, so dass die Latenzzeit-Einstellung niemals reagiert hat. Weil unser Abfrage-Intervall auf 5.000 Millisekunden steht, dauerte die Durchführung 50 Sekunden. Wir gehen davon aus, dass der Server läuft.

Beispiel 2: Der cOS-Core hat eine Anfrage mit 10 Versuchen an einen der Server abgeschlossen. Eine der Anfragen hatte aus einem unbekannten Grund einen Timeout, so dass

einer von 10 Abfrage-Versuchen fehlschlug. Weil wir „Anfrage-Fehlschläge max." auf 2 gesetzt haben, gehen wir weiterhin davon aus, dass der Server läuft.

Beispiel 3: Der cOS-Core hat sechs von 10 Abfrage-Versuchen abgeschlossen und alle Anfragen sind fehlgeschlagen, weil keine eine Antwort bekam. Weil der cOS-Core den Auftrag von 10 Versuchen noch nicht abgeschlossen hat, wird der Server noch nicht als ausgefallen angesehen, obwohl „Anfrage-Fehlschläge max." den Wert 2 hat.

Beispiel 4: Der cOS-Core hat jetzt alle 10 Abfrage-Versuche aus dem vorigen Beispiel abgeschlossen, und alle sind fehlgeschlagen. Weil die 10 Abfrage-Versuche abgeschlossen sind, weiß der cOS-Core jetzt, das von den 10 Versuchen mindestens zwei fehlgeschlagen sind. Der Server wird als ausgefallen angesehen.

Das bedeutet, obwohl wir schon zwei fehlgeschlagene Anfragen innerhalb des Abfrage-Intervalls hatten, wurde er nicht für ausgefallen erklärt, bis das Abfrage-Zeitfenster aller 10 Versuche abgeschlossen war. Das wiederum bedeutet, dass die Zeit, bis der Server als ausgefallen angesehen wird, nicht 10, sondern 50 Sekunden beträgt.

Diese Einstellungen können geändert werden, um strammer zu sein, indem wir das Abfrage-Intervall und die Anzahl der Versuche verringern. Es liegt jedoch beim Administrator, zu entscheiden, wie streng der cOS-Core beim Überwachen sein soll.

Mehr Anfragen an leistungsfähigere Server senden

Es kann Situationen geben, in denen eine Serverfarm Server verschiedener Größe und Prozessor-Leistungsfähigkeit enthält. In solchen Situationen kann es gewünscht sein, dass mehr Anfragen an einen bestimmten Server gesendet werden, der mehr Leistungsfähigkeit als andere mit geringeren Kapazitäten hat.

Es gibt keine direkte Option, um dies zu tun, aber wir können die Verteilung-Algorithmen nutzen, um dies zu erreichen. Das tun wir, indem wir denselben Server mehrfach hinzufügen, wie nachfolgend gezeigt.

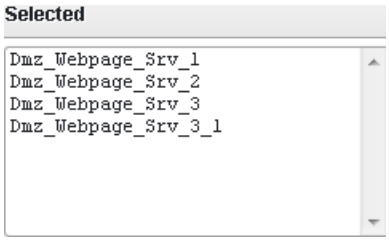


Abbildung 3.10.6 Srv_3 und Srv3_1 haben die gleiche IP-Adresse

Im obigen Beispiel, in dem wir das Rundlauf-Verfahren als Verteilung-Algorithmus benutzen, bedeutet das, dass wir nach einem vollständigen Server-Durchlauf in etwa das Folgende haben:

1. Eine Anfrage an **server_1**
2. Eine Anfrage an **server_2**
3. Eine Anfrage an **server_3**
4. Eine Anfrage an **server_3_1**

Aber weil Server **3** und **3_1** identisch sind, erhält er zwei Anfragen, was im Endeffekt mehr Datenverkehr an diesen bestimmten Server schickt.

Rezept 3.11. POP3-ALG benutzen

Ziele

Der Zweck dieses Rezepts ist, die Konfiguration des POP3-ALG (Post Office Protocol, Postamt-Protokoll) im cOS-Core zu besprechen.

POP3 ist ein Internet-Standardprotokoll auf der Anwendungsebene, das von lokalen E-Mail-Clients genutzt wird, um E-Mails über eine TCP-/IP-Verbindung von einem entfernten Server abzuholen. Praktisch alle modernen E-Mail-Clients unterstützen POP3, und neben IMAP (Internet Message Access Protocol, Internet-Nachrichtenzugang-Protokoll) ist es eines der beiden am meisten verbreiteten Protokolle für E-Mail-Abfragen. Viele Webmail-Dienstanbieter unterstützen entweder IMAP oder POP3, um zuzulassen, dass E-Mails von einem Mailserver heruntergeladen werden, wie nachfolgend in *Abbildung 3.11.1* gezeigt.

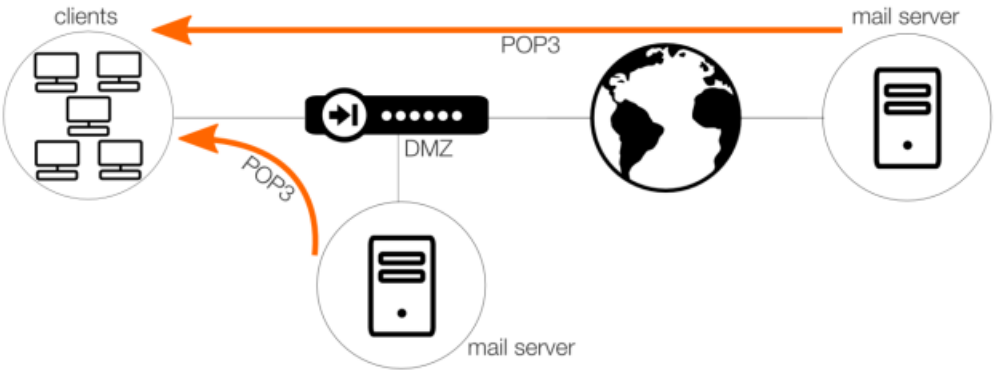


Abbildung 3.11.1 E-Mails mit POP3 von einem internen oder externen Server holen

Um Nutzer zu schützen, die das POP3-Protokoll nutzen, werden wir nicht nur das POP3-ALG für Datenverkehr einbauen, der von unseren internen Netzwerken zu/vom Internet generiert wird, sondern ebenfalls zwischen unseren internen Netzwerken und dem Mail-server, der sich in unserer DMZ befindet.

Der Vorgang, um ein ALG zu erzeugen, ist so wie bei den anderen besprochenen ALGs. Zuerst erzeugen wir das ALG, dann nutzen wir das ALG in einem Dienst und schließlich nutzen wir den Dienst in einer IP-Regel. Dieser dreiteilige Konfigurationsvorgang zum Verwenden irgendeines ALG kann zusammengefasst werden als: **ALG**, dann **Dienst**, dann **IP-Regel**.

Mehr Einzelheiten und Beispiele zum Gebrauch von ALGs finden Sie in *Rezept 3.5. Webzugang durch Webinhalt-Filter beschränken*

Detailbesprechung

Im Vergleich zu den komplexeren ALGs wie das HTTP-ALG hat das POP3-ALG nur relativ wenige Optionen. Die POP3-ALG-Optionen werden im nächsten WebUI-Bildschirmfoto gezeigt.

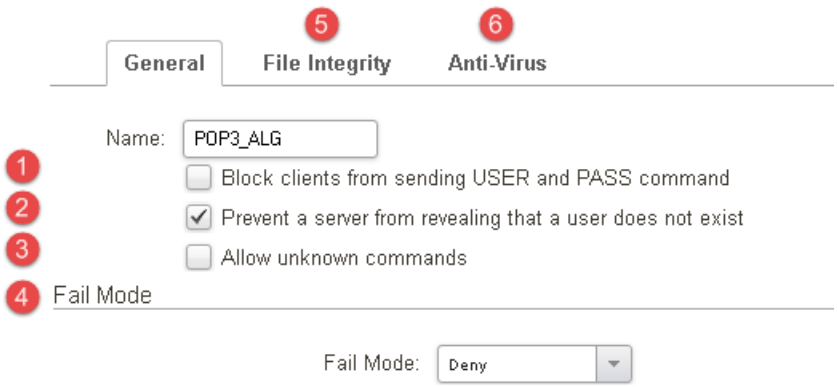


Abbildung 3.11.2 POP3-ALG-Optionen

Die erste Option (**1**) ermöglicht es uns, Verbindungen zwischen Client und Server zu blockieren, wenn die Kombination aus Nutzername und Passwort als leicht lesbarer Klartext gesendet wird (einige Server erlauben allerdings nur diese Methode). In unserer POP3-ALG werden wir dies zulassen, damit wir so kompatibel wie möglich sein wollen und weil dies bei Bedarf leicht geändert werden kann. Falls es keine Server gibt, die nur diese Option unterstützen, wird empfohlen, sie abzuschalten.

Die Option **Nutzer verbergen** (**2**) verhindert, dass der POP3-Server aufdeckt, wenn ein Nutzername nicht existiert. Das verhindert, dass Nutzer verschiedene Nutzernamen ausprobieren, bis sie einen gültigen finden. Wir schalten diese Option ein.

Die Option **Unbekannte Kommandos erlauben** (**3**) gestattet oder verbietet POP3-Kommandos, die nicht dem Standard entsprechen und nicht vom ALG erkannt werden. Um so kompatibel wie möglich zu sein, werden wir unbekannte Kommandos zulassen. Das kann bei Bedarf geändert werden.

Fehlschlag-Modus (**4**) - Wenn der Inhaltscanner feststellt, dass eine Datei schädlich sein könnte, kann die Datei erlaubt oder verboten werden. Diese Option ist hauptsächlich mit Datei-Integritätsprüfungen und Virenschutz-Scannern verbunden. Wir belassen diese Option bei ihrer Standardeinstellung, nämlich *Verweigern*.

Wir haben Virenschutz (**6**) schon mehrfach in anderen Rezepten besprochen, so dass wir die Virenschutz-Einstellungen hier nicht weiter vertiefen. Schauen Sie dazu bitte *Rezept 3.7 Virenschutz einstellen* an, um mehr Einzelheiten über die Virenschutz-Konfiguration zu erhalten. Für unser POP3-ALG setzen wir für Virenschutz den Schützen-Modus.

Sobald das ALG fertig ist, wenden wir den üblichen Drei-Schritte-Einrichtungsvorgang wie für jedes ALG an: **ALG**, dann **Dienst**, dann **IP Regel**.

POP3 benutzt TCP-Port 110, so dass dies der Zielport ist, den wir in unserem Dienst mit unserem POP3-ALG verwenden. Wir gehen nicht davon aus, dass POP3 so häufig wie HTTP oder HTTPS verwendet wird, also setzen wir das Sitzungslimit auf 1000, wie im nachfolgenden Bildschirmfoto gezeigt.

Abbildung 3.11.3 POP3-ALG: Option Sitzungen maximal

IP-Regeln für POP3

Für POP3 erzeugen wir zwei IP-Regeln für jede beteiligte Schnittstelle, wie nachfolgend gezeigt.

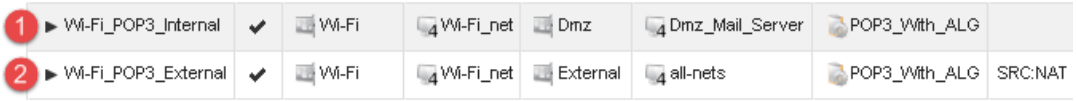


Abbildung 3.11.4 POP3-IP-Regeln

Diese Regeln werden für die Schnittstellen ADMIN, WLAN, DOZENTEN und WOHNHEIM wiederholt.

Die erste Regel (**1**) gestattet Kommunikation zwischen dem Client-Netzwerk und dem internen POP3-Server in der DMZ. Wir brauchen keinerlei Adressübersetzung für diese Regel, weil es sich um Kommunikation zwischen zwei internen Netzwerken handelt und wir keinen Grund haben, die Quell-IP des Clients zu maskieren.

Zudem ist es vorteilhaft, die Quell-IP des Clients sehen zu können, wenn wir mithilfe der Protokolle irgendwelche Probleme untersuchen, so dass schon aus diesem Grund Adressübersetzung möglichst vermieden werden sollte.

Die zweite Regel (**2**) gestattet Kommunikation zwischen dem Client-Netzwerk und einem Host/Server im Internet. Es gibt Grund zur Annahme, dass viele Nutzer E-Mail-Konten auf anderen Servern und nicht nur an der Universität haben.

Hinweis

Für Mailserver ist es nicht ungewöhnlich, SSL oder ähnliche verschlüsselte Protokolle für POP3- und SMTP-Datenverkehr zu nutzen. Der POP3-ALG unterstützt keinen verschlüsselten Datenverkehr, so dass es für solche verschlüsselten E-Mails nicht genutzt werden kann.

Rezept 3.12. SMTP-ALG einstellen

Ziele

Der Zweck dieses Rezepts ist, zu erläutern, wie das SMTP-ALG eingestellt wird. Zusätzlich werden wir auch besprechen, wie man die Anti-Spam-Funktion im SMTP-ALG einstellt und aktiviert.

Detailbesprechung

SMTP (Simple Mail Transfer Protocol, Einfaches Mail-Übertragungsprotokoll) ist ein textbasiertes Protokoll, das zur Übertragung von E-Mails zwischen Mailservern im Internet verwendet wird. Typischerweise befindet sich ein lokaler Mailserver in einer DMZ (Entmilitarisierte Zone), so dass E-Mails, die von entfernten Mailservern geschickt werden, die Clavister-Firewall durchlaufen müssen, um den lokalen Server zu erreichen.

Lokale Clients hinter der Firewall verwenden dann E-Mail-Clientsoftware, um E-Mails vom Server abzurufen und E-Mails an den Server zu senden, um sie an andere Mailserver im öffentlichen Internet weiterzuleiten.

Für die Kommunikation zwischen Clients und einem Mailserver können verschiedene Protokolle genutzt werden. Das Abrufen kann ebenfalls mit POP3 geschehen (siehe *Rezept 3.11. POP3-ALG benutzen*), aber das Versenden von E-Mails zum Server kann auch mit SMTP gemacht werden, wie nachfolgend in *Abbildung 3.12.1* dargestellt.

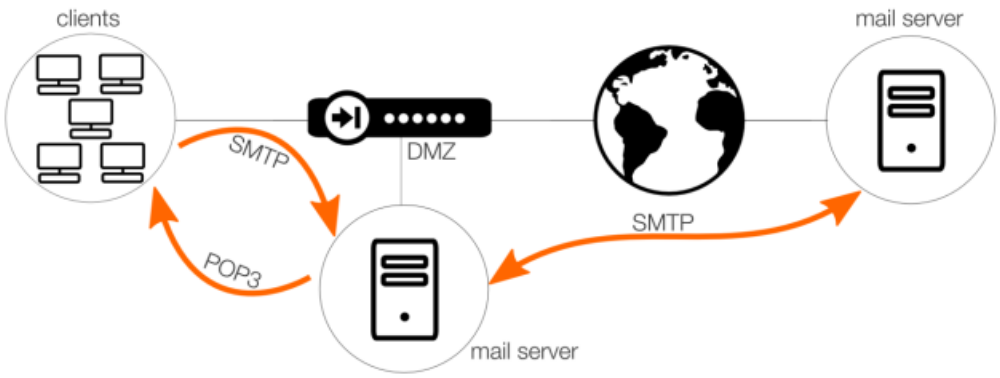


Abbildung 3.12.1 SMTP- und POP3-Kommunikation

SMTP-ALG erzeugen

Der Vorgang, um ein ALG zu erzeugen, ist so wie bei den anderen ALGs, die wir schon zuvor in diesem Kapitel besprochen haben (FTP, HTTP usw.). Mehr Informationen über ALGs im Allgemeinen finden Sie in *Rezept 3.5. Webzugang durch Webinhalt-Filter beschränken*

Erzeugen Sie zuerst das ALG, dann fügen Sie das ALG einem Dienst hinzu und nutzen ihn schließlich mit einer IP-Regeln. Die drei Schritte, die immer benötigt werden, wenn ein ALG verwendet werden soll, sind immer: **ALG**, dann **Dienst**, dann **IP Regel**.

Im ersten Schritt erzeugen wir das SMTP-ALG und geben ihm einen passenden Namen, wie nachfolgend gezeigt. Weil wir vorhaben, nur ein SMTP-ALG für dieses Szenario zu erzeugen, geben wir ihm einen sehr allgemeinen Namen.

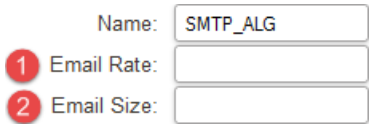


Abbildung 3.12.2 SMTP-ALG: Allgemeine Optionen

Es gibt zwei Optionen, die hier von Interesse sind. Die erste ist **E--Mail-Rate** (**1**). Diese Option kontrolliert, wie viele E-Mails vom selben Host binnen 60 Sekunden versendet werden dürfen. Wir lassen diese Option leer, weil wir nicht wissen, welche konkrete E-Mail-Rate wir nötig haben, und weil wir zu Anfang unsere Nutzer nicht einschränken wollen, bis wir das Datenverkehr-Aufkommen kennen. Was ist ein guter Wert? Das hängt immer von der Netzwerkgröße und dem Datenverkehr-Aufkommen ab. 10? Es liegt beim Administrator, einen passenden Wert für seine Umgebung festzulegen.

Die zweite Option, **E-Mail-Größe** (**2**), kontrolliert die maximale Größe der E-Mails, die durch das SMTP-ALG gesendet werden kann (in Kilobytes). Diese Option kann nützlich sein, wenn wir vermeiden wollen, dass Nutzer E-Mails mit großen Dateianhängen versenden. Auch diese Option lassen wir in unserem Beispiel leer, weil auch sie von den Netzwerk-Anforderungen abhängt, und davon, ob der Administrator dies einschränken will oder nicht.

SMTP-ALG: Funktions-Tabs und Optionen

Das SMTP-ALG hat die nachfolgend gezeigten Tabs. Einige dieser Eigenschaften haben wir bereits in früheren Rezepten besprochen und werden sie daher nicht mehr im Detail behandeln. Stattdessen gehen wir im Detail nur auf die Funktionen und Optionen ein, die sich speziell auf das SMTP-ALG beziehen.

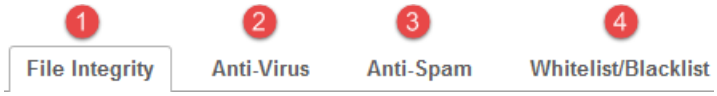


Abbildung 3.12.3 SMTP-ALG-Tabs und -Optionen

Datei-Integrität (**1**) ist eine Funktion, die genutzt werden kann, um bestimmte Dateiarten wie .exe oder .zip zu blockieren.

Anti-Spam (**3**) ist eine der Haupteigenschaften des SMTP-ALG, und wir werden uns die Details dieser Option später in diesem Abschnitt anschauen.

Whitelist/Blacklist (**4**) ist eine Funktion, die verwendet werden kann, um zu vermeiden, dass ein Nutzer versehentlich auf einer Blacklist landet (wie nachfolgend gezeigt). Wir wollen zum Beispiel nicht, dass der Administrator aus Versehen auf einer Blacklist landet. Um sicherzustellen, dass das niemals passiert, können wir diesen Nutzer in die Whitelist aufnehmen. Oder falls wir einen Nutzer haben, von dem wir wissen, dass er von einem Virus befallen oder auf andere Weise belastet ist, können wir ihn der Blacklist hinzufügen.

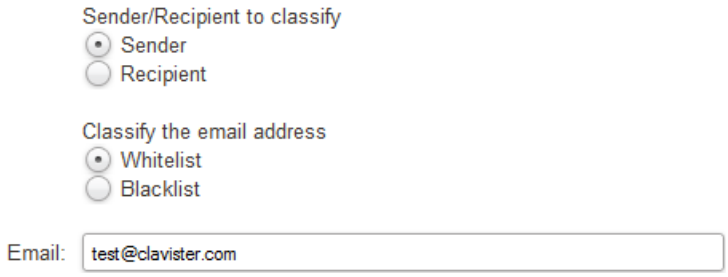


Abbildung 3.12.4 Whitelist und Blacklist nutzen

Sie können hier sog. Wildcards verwenden; z.B. kann der Listeneintrag **@clavister.com* verwendet werden, um alle möglichen E-Mail-Adressen zu bezeichnen, die sich auf diese Domäne beziehen.

Spam Spam Spam Spam Spam!

Unerwünschte E-Mails, häufig als Spam bezeichnet, sind zu einem der größten Probleme und auch zu einem Sicherheitsproblem im öffentlichen Internet geworden. Unerwünschte E-Mails, die in großen Massen von als Spammern bezeichneten Gruppen verschickt werden, können Ressourcen verschwenden, Schadsoftware mit sich bringen und auch versuchen, den Leser auf Webseiten zu locken, die Browser-Sicherheitslücken ausnutzen.

Der cOS-Core bietet zwei Ansätze, um mit Spam umzugehen:

- Er kann E-Mails verwerfen, die eine sehr hohe Wahrscheinlichkeit haben, Spam zu sein.
- Er kann E-Mails durchlassen, aber markieren, wenn sie eine mäßige Wahrscheinlichkeit haben, Spam zu sein.

Um eine dieser beiden Aktionen zu verwenden, müssen wir zuerst festlegen, was Spam ist und was nicht. Um dies zu erreichen, werden wir Datenbanken befragen, sogenannte *DNS-Blacklists*.

DNS-Blacklist-Datenbanken

Eine Anzahl vertrauenswürdiger Organisationen stellen öffentliche Datenbanken zur Verfügung, die die ursprüngliche IP-Adresse bekannter Spam-SMTP-Server enthalten, welche über das öffentliche Internet abgefragt werden können. Diese Datenbanken werden als DNS-Blacklist-Datenbanken (DNSBL) bezeichnet, und die Informationen werden durch eine standardisierte Anfragemethode zur Verfügung gestellt, die vom cOS-Core unterstützt wird.

Wenn die Anti-Spam-Filterfunktion des cOS-Cores eingerichtet ist, wird die IP-Adresse des Servers, der die E-Mail sendet, an einen oder mehrere DNSBL-Server geschickt, um herauszufinden, ob einer dieser Server meint, die E-Mail sei von einem Spammer, oder eben nicht. Die Antwort, die vom DNSBL-Server zurückkommt, ist entweder die Antwort „nicht gelistet" oder „gelistet". Falls sie gelistet ist, zeigt der DNSBL-Server an, dass die E-Mail Spam sein könnte und stellt normalerweise zudem Informationen in einem TXT-Datensatz zur Verfügung, der eine Textbeschreibung der Listung enthält.

Hinweis

DNSBL-Server führen keine Blacklists mit individuellen E-Mail-Adressen, sondern mit Mailserver-IPs.

Die nachfolgende Abbildung 3.12.5 zeigt den DNSBL-Vorgang. Wenn in diesem Beispiel Anti-Spam eingestellt ist, wird der cOS-Core zwei DNSBL-Server kontaktieren und fragen, ob der Sender einer eingehenden E-Mail ein potenzielles Risiko darstellt oder nicht, und entsprechend agieren, abhängig von der Antwort. Wir gehen später in diesem Abschnitt noch genauer darauf ein, wie dies durchgeführt wird.

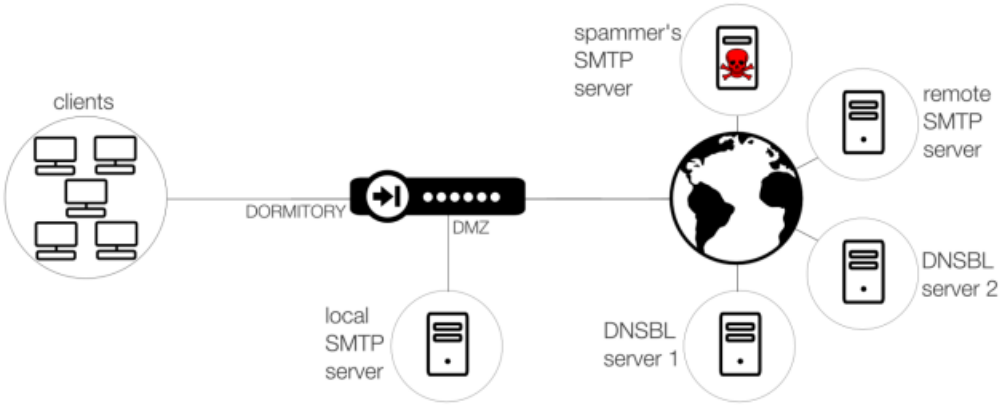


Abbildung 3.12.5 DNSBL für Anti-Spam nutzen

Anti-Spam und seine Optionen einstellen

Der Anti-Spam-Teil des SMTP-ALGs hat eine Vielzahl an Optionen. Beginnen wir mir den allgemeinen Optionen, die nachfolgend gezeigt werden.

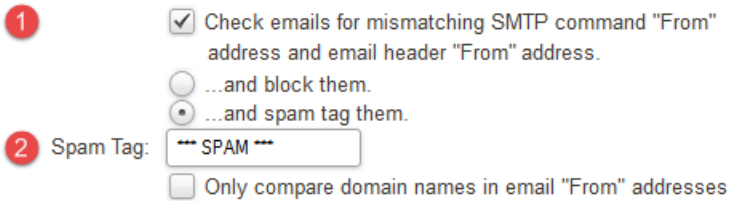


Abbildung 3.12.6 Allgemeine Anti-Spam-Optionen des SMTP-ALGs

Die erste Option (**1**) wird verwendet, um nicht identische „Von"-E-Mail-Adressen im SMTP-Protokoll und im aktuellen E-Mail-Header zu entdecken. Spammer können diese absichtlich unterschiedlich machen, um E-Mails alle Filter passieren zu lassen, so dass diese Funktion die E-Mail-Integrität nochmals prüft.

Wenn entdeckt wird, dass sie nicht identisch sind, kann eine von zwei Aktionen eingestellt werden: Blockieren oder die E-Mail als Spam markieren. In unserer Umgebung haben wir beschlossen, diese Art von E-Mails als Spam zu markieren. Es ist sehr verdächtig, wenn eine E-Mail ankommt, deren „Von"-Adresse zum Beispiel *test1@test1.com* heißt, während der E-Mail-Header sagt, sie laute *test2@test2.com*.

Wenn wir die Option „Als Spam markieren" (**2**) nutzen, können wir festlegen, wie die E-Mail im Falle, dass die E-Mail-Prüfung anschlägt, markiert werden soll. Die Spam-Markierung, die nachfolgend gezeigt wird, ist der standardmäßige Text.

Anti-Spam-Filteroptionen

Indem wir fortfahren, Anti-Spam zu konfigurieren, kommen wir zu den Haupt-Kontrolloptionen, die festlegen, wie Anti-Spam reagieren soll und welche DNSBL-Server wir für die Klassifizierung nutzen wollen.

Diese Optionen werden im nächsten WebUI-Bildschirmfoto gezeigt.

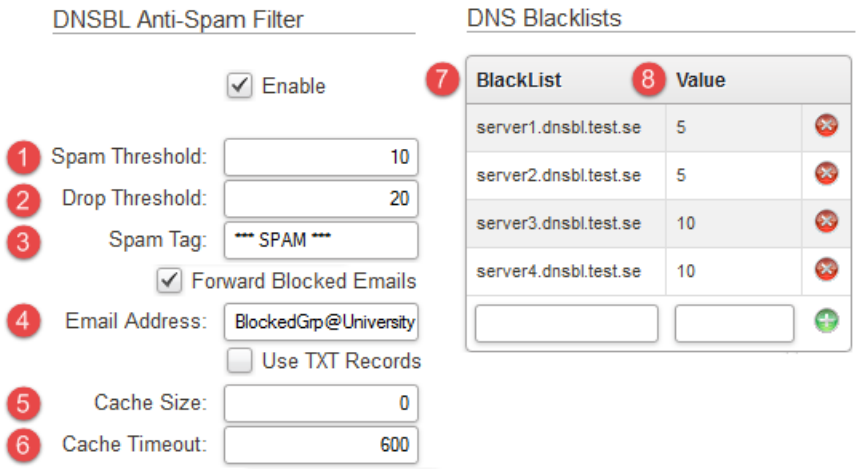


Abbildung 3.12.7 Anti-Spam-Konfigurationsoptionen

Sobald Anti-Spam aktiviert ist, haben wir eine Fülle von Optionen zu berücksichtigen. Um mit dem **Spam-Schwellwert** (**1**) beginnen: Diese Einstellungen legt den Gesamtwert fest, der nötig ist, um die E-Mail als Spam zu klassifizieren.

Wenn wir unsere Blacklist-Serverliste (**7**) und ihre Werte (**8**) ansehen, so haben wir momentan vier Server, zwei mit dem Wert 5 und zwei mit dem Wert 10. Diese Werte werden durch den Administrator festgelegt, abhängig davon, wie vertrauenswürdig die Antwort dieses bestimmten Servers ist. Wir trauen den DNSBL-Servern 1 und 2 nur halb so viel wie den DNSBL-Servern 3 und 4.

Mit diesen Werten im Hinterkopf kehren wir zurück zum betrachteten Spam-Schwellwert (**1**), bei dem wir momentan einen Wert von 10 haben. Das bedeutet, wenn die DNSBL-Server 1 und 2 (Ergebnis 5+5 = 10) antworten, wird für diese bestimmte E-Mail angenommen, dass sie von einem nicht vertrauenswürdigen/infizierten Host stammt und daher wird sie mit dem festgelegten Text als Spam markiert (**3**).

Lassen Sie uns jedoch einmal annehmen, dass die DNSBL-Server 1, 2 und 3 alle berichten, dass die IP (also der Server) nicht vertrauenswürdig oder infiziert ist. Dann haben wir einen Wert von 5+5+10 = 20, und unser Schwellwert für das Verwerfen (**2**) reagiert. Dies ist eine zweistufige Regel, die wir so einstellen können, dass wir E-Mails direkt verwerfen können, die starke Indizien für Spam mitbringen. Oder wir können sie an eine bestimmte E-Mail-Adresse weiterleiten, indem wir die Option **Blockierte E-Mail weiterleiten** aktivieren und eine entsprechende E-Mail-Adresse für die Weiterleitung festlegen (**4**).

Es ist Sache des Administrators, zu entscheiden, welche Aktionsebene hier genutzt werden soll. Eine Alternative wäre, den Verwerfen-Schwellwert auf einen höheren Wert zu setzen, als möglich ist. Dann würde diese Regel niemals reagieren und der cOS-Core würde E-Mails nur als Spam markieren, aber niemals löschen.

Cache-Größe (**5**) meint die Anzahl Einträge, die der Cache aufnehmen kann. Mit Eintrag meinen wir die IP und die Server-Antworten für diese IP-Adresse. Wenn dieser Wert auf Null gesetzt ist, wird der Cache nicht genutzt. Das Erhöhen der Cache-Größe erhöht auch den Speicherbedarf im cOS-Core für Anti-Spam. Der Maximalwert ist 500.

Cache-Timeout legt fest, wie lange eine Adresse gültig bleibt, sobald sie im Cache gespeichert ist. Nach dem Ablauf dieser Zeit muss eine neue Anfrage für eine zwischengespeicherte Absender-Adresse zu den DNSBL-Servern gesendet werden.

Anti-Spam-IP-Regel-Konfiguration

Weil wir unseren Mailserver in der DMZ schützen wollen, benutzen wir unser SMTP-ALG mit einer SAT-/Erlauben-Regel-Kombination. Das ermöglicht eingehende Verbindungen vom Internet zu unserem Webserver in der DMZ, wie in der nachfolgenden Regel-Zusammenfassung dargestellt.

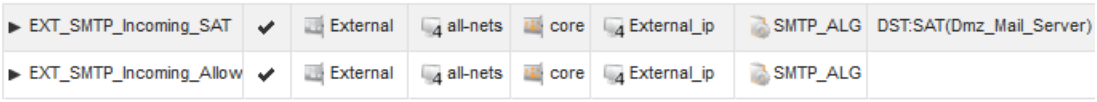


Abbildung 3.12.8 Anti-Spam-Konfigurationsoptionen

Für Fortgeschrittene: Wie behandle ich fehlgeschlagene DNSBL-Server-Anfragen

Wenn eine DNSBL-Anfrage einen Timeout hat, behandelt der cOS-Core sie als fehlgeschlagen und zieht den Wert des Servers sowohl vom Spam- als auch vom Verwerfen-Schwellwert ab.

Wann immer ein eingestellter DNSBL-Server nicht innerhalb der geforderten Zeit antwortet, wird eine Protokollnachricht generiert. Das wird jeweils nur einmal direkt am Anfang einer Serie von Antwort-Fehlschlägen eines Servers gemacht, um sich wiederholende Nachrichten zu vermeiden.

Für Fortgeschrittene: Die vom SMTP-ALG genutzte Ablaufreihenfolge

Der SMTP-Filter gehorcht der folgenden Ablaufreihenfolge, die ähnlich der Reihenfolge ist, die das HTTP-ALG befolgt, mit Ausnahme des hinzugefügten Spam-Filters:

1. Whitelist.
2. Blacklist.
3. Spam-Filter (falls aktiviert).
4. Virenschutz-Scanner (falls aktiviert).

Das bedeutet, wenn eine Sender-Adresse sowohl in der Blacklist als auch in der Whitelist ist, hat die Whitelist Vorrang, so dass ein Nutzer auf der Whitelist niemals irgendwelche Probleme haben wird, E-Mails zu senden oder zu empfangen.

Rezept 3.13. Anwendungskontrolle nutzenhatten

Ziele

Bis hier haben wir Zugangslevel mithilfe von Ports und bis zu einem gewissen Grad mit Anwendungsebene-Gateways (ALGs) kontrolliert. Es gibt jedoch viele Szenarios, in denen mehrere Anwendungen den gleichen Port oder das gleiche Protokoll nutzen. Wie können wir aber eine blockieren und die andere zulassen, wenn sie den gleichen Port nutzen? Der Zweck dieses Rezepts ist, die Konfiguration und die Verwendung von Anwendungskontrolle (AC, Application Control) zu erläutern, die entscheidet, welchen Programmen der Netzwerkzugang gestattet werden soll.

Detailbesprechung

In dem nachfolgend in *Abbildung 3.13.1* illustrierten Beispiel wollen wir Nutzern erlauben, sich mit Facebook zu verbinden, aber nicht mit YouTube.

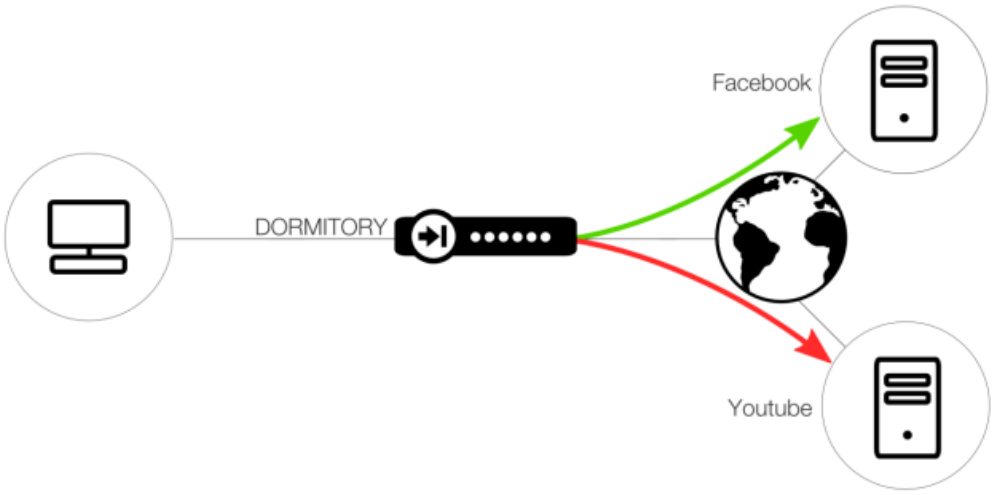


Abbildung 3.13.1 Zugang zu Facebook erlauben, aber nicht zu YouTube

Indem wir Anwendungskontrolle verwenden, können wir den Datenverkehr und die Datenpakete betrachten, die von unseren Nutzern erzeugt werden, und sie mit einer Anwendungssignaturen- Datenbank abgleichen. Jede Signatur entspricht einer Art von Anwendung.

Um dies zu erreichen, werden wir zunächst einen Anwendung-Regelsatz erzeugen, das festlegt, wie die Anwendungskontrolle sich verhalten soll und welche Anwendungen wir erlauben oder verweigern wollen. Wir können Anwendungskontrolle-Einstellungen auch direkt in einer IP-Regel anlegen und nutzen, aber wir werden einen Anwendung-Regelsatz erzeugen, weil wir denselben AC-Regelsatz in mehreren Regeln wiederverwenden wollen. Ein solcher Regelsatz wird im Richtlinien-Abschnitt gemacht, wie im nächsten Bildschirmfoto gezeigt.

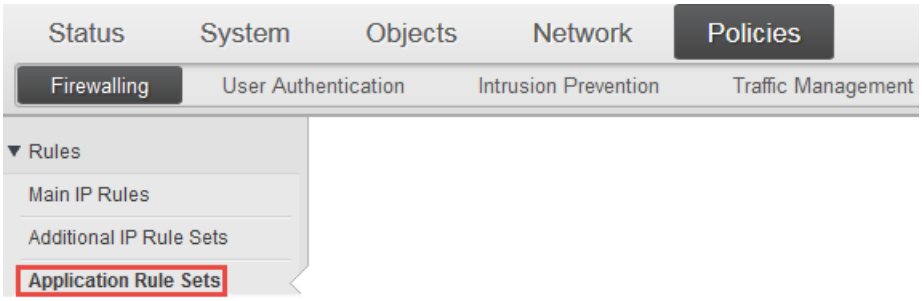


Abbildung 3.13.2 Die Position des Anwendung-Regelsatzes

Hinweis

Wir verwenden YouTube und Facebook hier als Beispiele, aber letztendlich liegt es beim Administrator, festzulegen, welche Anwendungen erlaubt oder verweigert werden sollen. Manche Admins wollen nur protokollieren, welche Anwendungen überhaupt genutzt werden.

Warum es wichtig ist, die Standardaktion-Option zu verstehen

Wenn wir einen Anwendung-Regelsatz erzeugen, werden uns zunächst einige allgemeine Optionen dargeboten, wie im nächsten WebUI-Bildschirmfoto gezeigt.

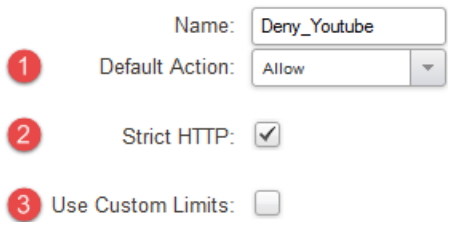


Abbildung 3.13.3 Allgemeine Anwendung-Regelsatz-Optionen

Die **Standardaktion** (**1**) ist eine sehr wichtige Einstellung. Sie kann entscheiden, wie AC Anwendungen behandelt, die unseren Filterkriterien entsprechen (wenn überhaupt).

Die zwei möglichen Werte für die Standardaktion sind:

- **Erlauben** - Im Erlauben-Modus werden alle Anwendungen zugelassen, außer den festgelegten Anwendungen, die wir in unseren AC-Regelfiltern zum Verweigern festgelegt haben. Verweigern Sie zum Beispiel YouTube und lassen Sie alle anderen Anwendungen zu.
- **Verweigern** - Im Verweigern-Modus werden alle Anwendungen verweigert außer den festgelegten Anwendungen, die wir in unseren AC-Regelfiltern zum Erlauben gewählt haben. Erlauben Sie zum Beispiel Facebook und DNS, und verweigern Sie alle anderen Anwendungen.

Hinweis

Es sollte nochmal hervorgehoben werden, wie wichtig es ist, den Unterschied dieser beiden Aktionen zu verstehen. Je nach Wahl machen sie, dass AC komplett unterschiedlich funktioniert.

Die Option **Striktes HTTP** (**2**) legt fest, wie streng der cOS-Core sein soll, wenn er reines HTTP behandeln soll, weil viele Programme den HTTP-Port nicht nur für HTTP-Daten nutzen. Diese Einstellung bewirkt, dass der cOS-Core sich HTTP-Daten genauer anschaut, um festzustellen, welcher Art sie sind.

Hinweis: Zusätzliche Informationen über Striktes HTTP

Viele Protokolle, die die Anwendungskontrolle prüft, sind dem HTTP-Protokoll aufgesetzt. In einigen Fällen, wenn HTTP selbst durch die Anwendungskontrolle blockiert ist, kann ein Protokoll, dass auf HTTP basiert, fälschlicherweise ebenfalls blockiert werden. Um zu versuchen, dieses Problem zu lösen, kann die Einstellung „Striktes HTTP" in den relevanten Anwendung-Regeln deaktiviert werden. Dadurch wird die Anwendungskontrolle gezwungen, die gesamte Protokollstruktur auszuwerten, bevor eine Entscheidung über die Art des Protokolls getroffen wird.

Die Einstellung **Benutzerdefiniertes Limit** (**3**) ermöglicht uns, die globale erweiterte Einstellung zu überschreiben, die kontrolliert, inwieweit ein Datenpaket gescannt werden soll, bevor wir es als „unbekannt" klassifizieren. Die maximal untersuchte Datenmenge, um diese Entscheidung zu treffen, wird im cOS-Core festgelegt, sowohl als Anzahl von Datenpaketen und als Anzahl Bytes.

Standardmäßig sind diese beiden Werte wie folgt:

- Nicht klassifizierte Datenpakete max.: 5
- Nicht klassifizierte Bytes max. 7.500

Wenn einer dieser Werte erreicht ist, wird entschieden, dass die Daten nicht klassifizierbar sind. Wenn der Administrator diese Einstellungen individuell abändern will, ohne sie global zu ändern, ist hier die richtige Stelle dafür. Wir lassen diese Einstellung bei ihren Standardwerten.

Diese Optionen können global unter **System -> Erweiterte Einstellungen -> Anwendungskontrolle-Einstellungen** geändert werden.

Ein AC-Beispiel: YouTube verweigern, alle anderen Anwendungen erlauben

In unserem ersten Beispiel wollen wir einen Anwendung-Regelsatz anlegen, der speziell den Zugang zu YouTube blockiert, aber alle anderen Anwendungen erlaubt.

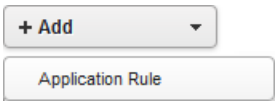


Abbildung 3.13.4 Eine neue Anwendung-Regel hinzufügen

Jetzt sind wir bei den Haupteinstellungen und -Optionen für Anwendungskontrolle angekommen, wie nachfolgend gezeigt. Wir werden unsere Bemühungen hauptsächlich auf den **Anwendung** (**1**)-Tab konzentrieren, wo wir mithilfe der Aktion (**2**) (Erlauben oder Verweigern) auswählen, welche Anwendungen erlaubt oder verweigert werden sollen. Bevor wir das tun, wollen wir einige der anderen hier verfügbaren Optionen erwähnen.

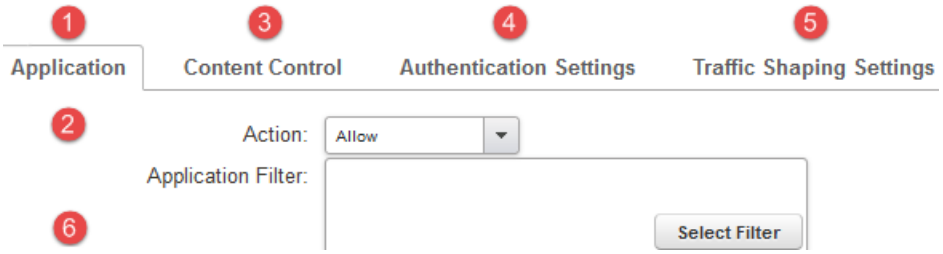


Abbildung 3.13.5 Anwendungskontrolle-Optionen und -Tabs

Inhaltskontrolle (**3**) bietet zusätzliche Filterdetails, abhängig davon, welche Anwendung (en) wir ausgewählt haben (**6**).

Wenn wir Facebook als Beispiel nehmen, gibt das nächste Bildschirmfoto einen Eindruck davon, was mithilfe von Inhaltskontrolle innerhalb von Facebook gefiltert werden kann.

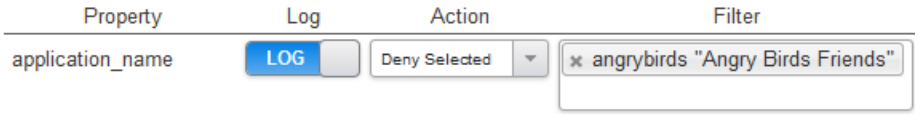


Abbildung 3.13.6 Filtern mit Inhaltskontrolle

Inhaltskontrolle gibt uns die Fähigkeit, Anwendungen innerhalb anderer Anwendungen zu kontrollieren. In diesem Beispiel werden wir keine Inhaltskontrolle benutzen, weil sie stark von den Anforderungen des Netzwerks und dem Detaillierungsgrad abhängt, in dem der Administrator Anwendungen kontrollieren will. Sie kann so einfach oder komplex eingestellt werden, wie es der Administrator möchte.

Mit den **Authentifizierung-Einstellungen** (**4**) können wir festlegen, dass die Regel nur auf bestimmte Nutzer oder Gruppen reagiert. Bei einer **Erlauben**-Regel wird dem anfragenden Client die Verbindung nur gestattet, wenn er bereits vom cOS-Core authentifiziert

wurde und einen der Nutzernamen hat oder zu einer der Gruppen gehört, die für die Regel festgelegt wurden.

Bei einer **Verweigern**-Regel wird dem anfragenden Client die Verbindung verweigert, wenn er authentifiziert ist und einen der festgelegten Nutzernamen hat oder zu einer der festgelegten Gruppen gehört. Die Authentifizierung kann durch irgendeine der Methoden durchgeführt worden sein, die in den Authentifizierung-Regel-Objekten des cOS-Cores verfügbar sind, einschließlich „Identity Awareness" (Identitätsbewusstsein). Wenn in der Regel keine Gruppen oder Nutzernamen festgelegt sind, wird die Authentifizierung ignoriert.

Im nächsten Kapitel werden wir uns eingehender mit Authentifizierung befassen.

Datenverkehrsformung-Einstellungen (**5**) - Datenverkehrsformung ist eine Funktion, mit der wir kontrollieren können, welche Bandbreite eine Gruppe von Anwendungen nutzen darf. Es kann sehr nützlich sein, die Bandbreite zwischen unterschiedlichen Anwendungen zu priorisieren und in Verbindung mit der Authentifizierung-Einstellung, auch für bestimmte Nutzer oder Nutzergruppen, die diese Anwendung verwenden.

Datenverkehrsformung ist nur anwendbar, wenn die Anwendung-Regel eine **Erlauben**-Aktion hat.

Wir werden Datenverkehrsformung im nächsten Kapitel eingehender besprechen und nutzen. Im Moment werden wir diese besondere Eigenschaft nicht aktivieren.

Anwendungen auswählen, wenn die Standardaktion „Erlauben" ist

Wenn unser Anwendung-Regelsatz erzeugt ist, müssen wir auswählen, welche Anwendungen wir erlauben oder ablehnen wollen. Weil wir in unserem aktuellen Beispiel die Standardaktion „Erlauben" nutzen, bedeutet dies, dass alles erlaubt ist, solange wir nicht ganz konkret Anwendungen zum Ablehnen hinzufügen.

Um auszuwählen, welche Anwendungen wir unserem Filter hinzufügen wollen, klicken wir den schon gezeigten Button **Filter wählen** und sehen anschließend die Filteroptionen, die im nächsten Bildschirmfoto gezeigt werden.

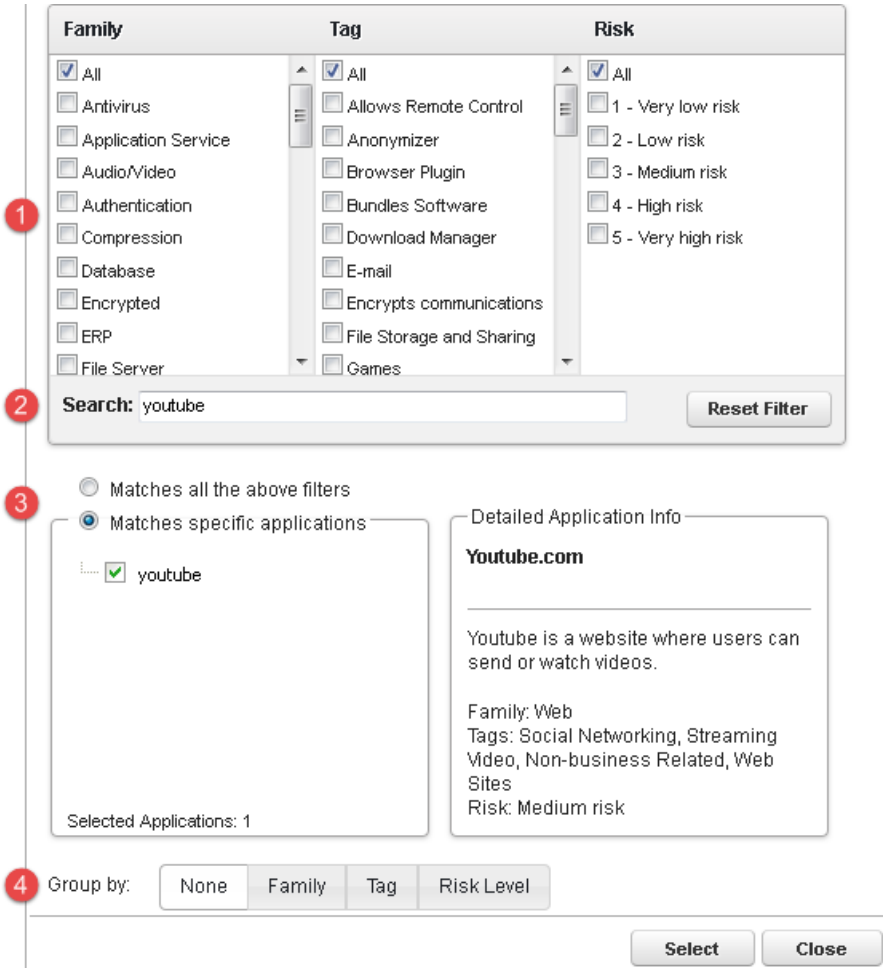


Abbildung 3.13.7 Die Anwendungsfilter-Ansicht mit Optionen

Die Anwendungssignaturen-Datenbank enthält mehr als 2.000 Signaturen, so dass es nötig ist, genauer einzugrenzen, wonach wir suchen. Um dies zu erreichen, stehen uns verschiedene Werkzeuge zur Verfügung.

Mit den ersten Optionen (**1**) können wir unsere Suche eingrenzen, oder wir wählen einfach eine bestimmte **Familie**, ein **Tag** oder **Risiko-Level**. Wenn wir wollen, können wir zum Beispiel entscheiden, die gesamte Gruppe *Sehr hohes Risiko* zu verweigern.

Mit der zweiten Option (**2**) können wir einen Text nutzen, um die Suche einzugrenzen. In unserem Beispiel haben wir ausgewählt, nach „youtube" zu suchen. This hat nur einen Treffer ergeben, der genau das ist, wonach wir suchen.

Die dritte Option (**3**) legt fest, wie legt fest, wie wir die Anwendungen wählen wollen, die zu unseren Filtern passen. Es gibt zwei Möglichkeiten:

- **Alle obigen Filter treffen zu**

  Diese Option bedeutet, dass Anwendungen auf unserer gewählten Familie, dem Tag oder der Risikogruppe basieren. Das Suchfeld ist dabei NICHT eingeschlossen. Es ist nicht möglich, anhand eines Suchtexts einen passenden Filter zu erstellen.

- **Bestimmte Anwendungen treffen zu**

  Diese Option bedeutet, dass die Zusammenfassungsansicht der Zielanwendungen sich ändert, so dass wir die Möglichkeit haben, bestimmte Anwendungen mithilfe einer Checkbox zu aktivieren/deaktivieren. Das Suchergebnis ergibt zum Beispiel drei Anwendungen und wir wollen nur eine davon nutzen. Dann können wir diese Option nutzen und die eine Anwendung auswählen, die am besten zu unseren Filtern passt, indem wir bei ihr den Haken setzen (**3**).

Die vierte und letzte Option () ermöglicht uns, die Anwendungsgruppierungen zu ändern. Standardmäßig ist keine Gruppierung gewählt, aber indem wir z.B. die Gruppierung **Risiko-Level** wählen (wie nachfolgend gezeigt), erhalten wir eine andere Art der Filteransicht, um rascher zu finden, wonach wir suchen.

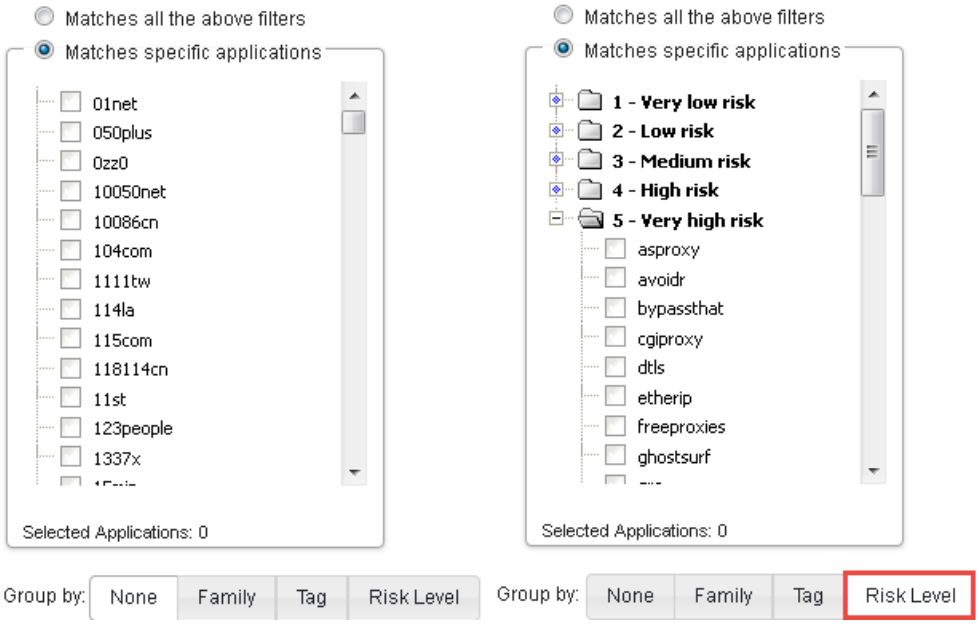


Abbildung 3.13.8 Verwendung von Risiko-Level-Gruppierung oder keiner Anwendungen-Gruppierung

Um die Beispiele einfach zu halten, haben wir uns entschieden, nur zwei Filterarten zu verweigern. Das wird im nachfolgenden WebUI-Bildschirmfoto gezeigt.

	Actio...	Application	Content Control ▲	User/Group	Forward Chain	Return Chain
1	Deny	youtube				
2	Deny	Tag='P2P File Sharing'				

Abbildung 3.13.9 Die Anwendung-Regelsatz-Filter „Standard_Erlauben"

Für unsere erste **Verweigern**-Regel haben wir die Suchfunktion genutzt, um die YouTube-Anwendung zu finden. Dann haben wir die Trefferart geändert, um die „Checkbox"-Methode freizuschalten, mit der Anwendungen ausgewählt werden können. Dadurch haben wir unsere Suche eingegrenzt, um nur eine Anwendung zu finden.

Für unsere zweite **Verweigern**-Regel nutzten wir die Standard-Trefferart, um eine bestimmte *Tag*-Gruppe zu wählen, in unserem Falle die Tag-Gruppe „Peer-to-Peer-Filesharing".

Hinweis

Es wird empfohlen, die angezeigten Anwendungen nochmal durchzusehen, wenn Sie eine Familie, ein Tag oder ein Risiko-Level gewählt haben. In unserem Beispiel haben wir entschieden, die „P2P-Filesharing"-Tag-Gruppe zu verweigern, aber diese Gruppe enthält auch Anwendungen, die wir in unserem Netzwerk vielleicht erlauben wollen, wie z.B. Spotify.

Anwendungen auswählen, wenn die Standardaktion „Verweigern" ist

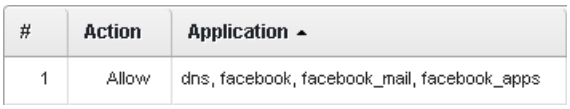
Zuvor haben wir einen Anwendung-Regelsatz genutzt, bei dem die Standardaktion **Erlauben** war. Das bedeutet, dass alle Anwendungen erlaubt werden, sofern sie nicht ausdrücklich blockiert werden. Diesmal werden wir genau das Gegenteil machen.

Abbildung 3.13.10 Den Anwendung-Regelsatz auf Verweigern einstellen

Indem wir die Standardaktion auf **Verweigern** einstellen, wie zuvor gezeigt, wird alles blockiert außer den Anwendungen, die wir zum Erlauben ausgewählt haben.

Das hat den großen Vorteil, falls es eine unbekannte Anwendung im Netzwerk gibt, die nicht durch AC identifizierbar ist, dass sie automatisch verboten wird. Es kann natürlich auch ein Nachteil sein, aber im Allgemeinen ist es das Beste, eine unbekannte Anwendung zunächst zu verweigern, bis wir wissen, was sie macht. Sobald wir das wissen, können wir sie immer noch verweigern oder in den Regeln eine Ausnahme für sie eintragen.

Als einfaches Beispiel erzeugen wir einen Regelsatz, der nur eine sehr begrenzte Anzahl an Anwendungen erlaubt, in unserem Fall nur DNS und Facebook, wie im nachfolgenden Bildschirmfoto gezeigt.



#	Action	Application ▲
1	Allow	dns, facebook, facebook_mail, facebook_apps

Abbildung 3.13.11 Die Erlauben-Liste für den Regelsatz „Standard=Verweigern"

Das heißt: wenn wir diesen Anwendung-Regelsatz benutzen, sind unsere Nutzer nur in der Lage, DNS-Namen aufzulösen und sich mit Facebook zu verbinden. Alle anderen Anwendungen würden verweigert.

Hinweis

Es kann nicht genug unterstrichen werden, wie wichtig es ist, die Unterschiede der Standardaktion zu verstehen, weil sie die Art und Weise, wie AC die verschiedenen im Netzwerk entdeckten Anwendungen behandelt, grundlegend ändert.

Den Anwendung-Regelsatz in unseren IP-Regeln verwenden

Jetzt haben wir Anwendung-Regelsätze angelegt, aber in ihrem aktuellen Zustand machen sie noch gar nichts. Anwendung-Regelsätze sind Vorlagen, die in unseren IP-Regeln verwendet werden können.

Öffnen wir zum Beispiel die IP-Regel, die wir an der WLAN-Schnittstelle für HTTP verwenden. In dieser Regel gibt es einen Abschnitt Anwendungskontrolle, wie nachfolgend gezeigt.

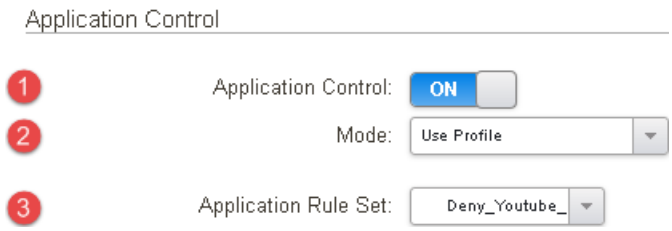


Abbildung 3.13.12 Anwendungskontrolle in einer IP-Regel aktivieren

Die erste Einstellung (**1**) kontrolliert, ob wir AC in dieser Regel überhaupt verwenden wollen. Sobald diese Option aktiviert ist, sehen wir zusätzliche Optionen wie den **Modus** (**2**) und den Anwendung-Regelsatz (**3**). Weil wir bereit einen Anwendung-Regelsatz angelegt haben, können wir denjenigen auswählen, den wir für die Anwendungskontrolle verwenden wollen.

Hinweis

Wenn wir das so auswählen, können wir einen Anwendungskontrolle-Filter direkt in dieser IP-Regel erzeugen. Der Nachteil dabei ist, dass er nur in dieser bestimmten Regel verwendet werden kann. Falls wir diesen Anwendung-Regelfiltersatz wiederbenutzen wollen, müssen wir es nochmal als Anwendung-Regelsatz-Profil anlegen.

Um uns nun die Regel-Zusammenfassung für diese besondere Regel ansehen, schauen wir uns das nachfolgende Bild an.

Abbildung 3.13.13 Regel-Zusammenfassung, wenn wir AC in einer IP-Regel aktivieren

Wie wir sehen können, gibt es jetzt Informationen im Anwendung-Feld, die besagten, dass in dieser bestimmten Regel jetzt die Anwendungskontrolle aktiviert ist.

Im vorigen Rezept haben wir das HTTP-ALG in dieser Regel so eingestellt, dass wir den Website-Zugang beschränkt haben; jetzt haben wir in ihr außerdem AC aktiviert. Also schränken wir nicht nur ein, welche Websitekategorie erlaubt ist, sondern blockieren zudem noch ganz konkret einige Anwendungen. In unserem Beispiel blockieren wir den P2P-Netzwerkzugang und die Möglichkeit, sich mit YouTube zu verbinden.

Erfolgreiche Anwendungskontrolle

Anwendungskontrolle ist ein sehr mächtiges Werkzeug, um Nutzer davon abzuhalten, eine bestimmte Anwendung, Funktion oder auch bestimmte Websites (z.B. Soziale Medien) zu nutzen.

Aber sie kann auch Probleme verursachen, wenn wir nicht aufpassen. Hier ein paar Tipps, die wir im Hinterkopf behalten sollten, wenn wir die Anwendungskontrolle zum ersten Mal konfigurieren.

Schritt 1: Nicht alles blockieren

Das mag auf den ersten Blick merkwürdig erscheinen. Bevor wir genau wissen, welche Art von Anwendungen im Netzwerk existieren und welche wir gestatten oder verbieten wollen, ist es grundsätzlich eine gute Idee, die Anwendungskontrolle so einzustellen, dass sie nur protokolliert, was im Netzwerk verwendet wird.

Um dies zu tun, können wir entweder einen Anwendung-Regelsatz erzeugen oder direkt in den entsprechenden IP-Regeln etwas einstellen. Wir werden eine **Standardaktion** nutzen, und zwar **Erlauben**. Im Signaturfilter werden wir nichts Besonderes auswählen. Stattdessen, werden wir nur die Filteroptionen öffnen und **Hinzufügen** anklicken. Das hat den Effekt, dass alle Anwendungen aus der Datenbank in dieser Regel verwendet werden. Das wird im nachfolgenden Bildschirmfoto gezeigt.

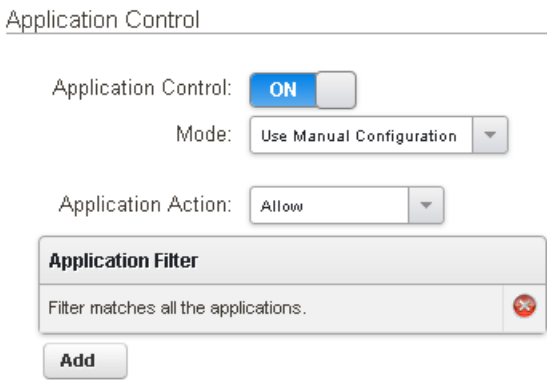


Abbildung 3.13.14 Alle verfügbaren Signaturen in einer AC-Regel verwenden

Weil wir nicht genau wissen, was im Netzwerk so abläuft, werden wir zunächst allen Datenverkehr zulassen, um zu sehen, was überhaupt verwendet wird und ob es erlaubt werden sollte oder nicht.

Hinweis

Alle Anwendungen zu verwenden, setzt den cOS-Core unter Stress, schlicht durch die schiere Anzahl an Signaturen, die er im gesamten Datenverkehr beobachten muss. Es könnte daher ratsam sein, diese Datensammelei auf jeweils nur ein bestimmtes Netzwerk zu beschränken, um den cOS-Core nicht zu überladen.

Schritt 2: Eine Liste der Anwendungen erstellen, die wir blockieren wollen

Aufgrund der Protokolle sollten wir in der Lage sein, einen ziemlich guten Überblick darüber zu bekommen, welche Art von Anwendungen im Netzwerk genutzt werden. Auf dieser Basis erstellen wir eine Liste aller Anwendungen, die unserer Meinung nach nicht im Netzwerk erlaubt werden sollten.

Schritt 3: Eine Liste der Anwendungen erstellen, die wir erlauben wollen

Erstellen Sie wie im vorigen Schritt eine Liste von Anwendungen, die Ihrer Meinung nach im Netzwerk erlaubt sein sollten.

Gedankenspiele

Abhängig von den Ereignissen müssen wir auf der Basis der folgenden Fragen einige Entscheidungen treffen:

- Wollen wir eine große Anzahl an Anwendungen blockieren?
- Oder wollen wir eine große Anzahl an Anwendungen erlauben?

Abhängig von der Antwort auf die obigen Fragen sollte entschieden werden, ob wir Anwendung-Regelsätze einsetzen sollten, die als **Standardaktion Erlauben** verwenden, oder lieber **Verweigern**.

Wenn wir nur eine sehr geringe Anzahl an Anwendungen erlauben wollen, ist es besser, als **Standardaktion Verweigern** zu verwenden, um zu vermeiden, dass wir eine große Liste von Anwendungen festlegen müssen, die verweigert werden sollen.

Falls wir nur einige wenige Anwendungen verweigern wollen, machen wir es genau andersherum und setzen die **Standardaktion** auf **Erlauben**, um dann die bestimmten Anwendungen festzulegen, die wir verweigern wollen.

Natürlich funktionieren beide Methoden, aber es ist wesentlich weniger Aufwand für den Administrator, der Situation entsprechend zu konfigurieren. Wenn wir die Aktion **Verweigern** verwenden, stellen wir damit ebenso sicher, dass irgendwelche neuen oder nicht erkannten Anwendungen im Netzwerk automatisch auch verworfen werden. Wenn wir stattdessen **Erlauben** verwenden, muss der Administrator solche Anwendungen extra zum **Verweigern** festlegen.

Das funktioniert natürlich auch andersherum. Wenn wir Erlauben nutzen, würden wir automatisch jede neue Anwendung im Netzwerk auch erlauben. Letztlich ist es eine Geschmacksfrage und von den Anforderungen abhängig, die durch den Administrator und/oder die Firmen-Richtlinie festgelegt sind.

Schritt 5: Bewertungsregel(n) erstellen

Sobald die gewünschte Methode gewählt ist, wäre es sinnvoll, eine Bewertungsregel zu erstellen, um zu prüfen, dass die eingestellten Anwendung-Regeln und -Filter tun, was wir wollen. Ein einfacher Ansatz, dies zu tun, ist, eine IP-Regel zu machen, die speziell auf einen einzigen Host anspricht, wie die, die im nächsten Bildschirmfoto gezeigt wird.

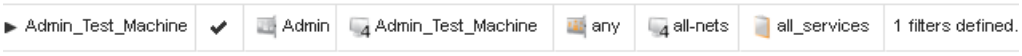


Abbildung 3.13.15 Eine IP-Regel, die nur auf eine Quell-IP reagiert

In der obigen Regel ist das Adressobjekt namens „Admin_Test_Maschine“ eine einzelne IPv4-Adresse (192.168.100.15). Daher wird diese besondere Regel nur auf einen bestimmten Host reagieren. Wenn wir dies testen, wird es keinen anderen Computer hinter der Admin-Schnittstelle stören und ist daher perfekt zum Testen und Bewerten.

Es ist außerdem wichtig, dass diese besondere Testregel im Regel-Abschnitt ganz oben in Bezug auf (in diesem Fall) das Admin-Netzwerk platziert wird. Der Grund dafür ist, dass wir wollen, dass diese Regel als erste reagiert und dass keine andere Regel unsere Tests stört. Falls zum Beispiel eine HTTP-Regel oberhalb dieser Regel platziert wäre, würden wir nicht die gewünschten Testergebnisse bekommen, wenn Anwendungen HTTP benutzen, weil dieser besondere Port und das Protokoll schon eine andere Regel angesprochen hätten.

Schritt 6: Stellen Sie zum Optimieren AC auf die richtigen Ports und/oder das richtige Protokoll ein

Ein anderer wichtiger Punkt, den Sie sich merken sollten, ist, dass Anwendungen spezielle Ports nutzen. Einige Anwendungen können dynamische Ports nutzen, aber wenn wir HTTP und FTP als Beispiel nehmen, sind diese normalerweise schon auf TCP-Ports 80 und 21 eingestellt.

Wenn wir die Anwendungen auswählen, die genutzt werden sollen, ist es daher ratsam, zu prüfen, dass die gewählten Anwendungen tatsächlich die Ports/Protokolle nutzen, die wir in unseren IP-Regeln festgelegt haben.

Ein Beispiel wäre, wenn wir in unserer FTP-Regel AC aktiviert hätten und uns dann entscheiden, Facebook zu blockieren. Das würde niemals funktionieren, weil Facebook niemals über FTP- Port 21 erreicht wird. Vermeiden Sie es, Signaturen auf Ports zu verwenden, von denen Sie wissen, dass sie niemals angesprochen werden; das erzeugt nur unnötige Last im cOS-Core, weil dadurch Signaturen bewertet werden, die niemals angesprochen werden.

Schritt 7: Endgültige Umsetzung und Aktivierung

Sobald wir damit zufrieden sind, dass unser Test-Host nur die Anwendungen erreichen und nutzen kann, die wir möchten, und dass keine Lecks vorhanden sind, können wir damit fortfahren, die Änderungen für unsere Nutzer zu veröffentlichen.

Mit „Leck" meinen wir Fehler in der Konfiguration, die bewirken könnten, dass Anwendungen, die eigentlich blockiert werden sollten, doch erlaubt werden - und anders herum.

Zusatzinformation 1: Sicherheitsüberlappungen

Bis hierher haben wir erst ein paar Sicherheitsmechanismen und -Funktionen aktiviert. Einige dieser Funktionen machen dabei etwas Ähnliches oder fast das Gleiche. Ein gutes Beispiel dafür ist, wenn wir zurückgehen und uns zunächst die vorige Grafik ansehen. *Die „Standard_Erlauben"-Anwendung-Regelsatz-Filter*.

Eine dieser von uns zum Blockieren gewählten Signaturen ist YouTube. Aber YouTube gehört genauso zu zwei Webinhalt-Filterkategorien:

- **7** - Unterhaltung.
- **Musik-Downloads.**

Und die Webinhalt-Filterregel, die wir zuvor für das WLAN-Netzwerk angelegt hatten, verweigert besonders die Kategorie „Musik-Downloads“.

Daher ist es für unsere WLAN-Schnittstelle gar nicht nötig, konkret YouTube zu blockieren, weil es bereits im Webinhalt-Filter verboten ist.

Es ist keine Katastrophe, sowohl AC als auch WCF zu nutzen, um YouTube zu blockieren; es ist mehr ein Beispiel dafür, wie Funktionen sich in manchen Situationen überlappen können. Mit der leistungsfähigen Hardware und Prozessorleistung ist die zusätzliche Arbeitslast, die durch solche Redundanzen verursacht wird, in den meisten Fällen minimal, aber wir sollten während der Konfiguration daran denken, damit das System auf mehr Tempo optimiert werden kann.

Zusatzinformation 2: Signatur-Vererbung

Die Anwendungskontrolle-Signaturen haben eine hierarchische Struktur; und es ist wichtig, sich zu merken, dass Berechtigungen ebenfalls vererbt werden. Ein Beispiel dazu ist die Signatur *http*. Wenn der Administrator die Anwendungskontrolle so einstellt, den gesamten HTTP-Datenverkehr zu blockieren, blockiert er auch alle Anwendungen, die HTTP verwenden, wie z.B. Facebook. Wenn der Administrator jedoch die Anwendungskontrolle so einstellt, dass die http-Signatur erlaubt ist, erlaubt er damit auch alle Anwendungen, die HTTP verwenden. Die Facebook-Signatur ist also ein Kind der HTTP-Signatur und wenn man HTTP-Datenverkehr erlaubt, erlaubt man damit auch Facebook-Datenverkehr. Wenn Facebook blockiert werden soll, aber HTTP soll erlaubt bleiben, muss es gesondert blockiert werden.

Zusatzinformation 3: Was, wenn Anwendung X, Y oder Z nicht in der Datenbank ist?

Es wird alles unternommen, um die Anwendungssignaturen-Datenbank so aktuell wie möglich zu halten. Es existieren allerdings tausende Anwendungen und einige sind nicht so bekannt. Es kann daher Situationen geben, in denen die Anwendungskontrolle des cOS-Cores eine bestimmte Anwendung nicht eindeutig identifizieren kann. Wenn das der Fall ist, ist Clavister auf die Mithilfe der Kundschaft angewiesen, um Kenntnis über obskure, aber möglicherweise wichtige Anwendungen zu erhalten; also wenden Sie sich mit Details an die Firma.

Rezept 3.14. Blockieren mit Zeitplänen

Ziele

Stellen Sie sich folgendes Szenario vor: Während normaler Vorlesungs- und Bürozeiten wollen wir den Nutzern und Studierenden den Zugang zu YouTube verweigern, aber nach diesen Zeiten sollen sie erreichen können, was immer sie möchten.

Der Zweck dieses Rezepts ist, Zeitpläne einzurichten, die dieses Szenario lösen, weil wir wollen, dass die Studierenden studieren und in der Klasse aufpassen, statt Videos anzuschauen.

Abbildung 3.14.1 YouTube während der Geschäftsstunden blockieren

Hinweis

Das ist selbstverständlich nur ein Beispiel. Was erlaubt oder verweigert wird, ist Entscheidungssache der Schule, Firma oder des Administrators.

Es gibt hier keine allgemeine Empfehlung, und jede Installation ist mit ihren eigenen Anforderungen einzigartig.

Detailbesprechung

Um dies zu bewerkstelligen, werden wir eine Funktion namens Zeitpläne nutzen. Wo Sie sie im WebUI finden, um Zeitpläne einzustellen, wird im nachfolgenden Bildschirmfoto gezeigt.

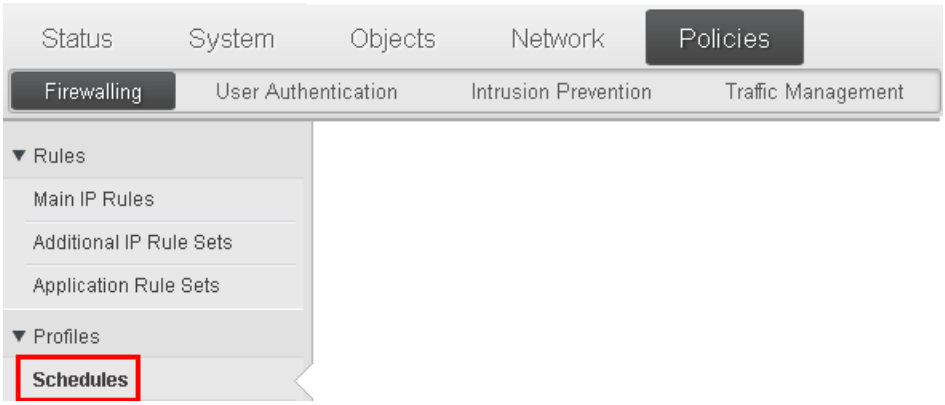


Abbildung 3.14.2 Die Position der Zeitplan-Profile im WebUI

Hinweis

Das ist nicht die einzige Stelle, an der Zeitpläne eingestellt werden können. Im nächsten Kapitel werden wir auch besprechen, wie man Zeitpläne mit Datenverkehrsformung nutzt.

Wenn wir ein Zeitplanprofil erzeugen, gibt es zwei Arten von Profil, die erzeugt werden können, wie im nachfolgenden WebUI-Bildschirmfoto gezeigt.

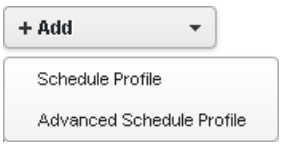


Abbildung 3.14.3 Zeitplanprofile anlegen

Das gewöhnliche **Zeitplanprofil** bietet einen Zeitplan, bei dem die folgenden Eigenschaften eingestellt werden können:

- *Nur reagieren von 07:00:00 bis 16:00:00 jeden Tag, Montag bis Freitag.*
- **Oder:** *Nur reagieren zwischen 07:00:00 und 16:00:00 jeden Tag, Montag bis Freitag, zwischen dem Datum 1. Januar 2015 und 1. Juni 2015.*

Ein **Erweitertes Zeitplanprofil** bietet erweiterte Profileigenschaften zum Einstellen, wie z.B. die folgenden Anforderungen:

- *Reagieren zwischen 07:00:00 und 16:00:00 am ersten Tag jedes Monats.*
- *Reagieren zwischen 07:00:00 und 16:00:00 am fünften Tag jedes Monats.*
- *Reagieren von 15:00:00 bis 16:00:00 am Sonntag jeder Woche.*

Ein Beispiel-Szenario

Nehmen wir die folgende Anforderung an:

Zwischen 07:00:00 und 16:00:00 jede Woche von Montag bis Freitag, Nutzer im WLAN-Netzwerk sollen weder YouTube noch P2P-Netzwerke nutzen dürfen.

Die obige Anforderung kann mit dem normalen Zeitplanprofil realisiert werden. Wir legen ein Profil an, das wie das nachfolgend gezeigte aussieht.

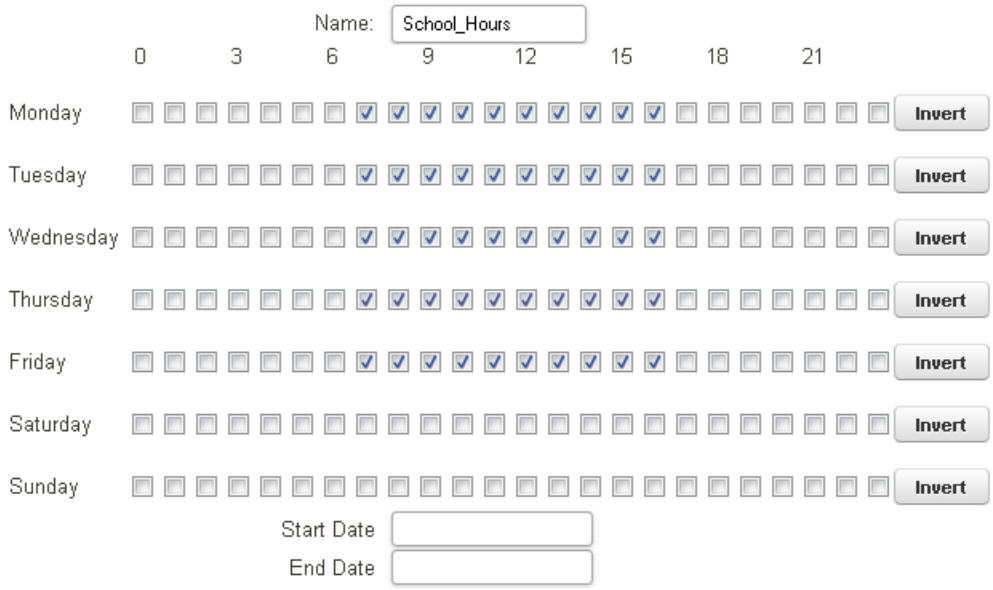


Abbildung 3.14.4 Beispiel eines normalen Zeitplanprofils

Wir haben die Felder „Start" und „Ende" absichtlich leer gelassen, weil wir wollen, dass dieser fortlaufende Zeitplan niemals abläuft.

Zeitpläne in Regeln nutzen

Da wir jetzt den Zeitplan erzeugt haben, ist es an der Zeit, ihn in unserem Regelsatz anzuwenden. In *Rezept 3.13. Anwendungskontrolle nutzen*, hatten wir zuletzt eine WLAN-IP-Regel, in der wir konkret YouTube und P2P-Anwendungen blockiert hatten.

Aber diese Regel hat keine eingestellten Zeitpläne, was bedeutet, dass diese Regel immer aktiv und die gewählten Anwendungen blockiert. Außerhalb der Schulstunden wollen wir diese Einschränkung nicht erzwingen und die Studierenden sollten in der Lage sein, möglichst alles zu bekommen, was sie wollen.

Also können wir unsere IP-Regel öffnen und das neu angelegte Zeitplanprofil in dieser Regel anwenden, wie nachfolgend gezeigt.

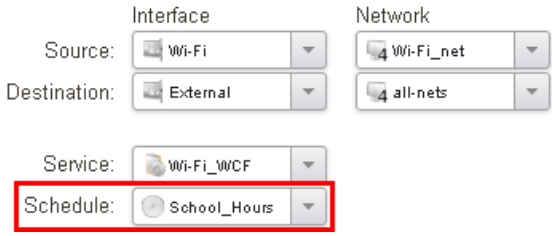


Abbildung 3.14.5 Einen Zeitplan in unserer zuvor erzeugten WLAN-IP-Regel anwenden

Das bedeutet, dass diese spezielle Regel nur noch von 07:00 und 16:00 von Montag bis Freitag anspricht.

Überprüfen Sie die IP-Regel, bevor Sie den neuen Zeitplan anwenden

Bevor Sie diese Änderungen herausgeben, lassen Sie uns den Status der IP-Regeln für die WLAN-Schnittstelle überprüfen. Unser aktueller Regelsatz sieht jetzt aus wie im nachfolgenden Bildschirmfoto gezeigt.

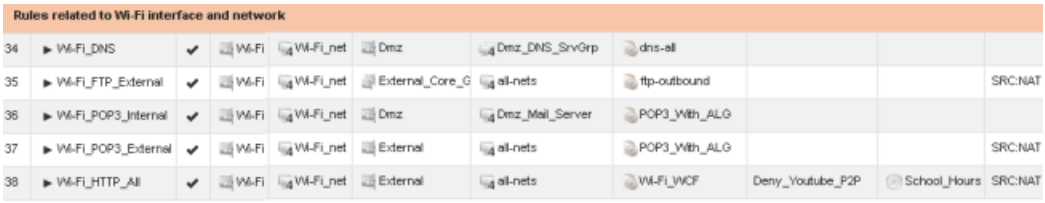


Abbildung 3.14.6 IP-Regeln mit angewendeten Zeitplänen

Wir können sehen, dass unser Zeitplan für „Schule_Stunden“ in der IP-Regel verwendet wird, die wir zuvor erzeugt hatten. Das bedeutet, dass unsere Zeitplan-Regel zwischen

07:00 und 16:00 reagieren und die gewählten Kategorien durch Webinhalt-Filter und Anwendungskontrolle blockieren wird.

Aber was passiert vor 07:00 und nach 16:00 Uhr? Welche Regel spricht dann an? Die Antwort ist: **Keine Regel wird reagieren**. Der gesamte HTTP-/HTTPS-Datenverkehr wird in dieser Zeit blockiert. An Wochenenden wird er genauso blockiert, weil die Zeitplan-IP-Regel nur von Montag bis Freitag anspricht. Um dieses Problem zu lösen, müssen wir eine andere IP-Regel erstellen, die zu allen Zeiten ansprechen sollte, die nicht von unsere Zeitplan-Regel erfasst werden.

Damit taucht die Frage auf, ob wir außerhalb der Schulstunden weniger streng in unserem WLAN-Netzwerk sein?

Das klingt sinnvoll, also erzeugen wir ein neues ALG, das weniger streng ist und nur einige der unerwünschten Kategorien blockiert, ohne dass irgendeine Anwendungskontrolle aktiviert ist (das hängt natürlich von den Anforderungen ab). Wir erzeugen anschließend eine IP-Regel, die dieses ALG und den Dienst nutzt, wie nachfolgend gezeigt.

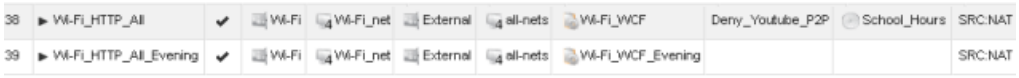


Abbildung 3.14.7 Zusätzliche IP-Regeln mit Zeitplänen erzeugen

Es ist sehr wichtig, dass die Regel an der richtigen Position platziert wird. Weil wir wollen, dass unsere Zeitplan-Regel während der darin eingestellten Zeitintervalle reagiert, MUSS es oberhalb unserer Abend-IP-Regel platziert werden.

Nur wenn unsere Zeitplan-Regel NICHT anspricht, rutschen wir tiefer, um unsere allgemeine Regel (#39) anzusprechen. Wie schon erwähnt werden IP-Regeln immer von oben nach unten im Regelsatz gelesen und interpretiert.

Rezept 3.15. Ein Lab-Netzwerk mit VLANs aufbauen

Ziele

Bisher haben wir in diesem Kapitel das Labor-Netzwerk noch nicht besonders oft erwähnt. Das kommt daher, dass es deutlich anders als unsere anderen Schnittstellen ist.

Das Konzept des Labor-Netzwerks ist, dass in diesem besonderen Netzwerk die Dozenten und Studierenden in der Lage sein sollten, mit beliebigen Netzwerk-Geräten, Programmen und Prototypen ohne Einschränkungen experimentieren zu können.

Wenn die Studierenden und Dozenten an irgendeinem Anwendungs- oder Netzwerk-bezogenen Projekt arbeiten, wollen sie nicht von irgendwelchen der Sicherheitssysteme gestört werden. Wie könnten sie bei einem Problem feststellen, ob es durch ihr Labor oder durch irgendein externes Sicherheitssystem entstanden ist?

Solch unbeschränkten Zugang zu haben, ist allerdings sehr gefährlich. Solche Netzwerke müssen so weit wie möglich isoliert und von allen anderen Netzwerken abgeschirmt bleiben.

Der Zweck dieses Rezepts ist, zu besprechen, wie wir ein Labor-Netzwerk einrichten können, das mit keinen anderen Schnittstellen und unserer Netzwerk-Sicherheit kollidiert.

Detailbesprechung

In unserer momentanen Konfiguration der Labor-Schnittstelle haben wir nur das Netzwerk 192.168.0.0/24 geroutet. Es wäre sehr chaotisch, wenn alle Studierenden und Dozenten dasselbe Labor-Netzwerk nutzen würden, weil es dann mit den Datenpaketen aller Maschinen überflutet würde. Das kann zu gegenseitigen Störungen führen und würde die Labor-Umgebung allgemein verschlechtern.

Wie also lösen wir dies? Wir haben keine weiteren physischen Schnittstelle in der Clavister-Firewall, aber wir können das Problem mithilfe eines Virtuellen LANs (VLAN) lösen!

VLAN erklärt

Das vom cOS-Core unterstützte Virtuelle LAN (VLAN) gestattet es uns, eine oder mehrere Virtuelle LAN-Schnittstellen zu definieren, die einer bestimmten physischen Schnittstelle zugewiesen sind. Diese werden als logische Schnittstellen vom cOS-Core angesehen und können wie alle anderen Schnittstellen in IP-Regelsätzen und Routingtabellen des cOS-Cores behandelt werden.

VLANs sind in diversen unterschiedlichen Szenarios nützlich. Eine typische Anwendung ist, eine Ethernet-Schnittstelle wie mehrere unterschiedliche Schnittstellen aussehen zu lassen.

Das heißt, dass die Anzahl der physischen Ethernet-Schnittstellen einer Clavister-Firewall der nächsten Generation keine Einschränkung dafür sind, wie viele total unterschiedliche externe Netzwerke verbunden werden können.

Eine andere übliche Verwendung von VLANs ist, Clients in einer Firma zu gruppieren, damit der Datenverkehr, der zu unterschiedlichen Gruppen gehört, komplett voneinander getrennt in verschiedenen VLANs gehalten wird.

Der Datenverkehr kann nur unter der Kontrolle des cOS-Cores zwischen den verschiedenen VLANs fließen und wird mithilfe der Sicherheitsrichtlinien gefiltert, die durch die Regelsätze des cOS-Cores beschrieben werden.

Das Labor-Netzwerk mit VLANs aufteilen

In unserem Labor-Netzwerk-Beispiel werden wir fünf verschiedene Labor-Netzwerke haben (sechs, wenn wir die physische Labor-Schnittstelle und das Labor-Netzwerk selbst mit hinzuzählen), von denen jedes sein eigenes VLAN und seine eigene VLAN-ID hat, wie nachfolgend in *Abbildung 3.15.1* dargestellt.

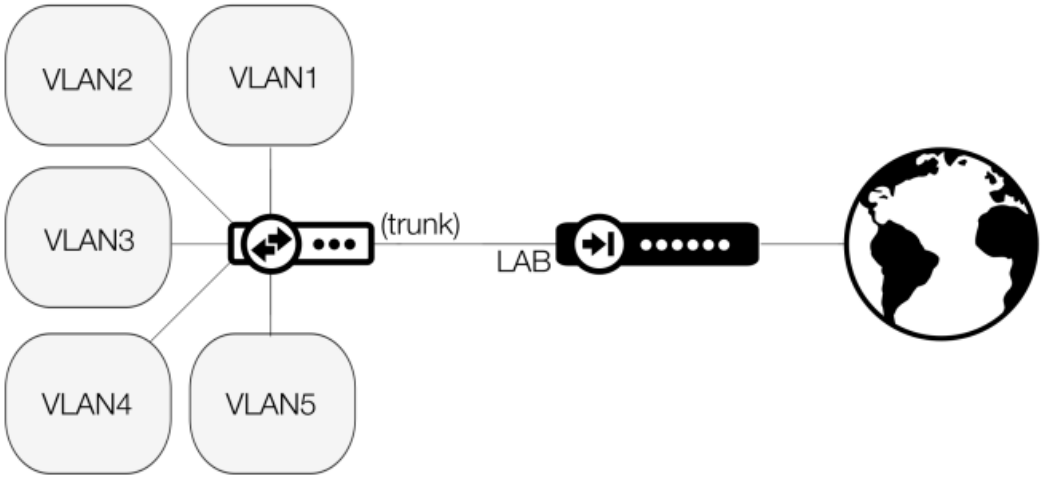


Abbildung 3.15.1 Das Labor-Netzwerk mit VLANs aufteilen

Wie nachfolgend in *Tabelle 3.15.2* aufgelistet, werden wir Netzwerke den verschiedenen VLAN-Schnittstellen und der physikalischen Stamm-Labor-Schnittstelle zuweisen (eine Stamm-Schnittstelle ist grundsätzlich eine Schnittstelle, von der mehrere VLANs abzweigen).

Schnittstellenname	VLAN-ID	Netzwerk
LABOR	Basisschnittstelle/Stamm	192.168.0.0/24
Labor_VLAN_01	1	192.168.1.0/24
Labor_VLAN_02	2	192.168.2.0/24

Schnittstellenname	VLAN-ID	Netzwerk
Labor_VLAN_03	3	192.168.3.0/24
Labor_VLAN_04	4	192.168.4.0/24
Labor_VLAN_05	5	192.168.5.0/24

Tabelle 3.15.2 Übersicht der VLAN-IDs und Netzwerke für jedes Segment des Labor-Netzwerks

Bevor wir die tatsächlichen VLAN-Schnittstellen erzeugen, rufen wir das Adressbuch auf und erzeugen alle für die neuen Schnittstellen benötigten Objekte. Wir brauchen zwei Objekte für jede Schnittstelle, eine IP-Adresse und ein Netzwerk.

Für die IP wählen wir in jedem Netzwerk die erste Adresse (192.168.1.1, 192.168.2.1, 192.168.3.1 und so weiter). Diese IP wird als Standard-Gateway für alle Labor-Geräte genutzt, die mit dem entsprechenden Netzwerk-Segment verbunden sind.

VLAN-Schnittstellen erzeugen

Um ein VLAN zu erzeugen, gehen wir im WebUI zu der Stelle, die im nachfolgenden Bildschirmfoto gezeigt wird, und wählen **Hinzuzufügen**, und dann **VLAN**.

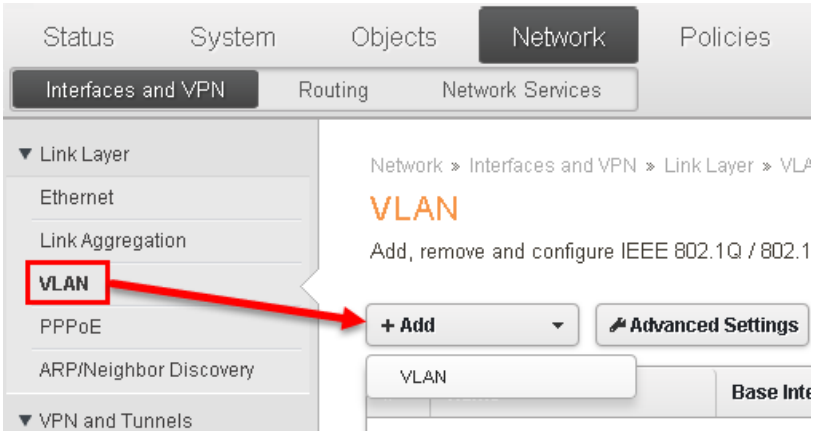


Abbildung 3.15.3 Ein VLAN anlegen

Für eine VLAN-Schnittstelle gibt es eine Vielzahl Optionen, die im nachfolgenden Bildschirmfoto gezeigt werden. Wir werden uns im Einzelnen anschauen, was jede Option macht.

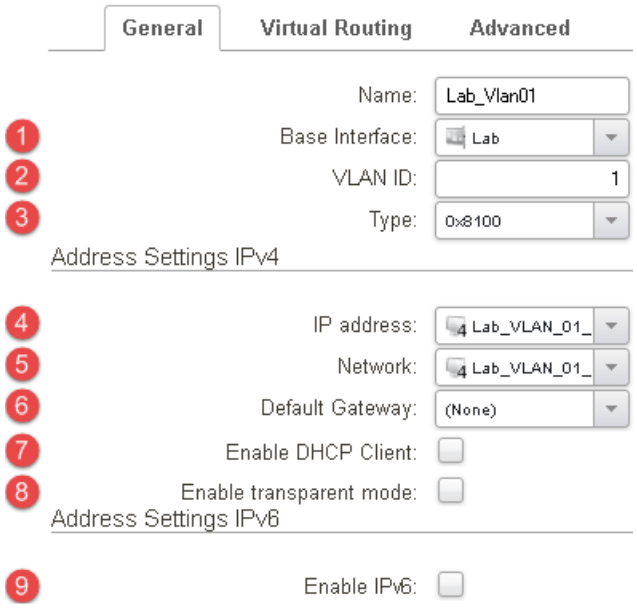


Abbildung 3.15.4 VLAN-Optionen

Die **Basisschnittstelle** (**1**) legt fest, an welcher Schnittstelle das VLAN verbunden werden soll. Wenn dieses bestimmte VLAN Datenverkehr sendet oder empfängt, wird die physische Schnittstelle LABOR genutzt.

Die **VLAN-ID** (**2**) bestimmt, welche VLAN-ID wir für diese Schnittstelle verwenden. In diesem Fall nutzen wir die VLAN-ID **1**, weil sie dem Netzwerk entspricht, das wir diesem VLAN zuweisen (192.168.1.0/24).

Der **Typ** (**3**) enthält die Möglichkeit, zu entscheiden, welcher Art das gewünschte VLAN sein soll. Ohne es zu sehr vertiefen zu wollen - es gibt grundsätzlich zwei Arten: Normales VLAN und Dienst-VLAN (QinQ).

Normales VLAN und Dienst-VLAN

Wenn wir normale VLANs konfigurieren, gibt es eine Begrenzung auf 4.096 VLANs pro physischer Schnittstelle. In einigen wirklich riesigen Netzwerken reicht dies nicht aus. In diesem Fall können wir Dienst-VLANs verwenden, was bedeutet, dass wir ein VLAN in einem anderen VLAN haben können, was wiederum die Anzahl VLANs dramatisch erhöht, die im Netzwerk eingestellt und genutzt werden können. Im Moment lassen wir den Standardtyp (0x8100), weil wir zu diesem Zeitpunkt keinen Bedarf für eine große Anzahl an

VLANs haben. Allerdings ist es eine Universität, also besteht durchaus die Chance, dass der Bedarf in Zukunft entsteht, wenn die Netzwerke wachsen.

Bei der Option **IP-Adresse** (**4**) nutzen wir das IP-Objekt, das wir zuvor im Adressbuch erzeugt hatten. Der vollständige Objektname ist tatsächlich „Labor_VLAN_01_IP", sowie „Labor_VLAN_01_Net“ für das Netzwerk (**5**). Der Name ist etwas lang, aber scheuen Sie sich nicht, lange Namen für Regeln und Objektnamen zu verwenden. Ein klar beschreibender Name kann äußerst nützlich sein.

Wir werden kein **Standard-Gateway** (**6**) verwenden, weil die Labor-Computer direkt mit einem Switch verbunden sein werden und nicht durch irgendwelche Router hindurchmüssen (im Unterschied zum cOS-Core).

Die Option **DHCP-Client** (**7**) wird ebenfalls nicht genutzt, weil wir in allen VLANs statische IP-Adressen nutzen. Auch der Transparent-Modus (**8**) wird nicht genutzt, weil wir im gesamten Universität-Netzwerk statisches Layer-3-Routing nutzen.

Wir werden zu diesem Zeitpunkt keinerlei IPv6-Adressen verwenden, also lassen wir die Option **IPv6 aktivieren** (**9**) deaktiviert.

Die letzte Option, die wir für jeden VLAN einstellen müssen, ist die HA-IP-Adresse. Weil dies ein Hochverfügbarkeitscluster ist, müssen wir die private IP-Adresse festlegen, die der Cluster für diese VLANs verwenden soll; eine Angabe in diesem Feld wird benötigt, wenn HA aktiviert ist. Diese Option wird im nachfolgenden Bildschirmfoto gezeigt.

Abbildung 3.15.5 Die private HA-IP-Adresse für die VLAN-Schnittstelle festlegen

Localhost als HA-Objekt in VLANs nutzen

Wie Sie in der vorigen Abbildung sehen können, haben wir uns entschieden, das Standardobjekt namens „localhost“ zu verwenden. Dieses Objekt besagt, dass die private IP-Adresse 127.0.0.1 ist, sowie 127.0.0.2 in allen VLANs.

Der Grund, warum wir dieses besondere Objekt nutzen, ist, weil es keinen konkreten Bedarf gibt, der privaten IP-Adresse andere IP-Adressen zu geben, weil diese IPs vorrangig vom cOS-Core genutzt werden, wenn der cOS-Core selbst versucht, irgendetwas hinter dieser Schnittstelle zu erreichen. Ein Beispiel könnte sein, wenn wir einen Protokollempfänger in diesem VLAN festgelegt haben oder wenn wir irgendwas in diesem Netzwerk von der

Kommandozeile aus anpingen. Solch ein Ping würde vom cOS-Core selbst eingeleitet und muss eine gültige Absender-IP-Adresse haben, damit es funktioniert.

Das ist allerdings kein großes Problem, weil wir beim Ping einen Unterparameter nutzen können, um zu wählen, welche IP er als Absender verwenden soll, aber darauf werden wir erst später im Detail eingehen.

Standardmäßig wird für diese VLANs in der Haupt-Routingtabelle eine Route hinzugefügt. Wenn Sie die Routingtabelle strukturieren wollen, empfehlen wir, die Option „Route automatisch hinzufügen" zu entfernen, damit sie die VLAN-Routen in einer Kommentargruppe platzieren können, was die Routingtabelle übersichtlicher macht.

Jedem VLAN-Segment zusätzliche DHCP-Server hinzufügen

Ähnlich wie bei unserer physischen Schnittstelle wollen wir auch für unsere VLANs DHCP-Server einrichten. Das wird sehr umständlich, wenn es viele Labor-Computer gibt und alle von Hand konfiguriert werden müssen, vor allem, wenn diese Nutzer-Geräte innerhalb der verschiedenen Labor-Netzwerke verschoben werden.

Um dies zu vereinfachen, werden wir jedem VLAN einen DHCP-Server hinzufügen, um die Labor-Verwaltung und den Zugang für unsere Labor-Nutzer zu erleichtern. Die DHCP-Serverliste wird im nachfolgenden Bildschirmfoto gezeigt.

# ▲	Name	Interface	Relayer Filter	IP Address Pool	Netmask	Enable logging
DHCP servers for the VLAN's						
7	DHCP_Vlan01	Lab_Vlan01	0.0.0.0/0	Lab_VLAN_01_DHCP_Pool	255.255.255.0	Yes
8	DHCP_Vlan02	Lab_Vlan02	0.0.0.0/0	Lab_VLAN_02_DHCP_Pool	255.255.255.0	Yes
9	DHCP_Vlan03	Lab_Vlan03	0.0.0.0/0	Lab_VLAN_03_DHCP_Pool	255.255.255.0	Yes
10	DHCP_Vlan04	Lab_Vlan04	0.0.0.0/0	Lab_VLAN_05_DHCP_Pool	255.255.255.0	Yes
11	DHCP_Vlan05	Lab_Vlan05	0.0.0.0/0	Lab_VLAN_05_DHCP_Pool	255.255.255.0	Yes

Abbildung 3.15.6 Zusammenfassung der in verschiedenen VLANs eingestellten DHCP-Server

Jeder Labor-VLAN-DHCP-Pool enthält etwa 150 IP-Adressen.

IP-Regeln für das Labor-Netzwerk konfigurieren

Jetzt kommen wir zum wichtigsten Teil, den IP-Regeln. Wie sollen wir den Netzwerkzugang für das Labor-Netzwerk einrichten - Soll Nutzer im Labor-Netzwerk erlaubt werden, Verbindungen zu anderen Netzwerken in der Universität zu errichten?

Die Antwort ist NEIN, wie nachfolgend in *Abbildung 3.15.7* gezeigt.

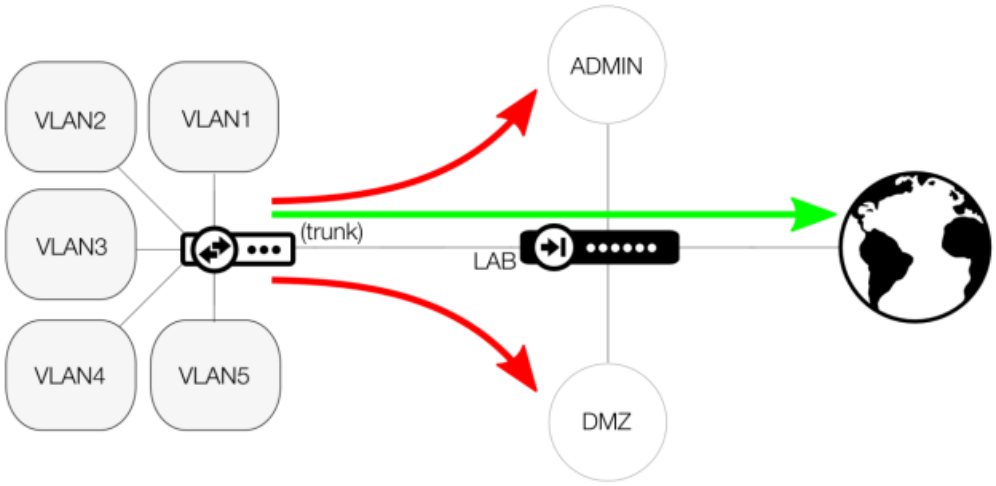


Abbildung 3.15.7 Labor-Netzwerkzugang beschränken

Wie wir schon festgelegt hatten, wird das Labor-Netzwerk ziemlich uneingeschränkt sein. Wir werden weder ALGs, Virenschutz, Webinhalt-Filter noch Anwendungskontrolle in diesem Netzwerk verwenden. Dass wir das tun, ist der Grund dafür, dass es zu Störungen in der Labor-Ausstattung und den verschiedenen Tests in diesem Netzwerk kommen kann.

Was ist mit eingehenden Verbindungen zum Labor-Netzwerk - sollten wir sie zulassen? Die Antwort ist NEIN. Wir wollen genauso wenig eingehende Verbindungen direkt ins Labor-Netzwerk von Quellen von außerhalb erlauben.

Das wiederum könnte jedoch in einigen Laboren zu Problemen führen, weil sie aus dem einen oder anderen Grund eingehende Verbindungen brauchen. Das Zulassen eingehender Verbindungen besprechen wir später. Im Moment werden wir sie in unseren IP-Regeln nicht zulassen.

Auch die Kommunikation zwischen den einzelnen Labor-Segmenten wird nicht erlaubt und wir werden sie aus Gründen voneinander getrennt halten. Möglichkeiten, dies temporär zu überschreiben, werden wir später besprechen.

Außerdem lassen wir keine Verbindungen vom Labor-Netzwerk z.B. zur DMZ zu, so dass die Labor-Netzwerk-Nutzer nicht in der Lage sind, DNS-Anfragen zu machen. Um dieses spezielle Problem zu lösen, richten wir zwei DNS-Server hinter der physischen Labor-Schnittstelle ein, die alle Nutzer im Labor-Netzwerk nutzen können.

Hinweis

Eine alternative DNS-Lösung wäre, den Labor-Nutzern zu gestatten, die DNS-Server des Internetdienstanbieters direkt anzusprechen. Dies ist kein besonders wünschenswerter Weg, um das DNS- Problem zu lösen, weil es eine hohe Wahrscheinlichkeit gibt, dass der Administrator interne Domänen- oder DNS-Namen verwendet, die mithilfe externer DNS-Server unmöglich aufgelöst werden können.

Das nachfolgende Bildschirmfoto zeigt die für die verschiedenen Labor-Netzwerke eingestellten Regeln.

Rules related to Lab interface and network								
50	▶ Lab_DNS_Server_Access	✔	Lab	Lab_DNS_Srv_Grp	Dmz	Dmz_DNS_SrvGrp	dns-all	
51	▶ Lab_All_Access_External	✔	Lab	Lab_net	External	all-nets	all_services	SRC:NAT
52	▶ Lab_Vlan1_Access_External	✔	Lab_Vlan01	Lab_VLAN_01_Net	External	all-nets	all_services	SRC:NAT
53	▶ Lab_Vlan2_Access_External	✔	Lab_Vlan02	Lab_VLAN_02_Net	External	all-nets	all_services	SRC:NAT
54	▶ Lab_Vlan3_Access_External	✔	Lab_Vlan03	Lab_VLAN_03_Net	External	all-nets	all_services	SRC:NAT
55	▶ Lab_Vlan4_Access_External	✔	Lab_Vlan04	Lab_VLAN_04_Net	External	all-nets	all_services	SRC:NAT
56	▶ Lab_Vlan5_Access_External	✔	Lab_Vlan05	Lab_VLAN_05_Net	External	all-nets	all_services	SRC:NAT

Abbildung 3.15.8 IP-Regeln-Zusammenfassung für Labor-Netzwerk-Schnittstellen

Der aktuelle IP-Regelsatz

Gestatten Sie uns noch einige Anmerkungen zu den oben gezeigten IP-Regeln.

IP-Regel **50** erlaubt den DNS-Servern im Labor-Netzwerk, mit den DNS-Servern in der DMZ zu kommunizieren. Dies gilt nur für DNS-Anfragen. Jeder andere Zugang vom Labor zur DMZ (oder irgendwelchen anderen Netzwerken/Schnittstellen, die nicht extern sind) ist verboten.

Die IP-Regeln **51** bis **56** sind alle identisch. Sie erlauben den verschiedenen Labor-Schnittstellen und -Netzwerken, mit uneingeschränktem Zugang mit dem Internet zu kommunizieren. Weil dies ja das Labor- Netzwerk ist, haben wir keinerlei Sicherheitsmechanismen aktiviert, weil dies dem Konzept widerspräche, dass wir ein

Labor- und Test-Netzwerk ohne irgendwelche Störungen in seinem Datenverkehr haben wollen.

Das kann möglicherweise ein Problem sein, aber wir werden später noch genauer darauf eingehen, wie wir die Labor-Netzwerke sogar noch weiter eingrenzen können.

Terminal-Serverzugang zum Labor-Netzwerk

Wie schon früher erwähnt, wollen wir keinerlei eingehende Verbindungen von Maschinen, die außerhalb unserer Kontrolle sind, ins Labor-Netzwerk zulassen. Was wir aber machen können, ist, „abgespeckte" Clients und Terminal-Server für jedes Labor-VLAN und -Netzwerk einzurichten. Danach können wir Nutzern an ihrer entsprechenden Schnittstelle (wie z.B. DOZENTEN oder WOHNHEIM) erlauben, die Labor-Netzwerke über diese Terminal-Server zu erreichen.

Diese Terminal-Server werden vom Administrator eingerichtet, wodurch sie besser kontrollierbar und geschützt sind, was die bestehenden Sicherheitsrisiken minimiert. Das wird nachfolgend in *Abbildung 3.15.9* dargestellt.

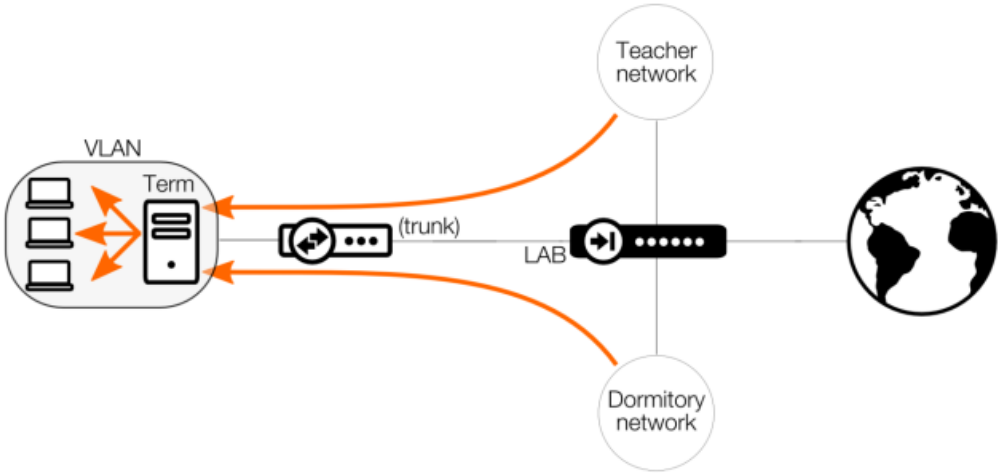


Abbildung 3.15.9 Ein Terminal-Server ermöglicht Fern-Zugang zum Labor-Netzwerk

In heutigen Netzwerkumgebungen wäre es sehr umständlich, unseren Studierenden und Dozenten nur Zugang zum Labor-Netzwerk zu gewähren, wenn sie physisch anwesend in dem entsprechenden Netzwerk sind.

Studierende müssen in der Lage sein, auch aus der Ferne von ihrem WOHNHEIM-Netzwerk aus zu arbeiten und ihre Projekte zu erreichen, und möglicherweise müssen sogar Clients an den WLAN- und DOZENTEN-Schnittstellen in der Lage sein, den Studierenden zu helfen und ihre Fortschritte zu prüfen. Die Lösung mit den abgespeckten Clients ist ein

bequemer Weg, solchen Zugang zu gewähren, ohne die gesamte Netzwerk-Sicherheit zu gefährden.

Weil diese eine Universität ist, wird ein Server pro Labor-Schnittstelle nicht ausreichen. Wenn das Netzwerk weiter wächst, wird auch der Bedarf zusätzlicher Server und weiterer Labor-Netzwerke und -Ausstattung wachsen.

Rezept 3.16. Zusätzliche Schnittstellen-IPs zuweisen

Ziele

Der Zweck dieses Rezepts ist, zu lernen, wie man mehrere IP-Adressen einer physischen (oder VLAN-)Schnittstelle zuweist. Das häufigste Szenario hierzu ist, wenn wir von unserem Internetdienstanbieter mehrere öffentliche IP-Adressen angefragt und erhalten haben und diese alle der externen Schnittstelle zuweisen wollen.

Der häufigste Grund hierfür ist, wenn eine Organisation eine Vielzahl oder verschiedene Server hat, die denselben Zielport nutzen werden. Weil wir denselben Port nicht mehrmals in Richtung derselben IP nutzen können, brauchen wir zusätzliche IP-Adressen, so dass wir die Portnummer wiederverwenden können. Dies gilt beispielsweise für die HTTP- und HTTPS-Ports, 80 und 443.

Detailbesprechung

Als Beispiel werden wir die EXTERN-Schnittstelle unserer Clavister-Firewall der nächsten Generation nutzen. Im Moment hat sie nur eine zugewiesene öffentliche IP-Adresse, die 203.0.113.10 lautet. Jetzt wollen wir die öffentlichen IP-Adressen von 203.0.113.11 bis 203.0.113.15 der EXTERN-Schnittstelle zuweisen, wie nachfolgend in *Abbildung 3.16.1* gezeigt.

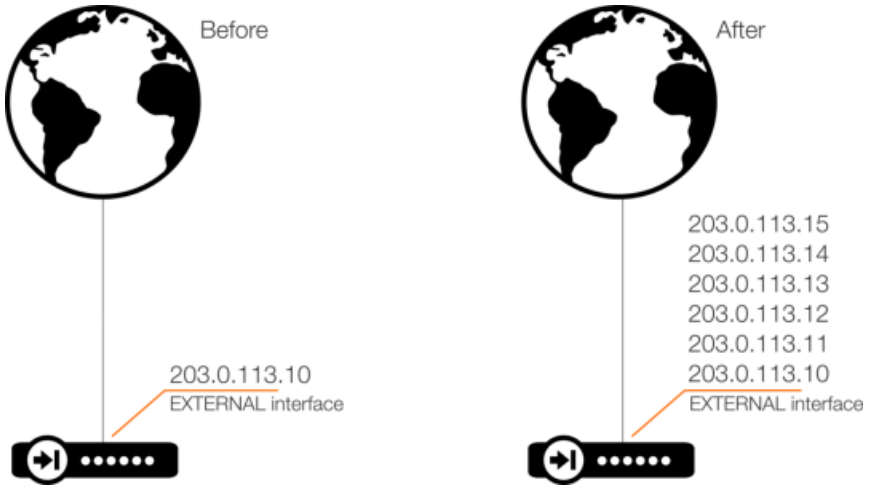


Abbildung 3.16.1 Mehrere IP-Adressen zuweisen

Zusätzliche Netzwerk-Objekte erzeugen

Um alles ordentlich zu machen, erzeugen wir zuerst zusätzliche Netzwerk-Objekte für die neuen IP-Adressen, wie nachfolgend gezeigt.

Networks related to internet and the external interface		
1	External_Gateway	203.0.113.1
2	External_ip_10	203.0.113.10
3	External_ip_11	203.0.113.11
4	External_ip_12	203.0.113.12
5	External_ip_13	203.0.113.13
6	External_ip_14	203.0.113.14
7	External_ip_15	203.0.113.15
8	External_net	203.0.113.0/24

Abbildung 3.16.2 Zusätzliche Adressbuch-Objekte für IPs

Es ist sehr wahrscheinlich, dass diese Objekte in verschiedenen IP-Regeln und anderen Funktionen genutzt werden, so dass es dringend empfohlen wird, Adressbuch-Objekte zu erzeugen und zu nutzen.

Zwei Methoden, um einer Schnittstelle zusätzliche IP-Adressen hinzuzufügen

Es gibt zwei Wege, um einer Schnittstelle zusätzliche IP-Adressen hinzuzufügen. Das kann etwas irritierend sein, weil keine dieser Methoden die IPs direkt in der Schnittstelle konfiguriert.

Methode 1 – ARP Publish

Die erste Methode nutzt eine Eigenschaft, die „ARP/Neighbor Discovery" (Nachbar entdecken) genannt wird. Im WebUI finden Sie diese Eigenschaft unter **Netzwerk > Schnittstellen > Link-Ebene**, wie nachfolgend gezeigt.

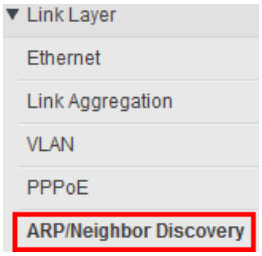


Abbildung 3.16.3 ARP/Neighbor Discovery verwenden

Hinweis

In diesem Stadium werden wir nicht weiter vertiefen, was genau ARP ist. Mehr Informationen über ARP finden Sie am Ende dieses Rezepts.

Wenn wir einen neuen ARP-Eintrag erzeugen, werden uns eine Menge Optionen geboten, wie nachfolgend gezeigt. Schauen wir uns die verschiedenen Optionen an.

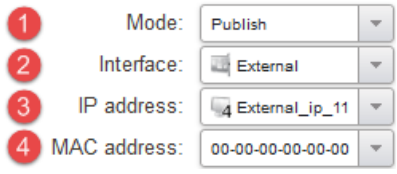


Abbildung 3.16.4 ARP-Optionen

Standardmäßig ist ein **Modus** (**1**) namens „Publish“ (Veröffentlichen) gewählt. Dieser Modus wird in 99 % aller Fälle gewählt. Mehr Informationen über die anderen Modi finden Sie am Ende dieses Rezepts.

Die Option „Publish“ bedeutet, dass wir dem cOS-Core mitteilen, dass er auf ARP-Anfragen an der gewählten Schnittstelle (**2**) und für die gewählte IP-Adresse (**3**) antworten soll. Das heißt, wenn eine externe Quelle (normalerweise der Router des Internetdienstanbieters) fragt, wem diese IP-Adresse gehört, antwortet der cOS-Core: „Diese IP-Adresse gehört mir, und meine MAC-Adresse (**4**) ist diese.“

Wenn im Feld **MAC-Adresse** der Standardwert *00-00-00-00-00-00* (**4**) steht, benutzt der cOS-Core die MAC-Adresse der gewählten Schnittstelle (**2**).

ARP Publish zu nutzen, ist die üblichste Entscheidung, wann man mehrere IP-Adressen der gleichen Schnittstelle zugewiesen hat, weil es kein Problem macht, die gleiche MAC-Adresse mit den Adressen zu assoziieren.

Methode 2 – Proxy ARP

Die zweite Methode, um mehrere IP-Adressen einer einzelnen Schnittstelle hinzuzufügen, wird „Proxy ARP“ genannt. Diese Methode wird im WebUI unter **Netzwerk > Routing** eingestellt.

Um einen Proxy-ARP-Eintrag zu erzeugen, erzeugen wir eine neue *Core*-Route, wie im nächsten Bildschirmfoto gezeigt.

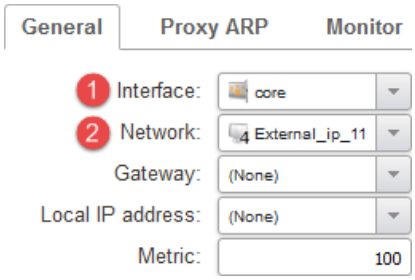


Abbildung 3.16.5 Eine Core-Route hinzufügen

Als Schnittstelle (**1**) müssen wir „Core“ wählen. Das nächste ist die IP-Adresse, die wir dem cOS-Core zuweisen wollen, also nehmen wir unsere ausgesuchte IP-Adresse (**2**). Mehr Einzelheiten über die Core-Schnittstelle finden Sie in *Rezept 2.5. DMZ einstellen und Zugang zu einem internen Webserver erlauben*.

Hinweis

Wir könnten natürlich alle unsere IP-Adressen in einer einzigen Route gruppieren, statt eine Route pro IP zu haben, aber um alles einfach und geradlinig zu halten, erzeugen wir in diesem Beispiel mehrere Routen. Das macht auch die Routingtabelle leichter lesbar und verständlicher.

Grundsätzlich können wir die Route so interpretieren: „*Weise IP-Adresse 203.0.113.11 der Core-Schnittstelle zu*".

Aber was passiert, wenn wir statt des Cores die externe Schnittstelle auswählen? Wenn wir dann die Route lesen, wird sie so interpretiert: „*Um 203.0.113.11 zu erreichen, nutze die Schnittstelle EXTERN*".

Das Verhalten würde also ziemlich unterschiedlich sein, abhängig davon, ob wir die Core-Schnittstelle nutzen oder nicht. Aber einfach nur die Core-Schnittstelle zu wählen, reicht nicht aus. Bisher haben wir nur dem cOS-Core mitgeteilt, dass er eine andere IP-Adresse hat, aber nicht, ob er für diese IP-Adresse an irgendeiner Schnittstelle auf ARP antworten soll.

Dafür müssen wir den Proxy-ARP-Tab aufrufen, der im nachfolgenden Bildschirmfoto gezeigt wird.

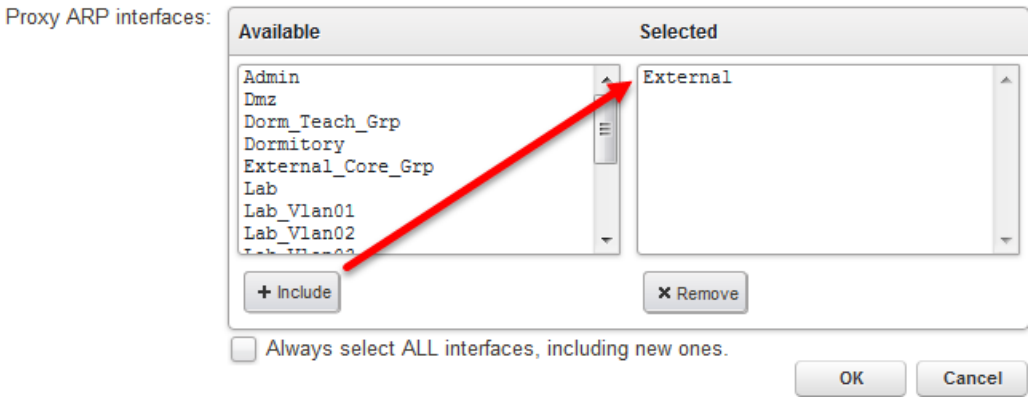


Abbildung 3.16.6 Proxy ARP einstellen

Hier wählen wir einfach die Schnittstelle(n), für die wir möchten, dass der cOS-Core auf ARP antwortet. In diesem Beispiel ist es nur eine Schnittstelle: EXTERN.

Jetzt ist alles eingestellt. Wenn ARP-Anfragen an der EXTERN-Schnittstelle ankommen und nach unserer gewählten IP fragen, wird der cOS-Core antworten und sagen, dass diese IP dem cOS-Core gehört. Nachdem wir alle unsere neuen Core-Routen hinzugefügt haben, sehen die Routen für die externe Schnittstelle jetzt aus wie in der nachfolgenden Liste.

#	Type	Interface	Network	Gateway
Routes related to the External/internet interface.				
1	Route IPv4	External	External_net	
2	Route IPv4	External	all-nets	External_Gateway
3	Route IPv4	core	External_ip_11	
4	Route IPv4	core	External_ip_12	
5	Route IPv4	core	External_ip_13	
6	Route IPv4	core	External_ip_14	
7	Route IPv4	core	External_ip_15	

Abbildung 3.16.7 Externe Routen

Welche Methode ist die beste?

Beide Methoden funktionieren, wenn wir einfach wollen, dass der cOS-Core für eine IP-Adresse auf ARP antwortet. Allerdings haben beide ihre Stärken und Schwächen.

Vorteile von ARP Publish: Zeigt deutlich an, was es macht. Bietet mehr benutzerdefinierbare Optionen, was MAC-Adresse und statische ARP-Möglichkeiten angeht.

Nachteile von ARP Publish: Kann nur für eine IP-Adresse gleichzeitig verwendet werden. Keine Möglichkeit, Core-Routen zu erzeugen. IP-Regeln müssen anders als für eine Schnittstellen-IP-Adresse konfiguriert werden.

Vorteile von Proxy ARP: Kann für ein ganzes Netzwerk genutzt werden. Kann mehrere Schnittstellen gleichzeitig wählen. Die Konfiguration der IP-Regel ist genauso wie für eine physische Schnittstelle.

Nachteile von Proxy ARP: XPublish kann nicht verwendet werden. Keine Möglichkeit, statische ARP-Einträge zu erzeugen. Nicht sehr übersichtlich.

Unterschiede beim Erzeugen von Regeln zwischen ARP Publish und Proxy ARP

Welche Methode wir wählen, hat ebenso Einfluss darauf, wie IP-Regeln eingestellt werden müssen. Wenn wir damit beginnen, eine physische Schnittstellen-IP-Adresse für eine eingehende SAT- und Erlauben-Regel zu nutzen, könnte sie wie im nachfolgenden Regelsatz aussehen.

Name	L...	Src If	Src Net	Dest If	Dest Net	Service
▶ SAT_Example	✔	External	all-nets	core	External_ip_10	http
▶ Allow_Example	✔	External	all-nets	core	External_ip_10	http

Abbildung 3.16.8 Beispiel von Schnittstelle-SAT und Erlauben-Regel

Wenn wir nun den gleichen Regelsatz anwenden, aber mit einer ARP-Publish-IP aus Methode 1, sieht der Regelsatz eher wie folgt aus.

Name	L...	Src If	Src Net	Dest If	Dest Net	Service
▶ SAT_Example	✔	External	all-nets	External	External_ip_11	http
▶ Allow_Example	✔	External	all-nets	External	External_ip_11	http

Abbildung 3.16.9 SAT + Erlauben-Regel mit ARP-Publish-IP als Ziel

Wir Sie sehen können, ist die Ziel-Schnittstelle nicht länger der Core, sondern die EXTERN-Schnittstelle. Das kann verwirren, weil der cOS-Core nach wie vor auf eingehende ARP-Anfragen in Richtung dieser IP antworten wird. Im Grunde ist ARP Publish eine veraltete cOS-Core-Eigenschaft, die schon lange Zeit existiert. Der Bedarf, ganze Netzwerke mit ARP Publish zu nutzen, führte dazu, dass im cOS-Core Proxy ARP implementiert wurde. Außerdem wurde es so möglich, die IP-Adresse über Proxy ARP der Core-Schnittstelle selbst zuzuweisen, so dass sie sich mehr wie eine Schnittstellen-IP-Adresse verhält.

Wenn wir das obige Regel-Beispiel auf eine vom Core geroutete Proxy-ARP-IP-Adresse anwenden, sieht das wie folgt aus.

Name	L...	Src If	Src Net	Dest If	Dest Net	Service
▶ SAT_Example	✔	External	all-nets	core	External_ip_11	http
▶ Allow_Example	✔	External	all-nets	core	External_ip_11	http

Abbildung 3.16.10 SAT + Erlauben-Regel mit Core-gerouteter Proxy-ARP-IP

Wie wir sehen können, gibt es keinen Unterschied zwischen dem obigen und dem ursprünglichen Regelsatz von SAT und Erlauben-Regeln. Das ist einer der Vorteile, wenn wir Core-Routen und Proxy ARP nutzen. Wenn die IP-Regeln erzeugt werden, werden sie genauso eingestellt wie die anderer Schnittstellen.

Optional: Wie findet man heraus, ob eine IP vom Core geroutet ist oder nicht

Manchmal kann es verwirrend sein, zu verstehen, wie die Regeln definiert werden sollten, wenn es um die Quell- oder Ziel-Schnittstelle geht. „Irgendwas" als Schnittstelle zu nutzen, ist natürlich eine Lösung, aber je weiter wir die Regeln einschränken, um bestimmte Schnittstellen zu nutzen, desto besser sollten wir das Netzwerk abgrenzen, damit es umso sicherer wird.

Wenn wir Regeln einsetzen, die auf mehreren Schnittstellen und/oder Netzwerken ansprechen, könnte das dazu führen, dass gegen unsere Netzwerk-Sicherheit verstoßen wird.

Eine leichte Methode, um herauszufinden, wo eine IP-Adresse geroutet wird, ist, die Kommandozeile des cOS-Cores zu nutzen. Rufen Sie die Kommandozeile auf und geben Sie folgenden Befehl ein:

```
Gerät:/> routes –lookup=<ip>
```

Die Ausgabe nach diesem Befehl könnte etwa so aussehen wir nachfolgend gezeigt:

```
Gerät:/> routes -lookup=8.8.8.8 Looking up 8.8.8.8 in routing
table „main":

 Matching route: 0.0.0.0/0
 Routing table : main
 Send via iface: EXTERN
 Gateway       : 203.0.113.1

 Proxy ARP on  :
 Local IP      : (use iface IP in ARP queries)
 Metric        : 100
 Flags         :
```

Schauen wir uns den Wert für „Send via iface" im obigen Beispiel an: es ist die „EXTERN"-Schnittstelle, also ist dies die Schnittstelle, die wir in unserer Regel verwenden müssen.

Optional: Informationen über ARP

Das „Address Resolution Protocol“ (ARP, Adressauflösungsprotokoll) gestattet es uns, eine Netzwerkebene- Protokoll- Adresse (OSI- Ebene 3) an eine Datenlinkebene- Hardwareadresse (OSI-Ebene 2) umzumappen. In Datennetzwerken wird das verwendet, um eine IPv4-Adresse in ihre zugehörige Ethernet-Adresse aufzulösen. ARP arbeitet in der OSI-Ebene 2 (Datenlink-Ebene) und wird für die Übertragung mit Ethernet-Headerdaten umschlossen.

Ein Host in einem Ethernet-Netzwerk kann mit einem anderen Host nur kommunizieren, wenn er die Ethernet-Adresse (MAC-Adresse) dieses Hosts kennt. Protokolle höherer Ebenen wie IP verwenden IP-Adressen, die sich grundsätzlich von den Hardware-Adressierungsschemata niedrigerer Ebenen, wie z.B. der MAC-Adresse, unterscheiden. ARP wird verwendet, um mithilfe der IP-Adresse eines Hosts seine Ethernet-MAC-Adresse abzurufen.

Wenn ein Host eine IPv4-Adresse auflösen muss, um die entsprechende Ethernet-Adresse zu erhalten, sendet er ein ARP-Anfrage-Datenpaket. Das ARP-Anfrage-Datenpaket enthält die MAC-Adresse der Quelle, die IPv4-Adresse der Quelle und die Ziel-IPv4-Adresse. Jeder Host im lokalen Netzwerk empfängt dieses Datenpaket. Der Host mit der angegebenen Zieladresse sendet dann ein ARP- Antwort- Datenpaket mit seiner MAC- Adresse an den ursprünglichen Host zurück.

Optional: Weitere ARP-Modi, wenn ARP Publish verwendet wird

Als wir Methode 1, ARP Publish, beschrieben haben, hatten wir den Publish-Modus verwendet, aber es gibt noch einige andere Einstellungen, die je nach Szenario von Interesse sein könnten. Diese Modi werden nachfolgend gezeigt.

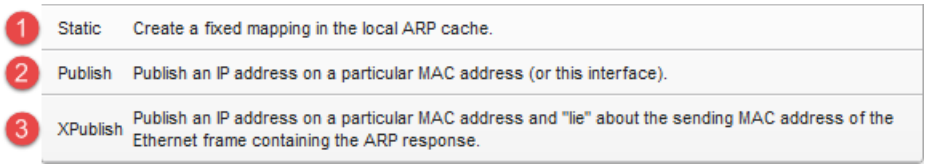


Abbildung 3.16.11 Die verschiedenen ARP-Modi

Statisch-Modus

Ein statisches ARP-Objekt fügt im ARP-Cache des cOS-Cores eine Transformation ein, die eine festgelegte IP-Adresse mit der MAC-Adresse der zugehörigen Ethernet-Schnittstelle verbindet. Dieser Modus dient nicht dazu, die Adresse für externe Geräte zu ver-

öffentlichen, sondern dazu, dem cOS-Core selbst mitzuteilen, wie er externe Geräte erreichen kann.

Ein statischer ARP-Eintrag teilt dem cOS-Core mit, dass eine bestimmte IP-Adresse an einer festgelegten Schnittstelle mithilfe einer bestimmten MAC-Adresse erreicht werden kann. Das heißt, wenn der cOS-Core mit der Adresse kommunizieren will, prüft er die statischen Einträge der ARP-Tabelle und kann so feststellen, dass sie über eine bestimmte MAC-Adresse an einer bestimmten Schnittstelle erreicht werden kann.

Meistens werden statische ARP-Objekte in Situationen verwendet, in denen irgendein externes Netzwerk-Gerät nicht korrekt auf ARP-Anfragen antwortet und eine falsche MAC-Adresse meldet. Einige Netzwerk-Geräte, wie z.B. WLAN-Modems, können diese Probleme haben. Auch kann man damit für verbesserte Sicherheit eine IP-Adresse für eine bestimmte MAC-Adresse festsetzen, oder um eine DDoS-Attacke zu verhindern, falls es nicht autorisierte Nutzer in einem Netzwerk gibt.

Solch ein Schutz bezieht sich jedoch nur auf Datenpakete, die an diese IP-Adresse gesendet werden. Er trifft nicht auf Datenpakete zu, die von dieser IP-Adresse aus gesendet werden.

Publish- und XPublish-Modi

Mit den Modi Publish und XPublish erzeugt das ARP-Objekt eine Verbindung zwischen einer IP-Adresse und einer MAC-Adresse, um sie an der Schnittstelle für externe Geräte zu veröffentlichen. Wenn die MAC-Adresse nicht festgelegt ist, wir die MAC-Adresse der zugehörigen Ethernet-Schnittstelle benutzt.

Um den Unterschied zwischen Publish und XPublish zu verstehen, ist es nötig, zu verstehen, dass es zwei MAC-Adressen im mit der ARP-Antwort gesendeten Ethernet-Rahmen gibt, wenn der cOS-Core auf eine ARP-Anfrage antwortet. Diese beiden Adressen werden in der nachfolgenden *Abbildung 3.16.12* gezeigt.

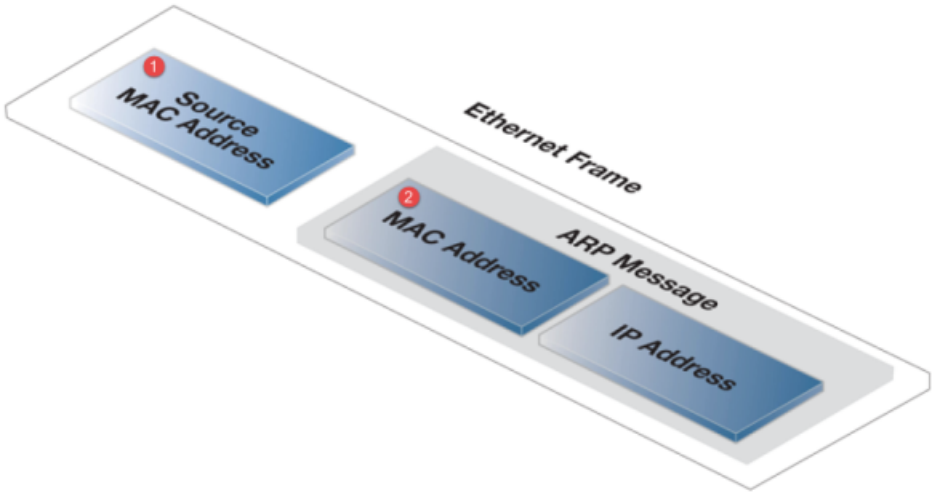


Abbildung 3.16.12 Der Ethernet-Rahmen einer ARP-Antwort

Die beiden in *Abbildung 3.16.12* dargestellten MAC-Adressen sind die folgenden:

1. Die MAC-Adresse im Ethernet-Rahmen der Ethernet-Schnittstelle, die die Antwort sendet.

2. Die MAC-Adresse in der ARP-Antwort, die mit in diesem Rahmen enthalten ist. Das ist normalerweise dieselbe wie **1**, Die Quell-MAC-Adresse im Ethernet-Rahmen, muss aber nicht so sein.

Die Option Publish nutzt die reale MAC-Adresse der sendenden Schnittstelle als Adresse (**1**) im Ethernet-Rahmen.

In seltenen Fällen erfordern einige Netzwerk-Komponenten, dass beide MAC-Adressen in der Antwort (**1** und **2**) identisch sind. In diesem Fall wird XPublish verwendet, weil es beide MAC-Adressen in der Antwort so abändert, dass sie der veröffentlichten MAC-Adresse entsprechen. Mit anderen Worten: XPublish „lügt“ über die Quelladresse der ARP-Antwort.

Wenn eine veröffentlichte MAC-Adresse dieselbe ist wie die MAC-Adresse der physischen Schnittstelle, spielt es keine Rolle, ob Publish oder XPublish gewählt wurde; das Ergebnis ist identisch.

Rezept 3.17. Öffentliche IPs geschützten Hosts zuweisen

Ziele

Der Zweck dieses Rezepts ist, öffentliche IP-Adressen verschiedenen Computern zuzuweisen, die sich im Labor-Netzwerk der Universität befinden. Wir werden Routing verwenden, um dem cOS-Core mitzuteilen, wo er die öffentlichen IP-Adressen findet und wie der cOS-Core sich verhalten soll, wenn Hosts mit der Welt außerhalb unseres Netzwerks kommunizieren wollen.

Detailbesprechung

Dieses Rezept geht im Detail auf einer Ebene für Fortgeschrittene auf das Standardverhalten von Netzwerk und ARP ein. Daher empfehlen wir, dass Sie zuvor *Rezept 3.16. Zusätzliche Schnittstellen-IPs zuweisen* gelesen und verstanden haben, bevor Sie fortfahren.

Es kommt sehr häufig vor, dass der Administrator eine öffentliche IP-Adresse direkt einem Gerät hinter der Clavister-Firewall zuweisen möchte. In unserem Beispiel-Szenario wollen wir jedem Host-Computer in unserem Labor-Netzwerk eine öffentliche IP-Adresse zuweisen. Das ergibt insgesamt fünf IP-Adressen, wie nachfolgend in *Abbildung 3.17.1* dargestellt.

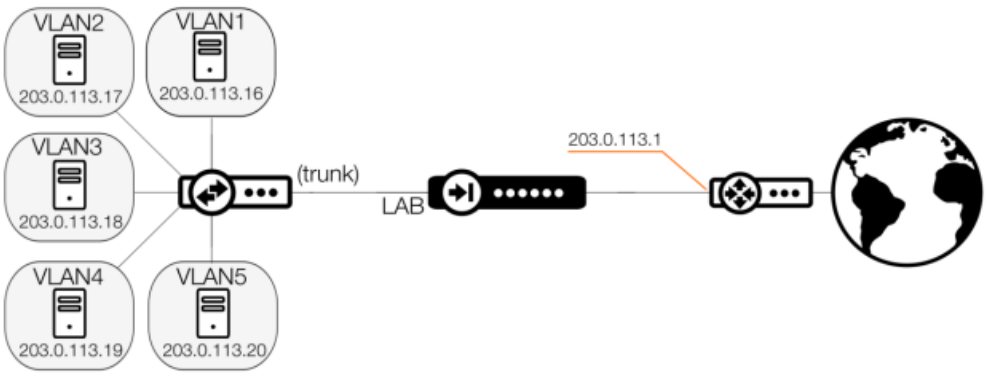


Abbildung 3.17.1 Öffentliche IPs den Labor-VLANs zuweisen

Wir lösen dies mithilfe von Routing, weil wir jetzt diese Adressen nicht einer cOS-Core-Schnittstelle zuweisen wollen, wie wir es zuvor gemacht haben.

Wir rufen die Routingtabelle *main* auf und erzeugen eine neue Route mit dem im nächsten Bildschirmfoto gezeigten Parameter.

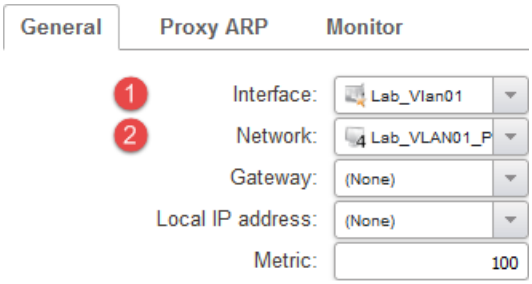


Abbildung 3.17.2 Eine Route für eine öffentliche IP in Richtung eines Labor-VLANs

Als Schnittstelle der Route (**1**) wählen wir die Schnittstelle, hinter der der Ziel-Host sich befindet. Bevor wir diese Route erzeugen, müssen wir bereits ein Objekt im Adressbuch für eine der öffentlichen IP-Adressen angelegt haben, das wir als unser Netzwerk (2) für unsere Route verwenden werden. In diesem Beispiel hat das erzeugte Objekt die IP-Adresse 213.0.113.16.

Diese neu angelegte Route bedeutet: *„Um 213.0.113.16 zu finden, sende eine ARP-Anfrage direkt an die Lab_Vlan01-Schnittstelle."*

Der Grund für dieses Verhalten liegt darin, dass wir keinerlei Standard-Gateway eingerichtet haben, was bedeutet, dass wir nicht durch einen Router müssen, um das Ziel-Netzwerk oder die Ziel-IP zu erreichen.

Dazu kommt eine wichtige Frage auf: Was ist die Quell-IP einer solchen ARP-Anfrage, die vom cOS-Core gesendet wird?

Lokale IPs mit verschiedenen Netzwerken hinter derselben Schnittstelle nutzen

Wenn der cOS-Core eine ARP-Anfrage aussendet, um 213.0.113.16 zu finden, nutzt er die Schnittstellenadresse als Absender. In unserem Beispiel ist das die Schnittstellenadresse, die wir für die Schnittstelle namens „Lab_Vlan01" festgelegt hatten, die 192.168.1.1 lautet.

Das heißt, dass das Zielgerät eine ARP-Anfrage von einer Quell-IP empfängt, die kein Mitglied seines eigenen zugewiesenen IP-Bereichs (213.0.113.xx) ist. Das Zielgerät wird in den meisten Fällen (je nachdem, wie die Netzmaske eingestellt ist), die Anfrage ignorieren und verwerfen. Solange dieses Problem weiter besteht, ist keine Kommunikation zwischen dem cOS-Core und dem Zielgerät möglich.

Wenn wir versuchen, eine öffentliche IP als Gateway-Adresse an unserem Host-Computer einzustellen, die nicht zum eigenen IP-Bereich des Hosts gehört, haben wir ein Problem.

Microsoft Windows beispielsweise wird eine Warnmeldung generieren, wenn wir so etwas versuchen, wie im nachfolgenden Bildschirmfoto gezeigt.

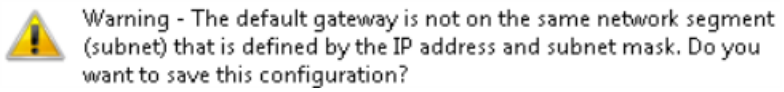


Abbildung 3.17.3 Gateway-Adresswarnung in Windows 7

Um dies zu lösen, müssen wir die Eigenschaft „Lokale IP" unserer neu erzeugten cOS-Core-Route einstellen, wie nachfolgend gezeigt.

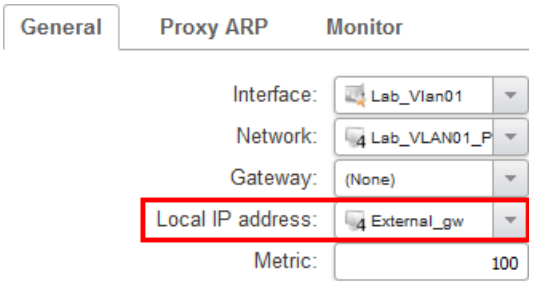


Abbildung 3.17.4 Lokale IP in einer Route einstellen

Die Einstellung „Lokale IP" erfüllt zwei wichtige Aufgaben:

- Die als Lokale IP konfigurierte IP-Adresse wird als Quell-IP für ARP-Anfragen verwendet, die vom cOS-Core gesendet werden.
- Der cOS-Core antwortet auf ARP in Richtung der eingestellten IP-Adresse an der Ziel-Schnittstelle.

Wenn dem Host-Computer die IP-Adresse 213.0.113.16 zugewiesen wurde, ist es vernünftig, dass er ein Gateway benutzt, das sich im gleichen Netzwerk-Segment befindet wie z.B. die Routeradresse 213.0.113.1 des Internetdienstanbieters.

Weitere Erläuterungen der Lokalen IP

Lassen Sie uns folgende Frage stellen: *„Wenn der cOS-Core auf die ARP-Anfrage für die IP 213.0.113.1 antwortet, erzeugt das keinen IP-Konflikt mit dem Router des Internetdienstanbieters?"*„.

Die Antwort ist: Nein, wird es nicht. Der Grund, warum das kein Problem ist, liegt darin, dass das Einstellen der „Lokalen IP“ nur heißt, dass der cOS-Core auf ARP-Nachrichten an der benannten Schnittstelle antwortet. Der Router des Internetdienstanbieters liegt hinter der „EXTERN"-Schnittstelle und ist nicht Lab_Vlan01.

Wir „lügen“ über den Standort der IP-Adresse, so dass die Maschine mit der öffentlichen IP denkt, sie spricht direkt mit dem Router des Internetdienstanbieters, während sie in Wirklichkeit mit dem cOS-Core spricht.

Die Notwendigkeit von Proxy ARP

Der Hauptzweck dieses Rezepts ist, einem Computer hinter der Firewall eine öffentliche IP-Adresse zuzuweisen. Damit das funktioniert, müssen wir jedoch auch beachten, wie der Router des Internetdienstanbieters sich verhält.

In den meisten Fällen hat der Router des Internetdienstanbieters (ISP) eine Route, die auf den Port oder die Schnittstelle zeigt, hinter denen sich die Firewall befindet. Das bedeutet, dass der ISP-Router ARP-Anfragen durchführt, um irgendwelche Hosts im benannten Netzwerk-Segment zu finden.

Ein Blick auf das vorige Bild, in dem die Route konfiguriert wurde (*Abbildung 3.17.4*), zeigt uns, dass wir die öffentliche IP auf die Lab_Vlan01-Schnittstelle geroutet haben.

Wenn der SIP eine ARP-Anfrage in Richtung dieser IP (213.0.113.16) sendet, wird sie an der EXTERN-Schnittstelle empfangen, nicht aber vom VLAN. Weil der Ziel-Host, dem die IP-Adresse gehört, sich hinter dem VLAN und nicht hinter der EXTERN-Schnittstelle befindet, wird der Host nicht antworten und die Kommunikation wird fehlschlagen.

Um dieses Problem zu lösen, müssen wir in unserer Route den Proxy-ARP-Tab aufrufen und die EXTERN-Schnittstelle als eine Schnittstelle hinzufügen, auf der wir per Proxy ARP das Netzwerk erreichen. Das wird im nächsten Bildschirmfoto gezeigt.

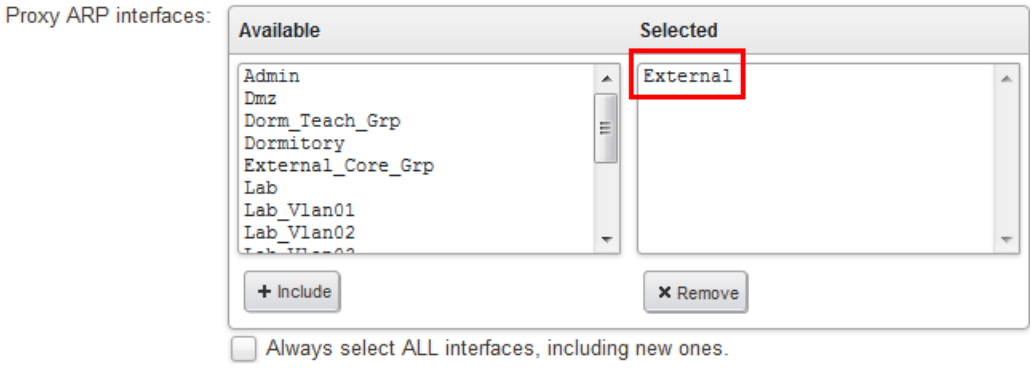


Abbildung 3.17.5 Proxy ARP an der EXTERN-Schnittstelle einstellen

Jetzt wird der cOS-Core auf ARP-Anfragen antworten, die vom ISP-Router gesendet wurden, und anschließend alle Datenpaket-Anfragen entsprechend der konfigurierten Routen weiterleiten.

IP-Regeln einstellen

IP-Regeln für die Kommunikation von/zu einer öffentlichen IP-Adresse zu erzeugen, die so eingestellt wurde, ist leichter, weil wir in keiner Richtung Adressübersetzung benötigen.

Hinweis

Weil dies ein Labor-Netzwerk in der Universität ist, können die Regeln äußerst großzügig sein. Intern eine öffentliche IP zu nutzen, würde normalerweise nicht erlaubt, außer unter besonderen Umständen. Ein derart exponierter Host mit einer öffentlichen IP ist ein vorrangiges Ziel für Hacker.

Daher sollte besondere Sorgfalt darauf verwendet werden, dass dieser Host niemals irgendwelche anderen Ressourcen in geschützten Netzwerken erreichen kann. Daher sollte er einen lokalen Virenschutz-Scanner haben und die lokale Firewall-Software sollte richtig konfiguriert und aktuell sein.

Ein Beispiel, wie die IP-Regeln eingestellt sind, wird nachfolgend gezeigt.

Rules related to the public IP addresses routed on each Lab VLAN segment							
63	▶ Incoming_Lab_Vlan1_Public	✔	External	all-nets	Lab_Vlan01	Lab_VLAN01_Pub	all_services
64	▶ Outgoing_Lab_Vlan1_Public	✔	Lab_Vlan01	Lab_VLAN01_Pub	External	all-nets	all_services

Abbildung 3.17.6 IP-Regeln einer öffentlichen IP-Adresse im Labor-Netzwerk

Optional: Datenverkehr-Flussbeschreibung

Um besser beschreiben zu können, was dieses Rezept erreicht hat, schauen wir auf das nachfolgende nächste Diagramm.

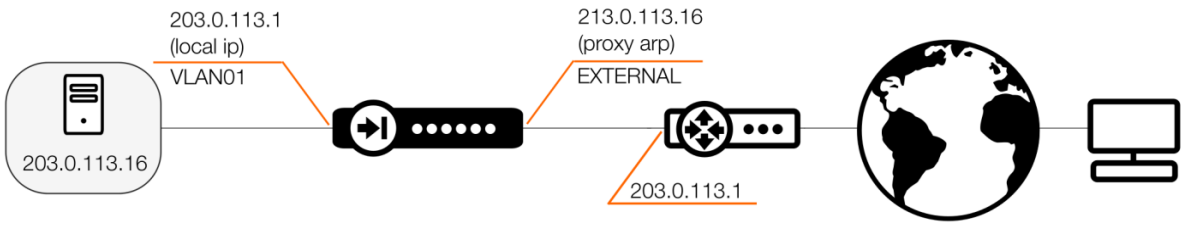


Abbildung 3.17.7 IP-Regeln einer öffentlichen IP-Adresse im Labor-Netzwerk

Die auftretenden Wechselwirkungen in der oben gezeigten *Abbildung 3.17.7* sind wie folgt:

1. Ein Client im Internet möchte sich mit dem internen Server an 213.0.113.16 verbinden.
2. Die Verbindungsanfrage kommt beim ISP-Router (IP 203.0.113.1) an, der eine ARP-Anfrage durchführt, um die IP-Adresse 213.0.113.16 zu finden.
3. Der cOS-Core empfängt die ARP-Anfrage (von IP 203.0.113.1) und antwortet dem ISP-Router, indem er ihm mitteilt „Mir gehört die IP 213.0.113.16".
4. Der ISP-Router weiß, wo sich die IP-Adresse befindet, und fängt an, eine Verbindung in Richtung der Ziel-IP aufzubauen.
5. Der cOS-Core versucht nun, den Besitzer der IP-Adresse 213.0.113.16 zu finden, von der er weiß, dass sie sich hinter der Lab_Vlan01-Schnittstelle befindet. Er macht dies, indem er eine ARP-Anfrage mit der Quell-IP 213.0.113.1 als Absender sendet.

6. Der interne Server mit der IP 213.0.113.16 hinter der Lab_Vlan01-Schnittstelle wird erkennen, dass die ARP-Anfrage von einem Host in seinem eigenen Netzwerk-Segment kommt, und wird auf die ARP-Anfrage antworten.

Der einleitende Teil der Kommunikation zwischen dem Client und dem Server ist jetzt vollständig, so dass die Verbindungen und Datenpakete zwischen den beiden Hosts zu fließen beginnen können.

Rezept 3.18. Bandbreiten-Verwaltung

Ziele

Der Zweck dieses Rezepts ist, bei den meisten Universitätsnetzwerken eine Bandbreiten-Begrenzung zu implementieren. Die Absicht dabei ist, eine Situation zu vermeiden, in der einigen wenigen Nutzern die gesamte verfügbare Bandbreite im Universitätsnetzwerk zugeteilt wird.

Wir werden Datenverkehrsformung nutzen, um anhand der Schnittstelle und des Netzwerks eine maximale Bandweitenbeschränkung einzurichten. Ein Beispiel dessen, was wir dazu machen wollen, wird in der nachfolgenden *Abbildung 3.18.1* gezeigt.

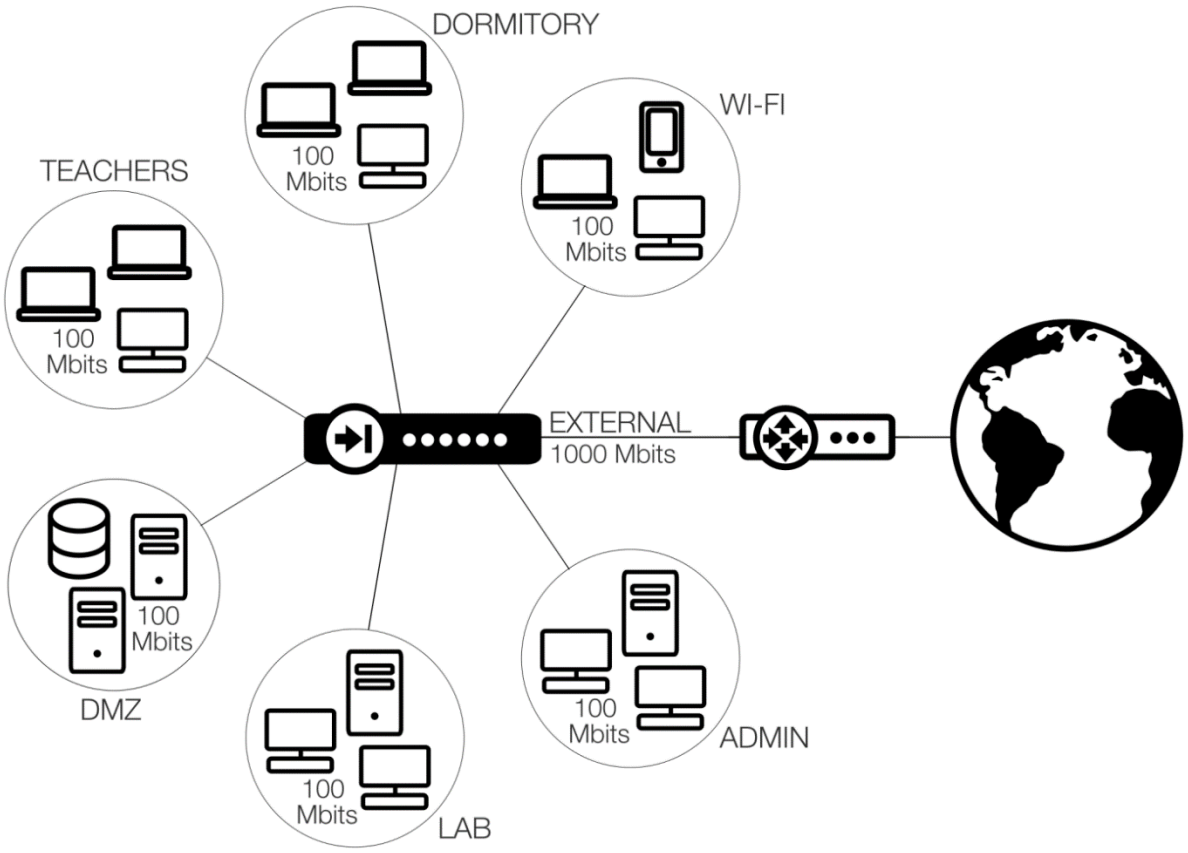


Abbildung 3.18.1 Bandweitenbeschränkungen für Schnittstellen und Netzwerke einstellen

Detailbesprechung

Der Hauptzweck der Verwendung von Datenverkehrsformung (auch Datenverkehrverwaltung, Piping oder Piping-Regeln genannt) ist, Einschränkungen in unserem Universitätsnetzwerk zu verhängen. In unserem Universitätsbeispiel haben wie eine Glasfaser- Internetverbindung mit 1.000 Megabits (Mbits). Indem wir an jedem Schnittstellensegment eine Begrenzung von 100 MBits einstellen, vermeiden wir eine Situation, in der eine einzelne Schnittstelle in der Lage wäre, die gesamte verfügbare Bandbreite zu verbrauchen.

Gerade bei den Schnittstellen LABOR und WOHNHEIM ist dies besonders wichtig, weil schon eine Handvoll Studierende mit Peer-to-Peer-Filesharing leicht große Teile der Bandbreite verbrauchen könnten. Das könnte in der Folge zu Datenpaketverlusten und generellen Netzwerkstörungen führen.

Um das Eingangsszenario einfach zu gestalten, wollen wir per Einschränkung festlegen, dass jede unserer Schnittstellen maximal in der Lage sein soll, mit einer Gesamtgeschwindigkeit von 100 Mbits pro Sekunde zu senden und zu empfangen. Das heißt, dass alle Nutzer hinter einer bestimmten Schnittstelle gezwungen werden, sich eine 100-Mbit-Verbindung zu teilen.

Hinweis

In diesem Beispiel nutzen wir eine ISP-Verbindung mit einer Bandbreite von 1.000 Mbits. In einem realen Netzwerk sind jedoch die 1.000 Mbits wahrscheinlich niemals zu 100 % verfügbar. Aus diesem Grund empfehlen wir, immer einen Fehlerbereich von etwa fünf bis acht Prozent von der insgesamt verfügbaren Bandbreite abzuziehen, wenn Sie die Datenverkehrverwaltung konfigurieren.

Statt also anzunehmen, die insgesamt verfügbare Bandbreite sei 1.000 Mbits, wäre es besser, anzunehmen, sie liege bei etwa 930 Mbits. Der Grund dafür ist, dass der cOS-Core sich so verhält, als ob die eingestellte gesamte Bandbreite immer verfügbar wäre. Wenn der ISP dies aber nicht tatsächlich zur Verfügung stellt, könnte das zu Datenpaketverlusten führen, weil der cOS-Core versucht, Bandbreite zuzuteilen, die tatsächlich vielleicht gar nicht zur Verfügung steht.

Bandbreite-Piping für jede Schnittstelle erzeugen

Um die Bandbreite-Begrenzung zu realisieren, müssen wir zuerst mindestens zwei neue „Pipes" anlegen. Eine *Pipe* ist ein cOS-Core-Konfigurationsobjekt, das benutzt wird, um Datenverkehrsformung zu definieren. Ein cOS-Core-Objekt namens *Piping-Regel* bestimmt dann, welcher Datenverkehr durch welche Pipes geleitet wird.

Datenverkehrsformung wird im WebUI unter **Richtlinien und Datenverkehrverwaltung** eingestellt, wie im nächsten Bildschirmfoto gezeigt.

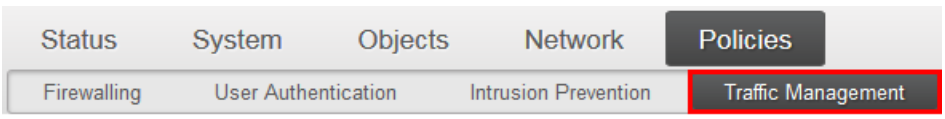


Abbildung 3.18.2 Datenverkehrverwaltung im WebUI

Im Abschnitt „Datenverkehrsformung“ können wir zwei Arten von Datenverkehrsformung-Objekten anlegen, Piping-Regeln und Pipes, wie nachfolgend gezeigt.

Abbildung 3.18.3 Datenverkehrsformung-Objekttypen

Wenn wir das erste Pipe-Objekt erzeugen, wird uns der Allgemein-Tab gezeigt, wie nachfolgend gezeigt.

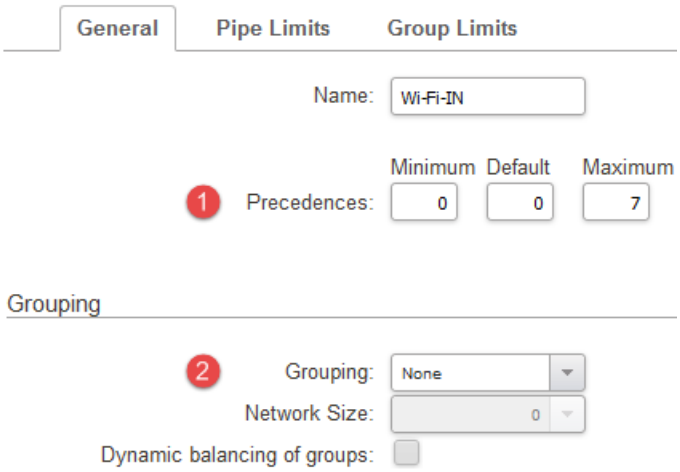


Abbildung 3.18.4 Allgemein-Tab für Datenverkehrsformung-Pipes

All Datenpakete, die durch die Datenverkehrsformung-Pipes des cOS-Cores geleitet werden, haben **Vorrang** (**1**). In diesem Rezept wird der Standardwert für Vorrang nicht geändert, so dass alle Datenpakete den Standard-Vorrang haben, der bei Null liegt.

Es gibt acht Vorränge, die von 0 bis 7 durchnummeriert sind. Vorrang 0 ist der unwichtigste Vorrang (niedrigste Priorität) und 7 ist der wichtigste Vorrang (höchste Priorität).

In einem späteren Kapitel werden wir uns im Detail mit Vorrang beschäftigen. Im Moment lassen wir ihn beim Standardwert.

Der cOS-Core bietet eine weitere Kontrollebene innerhalb von Pipes, weil er in der Lage ist, die Pipe-Bandbreite zwischen Nutzern in einer **Gruppierung** aufzuteilen (**2**) und jedem Nutzer ein Datenverkehr-Limit und eine -Garantie zu geben. Wir werden uns später in diesem Rezept eingehender mit Gruppierungen beschäftigen. In diesem Beispiel werden wir sie nicht konfigurieren und auf dem Standardwert *<keine>* belassen.

Piping-Grenzen

Wechseln wir nun zum Piping-Grenzen-Tab, der nachfolgend gezeigt wird.

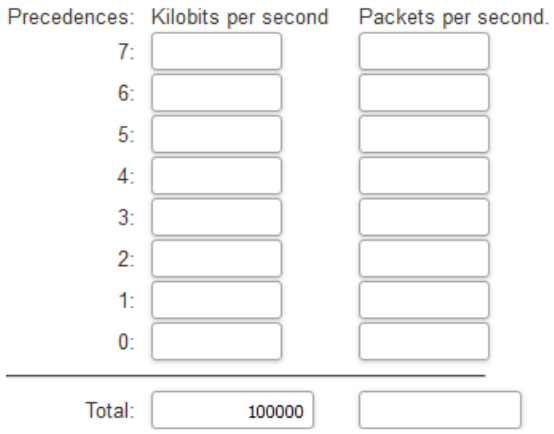


Abbildung 3.18.5 Der Piping-Grenzen-Tab

In diesem Tab stellen wir ein, welche Art Begrenzung wir für unsere momentan gewählte Pipe festlegen wollen. Wie zuvor gezeigt, haben wir in keinem Feld irgendwelche Werte eingetragen, außer dem Gesamtwert für die Begrenzung **Kilobits pro Sekunde**.

Wie schon am Anfang dieses Rezepts in unserem anfänglichen Netzwerk-Schema gezeigt, war der Plan, jeder Schnittstelle eine einfach Bandbreitenbegrenzung auf 100 Mbits zu geben. Dafür haben wir die maximale Piping-Grenze auf einen Wert von *100.000* (100 Mbits) für diese Pipe gesetzt.

Zwei Pipes werden benötigt, eine für jede Richtung

Ein beliebter Fehler in Bezug auf Pipes ist, zu vergessen, dass Datenpaket in zwei Richtungen fließen (was häufig auch *bidirektionale Kommunikation* genannt wird). Das bedeutet, wenn wir nur eine Pipe erzeugen und diese in unseren Piping-Regeln sowohl für eingehende als auch für ausgehende Datenpakete verwenden, wird sie geteilt. Das wiederum heißt im schlimmsten Fall, dass wir nur 50 Mbits für den Datenverkehrsfluss statt der beabsichtigten 100 Mbits haben.

Daher erzeugen wir zwei Pipes, eine für die eingehenden und eine weitere für die ausgehenden Datenpakete, wie im nächsten Bildschirmfoto gezeigt.

#	Name	Grouping	Network size	Total bandwidth limit	Total packet per second limit
Pipes for the Wi-Fi interface					
1	Wi-Fi-IN	None		100000	
2	Wi-Fi-Out	None		100000	

Abbildung 3.18.6 Die zwei Pipes für die WLAN-Schnittstelle, eine für jede Richtung

Hinweis

Bei Bandbreite sind „Kilo" und „Mega" Vielfache von 1.000, nicht von 1.024. Das heißt, ein eingestellter Wert von 1.000 Kilobits pro Sekunde für eine Pipe entspricht 1 Mbit.

Eine Piping-Regel anlegen

Bevor wir unsere soeben neu angelegten Pipes verwenden können, müssen wir zunächst die allgemeinen Eigenschaften in einer Piping-Regel anlegen und einstellen, wie nachfolgend gezeigt.

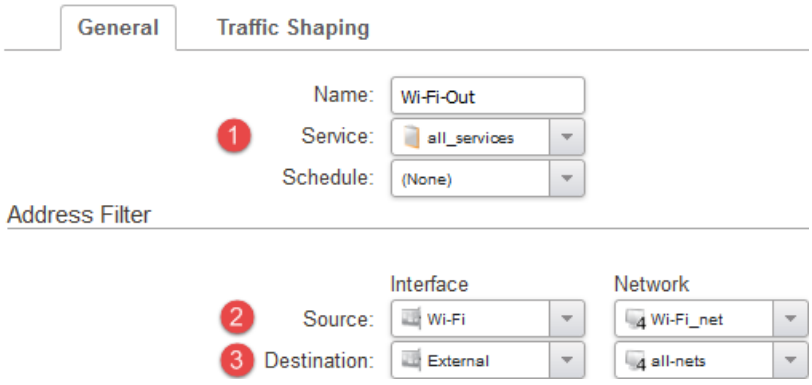


Abbildung 3.18.7 Die allgemeinen Eigenschaften einer Piping-Regel

Bei Pipes haben wir die Möglichkeit, eine Pipe für spezielle Dienste (**1**) wie z.B. HTTP, DNS oder ICMP zu machen. Etwa dann, wenn wir die Bandbreiteverwaltung sehr detailliert

machen wollen. Um das Beispiel überschaubar zu halten, werden wir unsere Datenverkehrsformung auf alle verfügbaren Dienste (alle Ports und Protokolle) anwenden.

Indem wir Einschränkungen für Quelle (**2**) und Ziel (**3**) in Schnittstelle und Netzwerk verwenden, sagen wir dem cOS-Core, dass wir unsere Pipes für Datenverkehr verwenden wollen, der von der WLAN-Schnittstelle und dem Netzwerk in Richtung der EXTERN-Schnittstelle (zum Internet) eingeleitet wird.

Anders gesagt: Wenn WLAN-Nutzer im Internet surfen wollen, wenden wir eine Pipe-Begrenzung auf die maximale Bandbreite an, die Nutzer hinter dem WLAN nutzen können, wenn sie Daten hoch- oder herunterladen.

Das ist auch der Grund, warum das Zielnetzwerk auf alle-netze eingestellt ist. Wir wissen nicht, mit welchem der zahllosen Server im Internet der Nutzer sich verbinden will.

Pipes in einer Piping-Regel verwenden

Jetzt ist es an der Zeit, unsere soeben erzeugte Pipe in unserer Piping-Regel zu verwenden. Dazu gehen wir zum Datenverkehrsformung-Tab, der im nächsten WebUI-Bildschirmfoto gezeigt wird.

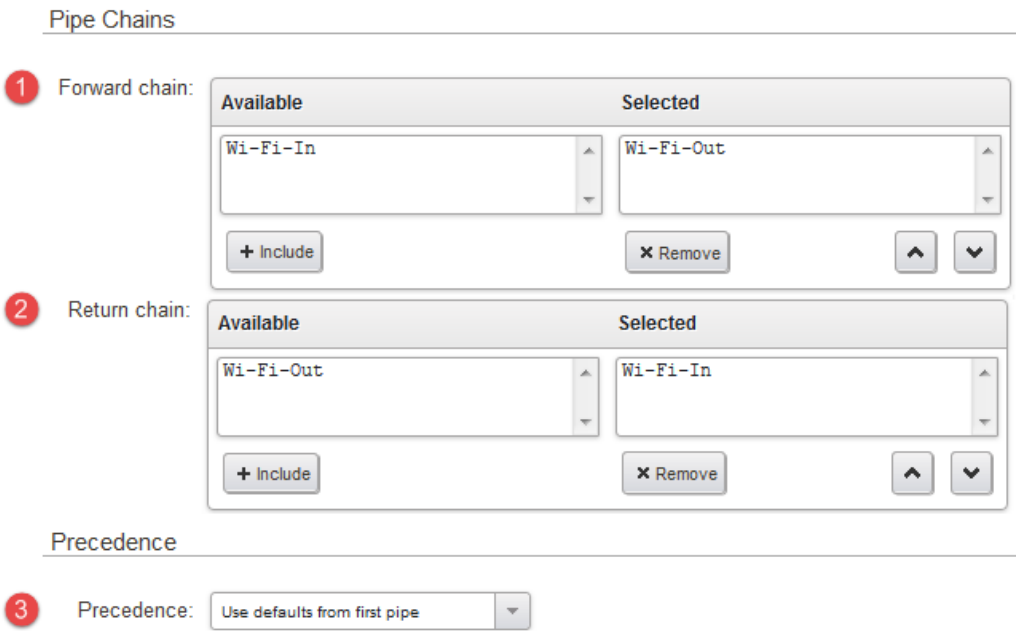


Abbildung 3.18.8 Die Piping-Regel für Datenverkehr, der hinter der WLAN-Schnittstelle initiiert wird

Hier spielt die Datenverkehr-Fließrichtung eine wichtige Rolle. Um auszuwählen, welche Pipe für die Richtung vorwärts (**1**) oder rückwärts(2) verwendet werden soll, müssen wir

uns erst darüber im Klaren sein, mit welcher Art von Datenverkehr wir es zu tun haben und in welche Richtung er fließen wird.

Zum Glück ist unser Beispiel sehr einfach, so dass es, selbst wenn wir aus Versehen die falsche Pipe wählen, immer noch funktionieren würde, weil beide Pipes dieselbe Größe haben. Dennoch ist es wichtig, dass wir uns über die Datenverkehr-Fließrichtung im Klaren sind.

Die nachfolgende Abbildung 3.18.9 hilft, den Datenverkehrsfluss und die Verwendung der Pipes für beide Richtungen besser zu verstehen.

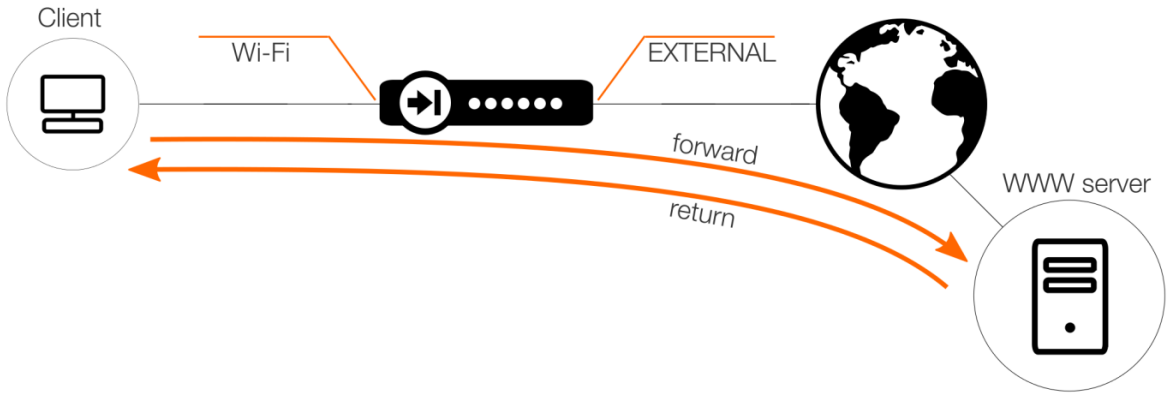


Abbildung 3.18.9 Vorwärts- oder Rückwärts-Ketten abhängig von der Verbindungsaufnahme verwenden

Die Vorrang-Einstellung (**3**) wird verwendet, wenn wir die Vorrang-Levels überschreiben wollen, die für Pipes festgelegt wurden. Diese Einstellung wird hauptsächlich genutzt, wenn in den Pipes verschiedene Vorrang-Levels in Verbindung mit Pipingketten verwendet werden. Ein Beispiel dafür wäre, wenn wir einer einzelnen IP höheren Vorrang vor allen anderen Nutzern im Netzwerk geben wollen, ohne zusätzliche Pipes zu erzeugen. In diesem Kapitel verwenden wir diese Einstellung nicht.

Wann mehrere Piping-Regeln benötigt werden

In unserem ersten Beispiel haben wir nur eine Piping-Regel erzeugt, und diese Regel behandelt den Datenverkehr, der von der WLAN-Schnittstelle in Richtung Internet fließt. Normalerweise würden wir zwei Piping-Regeln erzeugen, wobei die zweite Piping-Regel für Datenverkehr genutzt wird, der in der anderen Richtung fließt (Datenverkehr aus dem Internet in Richtung des WLAN-Netzwerks).

Der Grund dafür, warum wir keine zweite Piping-Regel erzeugt haben, ist, dass unser Universitätsnetzwerk es nicht erfordert, IP-Regeln zu erzeugen, die Datenverkehr vom Internet ausgehend ins WLAN-Netzwerk zulassen. Daher haben wir keinen Anlass, eine Piping-Regel für eingehenden Datenverkehr zu erzeugen, weil diese niemals angesprochen würde. Wenn Datenverkehr von keiner IP-Regel erlaubt wird, würde keine Pipe für denselben Datenverkehr jemals reagieren.

Piping-Regeln für eingehenden Datenverkehr erzeugen

Einige unserer anderen Schnittstellen erlauben aber definitiv eingehende Verbindungen. Als Beispiel nehmen wir die DMZ-Schnittstelle an, wenn wir eingehende Piping-Regeln anlegen.

Wie schon beim WLAN-Beispiel zuvor gemacht, werden wir zwei Pipes anlegen, eine für eingehende und eine für ausgehende Verbindungen, wie nachfolgend in *Abbildung 3.18.10* gezeigt.

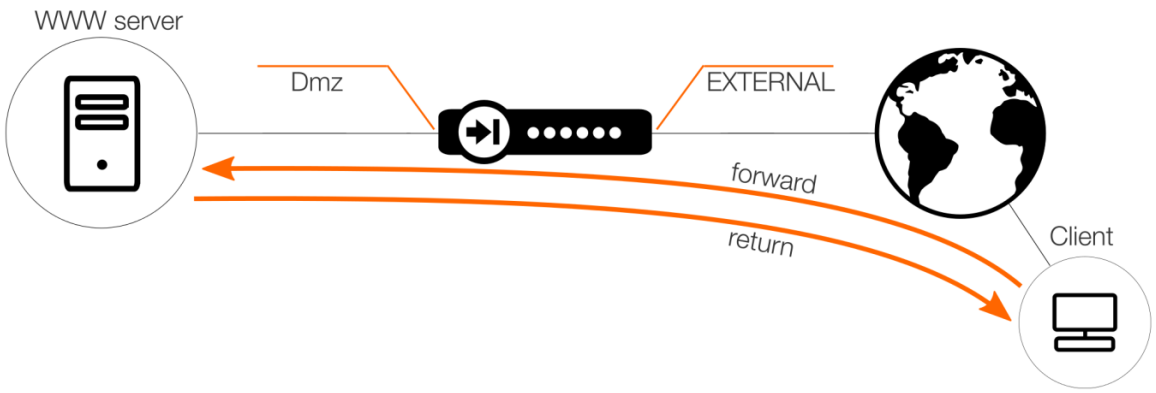


Abbildung 3.18.10 Beispiel einer Vorwärts-/Rückwärts-Kette für Verbindungen aus dem Internet

Wie wir im obigen Diagramm sehen können, ist die Pipe-Richtung umgedreht. Die Vorwärts-Kette ist für Datenverkehr, der VOM Internet IN RICHTUNG Webserver kommt. Denken Sie bei der Vorwärts-Richtung aus der Perspektive „Wer leitet die Verbindung ein“. So ist es einfacher, die Vorwärts- und Rückwärts-Ketten zu unterscheiden.

Wenn wir die für DMZ-Schnittstelle benötigten Pipes erzeugen, können wir einfach die schon für die WLAN-Schnittstelle angelegten Pipes klonen und umbenennen, wie nachfolgend gezeigt.

# ▲	Name	Grouping	Network size	Total bandwidth limit	Total packet per second limit
Pipes for the DMZ interface					
1	DMZ-In	None		100000	
2	DMZ-Out	None		100000	

Abbildung 3.18.11 Zwei Piping-Regeln für die DMZ-Schnittstelle

Danach erzeugen wir zwei Piping-Regeln, eine für den Datenverkehr, der in der DMZ eingeleitet wird, und eine andere Regel für Datenverkehr, der vom Internet aus gestartet wird. Die ausgehende Piping-Regel stellen wir genau so ein wie die Regel für die WLAN-Schnittstelle, außer dass wir hier die DMZ-Schnittstelle nutzen.

Die Regel, die unterschiedlich ist, ist die eingehende Piping-Regel. Der erste Teil der eingehenden Piping-Regel wird im nächsten Bildschirmfoto gezeigt.

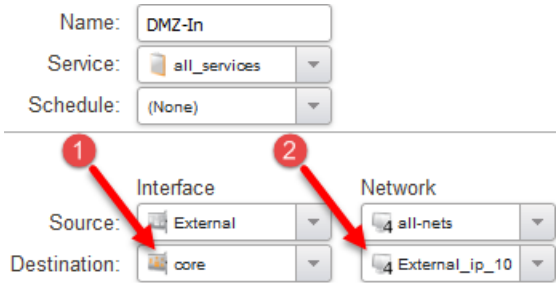


Abbildung 3.18.12 Die eingehende Piping-Regel für die DMZ-Schnittstelle

Der Unterschied hier ist, dass die Richtung des Datenverkehrsflusses umgedreht ist. Unsere Clients befinden sich im Internet und versuchen, sich mit irgendetwas in der DMZ zu verbinden, wie z.B. ein Webserver.

Aus diesem Grund wird EXTERN die Quell-Schnittstelle und das Quell-Netzwerk wird allenetze (weil wir nicht wissen, welche Quell-IP die Clients haben werden).

Was in diesem Szenario schwierig sein könnte, ist die Tatsache, dass die Ziel-Schnittstelle (**1** in der obigen Abbildung) der Core und das Ziel-Netzwerk (**2** in der obigen Abbildung) eine der öffentlichen IP-Adressen ist, die dem cOS-Core gehören. Die Vorwärts- und Rückwärts-Ketten für eingehende Verbindungen werden nachfolgend gezeigt.

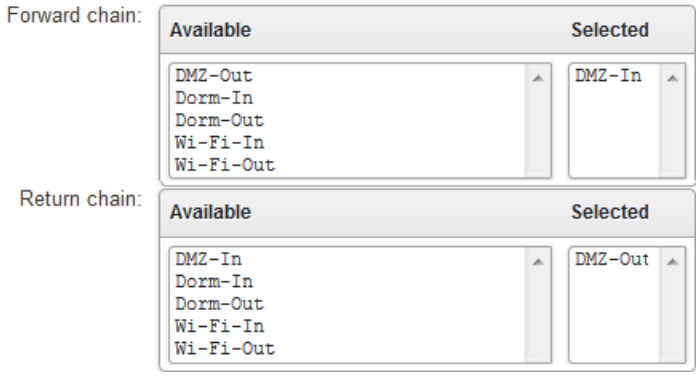


Abbildung 3.18.13 Vorwärts- und Rückwärtsketten für eingehenden Datenverkehr zur DMZ

Erklärung der Ziel-Schnittstelle des Cores

Die Ziel-Schnittstelle in diesem Szenario muss der Core sein, weil der Client im Internet versucht, die Verbindung VOM Internet IN RICHTUNG einer der IP-Adressen aufzubauen, die dem cOS-Core gehören.

Wichtig

Selbst wenn wir eine SAT-Regel nutzen, um den Datenverkehr an einen privaten Server im Innern umzuleiten, MUSS die Piping-Regel auf der Basis konfiguriert werden, wie der Datenverkehr ankommt, BEVOR irgendwelche Adressübersetzung erfolgt.

Das ist der Grund, warum die Ziel-Schnittstelle und das Ziel-Netzwerk für unseren eingehenden Datenverkehr NICHT die DMZ-Schnittstelle oder das Dmz-Net-Objekt sind.

Hinweis

Die Ziel-Schnittstelle sollte anhand der Routing-Entscheidung des cOS-Cores gewählt werden.

Hier kommt der schwierige Teil: Die Schnittstelle ist nicht immer der Core. Wie schon in *Rezept 3.16. Zusätzliche Schnittstellen-IPs zuweisen* erwähnt kann die Ziel-Schnittstelle unterschiedlich sein, abhängig davon, wohin die IP oder das Netzwerk geroutet werden. Wenn wir zu viele Teile des am Datenverkehr beteiligten Netzwerks in der Datenverkehrsformung-Konfiguration ein- oder ausschließen, kann das dazu führen, dass die Bandbreite-Zuteilung und -Berechnung fehlerhaft ist.

Bandbreite-Zuteilungen anhand der Anforderungen anpassen

Jetzt haben wir Pipes und Piping-Regeln für jede Schnittstelle, aber sind die Bandbreite-Zuteilungen sinnvoll? Sind 100 Mbits genug für das WLAN-Netzwerk? Was ist mit dem WOHNHEIM oder dem LABOR?

Hinweis

Um alles einfach und überschaubar zu halten, sehen wir für den Zweck des Beispiels das Labor-Netzwerk als eine der Schnittstellen an.

Weil wir 1.000 Mbits zum Herumspielen haben, kann es angebracht sein, die Bandbreite-Zuteilungen nochmal zu überprüfen, damit sie besser dem entsprechen, was wir für die verschiedenen Schnittstellen erwarten. Die Schnittstellen WLAN und WOHNHEIM werden höchstwahrscheinlich den meisten Datenverkehr generieren, weil die Studierenden sich Lehrvideos, YouTube, Netflix und so weiter ansehen wollen. Das kann einen Großteil der Bandbreite verbrauchen.

Wir haben sechs unterschiedliche Schnittstellen. Wenn wir jeder 100 Mbits zuweisen, haben wir insgesamt 600 Mbits und können immer noch etwa 400 Mbits verteilen.

Die Bandbreite-Zuteilung für WLAN und WOHNHEIM zu erhöhen, wäre ein guter Vorschlag, mit 200 für WLAN und 400 für WOHNHEIM. Das ist natürlich eine sinnvolle Annahme, aber jedes Netzwerk ist einzigartig, so dass vielleicht die DMZ-Schnittstelle mehr Bandbreite für eingehende Verbindungen braucht. Daher könnte es nötig sein, Zuteilungen für eingehende Bandbreite von der WOHNHEIM-Schnittstelle zur DMZ zu verschieben.

Letztendlich ist es die Entscheidung des Administrators.

Pipes und FwdFast-IP-Regeln

Pipes funktionieren nicht mit FwdFast-IP-Regeln, die keinen Status haben. Um eine Kontrolle über die Bandbreite-Nutzung zwischen zwei Hosts zu behalten, ist eine Voraussetzung, dass der Datenverkehr durch vom cOS-Core erzeugte Verbindungen gesendet wird. Weil statusfreie FwdFast-Regeln keine cOS-Core-Verbindungen erzeugen, können sie nicht in Verbindung mit Datenverkehrsformung verwendet werden.

Rezept 3.19. Dynamischer Bandbreiten-Ausgleich

Ziele

Im vorigen Rezept haben wir eine einfache Bandbreite-Begrenzung pro Schnittstelle umgesetzt. Das bedeutet aber nur, dass wir dem cOS-Core mitteilen, dass Nutzer hinter jeder Schnittstelle eine Bandbreite-Begrenzung haben, während nichts einen Nutzer davon abhält, 99 % der gesamten verfügbaren Bandbreite für sich zu beanspruchen.

Der Zweck dieses Rezepts ist, eine Bandbreite-Begrenzungsmethode zu implementieren, die die verfügbare Bandbreite dynamisch zwischen Nutzern abhängig von ihrer Quell-IP ausbalancieren kann, um zu vermeiden, dass ein Nutzer die gesamte Bandbreite der Schnittstelle mit Beschlag belegen kann, hinter der er sich befindet.

Detailbesprechung

Bis hierher haben wir das Thema Datenverkehrsformung nur sehr einfach behandelt. Es ist die einfachste mögliche Datenverkehrsformung-Situation, wenn wir für jede Schnittstelle ein festes Limit einstellen.

Das hat ein paar große Nachteile. Schauen wir uns zum Beispiel das WOHNHEIM-Netzwerk an, bei dem wir ein Limit von 400 Mbits in jeder Richtung eingestellt haben. Es gibt keine Begrenzung pro IP oder Nutzer, was bedeutet, dass ein einzelner Nutzer die gesamte verfügbare Bandbreite verbrauchen könnte (in diesem Beispiel 400 Mbits). Das führt für alle anderen Nutzer hinter dieser Schnittstelle zu Verwirrung und Frustration und führt zu der Situation, die in der nachfolgenden *Abbildung 3.19.1* dargestellt ist.

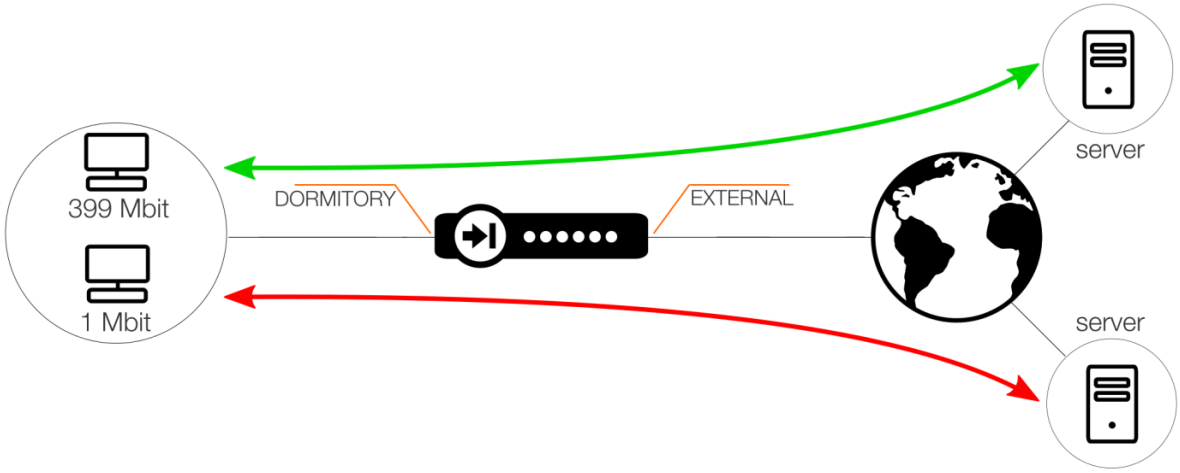


Abbildung 3.19.1 Ein Nutzer verbraucht fast die gesamte Bandbreite

Um dieses Problem zu lösen, müssen wir Gruppierung und dynamisches Balancieren einführen, so dass kein einzelner Nutzer die gesamte verfügbare Bandbreite verbrauchen kann, wenn andere Nutzer ebenfalls im Netzwerk aktiv sind.

In diesem Beispiel werden wir die WOHNHEIM-Schnittstelle des Universität-Netzwerks verwenden. Der Grund, warum wir diese Schnittstelle in unserem Beispiel verwenden, liegt darin, dass wir davon ausgehen, dass das WOHNHEIM-Netzwerk die höchste Last hat, weil die Studierenden höchstwahrscheinlich YouTube, Netflix und andere Dienste mit hohem Bedarf an Bandbreite vor allem abends aufrufen wollen, wenn sie sich nach einem langen Tag von Lesungen und vom Studieren erholen wollen. Unsere momentan für die WOHNHEIM-Schnittstelle konfigurierten Pipes und Piping-Regeln werden in den nachfolgenden drei Bildern gezeigt.

#	Name	Grouping	Network size	Total bandwidth limit
Pipes for the Dormitory interface				
1	Dorm-In	None		400000
2	Dorm-Out	None		400000

Abbildung 3.19.2 Momentan konfigurierte WOHNHEIM-Pipes

#	Name	Source interface	Source network	Destination interface	Destination network	Service
Pipe rules for Dormitory						
1	Dorm-Out	Dormitory	Dormitory_net	External	all-nets	all_services

Abbildung 3.19.3 Momentan konfigurierte WOHNHEIM-Piping-Regeln

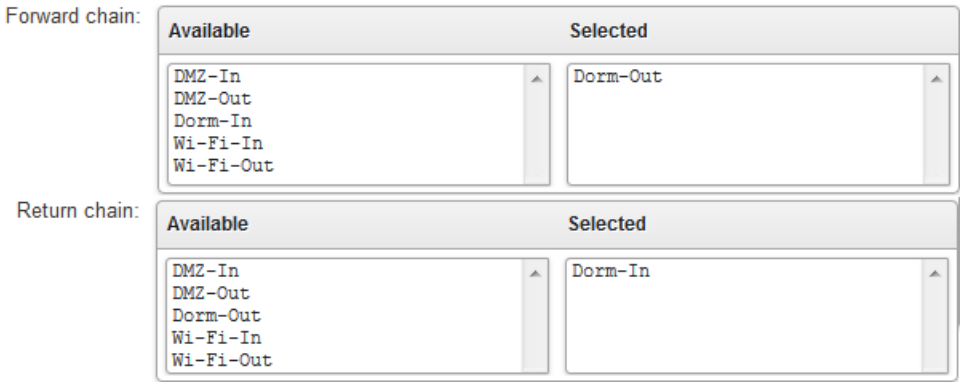


Abbildung 3.19.4 Momentan konfigurierte WOHNHEIM-Piping-Regelketten

Die Lösung: Dynamisches Balancieren von Gruppen

Um das Bandbreite-Zuteilungsproblem zu lösen, werden wir in unseren Pipes eine Option namens Gruppierung (**1**) in Verbindung mit der Option „Dynamisches Balancieren von Gruppen“ (**2**) in den Eigenschaften für die Wohnheim-Ausgangspipe verwenden, wie nachfolgend gezeigt.

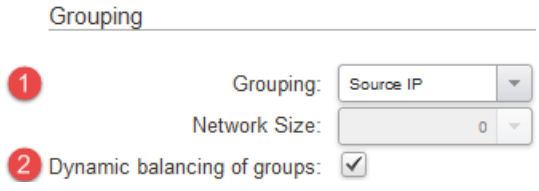


Abbildung 3.19.5 Optionen für Gruppierung und Dynamisches Balancieren in der Wohnheim-Ausgangspipe

Indem wir diese beiden Optionen aktivieren, teilen wir dem cOS-Core zwei Sachen mit:

- Wir sagen dem cOS-Core, dass jede IP-Adresse im WOHNHEIM-Netzwerk als ein Gruppenobjekt behandelt werden soll.
- Weiter sagen wir dem cOS-Core, dass jede Gruppe (IP) mit allen anderen balanciert werden soll, **wenn** die gesamte verfügbare Bandbreite in der Pipe das Gesamtlimit überschreitet.

Hinweis

Die Gruppierungsart ist unterschiedlich, je nachdem, ob wir die Vorwärts- oder Rückwärts-Pipingkette konfigurieren. Darauf gehen wir später in diesem Rezept noch ein.

Wenn wir die momentane Konfiguration unserer Pipes betrachten, sehen wir dass das Gesamtlimit auf 400 Mbits festgelegt wurde. Das heißt, solange wir dieses Bandbreite-Gesamtlimit nicht überschreiten, wird keinerlei Balancierung ausgeführt.

Ein Beispiel hierfür finden Sie in der nachfolgenden *Abbildung 3.19.6*.

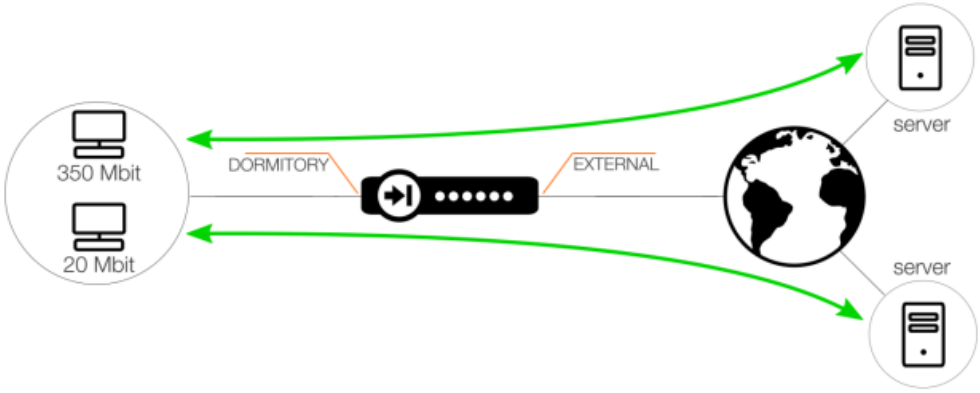


Abbildung 3.19.6 Jede IP/jeder Client bekommt die benötigte Bandbreite, weil die 400 Mbits nicht überschritten werden

Die von unseren beiden Clients genutzte Bandbreite liegt bei insgesamt 370 Mbits. Weil wir 400 Mbits zur freien Verfügung haben, gibt es für den cOS-Core momentan keinen Anlass, die Bandbreite zu balancieren.

Wenn das Bandbreite-Gesamtlimit überschritten ist

Wenn wir verschiedene Clients haben, die soviel Bandbreite anfragen, dass das festgelegte Gesamtlimit (in diesem Fall 400 Mbits) überschritten wird, wird das Dynamische Balancieren aktiviert und fängt an, die Bandbreite zwischen den anfragenden Clients auszubalancieren. Das wird als nächstes in *Abbildung 3.19.7* gezeigt.

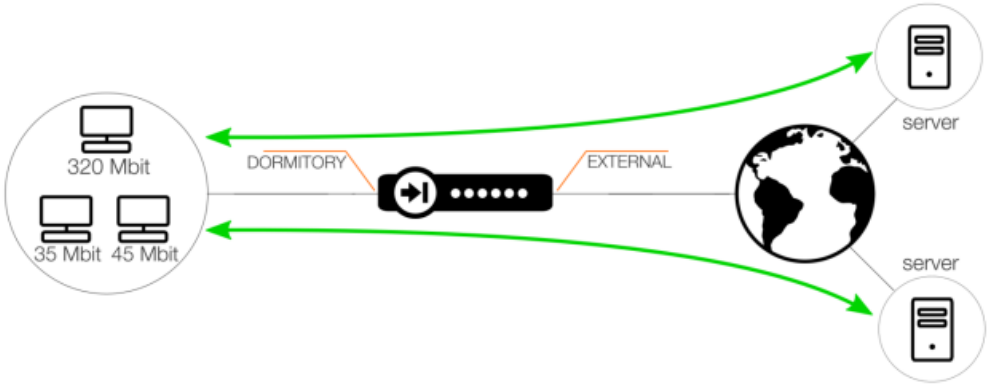


Abbildung 3.19.7 Bandbreite zwischen Clients auf teilen mit Dynamischem Balancieren

Weitere Erklärungen zu Vorwärts- und Rückwärts-Kette

Es ist wichtig, sich hier bewusst zu machen, dass die Regeln und Pipes dahingehend konfiguriert werden müssen, in welcher Richtung Datenpakete fließen. Im Beispiel unseres WOHNHEIM-Netzwerks, haben wir nur eine Piping-Regel, weil wir nicht zulassen, dass eingehende Verbindungen aus dem Internet in Richtung des WOHNHEIM-Netzwerks initiiert werden.

Für das WOHNHEIM haben wir eine Piping-Regel eingestellt, aber eine Piping-Regel sollte möglichst immer mit mindestens zwei Pipes konfiguriert werden. Eine für die Vorwärts-Kette und eine andere für die Rückwärts-Kette, wie in *Abbildung 3.19.8* dargestellt.

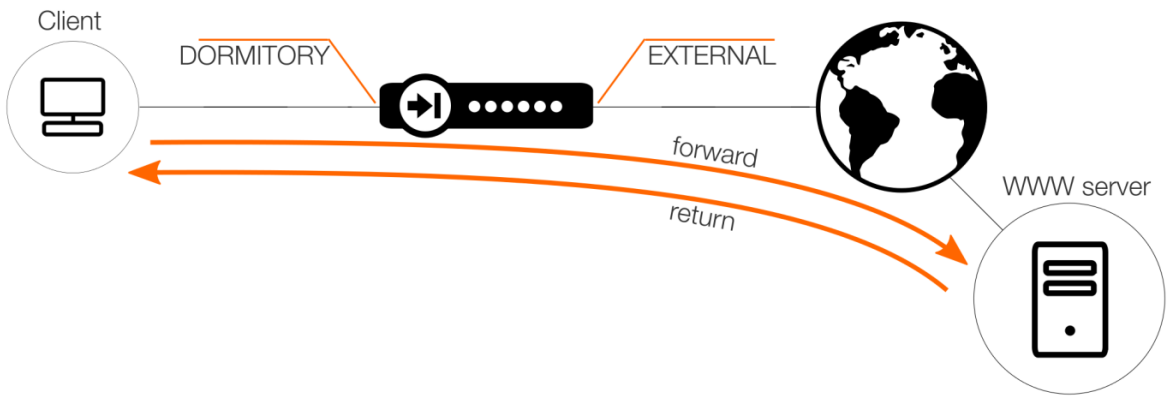


Abbildung 3.19.8 Vorwärts- und Rückwärts-Kette für die WOHNHEIM-Schnittstelle

Hier **leitet** der cOS-Core eine Anfrage/Verbindung eines Clients hinter der WOHNHEIM-Schnittstelle an einen Server im Internet weiter. Der Server **sendet** dann eine Antwort an den Client zurück. Das trifft natürlich auf sämtlichen Datenverkehr zu, der über diese Verbindung gesendet wird, nachdem sie erstmal steht.

Die Gruppierung ist für die eingehende und ausgehende Pipe unterschiedlich

Die Beschreibungen bezüglich Gruppierung und Dynamisches Balancieren bis hier bezogen sich auf das Wohnheim-Ausgangspipe-Objekt. Dieses Objekt wird in der Vorwärts-Kette in der Piping-Regel verwendet, wie zuvor dargestellt. Das bedeutet allerdings, dass wir nur die Hälfte der benötigten Pip-Änderungen gemacht haben, die dafür benötigt werden, dass Dynamisches Balancieren korrekt funktioniert.

Damit das Dynamische Balancieren bei der Rückwärts-Kette funktioniert, müssen wir unser „Wohnheim-Eingang"-Pipe-Objekt ebenfalls anpassen.

Für die „Wohnheim-Eingang"-Pipe legen wir Gruppierung anhand der Ziel-IP fest, wie in *Abbildung 3.19.9* gezeigt.

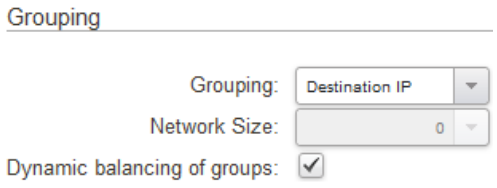


Abbildung 3.19.9 Gruppierung und Dynamisches Balancieren für die Wohnheim-Eingang-Pipe

Der Gruppierungswert für Wohnheim-Eingang (Rückwärts-Kette) ist die Ziel-IP, weil wir aus der Perspektive des cOS-Cores die Richtung beachten müssen, in der der Datenverkehr fließt.

Nehmen wir zum Beispiel einen PC im WOHNHEIM-Netzwerk mit der IP-Adresse 10.20.10.50 an, der sich mit einem Webserver im Internet mit der IP-Adresse 203.0.113.254 verbindet. Einschließlich der Portnummern wird der cOS-Core eine Verbindung wie folgt erzeugen:

WOHNHEIM:10.20.10.50:47335 -> EXTERN: 203.0.113.254:80

Wenn wir dann diese Verbindung umdrehen, sieht sie so aus:

EXTERN: 203.0.113.254:80 -> WOHNHEIM:10.20.10.50:47335

Das bedeutet, dass „EXTERN" die Quell-Schnittstelle und „203.0.113.254" das Quell-Netzwerk wird. „WOHNHEIM" und „10.20.10.50" werden Ziel-Schnittstelle und -Netzwerk. Das wird in der nachfolgenden *Abbildung 3.19.10* illustriert.

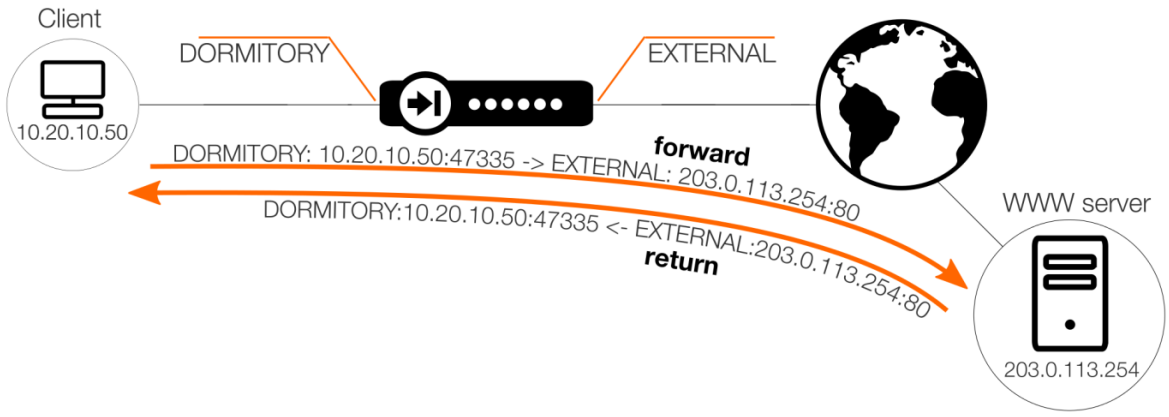


Abbildung 3.19.10 Beispiel einer Vorwärts- und Rückwärts-Kette

Es würde nicht sehr sinnvoll sein, die Rückwärts-Kette anhand der Quell-IP zu gruppieren, weil sie eine einzelne IP ist. Es ist besser, anhand der Ziel-IP zu gruppieren, weil wir wissen, dass sie immer aus den verschiedenen IP-Adressen unseres WOHNHEIM-Netzwerks besteht und somit gut für die Bandbreiten-Verteilung geeignet ist.

Es ist sinnvoll, anzunehmen, dass sich unsere Clients mit den gleichen Zielservern (wie z.B. Facebook, YouTube, Netflix) verbinden werden. Wenn wir sie anhand der Quell-IP für die Rückwärts-Kette gruppieren würden, würde die Bandbreite-Verteilung immer noch funktionieren, aber nicht so gut.

Nachwort

Anmerkungen des Autors

Wir haben jetzt das Ende des ersten cOS-Core-Kochbuchs erreicht. Ich hoffe, dass alle Rezepte, die wir bisher eingefügt haben, für Sie von Nutzen sind und dass sie zum besseren Verständnis des cOS-Cores beigetragen haben.

Dabei haben wir bis hier nur an der Oberfläche dessen gekratzt, was wir mit dem cOS-Core bewerkstelligen können. Ich glaube, dass manche in diesem Buch einen Abschnitt darüber vermissen, wie man verschlüsselte virtuelle private Netzwerktunnel (VPN) mithilfe von IPsec, L2TP, PPTP, GRE und SSL errichtet.

VPN ist ein sehr großes Themengebiet und kann einen aufgrund seiner Komplexität manchmal fast erdrücken. Daher ist es nötig, dass wir zuerst mit den Grundlagen beginnen und den Schwierigkeitsgrad und die Komplexität der Rezepte nach und nach steigern. Dieses Kochbuch konzentriert sich auf die Grundlagen und fängt dann an, in etwas komplexere Szenarios einzusteigen, aber es gibt noch jede Menge mehr zu erklären und zu besprechen. Seien Sie versichert, dass VPN in einer der kommenden Publikationen dieser Kochbuch-Serie enthalten sein wird. Wir haben gerade erst angefangen ...

Mit freundlichen Grüßen,
Peter Nilsson.

Die nächsten Rezepte

Es gibt noch eine Vielzahl an Szenarios und Rezepten zu beschreiben. Hier ist eine Vorschauliste der Rezepte, die für die nächste Veröffentlichung geplant sind:

Hinweis: Dies ist nur eine vorläufige Aufzählung, die sich noch ändern kann.

- Den DHCP-Client konfigurieren.
- Virtuelles Routing nutzen, um geschützte Labor-VLAN-Segmente zu erzeugen.
- Web-Authentifizierung für benutzerbezogenen Netzwerkzugang einrichten und nutzen.
- IDP einrichten, um eingehende Angreiferattacken zu blockieren.

- Pipe-Ketten für fortgeschrittene Bandbreiten-Verwaltung nutzen.
- Anwendungskontrolle und Pipes verwenden, um die Bandbreitenutzung pro Anwendung zu begrenzen.
- Internetredundanz mithilfe von Route-Ausfallsicherung implementieren.
- Eine Einführung in VPN.
- LAN-zu-LAN-Tunnel für Virtuelle Private Netzwerke (VPN) mithilfe von IPsec und vorab geteiltem Schlüssel (PSK, Pre-shared key) einrichten.
- LAN-zu-LAN-Tunnel für Virtuelle Private Netzwerke (VPN) mithilfe von IPsec und selbst ausgestellten Zertifikaten einrichten.
- LAN-zu-LAN-Tunnel für Virtuelle Private Netzwerke (VPN) mithilfe von IPsec und CA-signierten Zertifikaten einrichten (CA = Certificate Authority, Zertifizierungsstelle).
- Roaming- und Außendienstler-Tunnel für Virtuelle Private Netzwerke (VPN) mithilfe von IPsec und vorab geteiltem Schlüssel einrichten.
- Roaming- und Außendienstler-Tunnel für Virtuelle Private Netzwerke (VPN) mithilfe von IPsec und vorab geteiltem Schlüssel (PSK) in Kombination mit dem CFG-Modus und XAuth-Authentifizierung einrichten.
- Roaming- und Außendienstler-Tunnel für Virtuelle Private Netzwerke (VPN) mithilfe von IPsec und vorab geteiltem Schlüssel (PSK) und dem in Windows eingebauten L2TP/IPsec-Client einrichten.
- Roaming- und Außendienstler-Tunnel für Virtuelle Private Netzwerke (VPN) mithilfe von selbst ausgestellten Zertifikaten und dem in Windows eingebauten L2TP/IPsec-Client einrichten.
- Verschlüsselte Tunnel für Virtuelle Private Netzwerke (VPN) mithilfe des Punkt-zu-Punkt-Tunnel-Protokolls (PPTP) konfigurieren.
- SSL-VPN-Server errichten und den Client auf einem Windows-Rechner konfigurieren.

- GRE-Tunnel (Generic Routing Encapsulation, Generische Routing-Einkapselung) konfigurieren.

Wenn Sie weitere Vorschläge haben oder ein Thema Ihnen ganz besonders wichtig ist, Sie einen Änderungsvorschlag oder sonst etwas im nächsten Kochbuch sehen wollen, zögern Sie nicht, mit uns unter *cookbook@clavister.com* Kontakt aufzunehmen.

Alphabetischer Index

A

B

C

D

F

G

I

K

L

N

O

P

R

S

U

V

W

Z

Das Clavister

cOS Core Kochbuch

Eine Einführung in das Absichern von Netzwerken mit Clavister cOS Core

In diesem ersten Buch, das die Fähigkeiten des cOS-Core-Netzwerkbetriebssystems erkundet, zeigt Netzwerk-Sicherheitsexperte Peter Nilsson die Einfachheit und Leistungsfähigkeit auf, mit der Sie bei Verwendung von cOS Core eine Vielzahl wichtiger Netzwerk-Sicherheitsprobleme lösen können.

Beginnend beim einfachen Schutz von Webservern gegen hartnäckige und erfahrene Internet-Hacker bis hin zur ärgerlichen Frage, wie man harmlose Firmenmitglieder voneinander abschirmt, werden die eleganten Möglichkeiten des cOS Core in einer sorgfältig zusammengestellten Reihe von Beispielen aus der Praxis dargestellt. Das Buch ist für alle geeignet, die das erste Mal mit cOS Core arbeiten, und enthält Tipps und Ratschläge zur Sicherung kleiner Firmen-Netzwerke bis hin zu großen Unternehmens-Computer-Infrastrukturen.

Rückmeldungen zu diesem Buch und Vorschläge für Ergänzungen in zukünftigen Ausgaben können an cookbook@clavister.com gesendet werden.

clavister®

CONNECT . PROTECT

ISBN 978-91-982968-3-9