Collax Firewall und Security Grundlagen

Howto

Dieses Howto beschreibt die Konfiguration der Collax Firewall, um das Verhalten und die Protokollierung von Netzwerkdiensten behandeln zu können. Der Collax Server überwacht und steuert dabei den Datenverkehr zwischen Netzen, wie bspw. dem Localnet (LAN) und dem Internet. Außerdem gewährt bzw. verbietet er den Zugriff auf Dienste des Collax Servers.

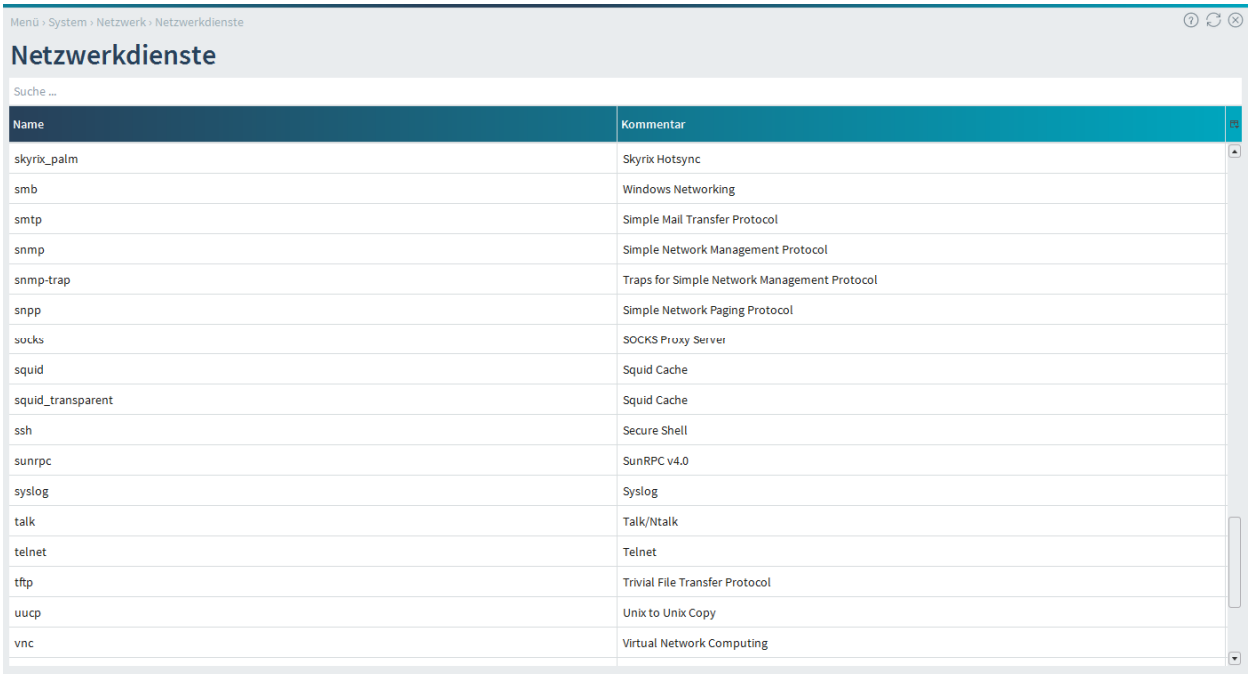
Voraussetzungen

- Collax Security Gateway
- Collax Business Server
- Collax Platform Server inkl. Collax Modul Gatekeeper

Grundlagen Dienste und Protokolle

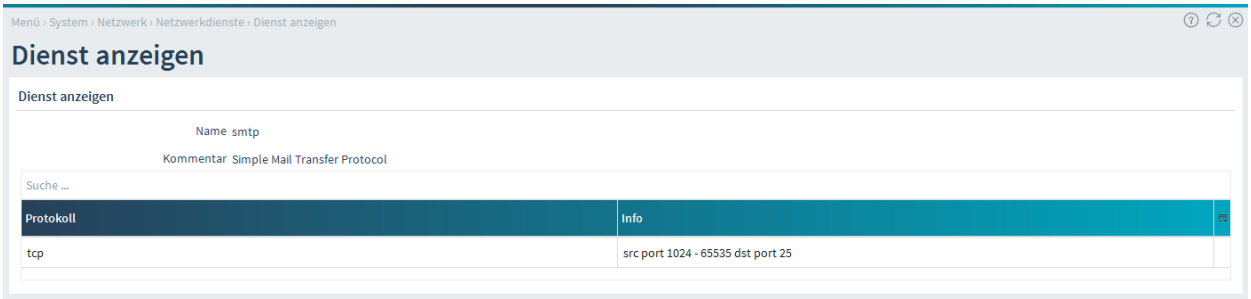
Um den Austausch von Daten zwischen vernetzten Computern zu ermöglichen, kommen Dienste zum Einsatz. Dabei handelt es sich um die Zuordnung von einem IP-Protokoll und zugehörigen Quell- und Zielports.

Unter *„System → Netzwerk → Firewall →Dienste“* werden bekannte Dienste angezeigt, die unter dem Namen des Dienstes im System an anderer Stelle ausgewählt werden können.



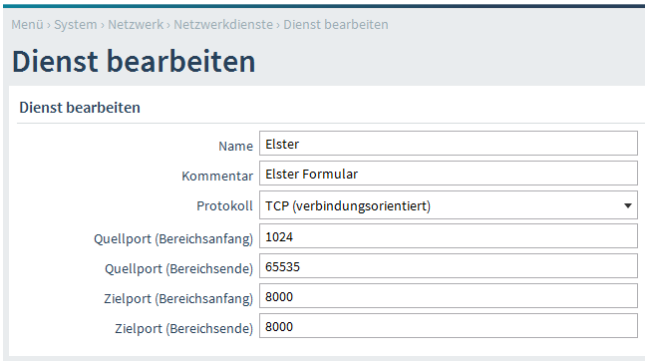
Um bspw. eine E-Mail zu übermitteln, kommt der Dienst „SMTP“ zum Einsatz.

Durch einen Doppelklick auf den Namen werden die genauen Einstellungen eines Dienstes angezeigt.



Um einen neuen Dienst hinzuzufügen, wählen Sie den Punkt *„Dienst hinzufügen“* aus. Im darauffolgenden Dialog können die Einstellungen eines selbstdefinierten Dienstes angegeben werden.

Im folgenden Beispiel legen wir den Dienst „Elster“ an für die elektronische Übermittlung der Steuererklärungsdaten an das Finanzamt durch die Software „ElsterFormular“.



Name Hier wird der Name für den Dienst angegeben.

Protokoll Hier muß das von dem Dienst genutzte Protokoll ausgewählt werden.

Neben den bekannten Protokollen „Internet Control Message Protocol“ (ICMP), welches dem Austausch von Meldungen über das „Internet Protocol“ (IP) dient (z.B.: ping) und den Transport Protokollen „Transmission Control Protocol“ (TCP) und „User Datagram Protocol“ (UDP) stehen noch „IPSec Encapsulated Security Payload“ (ESP) und „IPSec Authenticated Headers“ (AH) zur Verfügung, die in Verbindung mit dem IP-Sicherheitsprotokoll „IPSec“ Verwendung finden, sowie das „Generic Routing Encapsulation“ (GRE) Protokoll, welches dazu dient, andere Protokolle einzukapseln und so in Form eines Tunnels über IP zu transportieren. Der Dienst „PPTP“ unter Windows bspw. verwendet dieses, um VPN-Verbindungen aufzubauen.

Quellport (Bereichsanfang) Hier wird der Anfang des Quellportbereiches angegeben. Normalerweise wird der Quellport vom System, welches die Verbindung aufbaut, willkürlich vergeben. Meist liegt der Quellport im Bereich 1024 bis 65535. In bestimmten Fällen, etwa bei manchen UDP-Verbindungen, kommen Anfragen immer vom gleichen Absenderport. Dann kann hier eine sinnvolle Einschränkung gemacht werden.

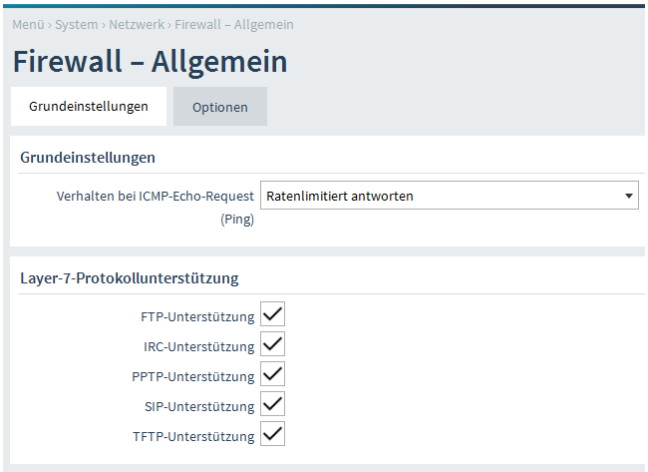
Quellport (Bereichsende) Hier wird das Ende des Quellportbereiches angegeben. Bleibt das Feld leer, wird nur der Anfangsport als einziger Quellport verwendet.

Zielport (Bereichsanfang) Hier wird der Anfang des Zielportbereiches angegeben.

Zielport (Bereichsende) Hier kann das Ende des Zielport-Bereiches angegeben werden. Bleibt das Feld leer, wird nur der Anfangsport als einziger Zielport verwendet. Bereichsanfang und –ende können auch denselben Wert enthalten.

Grundeinstellungen

Unter *„System → Netzwerk → Firewall → Allgemein“* werden einige Optionen für das Verhalten und die Protokollierung der Firewall eingestellt.



Verhalten bei ICMP-Echo-Request (Ping) ICMP-Echo-Request-Pakete (pings) dienen dazu, festzustellen, ob ein bestimmter Rechner erreichbar ist und wie lange die Laufzeit der Datenpakete dorthin ist. Hier wird eingestellt, wie der Collax Server auf ICMP-Echo-Requests reagiert.

Normalerweise wird *ratenlimitiert* auf ICMP-Echo-Requests geantwortet. Dann werden ca. 10 Ping-Pakete pro Sekunde beantwortet, alle anderen werden verworfen. Falls viele Systeme gleichzeitig versuchen, den Collax Server anzupingen, kann es auch erforderlich sein, *unlimitiert* zu antworten (dann wird jeder Ping beantwortet).

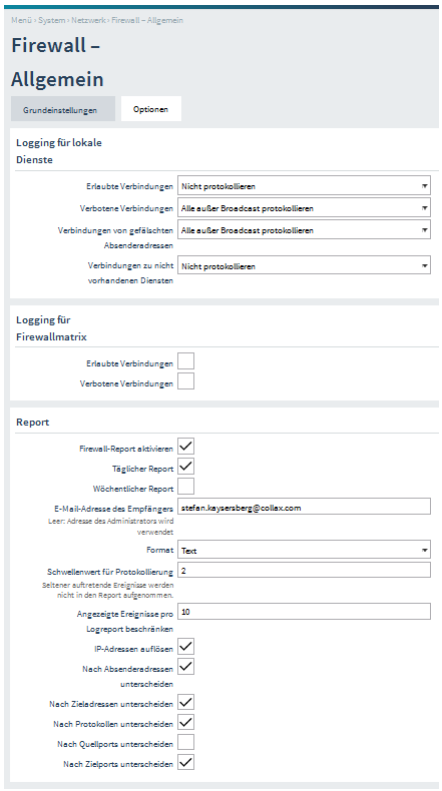
Darüberhinaus kann auch eingestellt werden, dass der Collax Server *nicht antwortet*.

Layer-7-Protokollunterstützung Mit Hilfe dieser Unterstützungsmodule werden für einzelne Protokolle die Datenpakete analysiert und es kann entsprechend auf die Besonderheiten des jeweiligen Protokolls reagiert werden. Bei einer FTP-Verbindung wird beispielsweise der neu geöffnete Datenkanal dem richtigen Client zugeordnet.

Einige IP-Protokolle verwenden mehr als eine Verbindung. Bei aktivem FTP wird beispielsweise zunächst vom Client zum Server eine Kontrollverbindung geöffnet, über die die Anmeldung am Server und die Kommandos des Clients geschickt werden. Für eine Datenübertragung (Verzeichnisanzeige, Download usw.) wird vom Server eine Datenverbindung zum Client aufgebaut. Gerade bei der Verwendung von „NAT/Masquerading“ führt dies zu Problemen, da die Firewall diese neue Verbindung einem internen, maskierten System zuordnen muß.

Protokollierungsoptionen

Die Protokollierungsoptionen betreffen nur Verbindungen, die direkt an den Collax Server gerichtet sind. Die Protokollierung durchlaufender Verbindungen wird in der Firewallmatrix konfiguriert.



Logging für lokale Dienste

Erlaubte Verbindungen Durch das Aktivieren dieser Option wird der Aufbau erlaubter Verbindungen auf den Collax Server protokolliert.

Verbotene Verbindungen Durch das Aktivieren dieser Option werden nichtautorisierte Verbindungsversuche protokolliert.

Verbindungen von gefälschten Absenderadressen Mit dieser Option werden Verbindungsversuche von gefälschten Absenderadressen protokolliert.

Verbindungen zu nicht vorhandenen Diensten Durch das Aktivieren dieser Option werden Verbindungsversuche auf Ports protokolliert, denen keine Dienste zugeordnet sind.

Logging für Firewallmatrix

Erlaubte Verbindungen Durch das Aktivieren dieser Option werden alle Verbindungen protokolliert, die in der Firewallmatrix als erlaubt eingestellt sind.

Verbotene Verbindungen Durch das Aktivieren dieser Option werden alle Verbindungsversuche zwischen Netzwerken protokolliert, deren Regel in der Firewallmatrix auf ablehnen oder wegwerfen gesetzt ist.

Report

Firewall-Report aktivieren Mit dieser Option wird die automatische Erstellung von Firewall-Reports aktiviert. Ein solcher Report enthält eine statistische Auswertung der Einträge in der Firewall-Logdatei.

Täglicher Report Mit dieser Option wird täglich ein Firewall-Report erstellt.

Wöchentlicher Report Mit dieser Option wird wöchentlich ein Firewall-Report erstellt.

E-Mail-Adresse des Empfängers In diesem Feld wird die E-Mail-Adresse angegeben, an die der Report gesendet wird.

Format Der Report kann wahlweise als einfacher Text oder HTML-formatiert werden.

Schwellenwert für Protokollierung Mit diesem Schwellenwert wird festgelegt, wie oft ein Ereignis auftreten muß, damit es in den Report aufgenommen wird.

Angezeigte Ereignisse pro Logreport beschränken Dieser Wert beschränkt die Anzahl der im Report aufgeführten Ereignisse.

IP-Adressen auflösen Durch das Aktivieren dieser Option werden IP-Adressen im Report über den Nameserver in Hostnamen aufgelöst. Dies kann erheblichen Netzwerkverkehr erzeugen und die Erstellung des Reports verlangsamen.

Nach Absenderadressen unterscheiden Verschiedene Logeinträge können als einzelne oder als getrennte Ereignisse aufgefaßt werden. Durch das Deaktivieren dieser Option können mehrere Meldungen mit unterschiedlichen Absenderadressen zu einem Ereignis zusammengefaßt werden.

Nach Zieladressen unterscheiden Durch das Deaktivieren dieser Option können mehrere Meldungen mit unterschiedlichen Zieladressen zu einem Ereignis zusammengefaßt werden.

Nach Protokollen unterscheiden Durch das Deaktivieren dieser Option können mehrere Meldungen mit unterschiedlichen Protokollen (TCP, UDP usw.) zusammengefaßt werden.

Nach Quellports unterscheiden Durch das Deaktivieren dieser Option können mehrere Meldungen mit unterschiedlichen Quellports zusammengefaßt werden.

Nach Zielports unterscheiden Durch das Deaktivieren dieser Option können mehrere Meldungen mit unterschiedlichen Zielports zusammengefaßt werden.

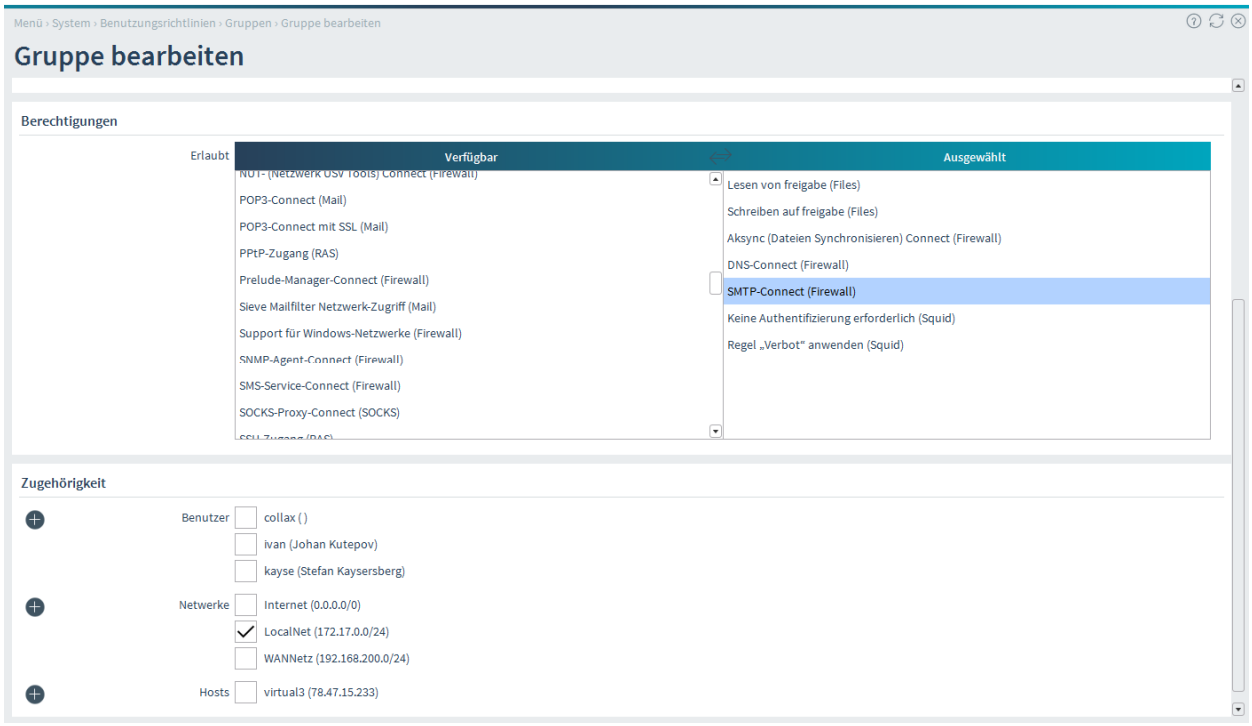
Durchlaufende und an den Collax Server gerichtete Verbindungen

Um die Collax Firewall besser verstehen zu können, unterscheidet man zwischen Verbindungen, die direkt an den Collax Server gerichtet sind und durchlaufende Verbindungen, die durch den Collax Server gehen (Routing). An den Collax Server gerichtete Verbindungen werden über die Gruppen und die darin enthaltenen Dienste und Netze konfiguriert. Durchlaufende Verbindungen werden hingegen in der Firewallmatrix konfiguriert.

Gruppen

Die Berechtigungen, um auf Dienste des Collax Servers zuzugreifen, wird über den Dialog *„System → Benutzungsrichtlinien → Richtlinien → Gruppen“* gesetzt.

Um Zugriff auf den E-Mail-Dienst *„SMTP“* zu erlauben, wird die entsprechende *Berechtigung* innerhalb der Gruppe gesetzt. Als *Mitglieder-Netz* der Gruppe geben wir das *Localnet* an, um den Zugriff von Clients daraus zu ermöglichen.



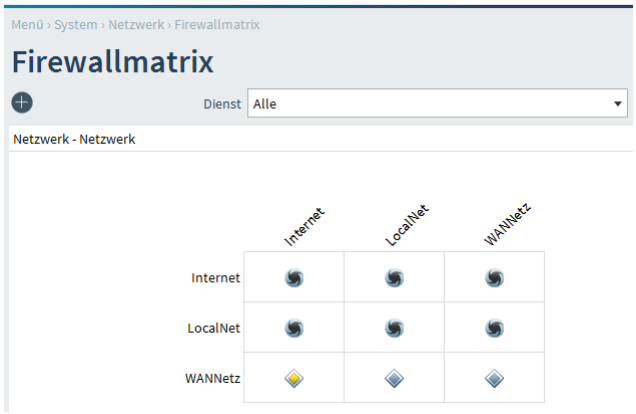
Weiteres Anwendungsbeispiel: Um eine SMTP-Verbindung zu einem Collax Server aus dem Internet aufbauen zu können, auf dessen externe IP-Adresse ein MX-Record konfiguriert ist, bedarf es neben der Berechtigung „SMTP“ innerhalb einer beliebigen Gruppe das Mitglieder-Netz *Internet*. Der Collax Server ist somit als offizieller Mailserver erreichbar. Authorisierte Clients können den Collax Server in dieser Konfiguration selbstverständlich auch als Postausgangsserver (Relayhost) verwenden.

Firewallmatrix

Dieser Dialog befindet sich unter *„System → Netzwerk → Firewall → Matrix“*.

Die Firewallmatrix ist eine visuelle Darstellung der integrierten Firewall und nur für durchlaufende Datenpakete relevant. Hier wird festgelegt, welche Netzwerkverbindungen zwischen einzelnen Netzen erlaubt bzw. geblockt sind.

Hinweis: Die Firewallmatrix ist nur für durchlaufende Datenpakete relevant. Zugriffe auf Dienste im Collax Server selbst werden in den Benutzungsrichtlinien gesteuert.



Die Matrix wird immer „von Zeile nach Spalte“ gelesen. Am Schnittpunkt wird eingestellt, wie der ausgewählte Dienst behandelt wird. Dabei werden leicht verständliche Symbole eingesetzt. Die Matrix wird daher auch als „Graphical Ruleset Generator“ bezeichnet.

Werden neue Netzwerke definiert, ist als Ziel in der Matrix die Standardregel „Wegwerfen“ zwischen diesen Netzwerken eingestellt. Neben einer „Default-Policy“ (Einstellung *Dienst: Alle*) können aus der Liste einzelne Dienste ausgewählt werden, für die jeweils die Firewall-Regeln eingestellt werden.

Links und oberhalb sind alle angelegten Netze bzw. die angelegten Gruppen als Beschriftung der Matrix aufgeführt. Durch Anklicken des linken oberen Felds können die Netze und Gruppen umgeschaltet werden. Bei Auswahl einer Gruppe werden die IP-Adressen aller Rechner, die Mitglied dieser Gruppe sind, zur Bildung der Firewallregeln herangezogen.

Ein „schwarzes Loch“ bedeutet, dass Pakete verworfen werden, ohne dass für den Absender eine ICMP-Meldung erzeugt wird („Drop“).

Das „Durchfahrt-verboten-Schild“ zeigt an, dass Verbindungen aktiv abgewiesen werden. Der Absender erhält eine entsprechende ICMP-Nachricht („Reject“).

Ein „Vorfahrtsstraßen-Schild“ zeigt an, dass der Verbindungsaufbau erlaubt ist („Accept“).

Ein „Umleitungsschild“ zeigt an, dass die Verbindungen umgeleitet werden, entweder über NAT oder durch einen transparenten Proxy (nur HTTP).

Ein „Achtung-Schild“ zeigt an, dass an dieser Stelle ein Konflikt besteht. Weitere Informationen dazu finden sich weiter unten bei den „Aktionen“.

Hinweis: In der Matrix muß immer nur eine Regel für das erste Paket der Verbindung, also für den Verbindungsaufbau, gesetzt werden. Die Folgepakete sind durch das im Collax Server integrierte „Connection Tracking“ automatisch enthalten.

Manuell gesetzte Regeln werden immer durch farbige Symbole dargestellt. Durch „Vererbung“, etwa aus Subnetzen oder über die Default-Policy, entstehen implizite Regeln. Diese werden in grau dargestellt und können jederzeit durch explizite Regeln „überschrieben“ werden.

Neben einer „Default-Policy“ (Einstellung Dienst: Alle) können aus der Liste einzelne Dienste ausgewählt werden, für die jeweils die Firewall-Regeln eingestellt werden.

Ist für einen bestimmten Dienst, wie HTTP oder DNS, eine Regel manuell gesetzt, wird dies in der Ansicht Dienst: Alle angezeigt. Das entsprechende Symbol wird dann durch zwei farbige Klammern ergänzt. Zusätzlich können im Popup-Fenster weitere Informationen zu den definierten Regeln und Diensten eingesehen werden.

Um eine explizite Regel für einen bestimmten Dienst zu setzen, wird dieser aus der Liste der einzelnen Dienste ausgewählt. Durch einen Klick auf den Schnittpunkt kann die Regel gesetzt werden.

Protokollieren Mit dem Aktivieren dieser Option werden die Verbindungen für diesen Dienst in der Logdatei protokolliert.

Regel In dieser Liste wird festgelegt, wie mit den Verbindungen verfahren werden soll:

Die Regel *Wegwerfen* blockiert den Verbindungsaufbau. Die Pakete werden gelöscht, und es wird keinerlei Rückmeldung per ICMP erzeugt.

Die Regel *Ablehnen* blockiert ebenfalls den Verbindungsaufbau. Allerdings wird eine ICMP-Nachricht an den Absender erzeugt, die darüber informiert, daß die Verbindung nicht erlaubt ist.

Mit der Regel *Erlauben* wird der Verbindungsaufbau gestattet.

NAT-Regeln Mit den Regeln *Source-NAT*, *Destination-NAT*, *Source-Netmap* und *Destination-Netmap* können die Pakete auf eine zu bestimmende Netzwerkadresse umgeschrieben werden. Der Verbindungsaufbau ist prinzipiell gestattet.

Bei der Auswahl einer NAT-Regel wird durch *Abbilden auf Netzwerk* das Netzwerk gewählt, auf das die Ziel-IP-Adressen abgebildet werden.

Wird eine NAT-Regel für einen bestimmten Port angelegt, kann im Feld *Zielport* zusätzlich ein Bereich für den Zielport angegeben werden.

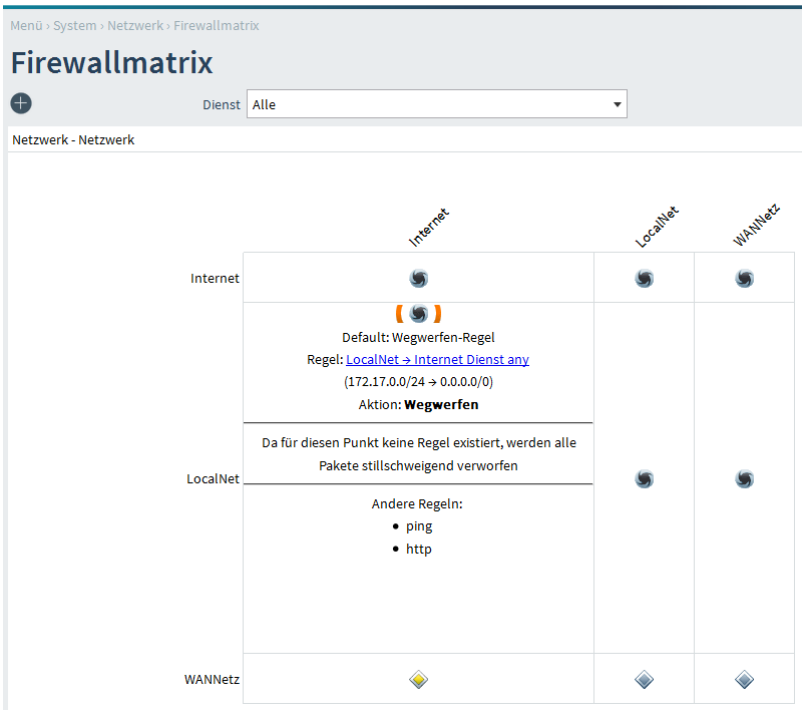
Bleibt das Feld leer, wird der Port beibehalten.

Hinweis: Über den Firewall-Viewer können nun auch explizite Regeln für einen bestimmten Dienst hinzugefügt werden. Dieser Dialog befindet sich unter *„System → Netzwerk → Firewall → Viewer“*

Eine Sonderstellung nimmt der Dienst *„http“* ein. Hier ist es neben den oben genannten Regeln auch möglich, die Regel *„Transparenter Proxy“* zu setzen. Dabei werden alle an Port 80 (http) gerichteten Anfragen abgegriffen und an den Proxyserver weitergeleitet.

Ist für einen bestimmten Dienst eine Regel manuell gesetzt, wird dies in der Ansicht *„Dienst: Alle“* angezeigt. Das entsprechende Symbol wird dann durch zwei farbige Klammern ergänzt.

Zusätzlich können weitere Informationen zu den definierten Regeln und Diensten in der Übersicht eingesehen werden.



Firewallmatrix und Hostgruppen

Neben den Netzwerkverbindungen zwischen einzelnen Netzen ist es auch möglich, den Verbindungsaufbau von einem Netz zu den Hosts einer Gruppe, von einer Host-Gruppe in ein weiteres Netz oder zu den Hosts einer weiteren Gruppe zu steuern.

Dabei sind folgende Kombinationen möglich:

(Von Netzwerk nach Netzwerk)
Von Netzwerk nach Hostgruppen
Von Hostgruppen nach Netzwerk
Von Hostgruppen nach Hostgruppen

Bei Hostgruppen werden in der Firewall Regeln für alle IP-Adressen der Hosts erstellt, die Mitglied der Gruppe sind.

Als Host werden einzelne Rechner bezeichnet, die dem Collax Server bekannt sind. Im einfachsten Fall muß nur die IP-Adresse und der Name eingetragen werden.

Dieser Dialog befindet sich unter *„System → Benutzungsrichtlinien → Richtlinien → Hosts“*

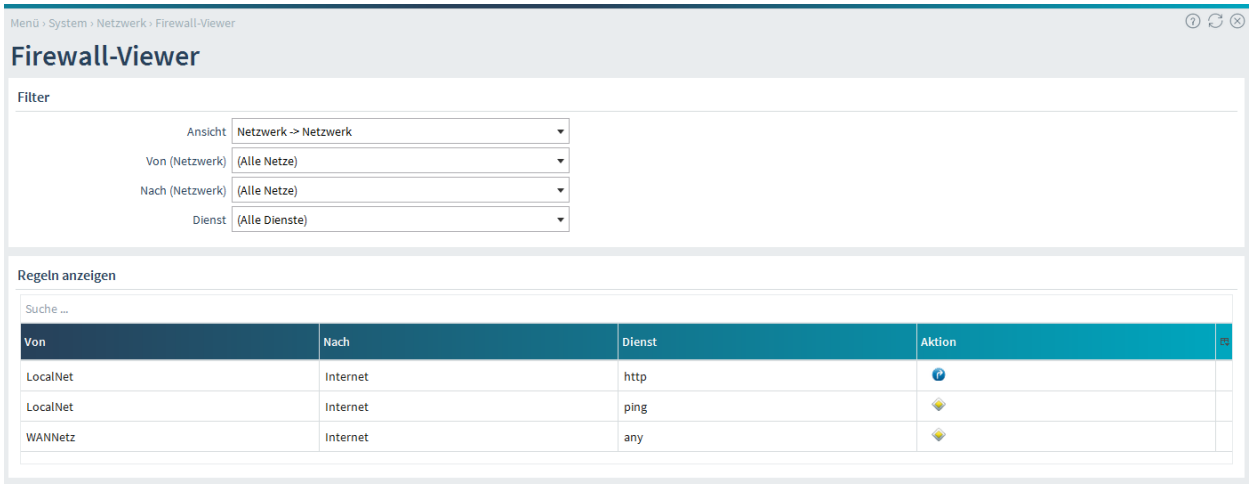
Damit kann ein Host über die Gruppenzugehörigkeit einer Gruppe zugeordnet werden.

In der Firewallmatrix kann nun bequem festgelegt werden, ob ein Verbindungsaufbau erlaubt oder verboten ist.

Firewall-Viewer

Über den Firewall-Viewer werden die in der Matrix eingestellten Firewallregeln in einer Listendarstellung angezeigt. Über Filteroptionen können einzelne Quell- und Zielnetze und Hostgruppen sowie Dienste ausgewählt werden.

Dieser Dialog befindet sich unter *„System → Netzwerk → Firewall → Viewer“*



In der Liste erscheinen nur Einträge, bei denen konkrete Regeln gesetzt sind. Die Standardregel *„Wegwerfen“* erscheint also nicht in der Liste der Regeln.

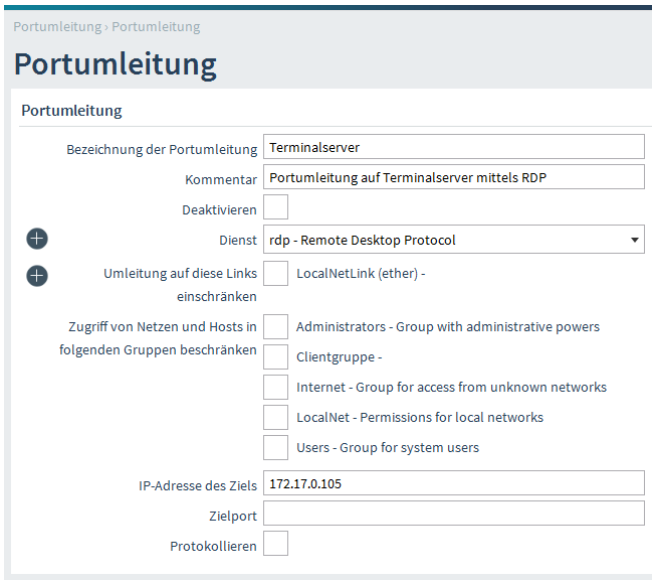
Hinweis: Über den Firewall-Viewer können nun auch explizite Regeln für einen bestimmten Dienst hinzugefügt werden.

Portumleitung

Eine Portumleitung oder Portweiterleitung dient dazu, eine Verbindung, die auf einem bestimmten Port eingeht, auf einen anderen Rechner umzuleiten.

Um aus dem Internet einen bestimmten Dienst auf einem Server im Netzwerk erreichbar zu machen, kann dafür eine Portumleitung angelegt werden. Es soll ein Terminalserver mit der IP-Adresse 172.17.0.105 mittels Remote Desktop Protocol (RDP) zur Fernwartung erreichbar gemacht werden.

Dieser Dialog befindet sich unter *„System → Netzwerk → Firewall → Portumleitung“*



Dienst Aus dieser Liste kann der Dienst ausgewählt werden, der weitergeleitet werden soll. Hier werden vordefinierte und auch selbst hinzugefügte Dienste zur Auswahl bereitgestellt.

Umleitung auf diese Links einschränken Die Auswahl bestimmt, auf welchen Links die Portumleitung angewendet werden soll. Wird kein Link gewählt, wird die Umleitung auf alle IP-Pakete angewendet, die an einem beliebigen lokalen Link ankommen. Wird ein Link gewählt, so wird die Portumleitung auf den entsprechenden Link beschränkt.

Zugriff von Netzen und Hosts in folgenden Gruppen beschränken Soll die Umleitung nur von bestimmten Netzwerken oder Hosts in Anspruch genommen werden können, ist hier die entsprechende Gruppe auszuwählen. Befinden sich die IP-Adresse des Ziels und die Source-IP-Adresse im selben Netzwerk, muss auf dem entsprechenden Link dieses Netzwerk maskiert werden. Sobald in einer Gruppe das Netz Internet enthalten ist, kann keine weitere Unterscheidung nach Netzwerken vorgenommen werden. Hier ist zu empfehlen, dass dann eine separate Portumleitung nur mit Zugriff aus dem Internet, und auf einen Internet-Link beschränkt, vorgenommen wird.

IP-Adresse des Ziels Der Rechner, auf den die Portanfragen umgeleitet werden sollen. Befinden sich die IP-Adresse des Ziels und die Source-IP-Adresse im selben Netzwerk, muss auf dem entsprechenden Netzwerk-Link dieses Netzwerk maskiert werden.

Zielport Der Zielport, auf den die Netzwerkpakete umgeschrieben werden sollen. Bleibt das Feld leer, wird der Port des weitergeleiteten Dienstes verwendet (hier: (rdp) port 3389)

Protokollieren Für eine weitere Überwachung der Funktion und ihrer Nutzung kann hier die Protokollierung der Netzwerkpakete aktiviert werden. Protokollierte Pakete können durch den Firewall-Report erfaßt werden.

Deaktivieren Eine Umleitung kann hier deaktiviert bzw. wieder reaktiviert werden. Dadurch kann wiederholtes Löschen und Neuanlegen vermieden werden, wenn eine Umleitung nur gelegentlich benötigt wird.

Brute Force-Schutz

Die Funktion dient dazu, Zugriffe auf Dienste im Collax Server selbst vor Brute-Force-Attacken zu schützen.

Dieser Dialog befindet sich unter *„System → Netzwerk → Firewall → Brute-Force-Schutz“*

Dauer der Sperrung Hier kann die Dauer der Sperrung festgelegt werden.

Anzahl erlaubter Loginversuche Hier kann die Anzahl der Loginversuche festgelegt werden. Wird die Anzahl überschritten, wird der Dienst gesperrt, sodass keine weiteren Versuche mehr möglich sind.

Nicht sperren Bestimmte Netzwerke, aus denen der Zugriff auf Dienste im Collax Server erfolgen, können hier von der Sperrung ausgenommen werden.

Brute Force-Schutz-Status

Im Dialog *„Status/Wartung → Status →Netzwerk → Brute-Force-Schutz-Status“* können IP-Adressen manuell gesperrt werden und Sperren wieder aufgehoben werden.

In diesem Eingabefeld werden die IP-Adressen eingetragen. Die einzelnen Adressen können mit Leerzeichen, Zeilenumbruch oder Komma getrennt werden.