IP-Zugriffslisten konfigurieren und filtern

Inhalt

Einleitung

In diesem Dokument werden verschiedene Arten von IP-Zugriffskontrolllisten (ACLs) und deren Filtermöglichkeiten für Netzwerkverkehr beschrieben.

Voraussetzungen

Anforderungen

Es sind keine besonderen Voraussetzungen erforderlich, um den Inhalt dieses Dokuments nachzuvollziehen. Die hier beschriebenen Konzepte sind ab Version 8.3 der Cisco IOS®-Software verfügbar. Angaben zur Verfügbarkeit der verschiedenen Zugriffslistenfunktionen finden Sie jeweils auch in den Abschnitten zu den einzelnen Funktionen.

Verwendete Komponenten

In diesem Dokument werden verschiedene Arten von Zugriffskontrolllisten behandelt. Einige Arten sind bereits seit Version 8.3 der Cisco IOS-Software verfügbar, andere wurden erst in späteren Software-Versionen eingeführt. Die Verfügbarkeit ist jeweils im Abschnitt der betreffenden Listenart angegeben.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Convention.

Hintergrundinformationen

In diesem Dokument wird beschrieben, wie IP-Zugriffskontrolllisten (Access Control Lists, ACLs) Netzwerkverkehr filtern können. Es enthält außerdem kurze Beschreibungen der verschiedenen Arten von IP-Zugriffskontrolllisten, Informationen zur Verfügbarkeit der unterschiedlichen Funktionen und ein Beispiel für die konkrete Anwendung in einem Netzwerk.

> **Anmerkung:** RFC 1700 enthält zugewiesene Nummern bekannter Ports.RFC 1918 enthält Adresszuweisung für private Internet, IP-Adressen, die normalerweise nicht im Internet zu sehen sind.

> **Anmerkung:** Nur registrierte Cisco Benutzer können auf interne Informationen zugreifen.

> **Anmerkung:** ACLs können auch verwendet werden, um Datenverkehr für Network Address Translate (NAT) zu definieren, Nicht-IP-Protokolle wie AppleTalk oder IPX zu verschlüsseln oder zu filtern. Eine genauere Erläuterung dieser Funktionen würde jedoch über den

Rahmen dieses Dokuments hinausgehen.

Grundlagen von Zugriffskontrolllisten

Masken

Masken werden mit IP-Adressen in IP-Zugriffskontrolllisten verwendet, um festzulegen, was zugelassen und was abgelehnt werden soll. Masken zur Konfiguration von IP-Adressen auf Schnittstellen beginnen mit "255". Dabei stehen die großen Werte links. (Beispiel: IP-Adresse "10.165.202.129" mit einer Maske "255.255.255.224") Masken für IP-Zugriffskontrolllisten sind das Gegenteil, z. B. Maske 0.0.0.255. Dies wird manchmal als invertierte Maske oder Platzhaltermaske bezeichnet. Wenn der Wert der Maske in eine Binärzahl (0 und 1 s) aufgeteilt wird, bestimmen die Ergebnisse, welche Adressbits bei der Verarbeitung des Datenverkehrs berücksichtigt werden müssen. "0" bedeutet, dass das betreffende Bit der Adresse berücksichtigt werden muss (exakte Übereinstimmung). eine 1 in der Maske ist ein *nicht kümmern*. In der Tabelle unten ist das Prinzip detaillierter dargestellt.

	Beispielmaske
Netzwerkadresse (zu verarbeitender Datenverkehr)	*10.1.1.0*
Maske	*0.0.0.255*
Netzwerkadresse (Binärformat)	*00001010.00000001.00000001.00000000*
Maske (Binärformat)	*00000000.00000000.00000000.11111111*

Anhand der Binärmaske lässt sich erkennen, dass die ersten drei Sätze (Oktette) exakt mit der angegebenen binären Netzwerkadresse (00001010.00000001.00000001) übereinstimmen müssen. Die letzten Zahlen sind *nicht interessiert* (.11111111). Daher ist es *egal*, ob der gesamte Datenverkehr, der mit 10.1.1 beginnt, übereinstimmt, seit dem letzten Oktett. Gilt diese Maske, werden also die Netzwerkadressen "10.1.1.1" bis "10.1.1.255" (10.1.1.x) verarbeitet.

Die invertierte Maske der Zugriffskontrollliste erhalten Sie durch Subtrahieren der normalen Maske von "255.255.255.255". Im Beispiel unten wird die invertierte Maske für die Netzwerkadresse "172.16.1.0" anhand einer normalen Maske "255.255.255.0" ermittelt:

- 255.255.255.255 − 255.255.255.0 (normale Maske) = 0.0.0.255 (invertierte Maske)

Beachten Sie die entsprechenden ACLs.

- Der Wert "0.0.0.0/255.255.255.255" für "source/wildcard" steht für **any.**
- Die Quelle/der Platzhalter von 10.1.1.2/0.0.0.0 entspricht dem **Host 10.1.1.2**.

Zusammenfassen von Netzwerken für Zugriffskontrolllisten

> **Anmerkung:** Subnetzmasken können auch als Notation mit fester Länge angegeben werden. Beispiel: "192.168.10.0/24" steht für "192.168.10.0 255.255.255.0".

In diesem Abschnitt wird beschrieben, wie mehrere Netzwerke zur Optimierung der Zugriffskontrolllisten unter einem einzigen Netzwerk zusammengefasst werden können. Angenommen, es existieren folgende Netzwerke:

```
192.168.32.0/24
192.168.33.0/24
192.168.34.0/24
192.168.35.0/24
192.168.36.0/24
192.168.37.0/24
192.168.38.0/24
192.168.39.0/24
```

Die ersten beiden Oktette und das letzte Oktett jeder Netzwerkadresse sind jeweils gleich. In der Tabelle unten wird erläutert, wie sich diese Netzwerke unter einem einzigen Netzwerk zusammenfassen lassen.

Das dritte Oktett für die vorherigen Netzwerke kann wie in dieser Tabelle dargestellt geschrieben werden, entsprechend der Oktett-Bitposition und dem Adresswert für jedes Bit.

Dezimal	128	64	32	16	8	4	2	1
32	0	0	1	0	0	0	0	0
33	0	0	1	0	0	0	0	1
34	0	0	1	0	0	0	1	0
35	0	0	1	0	0	0	1	1
36	0	0	1	0	0	1	0	0
37	0	0	1	0	0	1	0	1
38	0	0	1	0	0	1	1	0
39	0	0	1	0	0	1	1	1
	M	M	M	M	M	G	G	G

Da die ersten fünf Bits übereinstimmen, lassen sich die acht oben aufgeführten Netzwerke unter einem Netzwerk zusammenfassen ("192.168.32.0/21" oder "192.168.32.0 255.255.248.0"). Alle acht möglichen Kombinationen der drei niederwertigen Bits sind für die betreffenden Netzwerkbereiche relevant. Der Befehl unten definiert eine Zugriffskontrollliste, die dieses Netzwerk zulässt. Wenn Sie "255.255.248.0" (die normale Maske) von "255.255.255.255" subtrahieren, erhalten Sie "0.0.7.255".

```
access-list acl_permit permit ip 192.168.32.0 0.0.7.255
```

Schauen wir uns ein weiteres Beispiel zur Erläuterung an. Angenommen, es existieren folgende Netzwerke:

```
192.168.146.0/24
192.168.147.0/24
192.168.148.0/24
192.168.149.0/24
```

Die ersten beiden Oktette und das letzte Oktett jeder Netzwerkadresse sind jeweils gleich. In der Tabelle unten wird erläutert, wie sich diese Netzwerke zusammenfassen lassen.

Das dritte Oktett für die vorherigen Netzwerke kann wie in dieser Tabelle dargestellt geschrieben werden, entsprechend der Oktett-Bitposition und dem Adresswert für jedes Bit.

Dezimal	128	64	32	16	8	4	2	1
146	1	0	0	1	0	0	1	0
147	1	0	0	1	0	0	1	1
148	1	0	0	1	0	1	0	0
149	1	0	0	1	0	1	0	1
	M	M	M	M	M	?	?	?

Anders als im ersten Beispiel lassen sich diese Netzwerke nicht unter einem einzigen Netzwerk zusammenfassen. Wenn sie unter einem einzigen Netzwerk zusammengefasst würden, würde der Bereich "192.168.144.0/21" lauten, da im dritten Oktett fünf Bits gleich sind. Dieses zusammengefasste Netzwerk 192.168.144.0/21 deckt einen Netzwerkbereich von 192.168.144.0 bis 192.168.151.0 ab. Dazu gehören 192.168.144.0 und 192.168.145.0 192.168.150.0- und 192.168.151.0-Netzwerke sind nicht in der angegebenen Liste der vier Netzwerke enthalten. Um genau diese Netzwerke abzudecken, werden mindestens zwei zusammengefasste Netzwerke benötigt. Die vier oben aufgeführten Netzwerke können unter den folgenden zwei Netzwerken zusammengefasst werden:

- Bei den Netzwerken 192.168.146.x und 192.168.147.x stimmen alle Bits überein, mit Ausnahme des letzten Bits, das *nicht berücksichtigt werden muss*. Diese Netzwerke lassen sich zusammenfassen als "192.168.146.0/23" (oder "192.168.146.0 255.255.254.0").
- Bei den Netzwerken 192.168.148.x und 192.168.149.x stimmen alle Bits überein, mit Ausnahme des letzten Bits, das *nicht berücksichtigt werden muss*. Diese Netzwerke lassen sich zusammenfassen als "192.168.148.0/23" (oder "192.168.148.0 255.255.254.0").

Diese Ausgabe definiert eine zusammengefasste ACL für die zuvor verwendeten Netzwerke.

```
!--- This command is used to allow access access for devices with IP
!--- addresses in the range from 192.168.146.0 to 192.168.147.254. access-list 10 permit
192.168.146.0 0.0.1.255


!--- This command is used to allow access access for devices with IP
!--- addresses in the range from 192.168.148.0 to 192.168.149.254 access-list 10 permit
192.168.148.0 0.0.1.255
```

Verarbeiten von Zugriffskontrolllisten

In den Router fließender Datenverkehr wird mit den Einträgen in der Zugriffskontrollliste abgeglichen, in der Reihenfolge, in der die Einträge auf dem Router hinterlegt sind. Neue Anweisungen werden am Ende der Liste hinzugefügt. Der Router setzt den Abgleich so lange fort, bis eine Übereinstimmung gefunden wird. Erreicht der Router das Ende der Liste, ohne eine Übereinstimmung zu finden, wird der Datenverkehr abgelehnt. Aus diesem Grund müssen Sie die häufig angeklickten Einträge ganz oben in der Liste haben. Für nicht explizit zugelassenen Datenverkehr wird implizit eine "deny"-Anweisung angenommen. Eine ACL mit einem Eintrag und nur einem Deny-Eintrag kann den gesamten Datenverkehr verweigern. Wenn nicht sämtlicher Datenverkehr blockiert werden soll, müssen Sie in einer Zugriffskontrollliste also mindestens eine Anweisung des Typs "permit" definieren. Die beiden nachfolgenden Zugriffskontrolllisten (101 und 102) haben jeweils die gleiche Wirkung.

```
!--- This command is used to permit IP traffic from 10.1.1.0
!--- network to 172.16.1.0 network. All packets with a source
!--- address not in this range will be rejected. access-list 101 permit ip 10.1.1.0 0.0.0.255
172.16.1.0 0.0.0.255


!--- This command is used to permit IP traffic from 10.1.1.0
!--- network to 172.16.1.0 network. All packets with a source
!--- address not in this range will be rejected. access-list 102 permit ip 10.1.1.0 0.0.0.255
172.16.1.0 0.0.0.255
access-list 102 deny ip any any
```

Im nächsten Beispiel ist der letzte Eintrag ausreichend. Die ersten drei Einträge sind nicht erforderlich, da IP TCP, User Datagram Protocol (UDP) und Internet Control Message Protocol (ICMP) umfasst.

```
!--- This command is used to permit Telnet traffic
!--- from machine 10.1.1.2 to machine 172.16.1.1. access-list 101 permit tcp host 10.1.1.2 host
172.16.1.1 eq telnet


!--- This command is used to permit tcp traffic from
!--- 10.1.1.2 host machine to 172.16.1.1 host machine. access-list 101 permit tcp host 10.1.1.2
host 172.16.1.1


!--- This command is used to permit udp traffic from
!--- 10.1.1.2 host machine to 172.16.1.1 host machine. access-list 101 permit udp host 10.1.1.2
host 172.16.1.1


!--- This command is used to permit ip traffic from
!--- 10.1.1.0 network to 172.16.1.10 network. access-list 101 permit ip 10.1.1.0 0.0.0.255
172.16.1.0 0.0.0.255
```

Definieren von Ports und Nachrichtentypen

Sie können nicht nur die Quelle und das Ziel der Zugriffskontrollliste definieren, sondern auch Ports, ICMP-Nachrichtentypen und andere Parameter. Eine gute Informationsquelle für häufig verwendete Ports ist RFC 1700 . Die verschiedenen Typen von ICMP-Nachrichten werden in RFC 792 erläutert.

Der Router kann für einige der häufig verwendeten Ports Beschreibungen anzeigen. Verwenden Sie ein**?**, um Hilfe zu erhalten.

```
access-list 102 permit tcp host 10.1.1.1 host 172.16.1.1 eq ?
  bgp          Border Gateway Protocol (179)
  chargen      Character generator (19)
  cmd          Remote commands (rcmd, 514)
```

Während der Konfiguration wandelt der Router zudem Zahlenwerte in benutzerfreundlichere Werte um. In diesem Beispiel geben Sie die Nummer des ICMP-Nachrichtentyps ein und der Router wandelt die Nummer in einen Namen um.

```
access-list 102 permit icmp host 10.1.1.1 host 172.16.1.1 14
```

wird zu

```
access-list 102 permit icmp host 10.1.1.1 host 172.16.1.1 timestamp-reply
```

Anwenden von Zugriffskontrolllisten

Sie können ACLs definieren und diese dennoch nicht anwenden. Die Zugriffskontrolllisten greifen jedoch erst, wenn sie auf die Schnittstelle des Routers angewendet werden. Es empfiehlt sich,

Zugriffskontrolllisten auf die Schnittstelle anzuwenden, die der Datenverkehrsquelle am nächsten liegt. Wie in diesem Beispiel gezeigt, können Sie beim Blockieren von Datenverkehr von der Quelle zum Ziel eine eingehende ACL auf Router A anstelle einer ausgehenden Liste auf E1 auf Router C anwenden. Eine Zugriffsliste hat eine **adeny ip any** implizit am Ende einer Zugriffsliste. Wenn der Datenverkehr mit einer DHCP-Anfrage zusammenhängt und nicht explizit zulässig ist, wird der Datenverkehr verworfen, da die Quelladresse, wenn Sie die DHCP-Anfrage in IP betrachten, s=0.0.0.0 (Ethernet1/0), d=255.255.255.255, len 604, rcvd 2 UDP src=68, dst=68 lautet. 67. Beachten Sie, dass die Quell-IP-Adresse 0.0.0.0 und die Zieladresse 255.255.255.255 ist. Der Quell-Port ist 68 und das Ziel 67. Daher müssen Sie diese Art von Datenverkehr in der Zugriffsliste zulassen, da der Datenverkehr andernfalls aufgrund der impliziten Ablehnung am Ende der Anweisung verloren geht.

> **Anmerkung:** Damit UDP-Datenverkehr durchgeleitet werden kann, muss dieser von der ACL explizit zugelassen werden.

Definitionen der Begriffe "Eingang", "Ausgang", "Eingehend", "Ausgehend", "Quelle" und "Ziel"

Der Router verwendet die Begriffe "Eingang" (in), "Ausgang" (out), "Quelle" (source) und "Ziel" (destination) als Referenzen. Stellen Sie sich den Datenverkehr auf dem Router wie den Verkehrsfluss auf einer Autobahn vor. Wenn Sie ein Strafverfolgungsbeamter in Pennsylvania wären und einen Lastwagen stoppen wollten, der von Maryland nach New York fährt, dann ist die Quelle des Lastwagens Maryland, und das Ziel des Lastwagens ist New York. Die Straßensperre könnte an der Grenze zwischen Pennsylvania und New York (Ausgang) oder der Grenze zwischen Maryland und Pennsylvania (Eingang) gelten.

Bei einem Router haben die Begriffe jeweils folgende Bedeutung:

- **Ausgang (out): Datenverkehr, der den Router bereits durchflossen hat und die Schnittstelle verlässt.** Die Quelle ist der Punkt, von dem der Datenverkehr stammt (auf der anderen Seite des Routers), das Ziel ist der Punkt, zu dem der Datenverkehr fließt.
- **Eingang (in): Datenverkehr, der an der Schnittstelle ankommt und anschließend durch den Router fließt.** Die Quelle ist der Punkt, von dem der Datenverkehr stammt, das Ziel ist der Punkt, zu dem der Datenverkehr fließt (auf der anderen Seite des Routers).
- **Eingehend (inbound): Wenn eine eingehende Zugriffskontrollliste definiert ist und der Router ein Paket empfängt, führt die Cisco IOS-Software einen Abgleich mit den in der Zugriffsliste als Kriterien definierten Anweisungen ab.** Ist das Paket zulässig, fährt die Software mit der Verarbeitung des Pakets fort. Wird das Paket abgelehnt, verwirft die Software das Paket.
- **Ausgehend (outbound): Wenn eine ausgehende Zugriffskontrollliste definiert ist, wird ein empfangenes Paket zunächst von der Software an die ausgehende Schnittstelle weitergeleitet. Erst dort führt die Software einen Abgleich mit den in der Zugriffsliste als Kriterien definierten Anweisungen ab.** Wenn das Paket zulässig ist, überträgt die Software das Paket weiter. Wird das Paket abgelehnt, verwirft die Software das Paket.

Die Quelle einer Eingangszugriffskontrollliste befindet sich in einem Segment der Schnittstelle, auf

die die Liste angewendet wird. Das Ziel kann jede beliebige andere Schnittstelle sein. Die Quelle einer Ausgangszugriffskontrollliste befindet sich in einem Segment einer anderen Schnittstelle als der Schnittstelle, auf die die Liste angewendet wird. Das Ziel befindet sich auf der Schnittstelle, auf die die Liste angewendet wird.

Bearbeiten von Zugriffskontrolllisten

Bei der Bearbeitung einer Zugriffskontrollliste muss sehr sorgfältig vorgegangen werden. Möchten Sie beispielsweise eine bestimmte Zeile aus einer nummerierten Zugriffskontrollliste wie der unten abgebildeten löschen, wird die gesamte Zugriffskontrollliste gelöscht.

```
!--- The access-list 101 denies icmp from any to any network
!--- but permits IP traffic from any to any network. router#configure terminal
  Enter configuration commands, one per line.  End with CNTL/Z.
  router(config)#access-list 101 deny icmp any any
  router(config)#access-list 101 permit ip any any
  router(config)#^Z

  router#show access-list
  Extended IP access list 101
      deny icmp any any
      permit ip any any
  router#
  *Mar  9 00:43:12.784: %SYS-5-CONFIG_I: Configured from console by console

  router#configure terminal
  Enter configuration commands, one per line.  End with CNTL/Z.
  router(config)#no access-list 101 deny icmp any any
  router(config)#^Z

  router#show access-list
  router#
  *Mar  9 00:43:29.832: %SYS-5-CONFIG_I: Configured from console by console
```

Kopieren Sie die Konfiguration des Routers auf einen TFTP-Server oder in einen Text-Editor wie Notepad, um nummerierte Zugriffskontrolllisten zu bearbeiten. Nehmen Sie dann alle Änderungen vor, und kopieren Sie die Konfiguration zurück auf den Router.

Sie können auch Folgendes tun:

```
router#configure terminal
  Enter configuration commands, one per line.
  router(config)#ip access-list extended test

!--- Permits IP traffic from 10.2.2.2 host machine to 10.3.3.3 host machine. router(config-ext-
nacl)#permit ip host 10.2.2.2 host 10.3.3.3

!--- Permits www traffic from 10.1.1.1 host machine to 10.5.5.5 host machine. router(config-ext-
nacl)#permit tcp host 10.1.1.1 host 10.5.5.5 eq www

!--- Permits icmp traffic from any to any network. router(config-ext-nacl)#permit icmp any any

!--- Permits dns traffic from 10.6.6.6 host machine to 10.10.10.0 network. router(config-ext-
nacl)#permit udp host 10.6.6.6 10.10.10.0 0.0.0.255 eq domain
  router(config-ext-nacl)#^Z
  1d00h: %SYS-5-CONFIG_I: Configured from console by consoles-l

  router#show access-list
```

```
  Extended IP access list test
      permit ip host 10.2.2.2 host 10.3.3.3
      permit tcp host 10.1.1.1 host 10.5.5.5 eq www
      permit icmp any any
      permit udp host 10.6.6.6 10.10.10.0 0.0.0.255 eq domain
```

Alle Löschungen werden aus der Zugriffskontrollliste entfernt, und alle Einfügungen werden am Ende der Zugriffskontrollliste hinzugefügt.

```
router#configure terminal
   Enter configuration commands, one per line.  End with CNTL/Z.
   router(config)#ip access-list extended test

!--- ACL entry deleted. router(config-ext-nacl)#no permit icmp any any

!--- ACL entry added. router(config-ext-nacl)#permit gre host 10.4.4.4 host 10.8.8.8
   router(config-ext-nacl)#^Z
   1d00h: %SYS-5-CONFIG_I: Configured from console by consoles-l

   router#show access-list
   Extended IP access list test
       permit ip host 10.2.2.2 host 10.3.3.3
       permit tcp host 10.1.1.1 host 10.5.5.5 eq www
       permit udp host 10.6.6.6 10.10.10.0 0.0.0.255 eq domain
       permit gre host 10.4.4.4 host 10.8.8.8
```

In Cisco IOS können Sie nummerierten Standardzugriffskontrolllisten oder nummerierten erweiterten Zugriffskontrolllisten Zugriffskontrolllistenzeilen auch über die zugehörige Sequenznummer hinzufügen. Das nachfolgende Beispiel beschreibt die Konfiguration.

Konfigurieren Sie eine erweiterte Zugriffskontrollliste wie folgt:

```
Router(config)#access-list 101 permit tcp any any
Router(config)#access-list 101 permit udp any any
Router(config)#access-list 101 permit icmp any any
Router(config)#exit
Router#
```

Führen Sie den Befehl show access-list aus, um die ACL-Einträge anzuzeigen. Die Sequenznummern sollten ebenfalls in der Ausgabe angezeigt werden ("10", "20" und "30" im Beispiel unten).

```
Router#show access-list
Extended IP access list 101
    10 permit tcp any any
    20 permit udp any any
    30 permit icmp any any
```

Fügen Sie den Eintrag für die Zugriffsliste 101 mit der Sequenznummer 5 hinzu.

Beispiel 1:

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list extended 101
Router(config-ext-nacl)#5 deny tcp any any eq telnet
Router(config-ext-nacl)#exit
Router(config)#exit
Router#
```

In der Ausgabe des Befehls access-list wird die Zugriffskontrollliste mit der Sequenznummer 5 als erster Eintrag zur Zugriffsliste 101 hinzugefügt.

```
Router#show access-list
Extended IP access list 101
    5 deny tcp any any eq telnet
    10 permit tcp any any
    20 permit udp any any
    30 permit icmp any any
Router#
```

Beispiel 2:

```
internetrouter#show access-lists
Extended IP access list 101
    10 permit tcp any any
    15 permit tcp any host 172.16.2.9
    20 permit udp host 172.16.1.21 any
    30 permit udp host 172.16.1.22 any

internetrouter#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
internetrouter(config)#ip access-list extended 101
internetrouter(config-ext-nacl)#18 per tcp any host 172.16.2.11
internetrouter(config-ext-nacl)#^Z

internetrouter#show access-lists
Extended IP access list 101
    10 permit tcp any any
    15 permit tcp any host 172.16.2.9
    18 permit tcp any host 172.16.2.11
    20 permit udp host 172.16.1.21 any
    30 permit udp host 172.16.1.22 any
internetrouter#
```

Die Konfiguration einer Standardzugriffsliste funktioniert ähnlich:

```
internetrouter(config)#access-list 2 permit 172.16.1.2
internetrouter(config)#access-list 2 permit 172.16.1.10
internetrouter(config)#access-list 2 permit 172.16.1.11

internetrouter#show access-lists
Standard IP access list 2
    30 permit 172.16.1.11
    20 permit 172.16.1.10
    10 permit 172.16.1.2

internetrouter(config)#ip access-list standard 2
internetrouter(config-std-nacl)#25 per 172.16.1.7
internetrouter(config-std-nacl)#15 per 172.16.1.16

internetrouter#show access-lists
Standard IP access list 2
    15 permit 172.16.1.16
    30 permit 172.16.1.11
    20 permit 172.16.1.10
    25 permit 172.16.1.7
    10 permit 172.16.1.2
```

Der Hauptunterschied einer Standard-Zugriffsliste besteht darin, dass das Cisco IOS einen Eintrag in absteigender Reihenfolge der IP-Adresse hinzufügt, nicht in einer Sequenznummer.

Im Beispiel unten sehen Sie die verschiedenen Einträge, beispielsweise den Eintrag, mit dem eine IP-Adresse (192.168.100.0) oder die Netzwerke (10.10.10.0) zugelassen werden.

```
internetrouter#show access-lists
Standard IP access list 19
    10 permit 192.168.100.0
    15 permit 10.10.10.0, wildcard bits 0.0.0.255
    19 permit 10.101.110.0, wildcard bits 0.0.0.255
    25 deny any
```

Fügen Sie den Eintrag der Zugriffsliste 2 hinzu, um die IP-Adresse "172.22.1.1" als zulässig zu definieren:

```
internetrouter(config)#ip access-list standard 2
internetrouter(config-std-nacl)#18 permit 172.22.1.1
```

Dieser Eintrag wird am Anfang der Liste hinzugefügt, damit statt dem Netzwerk diese spezifische IP-Adresse Priorität erhält.

```
internetrouter#show access-lists
Standard IP access list 19
    10 permit 192.168.100.0
    18 permit 172.22.1.1
    15 permit 10.10.10.0, wildcard bits 0.0.0.255
    19 permit 10.101.110.0, wildcard bits 0.0.0.255
    25 deny   any
```

> **Anmerkung:** Die oben beschriebenen Zugriffskontrolllisten werden auf Sicherheits-Appliances wie der ASA/PIX Firewall nicht unterstützt.

Richtlinien für die Änderung von auf Crypto Maps angewendeten Zugriffslisten

- Wenn Sie eine aktuelle Zugriffslistenkonfiguration hinzufügen, müssen Sie die Crypto Map nicht entfernen. Ein direktes Hinzufügen ohne Entfernen der Crypto Map wird unterstützt und ist zulässig.
- Wenn Sie einen Zugriffslisteneintrag in einer aktuellen Zugriffsliste ändern oder löschen müssen, müssen Sie die Crypto Map von der Schnittstelle entfernen. Nehmen Sie nach dem Entfernen der Crypto Map alle gewünschten Änderungen vor, und fügen Sie die Crypto Map wieder hinzu. Änderungen wie das Löschen einer Zugriffsliste ohne Entfernen der Crypto Map werden nicht unterstützt und können zu unvorhersehbarem Verhalten führen.

Fehlerbehebung

Wie entferne ich eine Zugriffskontrollliste von einer Schnittstelle?

Wechseln Sie in den Konfigurationsmodus, und geben Sie wie im folgenden Beispiel gezeigt **no gefolgt vom Befehl access-group ein, um eine Zugriffskontrollliste von einer Schnittstelle zu entfernen.**

```
interface <interface-name> no ip access-group <acl-number> {in|out}
```

Was kann ich tun, wenn zu viel Datenverkehr abgelehnt wird?

Wenn zu viel Datenverkehr abgelehnt wird, sollten Sie sich zunächst die Logik Ihrer Liste anschauen oder versuchen, eine weitere, umfassendere Liste zu definieren und anzuwenden. Der Befehl **show ip access-lists gibt einen Wert für die Paketanzahl zurück, aus dem sich ablesen lässt, für welchen Eintrag in der Zugriffskontrollliste Übereinstimmungen ermittelt werden.** Das Keyword log am Ende der einzelnen Zugriffskontrolllisteneinträge gibt neben Informationen zum Port auch die Nummer der Zugriffskontrollliste zurück sowie Angaben dazu, ob ein Paket zugelassen oder abgelehnt wurde.

> **Anmerkung:** Das Keyword log-input steht ab Version 11.2 der Cisco IOS-Software zur Verfügung. Ebenso steht es in bestimmten Software-Versionen auf Basis von Version 11.1 der Cisco IOS-Software zur Verfügung, die speziell für den Serviceanbieter-Markt entwickelt wurden. Ältere Software unterstützt dieses Keyword nicht. Bei der Verwendung dieses Keyword müssen gegebenenfalls die Eingangsschnittstelle und die Quell-MAC-Adresse angegeben werden.

Wie kann ich eine Fehlersuche auf Paketebene durchführen, wenn ein Cisco Router verwendet wird?

Das nachfolgende Verfahren erläutert, wie Sie zur Fehlersuche vorgehen müssen. Vergewissern Sie sich zunächst, dass derzeit keine Zugriffskontrolllisten angewendet werden, dass eine Zugriffskontrollliste vorhanden ist und dass Fast Switching nicht deaktiviert ist.

> **Anmerkung:** Gehen Sie bei der Fehlersuche in Systemen mit hohem Datenverkehrsaufkommen äußerst vorsichtig vor. Verwenden Sie eine Zugriffskontrollliste, um die Fehlersuche auf bestimmten Datenverkehr zu konzentrieren. Aber stellen Sie den Prozess und den Verkehrsfluss sicher.

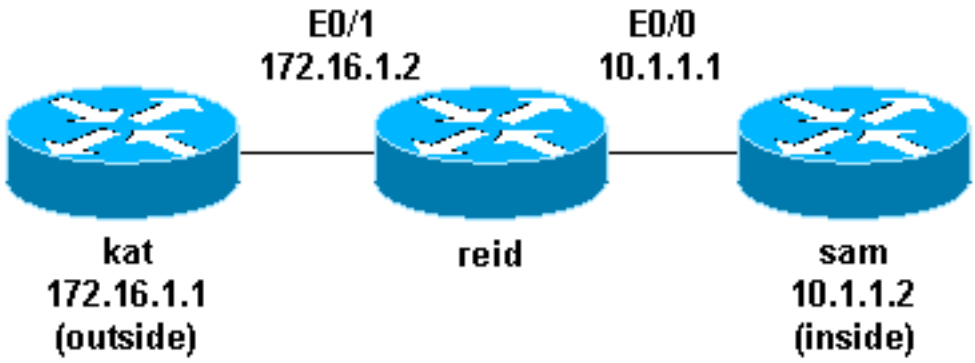
1. Verwenden Sie **den Befehl access-**list, um die gewünschten Daten zu erfassen.Im Beispiel unten wird die Datenerfassung für die Zieladresse "10.2.6.6" oder die Quelladresse "10.2.6.6" eingerichtet.
   ```
   access-list 101 permit ip any host 10.2.6.6
   access-list 101 permit ip host 10.2.6.6 any
   ```
2. Deaktivieren Sie Fast Switching auf allen betroffenen Schnittstellen. Wenn Fast Switching nicht deaktiviert wird, sehen Sie nur das erste Paket.
   ```
   configure terminal
   interface
   ```
3. Führen Sie den Befehl **terminal monitor** im privilegierten Modus (Enable-Modus) aus, um die Ausgabe des Befehls debug sowie Systemfehlermeldungen für das aktuelle Terminal und die aktuelle Sitzung abzurufen.
4. Verwenden Sie den Befehl **debug ip packet 101** oder den Befehl **debug ip packet 101 detail**, um den Debugvorgang zu starten.
5. Führen Sie den Befehl **no debug all im privilegierten Modus und den Befehl interface configuration aus, um die Fehlersuche zu stoppen.**
6. Starten Sie die Zwischenspeicherung neu.

```
configure terminal
interface
```

Arten von IP-Zugriffskontrolllisten

In diesem Abschnitt des Dokuments werden die verschiedenen Arten von Zugriffskontrolllisten beschrieben.

Netzwerkdiagramm



Standardzugriffskontrolllisten

Standardzugriffskontrolllisten sind die älteste Art von Zugriffskontrollliste. Sie reichen zurück bis zur Cisco IOS Software Version 8.3. Standard-ACLs steuern den Datenverkehr durch den Vergleich der Quelladresse der IP-Pakete mit den in der ACL konfigurierten Adressen.

Die Befehlssyntax für eine Standardzugriffskontrollliste hat folgendes Format:

```
access-list <access-list-number> {permit|deny} {host|source source-wildcard|any}
```

In allen Softwareversionen kann *access-list-number* jeder Wert im Bereich von 1 bis 99 sein. In Version 12.0.1 der Cisco IOS-Software verwenden standardmäßige Zugriffskontrolllisten zusätzliche Nummern (1300 bis 1999). Diese zusätzlichen Nummern werden als erweiterte IP-Zugriffskontrolllisten bezeichnet. Seit Version 11.2 der Cisco IOS-Software besteht die Möglichkeit, das Listenattribut *name in Standardzugriffskontrolllisten zu verwenden.*

Die Einstellung *source/source-wildcard* von 0.0.0.0/255.255.255.255 kann als **any** angegeben werden. Der Platzhalter kann weggelassen werden, wenn er ausschließlich aus Nullen besteht. Daher ist Host 10.1.1.2 0.0.0.0 mit Host 10.1.1.2 identisch.

Nachdem die Zugriffskontrollliste definiert wurde, muss sie auf die Schnittstelle (eingehend oder ausgehend) angewendet werden. In den frühen Versionen der Software war "out" der Standardwert, wenn weder das Keyword "out" noch das Keyword "in" angegeben waren. In späteren Versionen der Software muss die Richtung angegeben werden.

```
interface <interface-name>
 ip access-group number {in|out}
```

Im Beispiel unten wird eine Standardzugriffskontrollliste verwendet, um sämtlichen Datenverkehr außer dem Datenverkehr von Quelle "10.1.1.x" zu blockieren.

```
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip access-group 1 in
!
access-list 1 permit 10.1.1.0 0.0.0.255
```

Erweiterte Zugriffskontrolllisten

In Version 8.3 der Cisco IOS-Software wurden erweiterte ACLs eingeführt. Diese steuern den Datenverkehr durch den Vergleich der Quell- und Zieladressen der IP-Pakete mit den in der ACL konfigurierten Adressen.

Die Befehlssyntax für eine erweiterte Zugriffskontrollliste hat das unten dargestellte Format. Zeilen werden hier aus Platzgründen umbrochen.

IP

```
access-list access-list-number
     [dynamic dynamic-name [timeout minutes]]
     {deny|permit} protocol source source-wildcard destination destination-wildcard [precedence
precedence]
     [tos tos] [log|log-input] [time-range time-range-name]
```

ICMP

```
access-list access-list-number
     [dynamic dynamic-name [timeout minutes]]
     {deny|permit} icmp source source-wildcard destination destination-wildcard
     [icmp-type [icmp-code] |icmp-message] [precedence precedence] [tos tos] [log|log-input]
     [time-range time-range-name]
```

TCP

```
access-list access-list-number
     [dynamic dynamic-name [timeout minutes]]
     {deny|permit} tcp source source-wildcard [operator [port]]
     destination destination-wildcard [operator [port]]
     [established] [precedence precedence] [tos tos]
     [log|log-input] [time-range time-range-name]
```

UDP

```
access-list access-list-number
     [dynamic dynamic-name [timeout minutes]]
     {deny|permit} udp source source-wildcard [operator [port]]
     destination destination-wildcard [operator [port]]
     [precedence precedence] [tos tos] [log|log-input]
```

```
[time-range time-range-name]
```

In allen Softwareversionen kann *access-list-number* 100 bis 199 sein. In Version 12.0.1 der Cisco IOS-Software verwenden erweiterte Zugriffskontrolllisten zusätzliche Nummern (2000 bis 2699). Diese zusätzlichen Nummern werden als erweiterte IP-Zugriffskontrolllisten bezeichnet. Seit Version 11.2 der Cisco IOS-Software besteht die Möglichkeit, das Listenattribut *name in erweiterten Zugriffskontrolllisten zu verwenden.*

Der Wert "0.0.0.0/255.255.255.255" kann als **any angegeben werden.** Nachdem die Zugriffskontrollliste definiert wurde, muss sie auf die Schnittstelle (eingehend oder ausgehend) angewendet werden. In den frühen Versionen der Software war "out" der Standardwert, wenn weder das Keyword "out" noch das Keyword "in" angegeben waren. In späteren Versionen der Software muss die Richtung angegeben werden.

```
interface <interface-name>
 ip access-group {number|name} {in|out}
```

Diese erweiterte ACL ermöglicht den Datenverkehr im Netzwerk 10.1.1.x (intern) und den Empfang von Ping-Antworten von außen. Gleichzeitig werden unerwünschte Pings von externen Benutzern verhindert, wodurch der restliche Datenverkehr zugelassen wird.

```
interface Ethernet0/1
 ip address 172.16.1.2 255.255.255.0
 ip access-group 101 in
!
access-list 101 deny icmp any 10.1.1.0 0.0.0.255 echo access-list 101 permit ip any 10.1.1.0
0.0.0.255
```

> **Anmerkung:** Einige Anwendungen müssen Pings im Rahmen einer Keep-alive-Funktion ausführen. Dies gilt beispielsweise für Anwendungen zur Netzwerkverwaltung. In diesem Fall können Sie die eingehenden Pings einschränken, die in zulässigen/abgelehnten IPs blockiert werden, oder Sie können die Genauigkeit erhöhen.

Lock-and-Key-Zugriffskontrolllisten (dynamische Zugriffskontrolllisten)

Lock-and-Key-Zugriffskontrolllisten werden auch als dynamische Zugriffskontrolllisten bezeichnet und wurden in Version 11.1 der Cisco IOS-Software eingeführt. Diese Funktion ist von Telnet, Authentifizierung (lokal oder remote) und erweiterten Zugriffskontrolllisten abhängig.

Der erste Schritt bei der Einrichtung einer Lock-and-Key-Konfiguration ist die Anwendung einer erweiterten Zugriffskontrollliste zur Blockierung des Datenverkehrsflusses durch den Router. Benutzer, die auf das Netzwerk hinter dem Router zugreifen möchten, werden so lange von der erweiterten Zugriffskontrollliste blockiert, bis sie sich per Telnet beim Router authentifiziert haben. Die Telnet-Verbindung wird dann getrennt, und der vorhandenen erweiterten Zugriffskontrollliste wird eine dynamische Zugriffskontrollliste mit einem Eintrag hinzugefügt. Dadurch wird der Datenverkehr für einen bestimmten Zeitraum zugelassen. Dabei können sowohl Leerlaufzeitüberschreitungen als auch absolute Zeitüberschreitungen definiert werden.

Hier sehen Sie das Format der Befehlssyntax für eine Lock-and-Key-Konfiguration mit lokaler Authentifizierung:

```
username <user-name> password <password>
!
interface <interface-name>
 ip access-group {number|name} {in|out}
```

Nach der Authentifizierung wird die aus einem einzigen Eintrag bestehende Zugriffskontrollliste in diesem Befehl der bereits vorhandenen Zugriffskontrollliste dynamisch hinzugefügt.

```
access-list access-list-number dynamic name {permit|deny} [protocol]
{source source-wildcard|any} {destination destination-wildcard|any}
[precedence precedence][tos tos][established] [log|log-input]
[operator destination-port|destination port]

line vty <line_range>
login local
```

Nachfolgend ein einfaches Beispiel für das Lock-and-Key-Verfahren:

```
username test password 0 test

!--- Ten (minutes) is the idle timeout. username test autocommand access-enable host timeout 10
!
interface Ethernet0/0
  ip address 10.1.1.1 255.255.255.0
  ip access-group 101 in
!
access-list 101 permit tcp any host 10.1.1.1 eq telnet

!--- 15 (minutes) is the absolute timeout. access-list 101 dynamic testlist timeout 15 permit ip
10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
!
line vty 0 4
 login local
```

Nachdem der Benutzer an Adresse "10.1.1.2" eine Telnet-Verbindung zu "10.1.1.1" hergestellt hat, wird die dynamische Zugriffskontrollliste angewendet. Anschließend wird die Verbindung geschlossen, und der Benutzer erhält Zugriff auf das Netzwerk "172.16.1.x".

Benannte IP-Zugriffskontrolllisten

Benannte IP-Zugriffskontrolllisten wurden in Version 11.2 der Cisco IOS-Software eingeführt. So können Standard- und erweiterten Zugriffskontrolllisten Namen anstelle von Nummern zugewiesen werden.

Die Befehlssyntax für eine benannte IP-Zugriffskontrollliste hat folgendes Format:

```
ip access-list {extended|standard} name
```

Hier ein Beispiel für TCP:

```
{permit|deny} tcp source source-wildcard [operator [port]] destination destination-wildcard
[operator [port]] [established] [precedence precedence] [tos tos] [log] [time-range time-range-
name]
```

Im Beispiel unten wird eine benannte Zugriffskontrollliste verwendet, um sämtlichen Datenverkehr außer der Telnet-Verbindung von Host "10.1.1.2" zu Host "172.16.1.1" zu blockieren:

```
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip access-group in_to_out in
!
ip access-list extended in_to_out
 permit tcp host 10.1.1.2 host 172.16.1.1 eq telnet
```

Reflexive Zugriffskontrolllisten

In Version 11.3 der Cisco IOS-Software wurden reflexive Zugriffskontrolllisten eingeführt, mit denen IP-Pakete basierend auf Sitzungsinformationen der oberen Ebene gefiltert werden können. Sie werden in der Regel verwendet, um als Reaktion auf im Router geöffnete Sitzungen ausgehenden Datenverkehr passieren zu lassen und eingehenden Datenverkehr zu beschränken.

Reflexive Zugriffskontrolllisten können nur zusammen mit erweiterten benannten IP-Zugriffskontrolllisten definiert werden. Sie können nicht in Kombination mit nummerierten oder standardmäßigen benannten IP-Zugriffskontrolllisten oder mit Zugriffskontrolllisten auf Basis anderer Protokolle definiert werden. Eine Kombination von reflexiven Zugriffskontrolllisten mit anderen standardmäßigen oder statischen erweiterten Zugriffskontrolllisten ist zulässig.

Mit der folgenden Befehlssyntax lassen sich unterschiedliche reflexive Zugriffskontrolllisten umsetzen:

```
interface <interface-name>
 ip access-group {number|name} {in|out}
!
ip access-list extended <name>
 permit protocol any any reflect name [timeoutseconds]
!
ip access-list extended <name>
 evaluate <name>
```

Dies ist ein Beispiel für die Zulässigkeit des ausgehenden und eingehenden ICMP-Verkehrs, während nur TCP-Verkehr zugelassen wird, der von innen initiiert wurde, während anderer Verkehr abgelehnt wird.

```
ip reflexive-list timeout 120
!
interface Ethernet0/1
 ip address 172.16.1.2 255.255.255.0
 ip access-group inboundfilters in
 ip access-group outboundfilters out
!
ip access-list extended inboundfilters
 permit icmp 172.16.1.0 0.0.0.255 10.1.1.0 0.0.0.255
 evaluate tcptraffic

!--- This ties the reflexive ACL part of the outboundfilters ACL,
!--- called tcptraffic, to the inboundfilters ACL. ip access-list extended outboundfilters
 permit icmp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
```

```
 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 reflect tcptraffic
```

Zeitbasierte Zugriffskontrolllisten mit Zeiträumen

Zeitbasierte Zugriffskontrolllisten wurden in Version 12.0.1.T der Cisco IOS-Software eingeführt. Sie sind in ihrer Funktionsweise erweiterten Zugriffskontrolllisten ähnlich, ermöglichen jedoch eine zeitbasierte Zugriffskontrolle. Hierzu wird ein Zeitraum erstellt, der bestimmte Zeiten am Tag oder in der Woche festlegt, zu denen die zeitbasierten Zugriffskontrolllisten implementiert werden sollen. Der Zeitraum erhält einen Namen als Bezeichner und wird dann durch eine Funktion referenziert. Die Zeitbeschränkungen werden also auf die Funktion selbst angewendet. Der Zeitraum basiert auf der Systemuhr des Routers. Auch die Router-Uhr kann verwendet werden, doch arbeitet die Funktion am zuverlässigsten bei NTP-Synchronisierung (Network Time Protocol).

Hier sehen Sie die Befehle für eine zeitbasierte Zugriffskontrollliste:

```
!--- Defines a named time range. time-range time-range-name

!--- Defines the periodic times. periodic days-of-the-week hh:mm to [days-of-the-week] hh:mm

!--- Or, defines the absolute times. absolute [start time date] [end time date]

!--- The time range used in the actual ACL. ip access-list name|number time-rangename_of_time-
range
```

Im Beispiel unten werden Telnet-Verbindungen von innerhalb des Netzwerks nach außen montags, mittwochs und freitags während der Geschäftszeiten zugelassen:

```
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip access-group 101 in
!
access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet time-range
EVERYOTHERDAY
!
time-range EVERYOTHERDAY
 periodic Monday Wednesday Friday 8:00 to 17:00
```

Kommentierte Einträge in IP-Zugriffskontrolllisten

Kommentierte Einträge in IP-Zugriffskontrolllisten wurden in Version 12.0.2.T der Cisco IOS-Software eingeführt. Kommentare machen Zugriffskontrolllisten übersichtlicher und können in standardmäßigen sowie erweiterten IP-Zugriffskontrolllisten verwendet werden.

Die Befehlssyntax für eine kommentierte benannte IP-Zugriffskontrollliste sieht wie folgt aus:

```
ip access-list {standard|extended} <access-list-name> remark remark
```

Die Befehlssyntax für eine kommentierte nummerierte IP-Zugriffskontrollliste sieht wie folgt aus:

```
access-list <access-list-number> remark remark
```

Dies ist ein Beispiel für Kommentare innerhalb einer nummerierten ACL.

```
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip access-group 101 in
!
access-list 101 remark permit_telnet
access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 eq telnet
```

Kontextbasierte Zugriffskontrolle

Die kontextbasierte Zugriffskontrolle (CBAC, Context-Based Access Control) wurde in Version 12.0.5.T der Cisco IOS-Software eingeführt und setzt voraus, dass die Cisco IOS Firewall-Funktion aktiviert ist. CBAC überprüft den Datenverkehr, der durch die Firewall fließt, um Statusinformationen von TCP- und UDP-Sitzungen zu erfassen und zu verwalten. Anhand dieser Statusinformationen werden vorübergehende Öffnungen in den Zugriffskontrolllisten der Firewall eingerichtet. Konfigurieren Sie Prüflisten in Richtung der Initiierung des Datenverkehrs, um Rückverkehr und zusätzliche Datenverbindungen für zulässige Sitzungen zuzulassen, Sitzungen, die aus dem geschützten internen Netzwerk stammen.

Die Syntax für CBAC sieht wie folgt aus:

```
ip inspect name inspection-name protocol [timeoutseconds]
```

Das Beispiel unten zeigt, wie Sie mit CBAC ausgehenden Datenverkehr überprüfen können. Die erweiterte Zugriffskontrollliste 111 blockiert normalerweise sämtlichen zurückfließenden Datenverkehr außer ICMP-Datenverkehr, ohne dass CBAC Öffnungen für den zurückfließenden Datenverkehr einrichtet.

```
ip inspect name myfw ftp timeout 3600
ip inspect name myfw http timeout 3600
ip inspect name myfw tcp timeout 3600
ip inspect name myfw udp timeout 3600
ip inspect name myfw tftp timeout 3600
! interface Ethernet0/1 ip address 172.16.1.2 255.255.255.0 ip access-group 111 in ip inspect
myfw out !
access-list 111 deny icmp any 10.1.1.0 0.0.0.255 echo access-list 111 permit icmp any 10.1.1.0
0.0.0.255
```

Authentifizierungsproxy

Der Authentifizierungsproxy wurde in Version 12.0.5.T der Cisco IOS-Software eingeführt. Er setzt voraus, dass die Cisco IOS Firewall-Funktion aktiviert ist. Der Authentifizierungsproxy wird verwendet, um eingehende Benutzer, ausgehende Benutzer oder sowohl eingehende als auch ausgehende Benutzer zu authentifizieren. Benutzer, die normalerweise von einer Zugriffskontrollliste blockiert würden, können einen Browser öffnen, um sich über die Firewall bei einem TACACS+- oder RADIUS-Server zu authentifizieren. Nach der Authentifizierung übergibt der Server zusätzliche Zugriffskontrolllisteneinträge an den Router, damit die Benutzer zugelassen werden.

Der Authentifizierungsproxy arbeitet ähnlich wie Lock-and-Key-Zugriffskontrolllisten (dynamische

Zugriffskontrollisten). Es gibt jedoch folgende Unterschiede:

- Lock-and-Key-Zugriffskontrollisten werden durch eine Telnet-Verbindung zum Router aktiviert. Der Authentifizierungsproxy wird aktiviert, wenn HTTP-Datenverkehr durch den Router fließt.
- Der Authentifizierungsproxy muss einen externen Server verwenden.
- Der Authentifizierungsproxy unterstützt das Hinzufügen mehrerer dynamischer Listen. Das Lock-and-Key-Verfahren unterstützt lediglich das Hinzufügen einer einzigen solchen Liste.
- Für den Authentifizierungsproxy wird eine absolute Zeitüberschreitung definiert, jedoch keine Leerlaufzeitüberschreitung. Beim Lock-and-Key-Verfahren werden beide Arten von Zeitüberschreitung definiert.

Beispiele für einen Authentifizierungsproxy finden Sie im Cisco Secure Integrated Software Configuration Cookbook.

Turbozugriffskontrollisten

Turbozugriffskontrollisten wurden in Version 12.1.5.T der Cisco IOS-Software eingeführt und sind ausschließlich auf den Plattformen 7200 und 7500 sowie auf anderen High-End-Plattformen verfügbar. Turbozugriffskontrollisten wurden entwickelt, um die Verarbeitung von Zugriffskontrollisten effizienter zu machen und damit die Routerleistung zu verbessern.

Verwenden Sie den Befehl **access-list compiled für Turbozugriffskontrollisten.** Hier ein Beispiel für eine kompilierte Zugriffskontrolliste:

```
access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 eq telnet
access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 eq ftp
access-list 101 permit udp host 10.1.1.2 host 172.16.1.1 eq syslog
access-list 101 permit udp host 10.1.1.2 host 172.16.1.1 eq tftp
access-list 101 permit udp host 10.1.1.2 host 172.16.1.1 eq ntp
```

Nachdem eine Standardzugriffskontrolliste oder erweiterte Zugriffskontrolliste definiert wurde, können Sie die Liste mit dem Befehl **global configuration kompilieren.**

```
!--- Tells the router to compile. access-list compiled
!
interface Ethernet0/1
 ip address 172.16.1.2 255.255.255.0

!--- Applies to the interface.  ip access-group 101 in
```

Der Befehl **show acccess-list compiled gibt die Statistik der Zugriffskontrolliste zurück.**

Verteilte zeitbasierte Zugriffskontrollisten

Verteilte zeitbasierte Zugriffskontrollisten wurden in Version 12.2.2.T der Cisco IOS-Software eingeführt, um zeitbasierte Zugriffskontrollisten auf VPN-fähigen Routern der Serie 7500 zu implementieren. Vor der Einführung der Funktion für verteilte zeitbasierte Zugriffskontrollisten wurden zeitbasierte Zugriffskontrollisten auf Linecards für Cisco Router der Serie 7500 nicht unterstützt. Wurden dennoch zeitbasierte Zugriffskontrollisten konfiguriert, verhielten die Listen sich wie normale Zugriffskontrollisten. War eine Schnittstelle auf einer Linecard mit zeitbasierten Zugriffskontrollisten konfiguriert, wurden alle an die Schnittstelle geleiteten Pakete nicht über die

Linecard weiterverteilt, sondern zwecks Verarbeitung zum Routing-Prozessor umgeleitet.

Die Syntax für verteilte zeitbasierte ACLs ist dieselbe wie für zeitbasierte ACLs mit den zusätzlichen Befehlen in Bezug auf den Status der IPC-Nachrichten (Inter Processor Communication) zwischen dem Routingprozessor und der Linecard.

```
debug time-range ipc
show time-range ipc
clear time-range ipc
```

Empfangen Sie ACLs

Empfangszugriffskontrolllisten erhöhen die Sicherheit auf Cisco 12000-Routern, indem sie den GRP (Gigabit Route Processor) des Routers gegen unnötigen und potenziell bösartigen Datenverkehr absichern. Empfangszugriffskontrolllisten wurden als besondere Ausnahme für die Wartungsbeschränkungen in Version 12.0.21S2 der Cisco IOS-Software hinzugefügt und dann in Version 12.0(22)S integriert. Siehe GSR: Receive Access Control ListsWeitere Informationen.

Infrastrukturschutz-Zugriffskontrolllisten

Infrastruktur-ACLs werden verwendet, um das Risiko und die Effektivität direkter Infrastrukturangriffe zu minimieren, indem nur autorisierter Datenverkehr an die Infrastrukturausrüstung gesendet wird, während der gesamte andere Transitdatenverkehr zugelassen wird. Siehe das Schützen Ihres Kernes: Infrastructure Protection Access Control Lists (Core-Schutz: Zugriffskontrolllisten für Infrastrukturschutz).

Übertragungszugriffskontrolllisten

Übertragungszugriffskontrolllisten werden verwendet, um die Netzwerksicherheit zu erhöhen. Sie lassen ausschließlich nur solchen Datenverkehr in Netzwerke fließen, der erforderlich ist. Siehe Durchfahrt-Zugriffskontrolllisten: Filtering at Your Edge (Übertragungszugriffskontrolllisten: Filtern am Edge).

Zugehörige Informationen

- Konfigurieren häufig verwendeter IP-ACLs
- RFC 1700
- RFC 1918
- Support-Seite zum Thema Zugriffslisten
- Cisco IOS Firewall
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.