Fehlerbehebung bei Cisco IOS Firewall-Konfigurationen

Inhalt

Einführung

Dieses Dokument enthält Informationen zur Fehlerbehebung bei Cisco IOS® Firewall-Konfigurationen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Fehlerbehebung

Hinweis: Lesen Sie vor dem Ausgabe von **Debug**-Befehlen unter Wichtige Informationen zu Debug-Befehlen nach.

- Um eine Zugriffsliste umzukehren (zu entfernen), setzen Sie ein "Nein" vor den Befehl **access-group** im Schnittstellenkonfigurationsmodus:

```
int
```

- Wenn zu viel Datenverkehr verweigert wird, studieren Sie die Logik Ihrer Liste, oder versuchen Sie, eine zusätzliche, umfassendere Liste zu definieren, und wenden Sie sie dann stattdessen an. Beispiel:

```
access-list # permit tcp any any
access-list # permit udp any any
access-list # permit icmp any any
int
```

- Der Befehl **show ip access-lists** zeigt an, welche Zugriffslisten angewendet werden und welcher Datenverkehr von ihnen abgelehnt wird. Wenn Sie die Anzahl der vor und nach dem Fehlschlagen des Vorgangs abgelehnten Pakete mit der Quell- und Ziel-IP-Adresse betrachten, erhöht sich diese Zahl, wenn die Zugriffsliste Datenverkehr blockiert.
- Wenn der Router nicht stark geladen ist, kann das Debuggen auf Paketebene in der erweiterten Zugriffsliste oder der Zugriffsliste für die IP-Prüfung erfolgen. Wenn der Router stark ausgelastet ist, wird der Datenverkehr über den Router verlangsamt. Verwenden Sie Diskretion mit Debugbefehlen.Fügen Sie der Schnittstelle vorübergehend den Befehl **no ip route-cache** hinzu:

```
int
```

  Im Aktivierungs- (aber nicht im Konfigurationsmodus):

```
term mon
debug ip packet # det
```

  erzeugt eine ähnliche Ausgabe wie die folgende:

```
*Mar 1 04:38:28.078: IP: s=10.31.1.161 (Serial0), d=171.68.118.100 (Ethernet0),
   g=10.31.1.21, len 100, forward
*Mar 1 04:38:28.086: IP: s=171.68.118.100 (Ethernet0), d=9.9.9.9 (Serial0), g=9.9.9.9,
   len 100, forward
```

- Erweiterte Zugriffslisten können auch mit der Option "log" am Ende der verschiedenen Anweisungen verwendet werden:

```
access-list 101 deny ip host 171.68.118.100 host 10.31.1.161 log
access-list 101 permit ip any any
```

  Sie sehen daher auf dem Bildschirm Meldungen über zugelassenen und abgelehnten Datenverkehr:

```
*Mar 1 04:44:19.446: %SEC-6-IPACCESSLOGDP: list 111 permitted icmp 171.68.118.100
```

```
   -> 10.31.1.161 (0/0), 15 packets
*Mar  1 03:27:13.295: %SEC-6-IPACCESSLOGP: list 118 denied tcp 171.68.118.100(0)
   -> 10.31.1.161(0), 1 packet
```

- Wenn die Liste ip inspect verdächtig ist, generiert der Befehl **debug ip inspect <type_of_traffic>** Ausgaben wie diese Ausgabe:

```
Feb 14 12:41:17 10.31.1.52 56: 3d05h: CBAC* sis 258488 pak 16D0DC TCP P ack 3195751223
   seq 3659219376(2) (10.31.1.5:11109) => (12.34.56.79:23)
Feb 14 12:41:17 10.31.1.52 57: 3d05h: CBAC* sis 258488 pak 17CE30 TCP P ack 3659219378
   seq 3195751223(12) (10.31.1.5:11109) <= (12.34.56.79:23)
```

Weitere Informationen zu diesen Befehlen sowie weitere Informationen zur Fehlerbehebung finden Sie unter Troubleshooting Authentication Proxy.

Zugehörige Informationen

- Produktunterstützung für Cisco IOS Firewall
- Technischer Support und Dokumentation - Cisco Systems