DHCP-Client oder -Server mit ZBF-Router-Konfiguration

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie ein Router, der als DHCP-Server (Dynamic Host Control Protocol) oder DHCP-Client fungiert, mit der ZBF-Funktion (Zone-Based Firewall) konfiguriert wird. Da DHCP und ZBF in der Regel gleichzeitig aktiviert sind, stellen diese Konfigurationstipps sicher, dass diese Funktionen richtig interagieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie die zonenbasierte Firewall der Cisco IOS®-Software kennen. Weitere Informationen finden Sie im Design- und Anwendungshandbuch für zonenbasierte Firewall-Richtlinien.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

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 Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Informationen zu Funktionen

Wenn ZBF auf einem IOS-Router aktiviert ist, ist jeder Datenverkehr zur Kernzone (d. h. Datenverkehr, der an die Verwaltungsebene des Routers gerichtet ist) im IOS 15.x-Codezug standardmäßig zulässig.

Wenn Sie eine Richtlinie für eine Zone (z. B. "inside" oder "outside") zur Kernzone (out-to-self-Richtlinie) oder umgekehrt (self-to-out-Richtlinie) erstellt haben, müssen Sie den zulässigen Datenverkehr in den Richtlinien, die mit diesen Zonen verknüpft sind, explizit definieren. Verwenden Sie die Aktion inspect oder pass, um den zulässigen Datenverkehr zu definieren.

Datenanalyse

DHCP verwendet Broadcast User Datagram Protocol (UDP)-Pakete, um den DHCP-Prozess abzuschließen. Zonenbasierte Firewall-Konfigurationen, die die Aktion zum Überprüfen dieser Broadcast-UDP-Pakete festlegen, werden möglicherweise vom Router verworfen, und der DHCP-Prozess schlägt möglicherweise fehl. Möglicherweise wird Ihnen auch diese Protokollmeldung angezeigt:

```
%FW-6-DROP_PKT: Dropping udp session 0.0.0.0:68 255.255.255.255:67 on zone-pair
self-out class dhcp with ip ident 0
```

Weitere Informationen finden Sie unter der Cisco Bug-ID CSCso53376, "ZBF inspect does not work for broadcast traffic."

Um dieses Problem zu vermeiden, ändern Sie die zonenbasierte Firewall-Konfiguration so, dass die Aktion "pass" anstelle der Aktion "inspect" auf den DHCP-Datenverkehr angewendet wird.

> **Hinweis**: Dies ist nur erforderlich, wenn eine Richtlinie auf die Kernzone des Routers angewendet wird.

Zonenbasierte Firewall als DHCP-Client mit Weiterleitungsaktion für UDP-Datenverkehr

Konfigurieren

Bei dieser Beispielkonfiguration wird der Satz für die Weiterleitungsaktion anstelle der Aktion "inspect" (Einlesen) in der Richtlinienzuordnung für den gesamten UDP-Datenverkehr vom oder

zum Router verwendet.

```
zone security outside
zone security inside

interface Ethernet0/1
zone-member security outside
interface Ethernet0/2
zone-member security inside

class-map type inspect match-all dhcp
match protocol udp

policy-map type inspect out-to-self
class type inspect dhcp
pass
class class-default
drop
policy-map type inspect self-to-out
class type inspect dhcp
pass
class class-default
drop

zone-pair security out-to-self source outside destination self
service-policy type inspect out-to-self
zone-pair security self-to-out source self destination outside
service-policy type inspect self-to-out
```

Überprüfung

Überprüfen Sie die Syslogs, um sicherzustellen, dass der Router erfolgreich eine DHCP-Adresse erhalten hat.

Wenn sowohl die Out-to-Self- als auch die Self-to-Out-Richtlinien für die Weiterleitung von UDP-Datenverkehr konfiguriert sind, kann der Router eine IP-Adresse vom DHCP beziehen, wie in diesem Syslog dargestellt:

```
%DHCP-6-ADDRESS_ASSIGN: Interface Ethernet1/0 assigned DHCP address 192.168.1.5,
mask 255.255.255.0
```

Wenn nur die Out-to-Self-Zonenrichtlinie für die Weiterleitung von UDP-Datenverkehr konfiguriert ist, kann der Router auch eine IP-Adresse von DHCP beziehen. Das Syslog wird erstellt:

```
%DHCP-6-ADDRESS_ASSIGN: Interface Ethernet1/0 assigned DHCP address 192.168.1.6,
mask 255.255.255.0
```

Wenn nur die Self-to-Out-Zonenrichtlinie für die Weiterleitung von UDP-Datenverkehr konfiguriert ist, kann der Router eine IP-Adresse von DHCP beziehen, und das Syslog wird erstellt:

```
%DHCP-6-ADDRESS_ASSIGN: Interface Ethernet1/0 assigned DHCP address 192.168.1.7,
mask 255.255.25
```

Zonenbasierte Firewall mit Weiterleitungsaktion für DHCP-Datenverkehr

Konfigurieren

In dieser Beispielkonfiguration wird veranschaulicht, wie der gesamte UDP-Datenverkehr aus einer Zone in die Kernzone des Routers mit Ausnahme von DHCP-Paketen verhindert wird. Verwenden Sie eine Zugriffsliste mit spezifischen Ports, um nur DHCP-Datenverkehr zuzulassen. In diesem Beispiel werden der UDP-Port 67 und der UDP-Port 68 als übereinstimmend festgelegt. Auf eine Klassenzuordnung, die auf die Zugriffsliste verweist, wird die Übergabeaktion angewendet.

```
access-list extended 111
 10 permit udp any any eq 67

access-list extended 112
 10 permit udp any any eq 68

class-map type inspect match-any self-to-out
match access-group 111
class-map type inspect match-any out-to-self
match access-group 112

zone security outside
zone security inside

interface Ethernet0/1
zone-member security outside
interface Ethernet0/2
zone-member security inside

policy-map type inspect out-to-self
class type inspect out-to-self
pass
class class-default
drop
policy-map type inspect self-to-out
class type inspect self-to-out
pass
class class-default
drop

zone-pair security out-to-self source outside destination self
service-policy type inspect out-to-self
zone-pair security self-to-out source self destination outside
service-policy type inspect self-to-out
```

Überprüfung

Überprüfen Sie die Ausgabe des Befehls **show policy-map type inspect zone-pair sessions,** um sicherzustellen, dass der Router den DHCP-Datenverkehr über die Zone-Firewall zulässt. In diesem Beispiel zeigen die hervorgehobenen Leistungsindikatoren an, dass Pakete durch die Zonen-Firewall geleitet werden. Wenn diese Zähler 0 sind, liegt ein Problem mit der Konfiguration vor, oder die Pakete erreichen den Router nicht zur Verarbeitung.

```
router#show policy-map type inspect zone-pair sessions

policy exists on zp out-to-self
Zone-pair: out-to-self
```

```
Service-policy inspect : out-to-self
Class-map: out-to-self (match-any)
Match: access-group 112
3 packets, 924 bytes
30 second rate 0 bps
Pass
6 packets, 1848 bytes

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes

policy exists on zp self-to-out
Zone-pair: self-to-out
Service-policy inspect : self-to-out
Class-map: self-to-out (match-any)
Match: access-group 111
6 packets, 3504 bytes
30 second rate 0 bps
Pass
6 packets, 3504 bytes

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes
```

Szenario für falsche Konfigurationen

Dieses Beispielszenario zeigt, was passiert, wenn der Router nicht richtig konfiguriert ist, um die Aktion "inspect" für DHCP-Datenverkehr anzugeben. In diesem Szenario ist der Router als DHCP-Client konfiguriert. Der Router sendet eine DHCP-Ermittlungsnachricht, um zu versuchen, eine IP-Adresse zu erhalten. Die zonenbasierte Firewall ist so konfiguriert, dass sie diesen DHCP-Datenverkehr prüft. Dies ist ein Beispiel für die ZBF-Konfiguration:

```
zone security outside
zone security inside

interface Ethernet0/1
zone-member security outside

interface Ethernet0/2
zone-member security inside

class-map type inspect match-all dhcp
match protocol udp

policy-map type inspect out-to-self
class type inspect dhcp
inspect
class class-default
drop
policy-map type inspect self-to-out
class type inspect dhcp
inspect
class class-default
drop

zone-pair securiy out-to-self source outside destination self
```

```
service-policy type inspect out-to-self
zone-pair security self-to-out source self destination outside
service-policy type inspect self-to-out
```

Wenn die Self-to-Out-Richtlinie mit der Aktion "Inspect" für den UDP-Datenverkehr konfiguriert wird, wird das DHCP-Erkennungspaket verworfen, und das Syslog wird erstellt:

```
%FW-6-DROP_PKT: Dropping udp session 0.0.0.0:68 255.255.255.255:67 on zone-pair
self-out class dhcp with ip ident 0
```

Wenn sowohl die Richtlinie für die automatische als auch die Richtlinie für die automatische Prüfung mit der Aktion "inspect" für den UDP-Datenverkehr konfiguriert sind, wird das DHCP-Erkennungspaket verworfen, und das Syslog wird erstellt:

```
%FW-6-DROP_PKT: Dropping udp session 0.0.0.0:68 255.255.255.255:67 on zone-pair
self-out class dhcp with ip ident 0
```

Wenn für die Out-to-Self-Richtlinie die Aktion "inspect" aktiviert ist und für die Self-to-Out-Richtlinie die Aktion "pass" für UDP-Datenverkehr aktiviert ist, wird das DHCP-Angebotspaket nach dem Senden des DHCP-Discovery-Pakets verworfen, und dieses Syslog wird erstellt:

```
%FW-6-DROP_PKT: Dropping udp session 192.168.1.1:67 255.255.255.255:68 on zone-pair
out-self class dhcp with ip ident 0
```

Router als DHCP-Server

Wenn die interne Schnittstelle des Routers als DHCP-Server fungiert und die Clients, die eine Verbindung zur internen Schnittstelle herstellen, die DHCP-Clients sind, ist dieser DHCP-Verkehr standardmäßig zulässig, wenn es keine Richtlinien für interne Interaktionen oder für interne Interaktionen gibt.

Wenn jedoch eine dieser Richtlinien vorhanden ist, müssen Sie eine Weiterleitungsaktion für den relevanten Datenverkehr (UDP-Port 67 oder UDP-Port 68) in der Zonenpaar-Dienstrichtlinie konfigurieren.

Fehlerbehebung

Für diese Konfigurationen sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

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.