Grundlegendes Richtlinienrouting

Inhalt

Einführung

Richtlinienbasiertes Routing bietet ein Tool für die Weiterleitung und Weiterleitung von Datenpaketen, das auf Richtlinien basiert, die von Netzwerkadministratoren definiert wurden. Dies ist eine Möglichkeit, Routing-Protokoll-Entscheidungen durch die Richtlinie zu überschreiben. Richtlinienbasiertes Routing umfasst einen Mechanismus zur selektiven Anwendung von Richtlinien basierend auf Zugriffslisten, Paketgröße oder anderen Kriterien. Zu den ergriffenen Maßnahmen können das Routing von Paketen auf benutzerdefinierten Routen, das Festlegen der Rangfolge, der Art der Service-Bits usw. gehören.

In diesem Dokument wird eine Firewall verwendet, um private Adressen der Adresse 10.0.0.0/8 in im Internet routbare Adressen des Subnetzes 172.16.255.0/24 zu übersetzen. Eine visuelle Erklärung finden Sie im Diagramm unten.

Weitere Informationen finden Sie unter Richtlinienbasiertes Routing.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Hardware- oder Softwareversionen beschränkt.

Die in diesem Dokument angegebenen Informationen basieren auf den unten aufgeführten Software- und Hardwareversionen.

- Cisco IOS® Softwareversion 12.3(3)

- Cisco Router der Serie 2500

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

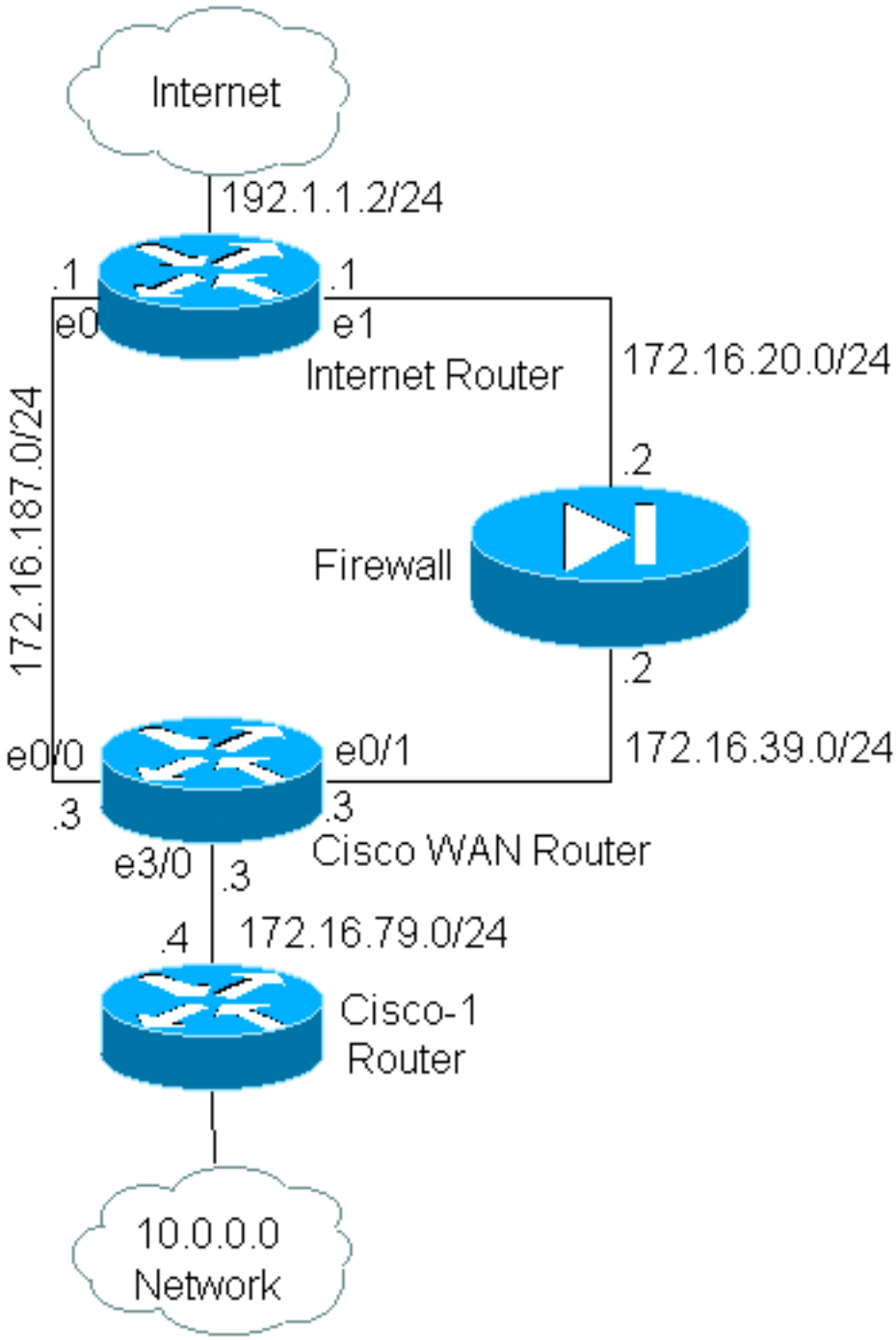
Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Konfigurationen

In diesem Beispiel führen bei normalem Routing alle Pakete vom Netzwerk 10.0.0.0/8 zum Internet den Pfad durch das SchnittstellenEthernet 0/0 des Cisco WAN-Routers (über das Subnetz 172.16.187.0/24), da es sich um den besten Pfad mit der niedrigsten Metrik handelt. Bei richtlinienbasiertem Routing sollen diese Pakete den Pfad über die Firewall zum Internet durchlaufen. Das normale Routing-Verhalten muss durch Konfigurieren des Richtlinien-Routings überschrieben werden. Die Firewall übersetzt alle Pakete aus dem Netzwerk 10.0.0.0/8, die ins Internet gehen. Dies ist jedoch für das Richtlinienrouting nicht erforderlich.

Netzwerkdiagramm



Konfiguration für Firewall

Die nachfolgende Firewall-Konfiguration bietet eine vollständige Übersicht. Sie ist jedoch nicht Teil des in diesem Dokument erläuterten Richtlinienrouting-Problems. Die Firewall in diesem Beispiel könnte problemlos durch ein PIX oder ein anderes Firewall-Gerät ersetzt werden.

```
!
ip nat pool net-10 172.16.255.1 172.16.255.254 prefix-length 24
ip nat inside source list 1 pool net-10
!
interface Ethernet0
 ip address 172.16.20.2 255.255.255.0
 ip nat outside
!
interface Ethernet1
```

```
 ip address 172.16.39.2 255.255.255.0
 ip nat inside
!
router eigrp 1
 redistribute static
 network 172.16.0.0
 default-metric 10000 100 255 1 1500
!
ip route 172.16.255.0 255.255.255.0 Null0
access-list 1 permit 10.0.0.0 0.255.255.255
!
end
```

Weitere Informationen zu Befehlen im Zusammenhang mit der **IP-Adressierung und** den Dienstbefehlen finden Sie unter IP-Adressierung und unter Dienstbefehle.

In diesem Beispiel führt der Cisco WAN-Router ein Richtlinien-Routing aus, um sicherzustellen, dass IP-Pakete, die vom Netzwerk 10.0.0.0/8 stammen, über die Firewall gesendet werden. Die nachfolgende Konfiguration enthält eine Zugriffslistenanweisung, die Pakete aus dem Netzwerk 10.0.0.0/8 an die Firewall sendet.

Konfiguration für Cisco_WAN_Router

```
!
interface Ethernet0/0
 ip address 172.16.187.3 255.255.255.0
 no ip directed-broadcast
!
interface Ethernet0/1
 ip address 172.16.39.3 255.255.255.0
 no ip directed-broadcast
!
interface Ethernet3/0
 ip address 172.16.79.3 255.255.255.0
 no ip directed-broadcast
 ip policy route-map net-10
!
router eigrp 1
 network 172.16.0.0
!

access-list 111 permit ip 10.0.0.0 0.255.255.255 any
!
route-map net-10 permit 10
 match ip address 111
 set interface Ethernet0/1
!
route-map net-10 permit 20
!
end
```

Weitere Informationen zu **route-map**-Befehlen finden Sie in der Dokumentation des **route-map**-Befehls.

Hinweis: Das **log**-Schlüsselwort im Befehl **access-list** wird vom PBR nicht unterstützt. Wenn das **log**-Schlüsselwort konfiguriert ist, werden keine Treffer angezeigt.

Konfiguration für Cisco-1 Router

```
!
version 12.3

!

interface Ethernet0

!-- Interface connecting to 10.0.0.0 network ip address 10.1.1.1 255.0.0.0 ! interface Ethernet1
!-- Interface connecting to Cisco_Wan_Router ip address 172.16.79.4 255.255.255.0 ! router eigrp
1 network 10.0.0.0 network 172.16.0.0 no auto-summary ! !---Output Suppressed
```

Konfiguration für Internet_Router

```
!
version 12.3

!
interface Ethernet1

!-- Interface connecting to Firewall ip address 172.16.20.1 255.255.255.0 interface Serial0 !---
Interface connecting to Internet ip address 192.1.1.2 255.255.255.0 clockrate 64000 no fair-
queue ! interface Ethernet0 !--- Interface connecting to Cisco_Wan_Router ip address
172.16.187.1 255.255.255.0 ! ! router eigrp 1 redistribute static !--- Redistributing the static
default route for other routers to reach Internet network 172.16.0.0 no auto-summary ! ip
classless ip route 0.0.0.0 0.0.0.0 192.1.1.1 !-- Static default route pointing to the router
connected to Internet !---Output Suppressed
```

Beim Testen dieses Beispiels wurde ein Ping, der von 10.1.1.1 auf dem Cisco-1-Router unter Verwendung des **erweiterten Ping-**Befehls stammt, an einen Host im Internet gesendet. In diesem Beispiel wurde 192.1.1.1 als Zieladresse verwendet. Um zu sehen, was auf dem Internet-Router geschieht, wurde das schnelle Switching deaktiviert, während der Befehl **debug ip packet 101 detail** verwendet wurde.

Warnung: Die Verwendung des Befehls **debug ip packet detail** auf einem Produktions-Router kann zu einer hohen CPU-Auslastung führen, die zu einer erheblichen Leistungsminderung oder einem Netzwerkausfall führen kann. Wir empfehlen, dass Sie vor der Verwendung von Debugbefehlen den Abschnitt Using the Debug Command (Verwenden des Befehls Ping und Traceroute) sorgfältig lesen.

Hinweis: Die **Zugriffsliste 101 lässt icmp jede beliebige** Anweisung zu, um die **Debug-IP-Paket-**Ausgabe zu filtern. Ohne diese Zugriffsliste kann der Befehl **debug ip packet** so viel Ausgabe an die Konsole generieren, dass der Router abstürzt. Verwenden Sie erweiterte Zugriffskontrolllisten, wenn Sie PBR konfigurieren. Wenn keine ACL konfiguriert ist, um die Anpassungskriterien festzulegen, wird der gesamte Datenverkehr richtliniengesteuert.

```
Results of ping from Cisco_1 to 192.1.1.1/internet taken from Internet_Router:
Packet never makes it to Internet_Router

Cisco_1# ping
Protocol [ip]:
Target IP address: 192.1.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.1
Type of service [0]:
```

```
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
.....
Success rate is 0 percent (0/5)
```

Wie Sie sehen, wurde das Paket nie zum Internet-Router gebracht. Die folgenden Debugbefehle wurden vom Cisco WAN-Router übernommen und zeigen, warum dies der Fall war.

```
Debug commands run from Cisco_WAN_Router:
"debug ip policy"
*Mar  1 00:43:08.367: IP: s=10.1.1.1 (Ethernet3/0), d=192.1.1.1, len 100, policy match
*Mar  1 00:43:08.367: IP: route map net-10, item 10, permit
 !--- Packet with source address belonging to 10.0.0.0/8 network !--- is matched by route-map
"net-10" statement 10. *Mar 1 00:43:08.367: IP: s=10.1.1.1 (Ethernet3/0), d=192.1.1.1
(Ethernet0/1), len 100, policy routed *Mar 1 00:43:08.367: Ethernet3/0 to Ethernet0/1 192.1.1.1
!--- matched packets previously are forwarded out of interface !--- ethernet 0/1 by the set
command.
```

Der Richtlinieneintrag 10 für das Paket wurde wie erwartet in der net-10-Richtlinienzuordnung zugeordnet. Warum also ist das Paket nicht zum Internet-Router gelangt?

```
"debug arp"
*Mar  1 00:06:09.619: IP ARP: creating incomplete entry for IP address: 192.1.1.1 interface
Ethernet0/1
*Mar  1 00:06:09.619: IP ARP: sent req src 172.16.39.3 00b0.64cb.eab1,
                 dst 192.1.1.1 0000.0000.0000 Ethernet0/1
*Mar  1 00:06:09.635: IP ARP rep filtered src 192.1.1.1 0010.7b81.0b19, dst 172.16.39.3
                 00b0.64cb.eab1 wrong cable, interface Ethernet0/1

Cisco_Wan_Router# show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.16.39.3             -   00b0.64cb.eab1  ARPA   Ethernet0/1
Internet  172.16.39.2             3   0010.7b81.0b19  ARPA   Ethernet0/1
Internet  192.1.1.1               0   Incomplete      ARPA
```

Das zeigt die **Debug-**ARP-Ausgabe. Der Cisco WAN-Router versucht, die Anweisungen zu erfüllen, und versucht, die Pakete direkt auf die Ethernet 0/1-Schnittstelle zu übertragen. Dies erfordert, dass der Router eine ARP-Anfrage (Address Resolution Protocol) für die Zieladresse 192.1.1.1 sendet, von der der Router erkennt, dass sie sich nicht auf dieser Schnittstelle befindet. Daher ist der ARP-Eintrag für diese Adresse "Incomplete" (Unvollständig), wie der Befehl **show arp** zeigt. Ein Kapselungsfehler tritt dann auf, da der Router das Paket nicht ohne ARP-Eintrag auf die Leitung legen kann.

Wenn wir die Firewall als Next-Hop festlegen, können wir dieses Problem verhindern und die Routing-Map wie vorgesehen durchführen:

```
Config changed on Cisco_WAN_Router:
!
route-map net-10 permit 10
 match ip address 111
 set ip next-hop 172.16.39.2
```

```
!
```

Mit dem gleichen Befehl **debug ip packet 101 detail** auf dem Internet-Router wird nun festgestellt, dass das Paket den richtigen Pfad verwendet. Wir können auch sehen, dass das Paket von der Firewall in 172.16.255.1 übersetzt wurde und dass der Rechner, an den gepingt wird, 192.1.1.1, wie folgt geantwortet hat:

```
Cisco_1# ping
Protocol [ip]:
Target IP address: 192.1.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/70/76 ms

Results of ping from Cisco_1 to 192.1.1.1/internet taken from Internet_Router:
Internet_Router#
*Mar  1 00:06:11.619: IP: s=172.16.255.1 (Ethernet1), d=192.1.1.1 (Serial0), g=192.1.1.1, len
100, forward
*Mar  1 00:06:11.619:     ICMP type=8, code=0
!--- Packets sourced from 10.1.1.1 are getting translated to 172.16.255.1 by !--- the Firewall
before it reaches the Internet_Router. *Mar 1 00:06:11.619: *Mar 1 00:06:11.619: IP: s=192.1.1.1
(Serial0), d=172.16.255.1 (Ethernet1), g=172.16.20.2, len 100, forward *Mar 1 00:06:11.619: ICMP
type=0, code=0 !--- Packets returning from Internet arrive with the destination !--- address
172.16.255.1 before it reaches the Firewall. *Mar 1 00:06:11.619:
```

Der Befehl **debug ip policy** auf dem Cisco WAN-Router zeigt, dass das Paket an die Firewall 172.16.39.2 weitergeleitet wurde:

Debug-Befehle werden von Cisco_WAN_Router ausgeführt

```
"debug ip policy"
*Mar  1 00:06:11.619: s=10.1.1.1 (Ethernet3/0), d=192.1.1.1, len 100, policy match
*Mar  1 00:06:11.619: IP: route map net-10, item 20, permit
*Mar  1 00:06:11.619: s=10.1.1.1 (Ethernet3/0), d=192.1.1.1 (Ethernet0/1), len 100, policy
routed
*Mar  1 00:06:11.619: Ethernet3/0 to Ethernet0/1 172.16.39.2
```

Richtlinienbasiertes Routing für verschlüsselten Datenverkehr

Leiten Sie den entschlüsselten Datenverkehr an eine Loopback-Schnittstelle weiter, um den verschlüsselten Datenverkehr basierend auf der Richtlinienweiterleitung weiterzuleiten, und führen Sie dann PBR auf dieser Schnittstelle durch. Wenn der verschlüsselte Datenverkehr über einen VPN-Tunnel weitergeleitet wird, `deaktivieren Sie ip cef` auf der Schnittstelle, und beenden Sie den VPN-Tunnel.

Zugehörige Informationen

- Support-Seite für IP-Routing
- NAT-Support-Seite
- Tools und Ressourcen für technischen Support
- Richtlinienbasiertes Routing
- Cisco IOS-Technologien
- Technischer Support und Dokumentation - Cisco Systems