Informazioni su Policy Routing

Sommario

Introduzione

Il routing basato su policy fornisce uno strumento per l'inoltro e l'instradamento dei pacchetti di dati basato su policy definite dagli amministratori di rete. In effetti, è un modo per fare in modo che la policy sostituisca le decisioni sul protocollo di routing. Il routing basato su criteri include un meccanismo per applicare in modo selettivo criteri basati sull'elenco degli accessi, sulle dimensioni dei pacchetti o su altri criteri. Le azioni eseguite possono includere il routing dei pacchetti su route definite dall'utente, l'impostazione della precedenza, il tipo di bit del servizio e così via.

In questo documento viene usato un firewall per convertire gli indirizzi privati 10.0.0.0/8 in indirizzi instradabili su Internet appartenenti alla subnet 172.16.255.0/24. Per una spiegazione visiva, vedere il diagramma seguente.

per ulteriori informazioni, fare riferimento a Policy-Based Routing.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni hardware o software.

Le informazioni fornite in questo documento si basano sulle versioni software e hardware riportate di seguito.

- Software Cisco IOS® versione 12.3(3)

- Cisco serie 2500 Router

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

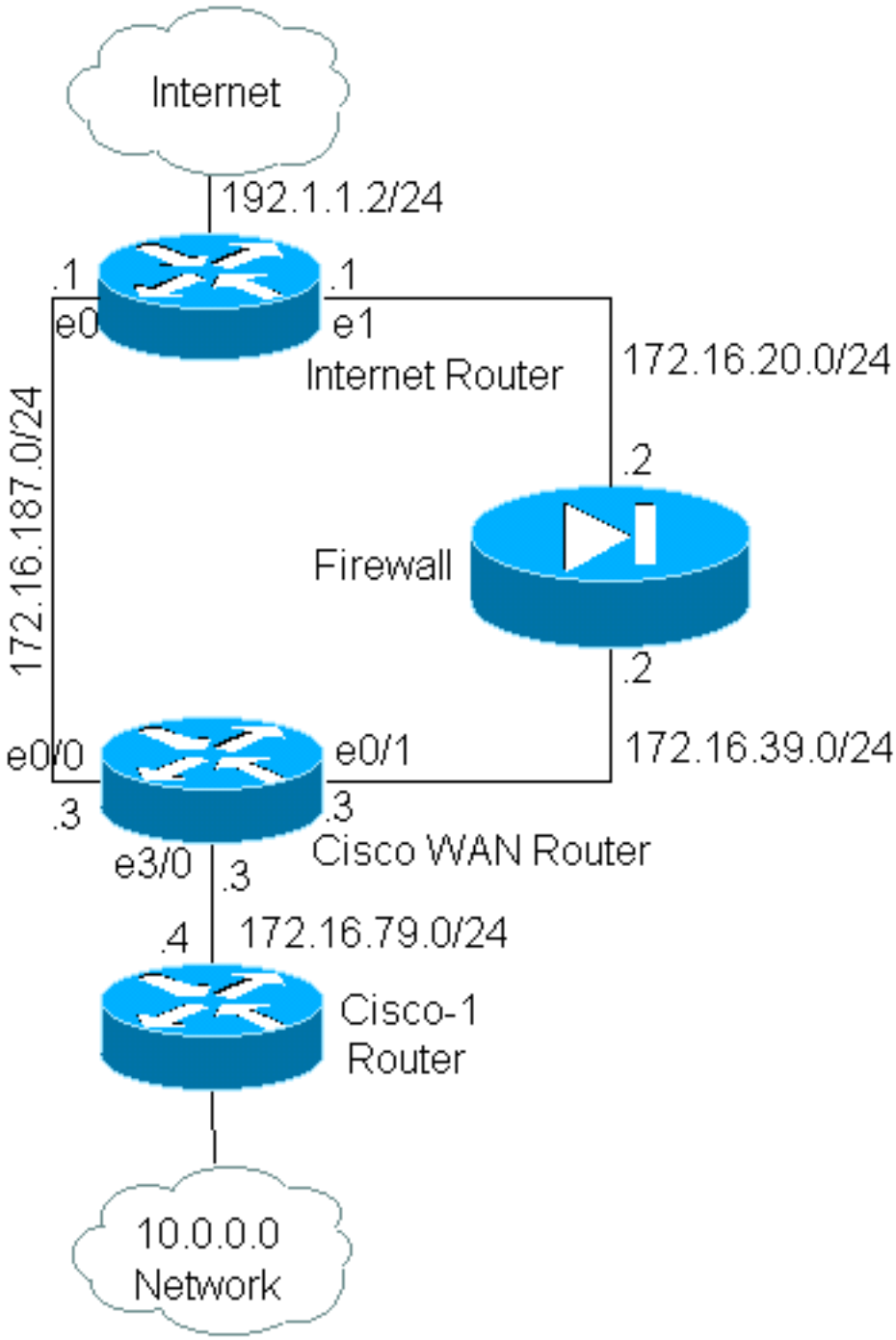
Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Configurazioni

In questo esempio, con il routing normale, tutti i pacchetti dalla rete 10.0.0.0/8 a Internet prendono il percorso attraverso l'interfaccia ethernet 0/0 di Cisco WAN Router (tramite la subnet 172.16.187.0/24) perché è il percorso migliore con il valore minimo. Con il routing basato su policy, si desidera che i pacchetti seguano il percorso attraverso il firewall verso Internet, è necessario ignorare il normale comportamento di routing configurando il routing delle policy. Il firewall converte tutti i pacchetti della rete 10.0.0.0/8 diretti a Internet, ma questa operazione non è necessaria per il corretto funzionamento del routing delle policy.

Esempio di rete



Configurazione per il firewall

La configurazione firewall riportata di seguito è inclusa per fornire un'immagine completa. Tuttavia, non fa parte del problema di routing delle policy illustrato in questo documento. In questo esempio, il firewall potrebbe essere facilmente sostituito da un PIX o da un altro dispositivo firewall.

```
!
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
```

Per ulteriori informazioni sui comandi relativi a **ip nat**, fare riferimento a Indirizzamento IP e comandi di servizio

Nell'esempio, il router WAN Cisco esegue il routing delle policy per garantire che i pacchetti IP provenienti dalla rete 10.0.0.0/8 vengano inviati attraverso il firewall. La configurazione seguente contiene un'istruzione access list che invia al firewall pacchetti provenienti dalla rete 10.0.0.0/8.

Configurazione per 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
```

Per ulteriori informazioni sui comandi relativi alla **mappa** delle **route,** consultare la documentazione del comando **route-map**.

Nota: la parola chiave **log** nel comando **access-list** non è supportata da PBR. Se è stata configurata la parola chiave **log**, non verrà visualizzato alcun risultato.

Configurazione per 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
```

Configurazione per 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
```

Nell'esempio, è stato inviato un ping da 10.1.1.1 sul router Cisco-1, usando il comando **ping** esteso, a un host su Internet. Nell'esempio, l'indirizzo di destinazione è 192.1.1.1. Per verificare cosa stava succedendo sul router Internet, l'opzione di commutazione veloce è stata disattivata mentre era in uso il comando **debug ip packet 101 detail**.

Avviso: l'uso del comando **debug ip packet detail** su un router di produzione può causare un elevato utilizzo della CPU e quindi un grave calo delle prestazioni o un'interruzione della rete. Si consiglia di leggere attentamente la sezione Uso del comando debug di Informazioni sui comandi ping e traceroute prima di usare i comandi di debug.

Nota: l'**access-list 101 permette l'icmp con qualsiasi** istruzione per filtrare l'output del **pacchetto ip di debug**. Senza questo elenco degli accessi, il comando **debug ip packet** può generare così tanto output sulla console che il router si blocca. Usare gli ACL estesi quando si configura il PBR. Se non si configura alcun ACL per stabilire i criteri di corrispondenza, tutto il traffico viene instradato tramite policy.

```
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)
```

Come si può vedere, il pacchetto non è mai arrivato al router Internet. I comandi di debug seguenti, tratti dal router Cisco WAN, mostrano il motivo per cui si è verificato.

```
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.
```

Il pacchetto corrisponde alla voce 10 nella mappa dei criteri net-10, come previsto. Perché il pacchetto non è arrivato al router Internet?

```
"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
```

L'output del comando **debug arp** visualizza questa condizione. Il router WAN Cisco tenta di eseguire le operazioni programmate e tenta di caricare i pacchetti direttamente sull'interfaccia Ethernet 0/1. A tal fine, è necessario che il router invii una richiesta ARP (Address Resolution Protocol) per l'indirizzo di destinazione 192.1.1.1, che il router capisce non essere su questa interfaccia. La voce ARP per questo indirizzo è quindi "Incomplete", come mostrato dal comando **show arp**. Si verifica quindi un errore di incapsulamento quando il router non è in grado di trasferire il pacchetto sul cavo senza alcuna voce ARP.

Specificando il firewall come hop successivo, è possibile evitare questo problema e fare in modo che la mappa del percorso funzioni come previsto:

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

Se si usa lo stesso comando **debug ip packet 101 detail** sul router Internet, il pacchetto sta prendendo il percorso corretto. Possiamo anche notare che il pacchetto è stato tradotto dal firewall

alla versione 172.16.255.1, e che il computer su cui viene eseguito il ping, 192.1.1.1, ha risposto:

```
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:
```

Il comando **debug ip policy** sul router WAN Cisco mostra che il pacchetto è stato inoltrato al firewall, 172.16.39.2:

Comandi di debug eseguiti da Cisco_WAN_Router

```
"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
```

Routing basato su criteri per il traffico crittografato

Inoltrare il traffico decrittografato a un'interfaccia di loopback per indirizzare il traffico crittografato in base al routing delle policy, quindi eseguire il PBR su tale interfaccia. Se il traffico crittografato viene passato su un tunnel VPN, `disabilitare ip cef` sull'interfaccia e terminare il tunnel vpn.

Informazioni correlate

- Pagina di supporto per il routing IP
- Pagina di supporto NAT
- Strumenti e risorse per il supporto tecnico

- Policy-Based Routing
- Tecnologie Cisco IOS
- Documentazione e supporto tecnico – Cisco Systems