Client o server DHCP con configurazione router ZBF

Sommario

Introduzione

In questo documento viene descritto come configurare un router che agisca come server DHCP (Dynamic Host Control Protocol) o come client DHCP con la funzionalità ZBF (Zone-Based Firewall). Poiché è abbastanza comune avere DHCP e ZBF abilitati contemporaneamente, questi suggerimenti di configurazione aiutano a garantire che queste funzionalità interagiscano correttamente.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza del firewall basato su zone software Cisco IOS®. Per ulteriori informazioni, vedere la Guida alla progettazione e all'applicazione di firewall per i criteri basati su aree.

Componenti usati

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

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.

Informazioni sulle funzionalità

Quando si abilita ZBF su un router IOS, per impostazione predefinita nel codice IOS 15.x è consentito tutto il traffico diretto all'area autonoma (ossia, il traffico destinato al piano di gestione del router).

Se è stato creato un criterio per una qualsiasi area, ad esempio 'interna' o 'esterna', all'area autonoma (criteri autonomi) o all'inverso (criteri autonomi), è necessario definire in modo esplicito il traffico consentito nei criteri associati a tali aree. Usare l'azione ispeziona o passa per definire il traffico consentito.

Analisi dei dati

Per completare il processo DHCP, DHCP usa i pacchetti UDP (Broadcast User Datagram Protocol). Le configurazioni del firewall basate su zona che specificano l'azione di ispezione per questi pacchetti UDP broadcast potrebbero essere scartate dal router e il processo DHCP potrebbe non riuscire. È inoltre possibile che venga visualizzato il seguente messaggio di registro:

```
%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
```

Fare riferimento al problema descritto nell'ID bug Cisco CSCso53376, "ZBF inspect does not work for broadcast traffic" (Il controllo ZBF non funziona per il traffico broadcast).

Per evitare questo problema, modificare la configurazione del firewall basata sulla zona in modo che l'azione pass-action anziché l'azione inspect venga applicata al traffico DHCP.

> **Nota**: questo campo è obbligatorio solo quando si applica un criterio all'area autonoma sul router.

Firewall basato su zona come client DHCP con azione di superamento per il traffico UDP

Configurazione

Questa configurazione di esempio utilizza il set di azioni pass anziché l'azione inspect nella mappa-policy per tutto il traffico UDP da o verso il router.

```
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
```

Verifica

Esaminare i syslog per verificare che il router abbia ottenuto un indirizzo DHCP.

Quando i criteri self-to-self e self-to-out sono configurati per il passaggio del traffico UDP, il router può ottenere un indirizzo IP da DHCP, come mostrato in questo syslog:

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

Quando solo il criterio di uscita verso la zona autonoma è configurato per passare il traffico UDP, il router può anche ottenere un indirizzo IP da DHCP e viene creato questo syslog:

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

Quando solo il criterio di zona self-to-out è configurato per passare il traffico UDP, il router può ottenere un indirizzo IP da DHCP e viene creato questo syslog:

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

Firewall basato su zona con azione di superamento per il traffico DHCP

Configurazione

In questa configurazione di esempio viene mostrato come impedire tutto il traffico UDP da una zona alla propria zona del router, ad eccezione dei pacchetti DHCP. Usare un elenco degli accessi con porte specifiche per consentire solo il traffico DHCP; nell'esempio, vengono specificate le porte UDP 67 e UDP 68 da abbinare. A una mappa di classe che fa riferimento all'elenco degli accessi viene applicata l'azione di passaggio.

```
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
```

Verifica

Esaminare l'output del comando **show policy-map type inspect zone-pair sessions** per verificare che il router stia autorizzando il traffico DHCP attraverso il firewall della zona. In questo output di esempio, i contatori evidenziati indicano che i pacchetti vengono passati attraverso il firewall della zona. Se i contatori sono pari a zero, si è verificato un problema con la configurazione oppure i pacchetti non vengono inviati al router per l'elaborazione.

```
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
```

Scenario per configurazioni errate

In questo scenario di esempio viene mostrato cosa succede quando il router non è configurato correttamente per specificare l'azione da ispezionare per il traffico DHCP. In questo scenario, il router è configurato come client DHCP. Il router invia un messaggio discover DHCP per provare a ottenere un indirizzo IP. Il firewall basato sulla zona è configurato per ispezionare il traffico DHCP. Questo è un esempio della configurazione ZBF:

```
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
```

Quando il criterio self-to-out è configurato con l'azione inspect per il traffico UDP, il pacchetto di

rilevamento DHCP viene scartato e viene creato il syslog seguente:

```
%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
```

Quando i criteri self-to-out e out-to-self sono configurati entrambi con l'azione inspect per il traffico UDP, il pacchetto di rilevamento DHCP viene scartato e viene creato questo syslog:

```
%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
```

Quando nel criterio da sola l'azione di ispezione è abilitata e nel criterio da sola in uscita l'azione di accesso è abilitata per il traffico UDP, il pacchetto dell'offerta DHCP viene scartato dopo l'invio del pacchetto di individuazione DHCP e viene creato il syslog seguente:

```
%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 come server DHCP

Se l'interfaccia interna dei router funziona come server DHCP e i client che si connettono all'interfaccia interna sono i client DHCP, il traffico DHCP è consentito per impostazione predefinita se non sono presenti criteri di zona da interno a sé o da sé all'interno.

Tuttavia, se uno di questi criteri esiste, è necessario configurare un'azione pass per il traffico di interesse (porta UDP 67 o porta UDP 68) nel criterio del servizio di coppia di zone.

Risoluzione dei problemi

Non sono attualmente disponibili informazioni specifiche sulla risoluzione dei problemi per queste configurazioni.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).