ZBF 라우터 컨피그레이션이 있는 DHCP 클라이언트 또는 서버

목차

소개

이 문서에서는 DHCP(Dynamic Host Control Protocol) 서버 또는 ZBF(Zone-Based Firewall) 기능을 사용하는 DHCP 클라이언트로 작동하는 라우터를 구성하는 방법에 대해 설명합니다. DHCP 및 ZBF를 동시에 활성화하는 것은 매우 일반적이므로 이러한 컨피그레이션 팁은 이러한 기능이 올바르게 상호 작용하도록 하는 데 도움이 됩니다.

사전 요구 사항

요구 사항

Cisco는 Cisco IOS® 소프트웨어 영역 기반 방화벽에 대한 지식이 있는 것을 권장합니다. 자세한 내용은 Zone-Based Policy Firewall Design and Application Guide를 참조하십시오.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

기능 정보

IOS 라우터에서 ZBF가 활성화된 경우 자체 영역에 대한 모든 트래픽(즉, 라우터의 관리 평면으로 향하는 트래픽)은 IOS 15.x 코드 트레인에서 기본적으로 허용됩니다.

자체 영역(Out-to-Self 정책) 또는 역방향(Self-to-Out 정책)에 대한 모든 영역(예: '내부' 또는 '외부')에 대한 정책을 생성한 경우 이러한 영역에 연결된 정책에서 허용 가능한 트래픽을 명시적으로 정의해야 합니다. 허용되는 트래픽을 정의하려면 inspect 또는 pass 작업을 사용합니다.

데이터 분석

DHCP는 DHCP 프로세스를 완료하기 위해 브로드캐스트 UDP(User Datagram Protocol) 패킷을 사용합니다. 이러한 브로드캐스트 UDP 패킷에 대한 검사 작업을 지정하는 영역 기반 방화벽 컨피그레이션은 라우터에 의해 삭제될 수 있으며 DHCP 프로세스가 실패할 수 있습니다. 다음 로그 메시지도 표시될 수 있습니다.

```
%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
```

Cisco 버그 ID CSCso53376, "ZBF inspect does not work for broadcast traffic"에 설명된 문제를 참조하십시오.

이 문제를 방지하려면 검사 작업 대신 통과 작업이 DHCP 트래픽에 적용되도록 영역 기반 방화벽 컨피그레이션을 수정합니다.

> **참고**: 이는 정책이 라우터의 자체 영역에 적용된 경우에만 필요합니다.

UDP 트래픽에 대한 통과 작업을 사용하는 DHCP 클라이언트로서의 영역 기반 방화벽

구성

이 예제 컨피그레이션에서는 라우터를 오가는 모든 UDP 트래픽에 대해 policy-map의 inspect 작업 대신 pass 작업 집합을 사용합니다.

```
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
```

다음을 확인합니다.

라우터가 DHCP 주소를 성공적으로 가져왔는지 확인하기 위해 syslogs를 검토합니다.

Out-to-self 및 self-to-out 정책이 모두 UDP 트래픽을 전달하도록 구성된 경우 라우터는 이 syslog에 표시된 대로 DHCP에서 IP 주소를 가져올 수 있습니다.

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

UDP 트래픽을 전달하도록 Out-to-Self 영역 정책만 구성된 경우 라우터는 DHCP에서 IP 주소를 가져올 수도 있으며 이 syslog가 생성됩니다.

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

Self-to-out 영역 정책만 UDP 트래픽을 전달하도록 구성된 경우 라우터는 DHCP에서 IP 주소를 가져올 수 있으며 이 syslog가 생성됩니다.

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

DHCP 트래픽에 대한 통과 조치가 포함된 영역 기반 방화벽

구성

이 예제 컨피그레이션에서는 DHCP 패킷을 제외한 영역에서 라우터의 자체 영역으로 들어오는 모든 UDP 트래픽을 차단하는 방법을 보여줍니다. DHCP 트래픽만 허용하려면 특정 포트와 함께 access-list를 사용합니다. 이 예에서는 UDP 포트 67과 UDP 포트 68이 일치하도록 지정됩니다. access-list를 참조하는 클래스 맵에는 pass 작업이 적용됩니다.

```
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
```

다음을 확인합니다.

라우터가 영역 방화벽**을 통과하는 DHCP 트래픽을 허용하는지** 확인하려면 show policy-map type inspect zone-pair sessions 명령의 출력을 검토합니다. 이 예제 출력에서 강조 표시된 카운터는 패킷이 영역 방화벽을 통해 전달되고 있음을 나타냅니다. 이러한 카운터가 0이면 컨피그레이션에 문제가 있거나 패킷이 처리를 위해 라우터에 도착하지 않는 것입니다.

```
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
```

잘못된 컨피그레이션에 대한 시나리오

이 샘플 시나리오는 라우터가 DHCP 트래픽에 대한 검사 작업을 지정하도록 잘못 구성된 경우 발생하는 상황을 보여줍니다. 이 시나리오에서 라우터는 DHCP 클라이언트로 구성됩니다. 라우터는 IP 주소를 얻기 위해 DHCP 검색 메시지를 보냅니다. 영역 기반 방화벽은 이 DHCP 트래픽을 검사하도록 구성됩니다. 다음은 ZBF 구성의 예입니다.

```
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
```

UDP 트래픽에 대한 inspect 작업으로 self-to-out 정책을 구성하면 DHCP 검색 패킷이 삭제되고 이 syslog가 생성됩니다.

```
%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
```

UDP 트래픽에 대한 inspect 작업으로 self-to-out 및 out-to-self 정책이 모두 구성된 경우 DHCP 검색 패킷이 삭제되고 이 syslog가 생성됩니다.

```
%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
```

Out-to-self 정책에 inspect 작업이 활성화되고 self-to-out 정책에 UDP 트래픽에 대한 pass 작업이 활성화된 경우 DHCP 검색 패킷이 전송된 후 DHCP 제안 패킷이 삭제되고 이 syslog가 생성됩니다.

```
%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
```

DHCP 서버로서의 라우터

라우터의 내부 인터페이스가 DHCP 서버 역할을 하고 내부 인터페이스에 연결되는 클라이언트가 DHCP 클라이언트인 경우, 내부 대 자체 또는 자체 대 내부 영역 정책이 없는 경우 이 DHCP 트래픽이 기본적으로 허용됩니다.

그러나 이러한 정책 중 하나가 존재하는 경우 영역 쌍 서비스 정책에서 관심 트래픽(UDP 포트 67 또는 UDP 포트 68)에 대한 통과 작업을 구성해야 합니다.

문제 해결

현재 이러한 컨피그레이션에 사용할 수 있는 구체적인 트러블슈팅 정보가 없습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.