영역 기반 방화벽 문제 해결

목차

소개

이 문서에는 영역 기반 방화벽에 대한 문제 해결 정보가 포함되어 있습니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 영역 기반 정책 방화벽과 함께 VPN 사용
- Zone-Based Policy Firewall 설계 및 애플리케이션 가이드

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.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

VPN 트래픽을 전달할 수 없음

문제

문제는 VPN 트래픽이 영역 기반 방화벽을 통과할 수 없다는 것입니다.

솔루션

영역 기반 Cisco IOS® 방화벽에서 VPN 클라이언트 트래픽을 검사하도록 허용합니다.

예를 들어, 다음은 라우터의 컨피그레이션에 추가할 라인입니다.

```
access-list 103 permit ip 172.16.1.0 0.0.0.255 172.22.10.0 0.0.0.255

class-map type inspect match-all sdm-cls-VPNOutsideToInside-1
  match access-group 103

policy-map type inspect sdm-inspect-all
  class type inspect sdm-cls-VPNOutsideToInside-1
   inspect

zone-pair security sdm-zp-out-in source out-zone destination in-zone
  service-policy type inspect sdm-inspect-all
```

GRE/PPTP를 전달할 수 없음

문제

문제는 GRE/PPTP 트래픽이 영역 기반 방화벽을 통과할 수 없다는 것입니다.

솔루션

영역 기반 Cisco IOS 방화벽에서 VPN 클라이언트 트래픽을 검사하도록 허용합니다.

예를 들어, 다음은 라우터의 컨피그레이션에 추가할 라인입니다.

```
agw-7206>enable

gw-7206#conf t
gw-7206(config)#policy-map type inspect outside-to-inside
gw-7206(config-pmap)#no class type inspect outside-to-inside
gw-7206(config-pmap)#no class class-default
gw-7206(config-pmap)#class type inspect outside-to-inside
gw-7206(config-pmap-c)#inspect
%No specific protocol configured in class outside-to-inside for inspection.
```

```
All protocols will be inspected
gw-7206(config-pmap-c)#class class-default
gw-7206(config-pmap-c)#drop
gw-7206(config-pmap-c)#exit
gw-7206(config-pmap)#exit
```

컨피그레이션을 확인합니다.

```
gw-7206#show run policy-map outside-to-inside
policy-map type inspect outside-to-inside
 class type inspect PPTP-Pass-Through-Traffic
  pass
 class type inspect outside-to-inside
  inspect
 class class-default
  drop
```

네트워크 연결성

문제

Cisco IOS 라우터에 영역 기반 방화벽에 대한 정책이 적용된 후에는 네트워크에 연결할 수 없습니다.

솔루션

이 문제는 비대칭 라우팅일 수 있습니다.Cisco IOS 방화벽은 비대칭 라우팅이 있는 환경에서는 작동하지 않습니다.패킷은 동일한 라우터를 통해 반환될 수 없습니다.

Cisco IOS 방화벽은 TCP/UDP 세션의 상태를 추적합니다.상태 정보의 정확한 유지 관리를 위해 패킷이 동일한 라우터에서 출발하여 반환되어야 합니다.

영역 기반 방화벽을 통해 DHCP 트래픽을 전달할 수 없음

문제

영역 기반 방화벽을 통해 DHCP 트래픽을 전달할 수 없습니다.

솔루션

이 문제를 해결하려면 자체 영역 트래픽 검사를 비활성화합니다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems
- ZBFW(Zone-Based Firewall)를 사용하는 IOS의 AnyConnect