Zone-gebaseerde probleemoplossing in de firewall

Inhoud

Inleiding

Dit document bevat informatie over probleemoplossing voor zone-gebaseerde firewall.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- VPN gebruiken met Zone-Based Policy Firewall
- Zone-Based Policy Firewall Design and Application Guide

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Kan VPN-verkeer niet doorgeven

Probleem

Het probleem is dat VPN-verkeer niet over zone-gebaseerde firewall kan lopen.

Oplossing

Laat het VPN clientverkeer geïnspecteerd worden door de op zone gebaseerde Cisco IOS® firewall.

Bijvoorbeeld, hier zijn de lijnen om op de configuratie van de router toe te voegen:

```
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
```

Kan geen GRE/PPTP doorgeven

Probleem

Het probleem is dat het verkeer GRE/PPTP niet door de op zone gebaseerde firewall kan passeren.

Oplossing

Laat het VPN clientverkeer worden geïnspecteerd door de op zone gebaseerde Cisco IOS-firewall.

Bijvoorbeeld, hier zijn de lijnen om op de configuratie van de router toe te voegen:

```
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
```

Controleer de configuratie:

```
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
```

Netwerkbereikbaarheid

Probleem

Nadat het beleid voor zone-gebaseerde firewall in de Cisco IOS router wordt toegepast, zijn de netwerken niet bereikbaar.

Oplossing

Dit probleem kan de asymmetrische routing zijn. Cisco IOS-firewall werkt niet in omgevingen met asymmetrische routing. Packets kunnen niet gegarandeerd door dezelfde router terugkeren.

Cisco IOS firewalls volgen de staat van TCP/UDP-sessies. Een pakje moet van dezelfde router afwijken en terugkeren om de staatsinformatie nauwkeurig te kunnen onderhouden.

Kan DHCP-verkeer niet doorgeven via een Zone-gebaseerde firewall

Probleem

U kunt DHCP-verkeer niet doorgeven via een op zone gebaseerde firewall.

Oplossing

Uitschakelen van een inspectie van het verkeer in een eigen gebied om dit probleem op te lossen.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems
- AnyConnect op IOS met Zone-gebaseerde firewall (ZBFW)