Hoe vorm ik op beleid gebaseerde routing (PBR) op een Cisco meerlaagse switch of router om verkeer naar de WSA te verzenden?

Inhoud

Vraag:

Hoe vorm ik op beleid gebaseerde routing (PBR) op een Cisco meerlaagse switch of router om verkeer naar de WSA te verzenden?

Milieu: Cisco Web Security Appliance (WSA), transparante modus - L4 switch

Wanneer WSA in transparante modus is geconfigureerd met behulp van een L4-schakelaar, is er geen configuratie nodig op de WSA. De omleiding wordt gecontroleerd door de L4-schakelaar (of router).

Het is mogelijk om op beleid gebaseerde routing (PBR) te gebruiken om webverkeer naar de WSA om te leiden. Dit wordt bereikt door het juiste verkeer aan te passen (op basis van TCP-poorten) en de router/schakelaar op te geven om dit verkeer naar de WSA te richten.

In het volgende voorbeeld is de gegevens/proxy-interface van WSA (of M1 of P1, afhankelijk van de configuratie) op een speciale VLAN-interface van de meerlaagse switch/router (VLAN 3) en de Internet-router is ook op een speciale VLAN-interface (VLAN4) aanwezig. Clients zijn op VLAN1 en VLAN2.

Eerste configuratie (alleen relevante onderdelen weergegeven)
interface-VLAN1 Desc-gebruiker VLAN 1 ip-adres 10.1.1.1 255.255.255.0 ! interface VLAN2 Ontwerpgebruiker VLAN 2 ip-adres 10.1.2.1 255.255.255.0 ! interface-VLAN3 Cisco WSA toegewijd VLAN ip-adres 192.168.1.1 255.255.255.252 ! interface-VLAN4

```
Cisco Internet Router toegewijd VLAN
ip-adres 192.168.2.1 255.255.255.252
!
ip-route 0.0.0.0 0.0.0.0 192.168.2.2
```

Gezien het bovenstaande voorbeeld en het feit dat Cisco WSA een IP-adres van 192.168.1.2 heeft, zou u de volgende opdrachten toevoegen aan een op beleid gebaseerde routing (PBR):

Stap 1: Webverkeer definiëren

```
! Overeenkomend HTTP-verkeer
toegangslijst 100 vergunningen TCP 10.1.1.0 0.0.0.255 elke eq 80
toegangslijst 100 vergunningen TCP 10.1.2.0 0.0.0.255 elke eq 80
! HTTPS-verkeer
toegangslijst 100 vergunningen TCP 10.1.1.0 0.0.0.255 elke eq 443
toegangslijst 100 vergunningen TCP 10.1.2.0 0.0.0.255 elke eq 443
```

Stap 2: Defineert een routekaart om te controleren waar pakketten worden uitgevoerd.

```
Routekaart naar voorwaartse webvergunning 10
matchen ip-adres 100
ip volgende-hop-192.168.1.2
```

Stap 3: Pas de routekaart op de juiste interface toe.

```
!Let op dat dit op de broninterface (clientkant) moet worden toegepast.
interface-VLAN1
IP-beleidsroutekaart ForwardWeb
!
interface VLAN2
IP-beleidsroutekaart ForwardWeb
```

Opmerking: Deze methode om verkeer te verplaatsen (PBR) heeft bepaalde beperkingen. Het belangrijkste probleem met deze methode is dat het verkeer altijd naar de WSA zal worden verwezen, zelfs als het apparaat niet bereikbaar is (door netwerkproblemen bijvoorbeeld). Dus er is geen mislukking boven optie.

Om aan deze tekortkoming te voldoen, kunt u een van de volgende configureren:

1. **PBR met opties voor het volgen** van de **opties** bij gebruik van Cisco-routers. Deze optie wordt gebruikt om de beschikbaarheid van de volgende hop te controleren alvorens verkeer om te leiden.

   Meer informatie over het volgende artikel:
   Op beleid gebaseerde routing met het voorbeeld van de configuratie van meerdere traceringsopties
2. De opties voor het overtrekken zijn niet beschikbaar voor Cisco Catalyst-switches. Er is echter een geavanceerde werkomgeving beschikbaar om hetzelfde gedrag te bereiken.

   Details zijn te vinden op de volgende Cisco Wiki:
   Op beleid gebaseerde routing (PBR) met tracering voor Catalyst 3xxx-switches - A workround met EEM