Como eu configuro o Policy Based Routing (PBR) em um switch multicamada ou em um roteador de Cisco para enviar o tráfego ao WSA?

Índice

Pergunta:

Como eu configuro o Policy Based Routing (PBR) em um switch multicamada ou em um roteador de Cisco para enviar o tráfego ao WSA?

Ambiente: Ferramenta de segurança da Web de Cisco (WSA), modo transparente - interruptor L4

Quando WSA é configurado no modo transparente usando um interruptor L4, nenhuma configuração está precisada no WSA. A reorientação é controlada pelo interruptor L4 (ou pelo roteador).

Épossível usar o Policy Based Routing (PBR) para reorientar o tráfego de web ao WSA. Isto é conseguido combinando o tráfego correto (baseado em portas tcp) e instruindo o roteador/interruptor para reorientar este tráfego ao WSA.

No exemplo seguinte, os dados de WSA/relação do proxy (M1 ou P1 segundo a configuração) estão em uma relação do vlan dedicada do switch multicamada/roteador (Vlan 3) e do roteador de Internet estão em uma relação do vlan dedicada também (Vlan4). Os clientes estão em Vlan1 e em Vlan2.

Configuração inicial (somente partes relevantes indicadas)
interface Vlan1 VLAN de usuário 1 do desc endereço IP 10.1.1.1 255.255.255.0 ! relação Vlan2 VLAN de usuário 2 do desc endereço IP 10.1.2.1 255.255.255.0 ! relação Vlan3 vlan dedicada de Cisco WSA do desc endereço IP 192.168.1.1 255.255.255.252

```
!
relação Vlan4
vlan dedicada do roteador de Internet do desc
endereço IP 192.168.2.1 255.255.255.252
!
rota 0.0.0.0 0.0.0.0 192.168.2.2 IP
```

Dado o exemplo acima, e Cisco WSA que tem um endereço IP de Um ou Mais Servidores Cisco ICM NT de 192.168.1.2, você adicionaria os comandos seguintes estabelecer o Policy Based Routing (PBR):

Passo 1: Defina o tráfego de web

```
! Combine o tráfego de HTTP
a lista de acesso 100 permite tcp 10.1.1.0 0.0.0.255 todo o eq 80
a lista de acesso 100 permite tcp 10.1.2.0 0.0.0.255 todo o eq 80
! Tráfego do fósforo HTTPS
a lista de acesso 100 permite tcp 10.1.1.0 0.0.0.255 todo o eq 443
a lista de acesso 100 permite tcp 10.1.2.0 0.0.0.255 todo o eq 443
```

Passo 2: Defina um mapa de rota para controlar onde os pacotes output.

```
licença 10 de ForwardWeb do mapa de rotas
endereço IP de Um ou Mais Servidores Cisco ICM NT 100 do fósforo
ajuste o salto seguinte 192.168.1.2 IP
```

Passo 3: Aplique o mapa de rota à relação correta.

```
! Note que isto deve ser aplicado à interface de origem (lado do cliente)
interface Vlan1
mapa de rotas ForwardWeb da política IP
!
relação Vlan2
mapa de rotas ForwardWeb da política IP
```

Note: Este método da reorientação do tráfego (PBR) tem algumas limitações. O problema principal com este método é que o tráfego estará reorientado sempre ao WSA mesmo se o dispositivo não é alcançável (devido aos problemas de rede por exemplo). Assim, não há nenhuma falha sobre a opção.

Àação alternativa esta deficiência, você pode configurar qualquer um do seguinte:

1. **PBR com opções de seguimento** ao usar roteadores Cisco. Esta característica é usada para verificar a Disponibilidade do salto seguinte antes de reorientar o tráfego.

   Mais detalhes no seguinte artigo:
   Policy Based Routing with the Multiple Tracking Options Feature Configuration Example
2. Seguindo opções não esteja disponível para o Switches do Cisco catalyst. Contudo, há uma ação alternativa avançada disponível para conseguir o mesmo comportamento.

   Os detalhes podem ser encontrados em seguinte Cisco Wiki:
   Policy-Based Routing (PBR) com seguimento para Catalyst 3xxx Switch - Uma ação

alternativa usando EEM