

Cisco Multilayer Switch 또는 라우터에서 트래픽을 WSA로 전달하도록 PBR(Policy Based Routing)을 구성하려면 어떻게 합니까?

목차

[질문:](#)

질문:

Cisco Multilayer Switch 또는 라우터에서 트래픽을 WSA로 전달하도록 PBR(Policy Based Routing)을 구성하려면 어떻게 합니까?

환경: Cisco WSA(Web Security Appliance), 투명 모드 - L4 스위치

WSA가 L4 스위치를 사용하여 투명 모드로 구성된 경우 WSA에 컨피그레이션이 필요하지 않습니다. 리디렉션은 L4 스위치(또는 라우터)에 의해 제어됩니다.

PBR(Policy Based Routing)을 사용하여 웹 트래픽을 WSA로 리디렉션할 수 있습니다. 이는 올바른 트래픽(tcp 포트 기반)을 매칭하고 라우터/스위치에서 이 트래픽을 WSA로 리디렉션하도록 지시함으로써 달성할 수 있습니다.

다음 예에서는 WSA의 데이터/프록시 인터페이스(구성에 따라 M1 또는 P1)가 멀티레이어 스위치/라우터(Vlan 3)의 전용 VLAN 인터페이스에 있고 인터넷 라우터는 전용 VLAN 인터페이스(Vlan4)에도 있습니다. 클라이언트는 Vlan1 및 Vlan2에 있습니다.

초기 구성(관련 부품만 표시됨)

```
인터페이스 VLAN1
설명 사용자 VLAN 1
ip 주소 10.1.1.1 255.255.255.0
!
인터페이스 VLAN2
설명 사용자 VLAN 2
ip 주소 10.1.2.1 255.255.255.0
!
인터페이스 VLAN3
설명 Cisco WSA 전용 VLAN
ip 주소 192.168.1.1 255.255.255.252
!
인터페이스 VLAN4
desc 인터넷 라우터 전용 VLAN
ip 주소 192.168.2.1 255.255.255.252
```

```
!
ip 경로 0.0.0.0 0.0.0.0 192.168.2.2
```

위의 예와 IP 주소가 192.168.1.2인 Cisco WSA의 경우 다음 명령을 추가하여 PBR(Policy Based Routing)을 설정합니다.

1단계:웹 트래픽 정의
<pre>!HTTP 트래픽 일치 access-list 100 permit tcp 10.1.1.0 any eq 80 access-list 100 permit tcp 10.1.2.0 any eq 80 !HTTPS 트래픽 일치 access-list 100 permit tcp 10.1.1.0 any eq 443 access-list 100 permit tcp 10.1.2.0 any eq 443</pre>
2단계:패킷이 출력되는 위치를 제어할 경로 맵을 정의합니다.
<pre>route-map ForwardWeb 허가 10 일치 ip 주소 100 ip next hop 192.168.1.2 설정</pre>
3단계:경로 맵을 올바른 인터페이스에 적용합니다.
<pre>! 소스 인터페이스(클라이언트측)에 적용해야 합니다. 인터페이스 VLAN1 ip policy route-map forwardWeb ! 인터페이스 VLAN2 ip policy route-map forwardWeb</pre>

참고:이 PBR(트래픽 리디렉션) 방법은 몇 가지 제한이 있습니다.이 방법의 주요 문제는 어플라이언스에 연결할 수 없는 경우에도(예: 네트워크 문제) 트래픽이 항상 WSA로 리디렉션된다는 점입니다. 따라서 장애 조치 옵션은 없습니다.

이 부족을 해결하려면 다음 중 하나를 구성할 수 있습니다.

1. Cisco 라우터 사용 시 **추적 옵션**이 있는 PBR이 기능은 트래픽을 리디렉션하기 전에 다음 hops의 가용성을 확인하는 데 사용됩니다.

다음 문서에 대한 자세한 내용:

[다중 추적 옵션 기능 구성을 사용한 정책 기반 라우팅](#)에

2. Cisco Catalyst 스위치에는 추적 옵션을 사용할 수 없습니다.그러나 동일한 동작을 수행하는 고급 해결 방법이 있습니다.

자세한 내용은 다음 Cisco Wiki에서 확인할 수 있습니다.

[Catalyst 3xxx 스위치에 대한 추적을 사용하는 PBR\(Policy-based Routing\) - EEM을 사용하는 해결 방법](#)