Come configurare Policy Based Routing (PBR) su uno switch multilivello o un router Cisco per inoltrare il traffico al server WSA?

Sommario

Domanda:

Come configurare Policy Based Routing (PBR) su uno switch multilivello o un router Cisco per inoltrare il traffico al server WSA?

Ambiente: Cisco Web Security Appliance (WSA), modalità trasparente - switch L4

Quando WSA è configurato in modalità trasparente utilizzando uno switch L4, non è necessaria alcuna configurazione su WSA. Il reindirizzamento è controllato dallo switch L4 (o router).

Èpossibile utilizzare Policy Based Routing (PBR) per reindirizzare il traffico Web al WSA. A tal fine, è necessario far corrispondere il traffico corretto (basato sulle porte tcp) e chiedere al router/switch di reindirizzare il traffico al server WSA.

Nell'esempio seguente, l'interfaccia dati/proxy WSA (M1 o P1 a seconda della configurazione) si trova su un'interfaccia VLAN dedicata dello switch/router multilivello (Vlan 3) e il router Internet su un'interfaccia VLAN dedicata (Vlan4). I client si trovano sulla Vlan1 e sulla Vlan2.

Configurazione iniziale (vengono visualizzate solo le parti rilevanti)
interface Vlan1 desc Utente VLAN 1 indirizzo ip 10.1.1.1 255.255.255.0 ! interface Vlan2 desc User VLAN 2 indirizzo ip 10.1.2.1 255.255.255.0 ! interface Vlan3 desc Cisco WSA dedicato VLAN indirizzo ip 192.168.1.1 255.255.255.252 ! interface Vlan4 VLAN dedicata desc Internet Router indirizzo ip 192.168.2.1 255.255.255.252

```
!
ip route 0.0.0.0 0.0.0.0 192.168.2.2
```

In base all'esempio precedente, se l'indirizzo IP di Cisco è 192.168.1.2, è possibile aggiungere i seguenti comandi per configurare Policy Based Routing (PBR):

Passaggio 1: Definizione traffico Web

```
! Corrispondenza traffico HTTP
access-list 100 allow tcp 10.1.1.0 0.0.0.255 any eq 80
access-list 100 allow tcp 10.1.2.0 0.0.0.255 any eq 80
! Corrispondenza traffico HTTPS
access-list 100 allow tcp 10.1.1.0 0.0.0.255 any eq 443
access-list 100 allow tcp 10.1.2.0 0.0.0.255 any eq 443
```

Passaggio 2: Definire una mappa percorsi per controllare dove vengono inviati i pacchetti.

```
route-map ForwardWeb permission 10
abbina indirizzo ip 100
set ip next-hop 192.168.1.2
```

Passaggio 3: Applicare la mappa del percorso all'interfaccia corretta.

```
!Notare che deve essere applicata all'interfaccia di origine (lato client)
interface Vlan1
ip policy route-map ForwardWeb
!
interface Vlan2
ip policy route-map ForwardWeb
```

Nota: Questo metodo di reindirizzamento del traffico (PBR) presenta alcune limitazioni. Il problema principale di questo metodo è che il traffico verrà sempre reindirizzato al server di accesso alla rete anche se l'accessorio non è raggiungibile (ad esempio a causa di problemi di rete). Quindi, non vi è alcuna opzione di failover.

Per risolvere questo problema, è possibile configurare uno dei seguenti elementi:

1. **PBR con opzioni di rilevamento** quando si utilizzano router Cisco. Questa funzione viene usata per verificare la disponibilità dell'hop successivo prima di reindirizzare il traffico.

   Ulteriori dettagli sul seguente articolo:
   Routing basato su criteri con configurazione della funzionalità Opzioni di rilevamento multiple
2. Le opzioni di rilevamento non sono disponibili per gli switch Cisco Catalyst. Tuttavia, è disponibile una soluzione avanzata per ottenere lo stesso comportamento.

   Ulteriori informazioni sono disponibili sul seguente wiki di Cisco:
   Policy-based Routing (PBR) con rilevamento per gli switch Catalyst 3xxx - Soluzione alternativa mediante EEM