Wie konfiguriere ich richtlinienbasiertes Routing (PBR) auf einem Cisco Multilayer Switch oder Router, um Datenverkehr an die WSA weiterzuleiten?

Inhalt

Frage:

Wie konfiguriere ich richtlinienbasiertes Routing (PBR) auf einem Cisco Multilayer Switch oder Router, um Datenverkehr an die WSA weiterzuleiten?

Umgebung: Cisco Web Security Appliance (WSA), transparenter Modus - L4-Switch

Wenn die WSA mithilfe eines L4-Switches im transparenten Modus konfiguriert wird, ist für die WSA keine Konfiguration erforderlich. Die Umleitung wird über den L4-Switch (oder Router) gesteuert.

Sie können Policy Based Routing (PBR) verwenden, um Webdatenverkehr an die WSA umzuleiten. Dies wird erreicht, indem der richtige Datenverkehr (basierend auf TCP-Ports) abgeglichen und der Router/Switch angewiesen wird, diesen Datenverkehr an die WSA umzuleiten.

Im folgenden Beispiel befindet sich die Daten-/Proxy-Schnittstelle der WSA (entweder M1 oder P1 je nach Konfiguration) auf einer dedizierten VLAN-Schnittstelle des Multilayer-Switches/Routers (VLAN 3), und der Internet-Router befindet sich ebenfalls in einer dedizierten VLAN-Schnittstelle (VLAN4). Die Clients befinden sich auf VLAN1 und VLAN2.

Erstkonfiguration (nur relevante Teile werden angezeigt)
interface Vlan1 VLAN 1 des dec-Benutzers ip address 10.1.1.1 255.255.255.0 ! Interface VLAN2 VLAN 2 des dec-Benutzers ip address 10.1.2.1 255.255.255.0 ! VLAN-Schnittstelle3 dediziertes Cisco WSA VLAN

```
ip address 192.168.1.1 255.255.255.252
!
VLAN-Schnittstelle4
dediziertes VLAN des dedizierten Internet-Routers
ip address 192.168.2.1 255.255.255.252
!
ip route 0.0.0.0 0.0.0.0 192.168.2.2
```

In Anbetracht des obigen Beispiels und der IP-Adresse der Cisco WSA 192.168.1.2 würden Sie die folgenden Befehle hinzufügen, um Policy Based Routing (PBR) einzurichten:

Schritt 1: Definieren des Webdatenverkehrs

```
! HTTP-Datenverkehr zuordnen
access-list 100 permit tcp 10.1.1.0 0.0.0.255 any eq 80
access-list 100 permit tcp 10.1.2.0 0.0.0.255 any eq 80
! HTTPS-Datenverkehr zuordnen
access-list 100 permit tcp 10.1.1.0 0.0.0.255 any eq 443
access-list 100 permit tcp 10.1.2.0 0.0.0.255 any eq 443
```

Schritt 2: Definieren Sie eine Routenübersicht, um zu steuern, wo Pakete ausgegeben werden.

```
route-map ForwardWeb permit 10
match IP-Adresse 100
set ip next-hop 192.168.1.2
```

Schritt 3: Wenden Sie die Routenübersicht auf die richtige Schnittstelle an.

```
!Beachten Sie, dass dies auf die Quellschnittstelle (clientseitig) angewendet werden soll.
interface Vlan1
ip policy route-map ForwardWeb
!
Interface VLAN2
ip policy route-map ForwardWeb
```

Hinweis: Diese Methode der Umleitung von Datenverkehr (PBR) weist einige Einschränkungen auf. Das Hauptproblem bei dieser Methode besteht darin, dass der Datenverkehr immer an die WSA umgeleitet wird, auch wenn die Appliance nicht erreichbar ist (z. B. aufgrund von Netzwerkproblemen). Es gibt also keine Failover-Option.

Um diesen Mangel zu umgehen, können Sie eine der folgenden Optionen konfigurieren:

1. **PBR mit Nachverfolgungsoptionen** bei Verwendung von Cisco Routern Diese Funktion wird verwendet, um die Verfügbarkeit des nächsten Hop zu überprüfen, bevor der Datenverkehr umgeleitet wird.

   Weitere Informationen zu folgendem Artikel:
   Richtlinienbasiertes Routing mit dem Konfigurationsbeispiel für mehrere Tracking-Optionen
2. Für Cisco Catalyst Switches sind keine Nachverfolgungsoptionen verfügbar. Es steht jedoch eine erweiterte Problemumgehung zur Verfügung, um dasselbe Verhalten zu erreichen.

   Details hierzu finden Sie im folgenden Cisco Wiki:

Policy-Based Routing (PBR) mit Tracking für Catalyst 3xxx Switches - eine Problemumgehung mit EEM