ASA上不同VPN場景的EEM示例

目錄

簡介

Cisco IOS®軟體內嵌式事件管理員(EEM)是一個功能強大且靈活的子系統，可提供即時網路事件偵測和機上自動化。本文檔提供了在不同的VPN場景中EEM可為您提供幫助的示例

必要條件

需求

思科建議您瞭解ASA EEM功能。

採用元件

本文檔基於運行軟體版本9.2(1)或更高版本的思科自適應安全裝置(ASA)。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

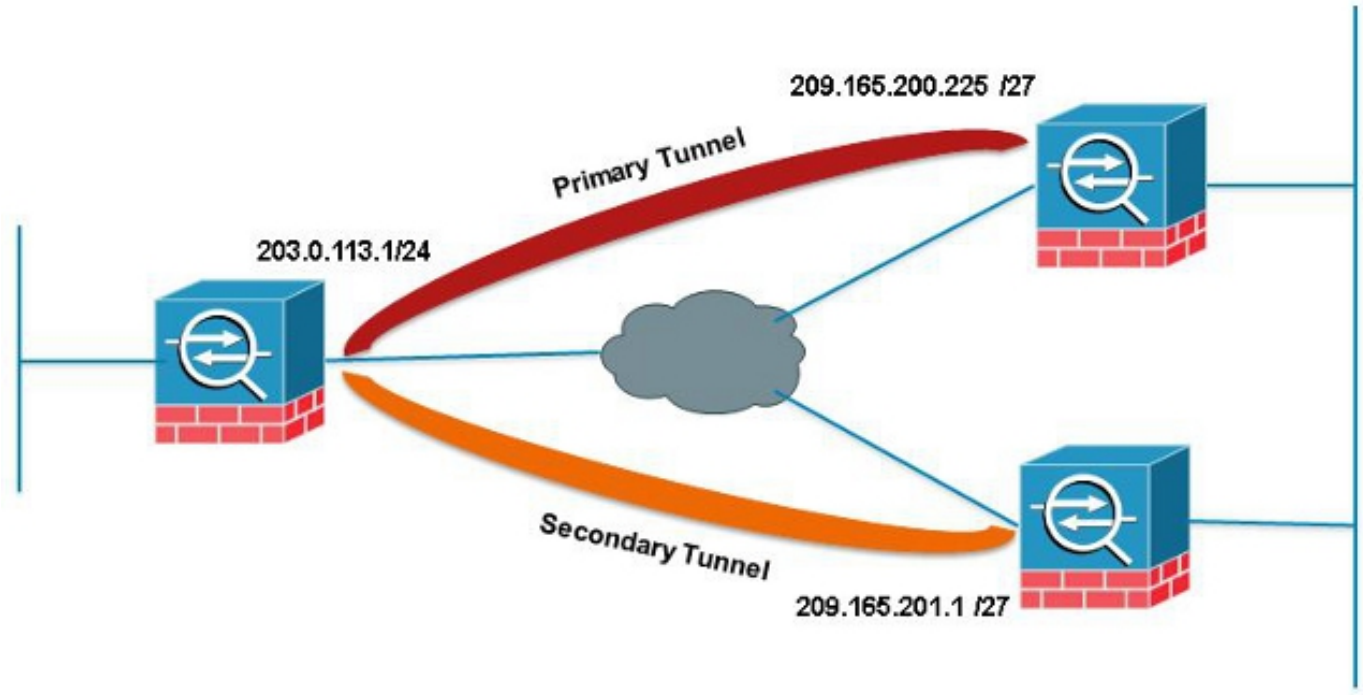
嵌入式事件管理器最初在ASA上稱為「background-debug」，是一種用於調試特定問題的功能。檢查後，發現它與Cisco IOS軟體EEM相似，因此進行了更新以匹配該CLI。

EEM功能使您可以調試問題，並提供用於故障排除的通用日誌記錄。EEM通過執行動作來響應EEM系統中的事件。有兩個元件：eem觸發的事件，以及定義操作的事件管理器小程式。您可以向每個事件管理器小程式新增多個事件，這將觸發它來呼叫已在其上配置的操作。

VPN搶佔

如果為加密條目配置多個對等IP地址的VPN，則一旦主對等體關閉，就會使用備份對等IP建立VPN。但是，一旦主對等體返回，VPN不會搶佔主IP地址。您必須手動刪除現有的SA，以便重新啟動VPN協商，將其切換到主IP地址。

```
ASA 1
crypto map outside_map 10 match address outside_cryptomap_20
crypto map outside_map 10 set peer 209.165.200.225 209.165.201.1
crypto map outside_map 10 set transform-set ESP-AES-256-SHA
crypto map outside_map interface outside
```



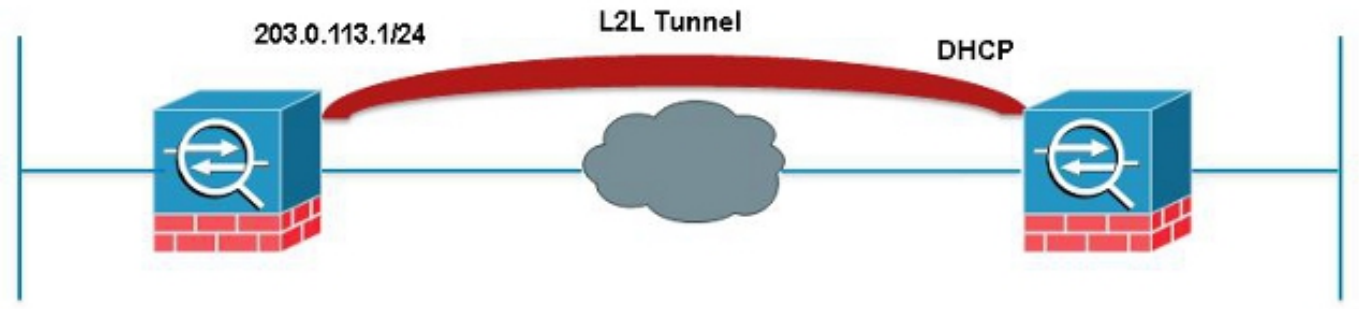
在此範例中，IP站台層級彙總(SLA)用於監控主通道。如果對等體發生故障，備份對等體將接管主節點，但SLA仍會監控主節點；主節點恢復後，生成的系統日誌將觸發EEM清除輔助隧道，允許ASA再次與主節點重新協商。

```
sla monitor 123
type echo protocol ipIcmpEcho 209.165.200.225 interface outside
num-packets 3
frequency 10

sla monitor schedule 123 life forever start-time now

track 1 rtr 123 reachability

route outside 209.165.200.225 255.255.255.0 203.0.113.254 1 track 1

event manager applet PREEMPT
event syslog id 622001 occurs 2
action 1 cli command "clear crypto ipsec sa peer 209.165.101.1"
output none
```

動態到靜態L2L始終啟動

建立LAN到LAN通道時，兩個IPSec對等體的IP地址都需要知道。如果其中一個IP地址是動態的（即通過DHCP獲取）因而未知，則唯一的替代方案是使用動態加密對映。由於另一個對等體不知道正在使用的IP，因此只能從具有動態IP的裝置啟動隧道。

如果裝置後面沒有人使用動態IP來啟動隧道，則出現此問題；因此始終需要啟用此隧道。即使您將idle-timeout設定為**none**，也不會解決問題，因為重新生成金鑰時，如果沒有流量通過隧道，將關閉。此時，再次啟動隧道的唯一方法是使用動態IP從裝置傳送流量。如果通道由於意外原因（例如DPD等）而關閉，同樣適用。



此EEM將在匹配所需SA的隧道中每60秒傳送一次ping，以便保持連線。

```
event manager applet VPN-Always-UP
event timer watchdog time 60
action 1 cli command "ping inside 192.168.20.1"
output none
```

在特定時間斷開所有VPN現有連線

ASA無法設定VPN會話的硬截止時間。但是您使用EEM執行此操作。此示例演示如何在下午5:00斷開VPN客戶端和Anyconnect客戶端

```
event manager applet VPN-Disconnect
event timer absolute time 17:00:00
action 1 cli command "vpn-sessiondb logoff ra-ikev1-ipsec noconfirm"
action 2 cli command "vpn-sessiondb logoff anyconnect noconfirm"
output none
```