ASA上不同VPN场景的EEM示例

目录

简介

Cisco IOS®软件嵌入式事件管理器(EEM)是功能强大且灵活的子系统，可提供实时网络事件检测和板载自动化。本文档提供了EEM在不同VPN场景中的帮助示例

先决条件

要求

思科建议您了解ASA EEM功能。

使用的组件

本文档基于运行软件版本9.2(1)或更高版本的思科自适应安全设备(ASA)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

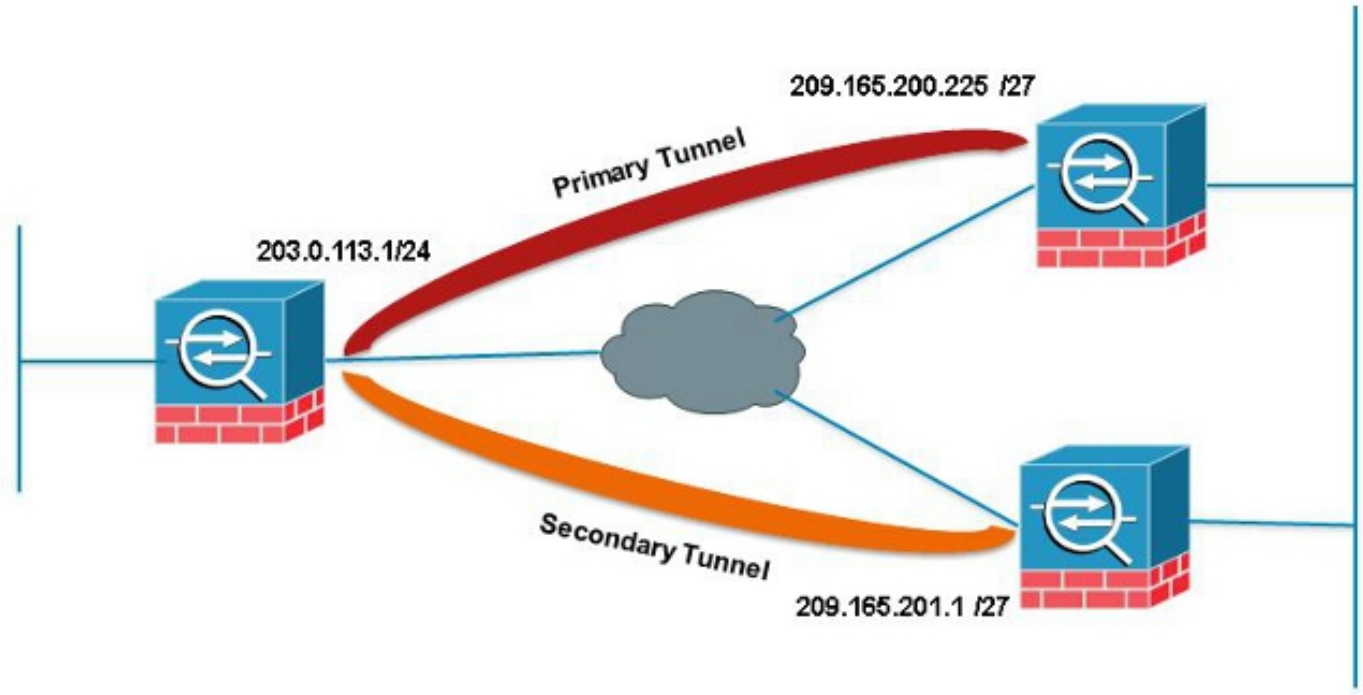
嵌入式事件管理器最初在ASA上称为“background-debug”，是用于调试特定问题的功能。经过回顾后，发现它与Cisco IOS软件EEM相似，因此更新后与该CLI匹配。

EEM功能使您能够调试问题并提供用于故障排除的通用日志记录。EEM通过执行操作来响应EEM系统中的事件。有两个组件：EEM触发的事件和定义操作的事件管理器小程序。您可以向每个事件管理器小程序添加多个事件，这会触发它调用已在其上配置的操作。

VPN抢占

如果为加密条目配置多个对等IP地址的VPN，则在主对等体关闭后，VPN将与备份对等体IP建立。不过，一旦主对等体恢复，该 VPN 不会抢占主 IP 地址。必须手动删除现有 SA 才能重新启动 VPN 协商以将它切换到主 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
```



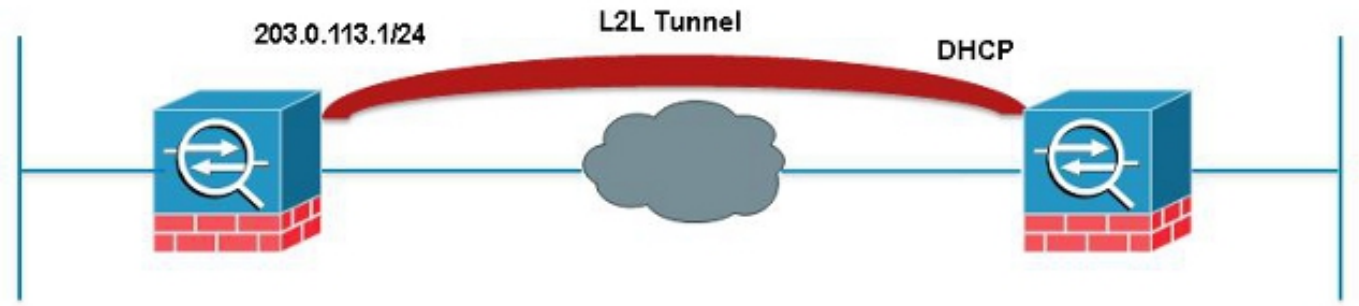
在本示例中，使用IP站点级聚合(SLA)来监控主隧道。如果该对等体发生故障，备用对等体将接管，但SLA仍会监控主对等体；一旦Primary恢复，生成的系统日志将触发EEM清除辅助隧道，允许ASA再次与Primary重新协商。

```
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
```

动态到静态L2L始终为up

当建立LAN到LAN隧道时，需要知道两个IPSec对等体的IP地址。如果其中一个IP地址因为动态（即通过DHCP获取）而不知道，则唯一的选择是使用动态加密映射。只能从具有动态IP的设备启动隧道，因为另一个对等体不知道正在使用IP。

如果设备后面没有人使用动态IP来启动隧道，以防隧道发生故障，则会出现此问题；因此需要始终打开这条隧道。即使您将idle-timeout设置为**none**，这也无法解决问题，因为在重新键入时，如果没有通过隧道的流量将关闭。此时，再次启用隧道的唯一方法是使用动态IP从设备发送流量。如果隧道因DPD等意外原因关闭，则同样适用。



此EEM将每60秒在与所需SA匹配的隧道中发送一次ping，以保持连接正常。

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

在特定时间断开所有VPN现有连接

ASA无法设置VPN会话的硬中断时间。无论您如何使用EEM。本示例演示如何在下午5:00分同时断开VPN客户端和Anyconnect客户端

```
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
```