不同的VPN方案的EEM示例在ASA

目录

简介

Cisco IOS软件被嵌入的活动管理器(EEM)是提供实时网元检测和自动化的一个强大和灵活子系统。本文提供您EEM可帮助用不同的VPN方案的示例

先决条件

要求

思科建议您有ASA EEM功能的知识。

使用的组件

本文根据Cisco可适应安全工具(ASA)该运行软件版本9.2(1)或以后。

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

嵌入式活动管理器最初呼叫“背景调试”在ASA，并且是用于的功能调试一个特定问题。在复核以后，发现足够类似于Cisco IOS软件EEM，因此更新匹配该CLI。

EEM功能使您调试问题和提供通用记录日志排除故障的。EEM响应对在EEM系统的事件由执行的操作。有两个组件：EEM触发的事件和定义了操作的活动管理器applet。您可以添加多个事件到每活动管理器applet，触发它调用操作配置对此。

VPN优先占用

如果配置VPN用一个crypto条目的多个对等项IP地址， VPN被设立与备份对等IP，一旦主对等体断开。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
```

在本例中， IP站点级别聚合(SLA)用于为了监控主要的通道。如果该对等体出故障，备份对等接管，但是SLA仍然监控主要的;一次主要的恢复生成的Syslog将触发EEM清除允许ASA的附属通道再重新协商与主要的。

```
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
```

动态对静态L2L总是

当设立LAN-to-LAN隧道时，两IPSec对等体的IP地址需要知道。如果其中一个IP地址不知道，因为动态，即获取通过DHCP，则唯一的替代方案是使用动态加密映射。因为另一对等体不知道使用的IP通道可能从有动态IP的设备只被发起。

这是问题，万一没人是在设备后以启动通道的动态IP，万一断开;因而需要有此通道总是。即使您设置idle-timeout对**无**，这不会解决问题，因为，在重新生成密钥，如果没有通过的流量通道将断开。在该瞬间启动通道的唯一方法再是发送从设备的流量有动态IP的。同一件事应用，如果通道为一个意外的原因断开例如DPDs等等。

此EEM将发送ping在匹配希望的SA的通道间的每60秒为了保持连接。

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

断开所有VPN现有连接在有些次

ASA没有一个方式设置VPN会话的艰难被中断的时期。然而您执行此与EEM。此示例如何给

dicsonnect VPN客户端和Anyconnect客户端展示在下午5:00

```
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
```