Exemplos de EEM para diferentes cenários de VPN no ASA

Contents

Introduction

O Cisco IOS® Software Embedded Event Manager (EEM) é um subsistema eficiente e flexível que oferece detecção de eventos de rede em tempo real e automação integrada. Este documento fornece exemplos de onde o EEM pode ajudar em diferentes cenários de VPN

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento do recurso ASA EEM.

Componentes Utilizados

Este documento é baseado no Cisco Adaptive Security Appliance (ASA) que executa o software versão 9.2(1) ou posterior.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

O Embedded Event Manager foi originalmente chamado de "background-debug" no ASA e foi um

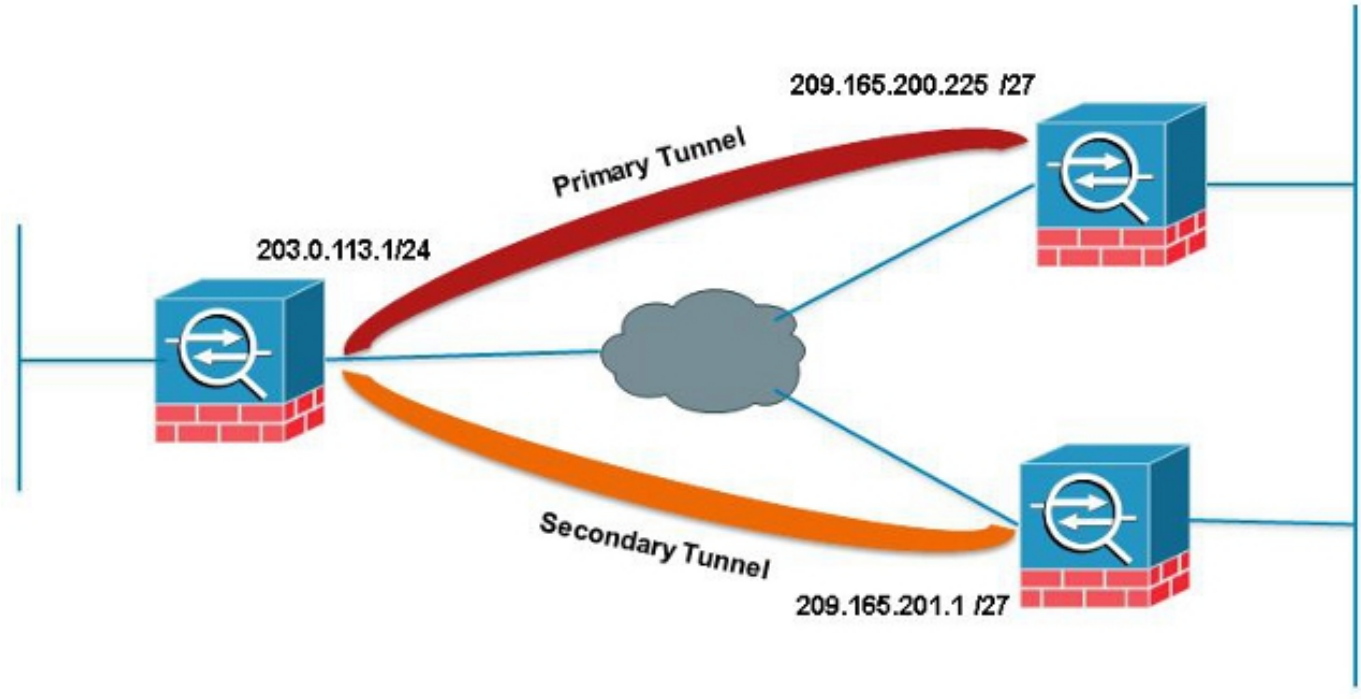
recurso usado para depurar um problema específico. Após a revisão, foi considerado suficientemente semelhante ao EEM do software Cisco IOS, por isso foi atualizado para corresponder a essa CLI.

O recurso EEM permite depurar problemas e fornece registro de finalidade geral para solução de problemas. O EEM responde a eventos no sistema EEM executando ações. Há dois componentes: eventos que o EEM aciona e miniaplicativos do gerente de eventos que definem ações. Você pode adicionar vários eventos a cada miniaplicativo do gerenciador de eventos, o que o ativa para invocar as ações que foram configuradas nele.

Preempt. VPN

Se você configurar a VPN com vários endereços IP de peer para uma entrada de criptografia, a VPN será estabelecida com o IP do peer de backup quando o peer principal for desativado. No entanto, quando o peer principal volta, a VPN não preempta o endereço IP principal. Você deve excluir manualmente a SA existente para reiniciar a negociação de VPN para alterá-la para o endereço IP principal.

```
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
```



Neste exemplo, uma agregação de nível de local IP (SLA) é usada para monitorar o túnel primário. Se esse peer falhar, o peer de backup assumirá o controle, mas o SLA ainda monitora o principal; quando o Primário voltar, o syslog gerado ativará o EEM para limpar o túnel Secundário, permitindo que o ASA negocie novamente com o Primário.

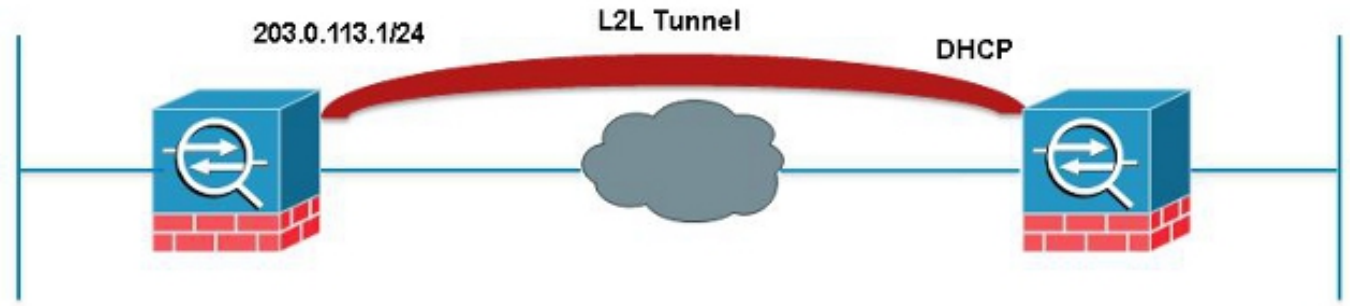
```
sla monitor 123
type echo protocol ipIcmpEcho 209.165.200.225 interface outside
num-packets 3
```

```
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
```

L2L dinâmico para estático sempre ativo

Ao estabelecer um túnel de LAN para LAN, o endereço IP de ambos os pares de IPSec precisa ser conhecido. Se um dos endereços IP não for conhecido porque é dinâmico, ou seja, obtido por DHCP, a única alternativa é usar um mapa de criptografia dinâmico. O túnel só pode ser iniciado do dispositivo com o IP dinâmico, já que o outro peer não tem ideia do IP sendo usado.

Este é um problema no caso de ninguém estar por trás do dispositivo com o IP dinâmico para ativar o túnel no caso de ele cair; assim, a necessidade de ter esse túnel sempre ativado. Mesmo que você defina o timeout de ociosidade como **nenhum,** isso não resolverá o problema porque, em uma chave, se não houver tráfego que passe pelo túnel, ele será desativado. Nesse momento, a única maneira de ativar o túnel novamente é enviar o tráfego do dispositivo com o IP dinâmico. O mesmo se aplica se o túnel cair por uma razão inesperada como DPDs, etc.



Este EEM enviará um ping a cada 60 segundos através do túnel correspondente ao SA desejado para manter a conexão ativa.

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

Desconecte todas as conexões VPN existentes em um determinado momento

O ASA não tem como definir um tempo de interrupção para sessões de VPN. No entanto, você faz isso com EEM. Este exemplo demonstra como desconectar clientes VPN e clientes Anyconnect às 17h

```
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
```