Exemplos EEM para cenários VPN diferentes no ASA

Índice

Introdução

O gerente encaixado Cisco IOS ® Software do evento (EEM) é um subsistema poderoso e flexível que forneça a detecção do evento de rede de tempo real e a automatização a bordo. Este documento dá-lhe os exemplos de onde EEM pode ajudar em cenários VPN diferentes

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento da característica ASA EEM.

Componentes Utilizados

Este documento é baseado na ferramenta de segurança adaptável de Cisco (ASA) esse versão de software das corridas 9.2(1) ou mais atrasado.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

O gerente encaixado do evento foi chamado originalmente “fundo-debuga” no ASA, e era uma característica usada para debugar uma edição específica. Após a revisão, encontrou-se para ser similar bastante ao Cisco IOS Software EEM, assim que foi atualizado para combinar esse CLI.

A característica EEM permite-o de debugar problemas e fornece-ao uso geral que registra pesquisando defeitos. O EEM responde aos eventos no sistema EEM executando ações. Há dois componentes: eventos que o EEM provoca, e applet do gerente do evento que definem ações. Você pode adicionar eventos múltiplos a cada applet do gerente do evento, que o provoca para invocar as ações que foram configuradas nele.

O VPN cancela

Se você configura o VPN com endereços IP de Um ou Mais Servidores Cisco ICM NT dos peer múltiplos para uma entrada cripto, o VPN obtém estabelecido com o IP do peer de backup uma vez que o peer principal vai para baixo. Contudo, uma vez que o peer principal volta, o VPN não cancela ao endereço IP primário. Você deve manualmente suprimir do SA existente a fim reinitiate a negociação VPN para comutá-la sobre ao endereço IP primário.

```
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 do nível do local IP (SLA) é usada a fim monitorar o túnel preliminar. Se esse par falha, o peer de backup toma sobre mas o SLA ainda monitora o preliminar; uma vez o preliminar vem apoio que o Syslog gerado provocará o EEM para cancelar o túnel secundário permitindo que o ASA renegocie com o preliminar outra vez.

```
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-à-estático sempre acima

Ao estabelecer um túnel de LAN para LAN, o endereço IP de Um ou Mais Servidores Cisco ICM NT de ambos os ipsec peer precisa de ser sabido. Se um dos endereços IP de Um ou Mais Servidores Cisco ICM NT não está sabido porque é dinâmico, isto é obtido através do DHCP, a seguir da única alternativa é usar um mapa cripto dinâmico. O túnel pode somente ser iniciado do dispositivo com o IP dinâmico desde que o outro par não tem nenhuma ideia do IP que está sendo usado.

Este é um problema caso que ninguém é atrás do dispositivo com o IP dinâmico para trazer acima o túnel caso que vai para baixo; assim a necessidade de ter este túnel sempre acima. Mesmo se você ajusta o quietude-intervalo a **nenhuns,** este não endereçará a edição porque, em cima de um rekey, se há um sem tráfego que passa o túnel irá para baixo. Nesse momento a única maneira de trazer acima o túnel é outra vez enviar o tráfego do dispositivo com o IP dinâmico. A mesma coisa aplica-se se o túnel vai para baixo para uma razão inesperada tal como DPD, etc.

Este EEM enviará a um sibilo cada 60 segundos através do túnel que combina o SA desejado a fim manter acima a conexão.

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

Desligue todas as conexões existentes VPN em alguma vez

O ASA não tem uma maneira de ajustar uma estadia eliminada dura para sessões de VPN. Contudo você faz este com EEM. Este exemplo demonstra como aos clientes VPN do dicsonnect e aos clientes de Anyconnect em 5:00 PM

```
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
```