Ejemplos de EEM para Diferentes Escenarios de VPN en ASA

Contenido

Introducción

Cisco IOS® Software Embedded Event Manager (EEM) es un subsistema potente y flexible que proporciona detección de eventos de red en tiempo real y automatización integrada. Este documento le ofrece ejemplos de dónde EEM puede ayudar en diferentes escenarios de VPN

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de la función ASA EEM.

Componentes Utilizados

Este documento se basa en Cisco Adaptive Security Appliance (ASA) que ejecuta la versión de software 9.2(1) o 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.

Antecedentes

Embedded Event Manager se llamaba originalmente "background-debug" en el ASA y era una

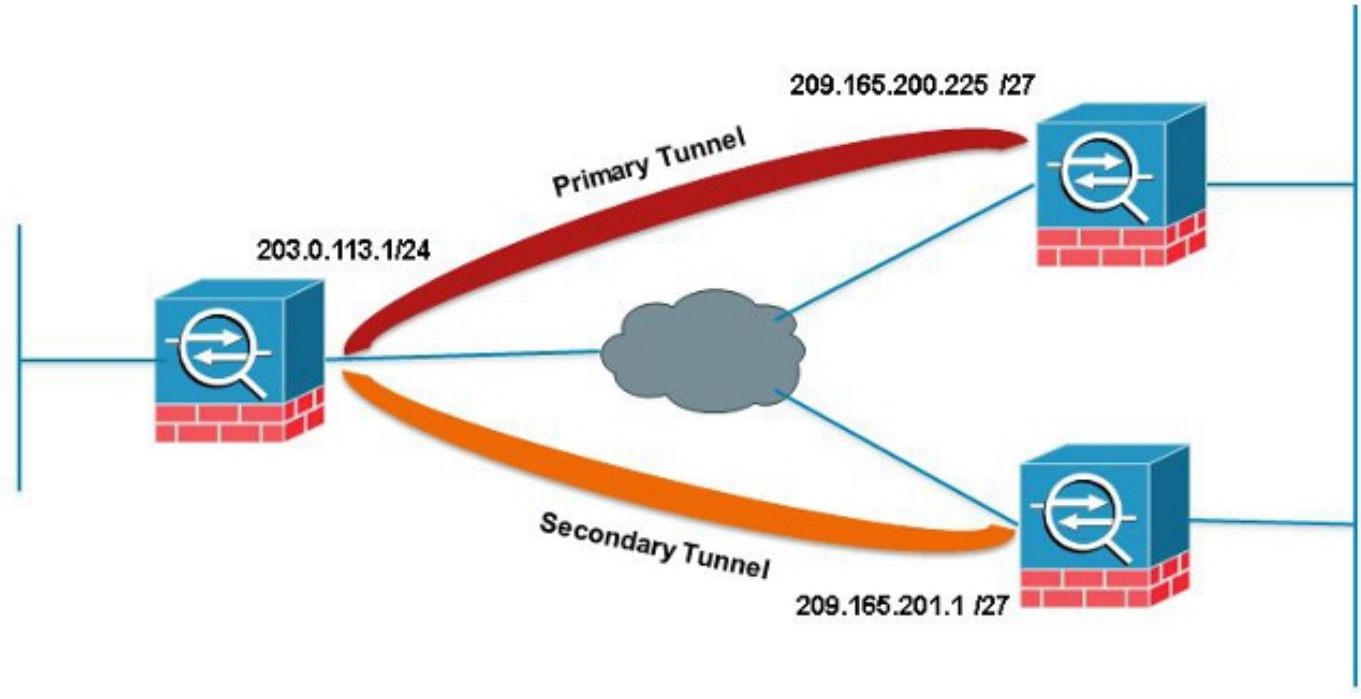
función utilizada para depurar un problema específico. Después de la revisión, se encontró que era lo suficientemente similar a Cisco IOS Software EEM, por lo que se actualizó para que coincidiera con esa CLI.

La función EEM le permite depurar problemas y proporciona registro de uso general para la resolución de problemas. El EEM responde a los eventos del sistema EEM realizando acciones. Hay dos componentes: eventos que activa EEM y applets del administrador de eventos que definen acciones. Puede agregar varios eventos a cada applet del administrador de eventos, lo que le permite invocar las acciones configuradas en él.

VPN Preempt

Si configura VPN con varias direcciones IP de peer para una entrada crypto, la VPN se establece con la IP de peer de respaldo una vez que el peer primario se desactiva. Sin embargo, una vez que el peer primario vuelve, la VPN no se adelanta a la dirección IP primaria. Debe eliminar manualmente la SA existente para reiniciar la negociación VPN para conmutarla a la dirección IP primaria.

```
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
```



En este ejemplo, se utiliza una agregación de nivel de sitio IP (SLA) para supervisar el túnel principal. Si ese par falla, el par de respaldo toma el control pero el SLA todavía monitorea el primario; una vez que el Primario vuelva a funcionar, el syslog generado activará el EEM para borrar el túnel secundario, permitiendo que el ASA vuelva a negociar con el Primario.

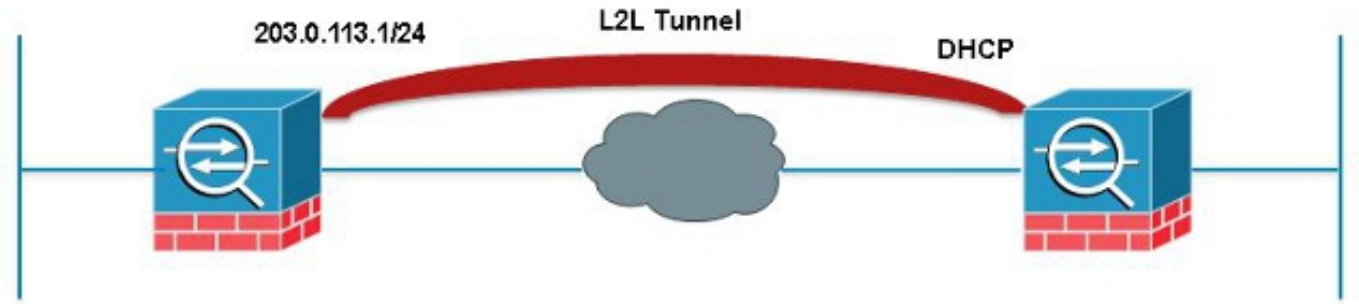
```
sla monitor 123
type echo protocol ipIcmpEcho 209.165.200.225 interface outside
num-packets 3
```

```
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 dinámico a estático siempre activo

Al establecer un túnel de LAN a LAN, se debe conocer la dirección IP de ambos pares IPSec. Si una de las direcciones IP no se conoce porque es dinámica, es decir, se obtiene a través de DHCP, entonces la única alternativa es utilizar un mapa criptográfico dinámico. El túnel sólo se puede iniciar desde el dispositivo con la IP dinámica ya que el otro par no tiene idea de la IP que se está utilizando.

Este es un problema en caso de que nadie esté detrás del dispositivo con la IP dinámica para activar el túnel en caso de que se caiga; por lo tanto, la necesidad de tener este túnel siempre activo. Incluso si establece el tiempo de espera inactivo en **none,** esto no resolverá el problema porque, al volver a encender la llave, si no hay tráfico que pase el túnel se desactivará. En ese momento, la única manera de activar el túnel de nuevo es enviar tráfico desde el dispositivo con la IP dinámica. Lo mismo se aplica si el túnel se desactiva por una razón inesperada como los DPD, etc.



Este EEM enviará un ping cada 60 segundos a través del túnel que coincida con la SA deseada para mantener la conexión activa.

```
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 las conexiones VPN existentes en un momento determinado

El ASA no tiene una manera de establecer un tiempo de corte duro para las sesiones VPN. Sin embargo, haga esto con EEM. Este ejemplo muestra cómo desconectar tanto clientes VPN como clientes Anyconnect a las 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
```