Ejemplos EEM para diversos escenarios de VPN en el ASA

Contenido

Introducción

El administrador del evento integrado Cisco IOS ® Software (EEM) es un subsistema potente y flexible que proporciona la detección en tiempo real del evento de red y a bordo de la automatización. Este documento le da los ejemplos de donde EEM puede ayudar en diversos escenarios de VPN

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento de la característica ASA EEM.

Componentes Utilizados

Este documento se basa en el dispositivo de seguridad adaptante de Cisco (ASA) esa versión de software de los funcionamientos 9.2(1) o más adelante.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

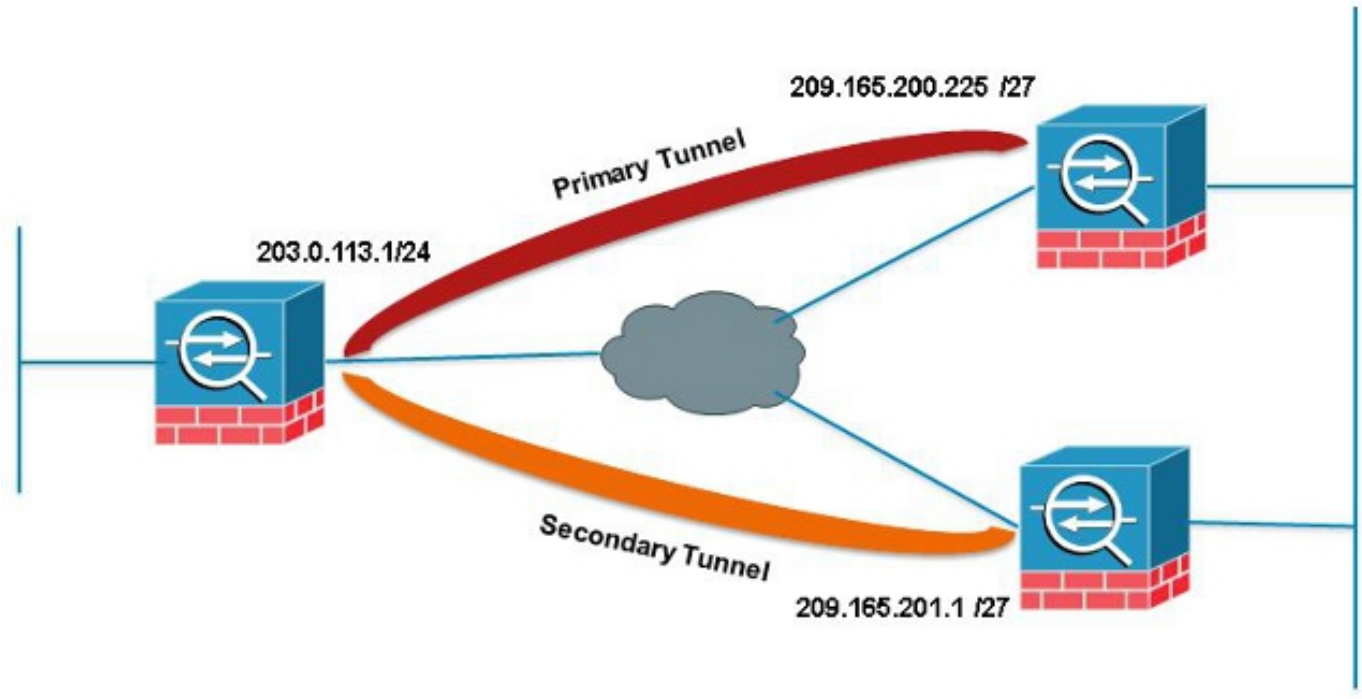
Llamaron “fondo-debug” en el ASA, y era una característica el administrador del evento integrado originalmente usada para hacer el debug de un problema específico. Después del estudio, fue encontrado para ser bastante similar al Cisco IOS Software EEM, así que fue puesto al día para hacer juego ese CLI.

La característica EEM le permite para hacer el debug de los problemas y proporciona el registro de fines generales para resolver problemas. El EEM responde a los eventos en el sistema EEM realizando las acciones. Hay dos componentes: eventos que el EEM acciona, y applet del administrador del evento que definen las acciones. Usted puede agregar los eventos múltiples a cada applet del administrador del evento, que lo acciona para invocar las acciones que se han configurado en él.

El VPN se apropia

Si usted configura el VPN con los IP Addresses del peer múltiple para una entrada crypto, el VPN consigue establecido con el IP del backup peer una vez que va el peer primario abajo. Sin embargo, una vez que se vuelve el peer primario, el VPN no se apropia al IP Address principal. Usted debe borrar manualmente el SA existente para reinitiate la negociación VPN para cambiarla al IP Address 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
```



En este ejemplo, una agregación del nivel del sitio IP (SLA) se utiliza para monitorear el túnel primario. Si ese par falla, el backup peer asume el control pero SLA todavía monitorea el primario; el primario viene una vez salvaguardia que el Syslog generado accionará el EEM para borrar el túnel secundario permitiendo que el ASA renegocie con el primario otra vez.

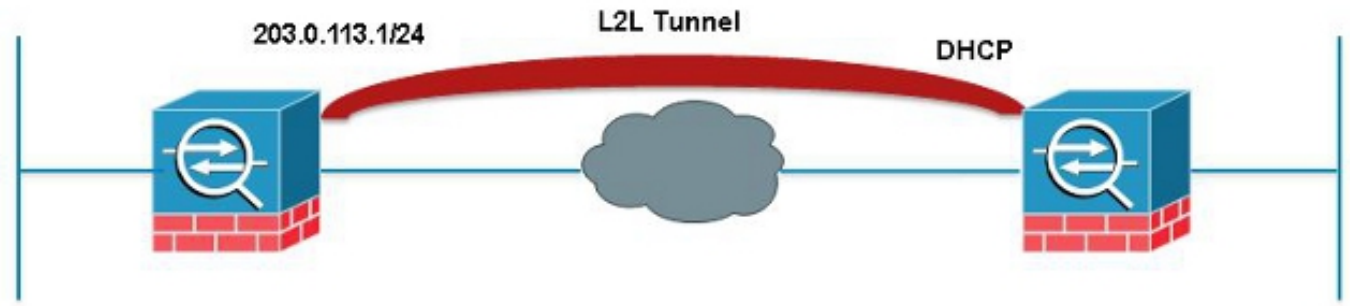
```
sla monitor 123
type echo protocol ipIcmpEcho 209.165.200.225 interface outside
num-packets 3
```

```
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 Dinámico-a-estático siempre para arriba

Al establecer un túnel de LAN a LAN, la dirección IP de ambos peeres IPSec necesita ser sabida. Si uno de los IP Addresses no se sabe porque son dinámicos, es decir obtenido vía el DHCP, después la única alternativa es utilizar una correspondencia cifrada dinámica. El túnel se puede iniciar solamente del dispositivo con IP dinámica puesto que el otro par no tiene ninguna idea del IP que es utilizado.

Esto es un problema en caso de que nadie esté detrás del dispositivo con IP dinámica para traer para arriba el túnel en caso de que vaya abajo; así la necesidad del tener este túnel siempre para arriba. Incluso si usted fija el ocioso-descanso a **ningunos,** éste no abordará el problema porque, sobre una reintroducción, si no hay tráfico que pasa irá el túnel abajo. En ese momento la única forma de traer para arriba el túnel es otra vez enviar el tráfico del dispositivo con IP dinámica. La misma cosa se aplica si el túnel va abajo por una razón inesperada tal como DPD, etc.



Este EEM enviará un ping cada 60 segundos a través del túnel que corresponde con el SA deseado para guardar la conexión para arriba.

```
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 existentes VPN a cierta vez

El ASA no tiene una manera de fijar un rato cortado duro para las sesiones de VPN. Sin embargo usted hace esto con EEM. Este ejemplo demuestra cómo a los clientes VPN del dicsonnect y a los clientes de Anyconnect en 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
```