Exemples EEM pour différents scénarios VPN sur ASA

Contenu

Introduction

Cisco IOS® Software Embedded Event Manager (EEM) est un sous-système puissant et flexible qui assure la détection des événements réseau en temps réel et l'automatisation intégrée. Ce document vous donne des exemples d'où le module EEM peut vous aider dans différents scénarios VPN

Conditions préalables

Conditions requises

Cisco vous recommande de connaître la fonctionnalité ASA EEM.

Components Used

Ce document est basé sur le dispositif de sécurité adaptatif (ASA) de Cisco qui exécute le logiciel version 9.2(1) ou ultérieure.

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.

Informations générales

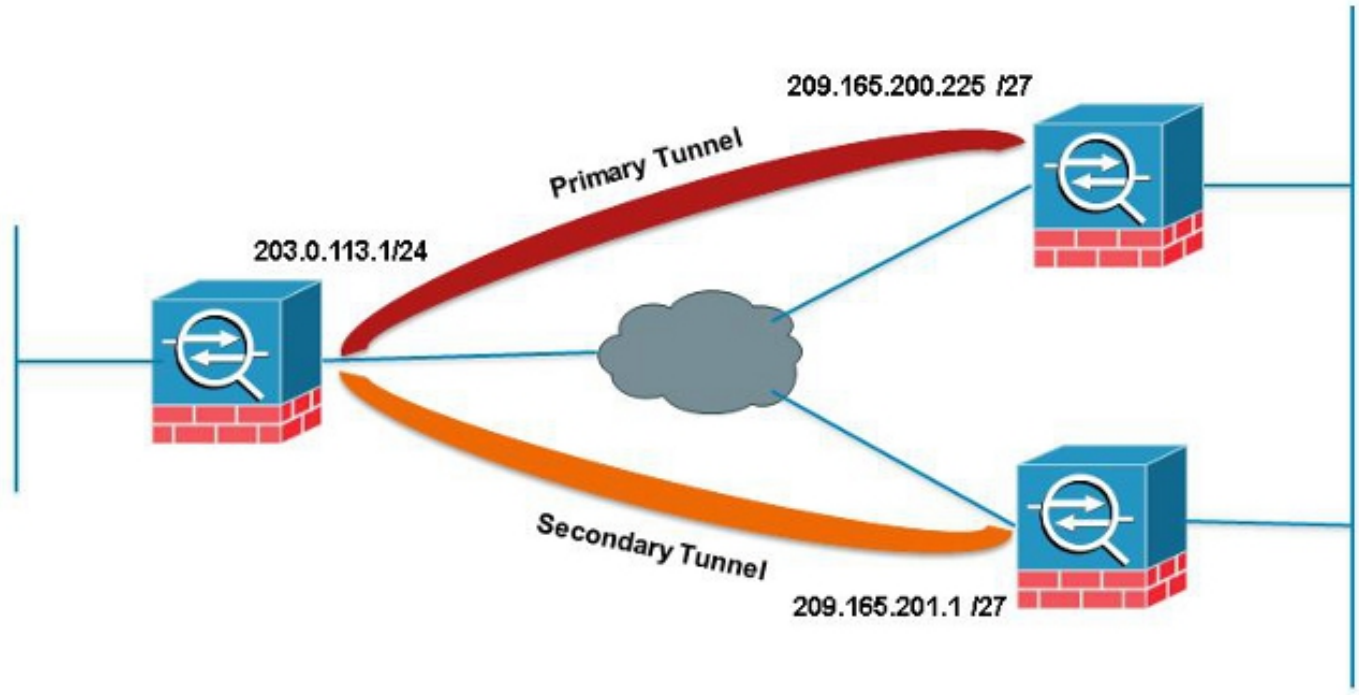
Embedded Event Manager était à l'origine appelé « Background-debug » sur l'ASA, et était une fonctionnalité utilisée pour déboguer un problème spécifique. Après examen, il s'est avéré qu'il était assez similaire à l'EEM du logiciel Cisco IOS, et il a donc été mis à jour pour correspondre à cette CLI.

La fonctionnalité EEM vous permet de déboguer des problèmes et fournit une journalisation à usage général pour le dépannage. L'EEM répond aux événements du système EEM en effectuant des actions. Il y a deux composants : les événements déclenchés par l'EEM et les applets du gestionnaire d'événements qui définissent les actions. Vous pouvez ajouter plusieurs événements à chaque applet du gestionnaire d'événements, ce qui le déclenche pour appeler les actions qui ont été configurées dessus.

Préemption VPN

Si vous configurez le VPN avec plusieurs adresses IP d'homologue pour une entrée de chiffrement, le VPN est établi avec l'IP d'homologue de sauvegarde une fois que le pair principal est hors service. Cependant, lorsque l'homologue primaire reprend, le VPN ne préempte pas l'adresse IP primaire. Vous devez manuellement supprimer la SA existante afin de réinitialiser la négociation VPN pour la basculer sur l'adresse IP primaire.

```
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
```



Dans cet exemple, une agrégation de niveau de site IP (SLA) est utilisée afin de surveiller le tunnel principal. Si cet homologue échoue, l'homologue de secours prend le relais mais le SLA surveille toujours le principal ; une fois que le primaire est rétabli, le syslog généré déclenchera l'EEM pour effacer le tunnel secondaire, ce qui permettra à l'ASA de renégocier avec le principal.

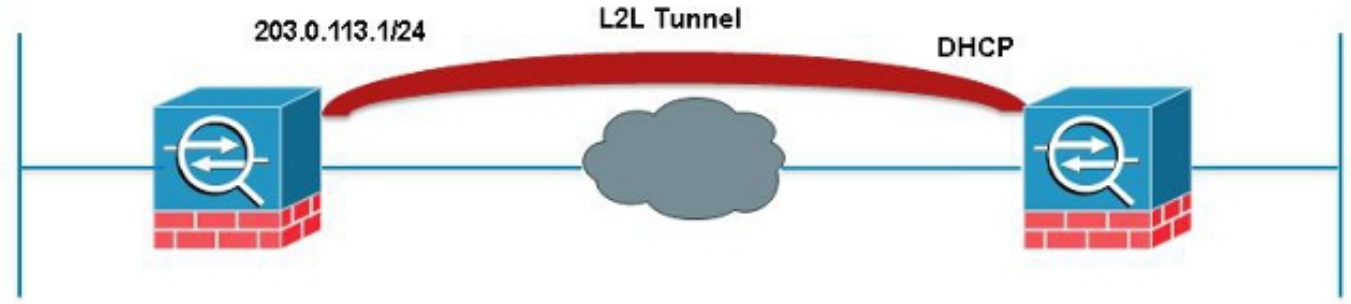
```
sla monitor 123
```

```
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 dynamique à statique toujours actif

Lors de l'établissement d'un tunnel LAN à LAN, l'adresse IP des deux homologues IPSec doit être connue. Si l'une des adresses IP n'est pas connue parce qu'elle est dynamique, c'est-à-dire obtenue via DHCP, alors la seule alternative est d'utiliser une carte de chiffrement dynamique. Le tunnel ne peut être lancé qu'à partir du périphérique avec l'adresse IP dynamique, car l'autre homologue n'a aucune idée de l'adresse IP utilisée.

C'est un problème au cas où personne n'est derrière le périphérique avec l'IP dynamique pour faire monter le tunnel en cas de panne ; il faut donc que ce tunnel soit toujours en service. Même si vous définissez le délai d'inactivité sur **aucun,** cela ne réglera pas le problème car, lors d'une retouche, s'il n'y a pas de trafic passant par le tunnel, il va s'arrêter. À ce moment-là, la seule façon de réactiver le tunnel est d'envoyer le trafic du périphérique avec l'IP dynamique. La même chose s'applique si le tunnel tombe en panne pour une raison inattendue telle que les DPD, etc.



Ce module EEM envoie une requête ping toutes les 60 secondes à travers le tunnel correspondant à l'SA souhaitée afin de maintenir la connexion.

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

Déconnecter toutes les connexions VPN existantes à un certain moment

L'ASA ne dispose pas d'un moyen de définir un temps d'arrêt dur pour les sessions VPN. Cependant, vous le faites avec EEM. Cet exemple montre comment déconnecter les clients VPN et les clients Anyconnect à 17 h

```
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
```