Exemples EEM pour différents scénarios VPN sur l'ASA

Contenu

Introduction

Le gestionnaire d'événement encastré par logiciel de Cisco IOS® (EEM) est un sous-système puissant et flexible qui fournit la détection d'événement réseau en temps réel et à bord de l'automatisation. Ce document te donne des exemples d'où EEM peut aider dans différents scénarios VPN

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de la caractéristique ASA EEM.

Composants utilisés

Ce document est basé sur l'appliance de sécurité adaptable Cisco (ASA) cette version de logiciel de passages 9.2(1) ou plus tard.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Le gestionnaire encastré d'événement s'est initialement appelé le « fond-debug » sur l'ASA, et était une caractéristique utilisée pour mettre au point une problématique spécifique. Après examen, il s'est avéré assez semblable au logiciel EEM de Cisco IOS, ainsi il a été mis à jour pour apparier ce CLI.

La caractéristique EEM te permet de mettre au point des problèmes et fournit l'usage universel se connectant pour le dépannage. L'EEM répond aux événements dans le système EEM en exécutant des actions. Il y a deux composants : événements que l'EEM déclenche, et events manager applet qui définissent des actions. Vous pouvez ajouter de plusieurs événements à chaque event manager applet, qui le déclenche pour appeler les actions qui ont été configurées là-dessus.

Le VPN acquièrent

Si vous configurez le VPN avec des adresses IP de plusieurs homologues pour une crypto entrée, le VPN obtient établi avec l'IP de backup peer une fois que le pair primaire descend. 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 ce pair échoue, le backup peer succède mais SLA surveille toujours le primaire ; une fois le primaire se réactive le Syslog généré déclenchera l'EEM pour effacer le tunnel secondaire permettant à l'ASA pour renégocier avec le primaire de nouveau.

```
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

En établissant un tunnel entre réseaux locaux, l'adresse IP des deux pairs d'IPSec doit être connue. Si une des adresses IP n'est pas connue parce qu'elle est dynamique, c.-à-d. obtenu par l'intermédiaire du DHCP, alors de la seule alternative est utiliser une crypto-carte dynamique. Le tunnel peut seulement être initié du périphérique avec l'IP dynamique puisque l'autre pair n'a

aucune idée de l'IP étant utilisé.

C'est un problème au cas où personne ne serait derrière le périphérique avec l'IP dynamique pour apporter le tunnel au cas où il descendrait ; ainsi le besoin de avoir ce tunnel toujours. Même si vous placez l'inactif-délai d'attente à **aucun,** ceci n'abordera pas la question parce que, sur un rekey, s'il n'y a aucun trafic passant le tunnel descendra. À ce moment la seule manière d'apporter le tunnel est de nouveau d'envoyer le trafic du périphérique avec l'IP dynamique. La même chose s'applique si le tunnel descend pour une raison inattendue telle que DPDs, etc.

Cet EEM enverra à un ping toutes les 60 secondes à travers le tunnel concurrençant SA désirée afin de garder 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
```

Déconnectez toutes les connexions existantes VPN à une certaine fois

L'ASA n'a pas une manière de placer un moment découpé difficile pour des sessions VPN. Cependant vous faites ceci avec EEM. Cet exemple explique comment aux clients vpn de dicsonnect et aux clients d'Anyconnect à 5:00 P.M.

```
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
```