Esempi EEM per diversi scenari VPN su appliance ASA

Sommario

Introduzione

Cisco IOS® Software Embedded Event Manager (EEM) è un sottosistema potente e flessibile che fornisce il rilevamento degli eventi di rete in tempo reale e l'automazione integrata. Questo documento offre esempi di come EEM può aiutare in diversi scenari VPN

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza della funzione EEM ASA.

Componenti usati

Questo documento si basa sulle appliance Cisco Adaptive Security (ASA) con software versione 9.2(1) o successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

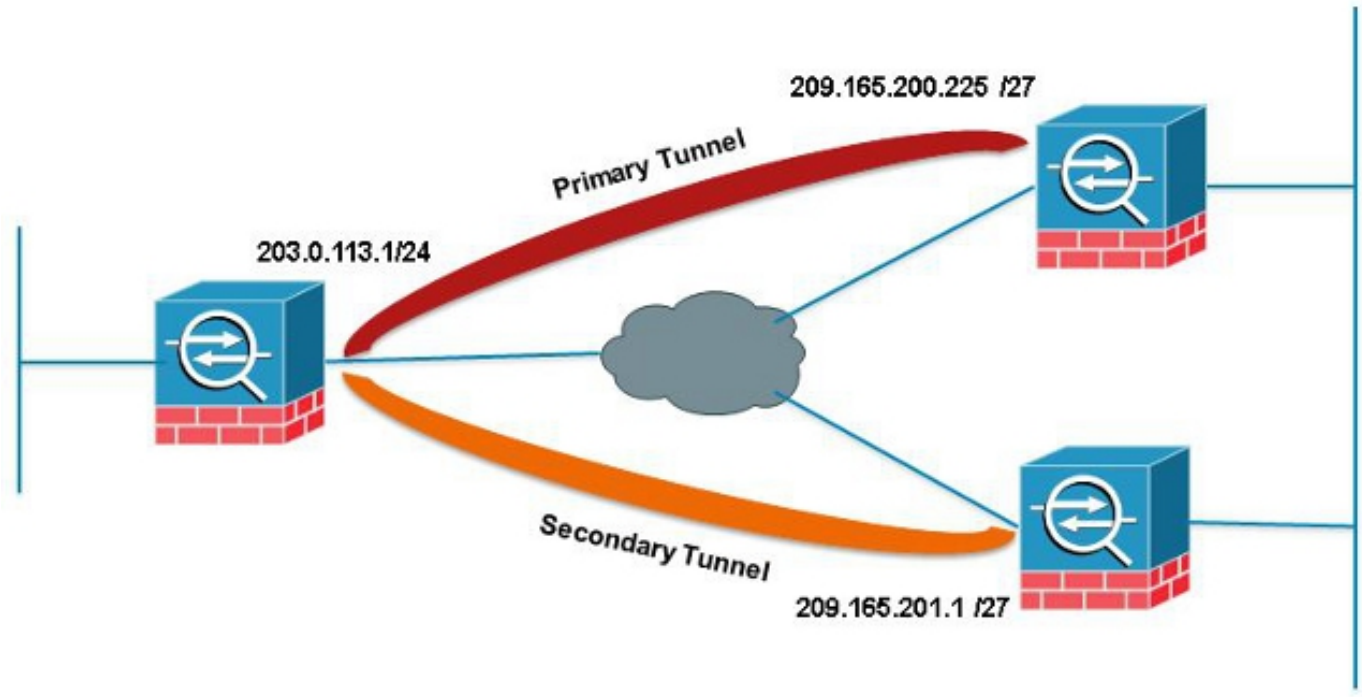
Embedded Event Manager era originariamente chiamato "background-debug" sull'appliance ASA ed era una funzionalità usata per eseguire il debug di un problema specifico. Dopo l'esame, è stato rilevato che era sufficientemente simile al software Cisco IOS EEM, quindi è stato aggiornato per corrispondere a tale CLI.

La funzionalità EEM consente di eseguire il debug dei problemi e fornisce la registrazione per scopi generici per la risoluzione dei problemi. L'EEM risponde agli eventi nel sistema EEM eseguendo azioni. Sono disponibili due componenti: gli eventi attivati da EEM e le applet del gestore eventi che definiscono le azioni. È possibile aggiungere più eventi a ogni applet di gestione eventi, in modo da richiamare le azioni configurate su di essa.

Priorità VPN

Se si configura una VPN con più indirizzi IP peer per una voce crittografica, la VPN viene stabilita con l'indirizzo IP peer di backup una volta che il peer primario diventa inattivo. Tuttavia, una volta che il peer primario ritorna, la VPN non ha diritto di priorità sull'indirizzo IP primario. È necessario eliminare manualmente l'associazione di protezione esistente per riavviare la negoziazione VPN e passare all'indirizzo IP primario.

```
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
```



Nell'esempio, viene usata un'aggregazione a livello di sito IP (SLA) per monitorare il tunnel primario. In caso di guasto del peer, il peer di backup subentra, ma lo SLA controlla ancora il server primario; una volta eseguito il backup del database primario, il syslog generato attiva l'EEM per cancellare il tunnel secondario, consentendo all'ASA di negoziare nuovamente con il database primario.

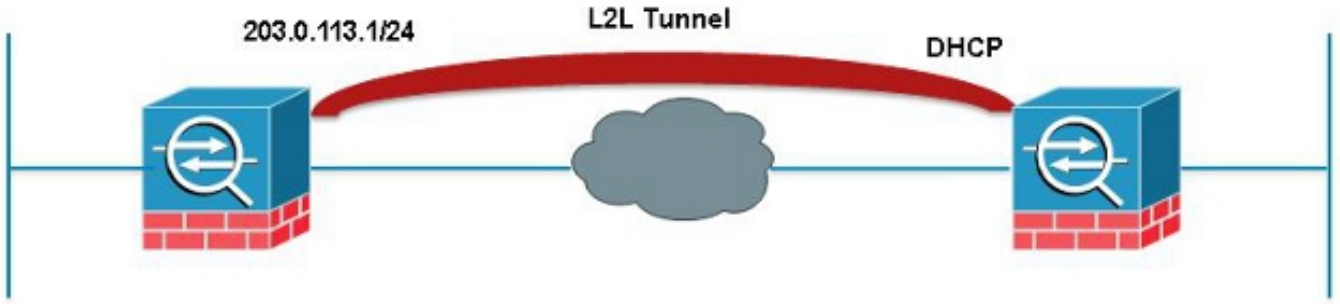
```
sla monitor 123
```

```
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 dinamico-statico sempre attivo

Quando si stabilisce un tunnel LAN-LAN, è necessario conoscere l'indirizzo IP di entrambi i peer IPSec. Se uno degli indirizzi IP non è noto perché è dinamico, ossia è ottenuto tramite DHCP, l'unica alternativa è utilizzare una mappa crittografica dinamica. Il tunnel può essere avviato solo dal dispositivo con l'IP dinamico, poiché l'altro peer non ha idea dell'IP in uso.

Questo è un problema nel caso in cui nessuno si trovi dietro il dispositivo con l'IP dinamico per attivare il tunnel in caso di disattivazione; quindi la necessità di avere sempre questo tunnel. Anche se si imposta il timeout di inattività su **none,** il problema non verrà risolto perché, in seguito a una nuova chiave, se non è presente traffico in transito sul tunnel, il problema si ridurrà. In quel momento, l'unico modo per far ripartire il tunnel è inviare il traffico proveniente dal dispositivo con l'IP dinamico. La stessa cosa si verifica se il tunnel si interrompe per un motivo imprevisto, ad esempio per un DPD, ecc.



L'EEM invierà un ping ogni 60 secondi attraverso il tunnel corrispondente all'associazione di sicurezza desiderata per mantenere la connessione attiva.

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

Disconnetti tutte le connessioni VPN esistenti in un determinato momento

L'appliance ASA non può impostare un tempo di interruzione delle sessioni VPN. In ogni caso, lo si fa con EEM. Nell'esempio viene mostrato come scollegare i client VPN e i client Anyconnect alle 17:00

```
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
```