EEM-Beispiele für unterschiedliche VPN-Szenarien auf ASA

Inhalt

Einführung

Der Cisco IOS® Software Embedded Event Manager (EEM) ist ein leistungsstarkes und flexibles Subsystem, das die Erkennung von Netzwerkereignissen in Echtzeit und integrierte Automatisierung ermöglicht. In diesem Dokument finden Sie Beispiele dafür, wie EEM in verschiedenen VPN-Szenarien hilfreich sein kann.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über die ASA EEM-Funktion verfügen.

Verwendete Komponenten

Dieses Dokument basiert auf der Cisco Adaptive Security Appliance (ASA), die Softwareversion 9.2(1) oder höher ausführt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

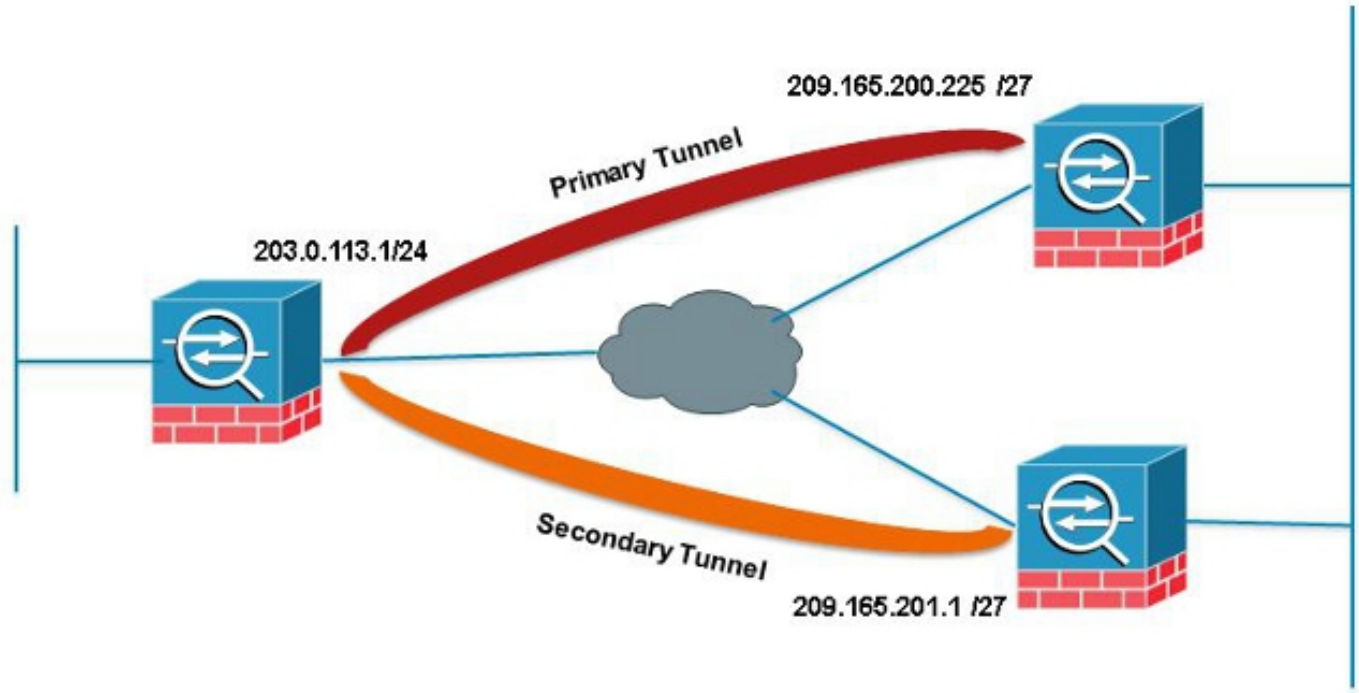
Der Embedded Event Manager wurde ursprünglich als "Hintergrunddebug" auf der ASA bezeichnet und war eine Funktion, die zum Debuggen eines bestimmten Problems verwendet wurde. Nach der Überprüfung wurde festgestellt, dass die EEM-Version der Cisco IOS-Software ähnlich war, sodass sie entsprechend der CLI aktualisiert wurde.

Die EEM-Funktion ermöglicht das Debuggen von Problemen und bietet eine allgemeine Protokollierung für die Fehlerbehebung. Der EEM reagiert durch Ausführen von Aktionen auf Ereignisse im EEM-System. Es gibt zwei Komponenten: Ereignisse, die der EEM auslöst, und Ereignismanager-Applets, die Aktionen definieren. Sie können jedem Ereignismanager-Applet mehrere Ereignisse hinzufügen, wodurch es veranlasst wird, die auf dem Applet konfigurierten Aktionen aufzurufen.

VPN-Preemption

Wenn Sie VPN mit mehreren Peer-IP-Adressen für einen Verschlüsselungseintrag konfigurieren, wird das VPN mit der Backup-Peer-IP eingerichtet, sobald der primäre Peer ausfällt. Sobald der primäre Peer wiederhergestellt ist, wird die primäre IP-Adresse vom VPN jedoch nicht vorbelegt. Sie müssen die vorhandene SA manuell löschen, um die VPN-Aushandlung erneut zu initiieren und auf die primäre IP-Adresse umzustellen.

```
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
```



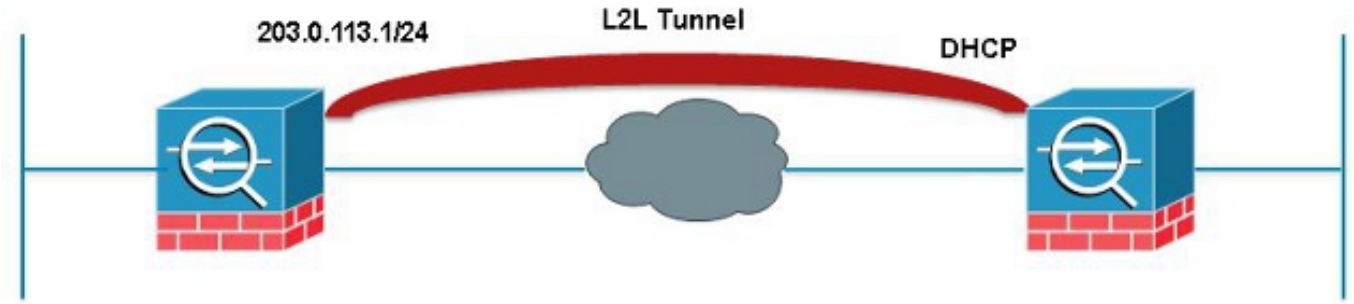
In diesem Beispiel wird eine IP Site Level Aggregation (SLA) verwendet, um den primären Tunnel zu überwachen. Wenn dieser Peer ausfällt, übernimmt der Backup-Peer, aber das SLA überwacht weiterhin das primäre Peer. Sobald der primäre Peer wieder aktiviert ist, löscht das generierte Syslog den EEM aus dem sekundären Tunnel, sodass die ASA erneut mit dem primären aushandeln kann.

```
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
```

Dynamisch zu statisch - L2L immer verfügbar

Beim Aufbau eines LAN-zu-LAN-Tunnels muss die IP-Adresse der beiden IPSec-Peers bekannt sein. Wenn eine der IP-Adressen nicht bekannt ist, weil sie dynamisch ist, d. h. über DHCP bezogen wird, ist die einzige Alternative die Verwendung einer dynamischen Crypto Map. Der Tunnel kann nur vom Gerät mit der dynamischen IP-Adresse initiiert werden, da der andere Peer keine Ahnung hat, welche IP-Adresse verwendet wird.

Dies ist ein Problem, falls niemand hinter dem Gerät mit der dynamischen IP-Adresse steht, um den Tunnel zu öffnen, falls er ausfällt. So muss dieser Tunnel immer verfügbar sein. Selbst wenn Sie die Leerlaufzeitüberschreitung auf **none** festlegen**,** wird das Problem dadurch nicht behoben, da bei einem erneuten Auftreten des Datenverkehrs der Tunnel ausfällt. In diesem Moment ist die einzige Möglichkeit, den Tunnel wieder hochzufahren, Datenverkehr vom Gerät mit der dynamischen IP zu senden. Dasselbe gilt, wenn der Tunnel aus einem unerwarteten Grund wie DPDs usw. ausfällt.



Dieser EEM sendet alle 60 Sekunden einen Ping an den Tunnel, der mit der gewünschten SA übereinstimmt, um die Verbindung aufrechtzuerhalten.

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

Trennen Sie alle vorhandenen VPN-Verbindungen zu einem bestimmten Zeitpunkt.

Die ASA bietet keine Möglichkeit, für VPN-Sitzungen eine feste Arbeitszeit festzulegen. Dies ist jedoch mit EEM möglich. Dieses Beispiel veranschaulicht, wie sowohl VPN-Clients als auch AnyConnect-Clients um 17:00 Uhr getrennt werden.

```
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
```