

ASA の異なる VPN シナリオに対する EEM の例

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[VPN のプリエンプション処理](#)

[Dynamic-to-Static L2L の常時稼働](#)

[既存のすべての VPN 接続を指定した時間に切断する](#)

概要

Cisco IOS[®] ソフトウェア Embedded Event Manager (EEM) は、リアルタイムのネットワーク イベント検出とオンボードの自動化を提供する強力で柔軟なサブシステムです。このドキュメントでは、さまざまな VPN シナリオで EEM を活用できる例を示します。

前提条件

要件

[ASA の EEM 機能](#)に関する知識があることを推奨します。

使用するコンポーネント

このドキュメントは、ソフトウェア バージョン 9.2(1) 以降が稼働する Cisco 適応型セキュリティ アプライアンス (ASA) に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

Embedded Event Manager は、当初は ASA の「バックグラウンド デバッグ」と呼ばれ、特定の問題をデバッグするために使用される機能でした。見直しの結果、これは Cisco IOS ソフトウエ

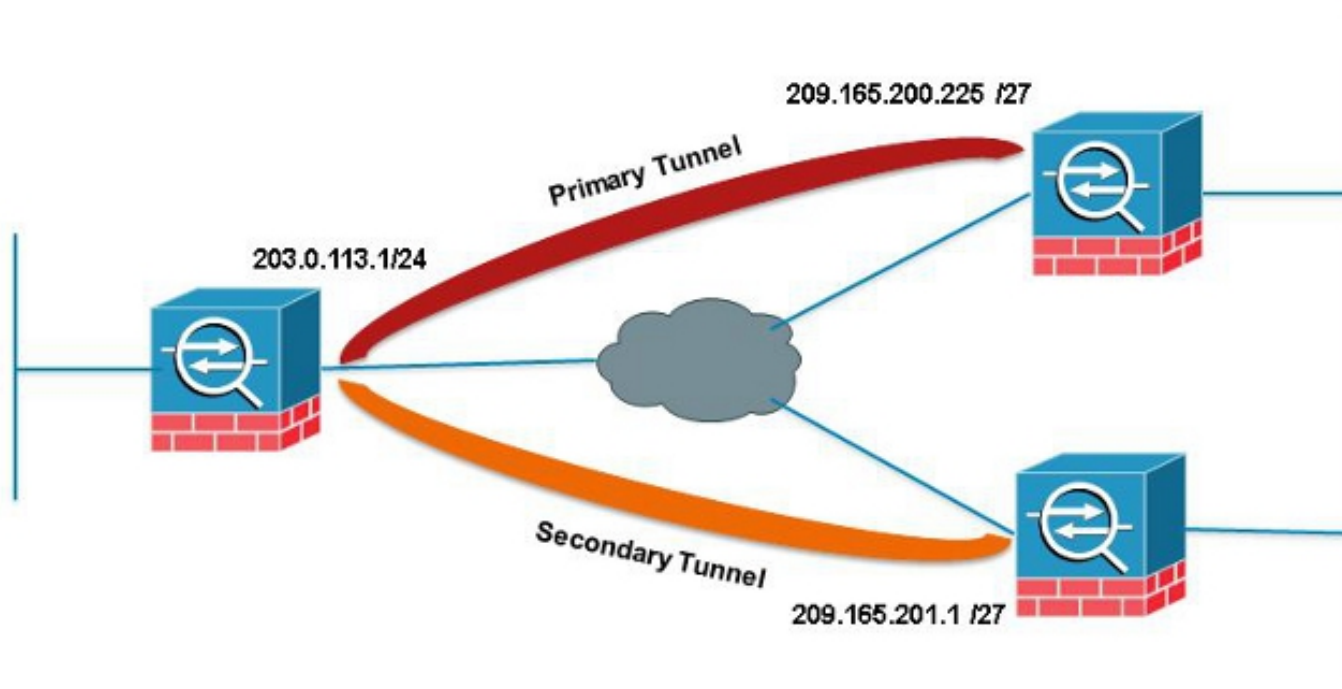
ア EEM とほぼ同じであることがわかったため、その CLI と一致するように更新されました。

EEM 機能を使用することで、問題をデバッグし、トラブルシューティング用の汎用ロギングを提供できます。EEM は、アクションを実行することで EEM システム内のイベントに応答します。2つのコンポーネントがあります。1つは EEM によってトリガーされるイベントで、もう1つはアクションを定義する Event Manager アプレットです。各 Event Manager アプレットに複数のイベントを追加できます。Event Manager アプレットはこれらのイベントをトリガーし、設定されたアクションを呼び出します。

VPN のプリエンブション処理

暗号エントリ用の複数のピア IP アドレスを使って VPN を設定すると、プライマリピアがダウンしたときにバックアップピアの IP を使って VPN が確立されます。しかし、プライマリピアが復帰しても、VPN はプライマリ IP アドレスにプリエンブションしません。プライマリ IP アドレスに切り替えるための VPN ネゴシエーションを再び開始するには、既存の SA を手動で削除する必要があります。

```
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
```



この例では、IP サイトレベル集約 (SLA) を使用してプライマリトンネルがモニタされています。そのピアに障害が発生すると、バックアップピアが引き継ぎますが、SLA は引き続きプライマリをモニタします。プライマリが復帰すると、生成された syslog によって EEM がトリガーされ、セカンダリトンネルがクリアされるため、ASA はプライマリと再びネゴシエートできるようになります。

```
sla monitor 123
type echo protocol icmpEcho 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

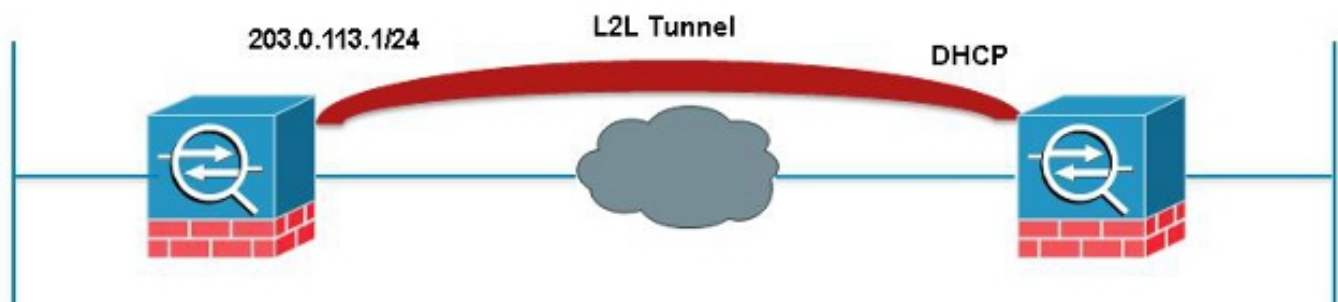
route outside 209.165.200.225 255.255.255.0 203.0.113.254 1 track 1

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
```

Dynamic-to-Static L2L の常時稼働

LAN 間トンネルを確立するときは、両方の IPsec ピアの IP アドレスを認識している必要があります。いずれかの IP アドレスが動的 IP アドレス (DHCP によって取得される IP アドレスなど) のために不明な場合、唯一の代替手段は、動的暗号マップを使用することです。トンネルは、動的 IP アドレスを持つデバイスからのみ開始できます。これは、もう一方のピアが使用される IP を特定できないためです。

これは、動的 IP を持つデバイスがダウンしたときに、その背後にトンネルを開始できるユーザがない場合に問題になります。このため、このトンネルを常に稼働させておく必要があります。アイドルタイムアウトをなしに設定しても、キーが再生成されたときに通過するトラフィックがなければトンネルがダウンするため、問題は解決しません。その場合にトンネルを再開する唯一の方法は、動的 IP アドレスを持つデバイスからトラフィックを送信することです。予想外の理由 (DPD など) でトンネルがダウンする場合も、同じことが当てはまります。



この EEM は、接続を維持するため、目的の SA に一致するトンネルを介して 60 秒ごとに ping を送信します。

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

既存のすべての VPN 接続を指定した時間に切断する

ASA には、VPN セッションを決まった時間に切断するよう設定する方法がありません。しかし、EEM を使ってこれを実行できます。次の例は、午後 5:00 に VPN クライアントと AnyConnect クライアントの両方を切断する方法を示しています。

```
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
```