# ASA의 다양한 VPN 시나리오에 대한 EEM 예

## 목차



## 소개

Cisco IOS® EEM(Software Embedded Event Manager)은 실시간 네트워크 이벤트 탐지 및 온보드 자동화를 제공하는 강력하고 유연한 서브시스템입니다.이 문서에서는 EEM이 다양한 VPN 시나리오에서 어떤 도움을 줄 수 있는지 예를 제공합니다

## 사전 요구 사항

### 요구 사항

Cisco에서는 ASA EEM 기능에 대해 알고 있는 것이 좋습니다.

### 사용되는 구성 요소

이 문서는 소프트웨어 버전 9.2(1) 이상을 실행하는 Cisco ASA(Adaptive Security Appliance)를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 배경 정보

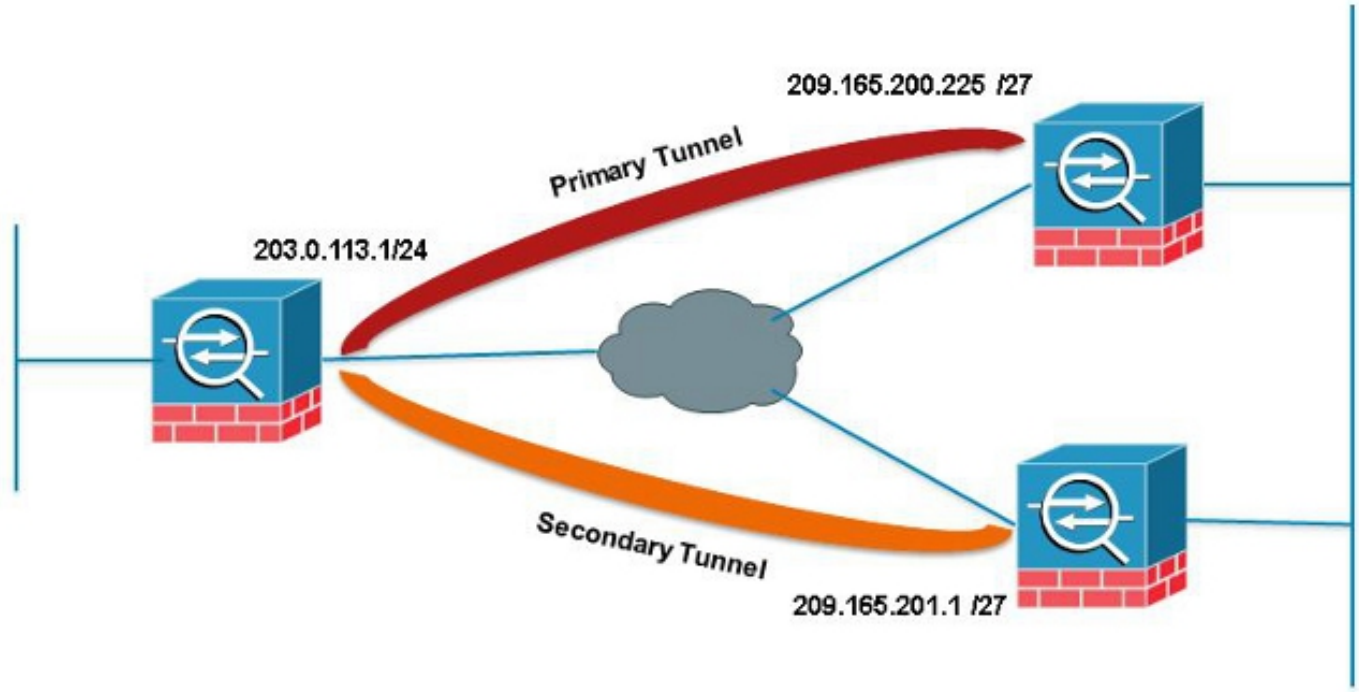
Embedded Event Manager는 원래 ASA에서 "background-debug"로 호출되었으며 특정 문제를 디버깅하는 데 사용되는 기능입니다.검토 후 Cisco IOS Software EEM과 충분히 비슷한 것으로 확인되었으므로 해당 CLI와 일치하도록 업데이트되었습니다.

EEM 기능을 사용하면 문제를 디버깅할 수 있으며 문제 해결을 위한 범용 로깅을 제공합니다 .EEM은 작업을 수행하여 EEM 시스템의 이벤트에 응답합니다.두 가지 구성 요소가 있습니다 .EEM이 트리거하는 이벤트 및 작업을 정의하는 이벤트 관리자 애플릿입니다.각 이벤트 관리자 애플릿에 여러 이벤트를 추가할 수 있으며, 이를 통해 구성된 작업을 호출하게 됩니다.

# VPN 선점

암호화 항목에 대해 여러 피어 IP 주소를 사용하여 VPN을 구성하는 경우 기본 피어가 다운되면 백업 피어 IP로 VPN이 설정됩니다.그러나 기본 피어가 돌아오면 VPN은 기본 IP 주소를 선점하지 않습니다.VPN 협상을 다시 시작하여 기본 IP 주소로 전환하려면 기존 SA를 수동으로 삭제해야 합니다.

```
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
```




이 예에서는 기본 터널을 모니터링하기 위해 IP SLA(Site Level Aggregation)를 사용합니다.해당 피어가 실패하면 백업 피어가 인계되지만 SLA는 여전히 기본 피어를 모니터링합니다.Primary(기본 )가 백업되면 생성된 syslog가 EEM을 트리거하여 보조 터널을 지워 ASA가 Primary(기본)와 다시 협상할 수 있게 합니다.

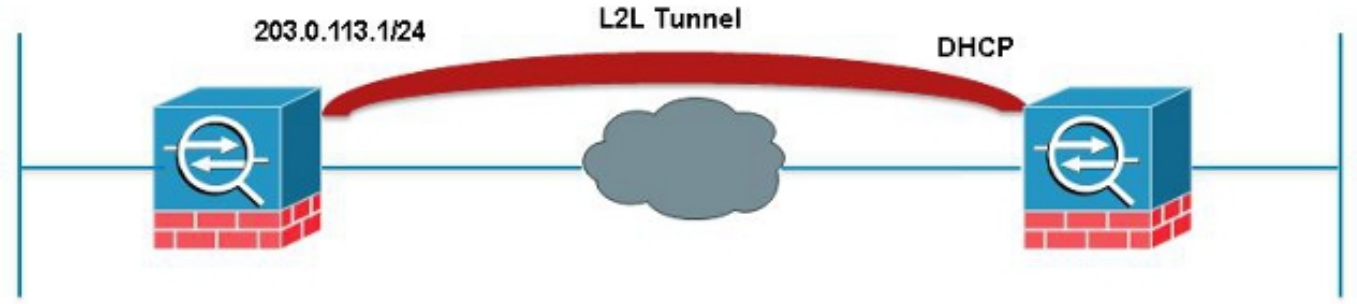
```
sla monitor 123
type echo protocol ipIcmpEcho 209.165.200.225 interface outside
num-packets 3
frequency 10

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
```

# Dynamic-to-Static L2L 항상 작동

LAN-to-LAN 터널을 설정할 때 두 IPSec 피어의 IP 주소를 알아야 합니다.IP 주소 중 하나가 동적(즉, DHCP를 통해 얻어진 경우, 동적 암호화 맵을 사용하는 것이 유일한 대안입니다.다른 피어가 사용 중인 IP를 알지 못하기 때문에 동적 IP를 사용하는 디바이스에서만 터널을 시작할 수 있습니다.

이 문제는 터널이 다운될 경우에 대비하여 동적 IP를 사용하여 디바이스 뒤에 있는 사람이 없는 경우에 발생합니다.따라서 이 터널을 항상 가동해야 합니다.idle-timeout을 **none**으로 설정하더라도 rekey에 따라 터널을 통과하는 트래픽이 없는 경우 터널이 중단되므로 이 작업은 문제를 해결하지 않습니다.이때 터널을 다시 가동하는 유일한 방법은 동적 IP를 사용하여 디바이스에서 트래픽을 보내는 것입니다.터널이 DPD와 같은 예기치 않은 이유로 다운될 경우에도 마찬가지입니다.




이 EEM은 연결을 유지하기 위해 원하는 SA와 일치하는 터널을 통해 60초마다 ping을 보냅니다.

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

# 특정 시간에 모든 VPN 기존 연결 끊기

ASA는 VPN 세션에 대해 하드 컷오프 시간을 설정할 방법이 없습니다.그러나 EEM을 사용하면 됩니다.이 예에서는 오후 5:00에 VPN 클라이언트와 Anyconnect 클라이언트를 모두 검색하는 방법을 보여 줍니다.

```
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
```