EEM Examples for Different VPN Scenarios on ASA

Contents

Introduction

The Cisco IOS® Software Embedded Event Manager (EEM) is a powerful and flexible subsystem that provides real-time network event detection and onboard automation. This document gives you examples of where EEM can help in different VPN scenarios

Prerequisites

Requirements

Cisco recommends that you have knowledge of the ASA EEM feature.

Components Used

This document is based on the Cisco Adaptive Security Appliance (ASA) that runs software Version 9.2(1) or later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

Embedded Event Manager was originally called "background-debug" on the ASA, and was a

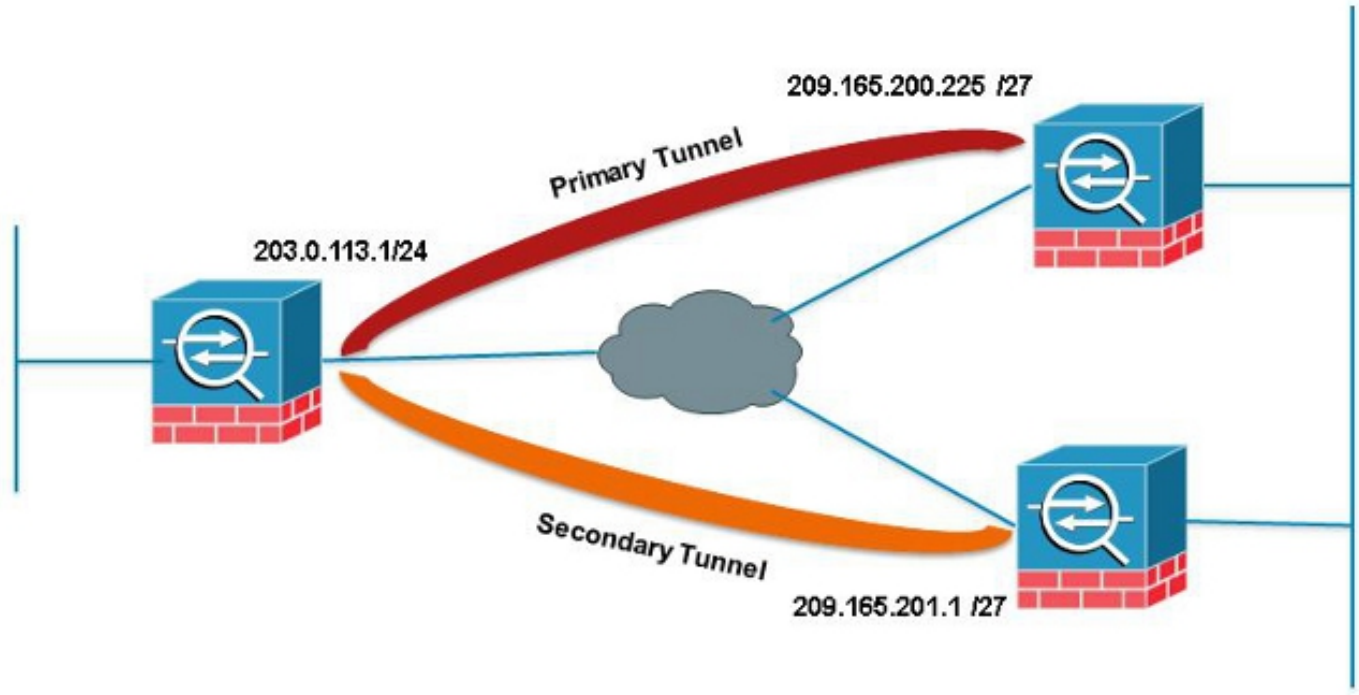
feature used to debug a specific issue. After review, it was found to be similar enough to Cisco IOS Software EEM, so it was updated to match that CLI.

The EEM feature enables you to debug problems and provides general purpose logging for troubleshooting. The EEM responds to events in the EEM system by performing actions. There are two components: events that the EEM triggers, and event manager applets that define actions. You may add multiple events to each event manager applet, which triggers it to invoke the actions that have been configured on it.

VPN Preempt

If you configure VPN with multiple peer IP addresses for a crypto entry, the VPN gets established with the backup peer IP once the primary peer goes down. However, once the primary peer comes back, the VPN does not preempt to the primary IP address. You must manually delete the existing SA in order to reinitiate the VPN negotiation to switch it over to the primary IP address.

```
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 this example, an IP site level aggregation (SLA) is used in order to monitor the Primary tunnel. If that peer fails, the backup peer takes over but the SLA still monitors the primary; once the Primary comes back up the generated syslog will trigger the EEM to clear the Secondary tunnel allowing the ASA to re-negotiate with the Primary again.

```
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
```

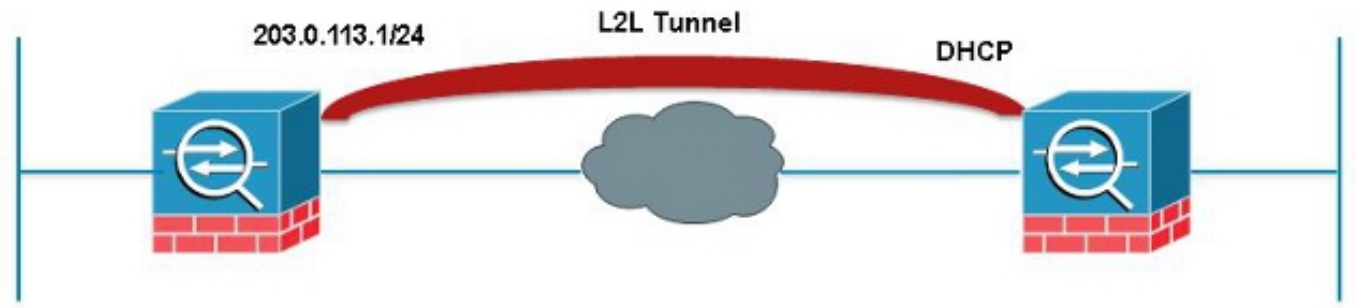
```
route outside 209.165.200.225 255.255.255.0 203.0.113.254 1 track 1

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 Always Up

When establishing a LAN-to-LAN tunnel, the IP address of both IPSec peers needs to be known. If one of the IP addresses is not known because it is dynamic, i.e. obtained via DHCP, then the only alternative is to use a dynamic crypto map. The tunnel can only be initiated from the device with the dynamic IP since the other peer has no idea of the IP being used.

This is a problem in case nobody is behind the device with the dynamic IP to bring up the tunnel in case it goes down; thus the need of having this tunnel always up. Even if you set the idle-timeout to **none,** this will not address the issue because, upon a rekey, if there is no traffic passing the tunnel will go down. At that moment the only way to bring up the tunnel again is to send traffic from the device with the dynamic IP. The same thing applies if the tunnel goes down for an unexpected reason such as DPDs, etc.



This EEM will send a ping every 60 seconds across the tunnel matching the desired SA in order to keep the connection up.

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

Disconnect All VPN Existing Connections at a Certain Time

The ASA does not have a way to set a hard cut off time for VPN sessions. However you do this with EEM. This example demonstrates how to dicsonnect both VPN Clients and Anyconnect Clients at 5:00 PM

```
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
```