Примеры EEM для других сценариев VPN на ASA

Содержание

Введение

Встроенный диспетчер событий (EEM) программного обеспечения Cisco IOS является мощной и гибкой подсистемой, которая предоставляет обнаружение события сети реального времени и встроенную автоматизацию. Этот документ дает вам примеры того, где EEM может помочь в других сценариях VPN

Предварительные условия

Требования

Cisco рекомендует ознакомиться с ASA функцию EEM.

Используемые компоненты

Этот документ основывается на устройстве адаптивной защиты Cisco (ASA), который работает под управлением ПО версии 9.2 (1) или позже.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

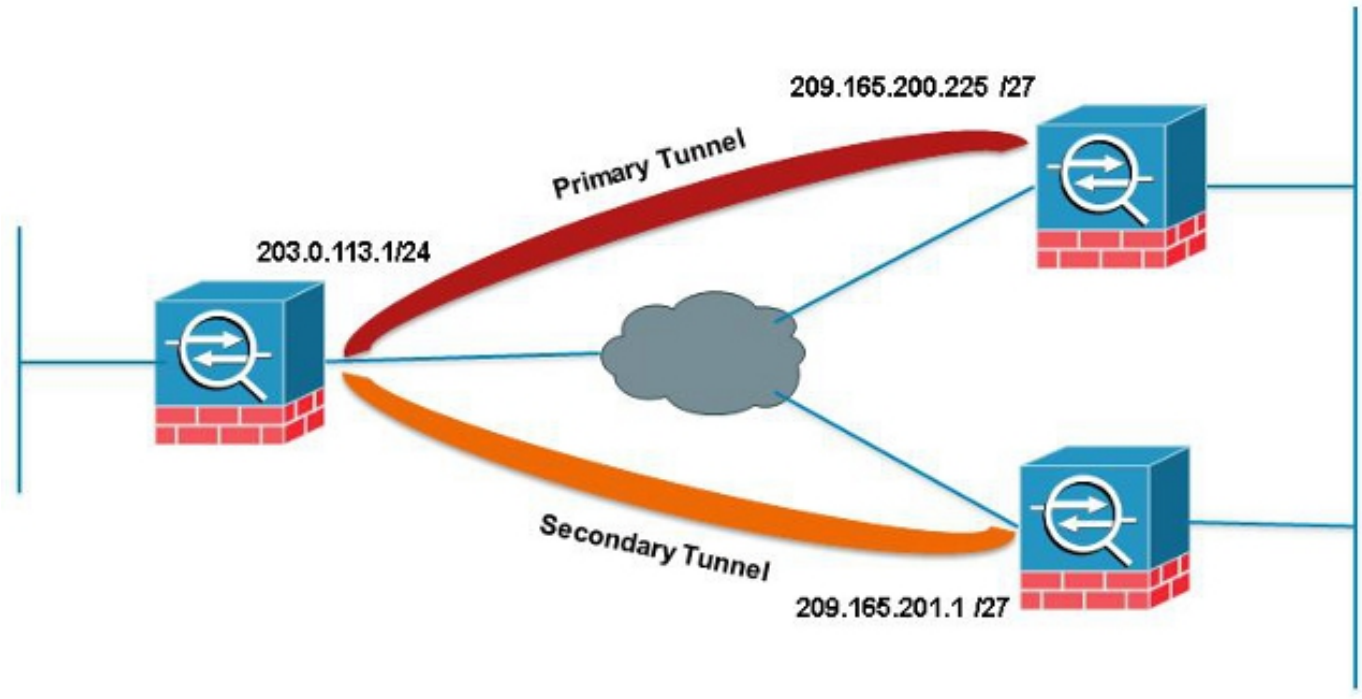
Встроенного Диспетчера событий первоначально назвали "фоновой отладкой" на ASA и был функцией, использованной для отладки конкретного вопроса. После анализа это, как находили, было достаточно подобно программному обеспечению Cisco IOS EEM, таким образом, это было обновлено для соответствия с тем CLI.

Функция EEM позволяет вам отладить проблемы и предоставляет регистрацию общей цели для устранения проблем. EEM отвечает на события в системе EEM путем выполнения действий. Существует два компонента: события, которые EEM инициирует, и event manager applet, который определяет действия. Можно добавить несколько событий к каждому event manager applet, который инициирует его для призыва действий, которые были настроены на нем.

VPN вытесняет

При настройке VPN с IP-адресами множественных одноранговых телефонных соединений для крипто-записи VPN установлена с IP резервного узла, как только выключается основная адресуемая точка. Однако, как только основная адресуемая точка возвращается, VPN не вытесняет к основному IP - адресу. Необходимо вручную удалить существующий SA, чтобы повторно инициировать согласование VPN для переключения его на основной IP - адрес.

```
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
```



В данном примере агрегация уровня узла (SLA) IP используется для мониторинга Основного туннеля. Если тот узел отказывает, резервный узел вступает во владение, но SLA все еще контролирует основного; как только Основной прибывает назад, генерируемый системный журнал инициирует EEM для очистки Вторичного туннеля, позволяющего ASA пересматривать с Основным снова.

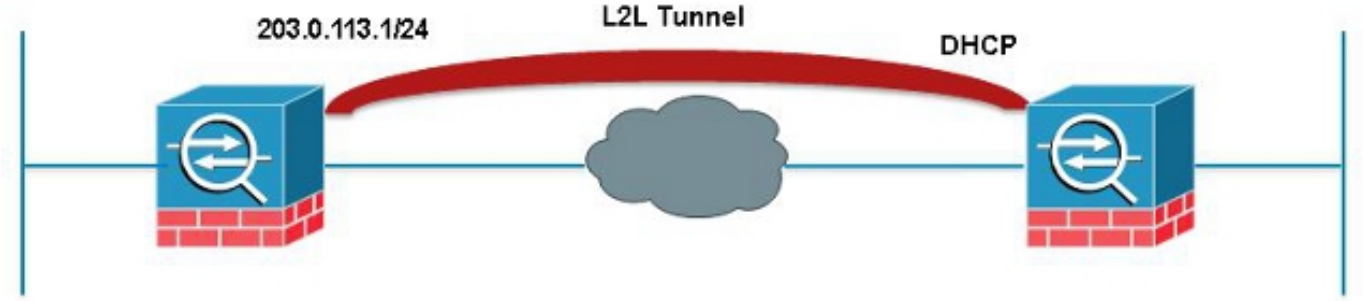
```
sla monitor 123
type echo protocol ipIcmpEcho 209.165.200.225 interface outside
```

```
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
```

Динамический-к-статичному L2L всегда

При установлении туннеля между локальными сетями (LAN-to-LAN) должен быть известен IP-адрес обоих Узлов IPsec. Если один из IP-адресов не известен, потому что это динамично, т.е. полученное через DHCP, то единственная альтернатива должна использовать динамическую криптокарту. Туннель может только инициироваться от устройства с динамическим IP, так как другой узел понятия не имеет об используемом IP.

Это - проблема в случае, если никто не находится позади устройства с динамическим IP для внедрения туннеля в случае, если это выключается; таким образом потребность наличия этого туннеля всегда. Даже при установке idle-timeout ни в **один** это не решит проблему потому что после повторно введения, если будет "no traffic" (нет трафика), передающий туннель, то выключится. В тот момент единственный способ перевести туннель в рабочее состояние снова состоит в том, чтобы передать трафик от устройства с динамическим IP. Если туннель выключается по неожиданной причине, такой как DPD, и т.д., та же вещь применяется.



Этот EEM будет передавать эхо-запрос каждые 60 секунд через туннель, совпадающий с желаемым SA для продолжения соединения.

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

Разъедините все существующие соединения VPN в определенное время

ASA не имеет способа установить трудное отключенное время для сеансов VPN. Однако, вы делаете это с EEM. Данный пример демонстрирует как к dicsonnect оба Клиента VPN и Клиенты Anyconnect в 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
```