Cisco IOS XE 라우터에서 Multi-SA 가상 터널 인터페이스 구성

목차

소개

이 문서에서는 Cisco IOS® XE 소프트웨어를 사용하여 Cisco 라우터에 Multi-SA(Multi-Security Association) VTI(Virtual Tunnel Interface)를 구성하는 방법에 대해 설명합니다. 마이그레이션 프로세스에 대해서도 설명합니다. Multi-SA VTI는 암호화 맵 기반(정책 기반) VPN 컨피그레이션을 대체하는 것입니다. 이는 암호화 맵 기반 및 기타 정책 기반 구현과 역호환됩니다. 이 기능에 대한 지원은 Cisco IOS XE Release 16.12 이상에서 제공됩니다.

사전 요구 사항

요구 사항

Cisco에서는 Cisco IOS XE 라우터의 IPsec VPN 컨피그레이션에 대해 알고 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco IOS XE Release 16.12.01a를 사용하는 ISR(Integrated Services Router) 4351을 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 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

암호화 맵에 대한 VTI의 장점

암호화 맵은 물리적 인터페이스의 출력 기능입니다. 서로 다른 피어에 대한 터널은 동일한 암호화 맵에서 구성됩니다. 암호화 맵 ACL(Access Control List) 항목은 특정 VPN 피어로 전송할 트래픽을 확인하는 데 사용됩니다. 이러한 컨피그레이션 유형을 정책 기반 VPN이라고도 합니다.

VTI의 경우 각 VPN 터널은 별도의 논리적 터널 인터페이스로 표시됩니다. 라우팅 테이블은 트래픽을 전송할 VPN 피어를 결정합니다. 이러한 컨피그레이션 유형을 경로 기반 VPN이라고도 합니다.

Cisco IOS XE Release 16.12 이전 릴리스에서는 VTI 컨피그레이션이 암호화 맵 컨피그레이션과 호환되지 않았습니다. 상호 운용을 위해서는 터널의 양 끝을 동일한 유형의 VPN으로 구성해야 했습니다.

Cisco IOS XE Release 16.12에는 터널 인터페이스가 프로토콜 레벨에서 정책 기반 VPN으로 작동하지만 터널 인터페이스의 모든 속성을 가질 수 있는 새로운 컨피그레이션 옵션이 추가되었습니다.

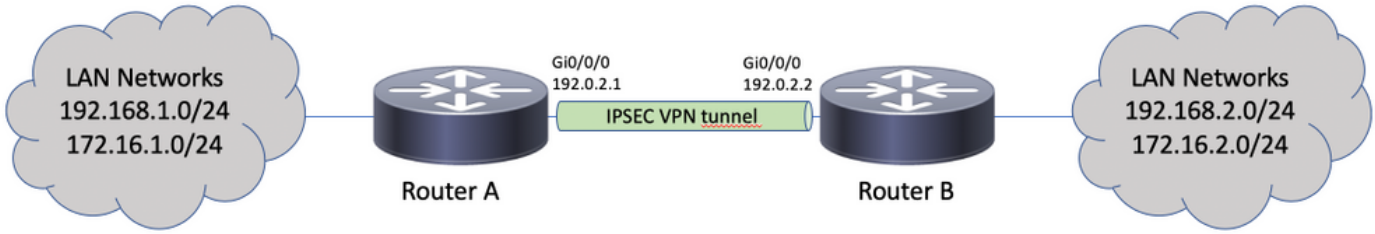
Cisco는 Cisco IOS XE Release 17.6에서 Cisco IPsec Static Crypto Map 및 Dynamic Crypto Map 기능의 End-of-Life 날짜를 발표했습니다.

암호화 맵에 비해 VTI의 장점은 다음과 같습니다.

- 터널 작동/중단 상태를 더 쉽게 확인할 수 있습니다.
- 문제 해결이 더 쉽습니다.
- QoS(Quality of Service), ZBF(Zone-Based Firewall), NAT(Network Address Translation), Netflow와 같은 기능을 터널별로 적용할 수 있습니다.
- 모든 유형의 VPN 터널에 대해 간소화된 컨피그레이션을 제공합니다.

구성

네트워크 다이어그램



라우팅 고려 사항

관리자는 원격 네트워크의 라우팅이 터널 인터페이스를 가리키는지 확인해야 합니다. 이 **reverse-route** ipsec 프로필 아래의 옵션을 사용하여 암호화 ACL에 지정된 네트워크에 대한 고정 경로를 자동으로 생성할 수 있습니다. 이러한 경로는 수동으로 추가할 수도 있습니다. 이전에 구성된 더 구체적인 경로가 있는 경우, 해당 경로는 터널 인터페이스가 아닌 물리적 인터페이스를 가리키므로 이러한 경로는 제거해야 합니다.

구성 예

암호화 맵 기반 IKEv1 터널을 Multi-SA sVTI로 마이그레이션

두 라우터 모두 IKEv1(Internet Key Exchange Version 1) 암호화 맵 기반 솔루션으로 사전 구성되어 있습니다.

라우터 A

```
crypto isakmp policy 10
encryption aes
hash sha256
authentication pre-share
group 14
!
crypto isakmp key cisco123 address 192.0.2.2
!
crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
!
crypto map CMAP 10 ipsec-isakmp
set peer 192.0.2.2
set transform-set TSET
match address CACL
!
ip access-list extended CACL
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
!
interface GigabitEthernet0/0/0
ip address 192.0.2.1 255.255.255.0
crypto map CMAP
```

라우터 B

```
crypto isakmp policy 10
encryption aes
hash sha256
authentication pre-share
group 14
!
crypto isakmp key cisco123 address 192.0.2.1
!
crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
!
crypto map CMAP 10 ipsec-isakmp
set peer 192.0.2.1
set transform-set TSET
match address CACL
!
ip access-list extended CACL
permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
permit ip 172.16.2.0 0.0.0.255 172.16.1.0 0.0.0.255
!
interface GigabitEthernet0/0/0
ip address 192.0.2.2 255.255.255.0
crypto map CMAP
```

라우터 A를 multi-SA VTI 컨피그레이션으로 마이그레이션하려면 다음 단계를 완료하십시오. 라우터 B는 기존 컨피그레이션에 그대로 유지되거나 유사하게 재구성될 수 있습니다.

1. 인터페이스에서 암호화 맵을 제거합니다.
   ```
   interface GigabitEthernet0/0/0
   no crypto map
   ```
2. IPsec 프로필을 생성합니다. Reverse-route는 원격 네트워크에 대한 고정 경로를 라우팅 테이블에 자동으로 추가하도록 선택적으로 구성됩니다.
   ```
   crypto ipsec profile PROF
   set transform-set TSET
   reverse-route
   ```
3. 터널 인터페이스를 구성합니다. 암호화 ACL은 터널 컨피그레이션에 IPsec 정책으로 연결됩니다. 터널 인터페이스에 구성된 IP 주소는 관련이 없지만 일부 값으로 구성해야 합니다. IP 주소는 **ip unnumbered** 명령을 사용합니다:
   ```
   interface Tunnel0
   ip unnumbered GigabitEthernet0/0/0
   tunnel source GigabitEthernet0/0/0
   tunnel mode ipsec ipv4
   tunnel destination 192.0.2.2
   tunnel protection ipsec policy ipv4 CACL
   tunnel protection ipsec profile PROF
   ```
4. 암호화 맵 항목은 이후에 완전히 제거될 수 있습니다.
   ```
   no crypto map CMAP 10
   ```

   최종 라우터 A 컨피그레이션

   ```
   crypto isakmp policy 10
   encryption aes
   hash sha256
   authentication pre-share
   group 14
   !
   crypto isakmp key cisco123 address 192.0.2.2
   !
   crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
   !
   crypto ipsec profile PROF
   set transform-set TSET
   reverse-route
   !
   ip access-list extended CACL
   permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
   permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
   !
   interface GigabitEthernet0/0/0
   ip address 192.0.2.1 255.255.255.0
   !
   interface Tunnel0
   ip unnumbered GigabitEthernet0/0/0
   tunnel source GigabitEthernet0/0/0
   tunnel mode ipsec ipv4
   tunnel destination 192.0.2.2
   tunnel protection ipsec policy ipv4 CACL
   tunnel protection ipsec profile PROF
   ```

암호화 맵 기반 IKEv2 터널을 Multi-SA sVTI로 마이그레이션

두 라우터 모두 IKEv2(Internet Key Exchange Version 2) 암호화 맵 기반 솔루션으로 사전 구성되어 있습니다.

라우터 A

```
crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
```

```
!
crypto ikev2 profile PROF
match identity remote address 192.0.2.2 255.255.255.255
authentication remote pre-share key cisco123
authentication local pre-share key cisco123
!
crypto map CMAP 10 ipsec-isakmp
set peer 192.0.2.2
set transform-set TSET
set ikev2-profile PROF
match address CACL
!
ip access-list extended CACL
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
!
interface GigabitEthernet0/0/0
ip address 192.0.2.1 255.255.255.0
crypto map CMAP
```

라우터 B

```
crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
!
crypto ikev2 profile PROF
match identity remote address 192.0.2.1 255.255.255.255
authentication remote pre-share key cisco123
authentication local pre-share key cisco123
!
crypto map CMAP 10 ipsec-isakmp
set peer 192.0.2.1
set transform-set TSET
set ikev2-profile PROF
match address CACL
!
ip access-list extended CACL
permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
permit ip 172.16.2.0 0.0.0.255 172.16.1.0 0.0.0.255
!
interface GigabitEthernet0/0/0
ip address 192.0.2.2 255.255.255.0
crypto map CMAP
```

라우터 A를 multi-SA VTI 컨피그레이션으로 마이그레이션하려면 다음 단계를 완료하십시오. 라우터 B는 기존 컨피그레이션을 그대로 유지하거나 유사하게 재구성할 수 있습니다.

1. 인터페이스에서 암호화 맵을 제거합니다.
   ```
   interface GigabitEthernet0/0/0
   no crypto map
   ```
2. IPsec 프로필을 생성합니다. 이 **reverse-route** 원격 네트워크에 대한 고정 경로를 라우팅 테이블에 자동으로 추가하도록 명령을 구성할 수도 있습니다.
   ```
   crypto ipsec profile PROF
   set transform-set TSET
   set ikev2-profile PROF
   reverse-route
   ```
3. 터널 인터페이스를 구성합니다. 암호화 ACL은 터널 컨피그레이션에 IPsec 정책으로 연결됩니다. 터널 인터페이스에 구성된 IP 주소는 관련이 없지만 일부 값으로 구성해야 합니다. IP 주소는 **ip unnumbered** 명령을 사용합니다:
   ```
   interface Tunnel0
   ip unnumbered GigabitEthernet0/0/0
   tunnel source GigabitEthernet0/0/0
   ```

```
tunnel mode ipsec ipv4
tunnel destination 192.0.2.2
tunnel protection ipsec policy ipv4 CACL
tunnel protection ipsec profile PROF
```

4. 이후에 암호화 맵을 완전히 제거합니다.

```
no crypto map CMAP 10
```

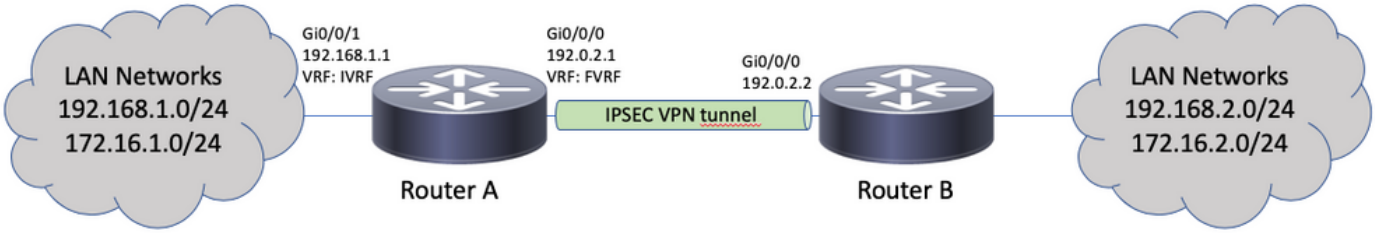
최종 라우터 A 컨피그레이션

```
crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
!
crypto ikev2 profile PROF
match identity remote address 192.0.2.2 255.255.255.255
authentication remote pre-share key cisco123
authentication local pre-share key cisco123
!
crypto ipsec profile PROF
set transform-set TSET
set ikev2-profile PROF
reverse-route
!
ip access-list extended CACL
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
!
interface GigabitEthernet0/0/0
ip address 192.0.2.1 255.255.255.0
!
interface Tunnel0
ip unnumbered GigabitEthernet0/0/0
tunnel source GigabitEthernet0/0/0
tunnel mode ipsec ipv4
tunnel destination 192.0.2.2
tunnel protection ipsec policy ipv4 CACL
tunnel protection ipsec profile PROF
```

VRF 인식 암호화 맵을 Multi-SA VTI로 마이그레이션

이 예에서는 VRF 인식 암호화 맵 컨피그레이션을 마이그레이션하는 방법을 보여줍니다.

토폴로지



암호화 맵 컨피그레이션

```
ip vrf fvrf
ip vrf ivrf
!
crypto keyring KEY vrf fvrf
pre-shared-key address 192.0.2.2 key cisco123
!
crypto isakmp policy 10
encryption aes
```

```
hash sha256
authentication pre-share
group 14
!
crypto isakmp profile PROF
vrf ivrf
keyring KEY
match identity address 192.0.2.2 255.255.255.255 fvrf
!
crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
!
crypto map CMAP 10 ipsec-isakmp
set peer 192.0.2.2
set transform-set TSET
set isakmp-profile PROF
match address CACL
!
interface GigabitEthernet0/0/0
ip vrf forwarding fvrf
ip address 192.0.2.1 255.255.255.0
crypto map CMAP
!
interface GigabitEthernet0/0/1
ip vrf forwarding ivrf
ip address 192.168.1.1 255.255.255.0
!
ip route vrf ivrf 172.16.2.0 255.255.255.0 GigabitEthernet0/0/0 192.0.2.2
ip route vrf ivrf 192.168.2.0 255.255.255.0 GigabitEthernet0/0/0 192.0.2.2
!
ip access-list extended CACL
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
```

다음은 multi-SA VTI로 마이그레이션하는 데 필요한 단계입니다.

```
! vrf configuration under isakmp profile is only for crypto map based configuration
!
crypto isakmp profile PROF
no vrf ivrf
!
interface GigabitEthernet0/0/0
no crypto map
!
no crypto map CMAP 10
!
no ip route vrf ivrf 172.16.2.0 255.255.255.0 GigabitEthernet0/0/0 192.0.2.2
no ip route vrf ivrf 192.168.2.0 255.255.255.0 GigabitEthernet0/0/0 192.0.2.2
!
crypto ipsec profile PROF
set transform-set TSET
set isakmp-profile PROF
reverse-route
!
interface tunnel0
ip vrf forwarding ivrf
ip unnumbered GigabitEthernet0/0/0
tunnel source GigabitEthernet0/0/0
tunnel mode ipsec ipv4
tunnel destination 192.0.2.2
tunnel vrf fvrf
tunnel protection ipsec policy ipv4 CACL
tunnel protection ipsec profile PROF
```

최종 VRF 인식 컨피그레이션

```
ip vrf fvrf
ip vrf ivrf
!
crypto keyring KEY vrf fvrf
pre-shared-key address 192.0.2.2 key cisco123
!
crypto isakmp policy 10
encryption aes
hash sha256
authentication pre-share
group 14
!
crypto isakmp profile PROF
keyring KEY
match identity address 192.0.2.2 255.255.255.255 fvrf
!
crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
!
interface GigabitEthernet0/0/0
ip vrf forwarding fvrf
ip address 192.0.2.1 255.255.255.0
!
interface GigabitEthernet0/0/1
ip vrf forwarding ivrf
ip address 192.168.1.1 255.255.255.0
!
ip access-list extended CACL
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
!
crypto ipsec profile PROF
set transform-set TSET
set isakmp-profile PROF
reverse-route
!
interface tunnel0
ip vrf forwarding ivrf
ip unnumbered GigabitEthernet0/0/0
tunnel source GigabitEthernet0/0/0
tunnel mode ipsec ipv4
tunnel destination 192.0.2.2
tunnel vrf fvrf
tunnel protection ipsec policy ipv4 CACL
tunnel protection ipsec profile PROF
```

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

Cisco CLI Analyzer(등록된 고객만 해당)는 **show** 명령을 사용합니다. Cisco CLI Analyzer를 사용하여 **show** 명령 출력.

터널이 성공적으로 협상되었는지 확인하기 위해 터널 인터페이스 상태를 확인할 수 있습니다. 마지막 두 열 - Status 및 Protocol - 상태 표시 up 터널이 작동 중인 경우:

```
RouterA#show ip interface brief | include Interface|Tunnel0
Interface IP-Address OK? Method Status Protocol
Tunnel0 192.0.2.1 YES TFTP up                    up
```

현재 암호화 세션 상태에 대한 자세한 내용은 **show crypto session** 성과. 이 Session status 의 UP-ACTIVE ike

세션이 올바르게 협상되었음을 나타냅니다.

```
RouterA#show crypto session interface tunnel0
Crypto session current status

Interface: Tunnel0
Profile: PROF
Session status: UP-ACTIVE
Peer: 192.0.2.2 port 500
Session ID: 2
IKEv2 SA: local 192.0.2.1/500 remote 192.0.2.2/500 Active
IPSEC FLOW: permit ip 172.16.1.0/255.255.255.0 172.16.2.0/255.255.255.0
Active SAs: 2, origin: crypto map
IPSEC FLOW: permit ip 192.168.1.0/255.255.255.0 192.168.2.0/255.255.255.0
Active SAs: 2, origin: crypto map
```

올바른 터널 인터페이스를 통해 원격 네트워크 포인트로 라우팅되는지 확인합니다.

```
RouterA#show ip route 192.168.2.0
Routing entry for 192.168.2.0/24
Known via "static", distance 1, metric 0 (connected)
Routing Descriptor Blocks:
* directly connected, via Tunnel0
Route metric is 0, traffic share count is 1

RouterA#show ip cef 192.168.2.100
192.168.2.0/24
attached to Tunnel0
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

IKE 프로토콜 협상 문제를 해결하려면 다음 디버그를 사용합니다.

> **참고:** 사용하기 전에 Debug 명령에 대한 중요 정보를 참조하십시오 **debug** 명령을 사용합니다.

```
! For IKEv1-based scenarios:
debug crypto isakmp
debug crypto ipsec

! For IKEv2-based scenarios:
debug crypto ikev2
debug crypto ipsec
```

자주 묻는 질문(FAQ)

터널이 자동으로 작동합니까, 아니면 터널을 가동하기 위해 트래픽이 필요합니까?

암호화 맵과 달리, 다중 SA VTI 터널은 암호화 ACL과 일치하는 데이터 트래픽이 라우터를 통해 흐르는지 여부에 관계없이 자동으로 발생합니다. 터널은 흥미로운 교통체증이 없더라도 항상 가동된다.

트래픽이 VTI를 통해 라우팅되지만 트래픽의 소스 또는 대상이 이 터널에 대한 IPsec 정책으로 구성된 암호화 ACL과 일치하지 않으면 어떻게 됩니까?

이러한 시나리오는 지원되지 않습니다. 암호화하려는 트래픽만 터널 인터페이스로 라우팅해야 합니다. PBR(Policy-based routing)은 특정 트래픽만 VTI로 라우팅하는 데 사용할 수 있습니다. PBR은 IPsec 정책 ACL을 사용하여 VTI로 라우팅될 트래픽과 일치시킬 수 있습니다.

각 패킷은 구성된 IPsec 정책에 대해 확인되며 암호화 ACL과 일치해야 합니다. 일치하지 않으면 암호화되지 않으며 터널 소스 인터페이스 외부로 일반 텍스트로 전송됩니다.

동일한 내부 VRF(iVRF) 및 전면 VRF(fVRF)가 사용되는 경우(iVRF = fVRF), 이로 인해 라우팅 루프가 발생하고 패킷이 이유 없이 삭제됩니다 **Ipv4RoutingErr**. 이러한 삭제에 대한 통계는 **show platform hardware qfp active statistics drop** 명령을 사용합니다:

```
RouterA#show platform hardware qfp active statistics drop
Last clearing of QFP drops statistics : never

-------------------------------------------------------------------------
Global Drop Stats Packets Octets
-------------------------------------------------------------------------
Ipv4RoutingErr 5 500
```

iVRF가 fVRF와 다른 경우, iVRF에서 터널에 진입하고 IPsec 정책과 일치하지 않는 패킷은 일반 텍스트로 fVRF에서 터널 소스 인터페이스를 종료합니다. VRF 간에 라우팅 루프가 없으므로 삭제되지 않습니다.

VRF, NAT, QoS 등의 기능이 멀티 SA VTI에서 지원됩니까?

예. 이러한 모든 기능은 일반 VTI 터널에서와 동일한 방식으로 지원됩니다.