보안 방화벽 및 Cisco IOS에 DVTI 구현

목차

소개

이 문서에서는 Adaptive Security Appliance에서 EIGRP를 사용하여 동적 가상 터널 인터페이스 허브 및 스포크 솔루션을 구현하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASA의 가상 터널 인터페이스에 대한 기본 이해
- 허브/스포크/ISP 간의 기본 언더레이 연결
- EIGRP에 대한 기본 이해

- Adaptive Security Appliance 버전 9.19(1) 이상

사용되는 구성 요소

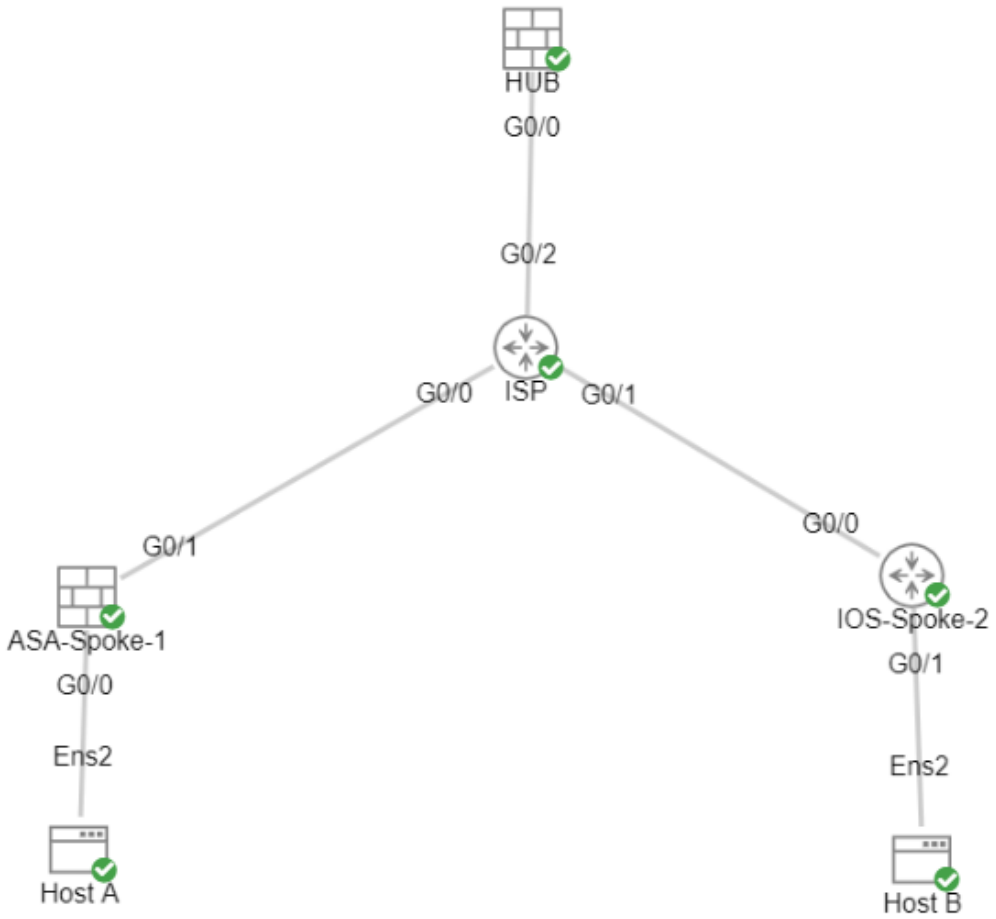
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 두 개의 ASAv 디바이스, 둘 다 버전 9.19(1). 스포크 1 및 허브에 사용
- 2개의 Cisco IOS® v 디바이스 버전 15.9(3)M4. ISP 디바이스용 1개, 스포크 2용 1개
- 터널을 의미하는 일반 트래픽에 대한 2개의 Ubuntu 호스트

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.

구성

네트워크 다이어그램



설정

허브 ASA에서 WAN 인터페이스 및 IKEv2 암호화 매개변수를 구성합니다

허브에서 컨피그레이션 모드로 들어갑니다.

```
interface g0/0
ip address 198.51.100.1 255.255.255.0
nameif OUTSIDE
```

허브 ASA에서 IKEv2 매개변수 구성

IKE 연결의 1단계 매개변수를 정의하는 IKEv2 정책을 생성합니다.

```
crypto ikev2 policy 1      (The number is locally significant on the device, this determine the order i
encryption aes-256         (Defines the encryption parameter used to encrypt the initial communication
integrity sha256           (Defines the integrity used to secure the initial communication between the
group 21                   (Defines the Diffie-Hellman group used to protect the key exchange between d
prf sha256                 (Pseudo Random Function, an optional value to define, automatically chooses
lifetime seconds 86400     (Controls the phase 1 rekey, specified in seconds. Optional value, as the de
```

트래픽 보호에 사용되는 2단계 매개변수를 정의하기 위한 IKEv2 IPsec-proposal을 생성합니다.

```
crypto ipsec ikev2 ipsec-proposal NAME                (Name is locally signicant and is used as a refer
protocol esp encryption aes-256                       (specifies that Encapsulating Security Payload an
protocol esp integrity sha-256                        (specifies that Encapsulating Security Payload an
```

IPsec-proposal을 포함하는 IPsec 프로필을 만듭니다.

```
crypto ipsec profile NAME                   (This name is referenced on the Virtual-Template Interface
set ikev2 ipsec-proposal NAME               (This is the name previously used when creating the ipsec-
```

루프백 및 가상 템플릿 인터페이스 만들기

```
interface loopback 1
ip address 172.16.50.254 255.255.255.255        (This IP address is used for all of the Virtual-Access
nameif LOOP1
```

```
interface Virtual-Template 1 type tunnel
ip unnumbered LOOP1                               (Borrows the IP address specified in Loopback1 for a
nameif DVTI
```

```
tunnel source Interface OUTSIDE                    (Specifies the Interface that the tunnel terminates
tunnel mode ipsec ipv4                             (Specifies that the mode uses ipsec, and uses ipv4)
tunnel protection ipsec profile NAME               (Reference the name of the previously created ipsec
```

터널 그룹을 생성하고 IKEv2 Exchange를 통해 터널 인터페이스 IP 알림

터널 유형 및 인증 방법을 지정하려면 터널 그룹을 생성합니다.

```
tunnel-group DefaultL2LGroup ipsec-attributes          ('DefaultL2LGroup' is a default tunnel-group
virtual-template 1                                     (This command ties the Virtual-Template previ
ikev2 remote-authentication pre-shared-key cisco123    (This specifies the remote authentication as
ikev2 local-authentication pre-shared-key cisco123     (This specifies the local authentication as a
ikev2 route set Interface                              (Advertises the VTI Interface IP over IKEv2 e
```

허브 ASA에서 EIGRP 라우팅 구성

```
router eigrp 100
network 172.16.50.254 255.255.255.255         (Advertise the IP address of the Loopback used for the Vi
```

스포크 ASA에서 인터페이스 구성

WAN 인터페이스를 구성합니다.

```
interface g0/1
ip address 203.0.113.1 255.255.255.0
nameif OUTSIDE-SPOKE-1
```

LAN 인터페이스를 구성합니다.

```
interface g0/0
ip address 10.45.0.4 255.255.255.0
nameif INSIDE-SPOKE-1
```

루프백 인터페이스를 구성합니다.

```
interface loopback1
ip address 172.16.50.1 255.255.255.255
```

```
nameif Loop1
```

스포크 ASA에서 IKEv2 암호화 매개변수 구성

허브의 매개변수와 일치하는 IKEv2 정책을 생성합니다.

```
crypto ikev2 policy 1
encryption aes-256
integrity sha256
group 21
prf sha256
lifetime 86400
```

허브의 매개변수와 일치하는 IKEv2 IPsec-proposal을 생성합니다.

```
crypto ipsec ikev2 ipsec-proposal NAME           (Name is locally signicant, this does not need to matc
protocol esp encryption aes-256
protocol esp integrity sha-256
```

IPsec-proposal을 포함하는 IPsec 프로필을 만듭니다.

```
crypto ipsec profile NAME               (This name is locally significant and is referenced in the SVTI
set ikev2 ipsec-proposal NAME           (This is the name previously used when creating the ipsec-propo
```

스포크 ASA에서 고정 가상 터널 인터페이스 구성

허브를 가리키는 고정 가상 터널 인터페이스를 구성합니다. 스포크 디바이스는 허브에 대한 정기적인 고정 가상 터널 인터페이스를 구성하며, 허브에만 Virtual-Template이 필요합니다.

```
interface tunnel1
ip unnumbered loopback1
nameif ASA-SPOKE-SVTI
tunnel destination  198.51.100.254          (Tunnel destination references the Hub ASA tunnel source. C
tunnel mode ipsec ipv4
tunnel protection ipsec profile NAME
```

터널 그룹 생성 및 IKEv2 Exchange를 통해 터널 인터페이스 IP 알림

```
tunnel-group 198.51.100.1 type ipsec-l2l                    (This specifies the connection type as ipsec
tunnel-group 198.51.100.1 ipsec-attributes                  (Ipsec attributes allows you to make changes
ikev2 remote-authentication pre-shared-key cisco123
ikev2 local-authentication pre-shared-key cisco123
ikev2 route set Interface
```

스포크 ASA에서 EIGRP 라우팅 구성

EIGRP 자동 시스템을 생성하고 광고할 네트워크를 적용합니다.

```
router eigrp 100
network 10.45.0.0 255.255.255.0        (Advertises the Host-A network to the hub. This allows the hub t
network 172.16.50.1 255.255.255.255    (Advertises and utilizes the tunnel IP address to form an EIGRP
```

스포크 라우터의 인터페이스 구성

```
interface g0/0
ip address 192.0.2.1 255.255.255.0
no shut
```

```
interface g0/1
ip address 10.12.0.2
no shut
```

```
interface loopback1
ip address 172.16.50.2 255.255.255.255
```

스포크 라우터에서 IKEv2 매개변수 및 AAA 구성

ASA의 1단계 매개변수와 일치하도록 IKEv2 제안서를 생성합니다.

```
crypto ikev2 proposal NAME       (These parameters must match the ASA IKEv2 Policy.)
encryption aes-cbc-256           (aes-cbc-256 is the same as the ASA aes-256. However, AES-GCM of any v
                                  and is not a matching parameter with plain AES.)
integrity sha256
group 21
```

제안을 첨부할 IKEv2 정책을 생성합니다.

```
crypto ikev2 policy NAME
proposal NAME               (This is the name of the IKEv2 proposal created in the step ikev2.)
```

IKEv2 권한 부여 정책을 생성합니다.

```
crypto ikev2 authorization policy NAME   (IKEv2 authorization policy serves as a container of IKEv2 loca
route set Interface
```

디바이스에서 AAA를 활성화합니다.

```
aaa new-model
```

AAA 권한 부여 네트워크를 생성합니다.

```
aaa authorization network NAME local    (Creates a name and method for aaa authorization that is refere
```

로컬 또는 원격 ID 및 인증 방법과 같은 IKE SA의 협상할 수 없는 매개변수의 리포지토리를 포함하는 IKEv2 프로필을 생성합니다.

```
crypto ikev2 profile NAME
match identity remote address  198.51.100.1    (Used to match the address of the Hub VTI source Interfa
identity local address  192.0.2.1              (Defines the local IKE-ID of the router for this IKEv2 p
authentication remote pre-share key cisco123
authentication local pre-share key cisco123
no config-exchange request                     (Applies to Cisco IOS, Cisco IOS-XE devices do this by d
                                                which is unsupported on the ASA.)
aaa authorization group psk list NAME NAME     (Specifies an AAA method list and username for group. Th
```

터널링 트래픽을 보호하는 데 사용되는 암호화 및 해싱 매개변수를 정의하기 위한 변형 집합을 생성합니다.

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

변형 집합 및 IKEv2 프로필을 저장할 암호화 IPsec 프로필을 만듭니다.

```
crypto ipsec profile NAME                  (Define the name of the ipsec-profile.)
set transform-set NAME                     (Reference the name of the created transform set.)
set ikev2-profile NAME                     (Reference the name of the created IKEv2 profile.)
```

스포크 라우터에서 고정 가상 터널 인터페이스 구성

허브를 가리키는 고정 가상 터널 인터페이스를 구성합니다.

```
interface tunnel1
ip unnumbered loopback1
tunnel source g0/0
tunnel mode ipsec ipv4
tunnel destination 198.51.100.1
tunnel protection ipsec profile NAME      (Reference the name of the created ipsec profile. This applies
                                           and transform set parameters to the tunnel Interface.)
```

스포크 라우터에서 EIGRP 라우팅 구성

EIGRP 자동 시스템을 생성하고 광고할 네트워크를 적용합니다.

```
router eigrp 100
network 172.16.50.2 0.0.0.0     (Routers advertise EIGRP networks with the wildcard mask.
                                 This advertises the tunnel IP address to allow the device to form an E
network 10.12.0.0 0.0.0.255      (Advertises the Host-B network to the hub. This allows the hub to noti
```

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

ASA 라우팅:

```
show run router

show eigrp topology

show eigrp neighbors

show route [eigrp]
```

ASA 암호화:

```
show run crypto ikev2
show run crypto ipsec
show run tunnel-group [NAME]
show crypto ikev2 sa
show crypto ipsec sa peer X.X.X.X
```

ASA 가상 템플릿 및 가상 액세스:

```
show run interface virtual-template # type tunnel
show interface virtual-access #
```

Cisco IOS 라우팅:

```
show run | sec eigrp
show ip eigrp topology
show ip eigrp neighbors
show ip route
show ip route eigrp
```

Cisco IOS Crypto:

```
show run | sec cry
show crypto ikev2 sa
show crypto ipsec sa peer X.X.X.X
```

Cisco IOS 터널 인터페이스:

```
show run interface tunnel#
```

문제 해결

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

ASA 디버그:

```
debug crypto ikev2 platform 255

debug crypto ikev2 protocol 255

debug crypto ipsec 255

debug ip eigrp #

debug ip eigrp neighbor X.X.X.X
```

Cisco IOS 디버깅:

```
debug crypto ikev2

debug crypto ikev2 error

debug crypto ikev2 packet

debug crypto ikev2 internal

debug crypto ipsec

debug crypto ipsec error

debug ip eigrp #

debug ip eigrp neighbor X.X.X.X
```

관련 정보

- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.