IPSec 라우터 간 허브 및 스포크 구성

목차

소개

이 문서에서는 하나의 라우터("허브")에서 다른 라우터("스포크")로 허브 및 스포크 암호화를 보여줍니다. 허브 라우터에는 세 개의 피어 뒤에 각각 네트워크를 지정하는 암호화 맵이 하나씩 있습니다 .각 스포크 라우터의 암호화 맵은 허브 라우터 뒤의 네트워크를 지정합니다.

다음 네트워크 간에 암호화가 수행됩니다.

- 160.160.160.x 네트워크에서 170.170.170.x 네트워크로
- 160.160.160.x 네트워크에서 180.180.180.x 네트워크로
- 160.160.160.x 네트워크에서 190.190.190.x 네트워크로

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® 소프트웨어 릴리스 12.0.7.T 이상
- Cisco 2500 라우터

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 표기 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

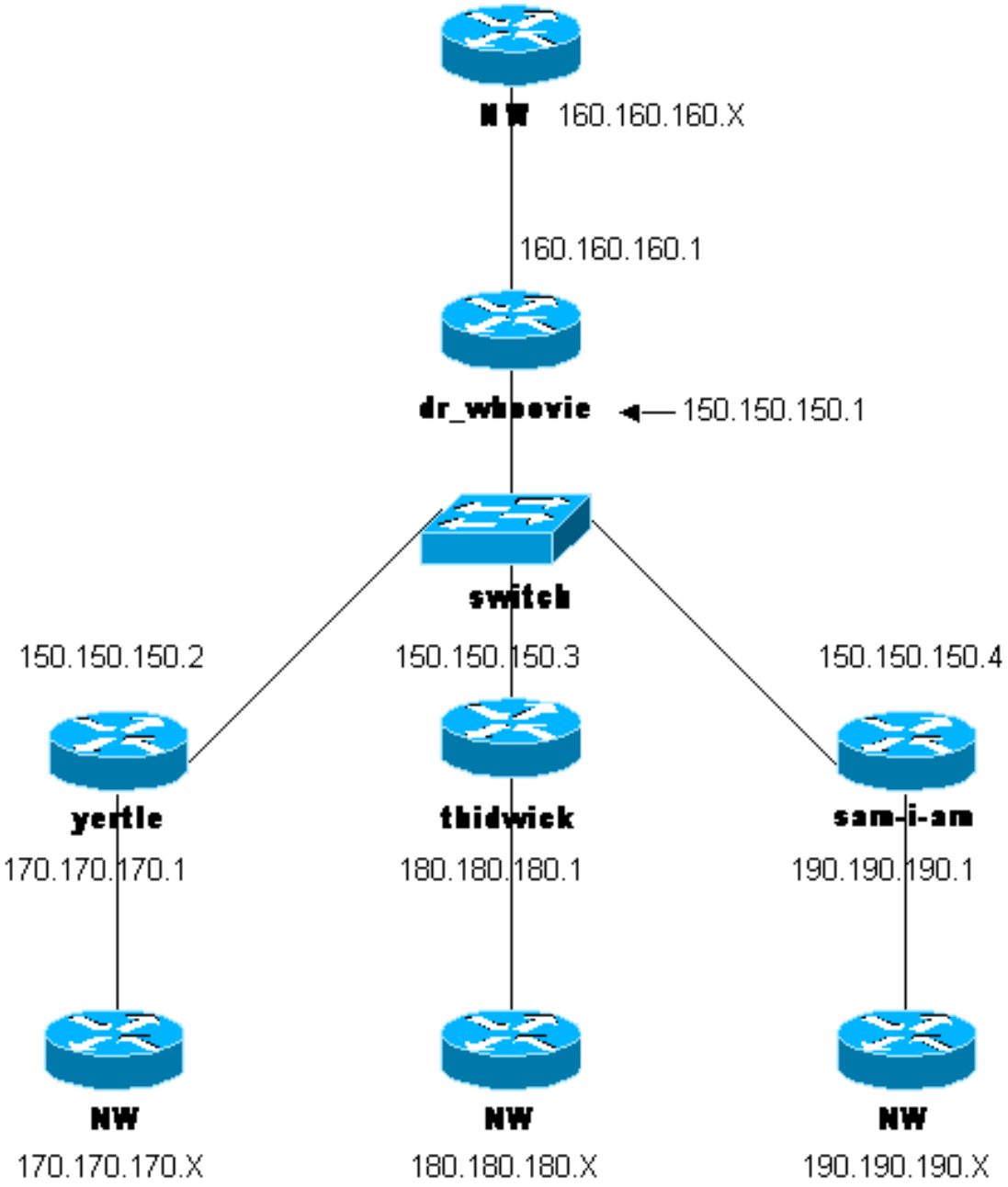
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 이 문서에 사용된 명령에 대한 추가 정보를 찾으려면 명령 조회 도구(등록된 고객만 해당)를 사용합니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

이 문서에서는 다음 구성을 사용합니다.

- dr_whoo 구성
- sam-i-am 컨피그레이션
- thidwick 구성
- 예틀 컨피그레이션

dr_whoo 구성

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
```

```
hostname dr_whoovie
!
enable secret 5 $1$KxKv$cbqKsZtQTLJLGPN.tErFZ1
enable password ww
!
ip subnet-zero
!
cns event-service server
!--- Configure the Internet Key Exchange (IKE) !---
policy and preshared key for each peer: !--- IKE policy
defined for peers. crypto isakmp policy 1
authentication pre-share
!--- Preshared keys for different peers. crypto isakmp
key cisco170 address 150.150.150.2
crypto isakmp key cisco180 address 150.150.150.3
crypto isakmp key cisco190 address 150.150.150.4
!--- Configure the IPSec parameters: !--- IPSec
transform sets. crypto ipsec transform-set 170cisco esp-
des esp-md5-hmac
crypto ipsec transform-set 180cisco esp-des esp-md5-hmac
crypto ipsec transform-set 190cisco esp-des esp-md5-hmac
!
crypto map ETH0 17 ipsec-isakmp
!--- Set the peer. set peer 150.150.150.2
!--- The IPSec transform set is used for this tunnel.
set transform-set 170cisco
!--- Interesting traffic for peer 150.150.150.2. match
address 170
crypto map ETH0 18 ipsec-isakmp
!--- Set the peer. set peer 150.150.150.3
!--- The IPSec transform set is used for this tunnel.
set transform-set 180cisco
!--- Interesting traffic for peer 150.150.150.3. match
address 180
crypto map ETH0 19 ipsec-isakmp
!--- Set the peer. set peer 150.150.150.4
!--- The IPSec transform set is used for this tunnel.
set transform-set 190cisco
!--- Interesting traffic for peer 150.150.150.4. match
address 190
!
interface Ethernet0
ip address 150.150.150.1 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
no mop enabled
!--- Apply crypto map on the interface. crypto map ETH0
!
interface Serial0
ip address 160.160.160.1 255.255.255.0
no ip directed-broadcast
no ip mroute-cache
no fair-queue
!
ip classless
ip route 170.170.170.0 255.255.255.0 150.150.150.2
ip route 180.180.180.0 255.255.255.0 150.150.150.3
ip route 190.190.190.0 255.255.255.0 150.150.150.4
no ip http server
!
!--- Access list that shows traffic to encryption from
yertle. access-list 170 permit ip 160.160.160.0
0.0.0.255 170.170.170.0 0.0.0.255
```

```
!--- Access list that shows traffic to encryption from
thidwick. access-list 180 permit ip 160.160.160.0
0.0.0.255 180.180.180.0 0.0.0.255
!--- Access list that shows traffic to encryption from
sam-i-am. access-list 190 permit ip 160.160.160.0
0.0.0.255 190.190.190.0 0.0.0.255 dialer-list 1 protocol
ip permit dialer-list 1 protocol ipx permit ! line con 0
transport input none line aux 0 line vty 0 4 password ww
login end
```

sam-i-am 컨피그레이션

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Sam-I-am
!
enable secret 5 $1$HDyw$qubSJdqfIC0f1VLvHmg/P0
enable password ww
!
ip subnet-zero
!
isdn switch-type basic-5ess
isdn voice-call-failure 0
cns event-service server
!--- Configure the IKE policy and preshared key for the
hub: crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco190 address 150.150.150.1
!--- Configure the IPSec parameters: !--- IPSec
transform set. crypto ipsec transform-set 190cisco esp-
des esp-md5-hmac
!--- Crypto map definition for the hub site. crypto map
ETH0 19 ipsec-isakmp
!--- Set the peer. set peer 150.150.150.1
!--- IPSec transform set. set transform-set 190cisco
!--- Interesting traffic for peer 150.150.150.1 (hub
site). match address 190
!
interface Ethernet0
ip address 150.150.150.4 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
no mop enabled
!--- Apply crypto map on the interface. crypto map ETH0
!
interface Serial0
ip address 190.190.190.1 255.255.255.0
no ip directed-broadcast
no ip mroute-cache
no fair-queue
!
ip classless
ip route 160.160.160.0 255.255.255.0 150.150.150.1
no ip http server
!--- Access list that shows traffic to encryption !---
for the hub site (dr_whoovie). access-list 190 permit ip
190.190.190.0 0.0.0.255 160.160.160.0 0.0.0.255
```

```
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
line con 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end
```

thidwick 구성

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname thidwick
!
enable secret 5 $1$Pcpo$fj4FNS1dEDY9lGg3Ne6FK1
enable password ww
!
ip subnet-zero
!
isdn switch-type basic-5ess
isdn voice-call-failure 0
cns event-service server
!--- Configure the IKE policy and preshared key for the
hub: crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco180 address 150.150.150.1
!--- Configure the IPSec parameters: !--- IPSec
transform set. crypto ipsec transform-set 180cisco esp-
des esp-md5-hmac
!--- Crypto map definition for the hub site. crypto map
ETH0 18 ipsec-isakmp
!--- Set the peer. set peer 150.150.150.1
!--- IPSec transform set. set transform-set 180cisco
!--- Interesting traffic for peer 150.150.150.1 (hub
site). match address 180
!
interface Ethernet0
ip address 150.150.150.3 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
no mop enabled
!--- Apply crypto map on the interface. crypto map ETH0
!
interface Serial1
ip address 180.180.180.1 255.255.255.0
no ip directed-broadcast
clockrate 4000000
!
interface BRI0
no ip address
no ip directed-broadcast
shutdown
isdn switch-type basic-5ess
```

```
!
ip classless
ip route 160.160.160.0 255.255.255.0 150.150.150.1
no ip http server
!--- Access list that shows traffic to encryption !---
for the hub site (dr_whoovie). access-list 180 permit ip
180.180.180.0 0.0.0.255 160.160.160.0 0.0.0.255
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
line con 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end
```

예를 컨피그레이션

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname yertle
!
enable secret 5 $1$me5Q$2kF5zKlPPTvHEBdGiEZ9m/
enable password ww
!
ip subnet-zero
!
cns event-service server
!--- Configure the IKE policy and preshared key for the
hub: crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco170 address 150.150.150.1
!--- Configure the IPSec parameters: !--- IPSec
transform set. crypto ipsec transform-set 170cisco esp-
des esp-md5-hmac
!--- Crypto map definition for the hub site. crypto map
ETH0 17 ipsec-isakmp
!--- Set the peer. set peer 150.150.150.1
!--- IPSec transform set. set transform-set 170cisco
!--- Interesting traffic for peer 150.150.150.1 (hub
site). match address 170
!
interface Ethernet0
ip address 150.150.150.2 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
no mop enabled
!--- Apply crypto map on the interface. crypto map ETH0
!
interface Serial0
no ip address
no ip directed-broadcast
no ip mroute-cache
shutdown
```

```
no fair-queue
!
interface Serial1
ip address 170.170.170.1 255.255.255.0
no ip directed-broadcast
!
ip classless
ip route 160.160.160.0 255.255.255.0 150.150.150.1
no ip http server
!--- Access list that shows traffic to encryption for !-
-- the hub site (dr_whoovie). access-list 170 permit ip
170.170.170.0 0.0.0.255 160.160.160.0 0.0.0.255
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
tftp-server flash:/c2500-jos56i-l.120-7.T
tftp-server flash:c2500-jos56i-l.120-7.T
tftp-server flash:
!
line con 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end
```

다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show 명령 출력의 분석 결과를 볼 수 있습니다.**

- **show crypto ipsec sa** - 2단계 보안 연결을 표시합니다.
- **show crypto isakmp sa** - 1단계 보안 연결을 표시합니다.

문제 해결

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

문제 해결 명령

참고: debug 명령을 실행하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug crypto ipsec** - 2단계의 IPSec 협상을 표시합니다.
- **debug crypto isakmp** - 1단계의 ISAKMP 협상을 표시합니다.
- **debug crypto engine** - 암호화된 트래픽을 표시합니다.
- **clear crypto isakmp** - 1단계와 관련된 보안 연결을 지웁니다.
- **clear crypto sa** - 2단계와 관련된 보안 연결을 지웁니다.

관련 정보

- IPSec 네트워크 보안 구성
- 인터넷 키 교환 보안 프로토콜 구성
- IPSec 지원 페이지
- Technical Support - Cisco Systems