NAT를 통한 라우터-라우터 동적-고정 IPSec 구성

목차

소개

이 샘플 컨피그레이션에서는 원격 라우터가 IPCP(IP Control Protocol)라는 PPP의 일부를 통해 IP 주소를 수신합니다. 원격 라우터는 IP 주소를 사용하여 허브 라우터에 연결합니다. 이 컨피그레이션을 사용하면 허브 라우터가 동적 IPSec 연결을 수락할 수 있습니다. 원격 라우터는 NAT(Network Address Translation)를 사용하여 허브 라우터 뒤의 개인 주소 지정 네트워크에 해당 라우터의 개인 주소 지정 디바이스를 "연결"합니다. 원격 라우터가 엔드포인트를 인식하고 허브 라우터에 대한 연결을 시작할 수 있습니다. 그러나 허브 라우터는 엔드포인트를 모르므로 원격 라우터에 대한 연결을 시작할 수 없습니다.

이 예에서 dr_whovie는 원격 라우터이고 sam-i-am은 허브 라우터입니다. 액세스 목록은 암호화할 트래픽을 지정합니다. 그러면 dr_whovie는 암호화할 트래픽과 sam-i-am 엔드포인트의 위치를 파악합니다. 원격 라우터가 연결을 시작해야 합니다. 양측이 NAT 오버로드를 수행합니다.

사전 요구 사항

요구 사항

이 문서에서는 IPSec 프로토콜에 대한 기본적인 이해가 필요합니다. IPSec에 대한 자세한 내용은 IPSec(IP 보안) 암호화 소개를 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® 소프트웨어 릴리스 12.2(24a)
- Cisco 2500 Series 라우터

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

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

구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 이 문서에 사용된 명령에 대한 자세한 내용은 Command Lookup Tool(등록된 고객만 해당)을 사용하십시오.

네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.

설정

이 문서에서는 다음 설정을 사용합니다.

- 삼이암
- 닥터 후비

<#root>

```
Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log up time
no service password-encryption
!
hostname sam-i-am
!
ip subnet-zero
!

!--- These are the IKE policies.


crypto isakmp policy 1
```

```
!--- Defines an Internet Key Exchange (IKE) policy. !--- Use the
crypto isakmp policy
 command !--- in global configuration mode. !--- IKE policies define a set of parameters to be used !--
hash md5
authentication pre-share

!--- Specifies pre-shared keys as the authentication method.

crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0

!--- Configures a pre-shared authentication key, !--- used in global configuration mode.
!
!--- These are the IPSec policies.

crypto ipsec transform-set rtpset esp-des esp-md5-hmac

!--- A transform set is an acceptable combination !--- of security protocols and algorithms. !--- This

crypto dynamic-map rtpmap 10

!--- Use dynamic crypto maps to create policy templates !--- that can be used to process negotiation re

set transform-set rtpset

!--- Configure IPSec to use the transform set "rtpset" !--- that was defined previously.

match address 115

!--- Assign an extended access list to a crypto map entry !--- that is used by IPSec to determine whic

crypto map rtptrans 10 ipsec-isakmp dynamic rtpmap

!--- Specifies that this crypto map entry is to reference !--- a preexisting dynamic crypto map.
!
interface Ethernet0
 ip address 10.2.2.3 255.255.255.0
 no ip directed-broadcast

ip nat inside

 !--- This indicates that the interface is connected to the !--- inside network, which is subject to NA
```

```
 no mop enabled
!
interface Serial0
 ip address 99.99.99.1 255.255.255.0
 no ip directed-broadcast

ip nat outside

 !--- This indicates that the interface is connected !--- to the outside network.

crypto map rtptrans

!--- Use the
crypto map
 interface configuration command !--- to apply a previously defined crypto map set to an interface.
!
ip nat inside source route-map nonat interface Serial0 overload

!--- Except the private network from the NAT process.
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0
no ip http server
!
access-list 115 permit ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 115 deny ip 10.2.2.0 0.0.0.255 any

!--- Include the private-network-to-private-network traffic !--- in the encryption process.

access-list 120 deny ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 120 permit ip 10.2.2.0 0.0.0.255 any

!--- Except the private network from the NAT process.

route-map nonat permit 10
 match ip address 120
!
line con 0
 transport input none
line aux 0
line vty 0 4
 password ww
 login
!
end
```

<#root>

```
Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname dr_whoovie
!
ip subnet-zero
!
!--- These are the IKE policies.

crypto isakmp policy 1

!--- Defines an Internet Key Exchange (IKE) policy. !--- Use the
crypto isakmp policy
 command !--- in global configuration mode. !--- IKE policies define a set of parameters to be used !--


hash md5
authentication pre-share

!--- Specifies pre-shared keys as the authentication method.

crypto isakmp key cisco123 address 99.99.99.1


!--- Configures a pre-shared authentication key, !--- used in global configuration mode.
!
!--- These are the IPSec policies.

crypto ipsec transform-set rtpset esp-des esp-md5-hmac

!--- A transform set is an acceptable combination !--- of security protocols and algorithms. !--- This
!
crypto map rtp 1 ipsec-isakmp


!--- Creates a crypto map and indicates that IKE will be used !--- to establish the IPSec SAs for prot

set peer 99.99.99.1
```

```
!--- Use the
set peer
 command to specify an IPSec peer in a crypto map entry.

set transform-set rtpset


!--- Configure IPSec to use the transform set "rtpset" !--- that was defined previously.


match address 115

!--- Include the private-network-to-private-network traffic !--- in the encryption process.

!
interface Ethernet0
ip address 10.1.1.1 255.255.255.0
 no ip directed-broadcast

ip nat inside


 !--- This indicates that the interface is connected to the !--- inside network, which is subject to NA

 no mop enabled
!
interface Serial0
 ip address negotiated


 !--- Specifies that the IP address for this interface !--- is obtained via PPP/IPCP address negotiatio

 no ip directed-broadcast

ip nat outside


 !--- This indicates that the interface is connected !--- to the outside network.

 encapsulation ppp
 no ip mroute-cache
 no ip route-cache

crypto map rtp


 !--- Use the
crypto map
 interface configuration command !--- to apply a previously defined crypto map set to an interface.
```

```
ip nat inside source route-map nonat interface Serial0 overload


!--- Except the private network from the NAT process.

ip classless
ip route 0.0.0.0 0.0.0.0 Serial0
no ip http server
!
access-list 115 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
access-list 115 deny ip 10.1.1.0 0.0.0.255 any


!--- Include the private-network-to-private-network traffic !--- in the encryption process.


access-list 120 deny   ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
access-list 120 permit ip 10.1.1.0 0.0.0.255 any


!--- Except the private network from the NAT process.

dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
route-map nonat permit 10
 match ip address 120

!
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.

- ping - 기본 네트워크 연결을 진단하는 데 사용됩니다.

  이 예에서는 dr_whivie의 10.1.1.1 이더넷 인터페이스에서 sam-i-am의 10.2.2.3 이더넷 인터페이스로 ping하는 방법을 보여 줍니다.

  <#root>

  dr_whoovie#

  ping

```
Protocol [ip]:
Target IP address: 10.2.2.3
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.3,
  timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
!!!!!
Success rate is 100 percent (5/5),
  round-trip min/avg/max = 36/38/40 ms
```

- show crypto ipsec sa - 2단계 SA(보안 연계)를 표시합니다.
- show crypto isakmp sa - 1단계 SA를 표시합니다.

샘플 출력

이 출력은 허브 라우터에서 실행된 show crypto ipsec sa 명령의 출력입니다.

<#root>

```
sam-i-am#
```

show crypto ipsec sa

```
interface: Serial0
    Crypto map tag: rtptrans, local addr. 99.99.99.1
```

local ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)

```
   current_peer: 100.100.100.1
     PERMIT, flags={}
    #pkts encaps: 6, #pkts encrypt: 6, #pkts digest 6
    #pkts decaps: 6, #pkts decrypt: 6, #pkts verify 6
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 0, #recv errors 0
```

local crypto endpt.: 99.99.99.1, remote crypto endpt.: 100.100.100.1

```
     path mtu 1500, ip mtu 1500, ip mtu interface Serial0
     current outbound spi: 52456533
```

```
inbound esp sas:

      spi: 0x6462305C(1684156508)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: rtptrans
        sa timing: remaining key lifetime (k/sec): (4607999/3510)
        IV size: 8 bytes
        replay detection support: Y

    inbound ah sas:

    inbound pcp sas:



outbound esp sas:

      spi: 0x52456533(1380279603)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: rtptrans
        sa timing: remaining key lifetime (k/sec): (4607999/3510)
        IV size: 8 bytes
        replay detection support: Y

    outbound ah sas:

    outbound pcp sas:
```

이 명령은 피어 디바이스 간에 구축된 IPSec SA를 표시합니다. 암호화된 터널은 dr_whovie의 100.100.1 인터페이스와 sam-i-am의 99.99.99.1 인터페이스를 연결합니다. 이 터널은 네트워크 10.2.2.3과 10.1.1.1 사이를 이동하는 트래픽을 전달합니다. 2개의 ESP(Encapsulating Security Payload) SA는 인바운드 및 아웃바운드에 구축됩니다. sam-i-am이 피어 IP 주소(100.100.1)를 모르더라도 터널이 설정됩니다. AH(Authentication Header) SA는 구성된 AH가 없으므로 사용되지 않습니다.

이러한 출력 샘플은 dr_whovie의 직렬 인터페이스 0이 IPCP를 통해 100.100.100.1의 IP 주소를 수신한다는 것을 보여줍니다.

- IP 주소를 협상하기 전에:

```
<#root>

dr_whoovie#

show interface serial0

Serial0 is up, line protocol is up
  Hardware is HD64570

Internet address will be negotiated using IPCP
```

```
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
```

- IP 주소가 협상된 후:

```
<#root>

dr_whoovie#

show interface serial0

Serial0 is up, line protocol is up
  Hardware is HD64570

Internet address is 100.100.100.1/32

  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
```

이 예는 dr_whovie의 직렬 0 인터페이스의 원격 끝에 IP 주소를 할당하기 위해 peer default ip address 명령을 사용하여 Lab에서 설정되었습니다. IP 풀은 원격 엔드에서의 ip local pool 명령으로 정의됩니다.

문제 해결

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

트러블슈팅 명령

OIT(Output Interpreter Tool)(등록된 고객만 해당)는 특정 show 명령을 지원합니다. OIT를 사용하여 show 명령 출력 분석을 볼 수 있습니다.

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

- debug crypto ipsec - 2단계의 IPSec 협상을 표시합니다.
- debug crypto isakmp - 1단계의 ISAKMP(Internet Security Association and Key Management Protocol) 협상을 표시합니다.
- debug crypto engine - 암호화된 트래픽을 표시합니다.
- debug ip nat detailed - (선택 사항) 라우터가 변환하는 모든 패킷에 대한 정보를 표시하여 NAT 기능의 작동을 확인합니다.

  주의: 이 명령은 많은 출력을 생성합니다. IP 네트워크의 트래픽이 낮은 경우에만 이 명령을 사용합니다.

- clear crypto isakmp - 1단계와 관련된 SA를 지웁니다.
- clear crypto sa - 2단계와 관련된 SA를 지웁니다.
- clear ip nat translation - 변환 테이블에서 동적 NAT 변환을 지웁니다.

관련 정보

- IPSec 지원 페이지
- Technical Support - Cisco Systems

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.