Cisco IOS Software에 연결하는 strongSwan as a Remote Access VPN Client(XAUTH) - 컨피그레이션 예

목차

소개

이 문서에서는 Cisco IOS® 소프트웨어에 연결되는 원격 액세스 IPSec VPN 클라이언트로 strongSwan을 구성하는 방법에 대해 설명합니다.

strongSwan은 IKE(Internet Key Exchange)/IPSec VPN 터널을 구축하고 Cisco IOS 소프트웨어를 사용하여 LAN-to-LAN 및 원격 액세스 터널을 구축하는 데 사용되는 오픈 소스 소프트웨어입니다.

사전 요구 사항

요구 사항

Cisco에서는 이러한 주제에 대한 기본적인 지식을 얻을 것을 권장합니다.

- Linux 구성
- Cisco IOS 소프트웨어의 VPN 구성

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco IOS Software 릴리스 15.3T
- 스트림스완 5.0.4
- Linux 커널 3.2.12

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.

구성

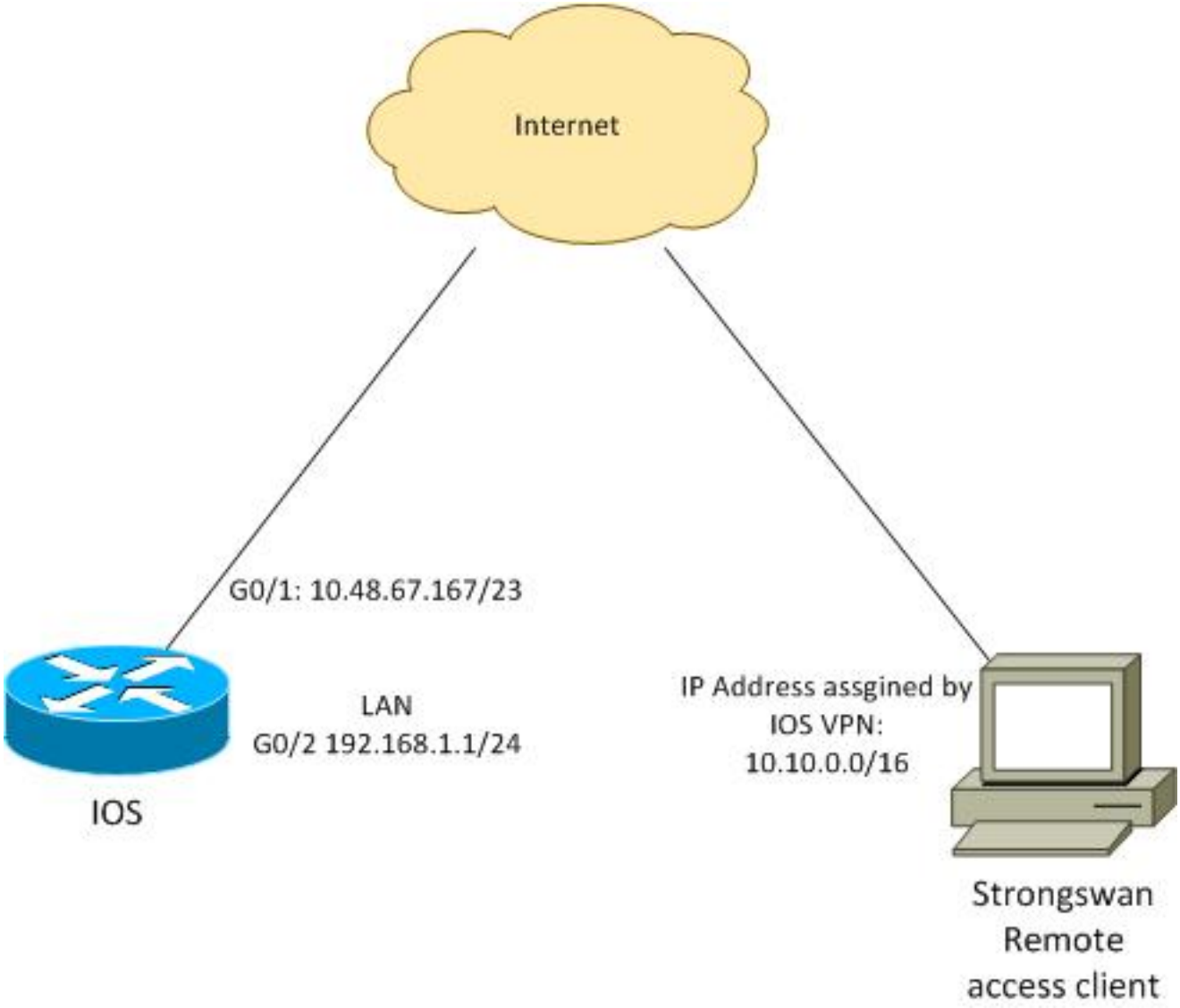
참고:

이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

debug 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

토폴로지



원격 클라이언트는 풀 10.10.0.0/16에서 IP 주소를 수신합니다. 10.10.0.0/16에서 192.168.1.0/24 사이의 트래픽은 보호됩니다.

Cisco IOS 소프트웨어 구성

이 예에서 strongSwan 클라이언트에는 Cisco IOS 소프트웨어 LAN 네트워크 192.168.1.0/24에 대한 보안 액세스가 필요합니다. 원격 클라이언트는 RA의 그룹 이름(IKEID임)과 cisco의 사용자 이름 및 Cisco의 비밀번호를 사용합니다.

클라이언트는 풀 10.10.0.0/16에서 IP 주소를 가져옵니다. 또한 분할 ACL(Access Control List)이 클라이언트에 푸시됩니다.ACL을 통해 클라이언트가 VPN을 통해 192.168.1.0/24으로 트래픽을 전송하도록 합니다.

```
aaa new-model
aaa authentication login AUTH local
aaa authorization network NET local
username cisco password 0 cisco

crypto isakmp policy 1
 encryption aes
 hash sha
 authentication pre-share
```

```
 group 2
 lifetime 3600
crypto isakmp keepalive 10

crypto isakmp client configuration group RA
 key cisco
 domain cisco.com
 pool POOL
 acl split
 save-password
 netmask 255.255.255.0

crypto isakmp profile test
   match identity group RA
   client authentication list AUTH
   isakmp authorization list NET
   client configuration address respond
   client configuration group RA
   virtual-template 1

crypto ipsec transform-set test esp-aes esp-sha-hmac
 mode tunnel

crypto ipsec profile ipsecprof
 set security-association lifetime kilobytes disable
 set transform-set test
 set isakmp-profile test

interface GigabitEthernet0/1
 ip address 10.48.67.167 255.255.254.0
!
interface GigabitEthernet0/2
description LAN
 ip address 192.168.1.1 255.255.255.0

interface Virtual-Template1 type tunnel
 ip unnumbered GigabitEthernet0/1
 tunnel source GigabitEthernet0/1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsecprof

ip local pool POOL 10.10.0.0 10.10.255.255
ip access-list extended split
 permit ip host 192.168.1.1 any
```

Virtual-Template에서는 일반적인 고정 IP 주소를 할당하지 않는 것이 좋습니다.Virtual-Access 인터페이스가 복제되어 상위 Virtual-Template에서 해당 컨피그레이션을 상속합니다. 그러면 중복 IP 주소가 생성될 수 있습니다.그러나 Virtual-Template은 인접성 테이블을 채우기 위해 'ip unnumbered' 키워드를 통해 IP 주소를 참조합니다.'ip unnumbered' 키워드는 라우터의 물리적 또는 논리적 IP 주소에 대한 참조일 뿐입니다.

IKEv2에서 IKE 라우팅과의 정방향 호환성을 위해 내부 주소를 사용하고 IPSec 'local address'를 'ip unnumbered'로 사용하지 마십시오.

strongSwan 구성

다음 절차에서는 strongSwan을 구성하는 방법에 대해 설명합니다.

1. /etc/ipsec.conf 파일에서 이 컨피그레이션을 사용합니다.

```
version 2
config setup
       strictcrlpolicy=no
       charondebug="ike 4, knl 4, cfg 2" #useful debugs

conn %default
       ikelifetime=1440m
       keylife=60m
       rekeymargin=3m
       keyingtries=1
       keyexchange=ikev1
       authby=xauthpsk

conn "ezvpn"
       keyexchange=ikev1
       ikelifetime=1440m
       keylife=60m
       aggressive=yes
       ike=aes-sha1-modp1024 #Phase1 parameters
       esp=aes-sha1 #Phase2 parameters
       xauth=client #Xauth client mode
       left=10.48.62.178 #local IP used to connect to IOS
       leftid=RA #IKEID (group name) used for IOS
       leftsourceip=%config  #apply received IP
       leftauth=psk
       rightauth=psk
       leftauth2=xauth #use PSK for group RA and Xauth for user cisco
       right=10.48.67.167 #gateway (IOS) IP
       rightsubnet=192.168.1.0/24
       xauth_identity=cisco #identity for Xauth, password in ipsec.secrets
       auto=add
```

어떤 트래픽을 보호해야 하는지 나타내기 위해 rightsubnet 키워드가 설정되었습니다. 이 시나리오에서는 IPSec SA(Security Association)가 192.168.1.0/24(Cisco IOS 소프트웨어)과 10.10.0.0/16 풀에서 수신되는 strongSwan IP 주소 사이에 구축됩니다.

오른쪽 서브넷을 지정하지 않으면 클라이언트 IP 주소와 0.0.0.0 네트워크 사이에 0.0.0.0 네트워크와 IPSec SA가 있을 수 있습니다.이는 Cisco IOS 소프트웨어를 클라이언트로 사용할 때의 동작입니다.

그러나 strongSwan의 예상은 정확하지 않습니다.오른쪽 서브넷을 정의하지 않은 strongSwan은 협상의 2단계에서 외부 게이트웨이(Cisco IOS 소프트웨어) IP 주소를 제안합니다.이 시나리오에서는 해당 게이트웨이가 10.48.67.167입니다. Cisco IOS 소프트웨어(192.168.1.0/24)에서 내부 LAN으로 이동하는 트래픽을 보호하는 것이 목적이며 외부 Cisco IOS 소프트웨어 IP 주소가 아닌 오른쪽 서브넷이 사용되었습니다.

2. /etc/ipsec.secrets 파일에서 이 컨피그레이션을 사용합니다.

```
10.48.67.167 : PSK "cisco"        #this is PSK for group password
cisco : XAUTH "cisco" #this is password for XAuth (user cisco)
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

다음 절차에서는 strongSwan 컨피그레이션을 테스트하고 확인하는 방법에 대해 설명합니다.

1. 디버그를 사용하도록 설정하여 strongSwan 시작:

```
gentoo1 ~ # /etc/init.d/ipsec start
 * Starting  ...
Starting strongSwan 5.0.4 IPsec [starter]...
Loading config setup
 strictcrlpolicy=no
 charondebug=ike 4, knl 4, cfg 2
Loading conn %default
 ikelifetime=1440m
 keylife=60m
 rekeymargin=3m
 keyingtries=1
 keyexchange=ikev1
 authby=xauthpsk
Loading conn 'ezvpn'
 keyexchange=ikev1
 ikelifetime=1440m
 keylife=60m
 aggressive=yes
 ike=aes-sha1-modp1024
 esp=aes-sha1
 xauth=client
 left=10.48.62.178
 leftid=RA
 leftsourceip=%config
 leftauth=psk
 rightauth=psk
 leftauth2=xauth
 right=10.48.67.167
 rightsubnet=192.168.1.0/24
 xauth_identity=cisco
 auto=add
found netkey IPsec stack
No leaks detected, 9 suppressed by whitelist
```

2. strongSwan에서 터널을 시작하면 1단계, Xauth 및 2단계에 대한 모든 일반 정보가 표시됩니다.

```
gentoo1 ~ # ipsec up ezvpn
initiating Aggressive Mode IKE_SA ezvpn[1] to 10.48.67.167
generating AGGRESSIVE request 0 [ SA KE No ID V V V V ]
sending packet: from 10.48.62.178[500] to 10.48.67.167[500] (374 bytes)
received packet: from 10.48.67.167[500] to 10.48.62.178[500] (404 bytes)
parsed AGGRESSIVE response 0 [ SA V V V V V KE ID No HASH NAT-D NAT-D ]
received Cisco Unity vendor ID
received DPD vendor ID
received unknown vendor ID: 8d:75:b5:f8:ba:45:4c:6b:02:ac:bb:09:84:13:32:3b
received XAuth vendor ID
received NAT-T (RFC 3947) vendor ID
generating AGGRESSIVE request 0 [ NAT-D NAT-D HASH ]
sending packet: from 10.48.62.178[500] to 10.48.67.167[500] (92 bytes)
received packet: from 10.48.67.167[500] to 10.48.62.178[500] (92 bytes)
parsed INFORMATIONAL_V1 request 3265561043 [ HASH N((24576)) ]
received (24576) notify
received packet: from 10.48.67.167[500] to 10.48.62.178[500] (68 bytes)
parsed TRANSACTION request 4105447864 [ HASH CP ]
generating TRANSACTION response 4105447864 [ HASH CP ]
```

```
sending packet: from 10.48.62.178[500] to 10.48.67.167[500] (76 bytes)
received packet: from 10.48.67.167[500] to 10.48.62.178[500] (68 bytes)
parsed TRANSACTION request 1681157416 [ HASH CP ]
XAuth authentication of 'cisco' (myself) successful
IKE_SA ezvpn[1] established between 10.48.62.178[RA]...10.48.67.167[10.48.67.167]
scheduling reauthentication in 86210s
maximum IKE_SA lifetime 86390s
generating TRANSACTION response 1681157416 [ HASH CP ]
sending packet: from 10.48.62.178[500] to 10.48.67.167[500] (68 bytes)
generating TRANSACTION request 1406391467 [ HASH CP ]
sending packet: from 10.48.62.178[500] to 10.48.67.167[500] (68 bytes)
received packet: from 10.48.67.167[500] to 10.48.62.178[500] (68 bytes)
parsed TRANSACTION response 1406391467 [ HASH CP ]
installing new virtual IP 10.10.0.1
generating QUICK_MODE request 1397274205 [ HASH SA No ID ID ]
sending packet: from 10.48.62.178[500] to 10.48.67.167[500] (196 bytes)
received packet: from 10.48.67.167[500] to 10.48.62.178[500] (180 bytes)
parsed QUICK_MODE response 1397274205 [ HASH SA No ID ID N((24576)) ]
connection 'ezvpn' established successfully
No leaks detected, 1 suppressed by whitelist
```

3. strongSwan에서 디버깅을 활성화하면 많은 정보가 반환될 수 있습니다.터널이 시작될 때 가장 중요한 디버그입니다.

```
#IKE Phase
06[CFG] received stroke: initiate 'ezvpn'
04[IKE] initiating Aggressive Mode IKE_SA ezvpn[1] to 10.48.67.167
03[CFG]   proposal matches
03[CFG] received proposals: IKE:AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
03[CFG] selected proposal: IKE:AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
16[IKE] IKE_SA ezvpn[1] state change: CONNECTING => ESTABLISHED
16[IKE] scheduling reauthentication in 86210s

#Xauth phase
15[KNL] 10.48.62.178 is on interface eth1
15[IKE] installing new virtual IP 10.10.0.1
15[KNL] virtual IP 10.10.0.1 installed on eth1

#Ipsec
05[CFG]   proposal matches
05[CFG] received proposals: ESP:AES_CBC_128/HMAC_SHA1_96/NO_EXT_SEQ
05[CFG] selected proposal: ESP:AES_CBC_128/HMAC_SHA1_96/NO_EXT_SEQ
05[KNL] adding SAD entry with SPI 7600acd8 and reqid

15[CFG] proposing traffic selectors for us:
15[CFG]  10.10.0.1/32
15[CFG] proposing traffic selectors for other:
15[CFG]  192.168.1.0/24

#Local settings
charon: 05[KNL] getting a local address in traffic selector 10.10.0.1/32
charon: 05[KNL] using host 10.10.0.1
charon: 05[KNL] using 10.48.62.129 as nexthop to reach 10.48.67.167
charon: 05[KNL] 10.48.62.178 is on interface eth1
charon: 05[KNL] installing route: 192.168.1.0/24 via 10.48.62.129 src 10.10.0.1
dev eth1
charon: 05[KNL] getting iface index for eth1
charon: 05[KNL] policy 10.10.0.1/32 === 192.168.1.0/24 out  (mark 0/0x00000000)
already exists, increasing refcount
charon: 05[KNL] updating policy 10.10.0.1/32 === 192.168.1.0/24 out
```

4. 클라이언트에서 트래픽 전송:

```
gentoo1 ~ # ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_req=1 ttl=255 time=1.19 ms
64 bytes from 192.168.1.1: icmp_req=2 ttl=255 time=1.19 ms
64 bytes from 192.168.1.1: icmp_req=3 ttl=255 time=1.12 ms
64 bytes from 192.168.1.1: icmp_req=4 ttl=255 time=1.16 ms
64 bytes from 192.168.1.1: icmp_req=4 ttl=255 time=1.26 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.128/1.171/1.199/0.036 ms
```

5. Cisco IOS 소프트웨어의 동적 인터페이스를 확인합니다.

```
Bsns-7200-2#sh int Virtual-Access1
Virtual-Access1 is up, line protocol is up
 Hardware is Virtual Access interface
  Interface is unnumbered. Using address of GigabitEthernet0/1 (10.48.67.167)
 MTU 17878 bytes, BW 100000 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation TUNNEL
 Tunnel vaccess, cloned from Virtual-Template1
 Vaccess status 0x4, loopback not set
 Keepalive not set
 Tunnel source 10.48.67.167 (GigabitEthernet0/1), destination 10.48.62.178
  Tunnel Subblocks:
     src-track:
        Virtual-Access1 source tracking subblock associated with
GigabitEthernet0/1
         Set of tunnels with source GigabitEthernet0/1, 2 members (includes
iterators), on interface <OK>
  Tunnel protocol/transport IPSEC/IP
 Tunnel TTL 255
 Tunnel transport MTU 1438 bytes
 Tunnel transmit bandwidth 8000 (kbps)
 Tunnel receive bandwidth 8000 (kbps)
 Tunnel protection via IPSec (profile "ipsecprof")
 Last input never, output never, output hang never
 Last clearing of "show interface" counters 00:07:19
 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
 Queueing strategy: fifo
 Output queue: 0/0 (size/max)
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
    5 packets input, 420 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    5 packets output, 420 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 unknown protocol drops
    0 output buffer failures, 0 output buffers swapped out
```

6. Cisco IOS 소프트웨어의 IPSec 카운터를 확인합니다.

```
Bsns-7200-2#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
```

```
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Virtual-Access1
Username: cisco
Profile: test
Group: RA
Assigned address: 10.10.0.1
Uptime: 00:39:25
Session status: UP-ACTIVE
Peer: 10.48.62.178 port 500 fvrf: (none) ivrf: (none)
     Phase1_id: RA
     Desc: (none)
 IKEv1 SA: local 10.48.67.167/500 remote 10.48.62.178/500 Active
         Capabilities:CDX connid:13002 lifetime:00:20:34
 IPSEC FLOW: permit ip 192.168.1.0/255.255.255.0 host 10.10.0.1
       Active SAs: 2, origin: crypto map
       Inbound:  #pkts dec'ed 5 drop 0 life (KB/Sec) KB Vol Rekey Disabled/1234
       Outbound: #pkts enc'ed 5 drop 0 life (KB/Sec) KB Vol Rekey Disabled/1234
```

7. strongSwan에서 상태 확인:

```
gentoo1 ~ # ipsec statusall
Status of IKE charon daemon (strongSwan 5.0.4, Linux 3.2.12-gentoo, x86_64):
 uptime: 41 minutes, since Jun 09 10:45:59 2013
 malloc: sbrk 1069056, mmap 0, used 896944, free 172112
 worker threads: 7 of 16 idle, 8/1/0/0 working, job queue: 0/0/0/0, scheduled: 2
 loaded plugins: charon aes des sha1 sha2 md5 random nonce x509 revocation
constraints pubkey pkcs1 pkcs8 pgp dnskey pem openssl gcrypt fips-prf gmp
xcbc cmac hmac attr kernel-netlink resolve socket-default stroke updown
eap-identity eap-sim eap-aka eap-aka-3gpp2 eap-simaka-pseudonym
eap-simaka-reauth eap-md5 eap-gtc eap-mschapv2 eap-radius xauth-generic dhcp
Listening IP addresses:
 192.168.0.10
 10.48.62.178
 2001:420:44ff:ff61:250:56ff:fe99:7661
 192.168.2.1
Connections:
      ezvpn:  10.48.62.178...10.48.67.167  IKEv1 Aggressive
      ezvpn:   local:  [RA] uses pre-shared key authentication
      ezvpn:   local:  [RA] uses XAuth authentication: any with XAuth identity
'cisco'
      ezvpn:   remote: [10.48.67.167] uses pre-shared key authentication
      ezvpn:   child:  dynamic === 192.168.1.0/24 TUNNEL
Security Associations (1 up, 0 connecting):
      ezvpn[1]: ESTABLISHED 41 minutes ago, 10.48.62.178[RA]...
10.48.67.167[10.48.67.167]
      ezvpn[1]: IKEv1 SPIs: 0fa722d2f09bffe0_i* 6b4c44bae512b278_r, pre-shared
key+XAuth reauthentication in 23 hours
      ezvpn[1]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
      ezvpn{1}:  INSTALLED, TUNNEL, ESP SPIs: c805b9ba_i 7600acd8_o
      ezvpn{1}:  AES_CBC_128/HMAC_SHA1_96, 420 bytes_i (5 pkts, 137s ago), 420
bytes_o (5 pkts, 137s ago), rekeying in 13 minutes
      ezvpn{1}:   10.10.0.1/32 === 192.168.1.0/24
No leaks detected, 1 suppressed by whitelist
```

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

요약

이 문서에서는 IPSec VPN 클라이언트로 Cisco IOS 소프트웨어에 연결하는 strongSwan 클라이언트의 컨피그레이션에 대해 설명합니다.

Cisco IOS 소프트웨어와 strongSwan 간에 IPSec LAN-to-LAN 터널을 구성할 수도 있습니다.또한 두 디바이스 간의 IKEv2는 원격 및 LAN-to-LAN 액세스에 모두 올바르게 작동합니다.

관련 정보

- Openswan 설명서
- StrongSwan 사용자 설명서
- FlexVPN 및 Internet Key Exchange 버전 2 컨피그레이션 가이드, Cisco IOS 릴리스 15M&T의 Internet Key Exchange 버전 2 및 FlexVPN Site-to-Site 섹션 구성
- 기술 지원 및 문서 – Cisco Systems