

strongSwan作为连接对Cisco IOS软件-配置示例的远程访问虚拟专用网客户端(Xauth)

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[拓扑](#)

[配置Cisco IOS软件](#)

[配置strongSwan](#)

[验证](#)

[故障排除](#)

[摘要](#)

[相关信息](#)

简介

本文描述如何配置strongSwan作为连接对Cisco IOS软件的远程访问IPSec VPN客户端。

strongSwan使用为了构建Internet Key Exchange (IKE) /IPSec VPN通道和构建有Cisco IOS软件的LAN对LAN和远程访问隧道的开放源软件。

[先决条件](#)

[要求](#)

Cisco 建议您具有以下主题的基础知识：

- Linux配置
- 在Cisco IOS软件的VPN配置

使用的组件

本文档中的信息基于以下软件版本：

- Cisco IOS软件版本15.3T

- strongSwan 5.0.4
- Linux内核3.2.12

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

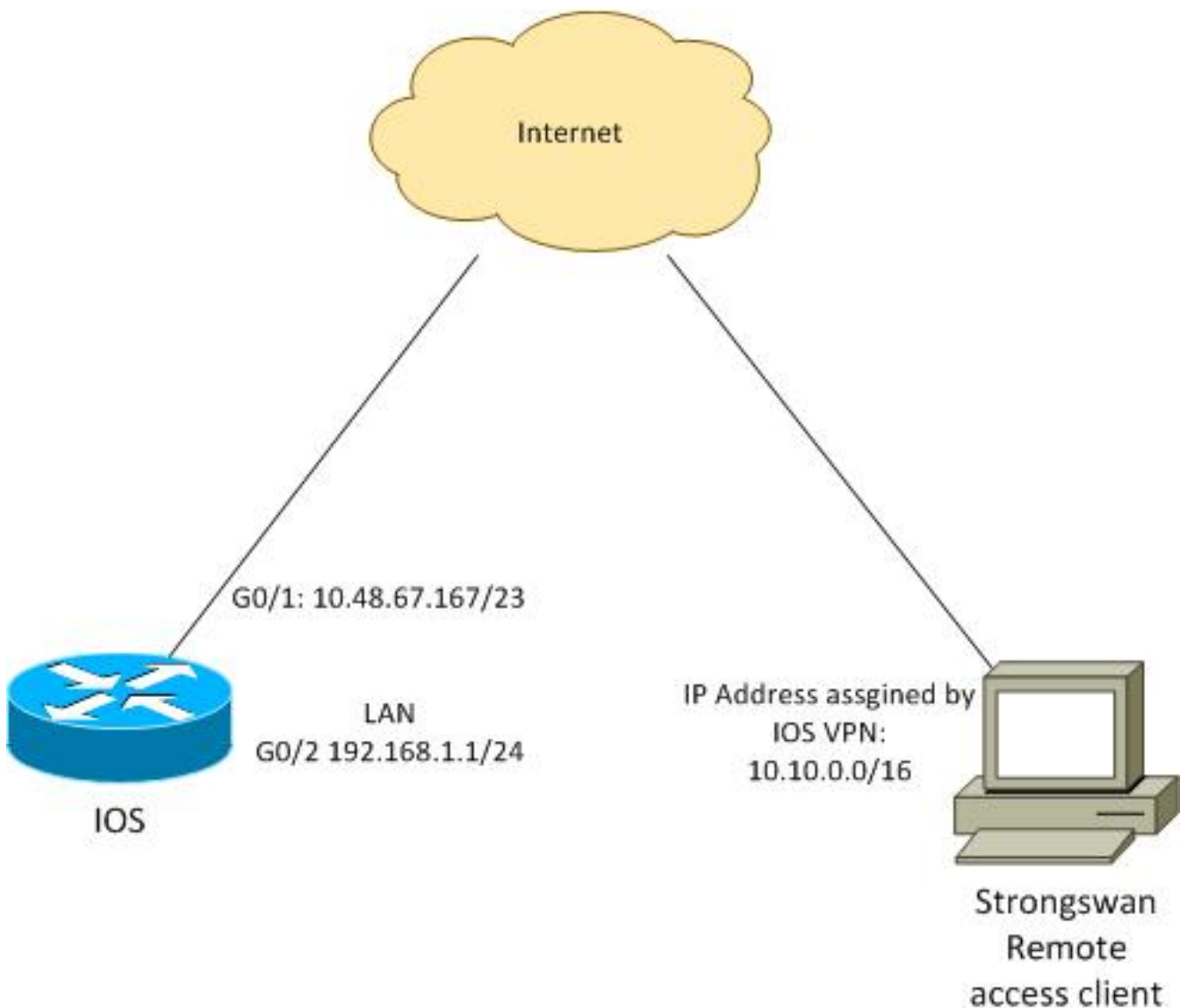
注意：

使用[命令查找工具](#)（[仅限注册用户](#)）可获取有关本部分所使用命令的详细信息。

[命令输出解释程序工具](#)（[仅限注册用户](#)）支持某些 **show** 命令。请使用Output Interpreter Tool为了查看show命令输出分析。

使用 **debug** 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

拓扑



远程客户端收到从池10.10.0.0/16的一个IP地址。10.10.0.0/16和192.168.1.0/24之间的流量保护。

配置Cisco IOS软件

在本例中，strongSwan客户端需要对Cisco IOS软件LAN网络192.168.1.0/24的安全访问。远程客户端使用RA组名(这是IKEID)以及思科cisco和密码用户名。

客户端从池10.10.0.0/16获得IP地址。并且，分开的访问控制表(ACL)推送给客户端;该ACL将迫使客户端发送流量到192.168.1.0/24通过VPN。

```
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-Templatel 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
```

思科建议您不分配在虚拟模板的通常静态IP地址。虚拟访问接口被克隆并且继承他们的从parent虚拟模板的配置，可能创建复制IP地址。然而，虚拟模板通过‘ip unnumbered’关键字参考IP地址为了填充邻接表。‘ip unnumbered’关键字是对一个物理或逻辑IP地址的一参考在路由器。

对于与路由在IKEv2的IKE的前向兼容性，请使用一内部地址，并且避免使用IPSec‘本地地址的作为‘ip unnumbered’。

配置strongSwan

此步骤描述如何配置strongSwan：

1. 请使用此配置在/etc/ipsec.conf文件：

```
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
```

rightsubnet关键字设置为了指示应该保护哪个流量。在此方案中，IPSec安全关联(SA)被建立在192.168.1.0/24 (在Cisco IOS软件)和strongSwan IP地址之间，从池10.10.0.0/16接收。

没有指定的rightsubnet，您也许期望有0.0.0.0网络和IPSec在客户端IP地址和0.0.0.0网络之间的SA。当Cisco IOS软件使用作为客户端时，那是行为。

但是此所需的为strongSwan不是正确。没有定义的rightsubnet，strongSwan报价在协商的第

2阶段的外部网关(Cisco IOS软件) IP地址;在此方案中，该网关是10.48.67.167。由于目标是保护去在Cisco IOS软件的流量(192.168.1.0/24)的一个内部LAN和一个外部Cisco IOS软件IP地址，使用了rightsubnet。

2. 请使用此配置在/etc/ipsec.secrets文件：

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

验证

使用本部分可确认配置能否正常运行。

此步骤描述如何测试和验证strongSwan配置：

1. 开始strongSwan与启用的调试：

```
gentool ~ # /etc/init.d/ipsec start
* Starting ...
Starting strongSwan 5.0.4 IPsec [starter]...
Loading config setup
  strictcrpolicy=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. 当从strongSwan的通道被发起时，关于phase1、Xauth和第2阶段的所有一般信息显示：

```
gentool ~ # 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. 当您在strongSwan的关闭调试，信息可以返回。当通道被发起时，这是使用的最重要的调试：

```

#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

#Ipssec
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. 从客户端的发送流量：

```

gentool ~ # 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. 检查在Cisco IOS软件的动态接口：

```

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. 检查在Cisco IOS软件的IPSec计数器：

```
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. 验证在strongSwan的状态：

```
gentool ~ # 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
```

故障排除

目前没有针对此配置的故障排除信息。

摘要

本文描述连接作为IPSec VPN客户端对Cisco IOS软件一个strongSwan客户端的配置。

配置在Cisco IOS软件之间的一个IPSec LAN到LAN隧道和strongSwan也是可能的。另外，在两个设备之间的IKEv2为远程和LAN对LAN访问正确地运作两个。

相关信息

- [Openswan文档](#)
- [StrongSwan用户文档](#)
- [配置FlexVPN和互联网密钥交换版本2配置指南的互联网密钥交换版本2和FlexVPN站点到站点部分, Cisco IOS版本15M&T](#)
- [技术支持和文档 - Cisco Systems](#)