

# strongSwan como um cliente VPN de acesso remoto (Xauth) que conecte ao Cisco IOS Software - exemplo de configuração

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Topologia](#)

[Configurar o Cisco IOS Software](#)

[Configurar strongSwan](#)

[Verificar](#)

[Troubleshooting](#)

[Resumo](#)

[Informações Relacionadas](#)

## Introdução

Este documento descreve como configurar strongSwan como um cliente do IPSec VPN do Acesso remoto que conecte ao software do <sup>®</sup> do Cisco IOS.

strongSwan é o software livre que é usado a fim construir túneis do Internet Key Exchange (IKE) /IPSec VPN e construir o LAN para LAN e os túneis de acesso remoto com Cisco IOS Software.

## Pré-requisitos

### Requisitos

Cisco recomenda que você tem o conhecimento básico destes assuntos:

- Configuração de Linux
- Configuração de VPN no Cisco IOS Software

### [Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software:

- Cisco IOS Software Release 15.3T
- 5.0.4 strongSwan
- Kernel (centro) de Linux 3.2.12

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Configurar

Notas:

Use a [Command Lookup Tool](#) ( [somente clientes registrados](#)) para obter mais informações sobre os comandos usados nesta seção.

[A ferramenta Output Interpreter](#) ([clientes registrados somente](#)) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos debug.

## Topologia

O cliente remoto recebe um endereço IP de Um ou Mais Servidores Cisco ICM NT do pool 10.10.0.0/16. O tráfego entre 10.10.0.0/16 e 192.168.1.0/24 é protegido.

## Configurar o Cisco IOS Software

Neste exemplo, o cliente strongSwan precisa o acesso seguro à rede de LAN 192.168.1.0/24 do Cisco IOS Software. O cliente remoto usa o nome do grupo do RA (este é o IKEID) assim como do username de Cisco e de senha de Cisco.

O cliente obtém o endereço IP de Um ou Mais Servidores Cisco ICM NT do pool 10.10.0.0/16. Também, o Access Control List rachado (ACL) é empurrado para o cliente; esse ACL forçará o cliente a enviar o tráfego a 192.168.1.0/24 através do 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

```

Cisco recomenda que você não atribua o endereço IP estático usual em um Virtual-molde. As interfaces de acesso virtual são clonadas e herdam sua configuração do Virtual-molde do pai, que poderia criar endereços de IP duplicados. Contudo, o Virtual-molde refere um endereço IP de Um ou Mais Servidores Cisco ICM NT com “a palavra-chave unnumbered IP” a fim povoar a tabela de adjacência. “A palavra-chave unnumbered IP” é apenas uma referência a um endereço IP de Um ou Mais Servidores Cisco ICM NT físico ou lógico no roteador.

Para a compatibilidade avançada com roteamento IKE em IKEv2, use um endereço interno, e evite o uso de endereços locais do IPsec os “como “o IP unnumbered.”

## Configurar strongSwan

Este procedimento descreve como configurar strongSwan:

## 1. Use esta configuração no arquivo de /etc/ipsec.conf:

```
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
```

A palavra-chave do rightsubnet foi ajustada a fim indicar que tráfego deve ser protegido. Nesta encenação, a associação de segurança IPsec (SA) é construída entre 192.168.1.0/24 (no Cisco IOS Software) e o endereço IP de Um ou Mais Servidores Cisco ICM NT strongSwan, que é recebido do pool 10.10.0.0/16.

Sem rightsubnet especificado, você pôde esperar ter a rede de 0.0.0.0 e IPsec SA entre o endereço IP cliente e a rede de 0.0.0.0. Aquele é o comportamento quando o Cisco IOS Software é usado como um cliente.

Mas esta expectativa não está correta para strongSwan. Sem rightsubnet definido, strongSwan propõe um endereço IP de Um ou Mais Servidores Cisco ICM NT externo do gateway (Cisco IOS Software) em phase2 da negociação; nesta encenação, esse gateway é 10.48.67.167. Porque o objetivo é proteger o tráfego que está indo a uma LAN interna no Cisco IOS Software (192.168.1.0/24) e não a um endereço IP de Um ou Mais Servidores Cisco ICM NT externo do Cisco IOS Software, o rightsubnet foi usado.

## 2. Use esta configuração no arquivo de /etc/ipsec.secrets:

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

# Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Este procedimento descreve como testar e verificar a configuração strongSwan:

## 1. Comece strongSwan com debuga permitido:

```
gentool ~ # /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. Quando o túnel de strongSwan é iniciado, toda a informação geral em phase1, em Xauth, e em phase2 está indicada:

```
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. Quando você permite debuga em strongSwan, muita informação pode ser retornada. Este é o mais importante debuga para usar-se quando o túnel é iniciado:

```

#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. Envie o tráfego do cliente:

```
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. Verifique a interface dinâmica no Cisco IOS Software:

```
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-Templatel
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. Verifique os contadores do IPsec no Cisco IOS Software:

```
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. Verifique o estado em strongSwan:

```
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
```



# Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

## Resumo

Este documento descreveu a configuração de um cliente strongSwan que conectasse como um cliente do IPSec VPN ao Cisco IOS Software.

É igualmente possível configurar um túnel de LAN para LAN de IPSec entre o Cisco IOS Software e strongSwan. Adicionalmente, IKEv2 entre ambos os dispositivos trabalha corretamente ambos para o telecontrole e o acesso do LAN para LAN.

## Informações Relacionadas

- [Documentação de Openswan](#)
- [Documentação de usuário de StrongSwan](#)
- [Configurando a seção de site para site da versão 2 e do FlexVPN do intercâmbio de chave de Internet de FlexVPN e de manual de configuração da versão 2 do intercâmbio de chave de Internet, Cisco IOS Release 15M&T](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)