

ASAおよびStrongswanを使用したサイト間VPNトンネルの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[シナリオ](#)

[ネットワーク図](#)

[ASA の設定](#)

[strongSwan 設定](#)

[便利なコマンド\(strongswan\)](#)

[確認](#)

[ASA上](#)

[フェーズ1の確認](#)

[フェーズ2の確認](#)

[strongSwan上](#)

[トラブルシューティング](#)

[ASA のデバッグ](#)

[strongSwanのデバッグ](#)

[関連情報](#)

はじめに

このドキュメントでは、ASAとstrongSwanサーバ間のCLIを使用してサイト間IPSecインターネットキーエクスチェンジバージョン1トンネルを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Adaptive Security Appliance (ASA)
- 基本的なLinuxコマンド
- 一般的な IPsec の概念

使用するコンポーネント

このドキュメントの情報は、次のバージョンに基づくものです。

- 9.12(3)9を実行するCisco ASA
- strongSwan U5.8.2を実行するUbuntu 20.04

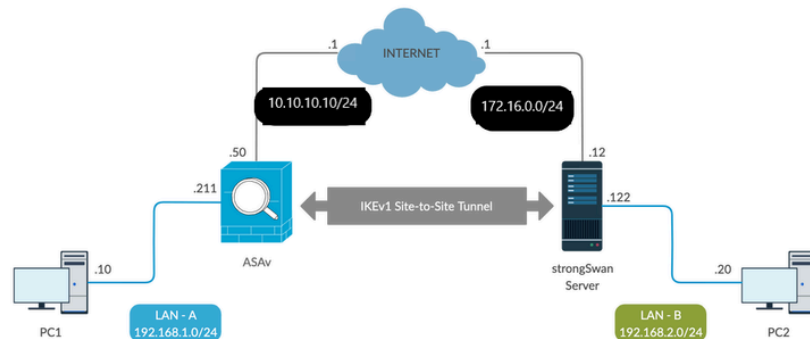
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定


このセクションでは、ASAおよびstrongSwanの設定を完了する方法について説明します。

シナリオ

この設定では、LAN-AのPC1がLAN-BのPC2と通信しようとしています。このトラフィックは暗号化され、ASAとstrongSwanサーバ間のInternet Key Exchange Version 1(IKEv1)トンネルを介して送信される必要があります。両方のピアは事前共有キー(PSK)で相互に認証します。



ネットワーク図

 注：内部ネットワークと外部ネットワークの両方、特にサイト間VPNトンネルを確立するために使用されるリモートピアへの接続があることを確認します。基本的な接続を確認するには、pingを使用できます。

ASA の設定

```
<#root>
```


```
!Configure the ASA interfaces
```


```
!  
interface GigabitEthernet0/0  
nameif inside  
security-level 100  
ip address 192.168.1.211 255.255.255.0  
!  
interface GigabitEthernet0/1  
nameif outside  
security-level 0  
ip address 10.10.10.10 255.255.255.0  
!  
  
!Configure the ACL for the VPN traffic of interest  
  
!  
object-group network local-network  
network-object 192.168.1.0 255.255.255.0  
!  
object-group network remote-network  
network-object 192.168.2.0 255.255.255.0  
!  
access-list asa-strongswan-vpn extended permit ip object-group local-network object-group remote-network  
!  
  
!Enable IKEv1 on the 'Outside' interface  
  
!  
crypto ikev1 enable outside  
!  
  
!Configure how ASA identifies itself to the peer  
  
!  
crypto isakmp identity address  
!  
  
!Configure the IKEv1 policy  
  
!  
crypto ikev1 policy 10  
authentication pre-share  
encryption aes-256  
hash sha  
group 5  
lifetime 3600  
!  
  
!Configure the IKEv1 transform-set  
  
!  
crypto ipsec ikev1 transform-set tset esp-aes-256 esp-sha-hmac  
!  
  
!Configure a crypto map and apply it to outside interface  
  
!  
crypto map outside_map 10 match address asa-strongswan-vpn  
crypto map outside_map 10 set peer 172.16.0.0
```

```
crypto map outside_map 10 set ikev1 transform-set tset
crypto map outside_map 10 set security-association lifetime seconds 28800
crypto map outside_map interface outside
!
```

!Configure the Tunnel group (LAN-to-LAN connection profile)

```
!
tunnel-group 172.16.0.0 type ipsec-l2l
tunnel-group 172.16.0.0 ipsec-attributes
ikev1 pre-shared-key cisco
!
```

 注：IKEv1 ポリシーが一致するのは、2つのピアからの両方のポリシーに、同じ認証、暗号化、ハッシュ、Diffie-Hellman パラメータ値が含まれている場合です。IKEv1 では、リモートピアのポリシーで指定されているライフタイムが、開始側から送信されたポリシーのライフタイム以下であることも必要です。ライフタイムが同じでない場合、ASAは短いライフタイムを使用します。また、特定のポリシーパラメータの値を指定しない場合は、デフォルト値が適用されます。

 注:VPNトラフィックのACLでは、ネットワークアドレス変換(NAT)の後に送信元と宛先のIPアドレスが使用されます。

NAT除外 (オプション):

通常、VPNトラフィックに対してNATを実行する必要はありません。そのトラフィックを除外するには、アイデンティティ NAT ルールを作成する必要があります。アイデンティティ NAT ルールは、あるアドレスを同じアドレスに変換するだけです。

```
<#root>
```

```
nat (inside,outside) source static
local-network local-network
destination static
remote-network remote-network
no-proxy-arp route-lookup
```

strongSwan 設定

Ubuntuでは、IPsecトンネルで使用する設定パラメータを使用して、これら2つのファイルを変更します。お気に入りのエディタを使用して編集できます。

```
/etc/ipsec.conf
```

/etc/ipsec.secrets

<#root>

/etc/ipsec.conf - strongSwan IPsec configuration file

basic configuration

config setup

strictcrlpolicy=no
uniqueids = yes
charondebug = "all"

VPN to ASA

conn vpn-to-asa

authby=secret
left=%defaultroute
leftid=172.16.0.0
leftsubnet=192.168.2.0/24
right=10.10.10.10
rightid=10.10.10.10
rightsubnet=192.168.1.0/24
ike=aes256-sha1-modp1536
esp=aes256-sha1
keyingtries=%forever
leftauth=psk
rightauth=psk
keyexchange=ikev1
ikelifetime=1h
lifetime=8h
dpddelay=30
dpdtimeout=120
dpdaction=restart
auto=start

config setup

- Defines general configuration parameters.

strictcrlpolicy

- Defines if a fresh CRL must be available in order for the peer authentication based on RSA signatures to succeed.

uniqueids

- Defines whether a particular participant ID must be kept unique, with any new IKE_SA using an ID deemed to replace all old ones using that ID.

charondebug

- Defines how much charon debugging output must be logged.

conn

- Defines a connection.

authby -

Defines how the peers must authenticate; acceptable values are secret or psk, pubkey, rsasig, ecdsasig

left -

Defines the IP address of the strongSwan's interface participating in the tunnel.

lefid -

Defines the identity payload for the strongSwan.

leftsubnet -

Defines the private subnet behind the strongSwan, expressed as network/netmask.

right -

Defines the public IP address of the VPN peer.

rightid -

Defines the identity payload for the VPN peer.

rightsubnet -

Defines the private subnet behind the VPN peer, expressed as network/netmask.

ike -

Defines the IKE/ISAKMP SA encryption/authentication algorithms. You can add a comma-separated list.

esp -

Defines the ESP encryption/authentication algorithms. You can add a comma-separated list.

keyingtries -

Defines the number of attempts that must be made to negotiate a connection.

keyexchange -

Defines the method of key exchange, whether IKEv1 or IKEv2.

ikelifetime -

Defines the duration of an established phase-1 connection.

lifetime -

Defines the duration of an established phase-2 connection.

dpddelay -

Defines the time interval with which R_U_THERE messages/INFORMATIONAL exchanges are sent to the peer. These are only sent if no other traffic is received.

dpdtimeout -

Defines the timeout interval, after which all connections to a peer are deleted in case of inactivity.

dpdaction -

Defines what action needs to be performed on DPD timeout. Takes three values as parameters :

clear

,

hold

, and

restart.

With

clear

the connection is closed with no further actions taken,

hold

installs a trap policy, which catches matching traffic and tries to re-negotiate the connection on demand and

restart

immediately triggers an attempt to re-negotiate the connection. The default is

none

which disables the active sending of DPD messages.

auto -

Defines what operation, if any, must be done automatically at IPsec startup (

start

loads a connection and brings it up immediately).

<#root>

/etc/ipsec.secrets -

This file holds shared secrets or RSA private keys for authentication.

RSA private key for this host, authenticating it to any other host which knows the public part.

172.16.0.0 10.10.10.10 : PSK "cisco"

便利なコマンド(strongswan)

開始/停止/ステータス :

```
$ sudo ipsec up <接続名>
```

```
<#root>
```

```
$ sudo ipsec up vpn-to-asa
```

```
generating QUICK_MODE request 656867907 [ HASH SA No ID ID ]
sending packet: from 172.16.0.0[500] to 10.10.10.10[500] (204 bytes)
received packet: from 10.10.10.10[500] to 172.16.0.0[500] (188 bytes)
parsed QUICK_MODE response 656867907 [ HASH SA No ID ID N((24576)) ]
selected proposal: ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ
detected rekeying of CHILD_SA vpn-to-asa{2}
CHILD_SA vpn-to-asa{3} established with SPIs c9080c93_i 3f570a23_o and TS 192.168.2.0/24 === 192.168.1.0/24
connection 'vpn-to-asa' established successfully
```

```
$ sudo ipsec down <接続名>
```

```
<#root>
```

```
$ sudo ipsec down vpn-to-asa
```

```
generating QUICK_MODE request 656867907 [ HASH SA No ID ID ]
sending packet: from 172.16.0.0[500] to 10.10.10.10[500] (204 bytes)
received packet: from 10.10.10.10[500] to 172.16.0.0[500] (188 bytes)
parsed QUICK_MODE response 656867907 [ HASH SA No ID ID N((24576)) ]
selected proposal: ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ
detected rekeying of CHILD_SA vpn-to-asa{2}
CHILD_SA vpn-to-asa{3} established with SPIs c9080c93_i 3f570a23_o and TS 192.168.2.0/24 === 192.168.1.0/24
connection 'vpn-to-asa' established successfully
anurag@strongswan214:~$ sudo ipsec down vpn-to-asa
closing CHILD_SA vpn-to-asa{3} with SPIs c9080c93_i (0 bytes) 3f570a23_o (0 bytes) and TS 192.168.2.0/24 === 192.168.1.0/24
sending DELETE for ESP CHILD_SA with SPI c9080c93
generating INFORMATIONAL_V1 request 3465984663 [ HASH D ]
sending packet: from 172.16.0.0[500] to 10.10.10.10[500] (76 bytes)
deleting IKE_SA vpn-to-asa[2] between 172.16.0.0[172.16.0.0]...10.10.10.10[10.10.10.10]
sending DELETE for IKE_SA vpn-to-asa[2]
generating INFORMATIONAL_V1 request 2614622058 [ HASH D ]
sending packet: from 172.16.0.0[500] to 10.10.10.10[500] (92 bytes)
IKE_SA [2] closed successfully
```

```
$ sudo ipsec再起動
```



```
Stopping strongSwan IPsec...
Starting strongSwan 5.8.2 IPsec [starter]...
```

\$ sudo ipsecステータス

```
Security Associations (1 up, 0 connecting):
vpn-to-asa[1]: ESTABLISHED 35 seconds ago, 172.16.0.0[172.16.0.0]...10.10.10.10[10.10.10.10]
vpn-to-asa{1}: REKEYED, TUNNEL, reqid 1, expires in 7 hours
vpn-to-asa{1}: 192.168.2.0/24 === 192.168.1.0/24
vpn-to-asa{2}: INSTALLED, TUNNEL, reqid 1, ESP SPIs: c0d93265_i 599b4d60_o
vpn-to-asa{2}: 192.168.2.0/24 === 192.168.1.0/24
```

\$ sudo ipsecステータス

```
Status of IKE charon daemon (strongSwan 5.8.2, Linux 5.4.0-37-generic, x86_64):
uptime: 2 minutes, since Jun 27 07:15:14 2020
malloc: sbrk 2703360, mmap 0, used 694432, free 2008928
worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
loaded plugins: charon aesni aes rc2 sha2 sha1 md5 mgf1 random nonce x509 revocation constraints pubkey
Listening IP addresses:
172.16.0.0
192.168.2.122
Connections:
vpn-to-asa: %any...10.10.10.10 IKEv1, dpddelay=30s
vpn-to-asa: local: [172.16.0.0] uses pre-shared key authentication
vpn-to-asa: remote: [10.10.10.10] uses pre-shared key authentication
vpn-to-asa: child: 192.168.2.0/24 === 192.168.1.0/24 TUNNEL, dpdaction=restart
Security Associations (1 up, 0 connecting):
vpn-to-asa[1]: ESTABLISHED 2 minutes ago, 172.16.0.0[172.16.0.0]...10.10.10.10[10.10.10.10]
vpn-to-asa[1]: IKEv1 SPIs: 57e24d839bf05f95_i* 6a4824492f289747_r, pre-shared key reauthentication in 4
vpn-to-asa[1]: IKE proposal: AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1536
vpn-to-asa{2}: INSTALLED, TUNNEL, reqid 1, ESP SPIs: c0d93265_i 599b4d60_o
vpn-to-asa{2}: AES_CBC_256/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 7 hours
vpn-to-asa{2}: 192.168.2.0/24 === 192.168.1.0/24
```

IPSecトンネルのポリシーと状態の取得：

\$ sudo ip xfrm状態

```
src 172.16.0.0 dst 10.10.10.10
proto esp spi 0x599b4d60 reqid 1 mode tunnel
replay-window 0 flag af-unspec
auth-trunc hmac(sha1) 0x52c84359280868491a37e966384e4c6db05384c8 96
enc cbc(aes) 0x99e00f0989fec6baa7bd4ea1c7fbefdf37f04153e721a060568629e603e23e7a
```

```
anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
src 10.10.10.10 dst 172.16.0.0
proto esp spi 0xc0d93265 reqid 1 mode tunnel
replay-window 32 flag af-unspec
auth-trunc hmac(sha1) 0x374d9654436a4c4fe973a54da044d8814184861e 96
enc cbc(aes) 0xf51a4887281551a246a73c3518d938fd4918928088a54e2abc5253bd2de30fd6
anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
```

\$ sudo ip xfrmポリシー

```
src 192.168.2.0/24 dst 192.168.1.0/24
dir out priority 375423
tmpl src 172.16.0.0 dst 10.10.10.10
proto esp spi 0x599b4d60 reqid 1 mode tunnel
src 192.168.1.0/24 dst 192.168.2.0/24
dir fwd priority 375423
tmpl src 10.10.10.10 dst 172.16.0.0
proto esp reqid 1 mode tunnel
src 192.168.1.0/24 dst 192.168.2.0/24
dir in priority 375423
tmpl src 10.10.10.10 dst 172.16.0.0
proto esp reqid 1 mode tunnel
src 0.0.0.0/0 dst 0.0.0.0/0
socket in priority 0
src 0.0.0.0/0 dst 0.0.0.0/0
socket out priority 0
src 0.0.0.0/0 dst 0.0.0.0/0
socket in priority 0
src 0.0.0.0/0 dst 0.0.0.0/0
socket out priority 0
src ::/0 dst ::/0
socket in priority 0
src ::/0 dst ::/0
socket out priority 0
src ::/0 dst ::/0
socket in priority 0
src ::/0 dst ::/0
socket out priority 0
```

サービスの実行中にシークレットをリロードします。

\$ sudo ipsec rereadsecrets

トラフィックがトンネルを通過するかどうかを確認します。


\$ sudo tcpdump esp

09:30:27.788533 IP 172.16.0.0 > 10.10.10.10: ESP(spi=0x599b4d60,seq=0x1e45), length 132

```
09:30:27.788779 IP 172.16.0.0 > 10.10.10.10: ESP(spi=0x599b4d60,seq=0x1e45), length 132
09:30:27.790348 IP 10.10.10.10 > 172.16.0.0: ESP(spi=0xc0d93265,seq=0x11), length 132
09:30:27.790512 IP 10.10.10.10 > 172.16.0.0: ESP(spi=0xc0d93265,seq=0x11), length 132
09:30:28.788946 IP 172.16.0.0 > 10.10.10.10: ESP(spi=0x599b4d60,seq=0x1e46), length 132
09:30:28.789201 IP 172.16.0.0 > 10.10.10.10: ESP(spi=0x599b4d60,seq=0x1e46), length 132
09:30:28.790116 IP 10.10.10.10 > 172.16.0.0: ESP(spi=0xc0d93265,seq=0x12), length 132
09:30:28.790328 IP 10.10.10.10 > 172.16.0.0: ESP(spi=0xc0d93265,seq=0x12), length 132
```

確認

トンネルがアップしているかどうか、およびトラフィックを通過させているかどうかを確認する前に、対象のトラフィックがASAまたはstrongSwanサーバのいずれかに送信されていることを確認する必要があります。

 注:ASAでは、対象のトラフィックと一致するパケットトレーサツールを使用して、IPSecトンネルを開始できます(たとえば、tcp 192.168.1.100内部のパケットトレーサ入力 12345192.168.2.200 80など)。

ASA上

フェーズ 1 の確認

IKEv1フェーズ1がASAでアップしているかどうかを確認するには、show crypto ikev1 sa(またはshow crypto isakmp sa)コマンドを入力します。正常な出力は、MM_ACTIVEstateが表示されます。

```
<#root>
```

```
ASAv#
```

```
show crypto ikev1 sa
```

```
IKEv1 SAs:
```

```
Active SA: 1
```

```
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
```

```
Total IKE SA: 1
```

```
1 IKE Peer:
```

```
172.16.0.0
```


```
Type : L2L Role : responder
```

```
Rekey : no State :
```

```
MM_ACTIVE
```

フェーズ 2 の確認

IKEv1フェーズ2がASAでアップしているかどうかを確認するには、`show crypto ipsec sa` コマンドを使用して、アップグレードを実行します。正常な出力は、着信および発信のセキュリティパラメータ インデックス (SPI) が表示されます。トラフィックがトンネルを通過する場合は、`encaps/decaps`カウンタが増加する必要があります。

 注：各ACLエントリに対して個別の着信/発信SAが作成され、その結果、`show crypto ipsec sa`コマンドの長い出力が発生する可能性があります (クリプトACLのACEエントリの数によって異なります) 。

<#root>

ASAv#

```
show crypto ipsec sa peer 172.16.0.0
```

interface:

outside

Crypto map tag: outside_map, seq num: 10, local addr: 10.10.10.10

```
access-list asa-strongswan-vpn extended permit ip 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
local ident (addr/mask/prot/port): (
```

```
192.168.1.0
```

```
/255.255.255.0/0/0)
```

```
remote ident (addr/mask/prot/port): (
```

```
192.168.2.0
```

```
/255.255.255.0/0/0)
```

```
current_peer:
```

```
172.16.0.0
```

#

```
pkts encaps: 37, #pkts encrypt: 37, #pkts digest: 37
```

#

```
pkts decaps: 37, #pkts decrypt: 37, #pkts verify: 37
```

```
#pkts compressed: 0, #pkts decompressed: 0
```

```
#pkts not compressed: 37, #pkts comp failed: 0, #pkts decomp failed: 0
```

```
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
```

```
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

```
#TFC rcvd: 0, #TFC sent: 0
```

```
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
```

```
#send errors: 0, #recv errors: 0
```

local crypto endpt.: 10.10.10.10/0, remote crypto endpt.:

172.16.0.0

/0

path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled

current outbound spi: C8F1BFAB

current inbound spi : 3D64961A

inbound esp sas:

spi: 0x3D64961A (1030002202)

SA State: active

transform: esp-aes-256 esp-sha-hmac no compression

in use settings ={L2L, Tunnel, IKEv1, }

slot: 0, conn_id: 31, crypto-map: outside_map

sa timing: remaining key lifetime (kB/sec): (4373997/27316)

IV size: 16 bytes

replay detection support: Y

Anti replay bitmap:

0x000001FF 0xFFFFFFFF

outbound esp sas:

spi: 0xC8F1BFAB (3371286443)

SA State: active

transform: esp-aes-256 esp-sha-hmac no compression

in use settings ={L2L, Tunnel, IKEv1, }

slot: 0, conn_id: 31, crypto-map: outside_map

sa timing: remaining key lifetime (kB/sec): (4373997/27316)

IV size: 16 bytes

replay detection support: Y

Anti replay bitmap:

0x00000000 0x00000001

または、show vpn-sessiondb コマンドを使用して、フェーズ1と2の両方の詳細をまとめて確認できます。

<#root>

ASAv#

show vpn-sessiondb detail l2l filter ipaddress 172.16.0.0

Session Type: LAN-to-LAN Detailed

Connection :

172.16.0.0

Index : 3 IP Addr : 172.16.0.0

Protocol :

IKEv1 IPsec

Encryption : IKEv1: (1)AES256 IPsec: (1)AES256

Hashing : IKEv1: (1)SHA1 IPsec: (1)SHA1

Bytes Tx : 536548 Bytes Rx : 536592

Login Time : 12:45:14 IST Sat Jun 27 2020

Duration : 1h:51m:57s

IKEv1 Tunnels: 1

IPsec Tunnels: 1

IKEv1:

Tunnel ID : 3.1

UDP Src Port : 500 UDP Dst Port : 500

IKE Neg Mode : Main Auth Mode : preSharedKeys

Encryption : AES256 Hashing : SHA1

Rekey Int (T): 3600 Seconds Rekey Left(T): 2172 Seconds

D/H Group : 5

Filter Name :

IPsec:

Tunnel ID : 3.2

Local Addr : 192.168.1.0/255.255.255.0/0/0

Remote Addr : 192.168.2.0/255.255.255.0/0/0

Encryption : AES256 Hashing : SHA1

Encapsulation: Tunnel

Rekey Int (T): 28800 Seconds Rekey Left(T): 22099 Seconds

Rekey Int (D): 4608000 K-Bytes Rekey Left(D): 4607476 K-Bytes

Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes

Bytes Tx : 536638 Bytes Rx : 536676

Pkts Tx : 6356 Pkts Rx : 6389

strongSwan上

<#root>

#

sudo ipsec statusall

Status of IKE charon daemon (strongSwan 5.8.2, Linux 5.4.0-37-generic, x86_64):

uptime: 2 minutes, since Jun 27 07:15:14 2020

malloc: sbrk 2703360, mmap 0, used 694432, free 2008928

worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3

```
Loaded plugins: charon aesni aes rc2 sha2 sha1 md5 mgf1 random nonce x509 revocation constraints pubkey
Listening IP addresses:
172.16.0.0
192.168.2.122
Connections:
vpn-to-asa: %any...10.10.10.10 IKEv1, dpddelay=30s
vpn-to-asa:

local: [172.16.0.0]

  uses pre-shared key authentication
vpn-to-asa:

remote: [10.10.10.10]

  uses pre-shared key authentication
vpn-to-asa:

child: 192.168.2.0/24 === 192.168.1.0/24 TUNNEL

, dpdaction=restart
Security Associations (1 up, 0 connecting):
vpn-to-asa[1]:

ESTABLISHED

  2 minutes ago, 172.16.0.0[172.16.0.0]...10.10.10.10[10.10.10.10]
vpn-to-asa[1]: IKEv1 SPIs: 57e24d839bf05f95_i* 6a4824492f289747_r, pre-shared key reauthentication in 4
vpn-to-asa[1]: IKE proposal: AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1536
vpn-to-asa{2}:

INSTALLED, TUNNEL,


  reqid 1, ESP SPIs: c0d93265_i 599b4d60_o
vpn-to-asa{2}: AES_CBC_256/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 7 hours
vpn-to-asa{2}:

192.168.2.0/24 === 192.168.1.0/24
```

トラブルシューティング


ASA のデバッグ

ASAファイアウォールでのIPSec IKEv1トンネルネゴシエーションをトラブルシューティングするには、次のデバッグコマンドを使用できます。

 注意:ASAでは、さまざまなデバッグレベルを設定できます。デフォルトでは、レベル1が使用されます。デバッグレベルを変更すると、デバッグの冗長性が増す場合があります。この場合、レベル127はトラブルシューティングに十分な詳細を提供します。特に実稼働環境では、注意して実行してください。

```
<#root>
```

```
debug crypto ipsec 127
debug crypto isakmp 127
debug ike-common 10
```

 注:ASAに複数のVPNトンネルがある場合、デバッグ出力に指定したピアだけが含まれるように制限するために、条件付きデバッグ(debug crypto condition peer A.B.C.D)を使用することをお勧めします。

strongSwanのデバッグ

ipsec.confファイルでcharonデバッグが有効になっていることを確認します。

```
<#root>
```

```
charondebug = "all"
```

最終的にログメッセージが表示される場所は、システムでのsyslogの設定方法によって異なります。一般的な場所は/var/log/daemon、/var/log/syslog、または/var/log/messagesです。

関連情報

- [strongSwan ユーザドキュメント](#)
- [Cisco IOS®とstrongSwan間のIKEv1/IKEv2の設定例](#)
- [ASAとCisco IOS®ルータ間のサイト間IPSec IKEv1トンネルの設定](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。