使用ASA和Strongswan配置站点到站点VPN隧道

目录

简介

本文档介绍如何通过ASA和strongSwan服务器之间的CLI配置站点到站点IPSec Internet密钥交换版本1隧道。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科自适应安全设备(ASA)
- 基本Linux命令
- 一般IPSec概念

使用的组件

本文档中的信息基于以下版本：

- 运行9.12(3)9的Cisco ASAv
- 运行strongSwan U5.8.2的Ubuntu 20.04

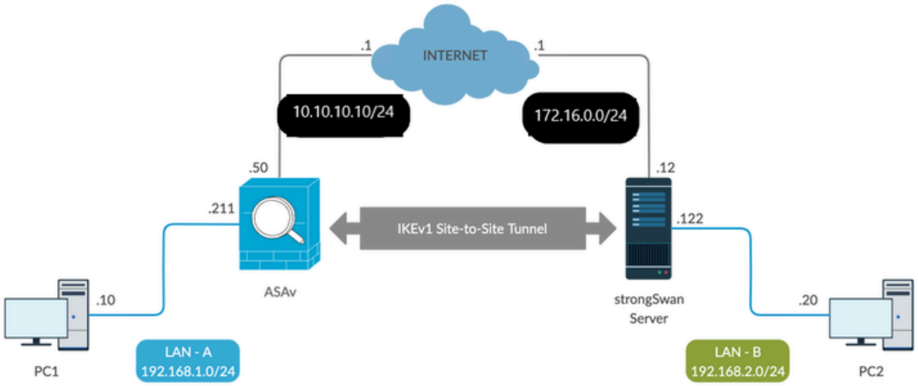
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

本节介绍如何完成ASA和strongSwan配置。

场景

在此设置中，LAN-A中的PC1要与LAN-B中的PC2通信。此流量需要加密，并通过ASA和stongSwan服务器之间的互联网密钥交换版本1(IKEv1)隧道发送。两个对等体使用预共享密钥(PSK)相互进行身份验证。



网络图

注：确保同时连接到内部和外部网络，尤其是连接到用于建立站点到站点VPN隧道的远程对等设备。您可以使用ping检验基本连通性。

ASA 配置

<#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-networ
!
```

!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
!
```

注意： 当来自两个对等体的两个策略包含相同的身份验证、加密、哈希和Diffie-Hellman参数值时，存在IKEv1策略匹配。对于IKEv1，远程对等体策略还必须指定小于或等于发起方发送的策略中的生存期的生存期。如果生存时间不同，则ASA使用更短的生存时间。 此外，如果没有为给定的策略参数指定值，则会应用默认值。

注:VPN流量的ACL在网络地址转换(NAT)后使用源和目标IP地址。

NAT免除（可选）：

通常，必须在VPN流量上不执行NAT。要免除该流量，您必须创建身份NAT规则。身份NAT规则仅将地址转换为同一地址。

<#root>

```
nat (inside,outside) source static

local-network local-network

 destination static

remote-network remote-network

 no-proxy-arp route-lookup
```

strongSwan配置

在Ubuntu上，您将使用要在IPsec隧道中使用的配置参数修改这两个文件。您可以使用您最喜欢的编辑器来编辑它们。

/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 paricipating 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 paramters :

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"
```

有用命令(strongswan)

开始/停止/状态：

$ sudo ipsec up <connection-name>

<#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.
connection 'vpn-to-asa' established successfully
```

$ sudo ipsec down <connection-name>

<#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.
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 192.168.2.0/2
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 restart

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

$ sudo ipsec status

```
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 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
```

获取IPsec隧道的策略和状态：

$ sudo ip xfrm state

```
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 policy

```
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
```

在服务运行时重新加载密钥：

```
$ sudo ipsec rereadsecrets
```

检查流量是否流经隧道：

```
$ 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
```

验证

在验证隧道是否启用以及是否传递流量之前，必须确保将相关流量发送到ASA或strongSwan服务器

。

✎ 注：在ASA上，可以使用与感兴趣流量匹配的Packet Tracer工具来启动IPSec隧道(例如tcp 192.168.1.100 12345 192.168.2.200 80内部的packet-tracer输入，详情如下)。

在ASA上

第1阶段验证

要验证ASA上的IKEv1第1阶段是否已启动，请输入show crypto ikev1 sa(或show crypto isakmp sa)命令。预期输出是查看MM_ACTIVEstate:

<#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
```

第2阶段验证

要验证ASA上的IKEv1第2阶段是否已启用，请输入 show crypto ipsec sa 命令。预期输出是查看入站和出站安全参数索引(SPI)。如果流量通过隧道，您必须看到封装/解封计数器递增。

✎ 注:对于每个ACL条目都创建了单独的入站/出站SA，这可能会导致长show crypto ipsec sa命令输出（取决于加密ACL中的ACE条目数）。

<#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
```

或者，您可以使用命令show vpn-sessiondb同时验证第1阶段和第2阶段的详细信息。

<#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
```

关于strongSwan

<#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
```

故障排除

ASA调试

要对ASA防火墙上的IPSec IKEv1隧道协商进行故障排除，您可以使用以下命令：

注意：在ASA上，您可以设置各种调试级别；默认情况下，使用级别1。如果更改调试级别，调试的详细程度可能会增加。在中，此案例级别127提供了用于故障排除的足够详细信息。请谨慎执行此操作，尤其是在生产环境中。

<#root>

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

注意：如果ASA上有多个VPN隧道，建议使用条件调试(debug crypto condition peer A.B.C.D)，以便将调试输出限制为仅包括指定的对等体。

strongSwan调试

确保在ipsec.conf文件中启用了charon调试：

<#root>

```
charondebug = "all"
```

日志消息最终结束的位置取决于系统日志的配置方式。常见位置为/var/log/daemon、/var/log/syslog或/var/log/messages。

相关信息

- strongSwan用户文档
- Cisco IOS®和strongSwan之间的IKEv1/IKEv2配置示例
- 在ASA和Cisco IOS®路由器之间配置站点到站点IPSec IKEv1隧道

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。