

strongSwan作為連線到Cisco IOS軟體的遠端訪問VPN客戶端(Xauth) — 配置示例

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[拓撲](#)

[設定Cisco IOS軟體](#)

[配置strongSwan](#)

[驗證](#)

[疑難排解](#)

[摘要](#)

[相關資訊](#)

簡介

本文檔介紹如何將strongSwan配置為連線到Cisco IOS®軟體的遠端訪問IPSec^{VPN}客戶端。

strongSwan是一種開源軟體，用於構建網際網路金鑰交換(IKE)/IPSec VPN隧道以及使用Cisco IOS軟體構建LAN到LAN和遠端訪問隧道。

必要條件

需求

思科建議您瞭解以下主題的基本知識：

- Linux配置
- Cisco IOS軟體上的VPN配置

採用元件

本檔案中的資訊是根據以下軟體版本：

- Cisco IOS軟體版本15.3T

- strongSwan 5.0.4
- Linux核心3.2.12

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

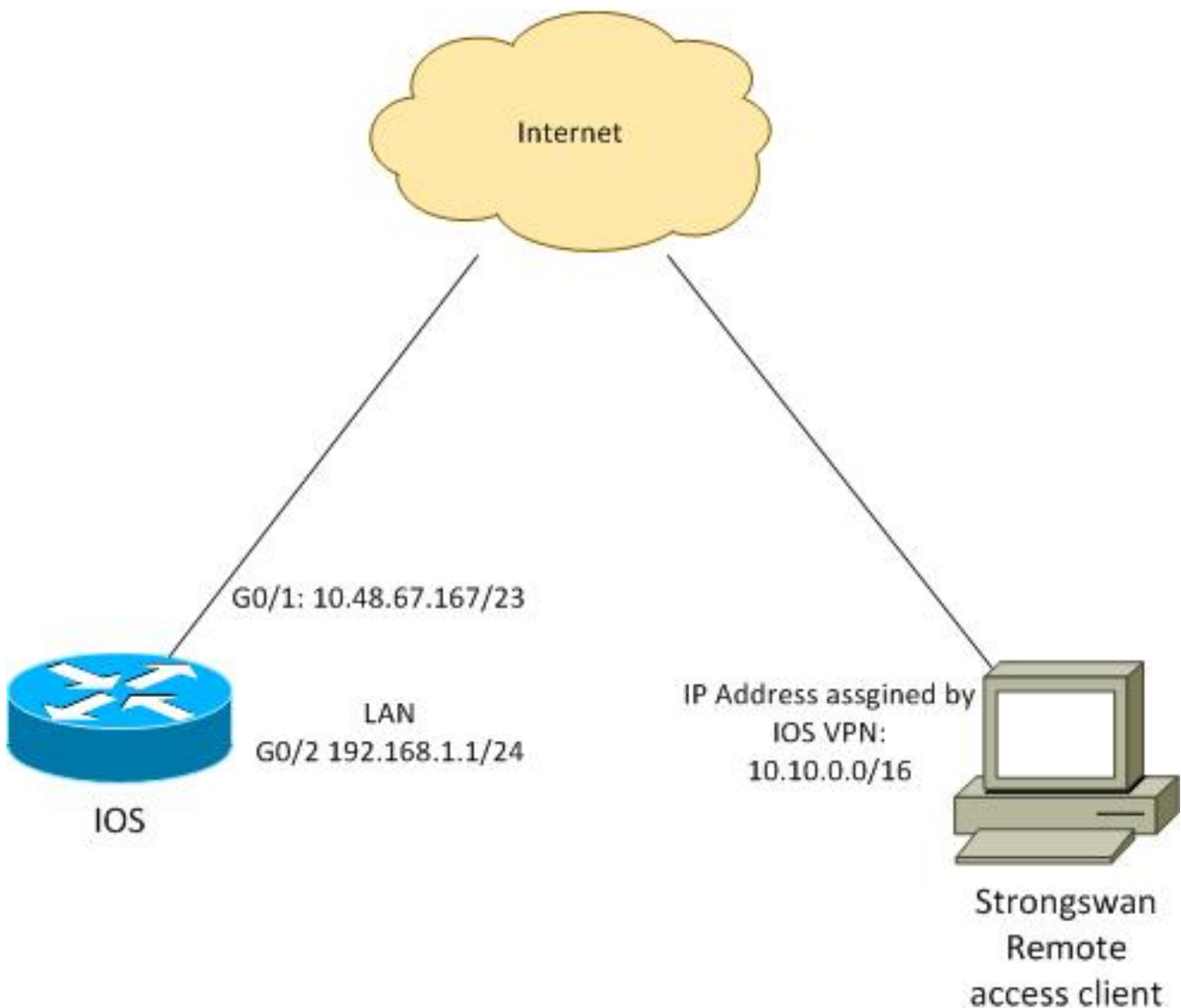
附註：

使用[命令查詢工具](#)(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

[輸出直譯器工具](#)(僅供已註冊客戶使用)支援某些show命令。使用輸出直譯器工具來檢視show命令輸出的分析。

使用 debug 指令之前，請先參閱[有關 Debug 指令的重要資訊](#)。

拓撲



遠端客戶端收到來自池10.10.0.0/16的IP地址。10.10.0.0/16和192.168.1.0/24之間的流量受到保護

。

設定Cisco IOS軟體

在本示例中，strongSwan客戶端需要安全訪問Cisco IOS軟體LAN網路192.168.1.0/24。遠端客戶端使用組名RA (這是IKEID) 以及cisco的使用者名稱和Cisco的密碼。

客戶端從池10.10.0.0/16獲取IP地址。此外，拆分訪問控制清單(ACL)被推送到客戶端；該ACL將強制客戶端通過VPN將流量傳送到192.168.1.0/24。

```
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
```

思科建議您不要在虛擬模板上分配通常的靜態IP地址。虛擬訪問介面被克隆並從父虛擬模板繼承其配置，這樣可能會建立重複的IP地址。但是，虛擬模板通過「ip unnumbered」關鍵字引用IP地址以填充鄰接表。「ip unnumbered」關鍵字僅僅是對路由器上物理或邏輯IP地址的引用。

為了與IKEv2中的IKE路由向前相容，請使用內部地址，並避免將IPSec「本地地址」用作「ip unnumbered」。

配置strongSwan

以下過程介紹了如何配置strongSwan:

1. 在/etc/ipsec.conf檔案中使用此配置：

```
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
```

已設定rightsubnet關鍵字以指示應保護哪些流量。在此案例中，IPSec安全關聯(SA)建立在192.168.1.0/24 (在Cisco IOS軟體上)與strongSwan IP位址(從池10.10.0.0/16接收)之間。

如果沒有指定rightsubnet，您可能希望客戶端IP地址與0.0.0.0網路之間具有0.0.0.0網路和IPSec SA。這就是將Cisco IOS軟體用作使用者端時的行為。

但這種預期對strongSwan來說是不正確的。在沒有定義正確的子網的情況下，strongSwan在協商的第2階段提議外部網關 (Cisco IOS軟體) IP地址；在此案例中，網關是10.48.67.167。由於目標是保護流向Cisco IOS軟體(192.168.1.0/24)上內部LAN的流量，而不是流向外部Cisco IOS軟體IP地址的流量，因此使用了正確的子網。

2. 在/etc/ipsec.secrets檔案中使用此配置：

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

驗證

使用本節內容，確認您的組態是否正常運作。

以下程式介紹如何測試和驗證strongSwan組態：

1. 啟動strongSwan並啟用調試：

```
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. 從strongSwan啟動隧道時，會顯示第1階段、第Xauth和第2階段的所有一般資訊：

```

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. 在strongSwan上啟用調試時，可以返回許多資訊。這是啟動通道時要使用的最重要的偵錯：

```

#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. 從客戶端傳送流量：

```

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. 檢查Cisco IOS軟體上的動態介面：

```

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. 檢查Cisco IOS軟體上的IPSec計數器：

```
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. 驗證strongSwan上的狀態：

```
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
```

```
mmap: 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
```

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

摘要

本文檔描述了作為IPSec VPN客戶端連線到Cisco IOS軟體的strongSwan客戶端的配置。

也可以在Cisco IOS軟體和strongSwan之間配置IPSec LAN到LAN隧道。此外，兩台裝置之間的IKEv2在遠端和LAN對LAN訪問中均正常工作。

相關資訊

- [Openswan檔案](#)
- [StrongSwan使用者檔案](#)
- [Cisco IOS版本15M&T的FlexVPN和Internet金鑰交換版本2配置指南的Configuring Internet Key Exchange Version 2 and FlexVPN Site-to-Site部分](#)
- [技術支援與文件 - Cisco Systems](#)