在两个路由器和 Cisco VPN 客户端 4.x 之间配置 IPSec

目录

简介

本文档展示如何在两个 Cisco 路由器与 Cisco VPN 客户端 4.x 之间配置 IPsec。Cisco IOS® 软件版本 12.2(8)T 及更高版本支持从 Cisco VPN 客户端 3.x 及更高版本进行连接。

请参阅配置 IPsec 路由器动态 LAN-to-LAN 对等体和 VPN 客户端，了解更多有关 L2L 隧道的一端由另一端动态分配 IP 地址的场景的信息。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 为IPsec将分配的地址池
- 名为 **3000clients** 的组使用 VPN 客户端的预共享密钥 cisco123
- 组和用户身份验证在 VPN 客户端的路由器上本地完成。
- **no-xauth** 参数用于 LAN-to-LAN 隧道的 ISAKMP 密钥命令。

使用的组件

本文档中的信息基于以下软件和硬件版本。

- 运行 Cisco IOS 软件版本 12.2(8)T 的路由器。**注意：** 本文最近使用 Cisco IOS 软件版本 12.3(1) 进行过测试。无需进行更改。
- Cisco VPN 客户端 for Windows 版本 4.x（所有 VPN 客户端 3.x 和更高版本正常工作）。

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。

路由器上的 **show version** 命令的输出如下所示。

```
vpn2611#show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-JK9O3S-M), Version 12.2(8)T,
   RELEASE SOFTWARE (fc2)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Thu 14-Feb-02 16:50 by ccai
Image text-base: 0x80008070, data-base: 0x81816184

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)

vpn2611 uptime is 1 hour, 15 minutes
System returned to ROM by reload
System image file is "flash:c2600-jk9o3s-mz.122-8.T"

cisco 2611 (MPC860) processor (revision 0x203)
   with 61440K/4096K bytes of memory.
Processor board ID JAD04370EEG (2285146560)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
2 Ethernet/IEEE 802.3 interface(s)
1 Serial network interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102
```

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

本部分提供用于配置本文档所述功能的信息。

网络图

本文档使用此网络设置。

注意： 本示例中的IP地址不能在全球互联网中进行路由，因为它们是实验室网络中的私有IP地址。

配置

配置 Cisco 2611 路由器

Cisco 2611 路由器

```
vpn2611#show run
Building configuration...

Current configuration : 2265 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname vpn2611
!
!--- Enable AAA for user authentication !--- and group
authorization. aaa new-model
!
!
!--- In order to enable X-Auth for user authentication,
!--- enable the aaa authentication commands.

aaa authentication login userauthen local

!--- In order to enable group authorization, enable !---
the aaa authorization commands.

aaa authorization network groupauthor local
aaa session-id common
!

!--- For local authentication of the IPSec user, !---
create the user with a password. username cisco password
0 cisco
ip subnet-zero
!
!
!
ip audit notify log
ip audit po max-events 100
!

!--- Create an Internet Security Association and !---
Key Management Protocol (ISAKMP) !--- policy for Phase 1
negotiations for the VPN 3.x Clients. crypto isakmp
policy 3
encr 3des
authentication pre-share
group 2
!

!--- Create an ISAKMP policy for Phase 1 !---
negotiations for the LAN-to-LAN tunnels. crypto isakmp
policy 10
hash md5
authentication pre-share

!--- Specify the PreShared key for the LAN-to-LAN
tunnel. !--- Make sure that you use the !--- no-xauth
parameter with your ISAKMP key.
```

```
crypto isakmp key cisco123 address 172.18.124.199 no-
xauth
!

!--- Create a group that is used to !--- specify the
WINS, DNS servers' address !--- to the client, along
with the pre-shared !--- key for authentication. crypto
isakmp client configuration group 3000client
key cisco123
dns 10.10.10.10
wins 10.10.10.20
domain cisco.com
pool ippool
!
!

!--- Create the Phase 2 Policy for actual data
encryption. crypto ipsec transform-set myset esp-3des
esp-md5-hmac
!

!--- Create a dynamic map and apply !--- the transform
set that was created earlier. crypto dynamic-map dynmap
10
set transform-set myset
!
!

!--- Create the actual crypto map, and !--- apply the
AAA lists that were created !--- earlier. Also create a
new instance for your !--- LAN-to-LAN tunnel. Specify
the peer IP address, !--- transform set, and an Access
Control List (ACL) for this !--- instance. crypto map
clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list
groupauthor
crypto map clientmap client configuration address
respond
crypto map clientmap 1 ipsec-isakmp
set peer 172.18.124.199
set transform-set myset
match address 100
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
!
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
!

!--- Apply the crypto map on the outside interface.

interface Ethernet0/0
ip address 172.18.124.159 255.255.255.0
half-duplex
crypto map clientmap
!
interface Serial0/0
no ip address
shutdown
!
interface Ethernet0/1
ip address 10.10.10.1 255.255.255.0
no keepalive
```

```
half-duplex
!
!
!--- Create a pool of addresses to be !--- assigned to
the VPN Clients. ip local pool ippool 14.1.1.100
14.1.1.200
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.1
ip http server
ip pim bidir-enable
!
!

!--- Create an ACL for the traffic !--- to be encrypted.
In this example, !--- the traffic from 10.10.10.0/24 to
10.10.20.0/24 !--- is encrypted. access-list 100 permit
ip 10.10.10.0 0.0.0.255 10.10.20.0 0.0.0.255
!
!
snmp-server community foobar RO
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
!
!
end
```

配置 3640 路由器

Cisco 3640 路由器

```
vpn3640#show run
Building configuration...

Current configuration : 1287 bytes
!
! Last configuration change at 13:47:37 UTC Wed Mar 6
2002
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname vpn3640
!
!
ip subnet-zero
ip cef
!
!--- Create an ISAKMP policy for Phase 1 !---
negotiations for the LAN-to-LAN tunnels. crypto isakmp
```

```
policy 10
hash md5
authentication pre-share

!--- Specify the PreShared key for the LAN-to-LAN !---
tunnel. You do not have to add the !--- X-Auth
parameter, as this !--- router does not do Cisco Unity
Client IPsec !--- authentication.

crypto isakmp key cisco123 address 172.18.124.159
!
!

!--- Create the Phase 2 Policy for actual data
encryption. crypto ipsec transform-set myset esp-3des
esp-md5-hmac
!

!--- Create the actual crypto map. Specify !--- the peer
IP address, transform !--- set, and an ACL for this
instance. crypto map mymap 10 ipsec-isakmp
set peer 172.18.124.159
set transform-set myset
match address 100
!
call RSVP-sync
!
!
!

!--- Apply the crypto map on the outside interface.
interface Ethernet0/0
ip address 172.18.124.199 255.255.255.0
half-duplex
crypto map mymap
!
interface Ethernet0/1
ip address 10.10.20.1 255.255.255.0
half-duplex
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.1
ip http server
ip pim bidir-enable
!

!--- Create an ACL for the traffic to !--- be encrypted.
In this example, !--- the traffic from 10.10.20.0/24 to
10.10.10.0/24 !--- is encrypted. access-list 100 permit
ip 10.10.20.0 0.0.0.255 10.10.10.0 0.0.0.255
snmp-server community foobar RO
!
dial-peer cor custom
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
login
!
end
```

配置 VPN 客户端 4.x

请按照下面的步骤配置 Cisco VPN 客户端 4.x。

1. 启动 VPN 客户端，然后单击 **New** 以创建新连接。
2. 输入必要信息，完成后单击 **Save**。
3. 右键单击最近创建的连接条目，然后单击 **Connect** 以连接到路由器。
4. 在 IPSec 协商期间，系统提示输入用户名和口令。
5. 窗口将显示“Negotiating security profiles”和“Your link is now secure”消息。

验证

本部分提供可帮助您确认配置是否正常运行的信息。

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

Cisco VPN 2611

```
vpn2611#show crypto isakmp sa
dst src state conn-id slot
172.18.124.159 172.18.124.199 QM_IDLE 5 0
!--- For the LAN-to-LAN tunnel peer. 172.18.124.159 64.102.55.142 QM_IDLE 6 0
!--- For the Cisco Unity Client tunnel peer. vpn2611#show crypto ipsec sa

interface: Ethernet0/0
Crypto map tag: clientmap, local addr. 172.18.124.159

protected vrf:
local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.10.20.0/255.255.255.0/0/0)
current_peer: 172.18.124.199:500
!--- For the LAN-to-LAN tunnel peer. PERMIT, flags={origin_is_acl,} #pkts encaps: 4, #pkts
encrypt: 4, #pkts digest 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress
failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 172.18.124.159, remote crypto endpt.:
172.18.124.199
path mtu 1500, media mtu 1500
current outbound spi: 892741BC

inbound esp sas:
spi: 0x7B7B2015(2071666709)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2000, flow_id: 1, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4607999/1182)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:
```

```
inbound pcp sas:

outbound ESP sas:
spi: 0x892741BC(2301051324)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2001, flow_id: 2, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4607999/1182)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound PCP sas:

protected vrf:
local ident (addr/mask/prot/port): (172.18.124.159/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (14.1.1.106/255.255.255.255/0/0)
current_peer: 64.102.55.142:500
!--- For the Cisco Unity Client tunnel peer. PERMIT, flags={} #pkts encaps: 0, #pkts encrypt: 0,
#pkts digest 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. Failed: 0, #pkts decompress
failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 172.18.124.159, remote crypto endpt.:
64.102.55.142
path mtu 1500, media mtu 1500
current outbound spi: 81F39EFA

inbound ESP sas:
spi: 0xC4483102(3293065474)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2002, flow_id: 3, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4608000/3484)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound PCP sas:

outbound ESP sas:
spi: 0x81F39EFA(2180226810)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2003, flow_id: 4, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4608000/3484)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound PCP sas:

protected vrf:
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (14.1.1.106/255.255.255.255/0/0)
current_peer: 64.102.55.142:500
!--- For the Cisco Unity Client tunnel peer. PERMIT, flags={} #pkts encaps: 4, #pkts encrypt: 4,
#pkts digest 4
```

#pkts decaps: 20, #pkts decrypt: 20, #pkts verify 20
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. Failed: 0, #pkts decompress
failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 172.18.124.159, remote crypto endpt.:
64.102.55.142
path mtu 1500, media mtu 1500
current outbound spi: B7F84138

inbound ESP sas:
spi: 0x5209917C(1376358780)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2004, flow_id: 5, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4607998/3474)
IV size: 8 bytes
replay detection support: Y
spi: 0xDE6C99C0(3731659200)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2006, flow_id: 7, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4607998/3493)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound PCP sas:

outbound ESP sas:
spi: 0x58886878(1485334648)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2005, flow_id: 6, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4608000/3474)
IV size: 8 bytes
replay detection support: Y
spi: 0xB7F84138(3086500152)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2007, flow_id: 8, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4607999/3486)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound PCP sas:

vpn2611#**show crypto engine connection active**
ID Interface IP-Address State Algorithm Encrypt Decrypt
5 Ethernet0/0 172.18.124.159 set HMAC_MD5+DES_56_CB 0 0
6 Ethernet0/0 172.18.124.159 set HMAC_SHA+3DES_56_C 0 0
2000 Ethernet0/0 172.18.124.159 set HMAC_MD5+3DES_56_C 0 4
2001 Ethernet0/0 172.18.124.159 set HMAC_MD5+3DES_56_C 4 0
2002 Ethernet0/0 172.18.124.159 set HMAC_MD5+3DES_56_C 0 0
2003 Ethernet0/0 172.18.124.159 set HMAC_MD5+3DES_56_C 0 0
2004 Ethernet0/0 172.18.124.159 set HMAC_MD5+3DES_56_C 0 9
2005 Ethernet0/0 172.18.124.159 set HMAC_MD5+3DES_56_C 0 0
2006 Ethernet0/0 172.18.124.159 set HMAC_MD5+3DES_56_C 0 79

```
2007 Ethernet0/0 172.18.124.159 set HMAC_MD5+3DES_56_C 4 0
vpn2611#
```

Cisco VPN 3640

```
vpn3640#show crypto isakmp sa
 DST src state conn-id slot
 172.18.124.159 172.18.124.199 QM_IDLE 4 0
!--- For the LAN-to-LAN tunnel peer. vpn3640#show crypto ipsec sa

 interface: Ethernet0/0
 Crypto map tag: mymap, local addr. 172.18.124.199

protected vrf:
 local ident (addr/mask/prot/port): (10.10.20.0/255.255.255.0/0/0)
 remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
 current_peer: 172.18.124.159:500
 !--- For the LAN-to-LAN tunnel peer. PERMIT, flags={origin_is_acl,} #pkts encaps: 4, #pkts
encrypt: 4, #pkts digest 4
 #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. Failed: 0, #pkts decompress failed: 0
 #send errors 11, #recv errors 0

 local crypto endpt.: 172.18.124.199, remote crypto endpt.: 172.18.124.159
 path mtu 1500, media mtu 1500
 current outbound spi: 7B7B2015

 inbound ESP sas:
 spi: 0x892741BC(2301051324)
 transform: esp-3des esp-md5-hmac ,
 in use settings ={Tunnel, }
 slot: 0, conn id: 940, flow_id: 1, crypto map: mymap
 sa timing: remaining key lifetime (k/sec): (4607998/1237)
 IV size: 8 bytes
 replay detection support: Y

 inbound ah sas:

 inbound PCP sas:

 outbound ESP sas:
 spi: 0x7B7B2015(2071666709)
 transform: esp-3des esp-md5-hmac ,
 in use settings ={Tunnel, }
 slot: 0, conn id: 941, flow_id: 2, crypto map: mymap
 sa timing: remaining key lifetime (k/sec): (4607999/1237)
 IV size: 8 bytes
 replay detection support: Y

 outbound ah sas:

 outbound PCP sas:


 vpn3640# show crypto engine connection active

 ID Interface IP-Address State Algorithm Encrypt Decrypt
 4 <none> <none> set HMAC_MD5+DES_56_CB 0 0
940 Ethernet0/0 172.18.124.199 set HMAC_MD5+3DES_56_C 0 4
 941 Ethernet0/0 172.18.124.199 set HMAC_MD5+3DES_56_C 4 0
```

验证加密映射序列号

如果在同一加密映射中配置了静态和动态对等体，则加密映射条目的顺序非常重要。动态加密映射条目的序列号**必须**高于其他所有静态加密映射条目。如果静态条目编号高于动态条目，则与这些对等体的连接将发生故障。

以下是一个正确编号的加密映射示例，其中包含一个静态条目和一个动态条目。请注意，动态条目具有最高的序列号，并且已留下空间以便添加其他静态条目：

```
crypto dynamic-map dynmap 10
set transform-set myset
crypto map clientmap 1 ipsec-isakmp
set peer 172.18.124.199
set transform-set myset
match address 100
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
```

故障排除

本部分提供帮助对配置进行故障排除的信息。

故障排除命令

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

注意： 在发出 **debug** 命令之前，请参阅有关 debug 命令的重要信息。

- **debug crypto ipsec** — 显示 IPSec 事件。该命令前面加上 no 表示禁止调试输出。
- **debug crypto isakmp** — 显示关于 IKE 事件的消息。该命令前面加上 no 表示禁止调试输出。
- **debug crypto engine** — 显示关于加密引擎的信息，如 Cisco IOS 软件进行加密或解密操作时。

相关信息

- IPsec 协商/IKE 协议支持页
- 技术支持和文档 - Cisco Systems