配置 Cisco PIX 到 Cisco Secure VPN 客户端的通配符、预置共享与模式配置

目录

简介

此配置展示如何通过使用通配符、模式设置和sysopt connection permit-ipsec命令连接VPN客户端到PIX防火墙。Sysopt connection permit-ipsec命令隐性允许来自IPSec隧道的所有数据包。此命令也绕过一个相关的access-list、conduit或者access-group命令报表用于IPSec连接的检查。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本。

- 有思科安全VPN客户端的1.0 Cisco Secure PIX软件版本6.3(3) (显示作为2.0.7在**Help > About**菜单)

或

- 有思科安全VPN客户端的1.1 Cisco Secure PIX软件版本6.3(3) (显示作为2.1.12在**Help > About**菜单)

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您的网络实际，请保证您了解所有命令潜在影响。

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

在此部分，您可以看到本文所描述功能的配置信息。

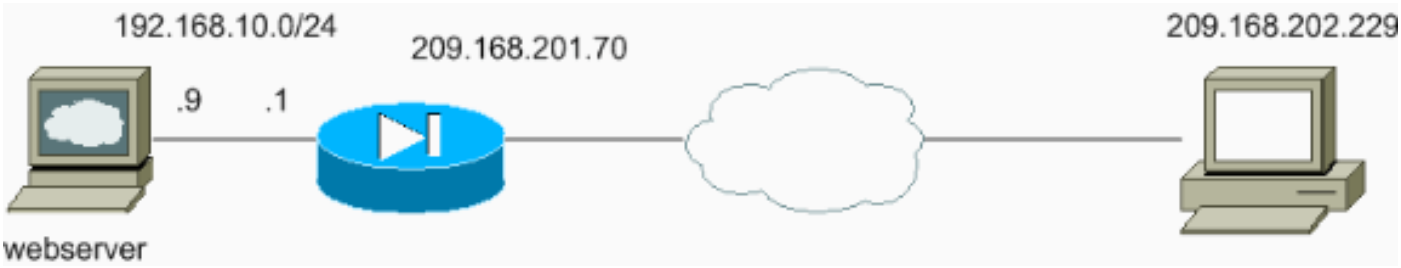
有VPN客户端的一个用户连接并且收到从互联网服务提供商的一个IP地址。这由从模式配置库的一个IP地址替换PIX的(172.16.1.1 - 172.16.1.255)。用户访问一切在防火墙的里面，包括网络。不运行VPN客户端的用户能连接到Web服务器在静态分配提供的地址帮助下。当用户连接到互联网时，内部的用户数据流不通过IPSec隧道。

注意： 加密技术目的是出口控制。是您的责任知道关于加密技术出口的法律。如果有关于出口控制的任何问题，请发送电子邮件对export@cisco.com。

注意： 为了找到关于用于本文的命令的其他信息，参考命令查找工具(仅限注册用户)。

网络图

本文档使用此网络设置。



配置

本文档使用以下配置。

- PIX 配置
- VPN 客户端配置

PIX 配置

```
sv2-5(config)#show run
: Saved
:
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname sv2-5
fixup protocol dns maximum-length 512
```

```
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
!--- Access-list defined for nat 0. access-list 101
permit ip 192.168.10.0 255.255.255.0 172.16.1.0
255.255.255.0
!--- Access-list applied on the outside interface.
access-list 102 permit tcp any host 209.168.201.9 eq www
access-list 102 permit icmp any any
pager lines 24
logging on
logging buffered debugging
mtu outside 1500
mtu inside 1500
ip address outside 209.168.201.70 255.255.255.0
ip address inside 192.168.10.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
!--- Set up the mode-config pool. ip local pool test
172.16.1.1-172.16.1.255
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
pdm history enable
arp timeout 14400
global (outside) 1 interface
!--- Do not do Network Address Translation (NAT) for the
VPN Client pool. nat (inside) 0 access-list 101
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
!--- Also allow *unencrypted* communication if desired.
static (inside,outside) 209.168.201.9 192.168.10.9
netmask 255.255.255.255 0 0
access-group 102 in interface outside
route outside 0.0.0.0 0.0.0.0 209.168.201.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
!--- These are IPSec parameters. crypto ipsec transform-
set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
```

```
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap client configuration address initiate
crypto map mymap client configuration address respond
crypto map mymap interface outside
!--- These are IKE parameters. isakmp enable outside
isakmp key ******** address 0.0.0.0 netmask 0.0.0.0
isakmp identity address
isakmp client configuration address-pool local test
outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
vpdn username cisco password ********* store-local
terminal width 80
Cryptochecksum:4f21dc73759ffae29935430132e662ef
: end
```

VPN 客户端配置

```
sv2-5(config)#show run
: Saved
:
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname sv2-5
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
!--- Access-list defined for nat 0. access-list 101
permit ip 192.168.10.0 255.255.255.0 172.16.1.0
255.255.255.0
!--- Access-list applied on the outside interface.
access-list 102 permit tcp any host 209.168.201.9 eq www
access-list 102 permit icmp any any
pager lines 24
logging on
logging buffered debugging
mtu outside 1500
mtu inside 1500
ip address outside 209.168.201.70 255.255.255.0
ip address inside 192.168.10.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
!--- Set up the mode-config pool. ip local pool test
```

```
172.16.1.1-172.16.1.255
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
pdm history enable
arp timeout 14400
global (outside) 1 interface
!--- Do not do Network Address Translation (NAT) for the
VPN Client pool. nat (inside) 0 access-list 101
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
!--- Also allow *unencrypted* communication if desired.
static (inside,outside) 209.168.201.9 192.168.10.9
netmask 255.255.255.255 0 0
access-group 102 in interface outside
route outside 0.0.0.0 0.0.0.0 209.168.201.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
!--- These are IPSec parameters. crypto ipsec transform-
set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap client configuration address initiate
crypto map mymap client configuration address respond
crypto map mymap interface outside
!--- These are IKE parameters. isakmp enable outside
isakmp key ******** address 0.0.0.0 netmask 0.0.0.0
isakmp identity address
isakmp client configuration address-pool local test
outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
vpdn username cisco password ********* store-local
terminal width 80
Cryptochecksum:4f21dc73759ffae29935430132e662ef
: end
```

验证

当前没有可用于此配置的验证过程。

故障排除

本部分提供的信息可用于对配置进行故障排除。

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。

为了看到VPN客户端一侧调试，请启用Cisco安全日志浏览器。

- **debug crypto ipsec sa** - 显示第 2 阶段的 IPSec 协商。
- **debug crypto isakmp**—显示第 1 阶段的 Internet 安全连接和密钥管理协议 (ISAKMP) 协商。

请参阅此**debug输出**：

```
crypto_isakmp_process_block:src:209.168.202.229,
dest:209.168.201.70 spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP: encryption DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 1
ISAKMP: auth pre-share
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): SA is doing pre-shared key authentication
using id type ID_IPV4_ADDR
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:209.168.202.229,
dest:209.168.201.70 spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE payload. message ID = 0

ISAKMP (0): processing vendor id payload

ISAKMP (0): processing vendor id payload

ISAKMP (0): received xauth v6 vendor id

return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:209.168.202.229,
dest:209.168.201.70 spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): processing NOTIFY payload 24578 protocol 1
spi 0, message ID = 0
ISAKMP (0): processing notify INITIAL_CONTACTIPSEC(key_engine):
got a queue event...
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with 209.168.202.229

ISAKMP (0): SA has been authenticated
```

!--- Phase 1 is complete. ISAKMP (0): ID payload next-payload : 8 type : 1 protocol : 17 port : 500 length : 8 ISAKMP (0): Total payload length: 12 return status is IKMP_NO_ERROR ISAKMP (0): sending phase 1 RESPONDER_LIFETIME notify ISAKMP (0): sending NOTIFY message 24576 protocol 1 VPN Peer: ISAKMP: Added new peer: ip:209.168.202.229/500 Total VPN Peers:1 VPN Peer: ISAKMP: Peer ip:209.168.202.229/500 Ref cnt incremented to:1 Total VPN Peers:1 crypto_isakmp_process_block:src:209.168.202.229, dest:209.168.201.70 spt:500 dpt:500 OAK_QM exchange **ISAKMP (0:0): Need config/address**
!--- Mode configuration. ISAKMP (0:0): initiating peer config to 209.168.202.229. ID = 2521514930 (0x964b43b2) return status is IKMP_NO_ERROR crypto_isakmp_process_block:src:209.168.202.229, dest:209.168.201.70 spt:500 dpt:500 ISAKMP_TRANSACTION exchange ISAKMP (0:0): processing transaction payload from 209.168.202.229. message ID = 16133588 ISAKMP: Config payload CFG_ACK ISAKMP (0:0): peer accepted the address! return status is IKMP_NO_ERROR crypto_isakmp_process_block:src:209.168.202.229, dest:209.168.201.70 spt:500 dpt:500 OAK_QM exchange oakley_process_quick_mode: OAK_QM_IDLE ISAKMP (0): processing SA payload. message ID = 1524017329 ISAKMP : Checking IPSec proposal 1 ISAKMP: transform 1, ESP_DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5 ISAKMP: encaps is 1 *!--- Phase 2 starts.* **ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request):**
proposal part #1,
(key eng. msg.) dest= 209.168.201.70, src= 209.168.202.229,
dest_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
src_proxy= 172.16.1.1/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

ISAKMP (0): processing NONCE payload. message ID = 1524017329

ISAKMP (0): processing ID payload. message ID = 1524017329
ISAKMP (0): ID_IPV4_ADDR src 172.16.1.1 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 1524017329
ISAKMP (0): ID_IPV4_ADDR_SUBNET dst 192.168.10.0/255.255.255.0 prot 0 port 0IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0x9f068383(2668004227) for SA
from 209.168.202.229 to 209.168.201.70 for prot 3

return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:209.168.202.229,
dest:209.168.201.70 spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
!--- Phase 2 complete IPSec SAs are created. **ISAKMP (0): Creating IPSec SAs**
inbound SA from 209.168.202.229 to 209.168.201.70
(proxy 172.16.1.1 to 192.168.10.0)
has spi 2668004227 and conn_id 2 and flags 4
outbound SA from 209.168.201.70 to 209.168.202.229
(proxy 192.168.10.0 to 172.16.1.1)
has spi 3326135849 and conn_id 1 and flags 4IPSEC
(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) dest= 209.168.201.70, src= 209.168.202.229,
dest_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
src_proxy= 172.16.1.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x9f068383(2668004227), conn_id= 2, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 209.168.201.70, dest= 209.168.202.229,
src_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
dest_proxy= 172.16.1.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0xc640ce29(3326135849), conn_id= 1, keysize= 0, flags= 0x4

```
VPN Peer: IPSEC: Peer ip:209.168.202.229/500 Ref cnt
incremented to:2 Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:209.168.202.229/500 Ref cnt
incremented to:3 Total VPN Peers:1
return status is IKMP_NO_ERROR
sv2-5#
```

相关信息

- IPSec 支持页面
- IPSec 简介
- 建立通过 Cisco PIX 防火墙的连接
- PIX 命令参考
- PIX 支持页
- 请求注解 (RFC)
- 技术支持 - Cisco Systems