单臂路由器上用于公共 Internet 的 PIX/ASA 和 VPN 客户端配置示例

目录

简介

本文档介绍了如何设置 ASA 安全设备 7.2 及更高版本以执行单臂 IPsec。此设置适用于 ASA 不允许分割隧道并且用户必须先直接连接到 ASA 然后才被允许访问 Internet 的特定案例。

注意： 在 PIX/ASA 版本 7.2 及更高版本中，intra-interface 关键字允许所有数据流（而不仅是 IPSec 数据流）进入和退出同一接口。

请参阅公用 Internet 的单臂路由器和 VPN 客户端配置示例以在中心站点路由器上完成相似配置。

请参阅 PIX/ASA 7.x 的使用 TACACS+ 身份验证增强的分支到客户端 VPN 配置示例以了解有关中心 PIX 将数据流从 VPN 客户端重定向到分支 PIX 的方案的详细信息。

注意： 为了避免网络中的 IP 地址重叠，请为 VPN 客户端分配一个完全不同的 IP 地址池（例如 10.x.x.x、172.16.x.x 和 192.168.x.x）。此 IP 编址方案有助于排除网络故障。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 中心 PIX/ASA 安全设备需要运行版本 7.2 或更高版本
- Cisco VPN 客户端版本 5.x

使用的组件

本文档中的信息基于 PIX 或 ASA 安全设备版本 8.0.2 和 Cisco VPN 客户端版本 5.0。

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。

相关产品

此配置也可用于 Cisco PIX 安全设备版本 7.2 及更高版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

发夹或 U 字型转向

对于进入某接口然后又从同一接口路由出去的 VPN 流量，此功能非常有用。例如，如果有星型 VPN 网络，其中安全设备是中心，而远程 VPN 网络是分支，那么，为使分支之间可以彼此通信，数据流必须进入安全设备，然后再流向其他分支。

请使用 **same-security-traffic** 命令以允许数据流进入和退出同一接口。

```
securityappliance(config)#same-security-traffic permit intra-interface
```

注意： 发夹或 U 字型转向也适用于 VPN 客户端到 VPN 客户端的通信。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：

PIX/ASA 的 CLI 配置

- PIX/ASA

在 PIX/ASA 上运行配置

```
PIX Version 8.0(2)
names
!
interface Ethernet0
nameif outside
security-level 0
ip address 172.18.124.98 255.255.255.0
!
interface Ethernet1
nameif inside
security-level 100
ip address 172.16.3.101 255.255.255.0
!
interface Ethernet2
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet3
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet4
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet5
shutdown
no nameif
no security-level
no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
ftp mode passive
!--- Command that permits IPsec traffic to enter and
exit the same interface. same-security-traffic permit
intra-interface access-list 100 extended permit icmp any
any echo-reply pager lines 24 logging enable logging
buffered debugging mtu outside 1500 mtu inside 1500 ip
local pool vpnpool 192.168.10.1-192.168.10.254 mask
255.255.255.0 no failover monitor-interface outside
monitor-interface inside icmp permit any outside no asdm
history enable arp timeout 14400 nat-control !--- The
address pool for the VPN Clients. !--- The global
address for Internet access used by VPN Clients. !---
Note: Uses an RFC 1918 range for lab setup. !--- Apply
an address from your public range provided by your ISP.
global (outside) 1 172.18.124.166 !--- The NAT statement
to define what to encrypt (the addresses from the vpn-
pool). nat (outside) 1 192.168.10.0 255.255.255.0 nat
(inside) 1 0.0.0.0 0.0.0.0 static (inside,outside)
172.16.3.102 172.16.3.102 netmask 255.255.255.255
access-group 100 in interface outside route outside
0.0.0.0 0.0.0.0 172.18.124.98 1 timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225
1:00:00 mgcp 0:05:00 timeout mgcp-pat 0:05:00 sip
```

```
0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute
!--- The configuration of group-policy for VPN Clients.
group-policy clientgroup internal group-policy
clientgroup attributes vpn-idle-timeout 20 !--- Forces
VPN Clients over the tunnel for Internet access. split-
tunnel-policy tunnelall no snmp-server location no snmp-
server contact snmp-server enable traps snmp !---
Configuration of IPsec Phase 2. crypto ipsec transform-
set myset esp-3des esp-sha-hmac !--- Crypto map
configuration for VPN Clients that connect to this PIX.
crypto dynamic-map rtpdynmap 20 set transform-set myset
!--- Binds the dynamic map to the crypto map process.
crypto map mymap 20 ipsec-isakmp dynamic rtpdynmap !---
Crypto map applied to the outside interface. crypto map
mymap interface outside !--- Enable ISAKMP on the
outside interface. isakmp identity address isakmp enable
outside !--- Configuration of ISAKMP policy. isakmp
policy 10 authentication pre-share isakmp policy 10
encryption 3des isakmp policy 10 hash sha isakmp policy
10 group 2 isakmp policy 10 lifetime 86400 isakmp policy
65535 authentication pre-share isakmp policy 65535
encryption 3des isakmp policy 65535 hash sha isakmp
policy 65535 group 2 isakmp policy 65535 lifetime 86400
telnet timeout 5 ssh timeout 5 console timeout 0 !---
Configuration of tunnel-group with group information for
VPN Clients. tunnel-group rtptacvpn type ipsec-ra !---
Configuration of group parameters for the VPN Clients.
tunnel-group rtptacvpn general-attributes address-pool
vpnpool !--- Disable user authentication.
authentication-server-group none !--- Bind group-policy
parameters to the tunnel-group for VPN Clients. default-
group-policy clientgroup tunnel-group rtptacvpn ipsec-
attributes pre-shared-key * ! class-map
inspection_default match default-inspection-traffic ! !
policy-map global_policy class inspection_default
inspect dns maximum-length 512 inspect ftp inspect h323
h225 inspect h323 ras inspect netbios inspect rsh
inspect rtsp inspect skinny inspect esmtp inspect sqlnet
inspect sunrpc inspect tftp inspect sip inspect xdmcp !
service-policy global_policy global
Cryptochecksum:1a1ad58226e700404e1053159f0c5fb0 : end
```

使用 ASDM 配置 ASA/PIX

要使用 ASDM 将 Cisco ASA 配置为远程 VPN Server，请完成以下步骤：

1. 从主窗口中选择 **Wizards > IPsec VPN Wizard**。
2. 选择 **Remote Access VPN** 隧道类型，并确保按照要求设置 VPN 隧道接口。
3. 已选择了唯一的可用 VPN 客户端类型。单击 **Next**。
4. 为“Tunnel Group Name”输入名称。提供要使用的身份验证信息。本示例中选择了 **Pre-shared Key**。**注意：** ASDM 上没有用来隐藏/加密预共享密钥的方法。原因是 ASDM 必须只由配置 ASA 的人员或帮助客户进行此配置的人员使用。
5. 选择是希望使用本地用户数据库对远程用户进行身份验证，还是希望使用外部 AAA 服务器组对远程用户进行身份验证。**注意：** 您将在步骤 6 中将用户添加到本地用户数据库中。**注意：** 有关如何通过 ASDM 配置外部 AAA 服务器组的信息，请参阅 PIX/ASA 7.x 的通过 ASDM 为 VPN 用户配置身份验证和授权服务器组的配置示例。
6. 如果需要，请将用户添加到本地数据库中。**注意：** 请不要从此窗口中删除当前用户。在 ASDM 主窗口中选择 **Configuration > Device Administration > Administration > User**

Accounts，以编辑数据库中的现存条目或将这些条目从数据库中删除。

7. 定义一个要在远程 VPN 客户端进行连接时动态分配给它们的本地地址池。
8. ***可选：***指定 DNS 和 WINS 服务器信息以及将被推送到远程 VPN 客户端的默认域名。
9. 为 IKE 指定参数，也称为 IKE 第 1 阶段。隧道两端的配置必须完全一致，但 Cisco VPN 客户端会自动为自己选择正确的配置。无需在客户端 PC 上执行 IKE 配置。
10. 为 IPSec 指定参数，也称为 IKE 第 2 阶段。隧道两端的配置必须完全一致，但 Cisco VPN 客户端会自动为自己选择正确的配置。无需在客户端 PC 上执行 IKE 配置。
11. 指定哪些内部主机或网络（如果有）可向远程 VPN 用户公开。如果将此列表留空，则将允许远程 VPN 用户访问 ASA 的整个内部网络。您还可以在此窗口上启用分割隧道。分割隧道对发往本过程中前面所定义的资源的数据流进行加密，并通过不以隧道形式传输该数据流提供对整个 Internet 的未加密访问。如果未启用分割隧道，则来自远程 VPN 用户的所有数据流将通过隧道传输到 ASA。这可能导致很高的带宽和处理器使用率，具体取决于您的配置。
12. 此窗口显示您已执行操作的汇总。如果对配置感到满意，请单击 **Finish**。
13. 单击图中所示的复选框时，将配置命令 **same-security-traffic** 以允许连接到同一接口的两个或更多主机之间传输数据流：
14. 选择 **Configuration > Firewall >NAT Rules**，并单击“Add Dynamic NAT Rule”以使用 ASDM 创建此动态转换。
15. 选择 **Inside** 作为源接口，然后输入要进行 NAT 转换的地址。对于“Translate Address on Interface”，选择 **outside** 并单击“OK”。
16. 选择 **outside** 作为源接口，然后输入要进行 NAT 转换的地址。对于“Translate Address on Interface”，选择 **outside** 并单击“OK”。
17. 当您选择 **Configuration > Firewall >NAT Rules** 时，转换将显示在“Translation Rules”中。

注释 1：需要配置 sysopt connection permit-vpn 命令。show running-config sysopt 命令验证是否配置了该命令。

注释 2：为可选 UDP 传输添加以下输出：

```
group-policy clientgroup attributes vpn-idle-timeout 20 ipsec-udp enable ipsec-udp-port 10000
split-tunnel-policy tunnelspecified split-tunnel-network-list value splittunnel
```

注释 3：在 PIX 设备的全局配置中配置此命令以通过 IPSec over TCP 连接 VPN 客户端：

```
isakmp ipsec-over-tcp port 10000
```

注意： 参考在思科ASA视频的 发夹关于可以使用两隧道间的本地交换的不同的方案的更多信息。

VPN 客户端配置

完成以下步骤以配置 VPN 客户端：

1. 选择 **New**。
2. 输入 PIX 外部接口 IP 地址以及用于身份验证的隧道组名和口令。
3. （*可选*）单击“Transport”选项卡下的 **Enable Transparent Tunneling**。（这是可选的，并且需要注释 2 中提到的附加 PIX/ASA 配置。）
4. 保存配置文件。

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

- show crypto isakmp sa - 显示对等体上的所有当前 IKE 安全关联 (SA)。
- show crypto ipsec sa — 显示所有当前 SA。查找 SA 上定义 VPN 客户端数据流的加密和解密数据包。

尝试从客户端 ping 或浏览公用 IP 地址（例如 www.cisco.com）。

注意： 除非在全局配置模式下配置 management-access 命令，否则不能 ping PIX 的内部接口以形成隧道。

```
PIX1(config)#management-access inside PIX1(config)# show management-access management-access
inside
```

VPN 客户端验证

完成以下步骤以验证 VPN 客户端。

1. 连接成功后，右键单击系统任务栏中的 VPN 客户端锁图标，并选择**统计信息**选项以查看加密和解密。
2. 单击“Route Details”选项卡以验证是否未从设备向下传送分割隧道列表。

故障排除

注意： 有关如何排除 VPN 问题的详细信息，请参阅 VPN 故障排除解决方案。

相关信息

- PIX 安全设备版本 7.0 的增强的分支到客户端 VPN 配置示例
- Cisco VPN 客户端
- IPsec 协商/IKE 协议
- Cisco PIX 防火墙软件
- Cisco Secure PIX 防火墙命令参考
- 安全产品 Field Notices（包括 PIX）
- 在思科ASA的发夹
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems