路由器允许 VPN Client 使用分割隧道连接 IPsec 和 Internet 的配置示例

目录

简介

本文档提供有关如何允许 VPN 客户端在通过隧道连接到 Cisco IOS® 路由器时访问 Internet 的分步说明。要允许 VPN 客户端通过 IPsec 安全访问公司资源并且同时允许对 Internet 进行非安全访问，需要进行此配置。此配置称为分割隧道。

注意： 配置分割隧道后可能会带来安全风险。由于 VPN 客户端可以对 Internet 进行非安全访问，因此它们可能被攻击者攻陷。然后该攻击者可以通过 IPsec 隧道访问公司 LAN。可以在完全隧道和分割隧道之间进行折衷，以允许 VPN 客户端仅访问本地 LAN。请参阅 PIX/ASA 7.x：允许 VPN 客户端访问本地 LAN 的配置示例。

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：

- 安装有 Cisco IOS 软件版本 12.4 的 Cisco 路由器 3640

- Cisco VPN Client 4.8

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。

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

远程访问 VPN 满足了移动工作者的安全连接组织网络的需要。移动用户可以使用安装在其 PC 机上的 VPN 客户端软件来建立安全连接。VPN 客户端将会向已配置为接受这些请求的中心站点设备发起连接。在本示例中，中心站点设备是使用动态加密映射的 Cisco IOS 路由器。

当您对 VPN 连接启用分割隧道时，需要在路由器上配置一个访问控制列表 (ACL)。在本示例中，**access-list 101** 命令与用于分割隧道的组关联，并且该隧道通向 10.10.10.x/24 网络。流向设备的未加密数据流（例如，Internet）将从 ACL 101 中配置的网络中排除。

```
access-list 101 permit ip 10.10.10.0 0.0.0.255 192.168.1.0 0.0.0.255
```

针对组属性应用 ACL。

```
crypto isakmp client configuration group vpngroup
 key cisco123
 dns 10.10.10.10
 wins 10.10.10.20
 domain cisco.com
 pool ippool
 acl 101
```

本配置示例针对 IPsec 隧道配置了以下要素：

- 应用到 PIX 上的外部接口的加密映射
- 根据本地身份验证对 VPN 客户端进行的扩展身份验证 (Xauth)
- 从地址池中为 VPN 客户端动态分配专用 IP 地址
- **nat 0 access-list** 命令功能，此功能允许 LAN 上的主机使用远程用户的专用 IP 地址，同时仍可从 PIX 处获得网络地址转换 (NAT) 地址，以访问不受信任的网络。

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：

注意： 此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

配置

本文档使用以下配置：

- 路由器
- Cisco VPN 客户端

路由器

```
VPN#show run Building configuration... Current
configuration : 2170 bytes ! version 12.4 service
timestamps debug datetime msec service timestamps log
datetime msec no service password-encryption ! hostname
VPN ! boot-start-marker boot-end-marker ! ! !--- Enable
authentication, authorization and accounting (AAA) !---
for user authentication and group authorization. aaa
new-model ! !--- In order to enable Xauth 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 ! resource
policy ! ! !--- For local authentication of the IPsec
user, !--- create the user with a password. username
user password 0 cisco ! ! !--- Create an Internet
Security Association and !--- Key Management Protocol
(ISAKMP) policy for Phase 1 negotiations. crypto isakmp
policy 3 encr 3des authentication pre-share group 2 !---
Create a group that is used to specify the !--- WINS and
DNS server addresses to the VPN Client, !--- along with
the pre-shared key for authentication. Use ACL 101 used
for !--- the Split tunneling in the VPN Clinet end.
crypto isakmp client configuration group vpnclient key
cisco123 dns 10.10.10.10 wins 10.10.10.20 domain
cisco.com pool ippool acl 101 ! !--- 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 reverse-route ! !--- Create the
actual crypto map, !--- and apply the AAA lists that
were created earlier. crypto map clientmap client
authentication list userauthen crypto map clientmap
isakmp authorization list groupauthor crypto map
clientmap client configuration address respond crypto
map clientmap 10 ipsec-isakmp dynamic dynmap ! ! ! !
interface Ethernet0/0 ip address 10.10.10.1
255.255.255.0 half-duplex ip nat inside !--- Apply the
crypto map on the outbound interface. interface
FastEthernet1/0 ip address 172.16.1.1 255.255.255.0 ip
nat outside ip virtual-reassembly duplex auto speed auto
crypto map clientmap ! interface Serial2/0 no ip address
! interface Serial2/1 no ip address shutdown ! interface
Serial2/2 no ip address shutdown ! interface Serial2/3
no ip address shutdown !--- Create a pool of addresses
to be !--- assigned to the VPN Clients. ! ip local pool
ippool 192.168.1.1 192.168.1.2 ip http server no ip http
secure-server ! ip route 0.0.0.0 0.0.0.0 172.16.1.2 !---
Enables Network Address Translation (NAT) !--- of the
inside source address that matches access list 111 !---
and gets PATed with the FastEthernet IP address. ip nat
inside source list 111 interface FastEthernet1/0
```

```
overload ! !--- The access list is used to specify which
traffic !--- is to be translated for the outside
Internet. access-list 111 deny ip 10.10.10.0 0.0.0.255
192.168.1.0 0.0.0.255 access-list 111 permit ip any any
!--- Configure the interesting traffic to be encrypted
from the VPN Client !--- to the central site router
(access list 101). !--- Apply this ACL in the ISAKMP
configuration. access-list 101 permit ip 10.10.10.0
0.0.0.255 192.168.1.0 0.0.0.255 control-plane ! line con
0 line aux 0 line vty 0 4 ! end
```

VPN 客户端 4.8 配置

执行以下步骤以配置 VPN Client 4.8：

1. 选择**开始 > 程序 > Cisco Systems VPN 客户端 > VPN 客户端**。
2. 单击 **New** 以启动 Create New VPN Connection Entry 窗口。
3. 输入 Connection Entry 的名称与说明，在 Host 框中输入路由器的外部 IP 地址，并输入 VPN Group 的名称和口令。单击 **Save**。
4. 单击要使用的连接，然后从 VPN 客户端主窗口中单击 **Connect**。
5. 出现提示时，输入 Xauth 的用户名和口令信息，然后单击 **OK** 以连接远程网络。
6. VPN客户端与中心站点的路由器连接。
7. 选择 **Status > Statistics** 以检查 VPN Client 的隧道统计数据。
8. 转至 Route Details 选项卡，以查看 VPN 客户端安全连接到路由器的路由。在本示例中，VPN 客户端可以安全访问 10.10.10.0/24，而所有其他数据流不会被加密，也不会通过隧道发送。受保护的网络从在中心站点路由器中配置的 ACL 101 下载。

验证

本部分提供的信息可帮助您确认您的配置是否可正常运行。

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)。`VPN#show crypto ipsec sa interface: FastEthernet1/0 Crypto map tag: clientmap, local addr 172.16.1.1 protected vrf: (none) local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0) current_peer 10.0.0.2 port 500 PERMIT, flags={} #pkts encaps: 270, #pkts encrypt: 270, #pkts digest: 270 #pkts decaps: 270, #pkts decrypt: 270, #pkts verify: 270 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors 0 local crypto endpt.: 172.16.1.1, remote crypto endpt.: 10.0.0.2 path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet1/0 current outbound spi: 0xEF7C20EA(4017889514) inbound esp sas: spi: 0x17E0CBEC(400608236) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } conn id: 2001, flow_id: SW:1, crypto map: clientmap sa timing: remaining key lifetime (k/sec): (4530341/3288) IV size: 8 bytes replay detection support: Y Status: ACTIVE inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0xEF7C20EA(4017889514) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } conn id: 2002, flow_id: SW:2, crypto map: clientmap sa timing: remaining key lifetime (k/sec): (4530354/3287) IV size: 8 bytes replay detection support: Y Status: ACTIVE outbound ah sas: outbound pcp sas:`
- **show crypto ipsec sa** — 显示当前 SA 使用的设置。`VPN#show crypto isakmp sa dst src state conn-id slot status 172.16.1.1 10.0.0.2 QM_IDLE 15 0 ACTIVE`

故障排除

故障排除命令

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。

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

- **debug crypto ipsec** - 显示第 2 阶段的 IPsec 协商。
- **debug crypto isakmp** - 显示第 1 阶段的 ISAKMP 协商。

相关信息

- IPsec 协商/IKE 协议
- Cisco VPN 客户端 - 产品支持
- Cisco 路由器 - 产品支持
- 技术支持和文档 - Cisco Systems