

使用NAT超载和Cisco Secure VPN Client配置IPSec路由器到路由器

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[故障排除](#)

[故障排除命令](#)

[相关信息](#)

简介

此实例配置加密从Light后的网络到House后网络(192.168.100.x 到 192.168.200.x 网络)的流量。网络地址转换 (NAT) 超载也已完成。加密的VPN客户端连接被允许进入Light，与通配符、预先共享密钥和模式设置。发送到 Internet 的流量已转换，但未加密。

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：

- Cisco IOS软件版本12.2.7和12.2.8T
- 思科安全VPN客户端1.1 (显示作为2.1.12在IRE客户端帮助> **About**菜单)
- Cisco 3600 路由器**注意**：如果使用Cisco 2600系列路由器这种VPN方案，则路由器必须安装与crypto IPSec VPN IOS镜像。

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](#)。

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：有关本文档所用命令的详细信息，请使用[命令查找工具](#)（[仅限注册用户](#)）。

网络图

本文档使用以下网络设置：

配置

本文档使用以下配置。

- [Light 配置](#)
- [House 配置](#)
- [VPN 客户端配置](#)

Light 配置

```
Current configuration : 2047 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Light ! boot system flash:c3660-ik9o3s-mz.122-
8T ! ip subnet-zero ! ip audit notify log ip audit po
max-events 100 ip ssh time-out 120 ip ssh
authentication-retries 3 ! !--- IPsec Internet Security
Association and !--- Key Management Protocol (ISAKMP)
policy. crypto isakmp policy 5 hash md5 authentication
pre-share !--- ISAKMP key for static LAN-to-LAN tunnel
!--- without extended authenticaton (xauth). crypto
isakmp key cisco123 address 10.64.10.45 no-xauth !---
ISAKMP key for the dynamic VPN Client. crypto isakmp key
123cisco address 0.0.0.0 0.0.0.0 !--- Assign the IP
address to the VPN Client. crypto isakmp client
configuration address-pool local test-pool ! ! ! crypto
ipsec transform-set testset esp-des esp-md5-hmac !
crypto dynamic-map test-dynamic 10 set transform-set
testset ! ! !--- VPN Client mode configuration
negotiation, !--- such as IP address assignment and
xauth. crypto map test client configuration address
initiate crypto map test client configuration address
respond !--- Static crypto map for the LAN-to-LAN
tunnel. crypto map test 5 ipsec-isakmp set peer
10.64.10.45 set transform-set testset !--- Include the
private network-to-private network traffic !--- in the
encryption process. match address 115 !--- Dynamic
crypto map for the VPN Client. crypto map test 10 ipsec-
```

```

isakmp dynamic test-dynamic ! call rsvp-sync ! ! ! ! !
fax interface-type modem mta receive maximum-recipients
0 ! controller E1 2/0 ! ! ! interface FastEthernet0/0 ip
address 10.64.10.44 255.255.255.224 ip nat outside
duplex auto speed auto crypto map test ! interface
FastEthernet0/1 ip address 192.168.100.1 255.255.255.0
ip nat inside duplex auto speed auto ! interface BRI4/0
no ip address shutdown ! interface BRI4/1 no ip address
shutdown ! interface BRI4/2 no ip address shutdown !
interface BRI4/3 no ip address shutdown ! !--- Define
the IP address pool for the VPN Client. ip local pool
test-pool 192.168.1.1 192.168.1.254 !--- Exclude the
private network and VPN Client !--- traffic from the NAT
process. ip nat inside source route-map nonat interface
FastEthernet0/0 overload ip classless ip route 0.0.0.0
0.0.0.0 10.64.10.33 ip http server ip pim bidir-enable !
!--- Exclude the private network and VPN Client !---
traffic from the NAT process. access-list 110 deny ip
192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255 access-
list 110 deny ip 192.168.100.0 0.0.0.255 192.168.1.0
0.0.0.255 access-list 110 permit ip 192.168.100.0
0.0.0.255 any !--- Include the private network-to-
private network traffic !--- in the encryption process.
access-list 115 permit ip 192.168.100.0 0.0.0.255
192.168.200.0 0.0.0.255 ! !--- Exclude the private
network and VPN Client !--- traffic from the NAT
process. route-map nonat permit 10 match ip address 110
! ! dial-peer cor custom ! ! ! ! ! line con 0 line 97
108 line aux 0 line vty 0 4 ! end

```

House 配置

```

Current configuration : 1689 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname house ! boot system flash:c3660-jk8o3s-mz.122-
7.bin ! ip subnet-zero ! ! no ip domain-lookup ! ip
audit notify log ip audit po max-events 100 ip ssh time-
out 120 ip ssh authentication-retries 3 ! !--- IPsec
ISAKMP policy. crypto isakmp policy 5 hash md5
authentication pre-share !--- ISAKMP key for static LAN-
to-LAN tunnel without xauth authenticaton. crypto isakmp
key cisco123 address 10.64.10.44 no-xauth ! ! crypto
ipsec transform-set testset esp-des esp-md5-hmac ! !---
Static crypto map for the LAN-to-LAN tunnel. crypto map
test 5 ipsec-isakmp set peer 10.64.10.44 set transform-
set testset !--- Include the private network-to-private
network traffic !--- in the encryption process. match
address 115 ! call rsvp-sync cns event-service server !
! ! ! ! fax interface-type modem mta receive maximum-
recipients 0 ! ! ! interface FastEthernet0/0 ip address
10.64.10.45 255.255.255.224 ip nat outside duplex auto
speed auto crypto map test ! interface FastEthernet0/1
ip address 192.168.200.1 255.255.255.0 ip nat inside
duplex auto speed auto ! interface BRI2/0 no ip address
shutdown ! interface BRI2/1 no ip address shutdown !
interface BRI2/2 no ip address shutdown ! interface
BRI2/3 no ip address shutdown ! interface
FastEthernet4/0 no ip address shutdown duplex auto speed
auto ! !--- Exclude the private network traffic !---
from the dynamic (dynamic association to a pool) NAT

```

```
process. ip nat inside source route-map nonat interface
FastEthernet0/0 overload ip classless ip route 0.0.0.0
0.0.0.0 10.64.10.33 no ip http server ip pim bidir-
enable ! !--- Exclude the private network traffic from
the NAT process. access-list 110 deny ip 192.168.200.0
0.0.0.255 192.168.100.0 0.0.0.255 access-list 110 permit
ip 192.168.200.0 0.0.0.255 any !--- Include the private
network-to-private network traffic !--- in the
encryption process. access-list 115 permit ip
192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255 !---
Exclude the private network traffic from the NAT
process. route-map nonat permit 10 match ip address 110
!!! dial-peer cor custom ! ! ! ! ! line con 0 line aux
0 line vty 0 4 login ! end
```

VPN 客户端配置

Network Security policy:

```
1- TOLIGHT
My Identity
Connection security: Secure
Remote Party Identity and addressing
ID Type: IP subnet
192.168.100.0
255.255.255.0
Port all Protocol all
```

Connect using secure tunnel

```
ID Type: IP address
10.64.10.44
```

Pre-shared Key=123cisco

Authentication (Phase 1)

```
Proposal 1
Authentication method: pre-shared key
Encrypt Alg: DES
Hash Alg: MD5
SA life: Unspecified
Key Group: DH 1
```

Key exchange (Phase 2)

```
Proposal 1
Encapsulation ESP
Encrypt Alg: DES
Hash Alg: MD5
Encap: tunnel
SA life: Unspecified
no AH
```

2- Other Connections

```
Connection security: Non-secure
Local Network Interface
Name: Any
IP Addr: Any
Port: All
```

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 ipsec sa** —显示第2阶段安全关联(SA)。
- [show crypto isakmp sa](#) - 显示第 1 阶段 SA。

故障排除

使用本部分可排除配置故障。

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。
- **debug crypto engine** - 显示已加密的数据流。
- [clear crypto isakmp](#) - 清除与第 1 阶段相关的 SA。
- [clear crypto sa](#) - 清除与第 2 阶段相关的 SA。

相关信息

- [配置 IPsec 网络安全](#)
- [配置 Internet 密钥交换安全协议](#)
- [IPsec 协商/IKE 协议支持页](#)
- [思科安全VPN客户端支持页面](#)
- [技术支持 - Cisco Systems](#)