# NAT オーバーロードと Cisco Secure VPN Client を使用する IPSec Router-to-Router の設定

## 目次



## 概要

この設定例では、Light の後方のネットワークから House の後方のネットワーク（192.168.100.x ネットワークから 192.168.200.x ネットワーク）へのトラフィックが暗号化されます。 ネットワーク アドレス変換（NAT）オーバーロードも行われます。 ワイルドカード、事前共有キー、モード設定を使用した Light への暗号化 VPN Client 接続が許可されています。 インターネットへのトラフィックは変換されますが、暗号化されません。

## 前提条件

### 要件

このドキュメントに関する固有の要件はありません。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS® ソフトウェア リリース 12.2.7 および 12.2.8T
- Cisco Secure VPN Client 1.1（IRE クライアントの [Help] > [About] メニューでは 2.1.12 と表示されます）
- Cisco 3600 ルータ**注:** このような VPN シナリオで Cisco 2600 シリーズ ルータを使用する場合、クリプト IPSec VPN IOS イメージを使用してルータをインストールする必要があります

。
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

## 表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

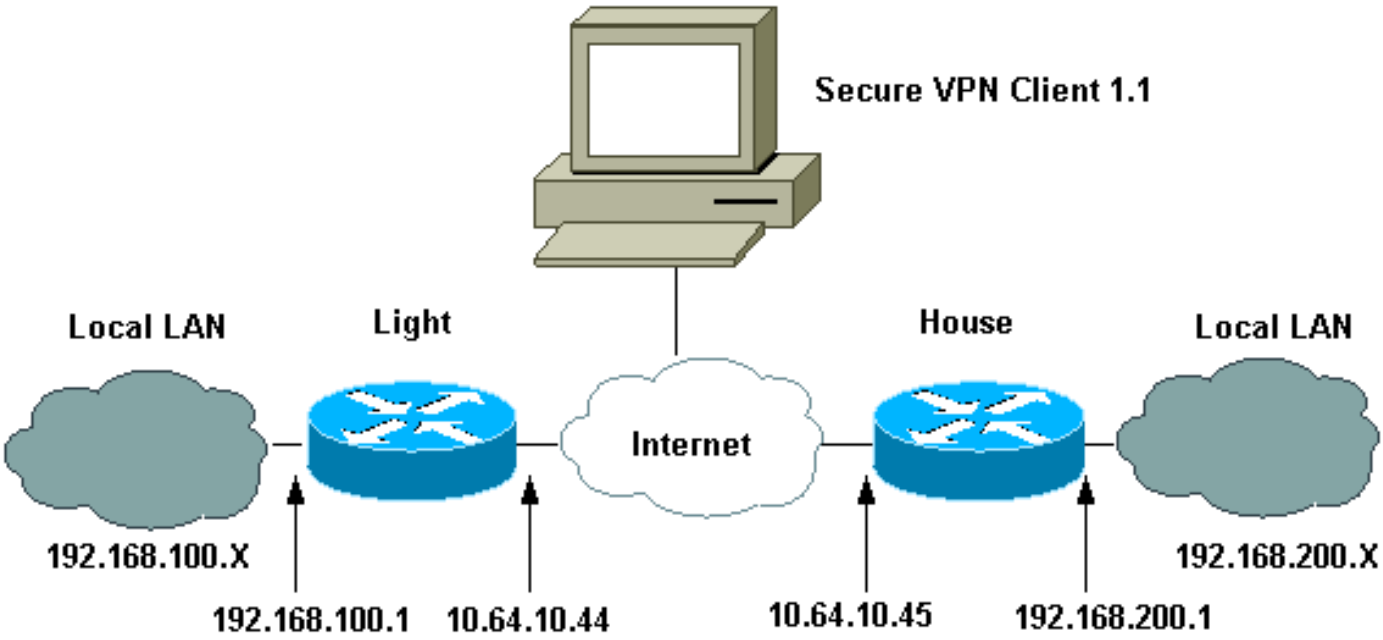
# 設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

**注:** このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

## ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。




## 設定

このドキュメントでは、次の設定を使用します。

- Light の設定
- House の設定
- VPN Client の設定

**Light の設定**

```
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 の設定

```
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 Client の設定

```
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
       Encryp 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
```

# 確認

ここでは、設定が正常に動作していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- **show crypto ipsec sa**：フェーズ 2 セキュリティ アソシエーションを表示します。
- **show crypto isakmp sa**：フェーズ 1 SA を表示します。

# トラブルシューティング

ここでは、設定に関するトラブルシューティングについて説明します。

## トラブルシューティングのためのコマンド

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

**注:** debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- **debug crypto ipsec**：フェーズ 2 の IPSec ネゴシエーションを表示します。
- **debug crypto isakmp**：フェーズ 1 の ISAKMP ネゴシエーションを表示します。
- **debug crypto engine**：暗号化されたトラフィックを表示します。
- **clear crypto isakmp**：フェーズ 1 に関連する SA をクリアします。
- **clear crypto sa**：フェーズ 2 に関連する SA をクリアします。

# 関連情報

- IPsec ネットワーク セキュリティの設定
- インターネット キー交換セキュリティ プロトコルの設定
- IPSec ネゴシエーション/IKE プロトコルに関するサポート ページ
- Cisco Secure VPN Client
- テクニカルサポート - Cisco Systems