配置IPSec路由器到路由器的NAT過載和Cisco安全VPN客戶端

目錄

簡介

此範例組態會加密從燈光後面的網路到House後面的網路（從192.168.100.x到192.168.200.x的網路）的流量。 網路地址轉換(NAT)過載也已完成。使用萬用字元、預共用金鑰和模式配置允許加密的VPN客戶端連線進入Light。到Internet的流量會被轉換，但不會加密。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco IOS®軟體版本12.2.7和12.2.8T
- Cisco安全VPN客戶端1.1(在IRE客戶端**幫助>關於**選單中顯示**為2.**1.12
- 思科3600路由器**注意：**如果將Cisco 2600系列路由器用於此類VPN場景，則路由器必須安裝加密IPsec VPN IOS映像。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

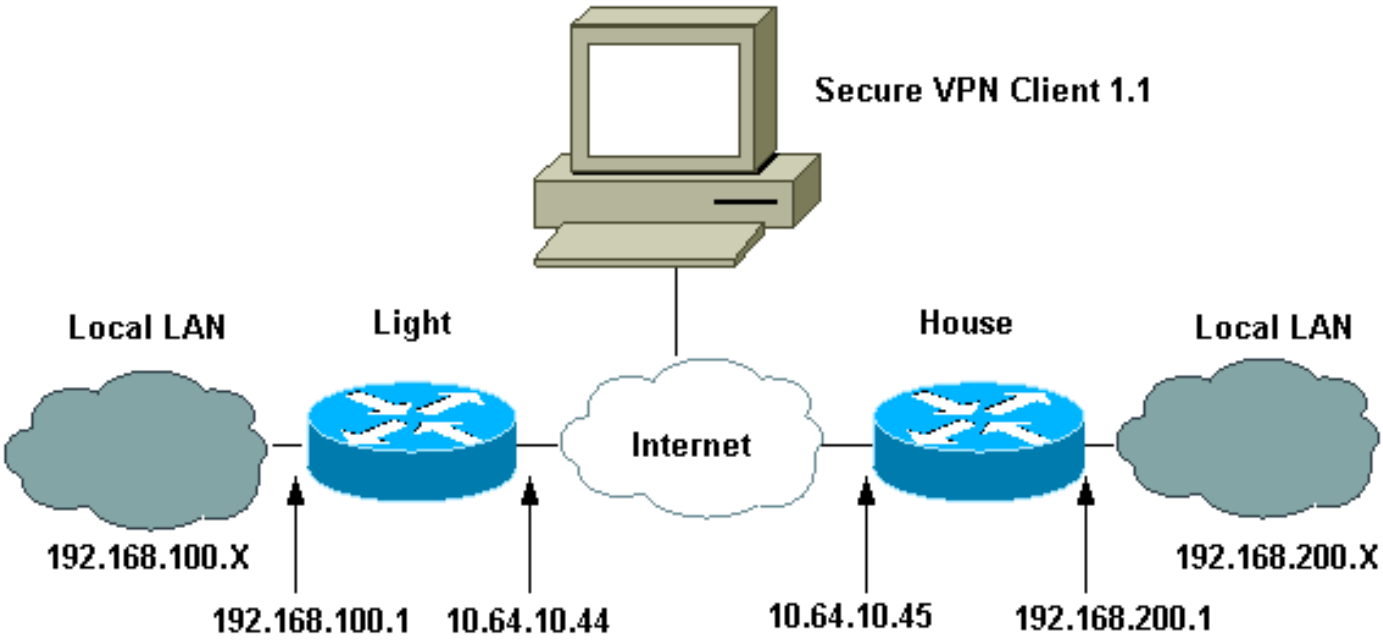
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用 Command Lookup Tool(僅限註冊客戶)查詢有關本文檔中使用的命令的更多資訊。

網路圖表

本檔案會使用以下網路設定：



組態

本檔案會使用這些設定。

- 燈光配置
- 房屋配置
- VPN客戶端配置

燈光配置

```
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
```

房屋配置

```
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客戶端配置

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
       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
```

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

- **show crypto ipsec sa** — 顯示第2階段安全關聯(SA)。
- **show crypto isakmp sa** — 顯示階段1 SA。

疑難排解

使用本節內容，對組態進行疑難排解。

疑難排解指令

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

附註：使用 **debug** 指令之前，請先參閱有關 Debug 指令的重要資訊。

- **debug crypto ipsec** — 顯示第2階段的IPsec協商。
- **debug crypto isakmp** — 顯示第1階段的ISAKMP協商。
- **debug crypto engine** — 顯示加密的流量。
- **clear crypto isakmp** — 清除與第1階段相關的SA。
- **clear crypto sa** — 清除與第2階段相關的SA。

相關資訊

- **配置IPSec網路安全**
- **配置Internet金鑰交換安全協定**
- **IPsec協商/IKE通訊協定支援頁面**
- **Cisco Secure VPN客戶端支援頁面**
- **技術支援 - Cisco Systems**