NAT 오버로드 및 Cisco Secure VPN Client로 IPSec 라우터 간 구성

목차

소개

이 샘플 컨피그레이션은 Light 뒤의 네트워크에서 House 뒤의 네트워크(192.168.100.x~192.168.200.x 네트워크)로 트래픽을 암호화합니다. NAT(Network Address Translation) 오버로드도 수행됩니다. 암호화된 VPN 클라이언트 연결은 와일드카드, 사전 공유 키 및 mode-config를 사용하여 Light로 허용됩니다. 인터넷에 대한 트래픽은 변환되지만 암호화되지 않습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® 소프트웨어 릴리스 12.2.7 및 12.2.8T
- Cisco Secure VPN Client 1.1(IRE 클라이언트 **도움말 > 정보** 메뉴에 2.1.12으로 표시됨)
- Cisco 3600 라우터**참고:** 이러한 종류의 VPN 시나리오에 Cisco 2600 Series 라우터를 사용하는 경우, 라우터는 crypto IPsec VPN IOS 이미지와 함께 설치해야 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든

명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

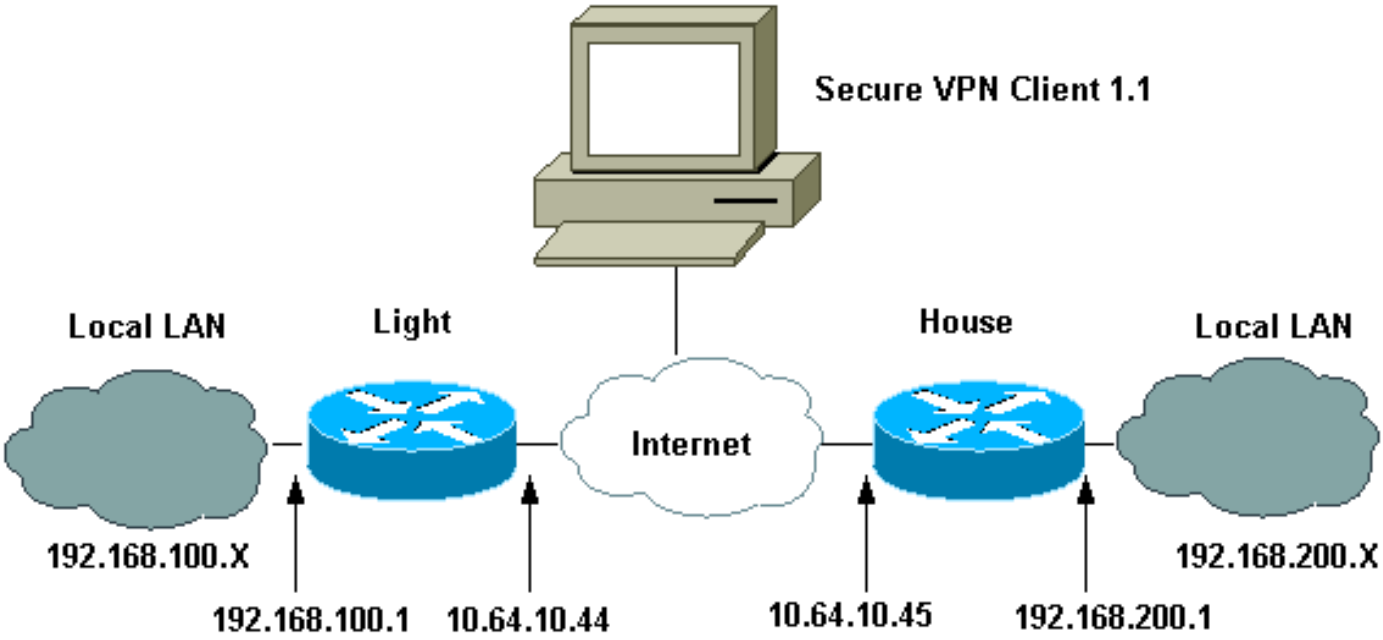
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 문서에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

이 문서에서는 이러한 구성을 사용합니다.

- 라이트 컨피그레이션
- 집 구성
- VPN 클라이언트 컨피그레이션

라이트 컨피그레이션

```
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
```

집 구성

```
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 클라이언트 컨피그레이션

```
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
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **show crypto ipsec sa** - 2단계 SA(보안 연결)를 표시합니다.
- **show crypto isakmp sa** - 1단계 SA를 표시합니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결할 수 있습니다.

문제 해결 명령

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug crypto ipsec** - 2단계의 IPsec 협상을 표시합니다.
- **debug crypto isakmp** - 1단계의 ISAKMP 협상을 표시합니다.
- **debug crypto engine** - 암호화된 트래픽을 표시합니다.
- **clear crypto isakmp** - 1단계와 관련된 SA를 지웁니다.
- **clear crypto sa** - 2단계와 관련된 SA를 지웁니다.

관련 정보

- IPSec 네트워크 보안 구성
- 인터넷 키 교환 보안 프로토콜 구성
- IPsec 협상/IKE 프로토콜 지원 페이지
- Cisco Secure VPN Client 지원 페이지
- Technical Support - Cisco Systems