Configuration d'IPSec de routeur à routeur, avec surcharge NAT et Cisco Secure VPN Client

Contenu

Introduction

Cet exemple de configuration effectue le chiffrement du trafic du réseau derrière Light au réseau derrière House (le réseau 192.168.100.x à 192.168.200.x). La surcharge de traduction d'adresses de réseau (NAT) est également effectuée. Les connexions de client VPN chiffrées sont permises dans Light avec des caractères de remplacement, des clés pré-partagées et la configuration de mode. Le trafic à Internet est traduit, mais non chiffré.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel Cisco IOS® versions 12.2.7 et 12.2.8T
- Cisco Secure VPN Client 1.1 (voir 2.1.12 dans le menu **Aide** du client IRE **> À propos**)
- Routeurs Cisco 3600**Remarque :** si vous utilisez les routeurs de la gamme Cisco 2600 pour ce type de scénario VPN, les routeurs doivent être installés avec des images IOS VPN IPsec cryptées.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

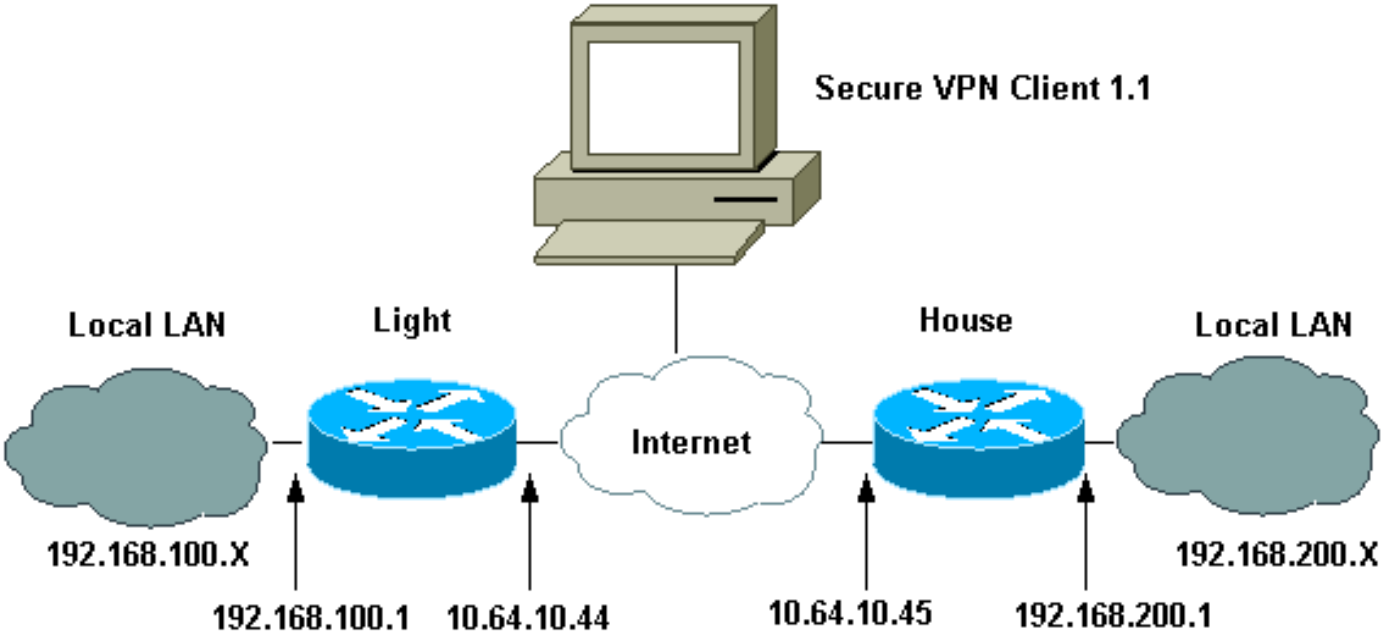
Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : Utilisez l'outil de recherche de commandes (clients inscrits seulement) pour en savoir plus sur les commandes figurant dans le présent document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Ce document utilise les configurations suivantes.

- Configuration de la lumière
- Configuration de la maison
- Configuration du client VPN

Configuration de la lumière
`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
```

Configuration de la maison

```
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
```

Configuration du client VPN

```
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
```

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

- **show crypto ipsec sa** - Affiche les associations de sécurité (SA) de phase 2.
- **show crypto isakmp sa** - Affiche les SA de phase 1.

Dépannage

Utilisez cette section pour dépanner votre configuration.

Dépannage des commandes

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **debug crypto ipsec : Cette commande affiche les négociations IPSec de la phase 2.**
- **debug crypto isakmp** - Affiche les négociations ISAKMP de la phase 1.
- **debug crypto engine - Montre le trafic crypté.**
- **clear crypto isakmp** : efface les SA liées à la phase 1.
- **clear crypto sa** : efface les SA liées à la phase 2.

Informations connexes

- Configuration de la sécurité des réseaux IPSec
- Configuration du protocole IKE (Internet Key Exchange)
- Page de support pour Protocole IKE/Négociation Ipsec
- Pages d'assistance Cisco Secure VPN Client
- Support technique - Cisco Systems