Konfigurieren von IPSec Router-to-Router mit NAT Overload und Cisco Secure VPN Client

Inhalt

Einführung

Diese Beispielkonfiguration verschlüsselt den Datenverkehr aus dem Netzwerk hinter Light in das Netzwerk hinter House (das Netzwerk 192.168.100.x bis 192.168.200.x). Die Network Address Translation (NAT) wird ebenfalls überlastet. Verschlüsselte VPN-Client-Verbindungen sind mit Wild-Card-, vorinstallierten Schlüsseln und Modus-Konfiguration in Light zugelassen. Der Datenverkehr ins Internet wird übersetzt, aber nicht verschlüsselt.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco IOS® Softwareversion 12.2.7 und 12.2.8T
- Cisco Secure VPN Client 1.1 (wird in der IRE-Client-**Hilfe** als 2.1.12 **> Info** angezeigt)
- Cisco Router der Serie 3600**Hinweis:** Wenn Sie die Cisco Router der Serie 2600 für ein derartiges VPN-Szenario verwenden, müssen die Router mit IPsec-VPN-IOS-Images mit Verschlüsselung installiert werden.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

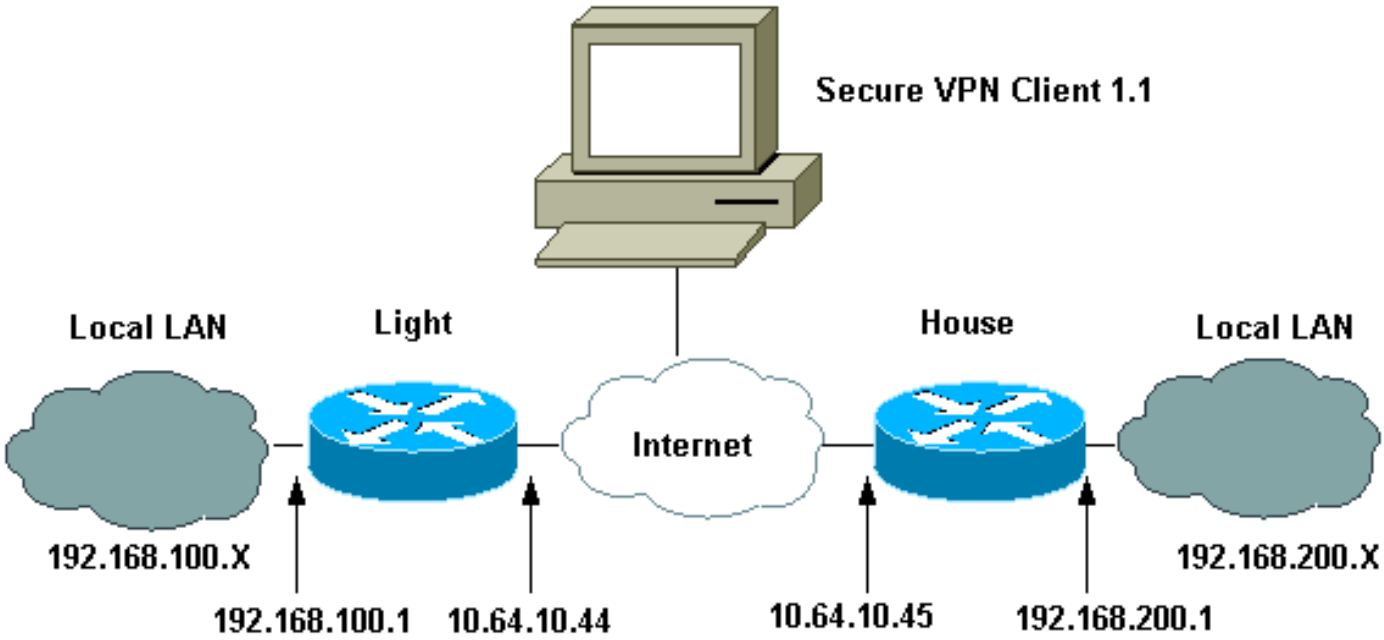
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument werden diese Konfigurationen verwendet.

- Lichtkonfiguration
- Hauskonfiguration
- VPN-Client-Konfiguration

Lichtkonfiguration

```
 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
```

Hauskonfiguration

```
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-Konfiguration

```
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
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- **show crypto ipsec sa**: Zeigt die Security Associations (SAs) der Phase 2.
- **show crypto isakmp sa** - Zeigt die SAs der Phase 1 an.

Fehlerbehebung

In diesem Abschnitt finden Sie eine Fehlerbehebung für Ihre Konfiguration.

Befehle zur Fehlerbehebung

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

- **debug crypto ipsec** - Zeigt die IPsec-Aushandlungen für Phase 2.
- **debug crypto isakmp** - Zeigt die ISAKMP-Verhandlungen für Phase 1.
- **debug crypto engine** - Zeigt den verschlüsselten Datenverkehr an.
- **clear crypto isakmp**: Löscht die SAs für Phase 1.
- **clear crypto sa**: Löscht die SAs für Phase 2.

Zugehörige Informationen

- Konfigurieren der IPSec-Netzwerksicherheit
- Konfigurieren des Internet Key Exchange Security Protocol
- Support-Seite für IPsec-Aushandlung/IKE-Protokoll
- Cisco Secure VPN Client - Support-Seiten
- Technischer Support - Cisco Systems