目次

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[表記法](#)
[設定](#)
[ネットワーク図](#)
[設定](#)
[確認](#)
[トラブルシューティング](#)
[トラブルシューティングのためのコマンド](#)
[関連情報](#)

概要

この設定例では、IPsec を使用して 2 つのプライベート ネットワーク間（10.50.50.x および 10.103.1.x）のトラフィックを暗号化する方法を示します。 ネットワークは、プライベート アドレスによって互いを認識します。

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 12.3.1a
- Cisco 2691 ルータ

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。

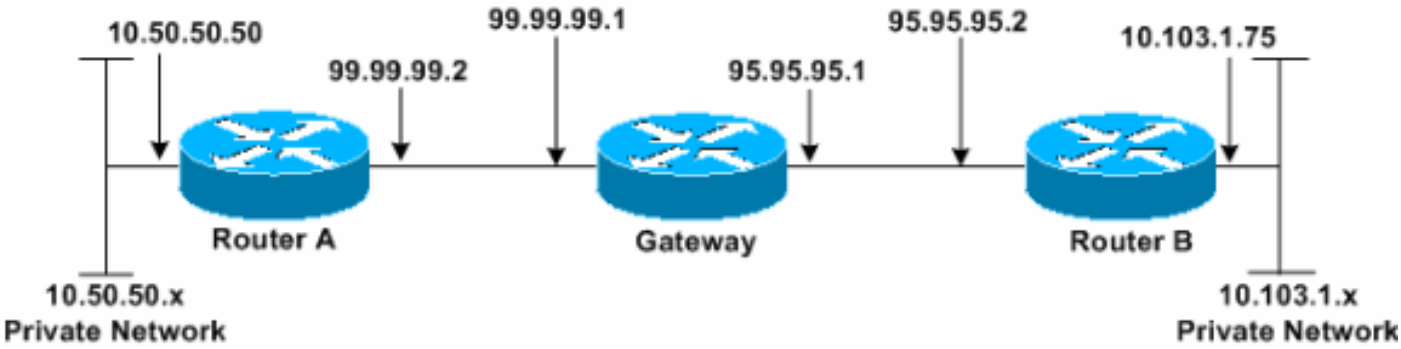
設定

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、次の図で示される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。

- ルータ A
- ルータ B

ルータ A

```
Router_A#write terminalBuilding configuration...Current
configuration : 1638 bytes ! version 12.3 service
timestamps debug datetime msec service timestamps log
datetime msec no service password-encryption ! hostname
Router_A ! boot system flash:c2691-ik9o3s-mz.123-1a.bin
! ip subnet-zero ! ip audit notify log ip audit po max-
events 100 no ftp-server write-enable ! crypto isakmp
policy 1 hash md5  authentication pre-share crypto
isakmp key cisco123 address 95.95.95.2 ! crypto ipsec
transform-set rtpset esp-des esp-md5-hmac  ! crypto map
rtp 1 ipsec-isakmp  set peer 95.95.95.2 set transform-
set rtpset  !--- Include the private network to private
network traffic !--- in the encryption process. match
address 115 ! no voice hpi capture buffer no voice hpi
capture destination  !  interface FastEthernet0/0 ip
address 99.99.99.2 255.255.255.0 ip nat outside duplex
auto speed auto crypto map rtp ! interface
FastEthernet0/1 ip address 10.50.50.50 255.255.255.0 ip
nat inside duplex auto speed auto ! !--- Except the
private network traffic from the !--- Network Address
Translation (NAT) process. ip nat inside source route-
map nonat interface FastEthernet0/0 overload ip http
server no ip http secure-server ip classless ip route
0.0.0.0 0.0.0.0 99.99.99.1 ! !--- Except the private
network traffic from the NAT process. access-list 110
deny ip 10.50.50.0 0.0.0.255 10.103.1.0 0.0.0.255
access-list 110 permit ip 10.50.50.0 0.0.0.255 any !---
Include the private network to private network traffic
!--- in the encryption process. access-list 115 permit
```

```
ip 10.50.50.0 0.0.0.255 10.103.1.0 0.0.0.255 ! !---
Except the private network traffic from the NAT process.
route-map nonat permit 10 match ip address 110 ! dial-
peer cor custom ! line con 0 exec-timeout 0 0 line aux 0
line vty 0 4 login ! end    Router_A#
```

ルータ B

```
Router_B#write terminalBuilding configuration...Current
configuration : 1394 bytes ! version 12.3 service
timestamps debug datetime msec service timestamps log
datetime msec no service password-encryption ! hostname
Router_B ! boot system flash:c2691-ik9o3s-mz.123-1a.bin
! ip subnet-zero ! ip audit notify log ip audit po max-
events 100 no ftp-server write-enable ! crypto isakmp
policy 1 hash md5  authentication pre-share crypto
isakmp key cisco123 address 99.99.99.2 ! crypto ipsec
transform-set rtpset esp-des esp-md5-hmac ! crypto map
rtp 1 ipsec-isakmp  set peer 99.99.99.2 set transform-
set rtpset  !--- Include the private network to private
network traffic !--- in the encryption process. match
address 115 ! no voice hpi capture buffer no voice hpi
capture destination  ! interface FastEthernet0/0 ip
address 95.95.95.2 255.255.255.0 ip nat outside duplex
auto speed auto crypto map rtp ! interface
FastEthernet0/1 ip address 10.103.1.75 255.255.255.0 ip
nat inside duplex auto speed auto ! !--- Except the
private network traffic from the NAT process. ip nat
inside source route-map nonat interface FastEthernet0/0
overload ip http server no ip http secure-server ip
classless ip route 0.0.0.0 0.0.0.0 95.95.95.1 ! !---
Except the private network traffic from the NAT process.
access-list 110 deny ip 10.103.1.0 0.0.0.255 10.50.50.0
0.0.0.255 access-list 110 permit ip 10.103.1.0 0.0.0.255
any !--- Include the private network to private network
traffic !--- in the encryption process. access-list 115
permit ip 10.103.1.0 0.0.0.255 10.50.50.0 0.0.0.255 ! !-
-- Except the private network traffic from the NAT
process. route-map nonat permit 10 match ip address 110
! dial-peer cor custom ! line con 0 exec-timeout 0 0
line aux 0 line vty 0 4 login ! end Router_B#
```

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

トラブルシューティングのためのコマンド

特定の **show** コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

注 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 sa** か。フェーズ2 の IPSec ネゴシエーションを表示する。
- **debug crypto isakmp sa** か。フェーズ 1.の Internet Security Association and Key Management Protocol（ISAKMP）ネゴシエーションを表示する。

- debug crypto engine か。暗号化されたセッションを表示する。

関連情報

- IP Security のトラブルシューティング：debug コマンドの説明と使用
- IPSec に関するサポート ページ
- テクニカルサポート - Cisco Systems