

プライベート ネットワーク間でのルータ間 IPSec、事前共有、NAT 過負荷の設定

内容

[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特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いています。

- 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ました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメントの表記法の詳細は、「[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。

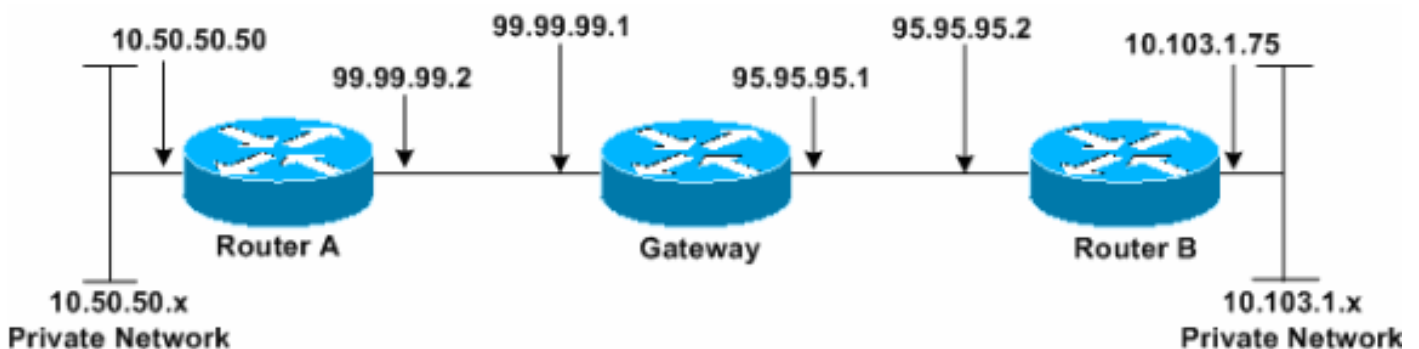
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：この文書で使用されているコマンドの詳細を調べるには、「[Command Lookup ツール](#)」を使用してください（登録ユーザのみ）。

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設定を使用しています。



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 terminal
Building 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 terminal
Building 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

一部の show コマンドは [アウトプット インタープリタ ツール](#) によってサポートされています ([登録ユーザ専用](#))。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

注 : debug コマンドを発行する前に、『[debug コマンドの重要な情報](#)』を参照してください。

- debug crypto ipsec sa : フェーズ 2 の IPsec ネゴシエーションを表示します。
- debug crypto isakmp sa : 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します。
- debug crypto engine : 暗号化されたセッションを表示します。

関連情報

- [IIP 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](#)