

プライベート ネットワークとパブリック ネットワーク間の IPsec ルータ相互間、事前共有、NAT オーバーロードの設定

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](#)

[show のサンプル出力](#)

[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 を使用してプライベート ネットワーク (10.103.1.x) とパブリック ネットワーク (98.98.98.x) 間のトラフィックを暗号化する方法を示します。98.98.98.x ネットワークは、プライベート アドレスにより 10.103.1.x ネットワークを認識します。10.103.1.x ネットワークは、パブリック アドレスにより 98.98.98.x ネットワークを認識します。

前提条件

要件

このマニュアルは、IPsec プロトコルに関する基本的知識を前提とします。IPsec の詳細については、『[IP Security \(IPsec \) 暗号化の概要](#)』を参照してください。

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 リース 12.3(5)
- Cisco 3640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。

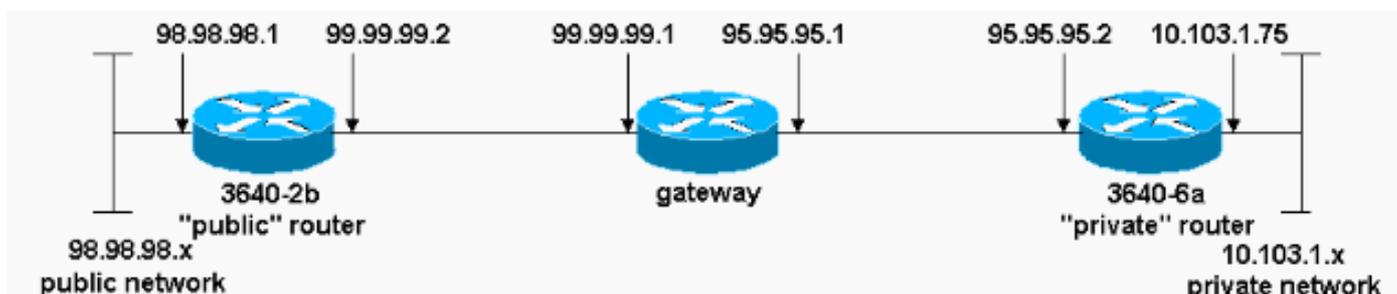
設定

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、次の構成を使用します。

- [3640-2b 「パブリック」ルータ](#)
- [3640-6a "プライベート"ルータ](#)

3640-2b 「パブリック」ルータ

```
rp-3640-2b#show running config
Building configuration...

Current configuration:
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rp-3640-2b
!
ip subnet-zero
!
```

```
!  
!--- Defines the Internet Key Exchange (IKE) policies.  
crypto isakmp policy 1  
  
!--- Defines an IKE policy. Use the crypto isakmp policy  
!--- command in global configuration mode. IKE policies  
!--- define a set of parameters !--- that are used  
during the IKE phase I negotiation.  
  
hash md5  
authentication pre-share  
  
!--- Specifies preshared keys as the authentication  
method. crypto isakmp key cisco123 address 95.95.95.2  
  
!--- Configures a preshared authentication key, used in  
!--- global configuration mode. ! crypto ipsec  
transform-set rtpset esp-des esp-md5-hmac  
  
!--- Defines a transform-set. This is an acceptable !---  
combination of security protocols and algorithms, !---  
which has to be matched on the peer router. ! crypto map  
rtp 1 ipsec-isakmp  
  
!--- Indicates that IKE is used to !--- establish the  
IPSec security associations (SAs) that protect !--- the  
traffic specified by this crypto map entry. set peer  
95.95.95.2  
  
!--- Sets the IP address of the remote end. set  
transform-set rtpset  
  
!--- Configures IPsec to use the transform-set !---  
"rtpset" defined earlier. match address 115  
  
!--- This is used to assign an extended access list to a  
!--- crypto map entry which is used by IPSec !--- to  
determine which traffic should be protected !--- by  
crypto and which traffic does not !--- need crypto  
protection. ! interface Ethernet0/0 ip address  
98.98.98.1 255.255.255.0 no ip directed-broadcast !  
interface Ethernet0/1  
ip address 99.99.99.2 255.255.255.0  
no ip directed-broadcast  
no ip route-cache  
  
!--- Enable process switching for !--- IPSec to encrypt  
outgoing packets. !--- This command disables fast  
switching. no ip mroute-cache crypto map rtp  
  
!--- Configures the interface to use !--- the crypto map  
"rtp" for IPSec. ! . . !--- Output suppressed. . . ip  
classless ip route 0.0.0.0 0.0.0.0 99.99.99.1  
  
!--- Default route to the next hop address. no ip http  
server ! access-list 115 permit ip 98.98.98.0 0.0.0.255  
10.103.1.0 0.0.0.255  
  
!--- This access-list option causes all IP traffic !---  
that matches the specified conditions to be !---  
protected by IPSec using the policy described by !---  
the corresponding crypto map command statements.
```

```
access-list 115 deny ip 98.98.98.0 0.0.0.255 any

!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

3640-6a "プライベート"ルータ

```
rp-3640-6a#show running config
Building configuration...

Current configuration:
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rp-3640-6a
!
!
ip subnet-zero

!--- Defines the IKE policies. ! crypto isakmp policy 1

!--- Defines an IKE policy. !--- Use the crypto isakmp
policy !--- command in global configuration mode. IKE
policies !--- define a set of parameters !--- that are
used during the IKE phase I negotiation.

hash md5
authentication pre-share

!--- Specifies preshared keys as the authentication
method. crypto isakmp key cisco123 address 99.99.99.2

!--- Configures a preshared authentication key, !---
used in global configuration mode. ! crypto ipsec
transform-set rtpset esp-des esp-md5-hmac

!--- Defines a transform-set. This is an !--- acceptable
combination of security protocols and algorithms, !---
which has to be matched on the peer router. crypto map
rtp 1 ipsec-isakmp

!--- Indicates that IKE is used to establish !--- the
IPSec SAs that protect the traffic !--- specified by
this crypto map entry. set peer 99.99.99.2

!--- Sets the IP address of the remote end. set
transform-set rtpset
```

```
!--- Configures IPSec to use the transform-set !---
"rtspset" defined earlier. match address 115

!--- Used to assign an extended access list to a !---
crypto map entry which is used by IPSec !--- to
determine which traffic should be protected !--- by
crypto and which traffic does not !--- need crypto
protection. . . !--- Output suppressed. . . ! interface
Ethernet3/0 ip address 95.95.95.2 255.255.255.0 no ip
directed-broadcast ip nat outside

!--- Indicates that the interface is !--- connected to
the outside network. no ip route-cache

!--- Enable process switching for !--- IPSec to encrypt
outgoing packets. !--- This command disables fast
switching. no ip mroute-cache crypto map rtp

!--- Configures the interface to use the !--- crypto map
"rtp" for IPSec. ! interface Ethernet3/2 ip address
10.103.1.75 255.255.255.0 no ip directed-broadcast ip
nat inside

!--- Indicates that the interface is connected to !---
the inside network (the network subject to NAT
translation). ! ip nat pool FE30 95.95.95.10 95.95.95.10
netmask 255.255.255.0

!--- Used to define a pool of IP addresses for !--- NAT.
Use the ip nat pool command in !--- global configuration
mode.

ip nat inside source route-map nonat pool FE30 overload

!--- Used to enable NAT of !--- the inside source
address. Use the ip nat inside source !--- command in
global configuration mode. !--- The 'overload' option
enables the router to use one global !--- address for
many local addresses.

ip classless
ip route 0.0.0.0 0.0.0.0 95.95.95.1

!--- Default route to the next hop address. no ip http
server ! access-list 110 deny ip 10.103.1.0 0.0.0.255
98.98.98.0 0.0.0.255
access-list 110 permit ip 10.103.1.0 0.0.0.255 any

!--- Addresses that match this ACL are NATed while !---
they access the Internet. They are not NATed !--- if
they access the 98.98.98.0 network. access-list 115
permit ip 10.103.1.0 0.0.0.255 98.98.98.0 0.0.0.255

!--- This access-list option causes all IP traffic that
!--- matches the specified conditions to be !---
protected by IPSec using the policy described !--- by
the corresponding crypto map command statements.

access-list 115 deny ip 10.103.1.0 0.0.0.255 any

route-map nonat permit 10
```

```
match ip address 110
!
!
line con 0

line vty 0 4

!
end
```

確認

ここでは、設定が正しく機能していることを確認するために使用する情報を示します。

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。

この設定を確認するには、プライベートルータ10.103.1.75のイーサネットインターフェイスを送信元とし、パブリックルータ98.98.98.1のイーサネットインターフェイスを宛先とする拡張 ping コマンドを試します

- [ping : 基本的なネットワーク接続を診断するために使用されます。](#)

```
rp-3640-6a#ping
Protocol [ip]:
Target IP address: 98.98.98.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.103.1.75
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 98.98.98.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/64/68 ms
```

- [show crypto ipsec sa : 現在の \(IPsec \) SA で使用されている設定を表示します。](#)
- [show crypto isakmp sa : ピアにある現在のすべての IKE SA を表示します。](#)
- [show crypto engine](#) : 暗号化エンジンの設定情報の概要を表示します。特権EXECモードで [show crypto engine](#) コマンドを使用します。

show のサンプル出力

この出力は、ハブ ルータ上で発行された show crypto ipsec sa コマンドからのものです。

```
rp-3640-6a#show crypto ipsec sa
interface: Ethernet0/0
```

```
Crypto map tag: rtp, local addr. 95.95.95.2

protected vrf:
local ident (addr/mask/prot/port): (10.103.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (98.98.98.0/255.255.255.0/0/0)
current_peer: 99.99.99.2:500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5
#pkts decaps: 14, #pkts decrypt: 14, #pkts verify 14
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 95.95.95.2, remote crypto endpt.: 99.99.99.2
path mtu 1500, media mtu 1500
current outbound spi: 75B6D4D7

inbound esp sas:
spi: 0x71E709E8(1910966760)
  transform: esp-des esp-md5-hmac ,
  in use settings = {Tunnel, }
  slot: 0, conn id: 2000, flow_id: 1, crypto map: rtp
  sa timing: remaining key lifetime (k/sec): (4576308/3300)
  IV size: 8 bytes
  replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x75B6D4D7(1974916311)
  transform: esp-des esp-md5-hmac ,
  in use settings = {Tunnel, }
  slot: 0, conn id: 2001, flow_id: 2, crypto map: rtp
  sa timing: remaining key lifetime (k/sec): (4576310/3300)
  IV size: 8 bytes
  replay detection support: Y

outbound ah sas:

outbound pcp sas:
```

このコマンドは、ピア間で構築された IPsec SA を示します。暗号化されたトンネルは、ネットワーク98.98.98.0と10.103.1.0の間を通過するトラフィック用に95.95.95.2と99.99.99.2の間に構築されます。着信と発信の2つのEncapsulating Security Payload(ESP)SAを確認できます。認証ヘッダー(AH)SAは、AHがないため使用されません。

[トラブルシューティング](#)

ここでは、設定のトラブルシューティングに使用できる情報を示します。

[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 コマンドを使用する前に、「[debug コマンドに関する重要な情報](#)」を参照してください

い。

- `debug crypto ipsec sa` : フェーズ2のIPSecネゴシエーションを表示するために使用します。
- `debug crypto isakmp sa` : フェーズ1のISAKMPネゴシエーションを表示するために使用します。
- `debug crypto engine` : 暗号化されたセッションを表示するために使用します。

関連情報

- [NATの処理順序](#)
- [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](#)
- [NAT に関するサポート ページ](#)
- [テクニカルサポート - Cisco Systems](#)