

Configuring IPSec Router-to-Router, Pre-shared, NAT Overload Between a Private and a Public Network

Document ID: 14142

Introduction

Prerequisites

Requirements

Components Used

Conventions

Configure

Network Diagram

Configurations

Verify

Sample show Output

Troubleshoot

Troubleshooting Commands

Related Information

Introduction

This sample configuration shows how to encrypt traffic between a private network (10.103.1.x) and a public network (98.98.98.x) with the use of IPSec. The 98.98.98.x network knows the 10.103.1.x network by the private addresses. The 10.103.1.x network knows the 98.98.98.x network by the public addresses.

Prerequisites

Requirements

This document requires a basic understanding of IPSec protocol. To learn more about IPSec, please refer to [An Introduction to IP Security \(IPSec\) Encryption](#).

Components Used

The information in this document is based on these software and hardware versions:

- Cisco IOS® Software Release 12.3(5)
- Cisco 3640 Routers

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

For more information on document conventions, refer to [Cisco Technical Tips Conventions](#).

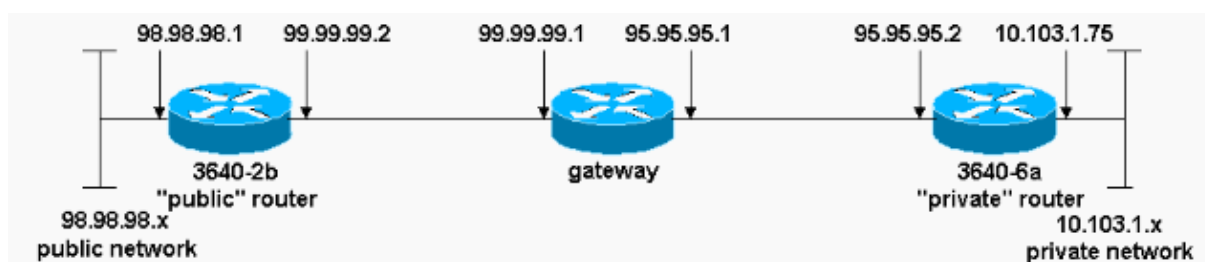
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only).

Network Diagram

This document uses the network setup shown in this diagram.



Configurations

This document uses these configurations:

- 3640-2b "Public" Router
- 3640-6a "Private" Router

3640-2b "Public" Router

```
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 "Private" Router

```

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  
!--- "rtpset" 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

```

Verify

This section provides information you can use to confirm your configuration is working properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

To verify this configuration, try an extended **ping** command sourced from the Ethernet interface on the private router 10.103.1.75, destined to the Ethernet interface on the public router 98.98.98.1

- **ping** Used to diagnose basic network connectivity.

```
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** Shows the settings used by current (IPSec) SAs.
- **show crypto isakmp sa** Shows all current IKE SAs at a peer.
- **show crypto engine** Shows a summary of the configuration information for the crypto engines. Use the **show crypto engine** command in privileged EXEC mode.

Sample show Output

This output is from the **show crypto ipsec sa** command issued on the hub router.

```
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:
```

This command shows IPSec SAs built between peers. The encrypted tunnel is built between 95.95.95.2 and 99.99.99.2 for traffic that goes between networks 98.98.98.0 and 10.103.1.0. You can see the two Encapsulating Security Payload (ESP) SAs built inbound and outbound. Authentication Header (AH) SAs are not used since there are no AHs.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

Note: Before issuing **debug** commands, please see Important Information on Debug Commands.

- **debug crypto ipsec sa** Used to see the IPSec negotiations of phase 2.
- **debug crypto isakmp sa** Used to see the ISAKMP negotiations of phase 1.
- **debug crypto engine** Used to display the encrypted sessions.

Related Information

- [NAT Order of Operation](#)
- [IP Security Troubleshooting – Understanding and Using debug Commands](#)
- [IPSec Support Page](#)
- [NAT Support Page](#)
- [Technical Support – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)