Configuring Router−to−Router Dynamic−to−Static IPSec with NAT

Document ID: 14131

Contents

Introduction

In this sample configuration, a remote router receives an IP address through part of PPP called IP Control Protocol (IPCP). The remote router uses the IP address to connect to a hub router. This configuration enables the hub router to accept dynamic IPSec connections. The remote router uses network address translation (NAT) to "join" the privately addressed devices behind it to the privately addressed network behind the hub router. The remote router knows the endpoint and can initiate connections to the hub router. But the hub router does not know the endpoint, so it cannot initiate connections to the remote router.

In this example, dr_whoovie is the remote router and sam−i−am is the hub router. An access list specifies what traffic is to be encrypted, so dr_whoovie knows what traffic to encrypt and where the sam−i−am endpoint is located. The remote router must initiate the connection. Both sides are doing NAT overload.

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 12.2(24a)
- Cisco 2500 Series 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

Refer to Cisco Technical Tips Conventions for more information on document conventions.

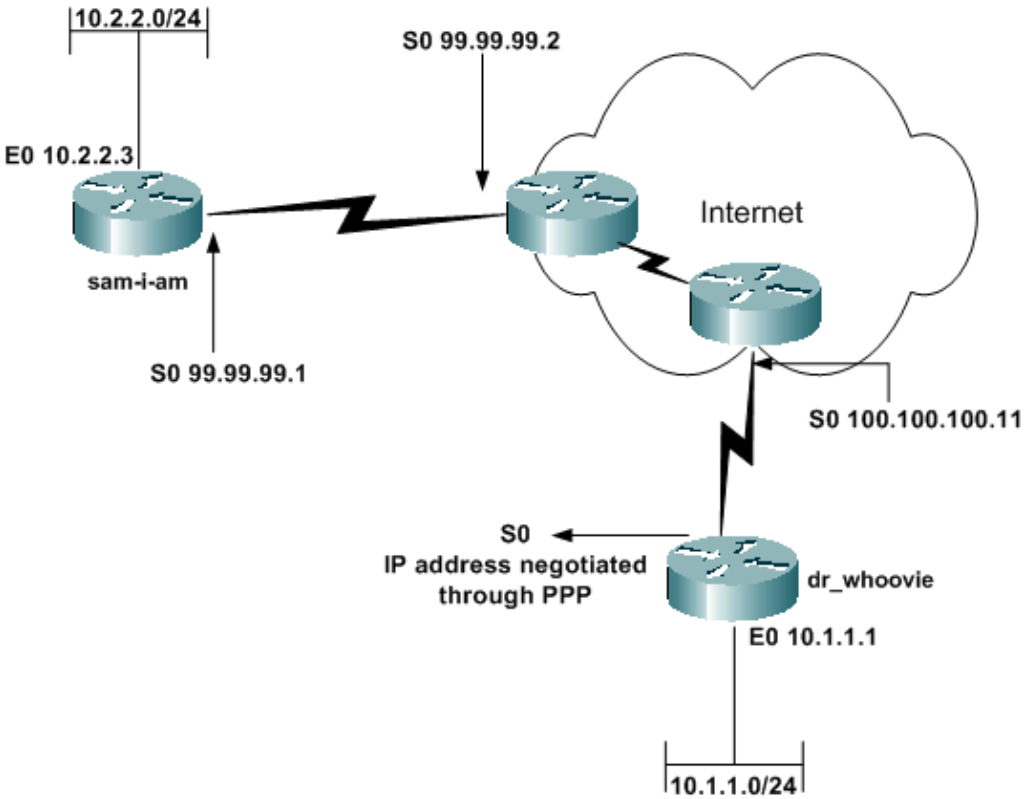
Configure

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

Note: Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

Network Diagram

This document uses this network setup:



Configurations

This document uses these configurations:

- sam−i−am
- dr_whoovie

sam−i−am

```
Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log up time
no service password-encryption
```

```
!
hostname sam-i-am
!
ip subnet-zero
!

!--- These are the IKE policies.

crypto isakmp policy 1

!--- Defines an Internet Key Exchange (IKE) policy.
!--- Use the crypto isakmp policy command
!--- in global configuration mode.
!--- IKE policies define a set of parameters to be used
!--- during the IKE phase I negotiation.

hash md5
authentication pre-share

!--- Specifies pre-shared keys as the authentication method.

crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0

!--- Configures a pre-shared authentication key,
!--- used in global configuration mode.

!

!--- These are the IPSec policies.

crypto ipsec transform-set rtpset esp-des esp-md5-hmac

!--- A transform set is an acceptable combination
!--- of security protocols and algorithms.
!--- This command defines a transform set
!--- that has to be matched on the peer router.

crypto dynamic-map rtpmap 10

!--- Use dynamic crypto maps to create policy templates
!--- that can be used to process negotiation requests
!--- for new security associations (SA) from a remote IPSec peer,
!--- even if you do not know all of the crypto map parameters
!--- required to communicate with the remote peer,
!--- such as the IP address of the peer.

set transform-set rtpset

!--- Configure IPSec to use the transform set "rtpset"
!--- that was defined previously.

match address 115

!--- Assign an extended access list to a crypto map entry
!--- that is used by IPSec to determine which traffic
!--- should be protected by crypto and which traffic
!--- does not need crypto protection.

crypto map rtptrans 10 ipsec-isakmp dynamic rtpmap

!--- Specifies that this crypto map entry is to reference
!--- a preexisting dynamic crypto map.

!
interface Ethernet0
 ip address 10.2.2.3 255.255.255.0
```

```
 no ip directed-broadcast
 ip nat inside

 !--- This indicates that the interface is connected to the
 !--- inside network, which is subject to NAT translation.

 no mop enabled
!
interface Serial0
 ip address 99.99.99.1 255.255.255.0
 no ip directed-broadcast
 ip nat outside

 !--- This indicates that the interface is connected
 !--- to the outside network.

crypto map rtptrans

!--- Use the crypto map interface configuration command
!--- to apply a previously defined crypto map set to an interface.

!
ip nat inside source route-map nonat interface Serial0 overload

!--- Except the private network from the NAT process.

ip classless
ip route 0.0.0.0 0.0.0.0 Serial0
no ip http server
!
access-list 115 permit ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 115 deny ip 10.2.2.0 0.0.0.255 any

!--- Include the private-network-to-private-network traffic
!--- in the encryption process.

access-list 120 deny ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 120 permit ip 10.2.2.0 0.0.0.255 any

!--- Except the private network from the NAT process.

route-map nonat permit 10
 match ip address 120
!
line con 0
 transport input none
line aux 0
line vty 0 4
 password ww
 login
!
end
```

dr_whoovie

```
Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname dr_whoovie
!
ip subnet-zero
```

```
!

!--- These are the IKE policies.

crypto isakmp policy 1

!--- Defines an Internet Key Exchange (IKE) policy.
!--- Use the crypto isakmp policy command
!--- in global configuration mode.
!--- IKE policies define a set of parameters to be used
!--- during the IKE phase I negotiation.

 hash md5
authentication pre-share

!--- Specifies pre-shared keys as the authentication method.

crypto isakmp key cisco123 address 99.99.99.1

!--- Configures a pre-shared authentication key,
!--- used in global configuration mode.

!

!--- These are the IPSec policies.

crypto ipsec transform-set rtpset esp-des esp-md5-hmac

!--- A transform set is an acceptable combination
!--- of security protocols and algorithms.
!--- This command defines a transform set
!--- that has to be matched on the peer router.

!
crypto map rtp 1 ipsec-isakmp

!--- Creates a crypto map and indicates that IKE will be used
!--- to establish the IPSec SAs for protecting
!--- the traffic specified by this crypto map entry.

set peer 99.99.99.1

!--- Use the set peer command to specify an IPSec peer in a crypto map entry.

set transform-set rtpset

!--- Configure IPSec to use the transform set "rtpset"
!--- that was defined previously.

 match address 115

!--- Include the private-network-to-private-network traffic
!--- in the encryption process.

!
interface Ethernet0
ip address 10.1.1.1 255.255.255.0
 no ip directed-broadcast
 ip nat inside

 !--- This indicates that the interface is connected to the
 !--- inside network, which is subject to NAT translation.

 no mop enabled
!
interface Serial0
```

```
 ip address negotiated

 !--- Specifies that the IP address for this interface
 !--- is obtained via PPP/IPCP address negotiation.
 !--- This example was set up in a lab with an IP address
 !--- assigned with IPCP.

 no ip directed-broadcast
 ip nat outside

 !--- This indicates that the interface is connected
 !--- to the outside network.

 encapsulation ppp
 no ip mroute-cache
 no ip route-cache
 crypto map rtp

 !--- Use the crypto map interface configuration command
 !--- to apply a previously defined crypto map set to an interface.

ip nat inside source route-map nonat interface Serial0 overload

!--- Except the private network from the NAT process.

ip classless
ip route 0.0.0.0 0.0.0.0 Serial0
no ip http server
!
access-list 115 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
access-list 115 deny ip 10.1.1.0 0.0.0.255 any

!--- Include the private-network-to-private-network traffic
!--- in the encryption process.

access-list 120 deny   ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
access-list 120 permit ip 10.1.1.0 0.0.0.255 any

!--- Except the private network from the NAT process.

dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
route-map nonat permit 10
 match ip address 120
!
line con 0
 transport input none
line aux 0
line vty 0 4
 password ww
 login
!
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.

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

This example shows a ping from the 10.1.1.1 Ethernet interface on dr_whoovie to the 10.2.2.3 Ethernet interface on sam−i−am.

```
dr_whoovie# ping
Protocol [ip]:
Target IP address: 10.2.2.3
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.1
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 10.2.2.3,
  timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
!!!!!
Success rate is 100 percent (5/5),
  round−trip min/avg/max = 36/38/40 ms
```

- **show crypto ipsec sa** Shows the phase 2 security associations (SA).
- **show crypto isakmp sa** Shows the phase 1 SAs.

Sample Output

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

```
sam−i−am# show crypto ipsec sa

interface: Serial0
    Crypto map tag: rtptrans, local addr. 99.99.99.1

   local  ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
   current_peer: 100.100.100.1
     PERMIT, flags={}
    #pkts encaps: 6, #pkts encrypt: 6, #pkts digest 6
    #pkts decaps: 6, #pkts decrypt: 6, #pkts verify 6
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 0, #recv errors 0

     local crypto endpt.: 99.99.99.1, remote crypto endpt.: 100.100.100.1
     path mtu 1500, ip mtu 1500, ip mtu interface Serial0
     current outbound spi: 52456533

     inbound esp sas:
      spi: 0x6462305C(1684156508)
        transform: esp−des esp−md5−hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: rtptrans
        sa timing: remaining key lifetime (k/sec): (4607999/3510)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
```

```
 spi: 0x52456533(1380279603)
   transform: esp-des esp-md5-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 2001, flow_id: 2, crypto map: rtptrans
   sa timing: remaining key lifetime (k/sec): (4607999/3510)
   IV size: 8 bytes
   replay detection support: Y

outbound ah sas:

outbound pcp sas:
```

This command shows IPSec SAs that are built between the peer devices. The encrypted tunnel connects the 100.100.100.1 interface on dr_whoovie and the 99.99.99.1 interface on sam−i−am. This tunnel carries traffic going between networks 10.2.2.3 and 10.1.1.1. Two Encapsulating Security Payload (ESP) SAs are built inbound and outbound. The tunnel is established even though sam−i−am does not know the peer IP address (100.100.100.1). Authentication Header (AH) SAs are not used since there are no AH configured.

These outputs samples show that the serial interface 0 on dr_whoovie receives an IP address of 100.100.100.1 through IPCP.

- Before the IP address is negotiated:

```
dr_whoovie#show interface serial0
Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address will be negotiated using IPCP
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
```

- After the IP address is negotiated:

```
dr_whoovie#show interface serial0
Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 100.100.100.1/32
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
```

This example was set up in a lab with the **peer default ip address** command to assign an IP address at the remote end of the serial 0 interface on dr_whoovie. The IP pool is defined with the **ip local pool** command at the remote end.

Troubleshoot

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

Troubleshooting Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug crypto ipsec** Shows the IPSec negotiations of phase 2.

- **debug crypto isakmp** Shows the Internet Security Association and Key Management Protocol (ISAKMP) negotiations of phase 1.
- **debug crypto engine** Shows the traffic that is encrypted.
- **debug ip nat detailed** (Optional) Verifies the operation of the NAT feature by displaying information about every packet that the router translates.

  
  Caution: This command generates a large amount of output. Use this command only when traffic on the IP network is low.
- **clear crypto isakmp** Clears the SAs related to phase 1.
- **clear crypto sa** Clears the SAs related to phase 2.
- **clear ip nat translation** Clears dynamic NAT translations from the translation table.

Related Information

- **IPSec Support Page**
- **Technical Support − Cisco Systems**

Updated: Jan 19, 2006 Document ID: 14131