

Configuring a Router IPsec Tunnel Private-to-Private Network with NAT and a Static

Document ID: 14144

Introduction

Prerequisites

Requirements

Components Used

Conventions

Why does the Deny Statement in the ACL specify the NAT Traffic?

What about the static NAT though, why can I not get to that address over the IPsec tunnel?

Configure

Network Diagram

Configurations

Verify

Troubleshoot

Troubleshooting Commands

Related Information

Introduction

This sample configuration shows you how to:

- Encrypt traffic between two private networks (10.1.1.x and 172.16.1.x).
- Assign a static IP address (external address 200.1.1.25) to a network device at 10.1.1.3.

You use access control lists (ACLs) to tell the router not to do Network Address Translation (NAT) to the private-to-private network traffic, which is then encrypted and placed on the tunnel as it leaves the router. There is also a static NAT for an inside server on the 10.1.1.x network in this sample configuration. This sample configuration uses the route-map option on the NAT command to stop it from being NAT'd if traffic for it is also destined over the encrypted tunnel.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

- Cisco IOS® Software Release 12.3(14)T
- Two Cisco 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.

Why does the Deny Statement in the ACL specify the NAT Traffic?

You conceptually replace a network with a tunnel when you use Cisco IOS IPsec or a VPN. You replace the Internet cloud by a Cisco IOS IPsec tunnel that goes from 200.1.1.1 to 100.1.1.1 in this diagram. Make this network transparent from the point of view of the two private LANs that are linked together by the tunnel. You usually do not want to use NAT for the traffic that goes from one private LAN to the remote private LAN for this reason. You want to see the packets which come from the Router 2 network with a source IP address from the 10.1.1.0/24 network instead of 200.1.1.1 when the packets reach the inside Router 3 network.

Refer to NAT Order of Operation for more information on how to configure a NAT. This document shows that the NAT takes place before the crypto check when the packet goes from inside to outside. This is why you must specify this information in the configuration.

```
ip nat inside source list 122 interface Ethernet0/1 overload

access-list 122 deny ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 122 permit ip 10.1.1.0 0.0.0.255 any
```

Note: It is also possible to build the tunnel and still use NAT. You specify the NAT traffic as the "interesting traffic for IPsec" (referred to as ACL 101 in other sections of this document) in this scenario. Refer to Configuring an IPsec Tunnel between Routers with Duplicate LAN Subnets for more information on how to build a tunnel while NAT is active.

What about the static NAT though, why can I not get to that address over the IPsec tunnel?

This setup also includes a static one-to-one NAT for a server at 10.1.1.3. This is NAT'd to 200.1.1.25 so that Internet users can access it. Issue this command:

```
ip nat inside source static 10.1.1.3 200.1.1.25
```

This static NAT precludes users on the 172.16.1.x network from reaching 10.1.1.3 via the encrypted tunnel. This is because you need to deny the encrypted traffic from being NAT'd with ACL 122. However, the static NAT command takes precedence over the generic NAT statement for all connections to and from 10.1.1.3. The static NAT statement does not specifically deny encrypted traffic from also being NAT'd. The replies from 10.1.1.3 are NAT'd to 200.1.1.25 when a user on the 172.16.1.x network connects to 10.1.1.3 and therefore do not go back over the encrypted tunnel (NAT happens before encryption).

You must deny encrypted traffic from being NAT'd (even statically one-to-one NAT'd) with a **route-map** command on the static NAT statement.

Note: The **route-map** option on a static NAT is only supported from Cisco IOS Software Release 12.2(4)T and later. Refer to NAT Ability to Use Route Maps with Static Translations for additional information.

You must issue these additional commands to allow encrypted access to 10.1.1.3, the statically NAT'd host:

```
ip nat inside source static 10.1.1.3 200.1.1.25 route-map nonat
!
```

```

access-list 150 deny ip host 10.1.1.3 172.16.1.0 0.0.0.255
access-list 150 permit ip host 10.1.1.3 any
!
route-map nonat permit 10
match ip address 150

```

These statements tell the router to only apply the static NAT to traffic that matches ACL 150. ACL 150 says not to apply the NAT to traffic sourced from 10.1.1.3 and destined over the encrypted tunnel to 172.16.1.x. However, apply it to all other traffic sourced from 10.1.1.3 (Internet-based traffic).

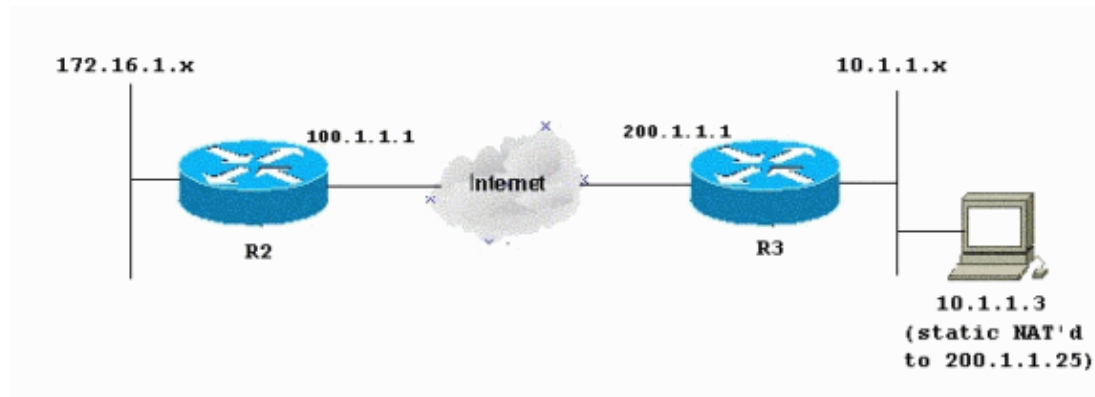
Configure

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:

- Router 2
- Router 3

R2 – Router Configuration
<pre> R2#write terminal Building configuration... Current configuration : 1412 bytes ! version 12.3 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname R2 ! boot-start-marker boot-end-marker ! ! </pre>

```
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
!
!
crypto isakmp policy 10
  authentication pre-share
!
crypto isakmp key ciscokey address 200.1.1.1
!
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto map myvpn 10 ipsec-isakmp
  set peer 200.1.1.1
  set transform-set myset

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

match address 101
!
!
!
interface Ethernet0/0
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Ethernet1/0
 ip address 100.1.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 crypto map myvpn
!
ip classless
ip route 0.0.0.0 0.0.0.0 100.1.1.254
!
ip http server
no ip http secure-server
!

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

ip nat inside source list 175 interface Ethernet1/0 overload
!

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

access-list 101 permit ip 172.16.1.0 0.0.0.255 10.1.1.0 0.0.0.255

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

access-list 175 deny ip 172.16.1.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 175 permit ip 172.16.1.0 0.0.0.255 any
!
!
!
control-plane
!
!
```

```
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  login
!
end
```

R3 – Router Configuration

```
R3#write terminal
Building configuration...
Current configuration : 1630 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
!
crypto isakmp policy 10
  authentication pre-share
crypto isakmp key ciscokey address 100.1.1.1
!
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto map myvpn 10 ipsec-isakmp
  set peer 100.1.1.1
  set transform-set myset

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

match address 101
!
!
!
interface Ethernet0/0
  ip address 10.1.1.1 255.255.255.0
  ip nat inside
  ip virtual-reassembly
!
interface Ethernet1/0
  ip address 200.1.1.1 255.255.255.0
  ip nat outside
  ip virtual-reassembly
  crypto map myvpn
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 200.1.1.254
```

```

!
no ip http server
no ip http secure-server
!
!--- Except the private network from the NAT process:
ip nat inside source list 122 interface Ethernet1/0 overload
!--- Except the static-NAT traffic from the NAT process if destined
!--- over the encrypted tunnel:
ip nat inside source static 10.1.1.3 200.1.1.25 route-map nonat
!
access-list 101 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
!--- Except the private network from the NAT process:
access-list 122 deny ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 122 permit ip 10.1.1.0 0.0.0.255 any
!--- Except the static-NAT traffic from the NAT process if destined
!--- over the encrypted tunnel:
access-list 150 deny ip host 10.1.1.3 172.16.1.0 0.0.0.255
access-list 150 permit ip host 10.1.1.3 any
!
route-map nonat permit 10
 match ip address 150
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end

```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

Use this section to troubleshoot your configuration.

Refer to IP Security Troubleshooting – Understanding and Using debug Commands for additional information.

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 sa** Displays the IPsec negotiations of Phase 2.
 - **debug crypto isakmp sa** See the ISAKMP negotiations of Phase 1.
 - **debug crypto engine** Displays the encrypted sessions.
-

Related Information

- **[IPsec Negotiation/IKE Protocols – Cisco Systems](#)**
 - **[Technical Support & Documentation – 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.](#)

Updated: Jun 05, 2006

Document ID: 14144
