



L2TP—IPSec Support for NAT and PAT Windows Clients

The L2TP—IPSec Support for NAT and PAT Windows Clients feature allows more than one Windows client to connect to a Layer 2 Tunneling Protocol (L2TP) Network Server (LNS) at one time with IP Security (IPSec) enabled and a network address translation (NAT) or port address translation (PAT) server between the Windows client and LNS.

Currently, if one Windows client is connected to a Cisco IOS LNS router through a NAT or PAT server with IPSec enabled, and then another Windows client connects to the same Cisco IOS LNS router, the first client's connection is effectively terminated. Enabling L2TP—IPSec Support for NAT and PAT Windows Clients ensures that Windows client connections in this environment are established and maintained until the connection is closed.

History for the L2TP—IPSec Support for NAT and PAT Windows Clients Feature

Release	Modification
12.3(11)T4	This feature was introduced.
12.4(1)	This feature was integrated into Release 12.4(1).

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for L2TP—IPSec Support for NAT and PAT Windows Clients, page 2](#)
- [Restrictions for L2TP—IPSec Support for NAT and PAT Windows Clients, page 2](#)
- [Information About L2TP—IPSec Support for NAT and PAT Windows Clients, page 2](#)
- [How to Enable L2TP—IPSec Support for NAT and PAT Windows Clients, page 4](#)
- [Configuration Examples for L2TP—IPSec Support for NAT and PAT Windows Clients, page 6](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

REVIEW DRAFT—CISCO CONFIDENTIAL

- [Additional References, page 8](#)
- [Command Reference, page 10](#)

Prerequisites for L2TP—IPSec Support for NAT and PAT Windows Clients

- You have an environment consisting of Windows clients and Cisco IOS LNS routers with IPSec enabled and a NAT or PAT server between the Windows client and LNS router.
- You must have a version of IPSec that contains the L2TP—IPSec Support for NAT and PAT Windows Clients feature.
- You must understand Windows 2000 concepts and configuration requirements.
- You must understand Cisco IOS LNS routers concepts and configuration requirements.
- You must understand NAT and PAT concepts and configuration requirements.
- You must understand IPSec concepts and configuration requirements.
- You must understand L2TP concepts and configuration requirements.

Restrictions for L2TP—IPSec Support for NAT and PAT Windows Clients

- Tested only with Windows 2000 L2TP/IPsec clients running hotfix 818043.
- Port translation is not a standard default behavior. Port translation is incompatible with standard IPSec because it changes the LNS header port information.
- L2TP requires the client to have Microsoft DUN configured. L2TP is supported solely by Windows 2000 MS-DUN (L2TP is not supported by Windows 95, Windows 98, or Windows NT).

Information About L2TP—IPSec Support for NAT and PAT Windows Clients

To use the L2TP—IPSec Support for NAT and PAT Windows Clients feature, the following concept should be understood:

- [How L2TP—IPSec Support for NAT and PAT Windows Clients Works, page 2](#)

How L2TP—IPSec Support for NAT and PAT Windows Clients Works

With the L2TP—IPSec Support for NAT and PAT Windows Clients feature not enabled, Windows clients lose connection with the Cisco IOS LNS router when another Windows client establishes an IPSec-protected L2TP tunnel to the Cisco IOS LNS router when IPSec is enabled and there is a NAT or PAT server between the Windows clients and the LNS.

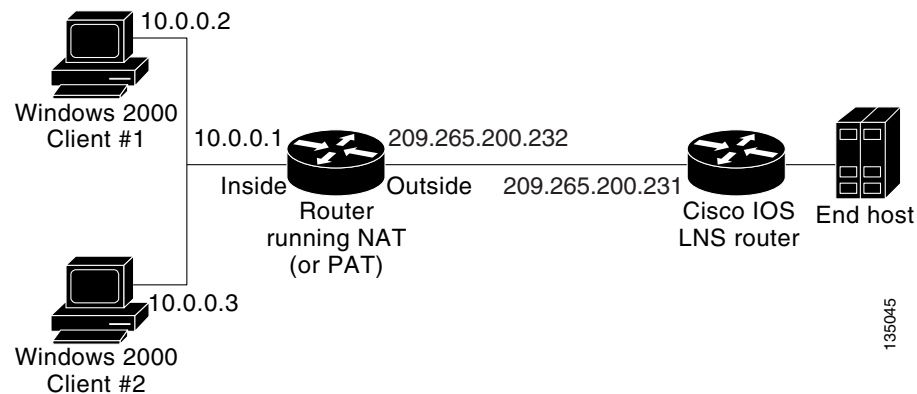
REVIEW DRAFT—CISCO CONFIDENTIAL**Note**

If you do not have IPSec enabled, or you do not have a NAT or PAT server, you can have multiple Windows clients connect to a LNS without this command enabled.

Without L2TP—IPSec Support for NAT and PAT Windows Clients Feature Enabled

For example, [Figure 1](#) shows two Windows 2000 clients that are trying to connect to the end host through the router running NAT or PAT and the same Cisco IOS LNS router. IPSec is enabled.

Figure 1 Multiple Windows 2000 Clients, NAT Router, and Cisco IOS LNS Router with IP Addresses



The Windows 2000 Client #1 establishes an IPSec-protected L2TP tunnel to the Cisco IOS LNS router. The Windows 2000 client and the Cisco IOS LNS router recognize that there is a router running NAT between them and IPSec and NAT-Traversal (NAT-T) are enabled. The Windows 2000 client attempts to establish an IPSec security association (SA) and requests transport mode (which it does by default) with proxies from 10.0.0.2, its local address, to 209.265.200.231, the Cisco IOS LNS router's address.

In transport mode NAT, running on the router, translates all outgoing connections (including 10.0.0.2) to its outside IP address (209.265.200.232), the address the traffic will come in on. However, NAT cannot modify the L2TP port designation (1701), which is protected by the IPSec encrypted area. So now, we have a local address of 209.265.200.231, a remote address of 209.265.200.232 and a remote port of 1701. All traffic is sent to the Windows 2000 Client #1 that matches the tunnel 209.265.200.231, port 1701.

Then Windows 2000 Client #2 establishes an IPSec-protected L2TP tunnel to the Cisco IOS LNS router, again in transport mode. And NAT, again, translates all outgoing connections to its outside IP address (209.265.200.232), but it cannot modify the L2TP port designation (1701). All traffic is now sent to Windows 2000 Client #2 that matches tunnel 209.265.200.231, port 1701. This second Windows client connection has effectively ended Windows Client #1's connection to the Cisco IOS LNS router since it is no longer receiving traffic.

With L2TP—IPSec Support for NAT and PAT Windows Clients Feature Enabled

With the L2TP—IPSec Support for NAT and PAT Windows Clients feature enabled, IPSec can translate the L2TP ports after decryption. This feature allows IPSec to map traffic from different hosts to different source ports. L2TP can now distinguish between traffic destined for multiple Windows 2000 clients.

So now, when an SA is created, a translated port will be assigned to it. This port is client-specific. The same port will be used for any new SA created by that client. When an encrypted request is received and decrypted, the source port is translated from the standard value, 1701, to a client specific value. The request with the translated port is then forwarded to L2TP.

REVIEW DRAFT—CISCO CONFIDENTIAL

As shown in [Figure 1](#) with port translation enabled, the Windows 2000 Client #1 would have a translated port number of 1024 assigned and Windows 2000 Client #2 would have a translated port number of 1025 assigned.

When L2TP sends the reply packet, it uses the translated port number and creates a packet to that destination port. IPSec uses the destination port number to select the SA with which to encrypt the packet. Before encrypting the packet, IPSec translates the destination port back to the standard port number, 1701, which the Windows 2000 client expects. IPSec encrypts the packet, either with the SA to Windows 2000 Client #1 if the destination port was 1024 or with the SA to Windows 2000 Client #2 if the destination port was 1025. And now, all traffic is sent to the appropriate client and multiple Windows clients can be connected to a Cisco IOS LNS router through a NAT server at the same time.

The connection is maintained until one of the following actions occurs:

- The IPSec connection is closed.
- The NAT or PAT device ends the session.
- The LNS closes the session.
- The Windows client closes the session.

How to Enable L2TP—IPSec Support for NAT and PAT Windows Clients

This section contains the following procedure that allows you to enable NAT/PAT port translation:

- [Enabling L2TP—IPSec Support, page 4](#)

Enabling L2TP—IPSec Support

Use the following task to enable L2TP—IPSec Support for NAT and PAT Windows Clients for environments that have IPSec enabled and include multiple windows clients, a NAT or PAT server, L2TP, and a Cisco IOS LNS router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* [**ipsec-isakmp**]
or
crypto dynamic-map *dynamic-map-name dynamic-seq-num*

REVIEW DRAFT—CISCO CONFIDENTIAL

4. **set nat demux**
5. **exit**
6. **exit**
7. **show crypto map** [*interface interface* | **tag map-name**]
or
show crypto dynamic-map [**tag map-name**]
8. **show crypto ipsec sa**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto map <i>map-name seq-num</i> [ipsec-isakmp] Example: Router(config)# crypto map STATIC_MAP 5 or crypto dynamic-map <i>dynamic-map-name</i> <i>dynamic-seq-num</i> Example: Router(config)# crypto dynamic-map DYNAMIC_MAP 10	Names the static crypto map entry to create (or modify) and enters crypto map configuration mode. or Names the dynamic crypto map entry to create (or modify) and enters crypto map configuration mode.
Step 4	set nat demux Example: Router(config-crypto-map)# set nat demux	Enables L2TP—IPSec support.
Step 5	exit Example: Router(config-crypto-map)# exit	Exits crypto map configuration mode and returns to global configuration mode.
Step 6	exit Example: Router(config)# exit	Exits global configuration mode and returns to privileged EXEC mode.

REVIEW DRAFT—CISCO CONFIDENTIAL

	Command or Action	Purpose
Step 7	<pre>show crypto map [interface interface tag map-name]</pre> <p>Example: Router# show crypto map</p> <p>or</p> <pre>show crypto dynamic-map [tag map-name]</pre> <p>Example: Router# show crypto dynamic-map</p>	<p>(Optional) Displays information about crypto map configuration.</p> <p>or</p> <p>(Optional) Displays information about dynamic crypto map configuration.</p>
Step 8	<pre>show crypto ipsec sa</pre> <p>Example: Router# show crypto ipsec sa</p>	<p>(Optional) Displays the settings used by current SAs.</p>

Configuration Examples for L2TP—IPSec Support for NAT and PAT Windows Clients

This section provides the following configuration example:

- [Dynamic Map Configuration: Example, page 6](#)

Dynamic Map Configuration: Example

The following example shows how to enable the L2TP—IPSec Support for NAT and PAT Windows Clients feature for a dynamic crypto map:

```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 72_LNS
!
boot-start-marker
boot-end-marker
!
aaa new-model
!
!
aaa authentication ppp default local
aaa session-id common
ip subnet-zero
!
!
no ip cef
no ip domain lookup
ip domain name cisco.com
```

REVIEW DRAFT—CISCO CONFIDENTIAL

```

ip dhcp excluded-address 20.0.0.8
ip dhcp excluded-address 20.0.0.10
!
!
ip vrf VPN
  rd 1:1
!
!Enable virtual private networking.
vpdn enable
vpdn ip udp ignore checksum
!
! Default L2TP VPDN group
vpdn-group L2TP
!
!Enables the LNS to accept dial in requests; specifies L2TP as the tunneling
!protocol; specifies the number of the virtual templates used to clone
!virtual-access interfaces
  accept-dialin
    protocol l2tp
    virtual-template 1

!Disables L2TP tunnel authentication.
no l2tp tunnel authentication
!
!
crypto keyring L2TP
  pre-shared-key address 0.0.0.0 0.0.0.0 key *****
!
!Defines an Internet Key Exchange (IKE) policy and assigns priority 1.
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
  lifetime 3600
!
crypto isakmp key cisco hostname w2k01
crypto isakmp keepalive 3600
!
crypto ipsec security-association lifetime seconds 600
!
!Defines a transform set.
crypto ipsec transform-set TS1 esp-3des esp-sha-hmac
  mode transport
!
!Names the dynamic crypto map entry and enters crypto map configuration mode; Enables
!L2TP—IPSec support; Specifies which transform sets can be used with the crypto map
!entry
crypto dynamic-map DYN_MAP 10
  set nat demux
  set transform-set TS1!
!
crypto map CRYP_MAP 6000 ipsec-isakmp dynamic DYN_MAP
!
interface Loopback0
  ip address 12.0.0.8 255.255.255.255
!
interface FastEthernet0/0
  ip address 11.0.0.8 255.255.255.0
  no ip route-cache
  duplex full
  speed 100
  crypto map CRYP_MAP
!

```

REVIEW DRAFT—CISCO CONFIDENTIAL

```

interface FastEthernet0/1
 ip address 20.0.0.8 255.255.255.0
 duplex full
 speed 100
!
interface FastEthernet2/0
 ip address 172.19.192.138 255.255.255.0
 duplex full
!
interface Virtual-Template1
 ip unnumbered Loopback0
 peer default ip address pool POOL
 ppp mtu adaptive
 ppp authentication chap ms-chap
!
router ospf 1
 log-adjacency-changes
 redistribute static subnets
 network 11.0.0.0 0.0.0.255 area 0
!
ip local pool POOL 20.0.0.100 20.0.0.110
ip classless
ip route 171.0.0.0 255.0.0.0 172.19.192.1
!
no ip http server
no ip http secure-server
!
!
control-plane
!
gatekeeper
 shutdown!
!
line con 0
 exec-timeout 0 0
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
!
end

```

Additional References

The following sections provide references related to L2TP—IPSec Support for NAT and PAT Windows Clients.

Related Documents

Related Topic	Document Title
IP Security and Encryption Overview	Cisco IOS Security Configuration Guide , Release 12.3
Configuring IPSec Network Security	Cisco IOS Security Configuration Guide , Release 12.3

REVIEW DRAFT—CISCO CONFIDENTIAL**Standards**

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

REVIEW DRAFT—CISCO CONFIDENTIAL

Command Reference

This section documents the following command only.

- [set nat demux](#)

REVIEW DRAFT—CISCO CONFIDENTIAL

set nat demux

To enable L2TP—IPSec support for NAT or PAT Windows clients, use the **set nat demux** command in crypto map configuration mode. To disable L2TP—IPSec support, use the **no** form of this command.

set nat demux

no set nat demux

Syntax Description

This command has no arguments or keywords.

Command Default

With this command disabled, Windows clients lose connection when another Windows client establishes an IP Security (IPSec) protected Cisco IOS Layer 2 Tunneling Protocol (L2TP) tunnel to the same Cisco IOS L2TP Network Server (LNS) when there is a network address translation (NAT) or port address translation (PAT) server between the Windows clients and the LNS.

Command Modes

Crypto map configuration

Command History

Release	Modification
12.3(11)T4	This command was introduced.
12.4(1)	This command was integrated into Release 12.4(1).

Usage Guidelines

Use this command if you have an environment with IPSec enabled and consisting of an LNS, and a network address translation (NAT) or port address translation (PAT) server between the Windows clients and the LNS.

This command has been tested only with Windows 2000 L2TP/IPsec clients running hotfix 818043.

You must enter the **crypto map** command if you are using static crypto maps or the **crypto dynamic-map** command if you are using dynamic crypto maps before issuing the **set nat demux** command.

**Note**

If you do not have IPSec enabled, or you do not have a NAT or PAT server, you can have multiple Windows clients connect to a LNS without this command enabled.

Examples

The following example shows how to enable L2TP—IPSec support for NAT or PAT Windows clients for a dynamic crypto map:

```
.
.
.
!Enable virtual private networking.
vpdn enable

! Default L2TP VPDN group
```

REVIEW DRAFT—CISCO CONFIDENTIAL

```

vpdn-group 1
!
!Enables the LNS to accept dial in requests; specifies L2TP as the tunneling
protocol; specifies the number of the virtual templates used to clone
virtual-access interfaces; specifies an alternate IP address for a VPDN tunnel
accept-dialin.
  protocol l2tp
  virtual-template 1
  source-ip 10.0.0.1
!
!Disables Layer 2 Tunneling Protocol (L2TP) tunnel authentication.
no l2tp tunnel authentication
!
!Defines an Internet Key Exchange (IKE) policy and assigns priority 1.
crypto isakmp policy 1
  encr 3des
  group 2
!
crypto isakmp policy 2
  encr 3des
  authentication pre-share
  group 2
!
!Defines a transform set.
crypto ipsec transform-set vpn esp-3des esp-md5-hmac
  mode transport
crypto mib ipsec flowmib history tunnel size 2
crypto mib ipsec flowmib history failure size 2
!
!Names the dynamic crypto map entry to create (or modify) and enters crypto map
configuration mode.
crypto dynamic-map dyn_map 1
!Specifies which transform sets can be used with the crypto map entry
  set transform-set vpn
!Enables L2TP-IPSec support.
  set nat demux
.
.
.

```

Related Commands

Command	Description
crypto dynamic-map	Names the dynamic crypto map entry to create (or modify) and enters crypto map configuration mode.
crypto map	Names the static crypto map entry to create (or modify) and enters crypto map configuration mode.
show crypto dynamic-map	Displays information about dynamic crypto maps.
show crypto ipsec sa	Displays the settings used by current SAs.
show crypto map	Displays information about static crypto maps.

REVIEW DRAFT—CISCO CONFIDENTIAL

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2005 Cisco Systems, Inc. All rights reserved

REVIEW DRAFT—CISCO CONFIDENTIAL