

Configuring IPsec Over ADSL on a Cisco 2600/3600 With ADSL-WIC and Hardware Encryption Modules

Document ID: 12908

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configurations

Caveats

Verify

Troubleshoot

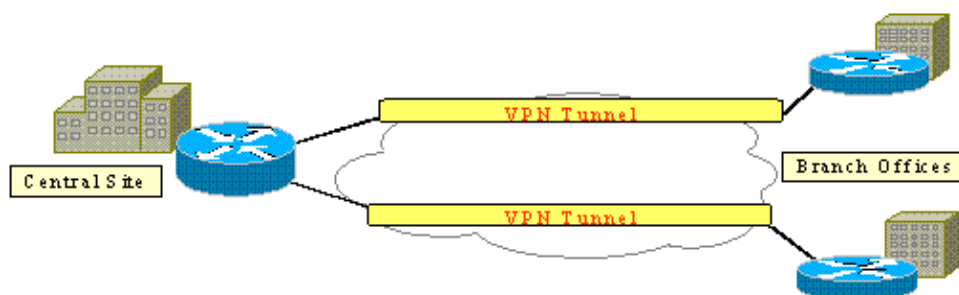
- Troubleshoot Commands

Summary

Related Information

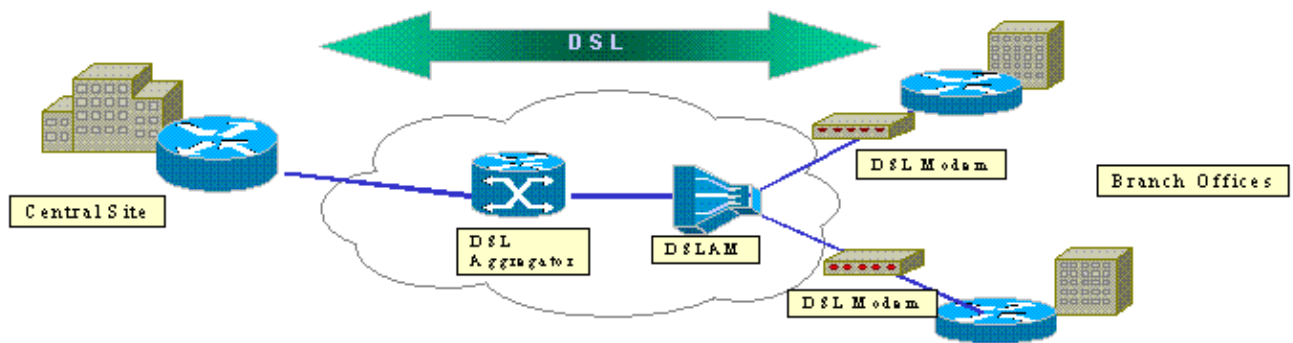
Introduction

As the Internet expands, branch offices demand that their connections to central sites are both reliable and secure. Virtual Private Networks (VPNs) protect information between remote offices and central sites as it travels across the Internet. IP Security (IPsec) can be used to guarantee that the data that passes across these VPNs is encrypted. The encryption provides another layer of network security.



This figure shows a typical IPsec VPN. A number of remote access and site-to-site connections are involved between branch offices and central sites. Usually, traditional WAN links such as Frame Relay, ISDN, and modem dialup are provisioned between the sites. These connections can involve an expensive one-time provisioning fee and expensive monthly charges. Also, for ISDN and modem users, there can be long connect times.

Asymmetric digital subscriber line (ADSL) offers an always-on, low-cost alternative to these traditional WAN links. IPsec encrypted data over an ADSL link offers a secure and reliable connection and saves customers money. A traditional ADSL customer premises equipment (CPE) set up in a branch office requires an ADSL modem that connects to a device that originates and terminates IPsec traffic. This figure shows a typical ADSL network.



The Cisco 2600 and 3600 routers support the ADSL WAN interface card (WIC-1ADSL). This WIC-1ADSL is a multi-service and remote access solution designed to meet the needs of a branch office. The introduction of the WIC-1ADSL and hardware encryption modules accomplishes the demand for IPsec and DSL in a branch office in a single router solution. The WIC-1ADSL eliminates the need for a separate DSL modem. The hardware encryption module provides up to ten times the performance over software-only encryption as it offloads the encryption that processes from the router.

For more information on these two products, refer to ADSL WAN Interface Cards for the Cisco 1700, 2600, and 3700 Series Modular Access Routers and Virtual Private Network Modules for the Cisco 1700, 2600, 3600, and 3700 Series.

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 2600/3600 Series Routers:

- Cisco IOS® Software Release 12.1(5)YB Enterprise PLUS 3DES Feature Set
- DRAM 64 MB for the Cisco 2600 series, DRAM 96 MB for the Cisco 3600 series
- Flash 16 MB for the Cisco 2600 series, Flash 32 MB for the Cisco 3600 series
- WIC-1 ADSL
- Hardware Encryption Modules
 - ◆ AIM-VPN/BP and AIM-VPN/EP for the Cisco 2600 series
 - ◆ NM-VPN/MP for the Cisco 3620/3640
 - ◆ AIM-VPN/HP for the Cisco 3660

Cisco 6400 Series:

- Cisco IOS Software Release 12.1(5)DC1
- DRAM 64 MB
- Flash 8 MB

Cisco 6160 Series:

- Cisco IOS Software Release 12.1(7)DA2
- DRAM 64 MB
- Flash 16 MB

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you work in a live network, ensure that you understand the potential impact of any command before you use it.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Configure

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

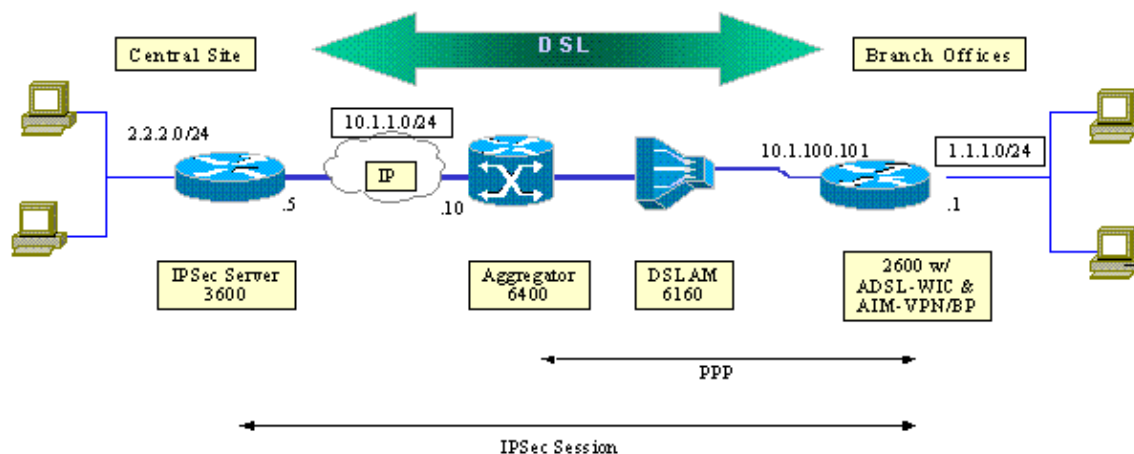
Note: In order to find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only).

Network Diagram

This document uses the network setup shown this diagram.

This test simulates an IPsec VPN connection that uses ADSL in a typical branch office environment.

The Cisco 2600/3600 with the ADSL-WIC and hardware encryption module trains up to a Cisco 6160 digital subscriber line access multiplexer (DSLAM). The Cisco 6400 is used as an aggregation device that terminates a PPP session that initiates from the Cisco 2600 router. The IPsec tunnel originates at the CPE 2600 and terminates at the Cisco 3600 in the central office, the IPsec headend device in this scenario. The headend device is configured to accept connections from any client instead of individual peering. The headend device is also tested with only pre-shared keys and 3DES and Edge Service Processor (ESP)-Secure Hash Algorithm (SHA)-Hash-based Message Authentication Code (HMAC).



Configurations

This document uses these configurations:

- Cisco 2600 Router
- IPSec Headend Device – Cisco 3600 Router
- Cisco 6160 DSLAM
- Cisco 6400 Node Route Processor (NRP)

Note these points about the configurations:

- A pre-shared key is used. In order to set up IPSec sessions to multiple peers, you must define multiple key definition statements or you need to configure a dynamic crypto map. If all the sessions share a single key, you must use a peer address of 0.0.0.0.
- The transform set can be defined for ESP, Authentication Header (AH), or both for double authentication.
- At least one crypto policy definition must be defined per peer. The crypto maps decide the peer to use to create the IPSec session. The decision is based on the address match defined in the access list. In this instance, it is access-list 101.
- The crypto maps must be defined for both the physical interfaces (interface ATM 0/0 in this case) and the virtual-template.
- The configuration presented in this document discusses only an IPSec tunnel over a DSL connection. Additional security features are probably needed in order to ensure that your network is not vulnerable. These security features can include additional access-control lists (ACLs), Network Address Translation (NAT), and the use of a firewall with an external unit or an IOS firewall feature set. Each of these features can be used in order to restrict non-IPSec traffic to and from the router.

```
Cisco 2600 Router
crypto isakmp policy 10
!--- Defines the ISAKMP parameters to be negotiated.
authentication pre-share
!--- Defines the pre-shared key to be exchanged with the peer.
crypto isakmp key pre-shared address 10.1.1.5
!
crypto ipsec transform-set strong esp-des esp-sha-hmac
!--- Defines the transform set for ESP and/or AH.
!
crypto map vpn 10 ipsec-isakmp
set peer 10.1.1.5
set transform-set strong
match address 102
!--- Defines the crypto policy that includes the peer IP address,
!--- transform set that is used, as well as the access list
!--- that defines the packets that are encrypted.
!
interface ATM0/0
no ip address
atm vc-per-vp 256
no atm ilmi-keepalive
dsl operating-mode auto
no fair-queue
```

```

!
interface ATM0/0.1 point-to-point
pvc 0/35
    encapsulation aal5mux ppp dialer
    dialer pool-member 1
    !
    crypto map vpn

!--- Applies the crypto map to the ATM sub-interface.

!
interface FastEthernet0/1
ip address 1.1.1.1 255.255.255.0
duplex 100
speed full
!
interface Dialer1
ip address 10.1.100.101 255.255.255.0
dialer pool 1
encapsulation ppp
ppp pap sent-username 2621a password 7 045802150C2E
crypto map vpn

!--- Applies the crypto map to the Dialer interface.

!
ip classless
!
ip route 2.2.2.0 255.255.255.0 10.1.1.5
ip route 10.1.1.0 255.255.255.0 10.1.100.1

!--- Static routes between 2600 CPE and IPSec server.

ip route 0.0.0.0 0.0.0.0 Dialer1
!
access-list 102 permit ip 1.1.1.0 0.0.0.255 2.2.2.0 0.0.0.255

!--- Access list that defines the addresses that are encrypted.

!
end

```

IPSec Headend Device – Cisco 3600 Router

```

crypto isakmp policy 10

!--- Defines the ISAKMP parameters to be negotiated.

authentication pre-share

!--- Defines the pre-shared key to be exchanged with the peer.

crypto isakmp key pre-shared address 10.1.100.101
!
crypto ipsec transform-set strong esp-des esp-sha-hmac

!--- Defines the transform set for ESP and/or AH.

!
crypto map vpn 10 ipsec-isakmp
set peer 10.1.100.101
set transform-set strong
match address 102

!--- Defines the crypto policy that includes the peer IP address,

```

```

!--- transform set that are used, and the access list
!--- that defines the packets to be encrypted.

!
interface FastEthernet0/0
 ip address 10.1.1.5 255.255.255.0
 duplex 100
 speed full
 crypto map vpn

!--- Applies the crypto map to the Fast Ethernet interface.

!
interface FastEthernet0/1
 ip address 2.2.2.1 255.255.255.0
 speed full
 full-duplex
!
ip route 1.1.1.0 255.255.255.0 10.1.1.10
ip route 10.1.100.0 255.255.255.0 10.1.1.10
!
access-list 102 permit ip 2.2.2.0 0.0.0.255 1.1.1.0 0.0.0.255

!--- Access list that defines the addresses to be encrypted.

!
end

```

Cisco 6160 DSLAM

```

dsl-profile full
 dmt bitrate maximum fast downstream 10240 upstream 1024
 dmt bitrate maximum interleaved downstream 0 upstream 0
 !
 atm address 47.0091.8100.0000.0004.6dd6.7c01.0004.6dd6.7c01.00
 atm router pnni
 no aesa embedded-number left-justified
 none 1 level 56 lowest
 redistribute atm-static
 !
 interface atm0/0
 no ip address
 atm maxvp-number 0
 atm maxvc-number 4096
 atm maxvci-bits 12
 !
 interface atm 1/2
 no ip address
 dsl profile full
 no atm ilmi-keepalive
 atm soft-vc 0 35 dest-address
 47.0091.8100.0000.0004.c12b.cd81.4000.0c80.8000.00 0 36
 rx-cttr 1 tx-cttr 1

!--- The previous two lines need to be on one line.
!--- The network service access point (NSAP)
!--- address comes from the NSP on the Cisco 6400. Issue
!--- a show atm address command.

!

```

Cisco 6400 NRP

```

!
username cisco password cisco

```

```

!
vc-class atm pppoa
 encapsulation aal5mux ppp Virtual-templatel
!
interface loopback 0
 ip address 10.1.100.1 255.255.255.0
!
interface atm 0/0/0
 no ip address
 no ip route-cache
 no ip mroute-cache
 no atm auto-configuration
 atm ilmi-keepalive 10
 pvc 0/16 ilmi
!
hold-queue 1000 in
!
interface atm 0/0/0.1 multipoint
 no ip route-cache
 no ip mroute-cach
 class-int pppoa
 pvc 0/36
!
interface fast 0/0/0
 ip address 10.1.1.10 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 half-duplex
!
interface Virtual-Templatel
 ip unnumbered Loopback0
 no ip route-cache
 peer default ip address pool pppoa
 ppp authentication pap chap
 ppp ipcp accept-address
 ppp multilink
 no ppp multilink fragmentation
!
 ip local pool pppoa 10.1.100.2 10.1.100.100
!

```

Caveats

ADSL connections can be configured with a virtual-template or a dialer interface.

A dialer interface is used in order to configure the DSL CPE to receive an address from the service provider (IP address is negotiated). A virtual-template interface is a down-down interface and does not support the negotiated address option, which is necessary in the DSL environment. Virtual-template interfaces were initially implemented for DSL environments. Currently a dialer interface is the recommended configuration on the DSL CPE side.

Two issues are found at the time of the configuration of dialer interfaces with IPsec:

- Cisco bug ID CSCdu30070 (registered customers only) Software-only IPsec over DSL: input queue wedge on DSL dialer interface.
- Cisco bug ID CSCdu30335 (registered customers only) Hardware-based IPsec over DSL: input queue wedge on dialer interface.

The current workaround for both of these issues is to configure the DSL CPE with the use of the virtual-template interface as described in the configuration.

Fixes for both of these issues are planned for Cisco IOS Software Release 12.2(4)T. After this release, an updated version of this document is posted in order to show the dialer interface configuration as another option.

Verify

This section provides the information you can use in order to confirm that your configuration works properly.

Several **show** commands can be used in order to verify that the IPSec session is established between the peers. The commands are necessary only on the IPSec peers, in this case the Cisco 2600 and 3600 series.

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

- **show crypto engine connections active** Shows each Phase 2 SA built and the amount of traffic sent.
- **show crypto ipsec sa** Shows IPSec SA built between peers.

This is sample command output for the **show crypto engine connections active** command.

show crypto engine connections active

| ID | Interface | IP-Address | State | Algorithm | Encrypt | Decrypt |
|-----|------------------|--------------|-------|--------------------|---------|---------|
| 1 | <none> | <none> | set | HMAC_SHA+DES_56_CB | 0 | 0 |
| 200 | Virtual-Templat1 | 10.1.100.101 | set | HMAC_SHA | 0 | 4 |
| 201 | Virtual-Templat1 | 10.1.100.101 | set | HMAC_SHA | 4 | 0 |

This is sample command output for the **show crypto ipsec sa** command.

show crypto ipsec sa

```
Interface: Virtual-Templat1
Crypto map tag: vpn, local addr. 10.1.100.101

Local ident (addr/mask/prot/port): (1.1.1.0/255.255.255.0/0/0)
Remote ident (addr/mask/prot/port): (2.2.2.0/255.255.255.0/0/0)
Current_peer: 10.1.1.5
PERMIT, flags= {origin_is_acl,}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr failed: 0, #pkts decompress failed: 0
#send errors 11, #recv errors 0

local crypto endpt: 10.1.100.101, remote crypto endpt.: 10.1.1.5
path mtu 1500, media mtu 1500
current outbound spi: BB3629FB

inbound esp sas:
spi: 0x70C3B00B(1891872779)
transform: esp-des, esp-md5-hmac
in use settings = {Tunnel,}
slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn
sa timing: remaining key lifetime (k/sec): (4607999/3446)
IV size: 8 bytes
Replay detection support: Y

Inbound ah sas:

Inbound pcp sas:

Outbound esp sas:
```

```
Spi: 0xBB3629FB(3140889083)
Transform: esp-des, esp-md5-hmac
In use settings = {Tunnel,}
Slot:0, conn id: 2001, flow_id: 2, crypto map: vpn
Sa timing: remaining key lifetime (k/sec): (4607999/3446)
IV size: 8bytes
Replay detection support: Y
```

Outbound ah sas:

Outbound pcp sas:

Troubleshoot

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

The "Modem state = 0x8" message which is reported by the **debug atm events** command usually means that the WIC1-ADSL is unable to receive Carrier Detect from the connected DSLAM. In this situation, the customer needs to check that the DSL signal is provisioned on the middle two wires relative to the RJ11 connector. Some Telcos provision the DSL signal on the outside two pins instead.

Troubleshoot 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 you issue **debug** commands, refer to the Important Information on Debug Commands.



Caution: Do not run debugging on a live network. The volume of information that displays can overload your router to the point where no data flows and CPUHOG messages are issued.

- **debug crypto IPsec** Displays IPsec events.
- **debug crypto Isakmp** Displays messages about IKE events.

Summary

Implementation of IPsec over an ADSL connection provides a secure and reliable network connection between branch offices and central sites. The use of the Cisco 2600/3600 series with the ADSL-WIC and hardware encryption modules offers lower cost of ownership to the customer as ADSL and IPsec can now be accomplished in a single router solution. The configuration and caveats listed in this paper need to serve as a basic guideline to set up this type of connection.

Related Information

- **An Introduction to IP Security (IPsec) Encryption**
 - **Cisco 2600 Series Routers**
 - **Virtual Private Networks**
 - **DSL and LRE Technical Support**
 - **Universal Gateways and Access Servers Products Support Pages**
 - **Dial Technology Support Pages**
 - **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.](#)

Updated: Jan 10, 2006

Document ID: 12908
