L2F Case Study Overview

Introduction

This case study describes how one Internet service provider (ISP) plans, designs, and implements an access virtual private network (VPN) by using Layer 2 Forwarding (L2F) as the tunneling protocol. L2F forwards Point-to-Point (PPP) sessions from one router to another router across a shared network infrastructure.

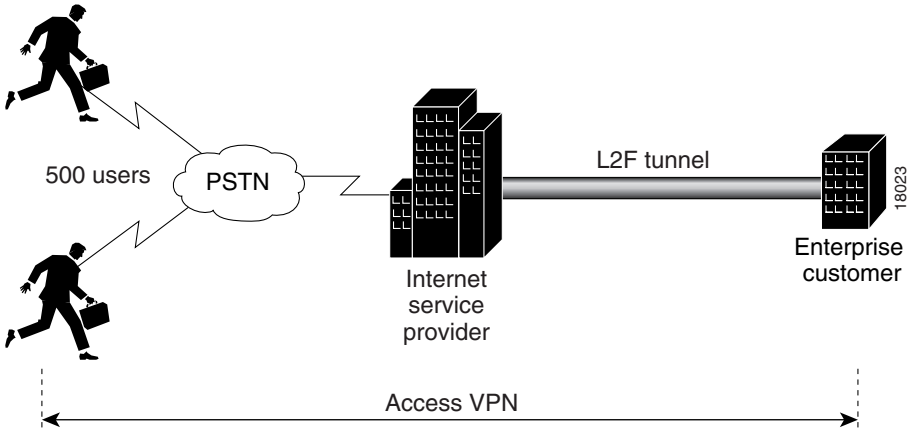
This case study is primarily intended for network administrators and operations teams working for ISPs who provide access VPN services to enterprise customers. This case study is also useful to enterprise customers who want to establish access VPNs.

This access VPN:

- Enables remote employees to access the enterprise customer's intranet resources when and where they want to
- Allows enterprise customer's networks to span from an intranet to remote clients who are connected to analog modems

Figure 6 shows an enterprise customer with a specific business objective. The enterprise customer wants to give 500 users dial-up modem access to intranet resources through the public switched telephone network (PSTN). To do this, the enterprise customer contracts with an ISP who is responsible for the required dial hardware and wide-area network (WAN) services. The ISP and enterprise customer decide to use L2F, because it is a stable tunneling protocol supported by many vendors and client software applications.

Figure 6 End-to-End Access VPN Solution



The ISP:

- Purchases, configures, and maintains the network access server (NAS). The NAS is the point-of-presence (POP) used to forward PPP sessions to the enterprise customer's network.
- Supports and maintains in-house modem pools.
- Maintains an authentication, authorization, and accounting (AAA) server that authenticates the IP tunnel endpoint and domain name assigned to the enterprise customer's home gateway.
- Maintains an edge router that connects the ISP's network to the enterprise customer's network.

The enterprise customer:

- Purchases, configures, and maintains a home gateway and clients.
- Authenticates and authorizes remote users' usernames and passwords by using a AAA server.

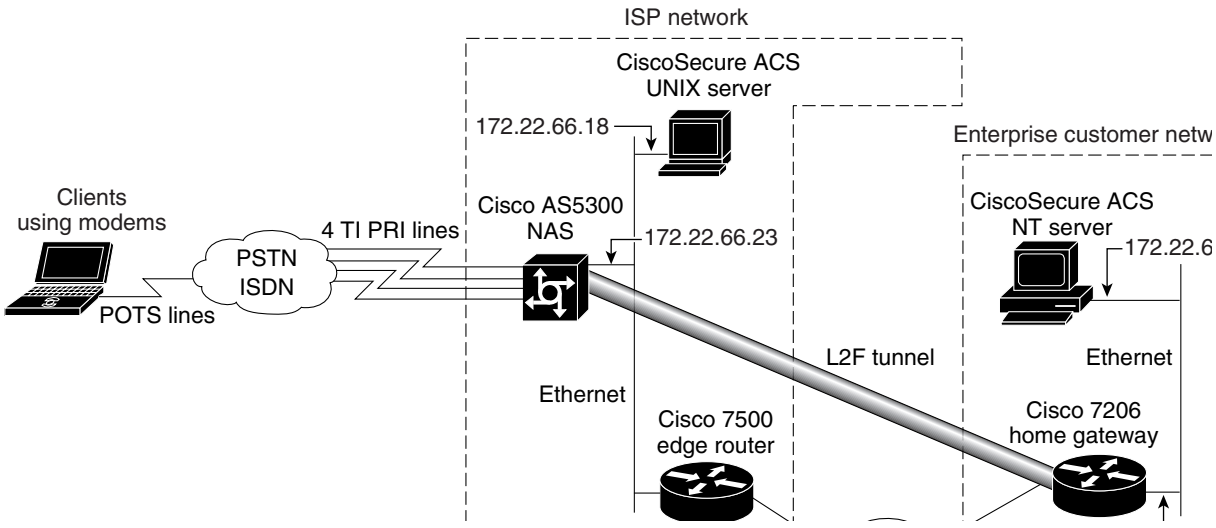
Note This case study illustrates one example of a NAS-initiated access VPN. Networks containing clients who initiate encrypted IP tunnels to home gateways are called client-initiated access VPNs.

Figure 7 shows the specific network devices used to build the access VPN in this case study.

- The ISP is responsible for a Cisco AS5300 network access server, a CiscoSecure ACS UNIX server, and a Cisco 4500-M edge router.
- The enterprise customer is responsible for a Cisco 7206 home gateway, a CiscoSecure ACS NT server, and the remote clients using modems.

The L2F tunnel runs between the Cisco AS5300 and Cisco 7206. The L2F tunnel is forwarded across a Frame Relay network.

Figure 7 Access VPN Case Study Network Topology



This case study does not describe how to configure the edge router, the Frame Relay data network, or the serial interfaces on the home gateway. Although these components are shown in Figure 7, they are not critical in understanding how to build an access VPN solution and are outside the scope of this case study. For more information about how to configure Frame Relay and serial interfaces, refer to the *Wide-Area Networking Configuration Guide* for Cisco IOS Release 12.0.

See "Overview of Access VPNs and Tunneling Technologies" earlier in this document for an overview of access VPN solutions.

Device Characteristics

Table 4 provides a more detailed description of the hardware and software components used in the case study.

Table 4 Hardware and Software Used in the Case Study

	NAS	Home Gateway	CiscoSecure ACS UNIX Server	CiscoSecure ACS NT Server	Client
Chassis type	Cisco AS5300	Cisco 7206	Sun workstation	PC workstation	PC laptop
Physical interfaces	• 1 Ethernet interface • 4 T1 PRI ports • 96 terminal lines	• 1 Fast Ethernet interface • 4 serial interfaces	1 Ethernet interface	1 Ethernet interface	1 RJ-11 port
Hardware components	• Cisco AS5300 network access server • 96 MICA modems, 2 MICA CC and 1 Quad T1/PRI • T1 cable RJ45 to RJ45	• Cisco 7206, 6-slot chassis, 1 AC power supply • Cisco 7200 series input/output controller with Fast Ethernet • Cisco 7200 series network processing engine • 4-port serial port adapter, enhanced • V.35 cable, DTE, male, 10 feet	1 Ethernet card	1 Ethernet card	1 internal modem
Software loaded	• Cisco IOS Release 11.3(7)AA • Cisco AS5300 series IP	• Cisco IOS Release 12.0(2)T • Cisco 7200 series IP	• CiscoSecure ACS UNIX version 2.3.1 • Solaris 2.6	• CiscoSecure ACS NT version 2.1 • Windows NT 4.0	Windows 95
Telephone number or username	5550945[1]	N/A	N/A	N/A	jeremy@hgw.com password = subaru

Table 4 Hardware and Software Used in the Case Study (Continued)

	NAS	Home Gateway	CiscoSecure ACS UNIX Server	CiscoSecure ACS NT Server	Client
Memory	• Cisco AS5300 main DRAM upgrade (from 32 MB to 64 MB) • Cisco AS5300 system Flash upgrade (from 8 MB to 16 MB) • Cisco AS5300 boot Flash upgrade (from 4 MB to 8 MB)	• Cisco 7200 I/O PCMCIA Flash memory, 20 MB • Cisco 7200 NPE 64 MB DRAM upgrade kit	128 MB RAM 128 MB swap space	128 MB RAM	64 MB RAM
Ethernet IP Address	172.22.66.23 255.255.255.192	172.22.66.25 255.255.255.192	172.22.66.18 255.255.255.192	172.22.66.13 255.255.255.192	172.30.2.1[2]

1. This is the PRI telephone number assigned to the central site (NAS). The PRI number is often called the hunt group number, which distributes calls among the available B channels. Make sure your PRI provider assigns all four PRI trunks on the Cisco AS5300 to this number.
2. The home gateway dynamically assigns this IP address to the client in this case study.

Configuration Tasks

To build the access VPN, the ISP and enterprise customer must perform three major tasks to build the access VPN in this case study:

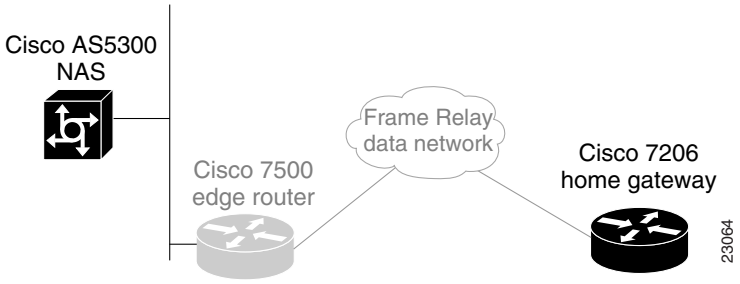
- Task 1—Configuring the NAS for Basic Dial Access
- Task 2—Configuring the Access VPN to Work with Local AAA
- Task 3—Configuring the Access VPN to Work with Remote AAA

Table 5 describes each task in more detail and identifies the devices related to each task.

A user named Jeremy with the username jeremy@hgw.com appears in many configurations, illustrations, and examples in this case study. The goal of the case study is to give Jeremy basic IP and modem services by forwarding his PPP session from the NAS to the home gateway. To help you understand how the various hardware and software components work together to forward the PPP session, follow Jeremy through the case study.

Note If you use this document to configure your own network, be sure to substitute your own IP addresses, passwords, usernames, hostnames, and telephone numbers.

Table 5 Relationship Between Configuration Tasks and Devices

Task	Description	Devices
1	Configuring the NAS for Basic Dial Access Performed by the ISP.	
2	Configuring the Access VPN to Work with Local AAA Performed by the ISP and the enterprise customer.	
3	Configuring the Access VPN to Work with Remote AAA Performed by the ISP and the enterprise customer.	ACS er CiscoSecure ACS NT server