

Compatible Systems Tech Notes: Ports and Protocols Necessary to Pass Through a Firewall with your LAN-to-LAN and Client VPN Tunnels

Document ID: 17638

Introduction

Prerequisites

Requirements

IP Protocols Necessary to Forward through a Firewall

UDP/TCP Ports Necessary to Forward through a Firewall

Related Information

Introduction

Forwarding VPN traffic through a Firewall depends on what Compatible Systems IntraPort Client software you use, what type of transforms are specified, and/or the type of LAN-to-LAN tunnel that is used. Both IP protocols and TCP/UDP ports must be opened in the Firewall.

Note: All Cisco routers must have a version 11.3 or later operating system in order to route IPsec traffic. Earlier versions do not route IPsec Protocols.

Prerequisites

Requirements

There are no specific requirements for this document.

IP Protocols Necessary to Forward through a Firewall

The IP protocols necessary to forward through a firewall are:

- **47 GRE (General Router Encapsulation)** This affects all STEP LAN-to-LAN tunnels without authentication or encryption. This type of LAN-to-LAN tunnel is compatible with non-IPsec tunnels offered in Cisco routers.
- **50 ESP (Encapsulating Security Payload)** All IKE 3.x clients if encryption is specified in the group's transform. All 2.x clients if encryption is specified in the VPN Group. 3.x and 2.x MAC clients only support ESP. Compatible Systems STEP LAN-to-LAN tunnels with encryption and no authentication. Also, IKE LAN-to-LAN tunnels where encryption is specified in the group's transform.
- **51 AH (Authentication Header)** All 3.x clients except for the MAC with authentication specified in the group's transform. All 2.x clients except for the MAC with authentication specified in the group. LAN-to-LAN STEP tunnels with authentication. Also, IKE LAN-to-LAN tunnels where authentication is specified in the group's transform.

UDP/TCP Ports Necessary to Forward through a Firewall

The UDP/TCP Ports necessary to forward through a firewall are:

- **UDP 500 ISAKMP (Internet Security Association Key Management Protocol)** All IKE Clients and LAN-to-LAN IKE tunnels require UDP Port 500 and their respective protocol to establish a tunnel. The IP protocols listed in this document also need to be considered. If the IntraPort traffic passes through a Firewall, then it needs to allow the same ports for the types of clients that attempt to connect with it.
- **TCP 80 (HTTP)** TCP port 80 is required to initiate communication between the IntraPort Client and the IntraPort Server when NAT (Network Address Translation) is used anywhere along the path between the two.

Note: This is relevant only for IntraPort Server software version 5.1 or later, and IntraPort Client version 3.3.0 or later.

Related Information

- **Technical Support & Documentation – Cisco Systems**

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jun 22, 2007

Document ID: 17638
