Virtual Private Networks and Internet Key Exchange for the Cisco VPN 5000 Concentrator Series

Contents

Introduction

Internet Key Exchange (IKE) is a standard method used to arrange secure, authenticated communications. The Cisco VPN 5000 Concentrator uses IKE to set up IPSec tunnels. These IPSec tunnels are the backbone of this product.

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:

- VPN 5000 Series Concentrator

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

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

IKE Tasks

IKE handles these tasks:

- Authentication
- Session Negotiation
- Key Exchange
- IPSec Tunnel Negotiation and Configuration

Authentication

Authentication is the most important task that IKE accomplishes, and it is the most complicated. Whenever you negotiate something, it is important to know with whom you negotiate. IKE can use one of several methods to authenticate negotiating parties to each other.

- **Shared key** - IKE uses a hashing technique to ensure that only someone who possesses the same key can send the IKE packets.
- **Digital Signature Standard (DSS) or Rivest, Shamir, Adelman (RSA) digital signatures** - IKE uses public-key digital-signature cryptography to verify that each party is who they claim to be.
- **RSA encryption** - IKE uses one of two methods to encrypt enough of the negotiation to ensure that only a party with the correct private key can continue the negotiation.

Session Negotiation

During session negotiation, IKE allows parties to negotiate how they will conduct authentication and how they will protect any future negotiations (that is, IPSec tunnel negotiation). These items are negotiated:

- **Authentication method** - This is one of the methods listed in the Authentication section of this document.
- **Key exchange algorithm** - This is a mathematical technique for securely exchanging cryptographic keys over a public medium (Diffie-Hellman). The keys are used in the encryption and packet-signature algorithms.
- **Encryption algorithm** - Data Encryption Standard (DES) or Triple Data Encryption Standard (3DES).
- **Packet signature algorithm** - Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA-1).

Key Exchange

IKE uses the negotiated key-exchange method (see the Session Negotiation section of this document) to create enough bits of cryptographic keying material to secure future transactions. This method ensures that each IKE session is protected with a new, secure set of keys.

Authentication, session negotiation, and key exchange constitute phase one of an IKE negotiation. For a VPN 5000 Concentrator, these properties are configured in the **IKE Policy** section through the Protection keyword. This keyword is a label which has three pieces: authentication algorithm,

encryption algorithm, and key exchange algorithm. The pieces are separated by an underscore. The label MD5_DES_G1 means use MD5 for IKE-packet authentication, use DES for IKE-packet encryption, and use Diffie-Hellman group 1 for key exchange. For more information, refer to Configuring the IKE Policy for IPSec Tunnel Security.

IPSec Tunnel Negotiation and Configuration

After IKE has finished negotiating a secure method for exchanging information (phase one), IKE is used to negotiate an IPSec tunnel. This is accomplished using IKE phase two. In this exchange, IKE creates fresh keying material for the IPSec tunnel to use (either using the IKE phase one keys as a base or by performing a new key exchange). The encryption and authentication algorithms for this tunnel are also negotiated.

IPSec tunnels are configured using the VPN Group (formerly the Secure Tunnel Establishment Protocol (STEP) Client) section for VPN Client tunnels and the Tunnel Partner section for LAN-to-LAN tunnels. The **VPN Users** section is where the authentication method for each user is stored. These sections are documented in Configuring the IKE Policy for IPSec Tunnel Security.

VPN 5000 Concentrator IKE Extensions

- **RADIUS** - IKE has no support for RADIUS authentication. RADIUS authentication is performed in a special information exchange that takes place after the first IKE packet from the VPN Client. If Password Authentication Protocol (PAP) is required, a special RADIUS authentication secret is required. For more information, refer to the documentation of NoCHAP and PAPAuthSecret in Configuring the IKE Policy for IPSec Tunnel Security. RADIUS authentication is authenticated and encrypted. The PAP exchange is protected by the PAPAuthSecret. However, there is only one such secret for the entire IntraPort, so the protection is as weak as any shared password.
- **SecurID** - IKE currently has no support for SecurID authentication. SecurID authentication is performed in a special informational exchange in between phase one and phase two. This exchange is fully protected by the IKE Security Association (SA) negotiated in phase one.
- **Secure Tunnel Access Management Protocol (STAMP)** - VPN Client connections exchange information with the IntraPort during the IKE process. Information such as if it is all right to save secrets, which IP networks to tunnel, or whether to tunnel Internetwork Packet Exchange (IPX) traffic, is sent in private payloads during the last two IKE packets. These payloads are only sent to compatible VPN Clients.

ISAKMP and Oakley

The Internet Security Association and Key Management Protocol (ISAKMP) is a language used to conduct negotiations across the Internet (for example, using the IP protocol). Oakley is a method for conducting an authenticated exchange of cryptographic key material. IKE puts the two together into one package, which allows secure connections to be set up across the unsecure Internet.

STEP and STAMP

Secure Tunnel Establishment Protocol (STEP) is the previous name of the VPN system. In the pre-IKE days, STAMP was used to negotiate IPSec connections. The VPN Client versions earlier

than 3.0 use STAMP to establish a connection with an IntraPort.

Related Information

- **Cisco VPN 5000 Series Concentrators End-of-Sales Announcement**
- **Configuring a Router-to-VPN 5000 Series Concentrator LAN-to-LAN Tunnel**
- **Cisco VPN 5000 Concentrator Product Support Page**
- **Cisco VPN 5000 Client Product Support Page**
- **IPSec Negotiation/IKE Protocols Technology Support**
- **Technical Support & Documentation - Cisco Systems**