Redes virtuais privadas e intercâmbio de chave de Internet para o Cisco VPN 5000 Concentrator Series

Contents

Introduction

O Internet Key Exchange (IKE) é um método padrão usado para organizar comunicações seguras e autenticadas. O Cisco VPN 5000 Concentrator usa IKE para configurar túneis IPSec. Esses túneis IPSec são o backbone deste produto.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- 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

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Tarefas de IKE

O IKE lida com estas tarefas:

- Autenticação
- Negociação de sessão
- Intercâmbio de chave
- Negociação e configuração de túnel de IPSec

Autenticação

A autenticação é a tarefa mais importante que a IKE realiza, e é a mais complicada. Sempre que negociamos algo, é importante saber com quem negociamos. A IKE pode usar um dos vários métodos para autenticar partes negociadoras entre si.

- **Chave compartilhada** - O IKE usa uma técnica de hash para garantir que somente alguém que possui a mesma chave possa enviar os pacotes IKE.
- **Digital Signature Standard (DSS) ou Rivest, Shamir, Adelman (RSA) assinaturas digitais** - A IKE usa criptografia de assinatura digital de chave pública para verificar se cada parte é quem diz ser.
- **Criptografia RSA** - O IKE usa um dos dois métodos para criptografar o suficiente da negociação para garantir que apenas uma parte com a chave privada correta possa continuar a negociação.

Negociação de sessão
Durante a negociação da sessão, o IKE permite que as partes negociem como conduzirão a autenticação e como protegerão quaisquer negociações futuras (isto é, a negociação de túnel IPSec). Esses itens são negociados:

- **Authentication method** - Este é um dos métodos listados na seção Authentication deste documento.
- **Algoritmo de troca de chaves** - Essa é uma técnica matemática para trocar chaves criptográficas com segurança em um meio público (Diffie-Hellman). As chaves são usadas nos algoritmos de criptografia e assinatura de pacotes.
- **Algoritmo de criptografia** - Data Encryption Standard (DES) ou Triple Data Encryption Standard (3DES).
- **Algoritmo de assinatura de pacote** - Message Digest 5 (MD5) e Secure Hash Algorithm 1 (SHA-1).

Intercâmbio de chave

O IKE usa o método de troca de chave negociado (consulte a seção Negociação de Sessão deste documento) para criar bits suficientes de material de chave criptográfica para proteger transações futuras. Esse método garante que cada sessão IKE seja protegida por um novo conjunto seguro de chaves.

A autenticação, a negociação de sessão e a troca de chaves constituem a fase um de uma negociação IKE. Para um VPN 5000 Concentrator, essas propriedades são configuradas na seção **Política IKE** através da palavra-chave Protection. Esta palavra-chave é um rótulo com três partes: algoritmo de autenticação, algoritmo de criptografia e algoritmo de troca de chave. As peças são separadas por um sublinhado. O rótulo MD5_DES_G1 significa usar MD5 para autenticação de pacote IKE, usar DES para criptografia de pacote IKE e usar Diffie-Hellman group 1 para troca de chaves. Para obter mais informações, consulte Configuração da Política IKE para Segurança de Túnel IPSec.

Negociação e configuração de túnel de IPSec

Depois que o IKE terminar de negociar um método seguro para troca de informações (fase um), o IKE é usado para negociar um túnel IPSec. Isso é realizado usando a fase dois do IKE. Nessa troca, a IKE cria um novo material de chaveamento para o túnel IPSec a ser usado (usando as chaves da fase 1 da IKE como base ou executando uma nova troca de chaves). Os algoritmos de criptografia e autenticação para este túnel também são negociados.

Os túneis IPSec são configurados usando a seção VPN Group (anteriormente o Secure Tunnel ESTABLISHProtocol (STEP) Client) para túneis de VPN Client e a seção Tunnel Partner para túneis LAN a LAN. A seção **Usuários de VPN** é onde o método de autenticação para cada usuário é armazenado. Estas seções estão documentadas em Configuração da Política IKE para Segurança de Túnel IPSec.

Extensões IKE do VPN 5000 Concentrator

- **RADIUS** - O IKE não tem suporte para autenticação RADIUS. A autenticação RADIUS é executada em uma troca de informações especial que ocorre após o primeiro pacote IKE do VPN Client. Se o Password Authentication Protocol (PAP) for necessário, um segredo de autenticação RADIUS especial será necessário. Para obter mais informações, consulte a documentação NoCHAP e PAPAuthSecret em Configuring the IKE Policy for IPSec Tunnel Security. A autenticação RADIUS é autenticada e criptografada. A troca PAP é protegida pelo PAPAuthSecret. No entanto, há apenas um segredo para toda a IntraPort, portanto, a proteção é tão fraca quanto qualquer senha compartilhada.
- **SecurID** - O IKE não tem suporte para autenticação SecurID. A autenticação SecurID é executada em uma troca de informações especial entre a fase um e a fase dois. Essa troca é totalmente protegida pela Associação de Segurança IKE (SA) negociada na fase um.
- **Secure Tunnel Access Management Protocol (STAMP)** - As conexões do VPN Client trocam informações com a IntraPort durante o processo IKE. Informações como se fosse correto salvar segredos, quais redes IP serão encapsuladas ou se o tráfego IPX (Internetwork Packet Exchange) será enviado em payloads privados durante os dois últimos pacotes IKE. Esses payloads são enviados apenas para VPN Clients compatíveis.

ISAKMP e Oakley

O Internet Security Association and Key Management Protocol (ISAKMP) é um idioma usado para conduzir negociações pela Internet (por exemplo, usando o protocolo IP). Oakley é um método para conduzir uma troca autenticada de material de chave criptográfica. A IKE reúne os dois em um único pacote, que permite que conexões seguras sejam configuradas na Internet não segura.

STEP e STAMP

O protocolo STEP (Secure Tunnel Setting Protocol) é o nome anterior do sistema VPN. Nos dias anteriores à IKE, o STAMP foi usado para negociar conexões IPSec. As versões do VPN Client anteriores à 3.0 usam STAMP para estabelecer uma conexão com uma IntraPort.

Informações Relacionadas

- Anúncio do fim do ciclo de comercialização dos concentradores Cisco VPN 5000 Series
- Configurando um túnel de LAN para LAN entre roteador e um concentrador do VPN 5000 Series
- Página de suporte do produto Cisco VPN 5000 Concentrator
- Página de suporte ao produto cliente Cisco VPN 5000
- Suporte à tecnologia de negociação de IPSec/protocolos IKE
- Suporte Técnico e Documentação - Cisco Systems