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

Índice

Introdução

O Internet Key Exchange (IKE) é um método padrão usado para arranjar comunicações seguras, autenticadas. O concentrador do Cisco VPN 5000 usa o IKE para estabelecer túneis de IPsec. Estes túneis de IPsec são o backbone deste produto.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Concentrador do VPN 5000 Series

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto

potencial de qualquer comando.

Convenções

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

Tarefas de IKE

O IKE segura estas tarefas:

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

Autenticação

A autenticação é a tarefa a mais importante que o IKE realiza, e é o mais complicado. Sempre que você negocia algo, é importante saber com quem você negocia. O IKE pode usar um de diversos métodos para autenticar entre si partidos de negócio.

- **Chave compartilhada** - O IKE usa uma técnica do hashing para assegurar-se de que somente alguém que possui a mesma chave possa enviar os pacotes de IKE.
- **Digital Signature Standard (DSS) ou Rivest, Shamir, assinaturas digital de Adelman (RSA)** - o IKE usa a criptografia da assinatura digital da chave pública para verificar que cada partido é quem reivindicam ser.
- **Criptografia RSA** - O IKE usa um de dois métodos para cifrar bastante da negociação para assegurar-se de que somente um partido com a chave privada correta possa continuar a negociação.

Negociação de sessão

Durante a negociação de sessão, o IKE permite que os partidos negociem como conduzirão a autenticação e como protegerão todas as negociações futuras (isto é, negociação do túnel IPSec). Estes artigos são negociados:

- **Método de autenticação** - Este é um dos métodos alistados na seção da autenticação deste documento.
- **Key Exchange Algorithm** - Esta é uma técnica matemática para firmemente trocar chaves criptográficas sobre um meio público (Diffie-Hellman). As chaves são usadas na criptografia e nos Algoritmos de assinatura de pacote.
- **Algoritmo de criptografia** - Data Encryption Standard (DES) ou Triple Data Encryption Standard (3DES).
- **Algoritmo de assinatura de pacote** - Message digest 5 (MD5) e algoritmo de mistura segura 1 (SHA-1).

Intercâmbio de chave

O IKE usa o método negociado das trocas de chave (veja a seção da negociação de sessão deste documento) para criar bastante bit do material de chaveamento criptográfico para fixar transações futuras. Este método assegura-se de que cada sessão de IKE esteja protegida com um grupo novo, seguro de chaves.

A autenticação, a negociação de sessão, e as trocas de chave constituem fase um de uma negociação de IKE. Para um VPN 5000 concentrator, estas propriedades são configuradas na **seção política de IKE** com as palavras-chave de proteção. Esta palavra-chave é uma etiqueta que tenha três partes: algoritmo de autenticação, algoritmo de criptografia, e Key Exchange Algorithm. As partes são separadas por um relevo. A etiqueta MD5_DES_G1 significa o uso MD5 para a autenticação do pacote IKE, o uso DES para a criptografia do pacote IKE, e o grupo Diffie-Hellman 1 do uso para trocas de chave. Para mais informação, refira configurar a política de IKE para a Segurança do túnel de IPsec.

Negociação e configuração de túnel de IPSec

Depois que o IKE terminou negociar um método de intercâmbio de informação seguro (fase um), o IKE está usado para negociar um túnel de IPsec. Isto é realizado usando a fase dois IKE. Nesta troca, o IKE cria o material de chaveamento atual para que o túnel de IPsec use-se (usando as chaves fase um IKE como uma base ou executando umas trocas de chave novas). A criptografia e os algoritmos de autenticação para este túnel são negociados igualmente.

Os túneis de IPsec são configurados usando a seção do grupo de VPN (anteriormente o cliente do protocolo secure tunnel establishment (ETAPA)) para túneis do cliente VPN e a seção do sócio de túnel para túneis de LAN para LAN. A seção dos **usuários VPN** é o lugar onde o método de autenticação para cada usuário é armazenado. Estas seções são documentadas em configurar a política de IKE para a Segurança do túnel de IPsec.

Extensões de IKE do VPN 5000 concentrator

- **RAIO** - O IKE não tem nenhum apoio para a autenticação RADIUS. A autenticação RADIUS é executada em uma troca de informação especial que ocorra após o primeiro pacote de IKE do cliente VPN. Se o protocolo password authentication (PAP) é exigido, um segredo especial da autenticação RADIUS está exigido. Para mais informação, refira a documentação de NoCHAP e de PAPAuthSecret em configurar a política de IKE para a Segurança do túnel de IPsec. A autenticação RADIUS é autenticada e cifrada. A troca PAP é protegida pelo PAPAuthSecret. Contudo, há somente um tal segredo para Intraport inteiro, assim que a proteção é tão fraca quanto toda a senha compartilhada.
- **SecurID** - O IKE não tem atualmente nenhum apoio para a autenticação securid. A autenticação securid é executada em um fase um da troca informativa especial e em uma fase no meio dois. Esta troca é protegida inteiramente pela associação de segurança IKE (SA) negociada em fase um.
- **Protocolo secure tunnel access management (SELO)** - Informação da troca das conexões de cliente de VPN com Intraport durante o processo IKE. A informação como se é toda direito salvar os segredos, que as redes IP a escavar um túnel, ou se escavar um túnel o tráfego das Trocas de Pacote Entre Redes IPX (IPX), é enviada em privado a cargas úteis durante os últimos dois pacotes de IKE. Estas cargas úteis são enviadas somente aos clientes VPN compatíveis.

ISAKMP e Oakley

O Internet Security Association and Key Management Protocol (ISAKMP) é uma língua usada para conduzir negociações através do Internet (por exemplo, usando o protocolo IP). Oakley é um método para conduzir uma troca autenticada do material de chave criptográfica. O IKE une os dois em um pacote, que permite que as conexões seguras se estabeleçam através das internet inseguras.

STEP e STAMP

O protocolo secure tunnel establishment (ETAPA) é o nome precedente do sistema de VPN. Nos dias PRE-IKE, o SELO foi usado para negociar conexões IPSec. As versões do cliente VPN mais cedo do que o SELO do uso do 3.0 para estabelecer uma conexão com Intraport.

Informações Relacionadas

- Anúncio End-of-Life de concentradores do 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 de concentrador do Cisco VPN 5000
- Página de suporte do produto do Cisco VPN 5000 Client
- Suporte por tecnologia da Negociação IPSec/Protocolos IKE
- Suporte Técnico e Documentação - Cisco Systems