Réseaux privés virtuels et échange de clés Internet pour le concentrateur Cisco VPN 5000

Contenu

Introduction

Internet Key Exchange (IKE) est une méthode standard utilisée pour organiser des communications authentifiées et sécurisées. Le concentrateur Cisco VPN 5000 utilise IKE pour configurer des tunnels IPSec. Ces tunnels IPSec constituent le réseau fédérateur de ce produit.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Concentrateur VPN 5000

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

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Tâches IKE

IKE gère ces tâches :

- Authentification
- Négociation de session
- Échange de clés
- Négociation et configuration du tunnel IPSec

Authentification

L'authentification est la tâche la plus importante que le protocole IKE effectue, et elle est la plus compliquée. Chaque fois que vous négociez quelque chose, il est important de savoir avec qui vous négociez. IKE peut utiliser l'une des méthodes suivantes pour authentifier les parties aux négociations.

- **Clé partagée** : IKE utilise une technique de hachage pour s'assurer que seule une personne possédant la même clé peut envoyer les paquets IKE.
- **Digital Signature Standard (DSS) ou Rivest, Shamir, Adelman (RSA) signatures numériques** - IKE utilise la cryptographie à clé publique pour vérifier que chaque partie est celle qu'elle prétend être.
- **Cryptage RSA** - IKE utilise l'une des deux méthodes pour chiffrer suffisamment de la négociation pour s'assurer que seule une partie possédant la clé privée correcte peut poursuivre la négociation.

Négociation de session

Au cours de la négociation de session, IKE permet aux parties de négocier la manière dont elles procéderont à l'authentification et la manière dont elles protégeront toute négociation future (c'est-à-dire la négociation de tunnel IPSec). Ces points sont négociés :

- **Méthode d'authentification** - Il s'agit d'une des méthodes répertoriées dans la section Authentification de ce document.
- **Algorithme d'échange de clés** - Technique mathématique permettant l'échange sécurisé de clés cryptographiques sur un support public (Diffie-Hellman). Les clés sont utilisées dans les algorithmes de chiffrement et de signature de paquet.
- **Algorithme de chiffrement** - Norme de chiffrement des données (DES) ou Norme de chiffrement des données triple (3DES).
- **Algorithme de signature de paquet** - Message Digest 5 (MD5) et Secure Hash Algorithm 1 (SHA-1).

Échange de clés

IKE utilise la méthode d'échange de clés négociée (voir la section Négociation de session de ce document) pour créer suffisamment de bits de matériel de clé cryptographique pour sécuriser les transactions futures. Cette méthode garantit que chaque session IKE est protégée par un nouvel ensemble sécurisé de clés.

L'authentification, la négociation de session et l'échange de clés constituent la première phase d'une négociation IKE. Pour un concentrateur VPN 5000, ces propriétés sont configurées dans la section **Stratégie IKE** via le mot clé Protection. Ce mot clé est une étiquette qui comporte trois éléments : algorithme d'authentification, algorithme de chiffrement et algorithme d'échange de clés. Les pièces sont séparées par un trait de soulignement. L'étiquette MD5_DES_G1 signifie utiliser MD5 pour l'authentification des paquets IKE, utiliser DES pour le chiffrement des paquets IKE et utiliser Diffie-Hellman groupe 1 pour l'échange de clés. Pour plus d'informations, référez-vous à Configuration de la stratégie IKE pour la sécurité du tunnel IPSec.

Négociation et configuration du tunnel IPSec

Une fois IKE terminé la négociation d'une méthode sécurisée d'échange d'informations (phase 1), IKE est utilisé pour négocier un tunnel IPSec. Ceci est réalisé à l'aide de la phase 2 du protocole IKE. Dans cet échange, IKE crée un nouveau matériau de frappe pour le tunnel IPSec à utiliser (soit en utilisant les clés de phase 1 IKE comme base, soit en effectuant un nouvel échange de clés). Les algorithmes de chiffrement et d'authentification de ce tunnel sont également négociés.

Les tunnels IPSec sont configurés à l'aide de la section VPN Group (anciennement client STEP (Secure Tunnel Establishment Protocol) pour les tunnels VPN Client et de la section Tunnel Partner pour les tunnels LAN à LAN. La section **Utilisateurs VPN** contient la méthode d'authentification de chaque utilisateur. Ces sections sont documentées dans Configuration de la stratégie IKE pour la sécurité du tunnel IPSec.

Extensions IKE du concentrateur VPN 5000

- **RADIUS** - IKE ne prend pas en charge l'authentification RADIUS. L'authentification RADIUS est effectuée dans un échange d'informations spécial qui a lieu après le premier paquet IKE du client VPN. Si le protocole PAP (Password Authentication Protocol) est requis, un secret d'authentification RADIUS spécial est requis. Pour plus d'informations, référez-vous à la documentation de NoCHAP et PAPAuthSecret dans Configuration de la stratégie IKE pour la sécurité du tunnel IPSec. L'authentification RADIUS est authentifiée et chiffrée. L'échange PAP est protégé par PAPAuthSecret. Cependant, il n'y a qu'un seul secret de ce genre pour l'ensemble de l'IntraPort, de sorte que la protection est aussi faible que n'importe quel mot de passe partagé.
- **SecurID** - IKE ne prend actuellement pas en charge l'authentification SecurID. L'authentification SecurID est effectuée dans un échange d'informations spécial entre les phases 1 et 2. Cet échange est entièrement protégé par l'association de sécurité IKE (SA) négociée au cours de la première phase.
- **Secure Tunnel Access Management Protocol (STAMP)** : les connexions du client VPN échangent des informations avec l'IntraPort pendant le processus IKE. Des informations telles que si l'enregistrement de secrets est correct, quels réseaux IP doivent être tunnels ou s'il faut ou non tunnel du trafic IPX (Internetwork Packet Exchange), sont envoyées dans des charges utiles privées au cours des deux derniers paquets IKE. Ces charges utiles sont envoyées uniquement aux clients VPN compatibles.

ISAKMP et Oakley

Le protocole ISAKMP (Internet Security Association and Key Management Protocol) est un

langage utilisé pour mener des négociations sur Internet (par exemple, en utilisant le protocole IP). Oakley est une méthode d'échange authentifié de matériel de clé cryptographique. IKE regroupe les deux dans un seul paquet, ce qui permet de configurer des connexions sécurisées sur Internet non sécurisé.

ÉTAPE et STAMP

Le protocole STEP (Secure Tunnel Establishment Protocol) est le nom précédent du système VPN. Dans les jours précédant l'IKE, le protocole STAMP a été utilisé pour négocier les connexions IPSec. Les versions du client VPN antérieures à la version 3.0 utilisent STAMP pour établir une connexion avec un IntraPort.

Informations connexes

- Annonce de fin de commercialisation des concentrateurs Cisco VPN 5000
- Configuration d'un tunnel LAN à LAN entre routeur et concentrateur VPN 5000
- Page d'assistance produit du concentrateur Cisco VPN 5000
- Page d'assistance produit du client Cisco VPN 5000
- Prise en charge de la technologie des protocoles IPSec/IKE
- Support et documentation techniques - Cisco Systems