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

Contenu

Introduction

L'Échange de clés Internet (IKE) est une méthode standard utilisée pour arranger des transmissions sécurisées et authentifiées. Le concentrateur de Cisco VPN 5000 emploie l'IKE pour installer des tunnels d'IPSec. Ces tunnels d'IPSec sont le circuit principal de ce produit.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- Concentrateur de la gamme VPN 5000

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

Tâches d'IKE

L'IKE gère ces tâches :

- Authentification
- Négociation de session
- Key Exchange
- Négociation et configuration de tunnel d'IPSec

Authentification

L'authentification est la tâche la plus importante que l'IKE accomplit, et il est le plus compliqué. Toutes les fois que vous négociez quelque chose, il est important de savoir avec qui vous négociez. L'IKE peut employer une de plusieurs méthodes pour authentifier les interlocuteurs de négociation entre eux.

- **Clé partagée** - L'IKE emploie une technique de hachage pour s'assurer que seulement quelqu'un qui possède la même clé peut envoyer les paquets d'IKE.
- **Norme de signature numérique (DSS) ou Rivest, Shamir, signatures numériques d'Adelman (RSA)** - l'IKE emploie le chiffrement de signature numérique de clé publique pour vérifier que chaque interlocuteur est qui ils prétendent être.
- **Cryptage RSA** - L'IKE emploie une de deux méthodes pour chiffrer assez de la négociation pour s'assurer que seulement un interlocuteur avec la clé privée correcte peut continuer la négociation.

Négociation de session

Pendant la négociation de session, l'IKE permet à des interlocuteurs pour négocier comment ils conduiront l'authentification et comment ils protégeront toutes les futures négociations (c'est-à-dire, négociation de tunnel d'IPSec). Ces éléments sont négociés :

- **Méthode d'authentification** - C'est l'une des méthodes répertoriées dans la section d'authentification de ce document.
- **Algorithme principal d'échange** - C'est une technique mathématique pour permuter sécurisé des clés cryptographiques au-dessus d'un support public (Diffie-Hellman). Les clés sont utilisées dans le cryptage et les algorithmes de paquet-signature.
- **Algorithme de chiffrement** - Norme de chiffrement de données (DES) ou Norme 3DES (Triple Data Encryption Standard).
- **Algorithme de signature de paquet** - Message Digest 5 (MD5) et Secure Hash Algorithm 1 (SHA-1).

Key Exchange

L'IKE emploie la méthode d'échange de clés négociée (voyez la section de négociation de session de ce document) pour créer assez de bits de matériel de base cryptographique pour sécuriser de futures transactions. Cette méthode s'assure que chaque session d'IKE est protégée avec un nouveau, sécurisé ensemble de clés.

L'authentification, la négociation de session, et l'échange clé constituent la phase une d'une négociation d'IKE. Pour un concentrateur VPN 5000, ces propriétés sont configurées dans la section de **stratégie IKE** par le mot clé de protection. Ce mot clé est une étiquette qui a trois parties : algorithme d'authentification, algorithme de chiffrement, et algorithme d'échange de clé. Les parties sont séparées par un trait de soulignement. L'étiquette MD5_DES_G1 signifie le MD5 d'utilisation pour l'authentification d'IKE-paquet, le DES d'utilisation pour le cryptage d'IKE-paquet, et l'échange de clé de 1par de groupe de Diffie-Hellman d'utilisation. Le pour en savoir plus, se rapportent à configurer la stratégie IKE pour le degré de sécurité de tunnel d'IPSec.

Négociation et configuration de tunnel d'IPSec

Après que l'IKE ait fini de négocier une méthode sécurisée pour permuter les informations (phase une), l'IKE est utilisé pour négocier un tunnel d'IPSec. Ce fait utilisant la phase deux d'IKE. Dans cet échange, l'IKE crée le matériel de base frais pour que le tunnel d'IPSec l'utilise (en utilisant la phase d'IKE on introduit comme base ou en exécutant un nouvel échange clé). Les algorithmes de cryptage et d'authentification pour ce tunnel sont également négociés.

Des tunnels d'IPSec sont configurés utilisant la section de groupe VPN (autrefois le client sécurisé de Protocol d'établissement de tunnel (ÉTAPE)) pour les tunnels de client vpn et la partie partenaire du tunnel pour des tunnels entre réseaux locaux. La section d'**utilisateurs VPN** est où la méthode d'authentification pour chaque utilisateur est enregistrée. Ces sections sont documentées en configurant la stratégie IKE pour le degré de sécurité de tunnel d'IPSec.

Extensions d'IKE du concentrateur VPN 5000

- **RAYON** - L'IKE n'a aucun soutien de l'authentification de RAYON. L'authentification de RAYON est exécutée dans un échange d'informations spécial qui a lieu après le premier paquet d'IKE du client vpn. Si le Password Authentication Protocol (PAP) est exigé, un secret spécial d'authentification de RAYON est exigé. Le pour en savoir plus, se rapportent à la documentation de NoCHAP et de PAPAuthSecret en configurant la stratégie IKE pour le degré de sécurité de tunnel d'IPSec. L'authentification de RAYON est authentifiée et chiffrée. L'échange PAP est protégé par le PAPAuthSecret. Cependant, il y a seulement un tel secret pour l'IntraPort entier, ainsi la protection en est aussi faible que mot de passe partagé.
- **SecurID** - L'IKE n'a actuellement aucun soutien de l'authentification de SecurID. L'authentification de SecurID est exécutée dans une phase intermédiaire une d'échange informationnel spécial et la phase deux. Cet échange est entièrement protégé par l'association de sécurité d'IKE (SA) négociée dans la phase une.
- **Sécurisez le protocole de gestion d'Access de tunnel (HORODATAGE DES MESSAGES)** - les informations d'échange de connexions client VPN avec l'IntraPort pendant le processus d'IKE. Les informations comme s'il est tout juste de sauvegarder les secrets, qui des réseaux IP à percer un tunnel, ou si percer un tunnel le trafic de l'Internetwork Packet Exchange (IPX), sont introduites les charges utiles privées pendant les deux derniers paquets d'IKE. Ces charges utiles sont seulement envoyées 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 à travers l'Internet (par exemple, utilisant le protocole IP). Oakley est une méthode pour conduire un échange authentifié de contenu de clé cryptographique. L'IKE remonte les deux dans un module, qui permet des connexions sécurisées à installer à travers l'Internet unsecure.

ÉTAPE et HORODATAGE DES MESSAGES

Sécurisez l'établissement de tunnel que Protocol (ÉTAPE) est le nom précédent du système VPN. Pendant les jours de pré-IKE, l'HORODATAGE DES MESSAGES a été utilisé pour négocier des connexions d'IPSec. Les versions de client vpn plus tôt HORODATAGE DES MESSAGES de que 3.0 utilisations pour établir une connexion avec un IntraPort.

Informations connexes

- Annonce de fin de ventes de Concentrateur VPN de la gamme Cisco 5000
- Configuration d'un tunnel LAN à LAN entre routeur et concentrateur VPN 5000
- Page de support de produit concentrateur de Cisco VPN 5000
- Page de support produit de Client VPN 5000 de Cisco
- Support technique de Négociation IPSec/protocoles IKE
- Support et documentation techniques - Cisco Systems