Virtual Private Networks und Internet Key Exchange für die Cisco VPN 500 Concentrator-Serie

Inhalt

Einführung

Internet Key Exchange (IKE) ist eine Standardmethode zur Organisation sicherer, authentifizierter Kommunikation. Der Cisco VPN 500 Concentrator verwendet IKE, um IPSec-Tunnel einzurichten. Diese IPSec-Tunnel bilden das Rückgrat dieses Produkts.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- VPN Concentrator der Serie 5000

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions.

IKE-Aufgaben

IKE übernimmt folgende Aufgaben:

- Authentifizierung
- Sitzungsverhandlung
- Schlüsselaustausch
- IPSec-Tunnelaushandlung und -konfiguration

Authentifizierung

Die Authentifizierung ist die wichtigste Aufgabe, die IKE erfüllt, und sie ist die komplizierteste. Wann immer man etwas verhandelt, ist es wichtig zu wissen, mit wem man verhandelt. IKE kann eine von mehreren Methoden verwenden, um die Verhandlungspartner untereinander zu authentifizieren.

- **Gemeinsamer Schlüssel** - IKE verwendet eine Hashing-Technik, um sicherzustellen, dass nur jemand, der denselben Schlüssel besitzt, die IKE-Pakete senden kann.
- **Digital Signature Standard (DSS) oder digitale Signaturen von Rivest, Shamir, Adelman (RSA)** - IKE verwendet Verschlüsselung für digitale Signaturen mit öffentlichem Schlüssel, um zu überprüfen, ob jede Partei die ist, die sie angeblich sind.
- **RSA-Verschlüsselung** - IKE verwendet eine von zwei Methoden, um genügend Aushandlungen zu verschlüsseln, um sicherzustellen, dass nur eine Partei mit dem richtigen privaten Schlüssel die Aushandlung fortsetzen kann.

Sitzungsverhandlung
Während der Sitzungsverhandlung ermöglicht IKE den Parteien, auszuhandeln, wie sie die Authentifizierung durchführen und wie sie künftige Verhandlungen schützen (d. h. IPSec-Tunnelverhandlungen). Diese Punkte werden ausgehandelt:

- **Authentifizierungsmethode** - Dies ist eine der Methoden, die im Abschnitt Authentifizierung dieses Dokuments aufgeführt sind.
- **Schlüsselaustauschalgorithmus** - Dies ist eine mathematische Technik für den sicheren Austausch kryptografischer Schlüssel über ein öffentliches Medium (Diffie-Hellman). Die Schlüssel werden in den Verschlüsselungs- und Paketsignaturalgorithmen verwendet.
- **Verschlüsselungsalgorithmus** - Data Encryption Standard (DES) oder Triple Data Encryption Standard (3DES).
- **Paketsignaturalgorithmus** - Message Digest 5 (MD5) und Secure Hash Algorithm 1 (SHA-1).

Schlüsselaustausch

IKE verwendet die ausgehandelte Schlüsselaustauschmethode (siehe Abschnitt Sitzungsverhandlung dieses Dokuments), um genügend Bits kryptografischen Keying-Materials zu

erstellen, um zukünftige Transaktionen zu sichern. Diese Methode stellt sicher, dass jede IKE-Sitzung mit einem neuen, sicheren Satz von Schlüsseln geschützt ist.

Authentifizierung, Sitzungsverhandlung und Schlüsselaustausch bilden die erste Phase einer IKE-Aushandlung. Für einen VPN 500-Konzentrator werden diese Eigenschaften über das Protection-Schlüsselwort im Abschnitt **IKE-Richtlinie** konfiguriert. Dieses Schlüsselwort ist ein Label, das aus drei Teilen besteht: Authentifizierungsalgorithmus, Verschlüsselungsalgorithmus und Schlüsselaustauschalgorithmus. Die Stücke werden durch einen Unterstrich voneinander getrennt. Das Label MD5_DES_G1 bedeutet, dass MD5 für die IKE-Paketauthentifizierung, DES für die IKE-Paketverschlüsselung und Diffie-Hellman-Gruppe 1 für den Schlüsselaustausch verwendet wird. Weitere Informationen finden Sie unter Konfigurieren der IKE-Richtlinie für IPSec-Tunnelsicherheit.

IPSec-Tunnelaushandlung und -konfiguration

Nachdem IKE die Aushandlung einer sicheren Methode für den Informationsaustausch abgeschlossen hat (Phase 1), wird IKE für die Aushandlung eines IPSec-Tunnels verwendet. Dies wird mithilfe von IKE Phase 2 erreicht. In diesem Austausch erstellt IKE neues Keying-Material für den zu verwendenden IPSec-Tunnel (entweder unter Verwendung der IKE-Phase-1-Schlüssel als Basis oder durch Durchführen eines neuen Schlüsselaustauschs). Die Verschlüsselungs- und Authentifizierungsalgorithmen für diesen Tunnel werden ebenfalls ausgehandelt.

IPSec-Tunnel werden für VPN-Client-Tunnel im Abschnitt "VPN Group" (ehemals "Secure Tunnel Establishment Protocol (STEP) Client") und für LAN-zu-LAN-Tunnel im Abschnitt "Tunnel Partner" konfiguriert. Im Abschnitt **VPN-Benutzer** wird die Authentifizierungsmethode für jeden Benutzer gespeichert. Diese Abschnitte werden unter Konfigurieren der IKE-Richtlinie für IPSec-Tunnelsicherheit dokumentiert.

VPN 5000 Concentrator IKE-Erweiterungen

- **RADIUS** - IKE unterstützt keine RADIUS-Authentifizierung. Die RADIUS-Authentifizierung erfolgt in einem speziellen Informationsaustausch, der nach dem ersten IKE-Paket vom VPN-Client stattfindet. Wenn Password Authentication Protocol (PAP) erforderlich ist, ist ein spezieller RADIUS-Authentifizierungsgeheimnis erforderlich. Weitere Informationen finden Sie in der Dokumentation von NoCHAP und PAPAuthSecret in der Konfiguration der IKE-Richtlinie für IPSec-Tunnelsicherheit. Die RADIUS-Authentifizierung wird authentifiziert und verschlüsselt. Der PAP-Austausch ist durch PAPAuthSecret geschützt. Es gibt jedoch nur einen solchen geheimen Schlüssel für den gesamten IntraPort, daher ist der Schutz so schwach wie jedes gemeinsam genutzte Passwort.
- **SecurID** - IKE unterstützt derzeit keine SecurID-Authentifizierung. Die SecurID-Authentifizierung wird in einem speziellen Informationsaustausch zwischen Phase 1 und Phase 2 durchgeführt. Dieser Austausch ist durch die IKE Security Association (SA), die in Phase 1 ausgehandelt wurde, vollständig geschützt.
- **Secure Tunnel Access Management Protocol (STAMP)** - VPN-Client-Verbindungen tauschen während des IKE-Prozesses Informationen mit dem IntraPort aus. In den letzten beiden IKE-Paketen werden Informationen, wie zum Beispiel, ob es gut ist, Geheimnisse zu speichern, welche IP-Netzwerke zu tunneln sind oder ob Internetwork Packet Exchange (IPX)-Datenverkehr tunnelt werden soll, in privaten Payloads gesendet. Diese Payloads werden nur an kompatible VPN-Clients gesendet.

ISAKMP und Oakley

Die Internet Security Association and Key Management Protocol (ISAKMP) ist eine Sprache, in der Verhandlungen über das Internet (z. B. über das IP-Protokoll) geführt werden. Oakley ist eine Methode für den authentifizierten Austausch von kryptographischem Schlüsselmaterial. IKE vereint beide in einem einzigen Paket, wodurch sichere Verbindungen über das unsichere Internet eingerichtet werden können.

SCHRITT und STAMP

Secure Tunnel Establishment Protocol (STEP) ist der vorherige Name des VPN-Systems. In der Zeit vor IKE wurde STAMP verwendet, um IPSec-Verbindungen auszuhandeln. Die VPN-Client-Versionen vor 3.0 verwenden STAMP, um eine Verbindung mit einem IntraPort herzustellen.

Zugehörige Informationen

- Cisco VPN Concentrators der Serie 5000 - Ankündigung des Vertriebsendes
- Konfigurieren eines Router-to-VPN Concentrator LAN-to-LAN-Tunnels der Serie 5000
- Produkt-Support-Seite für Cisco VPN 500 Concentrator
- Produkt-Support-Seite für Cisco VPN 500-Client
- Technologieunterstützung für IPSec-Aushandlung/IKE-Protokolle
- Technischer Support und Dokumentation - Cisco Systems