適用於Cisco VPN 5000集中器系列的虛擬專用網路和Internet金鑰交換

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[慣例](#)
[IKE任務](#)
[驗證](#)
[作業階段交涉](#)
[金鑰交換](#)
[IPSec通道交涉和設定](#)
[VPN 5000 Concentrator IKE Extensions](#)
[ISAKMP和Oakley](#)
[步驟和戳](#)
[相關資訊](#)

簡介

網際網路金鑰交換(IKE)是一種標準方法，用於安排安全且經過驗證的通訊。Cisco VPN 5000集中器使用IKE來設定IPSec隧道。這些IPSec通道是此產品的中樞。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- VPN 5000系列集中器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

IKE任務

IKE處理以下任務：

- 驗證
- 作業階段交涉
- 金鑰交換
- IPSec通道交涉和設定

驗證

身份驗證是IKE完成的最重要任務，也是最複雜的。無論何時協商某事，重要的是要瞭解您與誰協商。IKE可以使用多種方法之一來驗證相互協商的參與方。

- **共用密**鑰 — IKE使用雜湊技術來確保只有擁有相同金鑰的人才能傳送IKE資料包。
- **數位簽章標準(DSS)或Rivest、Shamir、Adelman(RSA)數位簽章 — IKE使用公鑰數位簽章加密來驗證每個參與方都聲稱自己是**誰。
- **RSA加密** - IKE使用兩種方法之一對足夠的協商進行加密，以確保只有具有正確私鑰的一方才能繼續協商。

作業階段交涉
在會話協商期間，IKE允許各方協商他們將如何執行身份驗證以及如何保護未來的協商（即IPSec隧道協商）。 該等專案乃透過磋商達成：

- **驗證方**法 — 這是本檔案「驗證」部分中列出的方法之一。
- **金鑰交換算**法 — 這是一種數學技術，用於在公共媒體(Diffie-Hellman)上安全交換加密金鑰。金鑰用於加密和資料包簽名演算法。
- **加密算**法 — 資料加密標準(DES)或三重資料加密標準(3DES)。
- **封包簽**名演演算法 — 訊息摘要5(MD5)和安全雜湊演演算法1(SHA-1)。

金鑰交換

IKE使用協商的金鑰交換方法(請參閱本文檔的會話協商部分)建立足夠的加密金鑰材料位以確保未來事務的安全。此方法確保每個IKE會話都使用一組新的安全金鑰進行保護。

身份驗證、會話協商和金鑰交換構成IKE協商的第一階段。對於VPN 5000集中器，這些屬性在**IKE Policy**部分中通過Protection關鍵字進行配置。此關鍵字是包含三個部分的標籤：認證演算法、加密演算法和金鑰交換演算法。這些部分之間用下劃線分隔。標籤MD5_DES_G1表示使用MD5進行IKE資料包身份驗證，使用DES進行IKE資料包加密，使用Diffie-Hellman組1進行金鑰交換。有關詳細資訊，請參閱為IPSec隧道安全配置IKE策略。

IPSec通道交涉和設定

在IKE完成協商交換資訊的安全方法（階段1）後，IKE用於協商IPSec隧道。這是使用IKE第二階段完成的。在此交換中，IKE為IPSec隧道建立新的金鑰材料（使用IKE第一階段金鑰作為基礎或通過執行新的金鑰交換）。 此通道的加密和驗證演算法也會經過交涉。

使用VPN客戶端隧道的VPN組(以前稱為「安全隧道建立協定(STEP)客戶端」)部分和LAN到LAN隧道的隧道合作夥伴部分配置IPSec隧道。**VPN Users**部分儲存了每個使用者的身份驗證方法。以下

各節在為IPSec隧道安全配置IKE策略中進行了說明。

VPN 5000 Concentrator IKE Extensions

- **RADIUS** - IKE不支援RADIUS驗證。RADIUS身份驗證是在來自VPN客戶端的第一個IKE資料包之後發生的特殊資訊交換中執行的。如果需要密碼驗證通訊協定(PAP)，則需要特殊的RADIUS驗證密碼。有關詳細資訊，請參閱為IPSec隧道安全配置IKE策略中的NoCHAP和PAPAuthSecret文檔。RADIUS驗證已驗證和加密。PAP交換受PAPAuthSecret保護。但是，整個IntraPort只有一個這樣的密碼，因此保護弱於任何共用密碼。
- **SecurID** - IKE當前不支援SecurID身份驗證。SecurID身份驗證是在第一階段和第二階段之間的特殊資訊交換中執行的。此交換由第一階段協商的IKE安全關聯(SA)提供完全保護。
- **安全通道存取管理通訊協定(STAMP)**- VPN使用者端連線在IKE過程中與IntraPort交換資訊。在最後兩個IKE資料包期間，在專用負載中傳送資訊，例如儲存機密是否正確、要將哪些IP網路隧道化，或者是否將網際網路資料包交換(IPX)流量隧道化。這些負載僅傳送到相容的VPN客戶端。

ISAKMP和Oakley

Internet安全關聯和金鑰管理協定(ISAKMP)是一種用於通過Internet（例如，使用IP協定）進行協商的語言。 Oakley是一種對金鑰材料進行身份驗證交換的方法。IKE將兩者整合到一個包中，這樣便可以在不安全的網際網路上建立安全連線。

步驟和戳

安全通道建立通訊協定(STEP)是VPN系統的先前名稱。在IKE之前的日子裡，使用STAMP協商IPSec連線。低於3.0的VPN客戶端版本使用STAMP與IntraPort建立連線。

相關資訊

- Cisco VPN 5000系列集中器銷售終止公告
- 配置路由器到VPN 5000系列集中器LAN到LAN隧道
- Cisco VPN 5000 Concentrator產品支援頁面
- Cisco VPN 5000客戶端產品支援頁
- IPSec協商/IKE通訊協定技術支援
- 技術支援與文件 - Cisco Systems