

Virtual Private Networks

Beschreibung der wesentlichen VPN-Verfahren und Aufbau eines Laborversuchs zur Simulation einer VPN-Verbindung zwischen zwei Firmenstandorten.

Projektarbeit vorgelegt von Roberto Vera im Fach „Netzwerksicherheit 1“

Virtual Private Networks

Ein virtuelles privates Netzwerk (VPN) ist ein Computernetz, das private Netze über öffentliche Netze verbindet. Sichere VPNs verwenden kryptographische Tunneling-Protokolle, um die beabsichtigte Vertraulichkeit, Absenderauthentifizierung und Integrität der Nachrichten bereitzustellen. Um ein vollständiges VPN zu bilden, müssen die Elemente Tunnel, Verschlüsselung und Authentifizierung zusammengefügt werden. Eine VPN-Verbindung kann mit verschiedenen Protokollen und auf verschiedenen Schichten des OSI-Referenzmodells aufgebaut werden. Die einzelnen Varianten sind im theoretischen Teil der Arbeit ausführlich dargestellt.

IPsec

Die Internet Protocol Security (IPsec) ist eine Sammlung von Protokollen zur Sicherung der IP-Kommunikation durch Authentifizierung und Verschlüsselung jedes IP-Pakets. IPsec enthält Protokolle für die gegenseitige Authentifizierung von Agenten zu Beginn der Sitzung und die Verhandlung der Schlüssel, die während der Sitzung verwendet werden sollen (IKE). Internet Key Exchange arbeitet dabei in zwei Phasen. In Phase 1 werden die Schlüssel über kryptographische Verfahren zwischen den Teilnehmern ausgehandelt. In der Phase 2 erfolgt dann die verschlüsselte Übertragung der Daten, wobei die Schlüssel während der Datenübertragung geändert werden.

Authentication Header und Encapsulating Security Payload

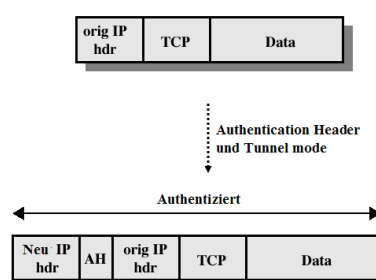
IPsec verwendet die "Authentication Header"- und die "Encapsulating Security Payload"- Protokolle, um verschiedene Funktionen durchzuführen.

Die **Authentication Header** wird verwendet und die Authentizität der übertragenen Pakete sicherzustellen und den Sender zu authentisieren. Die Datenherkunft wird abgesichert und nicht die Daten selbst.

Die **Encapsulating Security Payload** (ESP) wird verwendet, um Vertraulichkeit, die Datenherkunft, die Authentifizierung und die Verkehrsfluss-Vertraulichkeit bereitzustellen (Datenverschlüsselung).

Tunnel Mode und Transport Mode

Es gibt zwei Arten von IPsec-Betrieb: "Tunnel Mode" und "Transport Mode". Im **Tunnel Mode** wird das gesamte IP-Paket (Daten- und IP-Header) verschlüsselt und authentifiziert.

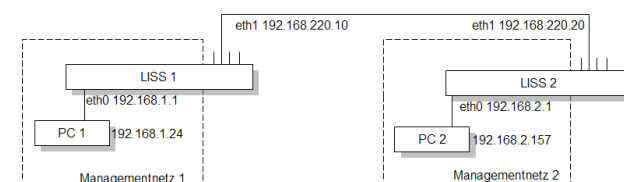


Es ist dann in ein neues IP-Paket eingekapselt und stellt das sicherere Verfahren dar.

Im **Transport Mode** werden nur die Daten im IP-Paket verschlüsselt. Das Routing ist intakt, da die IP-Header weder verändert noch verschlüsselt sind.

VPN-Aufbau mit LiSS Systeme

Die LiSS Series Systeme (Fa. TELCOTECH) sind Unified Threat Management Appliances. Sie vereinen verschiedene Sicherheitsaufgaben wie Firewall und Internet-Gateway auf einem System, welches als komplette Hardwarelösung angeboten wird. Verteilte Standorte oder Außendienstmitarbeiter können über die Konfiguration von IPsec-VPNs mit den LiSS-Systemen an einen zentralen Standort angebunden werden.



Im Security-Labor wurde ein praktisches Anwendungsszenario für eine VPN-Verbindung mit zwei LiSS-Geräten simuliert. Dabei können die Konfiguration des Tunnels, die Schlüsselaustauschvarianten und die Logdateien veranschaulicht werden. Im Zusammenhang mit den anderen LiSS-Funktionen lassen sich komplexe Aufgabenstellungen umsetzen.