IPsec

0 Index

1 Ziele der Internetprotokollsicherheit (IPsec)

Mit IPsec werden zwei Ziele verfolgt:

a. Schutz von IP Paketen.
b. Unterbinden von Netzwerkattacken.

Erreicht werden diese Ziele durch den Einsatz von kryptographiebasierten Diensten, Protokollen und der dynamischen Schlüsselverwaltung.

1.1 Einsatzmöglichkeiten der IPsec (Perimetersicherheit)

LAN: Client / Server, Peer2Peer.
WAN: Router2Router, Gateway2Gateway.
Remotezugriff: DFÜ-Clients, Internetzugriff für priv. Netze (Intranet, Extranet)

2 IPsec unter Win2000 / XP / 2003

a. bestehende Domäne als Vertrauensmodell
b. Authentifizierung über Kerberos v5
c. Zentralisierte IPsec Richtlinienverwaltung über Active Directory
d. Einmalige Konfiguration für alle Protokolle (TCP / UDP / usw.)
e. Systemseitige Schüsselverwaltung – IKE (Internet Key Exchange)
f. Systemseitige Sicherheitsaushandlung
g. Unterstützung von Zertifikaten basierend auf öffentlichen Schlüsseln
h. Unterstützung von gemeinsamen Authentisierungsschlüsseln

2.1 IPsec Protokolle & Ports (Verschlüsselung)

kerberos	88/tcp/udp	krb5 kerberos-sec	#Kerberos
isakmp	500/udp	ike	#Internet Key Exchange
Authentication Header		AH	#Protokoll 51 (Auth)
Encapsulation Security Payload		ESP	#Protokoll 50 (Crypt)

2.2 IPsec Kapselungsmodi (Aufbau)

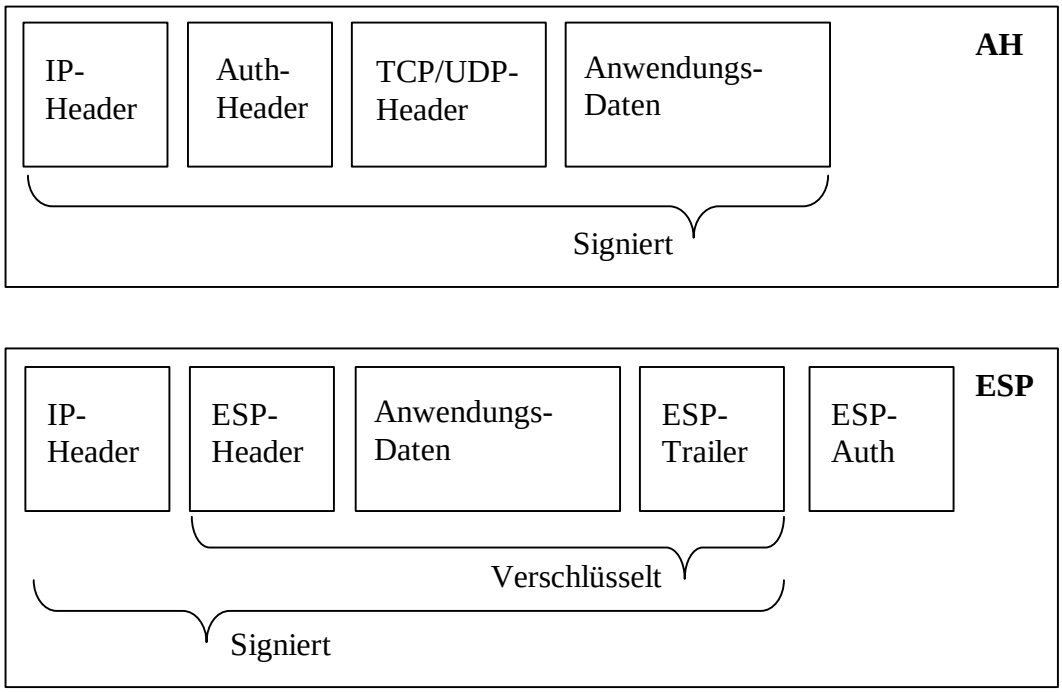
2.2.1Transportmodus:

Im Transportmodus verschlüsselt IPSec nur den Datenteil des zu transportierenden IP-Paketes: **Applikations-Header, TCP/UDP-Header und Daten werden verschlüsselt, die IP-Header sind lesbar**. Die Authentisierungsdaten werden auf Basis der Werte im IP-Header (und einigen anderen Sachen) berechnet. **Der Original-IP-Kopf bleibt dabei erhalten und es wird ein zusätzlicher IPSec-Kopf hinzugefügt**. Der Vorteil dieser Betriebsart ist, dass jedem Paket nur wenige Bytes hinzugefügt werden. Dem gegenüber steht, dass es für Angreifer möglich ist, den Datenverkehr im VPN zu analysieren, da die IP-Köpfe nicht modifiziert werden. **Die Daten selbst sind aber verschlüsselt**, so dass man nur feststellen kann, welche Stationen wie viele Daten austauschen, aber nicht welche Daten.

2.2.2 Tunnelmodus:

Im Tunnelmodus wird das **komplette IP-Paket verschlüsselt und mit einem neuen IP-Kopf und IPSec-Kopf versehen**. Dadurch ist das IPSec-Paket größer als im Transportmodus. Der Vorteil besteht hier darin, dass in den LANs, die zu einem VPN verbunden werden sollen, je ein Gateway so konfiguriert werden kann, dass es IP-Pakete annimmt, sie in IPSec-Pakete umwandelt und dann über das Internet dem Gateway im Zielnetzwerk zusendet, der das ursprüngliche Paket wiederherstellt und weiterleitet. Dadurch wird eine Neukonfiguration der LANs umgangen, da nur in den Gateways IPSec implementiert sein muss. **Außerdem können Angreifer so nur den Anfangs- und Endpunkt des IPSec-Tunnels feststell**

2.3 Darstellungen:



2.4 Automatisierte Schlüsselverwaltung mittels Internet Key Exchange (IKE)

IKE führt eine Zweiphasenoperation aus, um eine erfolgreiche sichere Kommunikation zu garantieren.

Phase I

a. Richtlinienaushandlung
- Verschlüsselungsalgorithmus (DES, 3DES)
- Hashalgorithmus (MD5 oder SHA)
- **Authentifizierungsmethoden (Zertifikat, gemeinsamer Schlüssel, Kerberos v5)**
- Diffie-Hellman-Gruppe (Basisschlüsselmaterial)

b. DH Austausch (von öffentlichen Werten)

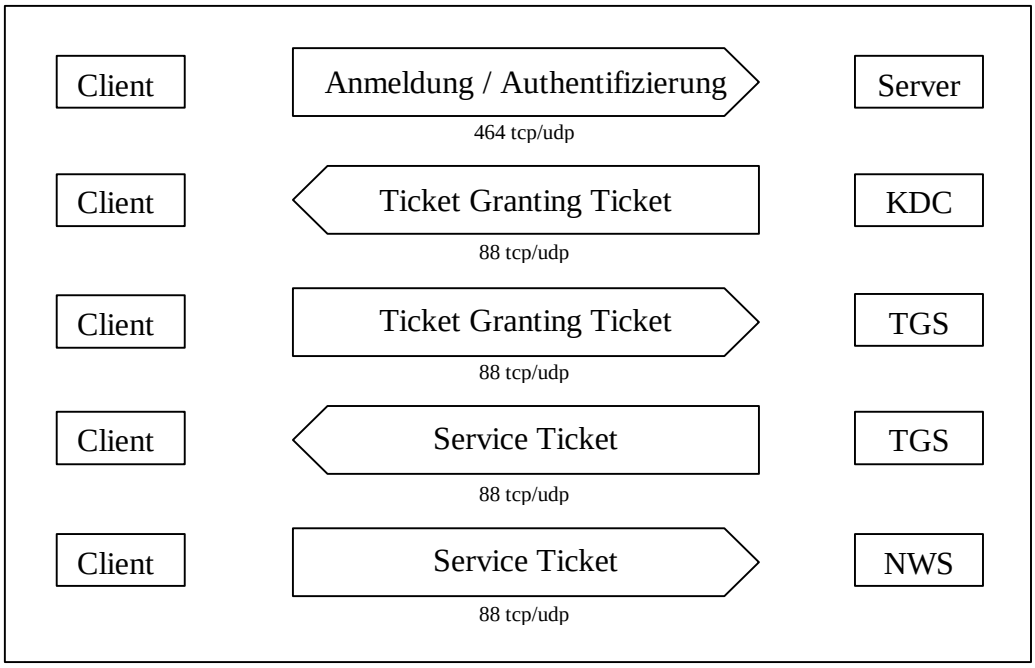
c. Authentifizierung

Phase II

a. Richtlinienaushandlung
- IPsec Protokoll (AH oder ESP)
- Hash für die Integrität und Auth (MD5 oder SHA)
- Algorithmus für die Verschlüsselung (falls angefordert) DES, 3DES

b. Aktualisierung/Generieren/Austauschen von Sitzungsschlüsseln
c. Sicherheitszuordnung und Schlüssel werden an IPsec Treiber übergeben

3 Funktionsweise Kerberos – TGP (Ticket Granting Protokoll)



Grundlegend arbeitet Kerberos mit Tickets, um Zugriff auf die im Netzwerk vorhandenen Dienste durchzuführen. Das Ticket weißt einen größtenteils verschlüsselten Inhalt auf, der die Identität eines Benutzers einem bestimmten Dienst gegenüber eindeutig bestätigt.

Der Client authentifiziert sich mittels Benutzername und Passwort (alternativ SmartCard) am Server / KDC (Key Distribution Center = Schlüsselverteilungscenter). Nach erfolgreicher Authentifizierung stellt das KDC dem Client ein TGT (Ticket Granting Ticket = ticketgarantierendes Ticket) aus. Unter Vorlage dieses TGT bekommt der Client vom TGS (Ticket Granting Service = ticketgarantierender Service) ein ST (Service Ticket) für die aktuelle Sitzung ausgestellt, dass der Client an jeden beliebigen Netzwerkdienst übergeben kann um somit seine Identität gegenüber dem Dienst, und umgekehrt, zu belegen.
Die Kommunikation des KDC findet über Port 88 TCP/UDP statt.

3.1 Kerberos v5 Ports

kerberos	88/tcp	krb5 kerberos-sec	#Kerberos
kerberos	88/udp	krb5 kerberos-sec	#Kerberos
kpasswd	464/tcp		#Kerberos (v5)
kpasswd	464/udp		#Kerberos (v5)
klogin	543/tcp		#Kerberos login
kshell	544/tcp	krcmd	#Kerberos remote shell
kerberos-adm	749/tcp		#Kerberos administration
kerberos-adm	749/udp		#Kerberos administration
kx	2111/tcp		#X over Kerberos
afs3-kaserver	7004/tcp		#Kerberos authentification
afs3-kaserver	7004/udp		#Kerberos authentification

3.2 Abkürzungsverzeichnis Kerberos

TGP	Ticket Granting Protokoll	ticketgenehmigendes Protokoll
KDC	Key Distribution Center	Schlüsselverteilungscenter
TGT	Ticket Granting Ticket	ticketgenehmigendes Ticket
TGS	Ticket Granting Service	ticketgenehmigender Dienst
NWS	Networkservices	Netzwerkdienste

4 Ipsec –standart- Sicherheitsrichtlinien

Client (nur Antwort) (Respond Only)
Normale (ungesicherte) Kommunikation verwenden. Verwenden Sie die Standardantwortregel, um Sicherheit mit Hosts auszuhandeln, die Sicherheit anfordern. Nur das angeforderte Protokoll und Datenverkehr über den Anschluss mit dem Host sind gesichert.

Server (Sicherheit anfordern) (Request Security)
Sicherheit ist für den gesamten IP-Verkehr erforderlich, unter Verwendung von Kerberos. Ungesicherte Kommunikation mit Clients, die nicht auf die Anforderung antworten, ist zugelassen.

Sicherer (Secure) Server (Sicherheit erforderlich) (Require Security)
Verwendung von Kerberos. Ungesicherte Kommunikation mit nicht vertrauenswürdigen Clients ist nicht zugelassen.

5 Blick, rüber zum VPN-Tellerrand

Fälschlicher Weise geht die breite Masse des (fach)kundigen Personals davon aus, das der Einsatz eines VPN Tunnels zwangsweise die Verwendung von IPsec beinhaltet? Wer sich allerdings näher mit den VPN-Protokollen (PPTP - Point-to-Point Tunneling Protocol; L2TP – Layer Two Tunneling Protocol) auseinander setzt wird feststellen, dass eine Verwendung von IPsec unabhängig konfiguriert werden muss (Securing PPTP/L2TP using IPsec) – und nicht zwingend erforderlich ist!
Näheres zu VPN vielleicht in einem der folgenden Texte...

6 Quellen

Microsoft Windows 2000 Server ‚Die technische Referenz' TCP/IP Netzwerke
VPN betrachtet http://www.id.ethz.ch/services/list/vpn/was_ist_vpn
Security Architecture for IP ftp://ftp.isi.edu/in-notes/rfc2401.txt