
Gesicherte SAP-Anbindung über einen SAProuter-Proxy unter Verwendung von IPsec und X.509v3-Zertifikaten

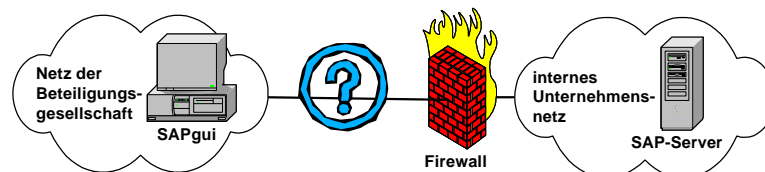
Dr. Tim Sattler
Tireno Innovations GmbH

Mai 2001
Seite 1

Dr. Tim Sattler: Gesicherte SAP-Anbindung
Tireno Innovations GmbH

Einleitung

Beispiel: SAP R/3



- Beteiligungsgesellschaften soll Zugriff auf Serversysteme im internen Unternehmensnetz ermöglicht werden
- Insbesondere bei *Minderheitsbeteiligungen* kein ausreichender Einfluss auf Firewall- und PC-Sicherheitsrichtlinie der Beteiligungsgesellschaft
- *Sicherheitsverlust* durch Öffnung der Firewall für Clientsysteme der Beteiligungsgesellschaft muss minimiert werden

Mai 2001
Seite 2

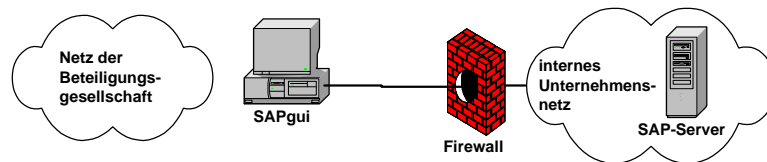
Dr. Tim Sattler: Gesicherte SAP-Anbindung
Tireno Innovations GmbH

Agenda

- *Anforderungen* an gesicherte SAP-Anbindung
- *Realisierung* der gesicherten SAP-Anbindung
 - SAProuter-Proxy
 - IPsec und X.509v3-Zertifizierung
 - Implementation der IPsec-Komponenten
- *Einschränkungen* der realisierten Lösung
- Zusammenfassung

Anforderungen an gesicherte SAP-Anbindung

Bisherige Lösung



- SAPgui-Clientsysteme in dediziertem Netzsegment zusammengefasst und direkt an das interne Unternehmensnetz angebunden.
- Benutzer der Clientsysteme vom Netz der Beteiligungsgesellschaft (E-Mail, Datei- und Druckdienste, etc.) abgeschnitten
 - Probleme mit der Arbeitsorganisation
- Keine ausreichende Kontrolle der strikten Trennung

Sicherheitsanforderungen

- Zugriff nur auf *ausgewählte SAP R/3-Systeme* und nur durch *berechtigte Benutzer*
- *Kein Zugriff auf andere Systeme* im internen Unternehmensnetz
- *Minimale Öffnung der Firewall* zum internen Unternehmensnetz
- Hohe *Verfügbarkeit* der Anbindung
- *Vertraulichkeit* und *Integrität* der übertragenen Daten
 - vom LAN der Beteiligungsgesellschaft zum internen Unternehmensnetz
 - im LAN der Beteiligungsgesellschaft
- *Schutz vor Mißbrauch* der Client-IP-Adressen und *IP-Spoofing*

Weitere Anforderungen

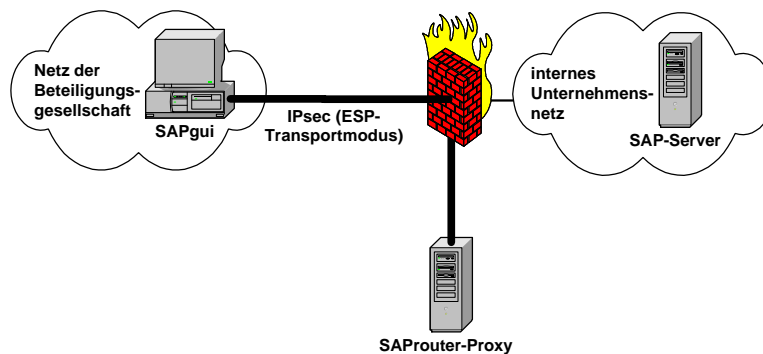
- Problemlose *Integration* der Anbindung in bestehende und zukünftige IT-Infrastruktur
- Möglichst geringfügige Beeinträchtigung der Arbeitsorganisation
- *Interoperabilität* mit Clientsystemen unter
 - Windows 2000 Professional
 - Windows NT 4
 - Windows 95
- Weitestgehende *Verwendung offener Standards*

Mai 2001
Seite 7

Dr. Tim Sattler: Gesicherte SAP-Anbindung
Tireno Innovations GmbH



Neue Lösung



- Zugangskontrolle und -protokollierung über SAProuter-Proxy
- Verschlüsselte Verbindung zwischen SAPgui-Clients und SAProuter-Proxy über IPsec
- Authentisierung der Kommunikationspartner über Digitale Signatur mit X.509v3-Zertifizierung

Mai 2001
Seite 8

Dr. Tim Sattler: Gesicherte SAP-Anbindung
Tireno Innovations GmbH



Realisierung der gesicherten SAP-Anbindung

- SAProuter-Proxy
 - IPsec und X.509v3-Zertifizierung
 - Implementation der IPsec-Komponenten

SAProuter-Proxy: Eigenschaften

- SAProuter stellt Proxy in Netzwerkverbindung zwischen SAP R/3-Systemen dar
- Ermöglicht Zugangskontrolle und –protokollierung nach IP-Adressen und TCP/UDP-Ports
 - Zugriff nur auf ausgewählte SAP R/3-Systeme und -Instanzen
- SAProuter-Proxy wird in der Regel als Ergänzung zu einem bestehenden Firewall-System (*Packet Screen*) eingesetzt
- SAProuter-Software steht für eine große Zahl von OS-Plattformen zur Verfügung (u.a. Solaris, Linux, Windows NT)

SAProuter-Proxy: Einbindung

- Aufstellung des Proxys als eigenständiges System in DMZ an der Firewall zum internen Unternehmensnetz
- Nur SAPgui-Clientsysteme erhalten Zugriff auf Proxy
- Nur Proxy kann auf SAP R/3-Serversysteme zugreifen
 - Minimale Öffnung der Firewall zum internen Unternehmensnetz
- Dedizierte Leitung von den SAPgui-Clientsystemen zum Proxy (Mindestübertragungsrate pro Client: 4 kbit/s)
 - Hohe Verfügbarkeit der Anbindung

Realisierung der gesicherten SAP-Anbindung

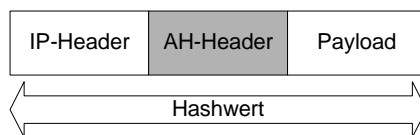
- SAProuter-Proxy
- IPsec und X.509v3-Zertifizierung
- Implementation der IPsec-Komponenten

IPsec für IPv4: Eigenschaften

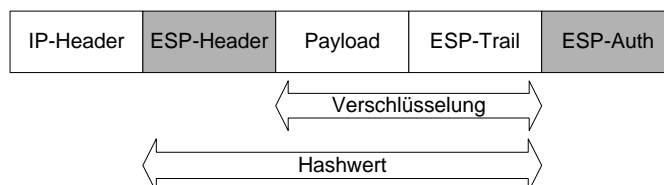
- IPsec bietet Verschlüsselungs- und Authentisierungsdienste auf der Netzwerkschicht
- IPsec stellt zwei IP-Protokollergänzungen zur Verfügung
 - **Authentication Header** (AH; IP-Protokoll 51) schützt *Integrität* der übertragenen Daten und gewährleistet ihre *Authentizität*
 - **Encapsulating Security Payload** (ESP; IP-Protokoll 50) beinhaltet AH-Funktionalität, kapselt aber zusätzlich die zu schützenden Daten ein und gewährleistet deren *Vertraulichkeit* durch Verschlüsselung
- AH und ESP sind „*Frameworkprotokolle*“
 - Es werden keine Algorithmen zur Erzeugung der Schlüssel und Hashwerte *definiert*

IPsec für IPv4: AH und ESP

AH-Protokoll

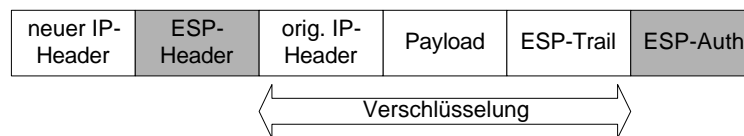


ESP-Protokoll



IPsec für IPv4: ESP-Betriebsmodi I

- Tunnelmodus
 - Ursprüngliches IP-Paket wird in ein neues IP-Paket eingekapselt
 - Anwendung: Kommunikation zwischen zwei Sicherheits-Gateways über ein öffentliches Netz (VPN)
 - IP-Adressen des Ursprungs- und Zielsystem bleiben anonym
 - Verwendung *privater* IP-Adressen über öffentliches Netz möglich

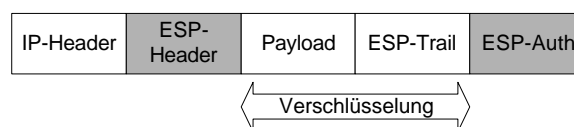


Mai 2001
Seite 15

Dr. Tim Sattler: Gesicherte SAP-Anbindung
Tireno Innovations GmbH

IPsec für IPv4: ESP-Betriebsmodi II

- Transportmodus
 - Nur Daten der Transportschicht werden verschlüsselt, nicht aber der IP-Header
 - Anwendung: *Host-to-Host*-Kommunikation, d.h. im *Tunnelmodus* wäre neu erzeugter IP-Header mit ursprünglichem IP-Header identisch
 - Verwendung *privater* IP-Adressen nur über dedizierte Leitungen möglich



- Kommunikation zwischen SAPgui-Clients und SAProuter-Proxy erfolgt im ESP-Transportmodus

Mai 2001
Seite 16

Dr. Tim Sattler: Gesicherte SAP-Anbindung
Tireno Innovations GmbH

IPsec für IPv4: Internet Key Exchange

- *Internet Key Exchange (IKE)* ist das Standardprotokoll für das Schlüsselmanagement
 - Authentisierung der Kommunikationspartner
 - Aushandeln der *Security Associations (SA)*: Festlegung der verwendeten Verschlüsselungs- und Hashalgorithmen
 - Erzeugung und –regenerierung der Sitzungsschlüssel
- IKE basiert auf zwei Protokollen
 - ISAKMP-Frameworkprotokoll (*Internet SA and Key Management Protocol*)
 - Definiert SAs und setzt Rahmen für Authentisierung und Schlüsselaustausch
 - *Oakley*-Protokoll
 - Konkrete Ausführung der Schlüsselerzeugung

X.509v3-Zertifizierung

- Es erfolgt eine clientbasierte Authentisierung der Kommunikationspartner mit Digitaler Signatur
- Als kryptographischer Algorithmus wird RSA mit einer Schlüssellänge von 1024 bit verwendet
- Für öffentliche RSA-Schlüssel der SAPgui-Clients und des SAProuter-Proxys wird durch unternehmensinterne Zertifizierungsstelle jeweils ein X.509v3-Zertifikat ausgestellt
 - Schutz gegen Missbrauch der Client-IP-Adressen
- Spätere Integration in unternehmensweite PKI vorgesehen

IPsec und Firewalls: Filtereigenschaften

Beispiel: ESP-Transportmodus

Richtung	Quell- adresse	Ziel- adresse	Protokoll	Quellport	Zielport
eingehend	SAPgui- Client	SAProuter- Proxy	UDP 17	ISAKMP 500	ISAKMP 500
ausgehend	SAProuter- Proxy	SAPgui- Client	UDP 17	ISAKMP 500	ISAKMP 500
eingehend	SAPgui- Client	SAProuter- Proxy	ESP 50	N/A	N/A
ausgehend	SAProuter- Proxy	SAPgui- Client	ESP 50	N/A	N/A

Mai 2001
Seite 19

Dr. Tim Sattler: Gesicherte SAP-Anbindung
Tireno Innovations GmbH



IPsec und Firewalls: Einschränkungen

- Firewall muss verschlüsselte IP-Pakete anhand des verwendeten IP-Protokolls 50 (ESP) bzw. 51 (AH) filtern können (z.B. Checkpoint FW-1)
- Zugriffe auf nicht für die Anwendung (SAP R/3) erforderliche TCP/UDP-Ports müssen auf dem IPsec-Zielsystem hinter der Firewall (SAProuter-Proxy) abgewehrt werden
- NAT bzw. *IP Masquerading* zwischen IPsec-Kommunikationspartnern (SAPgui-Client ↔ SAProuter-Proxy) problematisch
 - NAT modifiziert den Header der durchgehenden IP-Pakete
 - IPsec-Authentisierung schlägt fehl, falls die übermittelten IP-Pakete auf dem Weg zwischen den IPsec-Kommunikationspartnern modifiziert wurden

Mai 2001
Seite 20

Dr. Tim Sattler: Gesicherte SAP-Anbindung
Tireno Innovations GmbH



Realisierung der gesicherten SAP-Anbindung

- SAProuter-Proxy
- IPsec und X.509v3-Zertifizierung
- Implementation der IPsec-Komponenten

IPsec-Implementation auf SAProuter-Proxy

- Getestete OS-Plattformen
 - *Sun Microsystems Solaris 8*
 - Vorteil: OS unterstützt AH und ESP
 - Nachteil: Schlüsselmanagement durch proprietäres SKIP-Verfahren (*Simple Key-management for Internet Protocols*), keine IKE-Unterstützung
 - *Linux (Kernel 2.2.16) mit IPsec-Implementation FreeS/WAN Version 1.8*
 - Vorteil: IKE-Unterstützung durch FreeS/WAN, GPL-Software
 - Nachteil: Für RSA-Authentisierung basierend auf X.509v3-Zertifikaten zusätzlicher Patch benötigt
- Für den SAProuter-Proxy wird Linux FreeS/WAN eingesetzt

Linux FreeS/WAN: Komponenten

- KLIPS (Kernel IPsec)
 - Verschlüsselung
 - Berechnung der Hashwerte
 - Erzeugung der ESP- und AH-Header für ausgehende IP-Pakete
 - Interpretation der ESP- und AH-Header für eingehende IP-Pakete
- Pluto (IKE-Dämon)
 - Authentisierung der Kommunikationspartner
 - Aushandeln der ISAKMP und IPsec SAs
 - Schnittstelle zu KLIPS

Linux FreeS/WAN: Verwendete Algorithmen

- Linux FreeS/WAN unterstützt als einziges *symmetrisches* Verschlüsselungsverfahren *Triple DES* (3DES) mit einer Schlüssellänge von $3 \cdot 56 = 168$ bits und drei unterschiedlichen Schlüsseln in der Operationsfolge EDE (*encrypt-decrypt-encrypt*)
- DES-Unterstützung ist zwar Bestandteil des IPsec-Standards; das Verfahren gilt jedoch inzwischen als nicht ausreichend sicher und wird daher von Linux FreeS/WAN nicht unterstützt
- Als Hash-Algorithmen können sowohl MD5 als auch SHA-1 verwendet werden

IPsec-Implementation auf SAPgui-Clients

- Getestete OS-Plattformen und VPN-Clients
 - Windows 2000 Professional
 - Vorteil: OS unterstützt IPsec und X.509v3-Zertifikate
 - Nachteil: Ohne *High Encryption Pack* nur einfache DES-Verschlüsselung
 - PGPnet 6.5.3 und 7.0.3
 - Vorteil: Läuft auf allen Windows-Plattformen
 - Nachteil: Relativ hohe Lizenzkosten
 - SafeNet SoftPK 5.1.0
 - Vorteil: Relativ günstige Lizenzkosten, läuft auf allen Windows-Plattformen
 - Nachteil: ASN.1 *Distinguished Name* (DN) der X.509v3-Zertifikate darf kein EMAIL-Attribut enthalten, unnötige Einschränkung der Flexibilität

Einschränkungen der realisierten Lösung

Missbrauch einer authentisierten Verbindung

- Kompromittierung der SAPgui-Clientsysteme
 - Viren
 - Würmer
 - Trojaner
- Fehlverhalten berechtigter Benutzer
 - Weitergabe des Passworts
 - Sabotage
- Minimalanforderungen an Schutz des Netzes auf der Clientseite
 - Virens Scanner
 - Firewall

Abhören im internen Unternehmensnetz

- Fehlende Verschlüsselung der IP-Pakete im internen Unternehmensnetz
- Möglichkeit des Abhörens in diesem Bereich weniger relevant als im Netz der Beteiligungsgesellschaft
- SAPgui-Clients im internen Unternehmensnetz nutzen in der Regel keine Verschlüsselung

Zusammenfassung

- Lösung für die gesicherte Anbindung externer SAPgui-Clients an SAP R/3-Server im internen Unternehmensnetz
- Zugangskontrolle und –protokollierung durch Anbindung über einen Proxy mit SAProuter-Software
- Gewährleistung von Integrität, Vertraulichkeit und Authentizität der übertragenen Daten durch Verschlüsselung der IP-Pakete auf dem gesamten Übertragungsweg zum Proxy und RSA-Authentisierung der Kommunikationspartner basierend auf X.509v3-Zertifikaten
- Interoperabilität der IPsec-Implementation Linux FreeS/WAN auf dem Proxy mit Windows 2000 Professional und kommerzieller VPN-Clientsoftware
- Leichte Übertragbarkeit auf andere Anwendungsfälle, sofern ein geeigneter Proxy zur Verfügung steht