Att bygga VPN

Kenneth Löfstrand, IP-Solutions AB

kenneth@ip-solutions.se

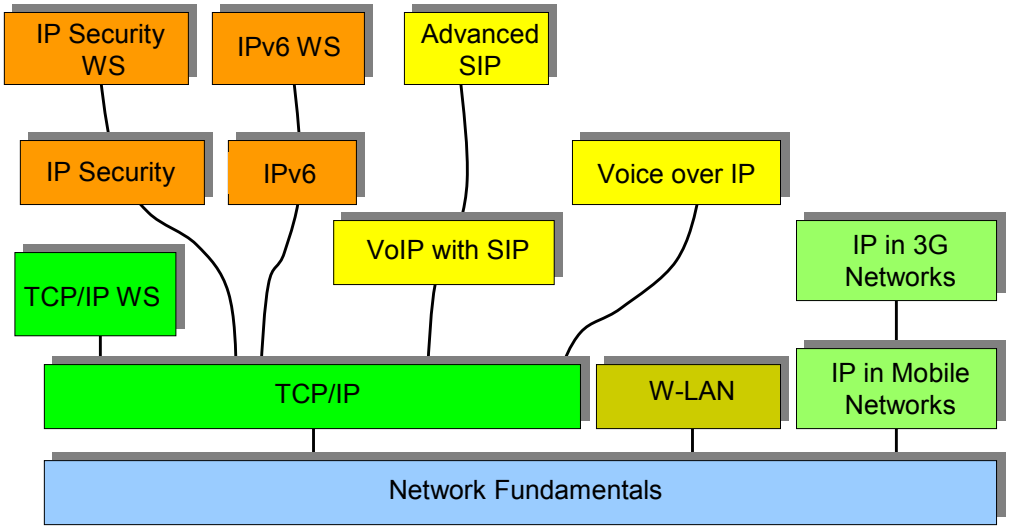
Agenda

- Olika VPN scenarios
- IPsec LAN - LAN
- IPsec host - host
- SSH

IP-Solutions - Konsultverksamhet

Oberoende konsulter!

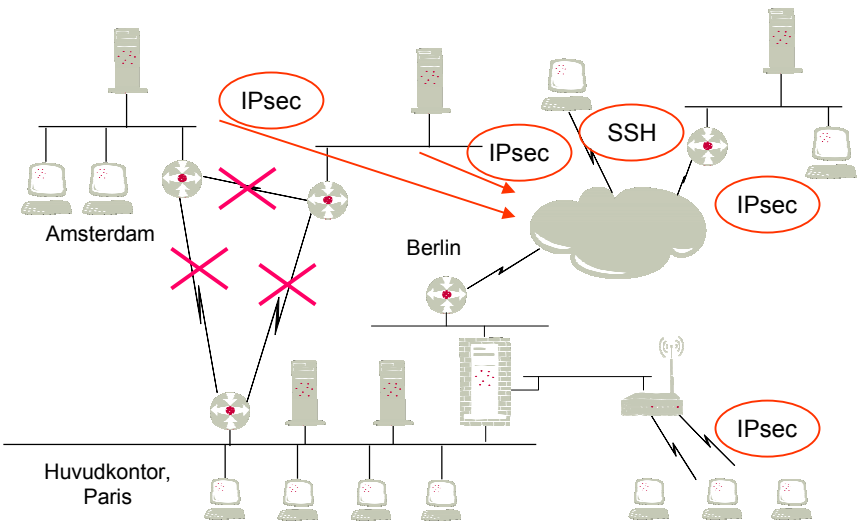
IP-Solutions - Kursverksamhet



Olika IP-baserade VPN-lösningar

DNS **DNSSEC**	E-mail **PGP, SMIME**	**…**	Applikation
TCP **SSH, SSL/TLS**	UDP		Transport
IP **IPsec**			Internet
L2TP			Data Länk

VPN



IPsec - I korthet

- **Tunnel mode**
  - trafiken går via en gateway
  - används vanligtvis nät-till-nät
  - trafiken mellan gateway och ändutrustning är oskyddad
- **Transport mode**
  - ingen gateway används
  - används mellan ändutrustningar
  - trafiken skyddad hela vägen
- **AH - IP Authentication Header**
  - verifikation av avsändarens identitet
  - kontrollerar ett meddelande inte förändras
  - säkerställer avsändarens IP adress
- **ESP - Encapsulating Security Payload**
  - verifikation av avsändarens identitet
  - kontrollerar ett meddelande inte förändras
  - krypterat data
- **Öppen för olika krypterings- och autentiseringsalgoritmer**

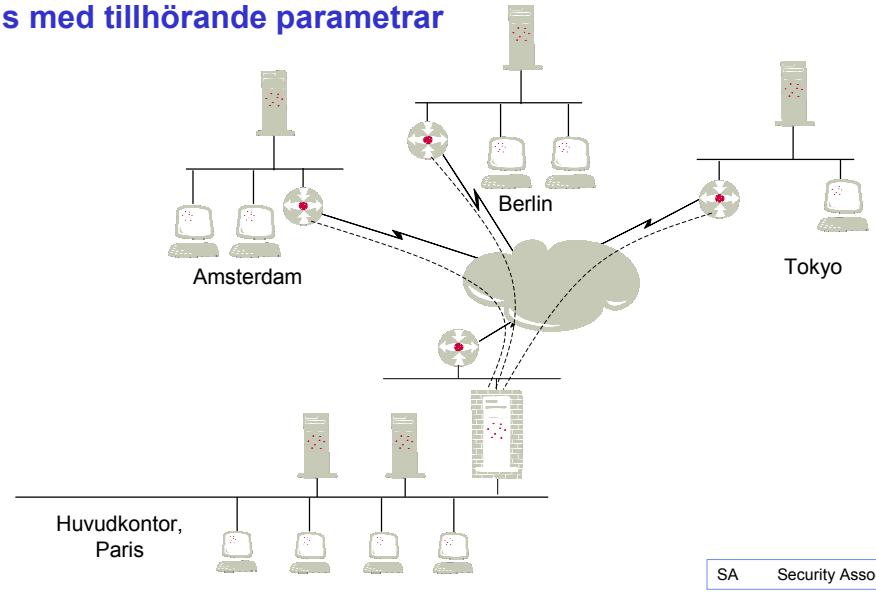
Vilka algoritmer ska användas? Vilka nycklar?

- **Autentisering**
  - MD5
  - SHA-1
- **Kryptering**
  - DES
  - 3DES
  - IDEA
  - Blowfish
  - AES

Är detta viktiga frågor?

Självklart, men vi vill att programvarorna kommer överens om vad som ska användas!

SA's med tillhörande parametrar



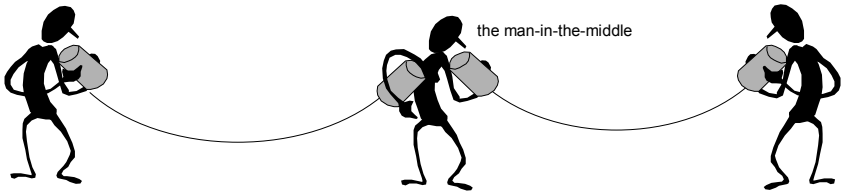
SA Security Association

Frågeställningar och svar

Transport eller tunnel mode?	Tunnel mode (i dessa fall)
Algoritmer?	Låt programvarorna välja (ISAKMP) exkludera dom du inte gillar och/eller andra sidan inte stödjer
Kryptonycklar?	Låt programvarorna välja (Diffie-Hellman)
Hur kan vi lita på att andra sidan är en av våra vänner?	?
Vilken trafik tillåter vi?	Det måste vi någonstans beskriva för programvaran (SPD)

Nyckelutbyte

- **Diffie-Hellman nycklarna skickas i vanliga IP-paket, som lätt kan förfalskas!**
  - Vi måste kunna authenticera dessa, och säkerställa avsändaren
- **Hur?**
  - Pre-shared key, dvs lösenord.
  - Publik Key Crypto, Asymmetriska krypteringsalgoritmer
  - Digitala signaturer, oftast X.509 certifikat.



Public Key

- Skapa nyckelpar för varje gateway
- Allas publika nycklar distribueras till samtliga gateways

Skapa en CA

- Generera nyckelpar, publik och privat nyckel
- CA skapar ett “certificate request”
  - Detta är början till certifikatet, men ännu ej signerat
- CA signerar sitt eget “certificate request” med sin egen privata nyckel
  - Nu har vi ett CA certifikat innehållande CA:s publika nyckel
- Detta certifikat distributeras till alla gateways
  - => Alla måste lita på vår CA
  - Se till att CA certifikatet distribueras på ett säkert sätt

Detta är enkelt att göra inom en egen organisation

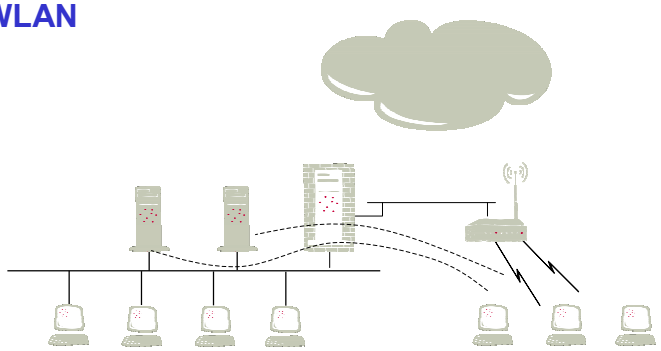
För att certifikat ska fungera mellan organisationer krävs en CA ”i toppen”

CA	Certificate Authority

Gateway certifikat

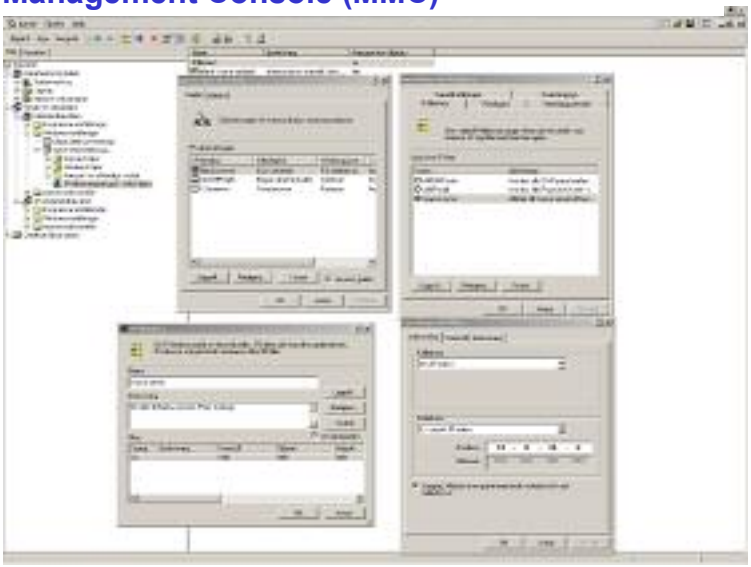
- Generera nyckelpar, publik och privat nyckel
- Skapa ett “certificate request”
- Skicka detta “certificate request” till CA
- CA signerar gatewayens “certificate request” med sin egen privata nyckel
  - Certifikatet för gatewayen är klart
- Skicka certifikatet till gatewayen

IPsec över WLAN



- Transport mode
- I mindre skala kanske det duger med pre-shared keys
- Policydatabasen sätts upp så att viss trafik skyddas av IPsec (till interna servers) och annan trafik (till Internet) inte påverkas

Microsoft Management Console (MMC)

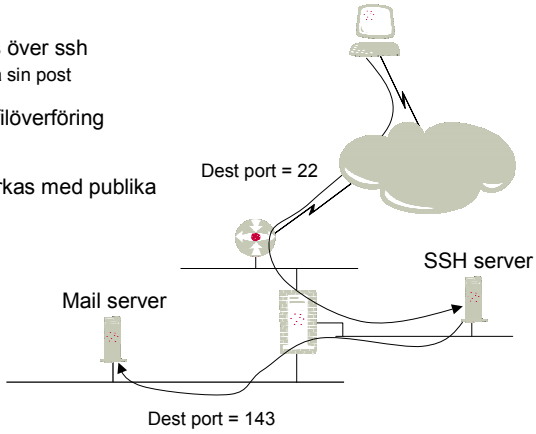


SSH, Secure Shell

- Krypterad terminalförbindelse
  - …
- Annan trafik kan tunnlas över ssh
  - Ofta använt för att läsa sin post
- Finns även funktion för filöverföring
  - SFTP eller scp
- Autentiseringen kan stärkas med publika nycklar

Mail klient konfigureras för att hämta post från 127.0.0.1

SSH klient konfigureras för att acceptera port 143 och skicka denna trafik till mail server via ssh server



Vad kostar kalaset?

IPsec och ISAKMP	Finns redan i de vanligaste operativsystemen
Arbetsinsats	Enstaka timmar (per dator)
SSH Server	Ingår i BSD, Linux Windows 2000: Cygwin (freeware) Windows: VShell Enterprise (Van Dyke): cirka 5000 kronor
SSH Klient	Ingår i BSD, Linux Putty (Windows XX): Freeware Secure CRT: cirka 1000 kr per klient

Fallgropar

- DHCP adresser
- Privata adresser som översätts
- Olika programvaror i de två ändarna
- Implementationen av VPN blir en del av övrig infrastruktur
- Mänskliga kommunikationsproblem
- Blev trafiken krypterad?
- Policy för hantering av certifikat

Sammanfattning

- IPsec är en Internet standard för VPN
- IPsec är kraftfullt och en avancerad/komplicerad teknik
- Operativsystemen har numera stöd för IPsec och IKE/ISAKMP
- Finliret handlar om design, autentisering (kan inkludera hantering av certifikat) och policy
- WLAN är till sin natur öppna men trafiken kan säkras upp genom att använda IPsec
- SSH kan med fördel användas för att säkra upp trafik från hemmet, hotellrum och så vidare mot företagsnät