The golden age of hacking

Firewalls

ARP

Application level security

SSL, IPSec

Router and Firewalls

Movie: http://www.warriorsofthe.net

- Static routes
- Dynamic routes
  - Routing Information Protocol (RIP)
  - Open Shortest Path First (OSPF)
  - Border Gateway Protocol (BGP)
- Source Routing
  - Every packet has its own route list
- En firewall kan ses som en slags gränsvakt för datatrafiken, vilket är ett naturligt steg - jmf. lås i ytterdörren (på både insida och utsida)
  - Personlig eller gemensam i nätverket?
  - Erbjuder separation mellan olika nät beroende på tillit
  - Att sätta upp skalskydd kräver inventering och analys av nätverkstrafik, behov etc. vilka tjänster ska exponeras?

Router attacker

- Ändra i routingtabellens konfiguration (intrång)
- Göra routingtabellen korrupt (sända felaktig data)
  - Ganska enkelt då det inte finns någon autentiseringsmekanism i RIP (Routing Information Protocol)
  - Felaktig routertabell innebär att IP-paket anländer till fel destination
- RIP v2 och OSPF (Open Shortest Path First) har ett autentiseringsfält men det sänds okrypterat med varje meddelande
- Ett annat routingprotokoll BGP (Border Gateway Protocol) sätter upp en TCP länk och är svårare att hacka
  - En attackerare kan dock sända felaktiga ICMP ”redirect” meddelanden och därigenom få routern att skapa en ny path till en viss destination
  - ICMP ”destination unreachable” (type = 3) kan också vara ett hot i syfte att ta bort en path, se control message koder
- Bästa skyddet är att ha statiska (manuella) tabeller för alla externa hostar och/eller blockera inkommande router meddelanden från utomstående hostar

Firewalls (brandväggar)

- Grundtekniker och funktioner i brandväggen
  - Paketfiltrering (vad man oftast menar med firewall)
  - Routing, NAT (Network Adress Translation)
  - Proxyfunktion (oftast bundet till en applikation)
  - Övervakning och loggning
- Extra funktioner
  - Cachelagring (hämtar data som passerat flera ggr. genom brandväggen från en cache istället från nätet)
  - Intrångsupptäckt (om ett visst misstänkt mönster uppträder, larma admin och blocka IP-adressen)
- Begränsningar
  - Skyddar inte mot attacker som inte passerar genom brandväggen, t.ex. uppringd förbindelse, WLAN etc.
  - Hindrar inte elak kod (malware)
- Två grundmallar kan sägas finnas
  - Allt som inte är tillåtet är förbjudet (bäst!)
  - Allt som inte är förbjudet är tillåtet

Tillståndslös paketfiltrering

- First generation firewalls
- Oftast i enklare FW eller i kombination med mjukvaru-router
- Paketets header inspekteras utifrån protokolltyp, IP-adress, TCP/UDP-port, control bits, m.m.
  - Beslutet grundas enbart på aktuellt paket
  - Nyttoprogram kan blockeras om deras paket har ogiltig header (tex. fragmenterat pga. MTU skillnad i WAN/LAN), använder portar dynamiskt eller använder UDP (förbindelselöst)
- Otillåtna protokoll/paket blockas/kastas bort via filter baserat på
  - Källadress och port
  - Destinationsadress och port
  - Förbindelsens riktning (TCP ACK flaggan)
  - Trusted - untrusted network
- Filterreglerna kallas för ACL (Access Control List)
  - ALLOW (PERMIT), DENY (BLOCK, DROP) etc.
- Trots nackdelar så är tillståndslös paketfiltrering ändå effektivt i att stoppa broadcast-attacker (smurf) och att blockera portar

Tillståndsstyrd paketfiltrering

- Second generation firewalls
- Dynamisk uppdaterad ”state”-tabell
- Jobbar på samma sätt som tillståndslös paketfiltrering men gör ALLOW eller DENY baserat på
  - Innehållet i nuvarande paket och i föregående paket
- Löser många av problemen med tillståndslös paketfiltrering genom att hålla en kommunikationsförbindelse öppen
  - Caching av första paketfragmentet eller
  - Tillåta reply till ”godkända” utomstående UDP requests
  - Strömmar av samma trafik kan därigenom spåras
- Ofta ingår även proxy-funktioner
- Som regel en tyngre serverapplikation, t.ex.
  - Check Point FireWall-1, Cisco PIX

Application filtrering

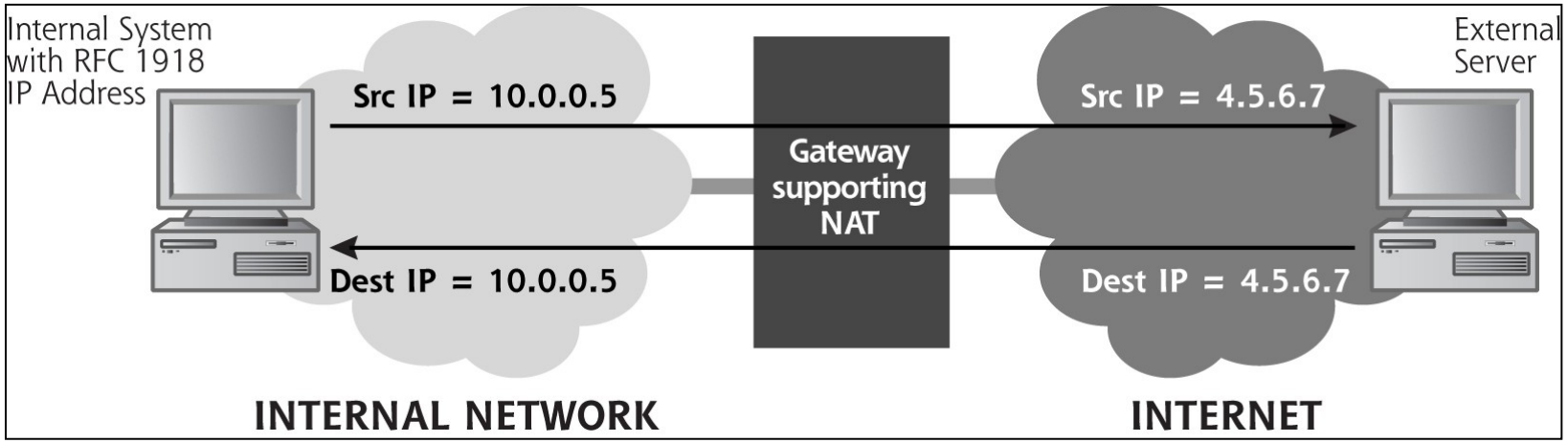
- Third generation firewalls, 2009/2010 >
- Network-based application firewalls
- Host-based application firewalls
- The key benefit of application layer filtering is that it can "understand" certain applications and protocols such as File Transfer Protocol, DNS or HTTP etc.
- It can detect if an unwanted protocol is sneaking through on a non-standard port or if a protocol is being abused in any harmful way
- An application firewall is much more secure and reliable compared to packet filter firewalls because it works on all seven layers of the OSI model, from the application down to the physical Layer
- Examples: MS-ISA (Internet Security and Acceleration) server, McAfee Firewall Enterprise
- http://en.wikipedia.org/wiki/Application_layer_firewall

Circuit-Level Gateway (CLG)

- Arbetar på transportlagret
  - Dvs. TCP/UDP, firewalls jobbar även på IP (nätverk)
- Klienten ansluter till en TCP port på servern som har en tjänst igång som ”osynligt” vidarebefordrar trafiken i båda riktningarna
  - Exempel på tjänst: Socket Secure (SOCKS), arbetar på session layer 5 i OSI
- Vissa program har egna inställningar för SOCKS som t.ex. webbläsare etc.
- Finns inbyggt i vissa firewalls och blir där transparent för användaren
- Finns även som fristående applikation, tex.
  - Dante, WinGate
- Listor finns på Internet med öppna SOCKS-servar

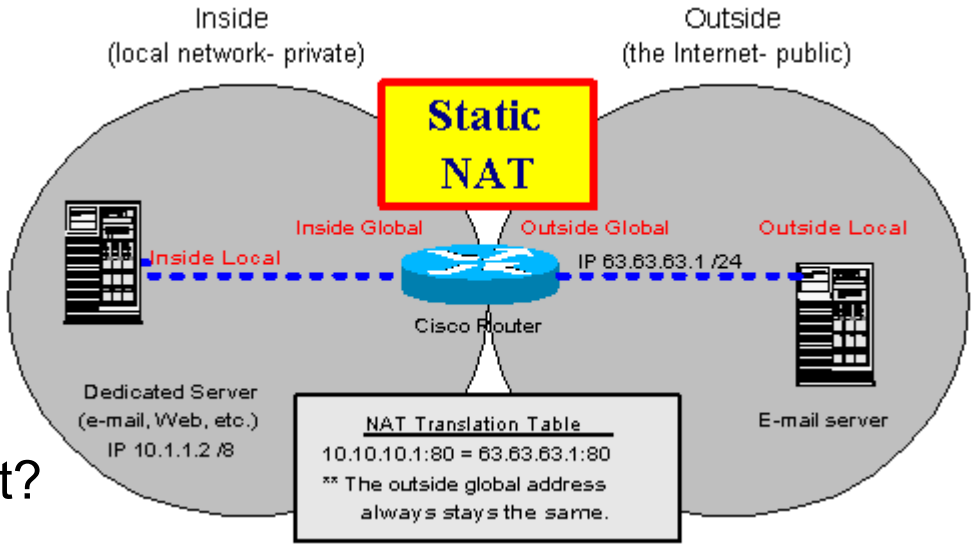
NAT eller network/IP-masquerading

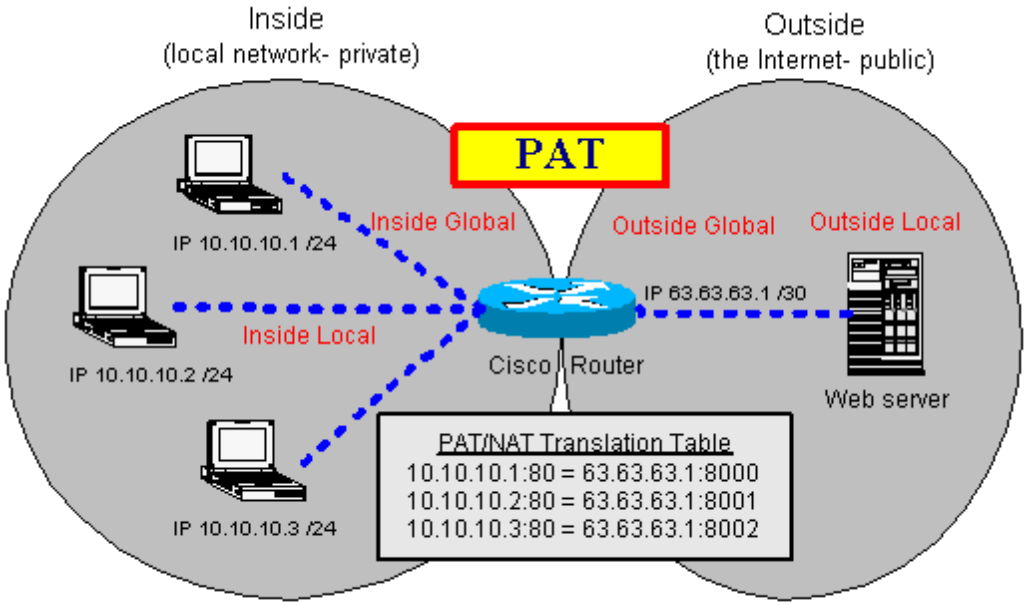
- Mycket vanligt i routrar hemma eller på små arbetsplatser
- Tillåter ett antal privata adresser att nå Internet via en publik adress genom manipulation av IP-headern (NAT mapping)
  - Mapping to single external IP address
  - One to one mapping
  - Dynamically allocated address (address multiplexing, uncommon)
- Omvandlar dolda privata (interna) IP-adresser till publika IP-adresser, privata IP-serier:
  - 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255 och 192.168.0.0 – 192.168.255.255
- Nackdelen är att protokoll/applikationer som kräver en öppen returkanal ofta inte fungerar korrekt t.ex. PPTP (Point-to-Point Tunneling Protocol)
- **Do a NAT gateway increase security?**

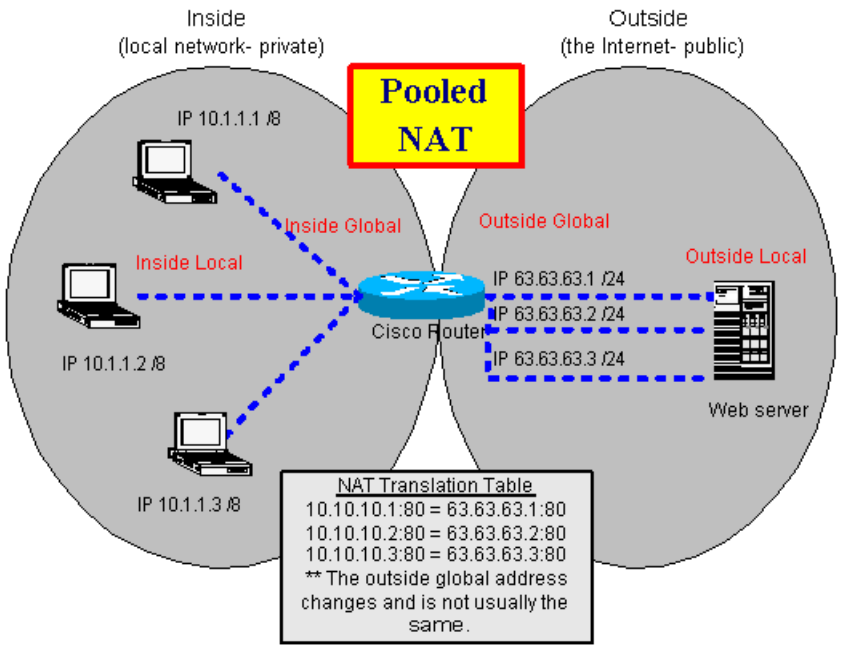


PAT (Port Address Translation)

- Kallas även NAPT
- NAT konfigureras på 3 sätt
- Static NAT
  - Port forwarding (permanent open)
  - Port triggering (opened from inside)
- PAT = NAT overloaded
- Pooled NAT
- NAT/PAT local loopback support?



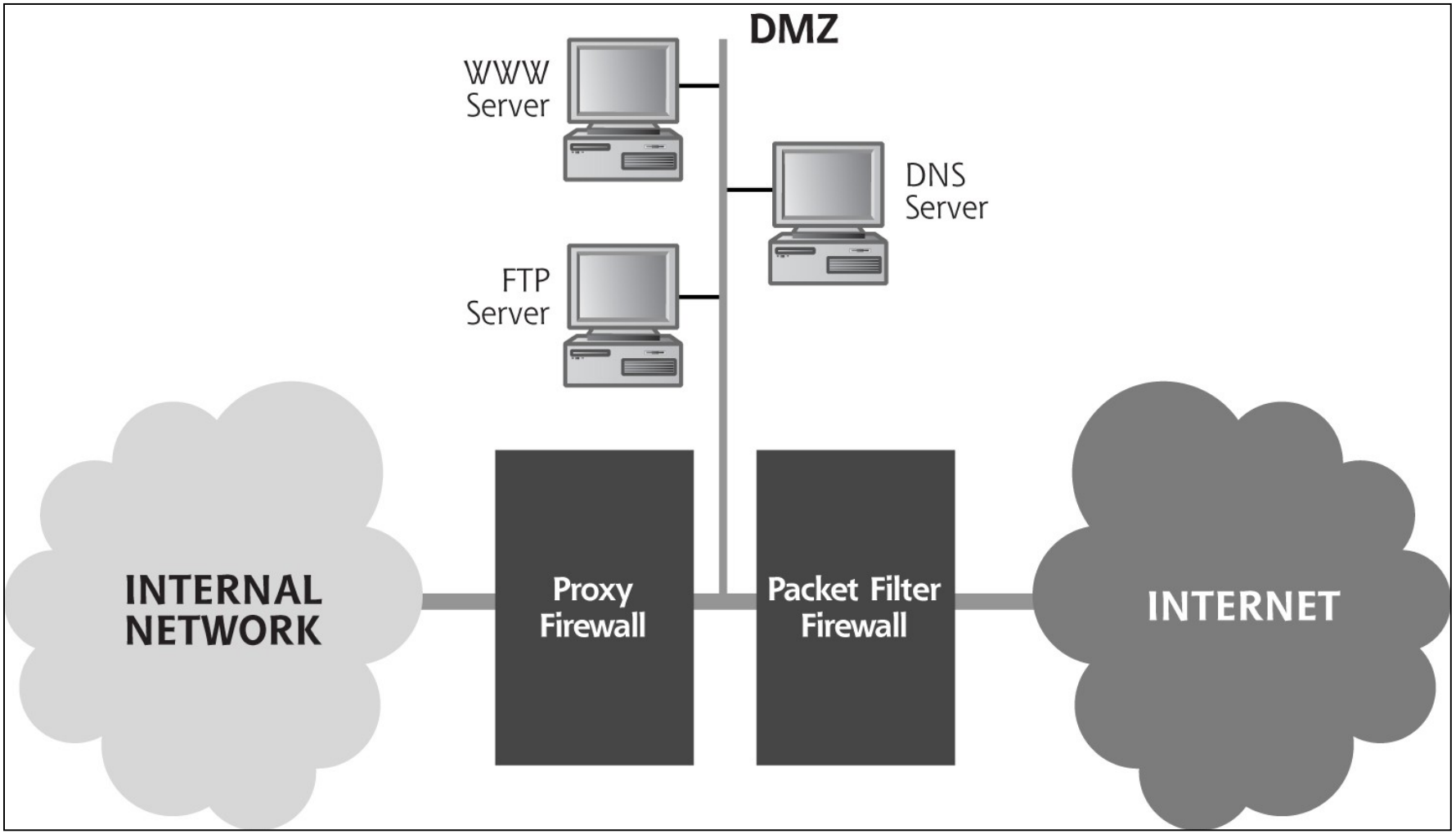




Proxyfunktion

- Funktionen påminner om föregående brandväggstekniker och i synnerhet CLG:er men ligger på en högre nivå
- En proxyserver tillåter klienter att skapa en indirekt nätverksförbindelse på protokoll/applikationsnivå (oftast HTTP)
- En klient som t.ex. begär en fil från en webbserver hämtar denna via proxyn, som i sin tur endera hämtar den från en egen cache eller från webbservern
- Proxyn kan inspektera, kontrollera äkthet och ändra i klientens begäran eller webbserverns retur och ibland även neka/blockera åtkomsten
- Proxyn loggar oftast nätverkstrafiken
- Flera kommersiella och fria Proxies finns
  - Juniper, Symantec Enterprise Firewall, Squid, MS Proxy Server etc.
- Den viktigaste skillnaden mellan teknikerna är att
  - Proxies och CLG:er agerar som ändanslutning för klienterna
  - Tillståndsfilter gör det inte

Common proxy & firewall architecture



Firewalls (brandväggar)

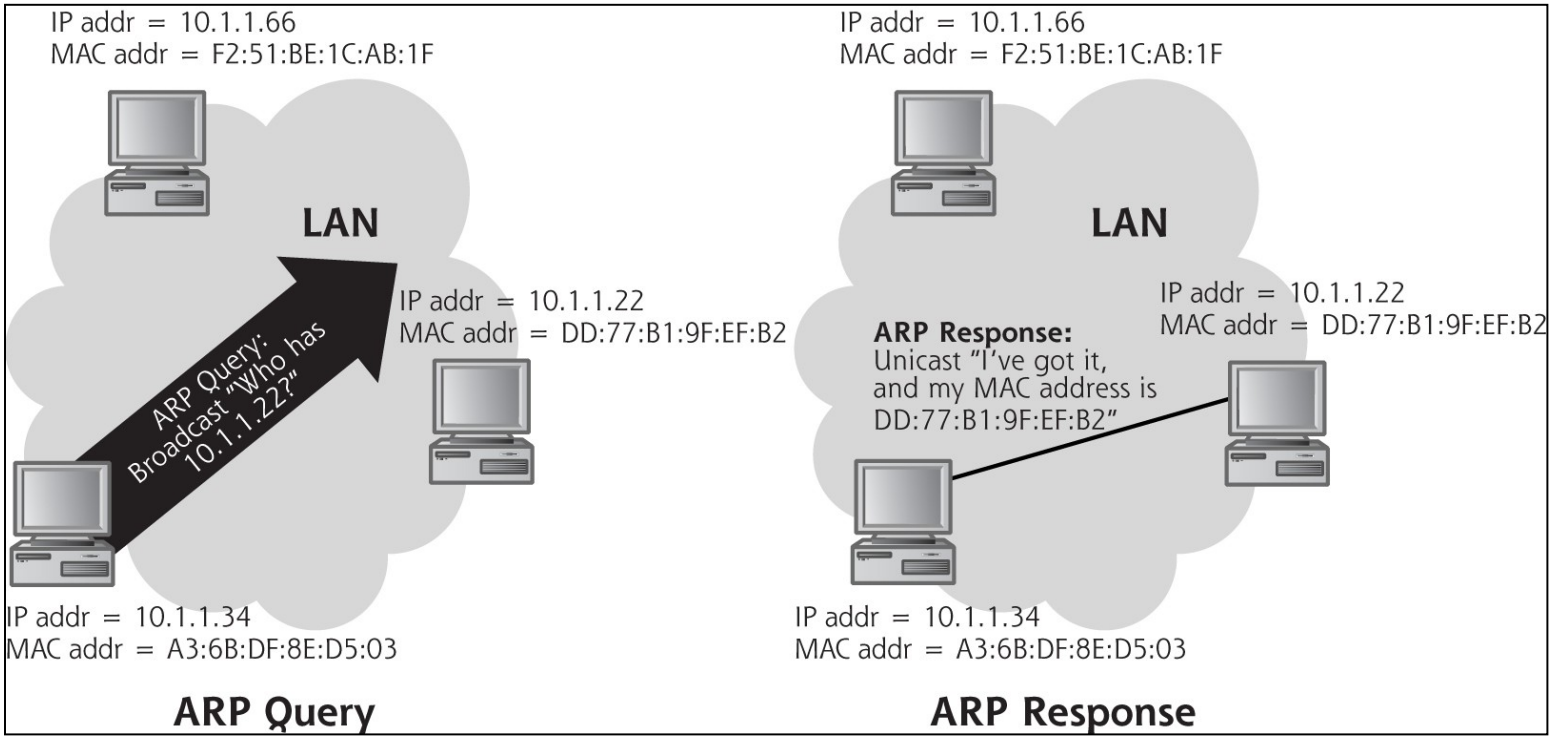
- Krav på funktioner och budget styr valet av brandvägg
  - Säkerhetskrav
  - Trafiknivå
  - Vilka tjänster
  - Lista finns på http://www.timberlinetechnologies.com/products/firewalls.html
- Ofta får man problem med vissa tjänster utåt om man lägger hela nätet bakom en brandvägg
  - Prestanda
  - Säkerhet
  - Åtkomst (inifrån <-> ut)
  - Administration
- Single-box (Screened router)
- Dual-Homed Host
- Screened Host Arkitektur
- Screened Subnet Arkitektur
- Läs mer
  - http://hem.passagen.se/jborge/brand/3.html

Personlig brandvägg

- En programvara som liknar en nätverksbrandvägg fast mycket enklare
- Filtrerar in och utgående data baserat på TCP/UDP portnummer och/eller protokoll-id/applikations-id
- Mål - enkel att ställa in och använda
- Post- och telestyrelsen har ett test och andra tips för både hemanvändare och företagare/ansvariga
  - ShieldsUP > https://www.grc.com/x/ne.dll?bh0bkyd2
  - PTS > https://testadatorn.pts.se
- Loggar och varnar
  - De flesta användare brukar stänga av funktionen
- Exempel
  - MS Windows firewall (Security Center, kom med XP sp2), BlackICE, ZoneAlarm m.fl.

ARP (Address Resolution Protocol)

- MAC (Media Access Control), unique 48 bit hardware address
  - Används inom IPv4 för att koppla samman en Ethernet MAC hårdvaru-adress till en IP-adress
- ARP protokollet är metoden (mellanhanden) som används för att hitta en värds hårdvaruadress när endast protokoll (t.ex. IP) -adressen är känd, dvs. klistret mellan länk och nätverkslager

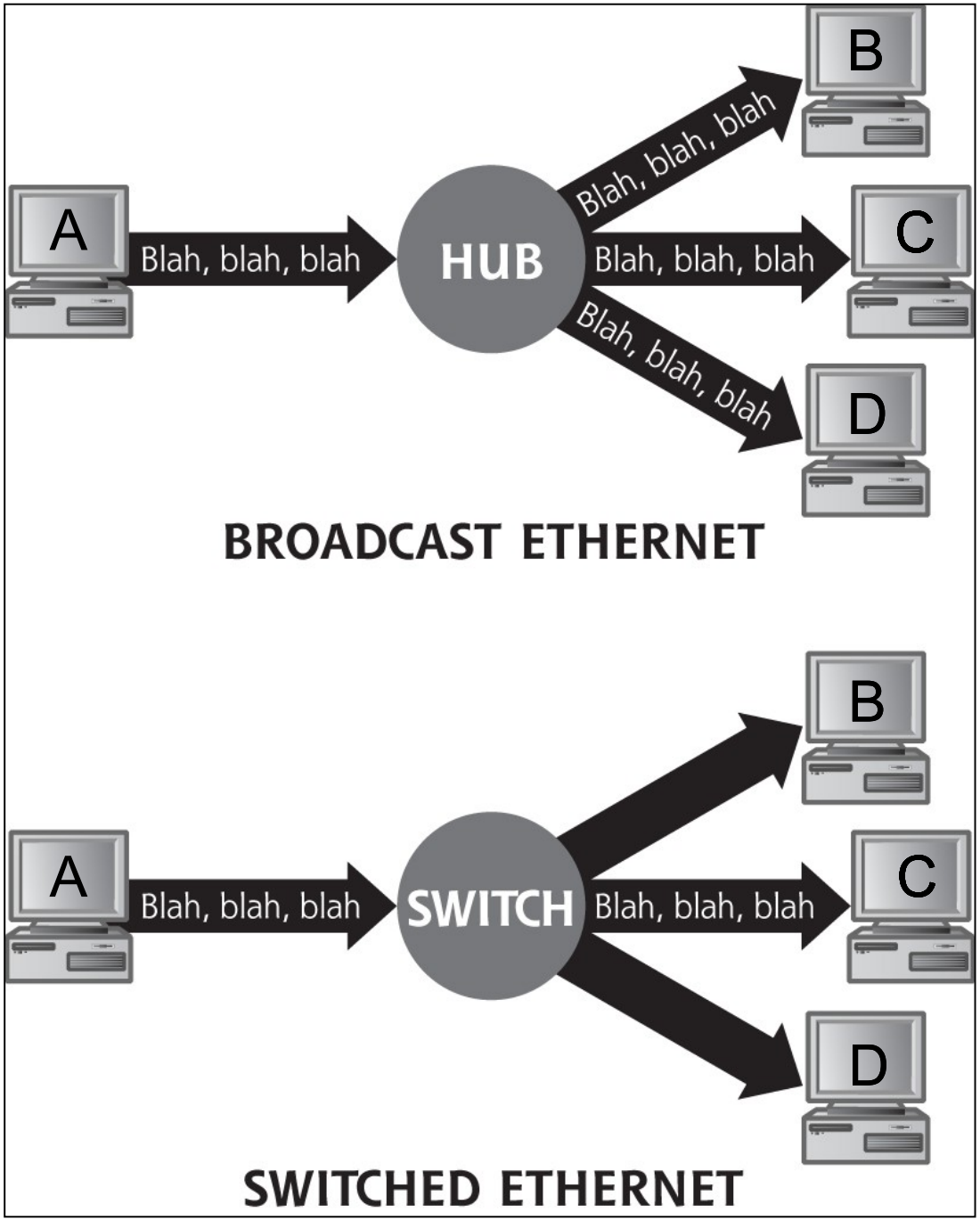


ARP (Address Resolution Protocol)

- Värdnamnet, ARP och IP identifierar värden men har ingen metod för att verifiera identiteten (att rätt MAC/IP adress är kopplad)
  - Vanligaste hotet är att värden maskerar sig som en annan redan auktoriserad värd
- ARP används när värdar kommunicerar direkt/indirekt, tex. när:
  - Två värdar finns på samma nätverk och en vill sända ett meddelande
  - Två värdar finns på olika nät och de måste använda en router/gateway för att nås
  - En router behöver forwarda ett meddelande från en värd genom en annan router
  - En router behöver forwarda ett meddelande från en värd till destinationsvärden på samma nätverk
- Alla värdar har en ARP tabell
  - Är en slags cache där IP/MAC adress-mappningen finns, förnyas periodiskt
  - Kommandot arp -a listar aktuella entrys i tabellen
- Referens: http://www.eventhelix.com/RealtimeMantra/Networking/Arp.pdf

Switch vs Hub

- Destination MAC address is C
- Only send/forward information on interface connected to C

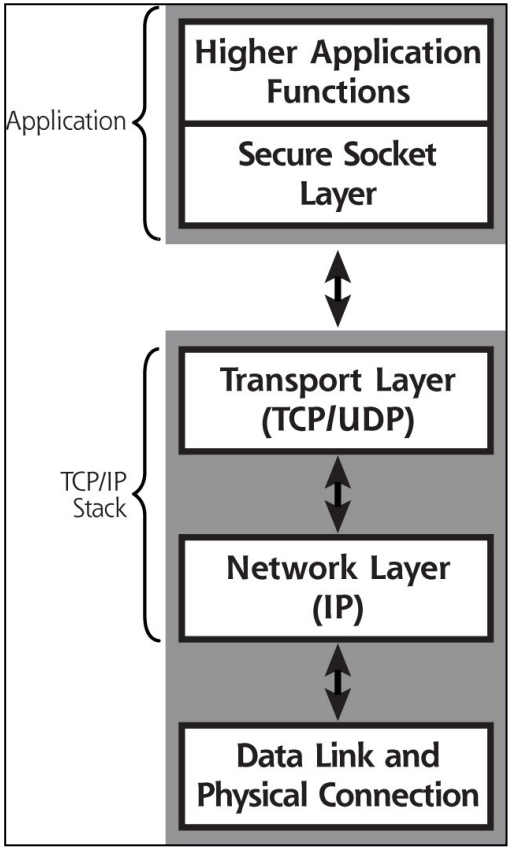


Wi-Fi, WLAN, 802.11x

- Very similar to a hub, first standard defined in 1997
  - Old standars as 802.11a, 802.11b - not common
  - 802.11g - 54 Mbit, WPA-PSK [TKIP]
  - 802.11i – with stronger encryption, WPA2-PSK [AES] (CCMP)
  - 802.11n – standard 2009, 54 - 600 Mbit/s
  - 802.11ac – draft 4.0 2013, 0,5 – 1 Gbit/s
- Two modes
  - Infrastructure (AP – Access Point)
  - Independent (peer-to-peer)
- Controlled by management frames (used by the attackers)
  - Beacon – Announce existence
  - Probe request – List AP:s
  - Probe response – Indicate presence
  - Association request – Join WLAN
  - Association response – AP grant access
  - Disassociation – Tear down

Nätverkskrypteringstjänster

- TCP/IP got no native security
- Applikationskryptering
  - T.ex. PGP, S/MIME, SSH
  - Kräver användarinteraktion
- ”Middleware”-kryptering
  - T.ex. SSL/TLS
  - Kräver att applikationen är skriven mot krypteringstjänstens API, t.ex. HTTPS är modifierat att gå över SSL
- Kryptering på nätverksnivå
  - T.ex. IPsec
  - Kräver inget av ovanstående (IP/nätverksnivån…)



Secure Sockets Layer (SSL) och efterträdaren Transport Layer Security (TLS)

- SSL (standardiserat av Netscape) och TLS erbjuder end-to-end säkerhet för autentisering och information genom kryptering
- Typiska användningen är att endast servern är autentiserad (dvs. dess identitet verifierad) medan klienten är icke-autentiserad
- Skall båda autentiseras så måste PKI eller liknade användas
- Klienten och server förhandlar om vilka algoritmer som stöds
  - För public-key krypto: RSA, Diffie-Hellman, DSA eller Fortezza
  - För symmetriska chiffer: RC2, RC4, IDEA, DES, Triple DES eller AES
  - För one-way hash funktioner: MD5 eller SHA-x
- Protokollet förhindrar (i bästa fall):
  - Avlyssning (kan tolka innehållet - eavesdropping) ”man in the middle” attacker (MITM)
  - Förändring (tamper-evident)
  - Förfalskning (message forgery)

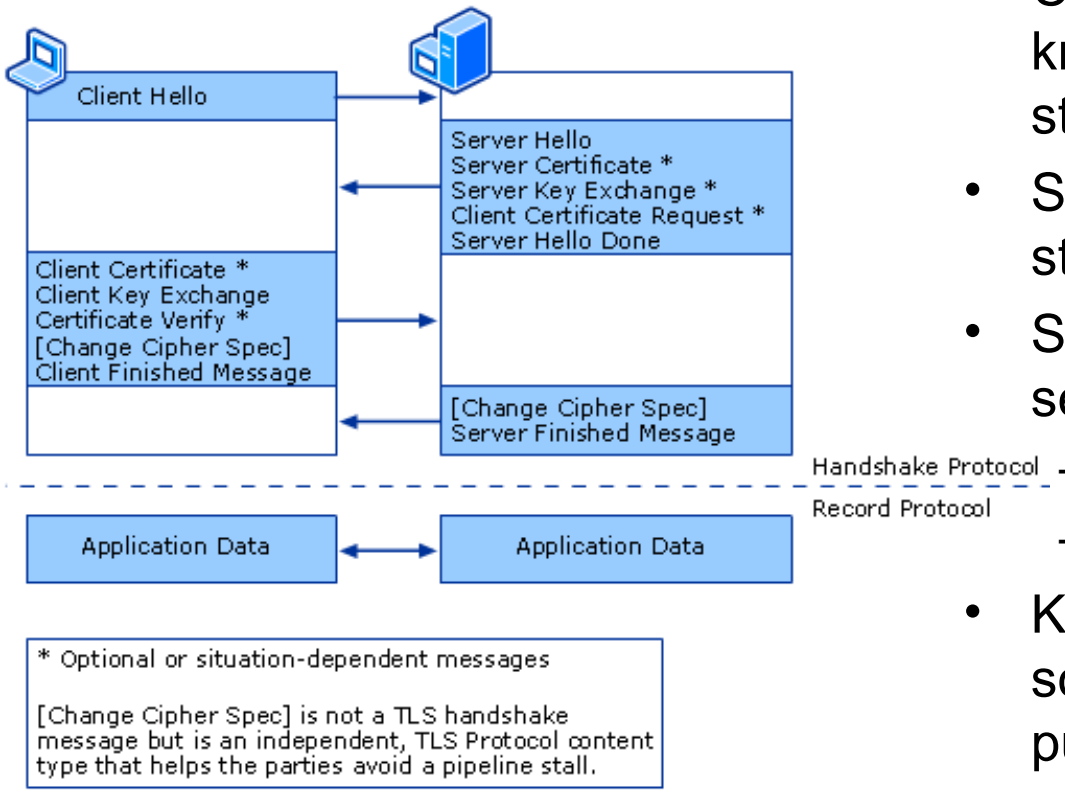
HTTPS (HTTP med SSL/TLS)

- SSL/TLS körs på en nivå under andra applikationsprotokoll som:
  - HTTP, SMTP, NNTP osv.
  - Och en nivå ovanför TCP - vilket innebär att det kan användas till de flesta applikationer/protokoll som inte har eget stöd för SSL/TLS
  - T.ex. Stunnel (www.stunnel.org) och SSL VPN - kapslar in datatrafiken
- HTTPS är mycket vanligt när vi surfar till banken etc. eller andra viktiga e-tjänster på nätet och körs default på port 443
- För att köra igång en webbserver med HTTPS krävs
  - Ett public key certifikat skapat med t.ex. OpenSSL:s ssl-ca
  - Certifikatet måste sedan signeras av en CA (Certification Athority)
    - ”Single sites” och organisationer kan ha en egen CA, som t.ex. HDa
    - Vanligen köper man ett certifikat av någon stor CA som t.ex. **VeriSign** eller **thawte** som anslutna webbläsare kan verifiera servern emot
  - Installation och konfiguration av SSL/TLS moduler för webbservern
  - Oftast krävs en äkta adress – ej virtuell hostning av servern
  - CA root certifikat måste finnas på klienter som verifierar server cert.

SSL/TLS connection

MS technical reference: http://technet2.microsoft.com/WindowsServer/en/Library/e8f50ce4-8a4c-44ba-a6f5-ff284082a6891033.mspx?pf=true

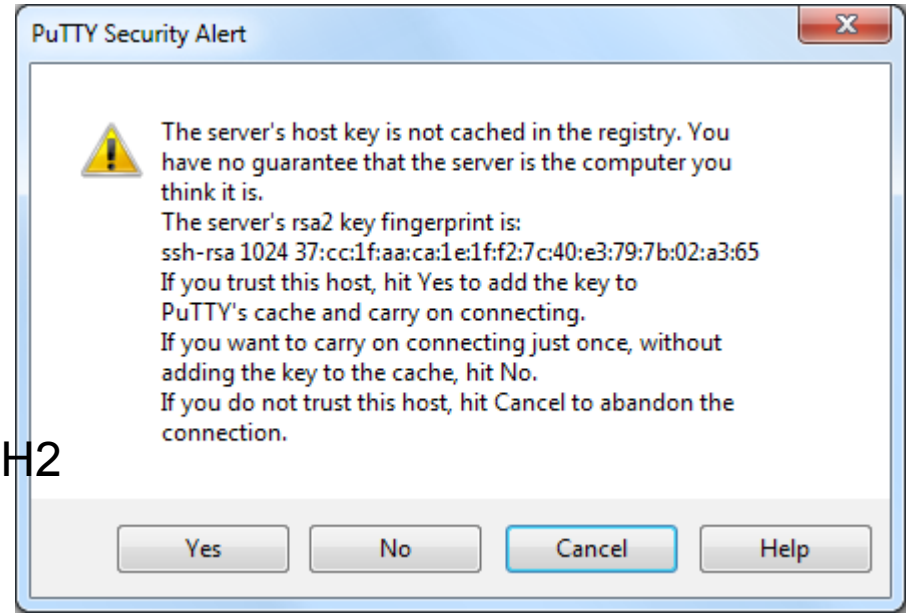
TLS handskakning



- Client Hello innehåller en lista med krypto standars som klienten stödjer
- Server Hello väljer och sänder den starkaste som båda stödjer
- Server Hello innehåller även serverns digitala certifikat
  - Autentiserar servern
  - Publicerar serverns publika nyckel
- Klienten genererar en session key som krypteras med serverns publika nyckel och sänder den till servern
- Svagheter?

Secure Shell Version 2 (SSH2)

- Exempel på ett middleware krypteringssystem
  - Finns till Windows och UNIX
    - Kommersiell: ssh.com och fria: OpenSSH och PuTTY
  - SSH erbjuder konfidentialitet, autentisering och integritetskontroll
  - Många program kan köra via en SSH2 krypterad tunnel (fattig mans VPN)
  - Primära uppgiften är dock säkert remote shell (telnet)



- Fördelen med kryptering lokalt end-to-end är att data är skyddat hela vägen
  - Nackdelen är att konfiguration krävs på varje dator och att brandväggar etc. inte kan inspektera innehållet
- Fördelen med kryptering i en gateway/extern enhet är transparens och att brandväggar kan inspektera innehåll
  - Nackdelen är att data är oskyddat en kort stund på resan

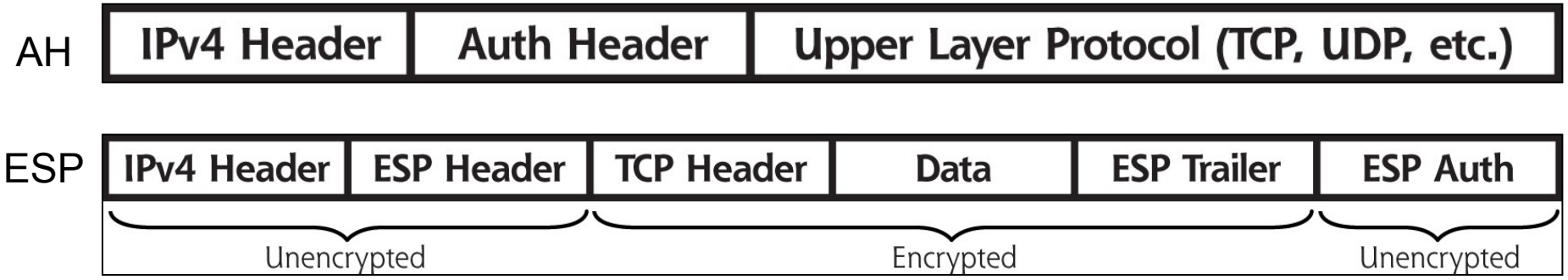
VPN Teknik

- Vanligen ligger VPN-servern bakom brandväggen, vissa portar behöver därför öppnas beroende på lösning
- Om brandväggen använder NAT kan ej L2TP, PPTP och IPsec användas utan speciellt stöd i den
- Fördelen med VPN är att stora pengar kan sparas genom att använda en vanlig Internetförbindelse jämfört med en hyrd dedikerad kommunikationslösning
- De potentiella säkerhetsproblem som finns går att komma tillrätta med genom:
  - Brandvägg
  - Säkra operativsystemet
  - Avvisa okända datorer (med paketfilter)
  - Använda PKI-kryptering/säker autentisering

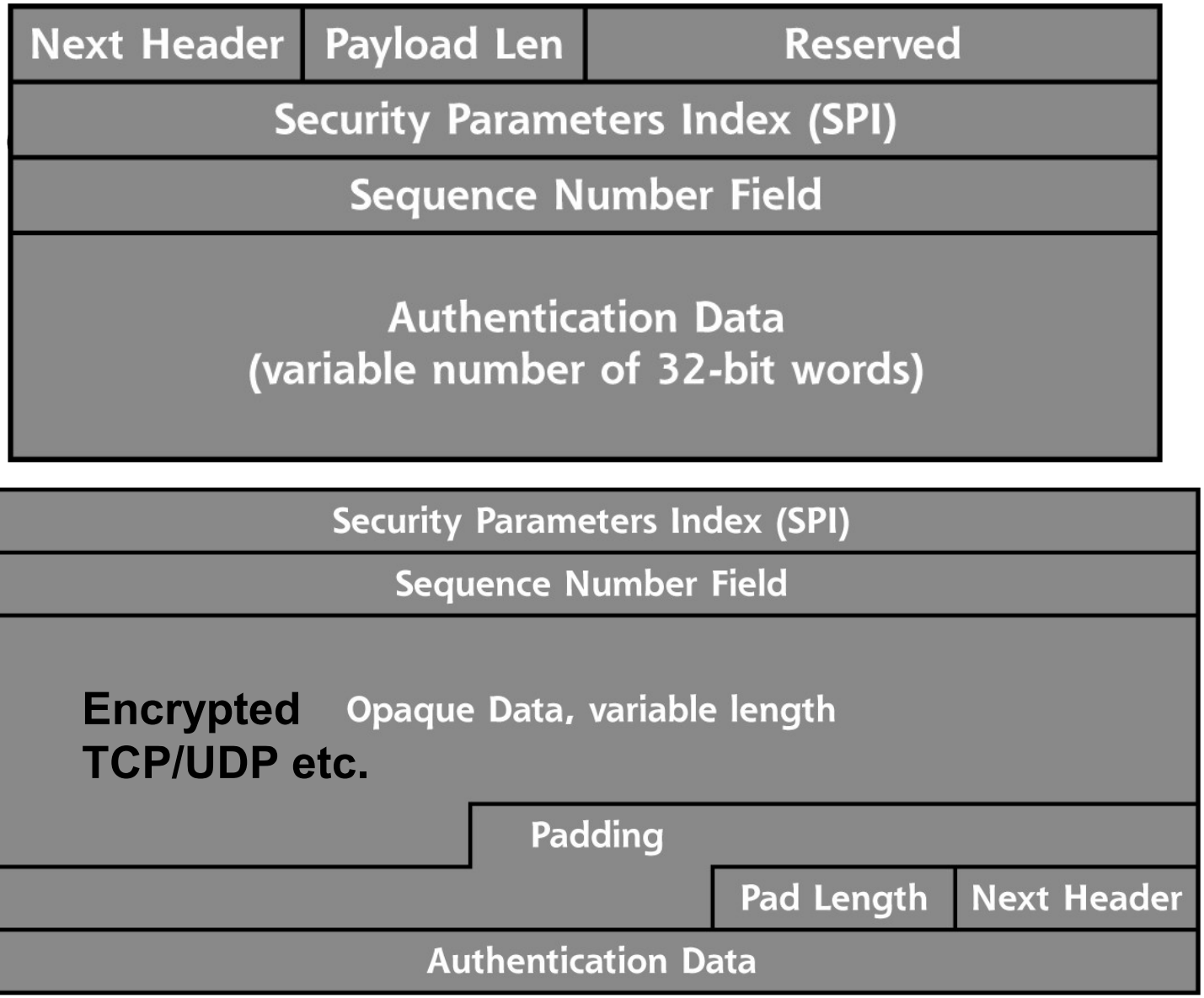
VPN Teknik
IPsec (Internet Security Protocol)

- IPsec är en öppen standard som säkrar upp nätverkstrafik genom att kryptera och/eller autentisera alla IP-paket
- Är inbyggt i IPv6 och optional i IPv4, ingår i de flesta nya OS eller kan adderas
- När IPsec aktiveras ersätter det de vanliga IP-paketen med två olika nivåer på säkerhet
  - Authentication Header (AH) – gör en **digital signering** av IP-headern - mottagande dator verifierar signaturen med en delad kryptonyckel – själva datainformationen finns i klartext
  - Encapsulating Security Protocol (ESP) – krypterar, annars samma operationer som AH

Transportläge eller tunnelläge (**hela** IP-paketet autentiseras/krypteras)



IPsec – AH vs ESP header



IPsec
Internet Key Exchange (IKE)

- Genom IKE autentiseras två enheter mot varandra, utväxlar en hemlig kryptonyckel och enas om protokoll, algoritmer m.m.
  - http://en.wikipedia.org/wiki/Internet_key_exchange
- Detta kallas Security Association (SA) och återupprepas efter givna intervall
  - Manual Keying – innebär att SA görs manuellt
- IKE protokollet har tre metoder för autentisering och nyckelutväxling
  - Pre-shared secrets – använder förkonfigurerade lösenord
  - Kerberos – IETF protokoll med servertjänst som distribuerar nycklar (Diffie-Hellman)
  - Digitala certifikat – sker i en PKI-miljö med gemensam CA-tjänst

IPsec och de två användningslägena

- Transportläge (värd till värd)
  - Ändpunktsutrustningen ansvarar för signering och kryptering
  - Används oftast av mobila användare eller trådlösa nätverk
- Tunnelläge (nätverk till nätverk)
  - Gatewayen (routern) i sändande och mottagande ände ansvarar för signering och kryptering
  - Används oftast mellan olika fjärrkontor där kravet på säkerhet inom kontoret inte är så stor