Datasäkerhet och integritet

OH-6 v1

- Brandväggar
- TCP/IP paketstruktur
- IDS & IPS
- VPN
- IPsec
- SSL/TLS & HTTPS

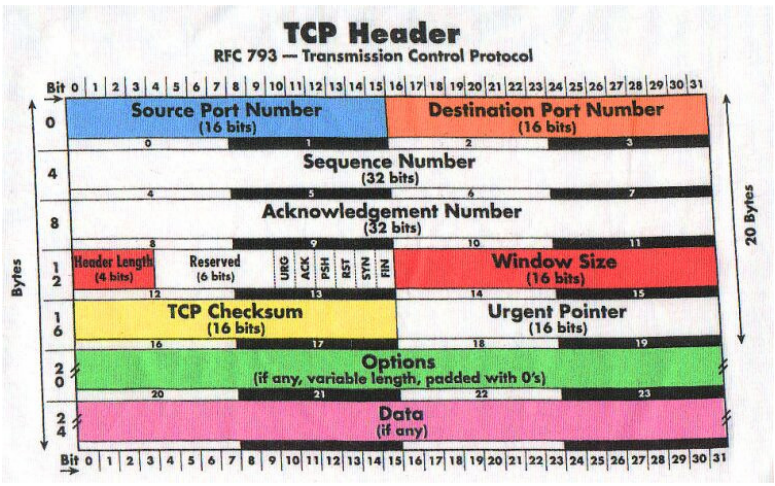
Firewalls (brandväggar)

- Kan ses som ett slags gränsvakt för datatrafiken, vilket är ett naturligt steg - jmf. lås i ytterdörren
  - Se film http://www.warriorsofthe.net
  - 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 skall exponeras?
- Grundtekniker och funktioner i brandväggen
  - Paketfiltrering (vad man oftast menar med firewall)
  - NAT (Network Adress Translation)
  - Proxyfunktion (oftast bundet till en applikation)
  - Övervakning och loggning

Firewalls (brandväggar)

- 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
  - Hindrar inte virus eller trojaner
- Två grundmallar kan sägas finnas
  - Allt som inte är tillåtet är förbjudet (bäst!)
  - Allt som inte är förbjudet är tillåtet

TCP paketstruktur
Header & data



TCP paketstruktur
Header & data

- Source port - sändningsport
- Destination port - mottagarport
- Sequence number – Om SYN flaggan är satt så är detta initiala Seq.Nr och den första databyten är Seq.Nr + 1, annars är första databyten Seq.Nr
- Acknowledgement number – Om ACK flaggan är satt är detta nästa Seq.Nr som sändaren förväntar sig att motta
- Header Length (data offset) – specificerar TCP-headerns storlek i 32-bit words, min 5 och max 20
- Reserverad – för framtida användning

TCP paketstruktur
Header & data

- Flags (kontroll bitar)
  - URG – Urgent pointer är satt
  - ACK – Ack är satt
  - PSH – push funktion
  - RST – resetta förbindelsen
  - SYN – Synkronisera sequence nummer
  - FIN – ingen mer data från sändaren
- Window size – antalet bytes sändaren av detta segmet är villig att ta emot
- Checksum – 16 bitars kontrollsumma på header & data
- Urgent pointer – om URG är satt så är detta en positiv offset till slutet för urgent data
- Options – ytterligare options
- Data – tillhör ej header, innehåller själva sändningen

Mer om TCP

- TCP över Wireless
  - Ej optimerat för denna typ av nätverk
- Debugga/analysera nätet med paketsniffer
  - Promiskuöst mode tar bort adress-filtrering
  - Tcpdump och Windump, Ethereal, AiroPeek mfl.
  - Winpcap lista: http://www.winpcap.org/misc/links.htm#tools
- Svagheter & alternativ
  - Omsändningsgaranti
    - Programvaror kan inte få tillgång till data efter ett tappat paket förrän det felaktiga paket omsänts
  - Ganska komplext
    - En hel del buggar har existerat eller existerar
  - Ej lämpligt i system med hög bandbredd
    - Där TCP är olämpligt kan UDP användas
  - SCTP (Stream Control Transmission Protocol) – kombinerar TCP och UDP med nya funtioner

Tillståndslös paketfiltrering

- Oftast i enklare FW eller i kombination med mjukvaru-router
- Paketets header inspekteras utifrån protokolltyp, IP-adress, TCP/UDP-port m.m.
  - Beslutet grundas enbart på headerinfo i aktuellt paket
  - Nyttoprogram kan blockeras om de har ogiltig header (fragmenterad pga. MTU skillnad i WAN/LAN), använder portar dynamiskt eller använder UDP (förbindelselöst!)
- Otillåtna protokoll/paket filtreras bort baserat på:
  - Källadress och port
  - Destinationsadress och port
  - Förbindelsens riktning (TCP ACK flaggan)
- Filterreglerna kallas för ACL (Access Control List)
  - ALLOW, DENY/BLOCK
- Trots nackdelar så är tillståndslös paketfiltrering ändå effektivt i att stoppa broadcast-attacker och att blockera många portar

Tillståndsstyrd paketfiltrering

- 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, exempel
  - Check Point FireWall-1, Cisco IPX

Circuit-Level Gateway (CLG)

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

NAT eller network/IP-masquerading

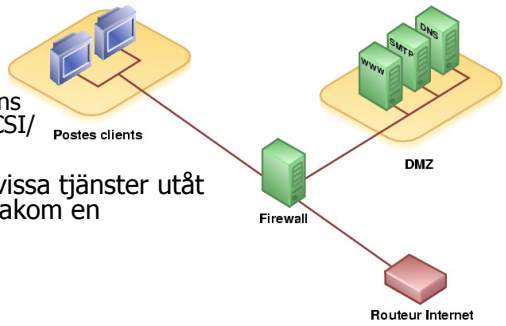
- Mycket vanligt i routrar hemma eller på små arbetsplatser, kan sägas vara en variant på tillståndslös paketfiltrering
- Tillåter ett antal privata adresser att nå Internet via en publik adress genom manipulation av TCP-headern
- Omvandlar dolda privata (interna) adresser till publika IP-adresser, privata IP-serier:
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 – 172.31.255.255
  - 192.168.0.0 – 192.168.255.255
- Nackdelen är att protokoll/applikationer som kräver öppen returkanal inte fungerar korrekt
  - Kan oftast konfigureras till att fungera
- Innebär ett visst skydd mot utomstående, men inte 100%
  - Konfigurationen…
  - En trojan inifrån kan koppla upp sig mot attackeraren

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 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

Brandväggsval?

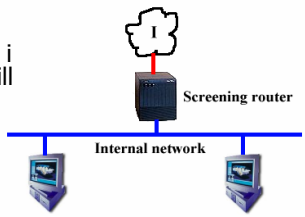
- Krav på funktioner och budget styr valet av brandvägg
  - Säkerhetskrav
  - Trafiknivå
  - Vilka tjänster
  - Lista över kommersiella finns på http://www.spirit.com/CSI/
- Ofta får man problem med vissa tjänster utåt om man lägger hela nätet bakom en brandvägg
  - Prestanda
  - Säkerhet
  - Åtkomst (inifrån <-> ut)
  - Administration

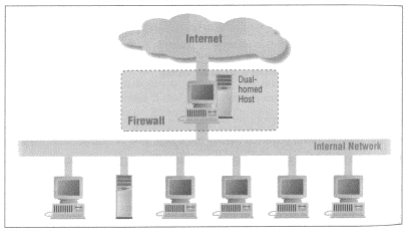


Brandväggsarkitektur

http://www2.hh.se/staff/jovall/secure/bidrag_2/wall1/firewall_1.html

- Single-box (Screened router)
  - Innebär att ett objekt (router och brandvägg i samma) agerar brandvägg, vilket gör detta till den enklaste arkitekturen av en brandvägg
- Dual-Homed Host
  - Denna dator har minst två nätverksinterface
  - System som finns utanför och innanför brandväggen kan inte kommunicera direkt med varandra utan all kommunikation måste gå via dual-homed host. IP-trafiken mellan systemen är på så sätt totalblockerade
  - Fungerar bra när trafiken är liten



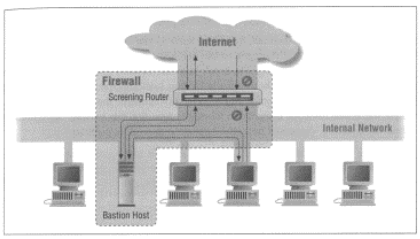


Dual-homed host architecture

Brandväggsarkitektur

http://www2.hh.se/staff/jovall/secure/bidrag_2/wall1/firewall_1.html

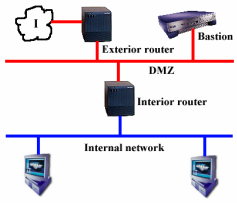
- Screened Host Arkitektur
  - Denna arkitektur genererar tjänster från en värd som är kopplad till det interna nätverket och använder sig av en separat router. Det är framför allt paketfiltringen som ger säkerheten. Paketfiltrering på screening router sätts upp så att bastion host är det enda systemet på det interna nätverket och via denna sker all koppling med Internet. Bastion host låter bara vissa kontakter med värdar från externa nätverk att göras och är vanligen ett tillståndsstyrd paketfilter eller proxy
  - I de flesta fall ger screening host arkitektur bättre säkerhet och användbarhet än vad dual-homed host arkitekturen kan. Tyvärr finns det dock inget som stoppar en hacker från att ta sig in i resten av det interna nätverket om han/hon lyckats ta sig in i bastion host.



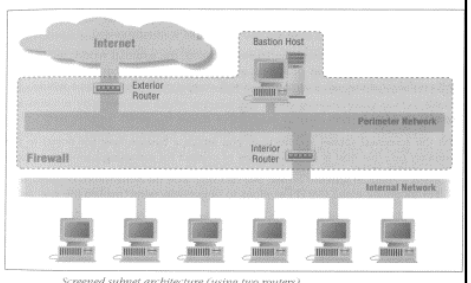
Screened host architecture

Brandväggsarkitektur

http://www2.hh.se/staff/jovall/secure/bidrag_2/wall1/firewall_1.html



- Screened Subnet Arkitektur
  - Som nyss nämndes så finns det ingen säkerhet som stoppar en hacker från att ta sig vidare i det interna nätverket när han/hon kommit in i bastion host. Bastion host är en känslig maskin vilket gör att de lätt attackeras. För att öka säkerheten kan man lägga till ett extra lager, perimeternätverk på screened host arkitekturen Dessa nätverk kalls ibland DMZ (De-Militarized Zone). Detta lager isolerar det interna nätverket från Internet. Attackerna på en bastion host minskar när det finns fler hinder som hackern måste ta sig förbi.
  - På den enklaste arkitekturen av screened subnets finns det två screeningroutrar som är kopplade till perimeternätet. En router sitter mellan perimeternätet och det interna nätverket och en router sitter mellan perimeternätet och det externa nätverket. För att hackern nu skall kunna ta sig in i det interna nätverket, måste han/hon ta sig förbi båda routrarna



Screened subnet architecture (using two routers)

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/program-id
- Mål - Enkel att ställa in och använda
- Post- & telestyrelsen har ett test och andra tips för både hemanvändare och företagare/ansvariga
  - https://www.testadatorn.se
- Loggar och varnar
  - De flesta användare brukar stänga av funktionen
- Exempel
  - MS firewall (Security Center, kom med XP sp2), BlackICE, ZoneAlarm

IDS (Intrusion Detection Systems)

- Används för att detektera att intrång har skett, försiggår eller försök gjorts
- Nätverksbaserat
  - System med programvara som ”sniffar” (fångar nätverkstrafik) av nätverket i realtid via ett promiskuöst nätverkskort
  - Analyserar typ av paket, frekvens, avvikelser, mönster m.m.
- Server/klientbaserat
  - Använder sig av intelligenta agentprogram som övervakar alla processer i realtid
  - Analyserar systemanrop, loggar, filsystem m.m.
- Eller båda teknikerna tillsammans
- Konsollen är admins gränssnitt för att kontrollera IDS
  - Policy
  - Processa alarm
  - Hämta och visa data från sensorer

IPS (Intrusion Prevention System)

- Används för att filtrera viss trafik vid en specifik händelse utifrån IDS, T.ex.
  - Blockera ett visst nätverkssegment från attacker
  - Filtrera bort en viss IP-adress
  - Meddela administratörer att något pågår t.ex. via e-post
  - Meddela ISP (Internet Service Provider)
- Implementation av IDS/IPS kräver som vanligt någon form av analys, i detta fall indelning av detekteringszoner
- Intern IPS
  - Övervakar och skyddar intern information
  - T.ex. Code Green Networks CI-1100 specialserver

Honungsfällor

- Honeypot/honeynet är simulerade eller produktionslika datorer i ett isolerat nätverk
- Används för att locka hackare att ta sig in i och därigenom begränsa skadeverkningarna
- Placeras bakom en omvänd brandvägg som sniffar av all in/utgående trafik
- Angrepp loggas i syfte att
  - Förstå hur angreppet gått till
  - För att hitta svagheter i det egna skyddet
  - Säkra spår av förövarna
- Generation I och II honeynät samt virtuella honeynät
- Insider honeypots
- www.honeynet.org (har CD med GenIII teknologi)

Nätverkskrypteringstjänster

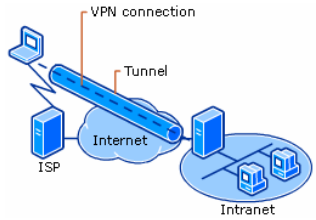
- Var skall krypteringen ske?
  - Applikationskryptering
    - T.ex. PGP
    - Kräver användarinteraktion
  - ”Middleware”-kryptering
    - T.ex SSL (Socket Secure Layer)
    - Kräver att applikationen är skriven mot krypteringstjänstens API, t.ex. HTTPS är modifierat att gå över SSL
  - Kryptering på nätverksnivå
    - T.ex IPsec
    - Kräver inget av ovanstående (nätverksnivån…)

VPN (Virtual Private Network)

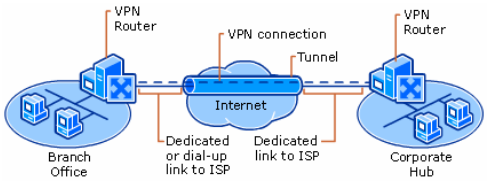
- En säker krypterad punkt till punkt förbindelse mellan två privata nät (eller datorer) på ett publikt nät som t.ex. Internet
- 3 VPN varianter finns
  - Serverbaserad - standardserver konfigureras
  - Brandväggsbaserad - samma brandvägg i ändarna eller speciell klientprogramvara
  - Routerbaserad - tilläggsfunktion i routern
- Följande parametrar krävs för ett VPN
  - Inkapsling
  - Autentisering och integritetstjänster (inte stor ide att kryptera om inte andra änden är autentiserad och datat skulle vara modiferat)
  - Datakryptering
  - Integration av interna namn och adresser

How VPN Works

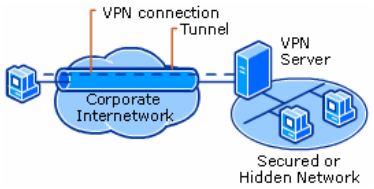
http://technet2.microsoft.com/WindowsServer/en/Library/6e2e7206-de85-45bf-89fa-634a67be37081033.mspx?pf=true



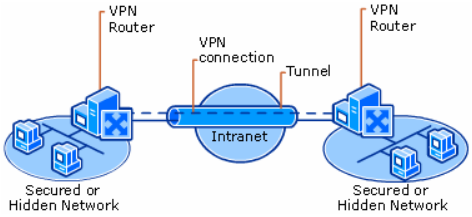
Remote Client to a Private Intranet



Two Remote Sites Across the Internet



Remote Access to a Secured Network over an Intranet



Two Networks over an Intranet

VPN Teknik 1

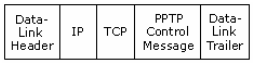
- Inkapsling
  - Med detta menas den virtuella tunnel där datatrafiken går
  - Transparent datahantering vad gäller autentisering, kryptering, data och tunnelprotokoll
- Autentiserings-metoder
  - Extensible Authentication Protocol (EAP)
  - Challenge Handshake Authentication Protocol (CHAP) och MS-CHAP som Microsofts utökning heter
  - De ovanstående är bäst eftersom de ej sänder lösenordet över förbindelsen, ett hashvärde sänds över istället (enligt tidigare exempel i kursen)
  - SPAP, PAP osv.

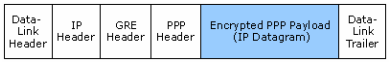
VPN Teknik 2

- Datakryptering
  - Krypterar datainnehållet eller hela paketet
  - DES, RC4, AES etc.
- Integration av interna namn och adresser
  - Klienten skall uppleva att den är direkt ansluten till andra änden
  - Åstadkoms genom att VPN-klientens logiska nätverkskort (mjukvara) får en IP-adress m.m. från andra änden

VPN Teknik - Protokoll

- Point-to-Point Tunneling Protocol (PPTP)

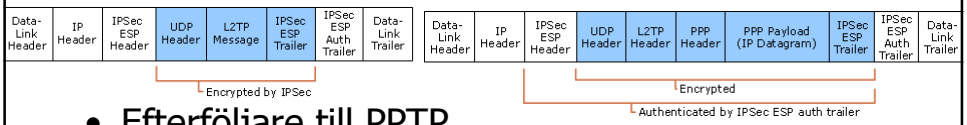




- Kontrollpaket används för att upprätthålla tunnelförbindelsen med TCP på port 1723
- Dataöverföringen kapslas in i ett IP-paket med PPP (Point-To-Point) och GRE (Generic Routing Encapsulation)-protokollet
- PPTP krypterar data endast mellan tunneländarna, ej klient <-> klient
- PPTP anses inte längre vara säkert (krypteringsalgoritmen kan knäckas för lätt)

VPN Teknik - Protokoll

- Layer 2 Tunneling Protocol (L2TP)



- Efterföljare till PPTP
- Upprätthåller tunnelförbindelsen och sänder data med UDP på port 1701
- Är mer flexibelt än PPTP (IP, ATM X.25)
- En kombination av PPTP och L2F (Layer 2 Forwarding), säkerhet via IPsec

VPN Teknik

- Vanligen ligger VPN-servern bakom brandväggen, vissa portar behöver därför öppnas beroende på lösning
- Om brandväggen använder NAT kan ej L2TP användas
- Fördelen med VPN är att stora pengar kan sparas genom att använda en vanlig Internetförbindelse jämfört med en hyrd ledning
- 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 obligatorisk 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 **hela** IP-paketet, annars samma operationer som AH

IPsec
Internet Key Exchange (IKE)

- Genom IKE autentiseras två enheter mot varandra, utväxlar en hemlig kryptonyckel och enas om protokoll, algoritmer m.m.
- 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
Internet Key Exchange (IKE)

- 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

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
- Protokollet förhindrar:
  - Avlyssning (kan tolka innehållet - eavesdropping) ”man in the middle” attacker (MITM)
  - Förändring (tamper-evident)
  - Förfalskning (message forgery)

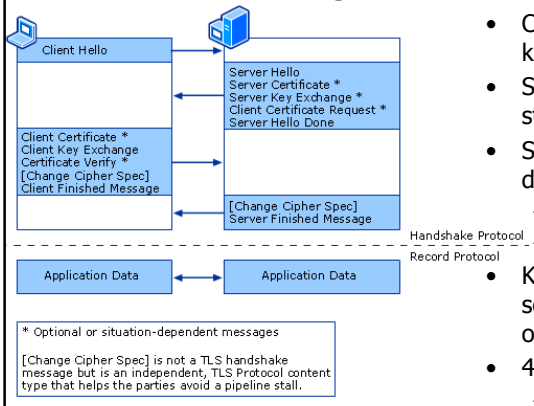
HTTPS (HTTP med SSL/TLS)

- 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) - 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

SSL/TLS (hybrid krypto?)

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 ett slumpnummer som krypteras med serverns nyckel och sänder det till servern
- 4 nycklar skapas utifrån slumpnr.
  - Krypteringsnyckel för server o client
  - Autentiseringsnyckel för server o client

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 shell (telnet)
- Fördelen med kryptering i datorer end-to-end är att
  - Datat 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 extern enhet är att det blir transparent och att brandväggar kan inspektera innehåll
  - Nackdelen är att data är oskyddat en kort stund på resan