Intranet e Internet

Internet rete intrinsecamente insicura

Collegamento di Intranet aziendali ad Internet è un problema molto sentito, soprattutto per:

- economicità (*basso costo collegamenti*)
- mercato globale (*WWW*)
- supporto mobilità utenti

Principio fondamentale

se si vuole essere sicuri, è meglio non essere connessi

Possibilità
di accedere ai servizi di rete
accesso dall'interno verso l'esterno
accesso dall'esterno verso l'interno
senza compromettere il sistema interno

Per le **organizzazioni commerciali** o **bancarie**
diventa vitale trovare soluzioni accettabili

*A parte la **disconnessione***
possibili politiche e meccanismi di **separazione**
tra gli **ambienti** eventualmente **sicuri interni (*Intranet*)** e ***Internet*** *(uso di sistemi firewall e VPN)*

Fattori di Perdita di Sicurezza

TCP/IP come sistema aperto
uso di risorse esterne per routing
vulnerabilità intrinseche dei servizi e protocolli
estrema complessità di meccanismi di controllo

Facilità di monitoraggio dell'attività di rete:
comunicazioni in chiaro

Controllo degli accessi e autenticazione utenti
basati su password (statiche e riusabili)

Connessioni di rete tramite risorse esterne
linee condivise e router di terzi

Minacce: IP spooofing, password sniffing, session hijacking, denial of service, ...

Soluzioni di Sicurezza

A quale livello conviene integrare soluzioni di sicurezza?

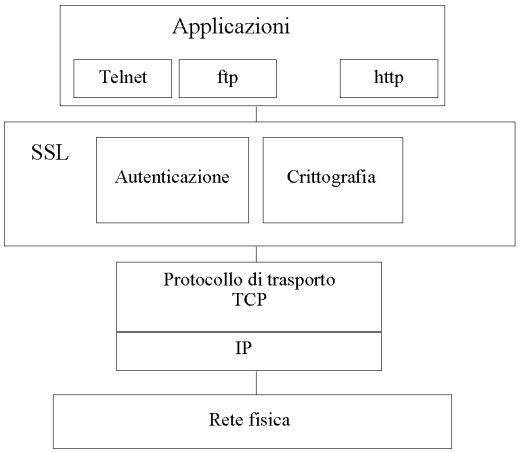
Livello applicativo o livello di rete?

Livello applicativo: SSL, TLS, SSH, ….

Livello di Rete: IPSEC

Secure Socket Layer (SSL) (1.)

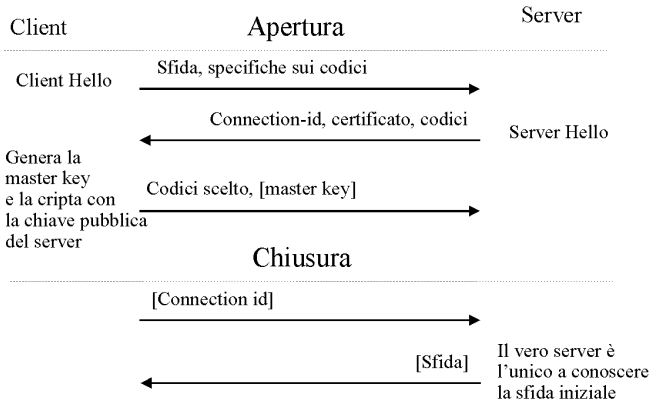
- Inizialmente proposta da Netscape, al momento in fase di standardizzazione in ambito IETF col nome di TSL
- Utilizza una combinazione di codici per la varie funzioni da svolgere
- Si colloca logicamente fra strato di trasporto e applicazioni: *non richiede una modifica delle applicazioni*



Secure Socket Layer (SSL) (2.)

E' logicamente suddiviso in due parti:

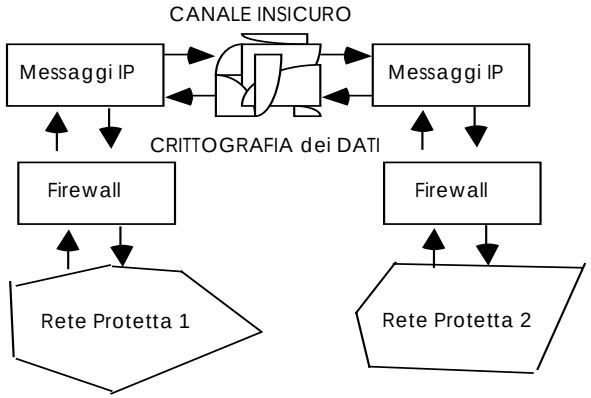
- SSL Handshake Protocol (SSLHP)
  - negozia l'algoritmo simmetrico da utilizzare
  - si occupa dell'autenticazione di client (opzionale) e server
  - invia la chiave segreta (master key) utilizzata per lo scambio dei dati
- SSL Record protocol (SSLRP)
  - impacchetta i dati da inviare in records
  - si occupa della cifratura/decifrazione dei records in modo conforme a quanto negoziato



IP Tunneling

Tecnologia con cui un pacchetto di un qualunque protocollo viene incapsulato in un datagramma IP.

Esempio: i pacchetti NetBeui incapsulati in un datagramma IP possono muoversi su Internet.



possibile applicazione della crittografia al sistema, con **chiavi note** solo all'interno dei due sistemi protetti

IPsec (secure IP)(RFC 2401)

Protocollo IP sicuro, fornisce la cifratura a livello IP, più in basso di SSL o VPN.

- Protegge da sniffing, modifica, ripetizione di messaggi
- Protegge le intestazioni e/o i dati dei pacchetti
  - **Authentication Header (AH)** : autentica l'origine dei datagrammi e protegge dalla loro replicazione (opzionale)
  - **Encapsulation Security Payload (ESP)** : garantisce la segretezza dei dati, autentica ed impedisce la replicazione
- Security Parameter Index (SPI) contenuto in ogni intestazione conforme a IPSec definisce le chiavi e gli algoritmi utilizzati

IPSec: Security Association

- La security association SA è una struttura dati che contiene le informazioni necessarie per realizzare una connessione sicura:
  - simplex (in una sola direzione)
  - utilizzando ESP o AH (non entrambe)
- E' indirizzata univocamente dalla combinazione di SPI, numero IP e protocollo di sicurezza (AH o ESP)
- Specifica:
  - algoritmi e chiavi di autenticazione e crittografia
  - il tempo di vita delle chiavi e della SA

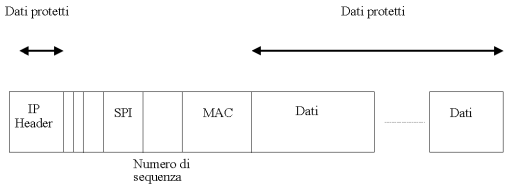
  un numero di sequenza per impedire la replicazione

IPSec: gestione delle SA

- Le SA devono essere gestibili in modo automatico
- A questo scopo esiste un protocollo ad hoc per la:
  - creazione
  - negoziazione
  - modifica
  - cancellazione di SA
- Questo protocollo si chiama Internet Key Exchange (IKE) e opera in due fasi:
  - durante la prima fase crea un canale sicuro fra due host e definisce le SA da utilizzare per la negoziazione
  - negozia le SA per le varie sessioni di comunicazione

IPSec: AH (RFC 2402)

- Autentica ma lascia in chiaro i datagrammi,
  - non impone funzioni di cifratura/decifrazione per ogni intestazione in ogni router
- SPI dice all'host ricevente:
  - quale hash utilizzare
  - quale chiave utilizzare unitamente all'hash

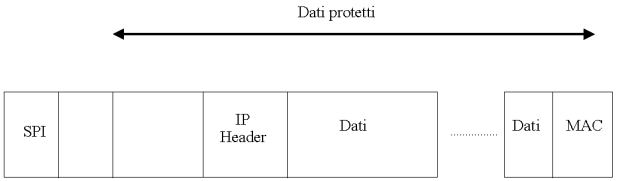


IPSec: AH

- Operazioni di default:
  - hash con MD5, uso di un HMAC
  - abilitazione di anti-reply
- Operazioni opzionali
  - SHA-1 al posto di MD5
  - HMAC può essere disabilitato
  - anti-reply può essere disabilitato

IPSec: ESP (RFC 2406)

- Dati e intestazione sono criptati ed autenticati
- SPI specifica
  - quale algoritmo utilizzare
  - se è stata utilizzata AH oltre ad ESP
  - quale chiave utilizzare



IPSec: ESP

- Default:
  - DES per la crittografia
  - uso di AH
- Operazioni opzionali

altri algoritmi (IDEA, CAST,

Firewall

Un **firewall** garantisce la sicurezza del collegamento di una Intranet verso Internet.

Un firewall è un sistema costituito di molti componenti che:

- costituisce **l'unico punto di contatto** della rete **interna** con l'**esterna**
- filtra e **controlla** tutto il traffico tra le due reti.
- concentra i **meccanismi di sicurezza**
- impone la **politica di sicurezza** della organizzazione
- nasconde informazioni della rete interna
- registra eventi (**logging)** ed elabora statistiche sul traffico di rete (**auditing**)

Separazione politiche-meccanismi

Attenzione alla scelta dei servizi che devono transitare attraverso il firewall.

POLITICHE DI UN FIREWALL

il **firewall** deve implementare una **politica di accesso** in modo **separato** e **concentrato**

===>

☹ senza firewall le stesse funzioni vengono ottenute attraverso la cooperazione di tutti gli host

Problemi

un firewall non risolve tutti i problemi

☹ un **firewall** restringe la possibilità di accesso a servizi
☹ la topologia di rete può essere inadeguata a un firewall
☹ non protegge contro i ***virus***
☹ problemi di ***attacchi interni***
==> *giusto compromesso tra sicurezza e funzionalità*

😐 attenzione alle vie di accesso secondarie (**backdoor**)
==> *accesso tramite modem*

☹ come punto **concentrato** di affidabilità
ma può diventare un **collo di bottiglia** (bottleneck)

Aspetti progettuali da considerare in un firewall

- esigenze da soddisfare (quali servizi)
- architettura
- autenticazione
- politica di autorizzazione di rete

Metodologie di autenticazione

tecniche di autenticazioni robuste
anche basate su meccanismi differenziati

*password usa e getta (***one-time password***)*
carta magnetica
impronta digitale

==> caratteristica comune
utilizzo di password non riusabili

Politiche di autorizzazione opposte

tutto ciò che non è espressamente permesso è vietato

- maggiore sicurezza
- più difficile da gestire

tutto ciò che non è espressamente vietato è permesso

- minor sicurezza
- più facile da gestire

Problemi di efficienza

Il firewall comporta una inefficienza nei servizi che sono disponibili e un ritardo nei tempi di risposta

il firewall *potrebbe anche diventare il collo di bottiglia dell'intero sistema*

Considerazioni generali

- grossi oggetti sono difficili da verificare
  ('grande non è bello')
- se una risorsa dinamica non è attiva non preoccupa
- definire assunzioni di default => tutti sono sospettati
- usare risorse dedicate solo ai meccanismi di sicurezza

Esempi di configurazioni di sistemi firewall

- grado di controllo sugli errori e buchi di sicurezza
- zona di rischio (# di host esposti a possibili attacchi)
- politica di autorizzazione adottata

Router *un gateway che separa la rete interna dalla esterna*

Dual-Home gateway *macchina sicura con due accessi separati alla rete*

Bastion host *macchina sicura dedicata al controllo del sistema per la sicurezza* ==> ***auditing*** ossia verifica e traccia degli eventi nel sistema

Packet filtering (filtraggio livello rete)

Traffico filtrato sulla base dei campi contenuti nel datagramma IP

sourceIP *sourcePORT*
destinationIP *destinationPORT*

Si possono così *escludere alcuni host come mittenti o come destinatari, escludere alcuni servizi*

azioni specificate a mano

tipo	Indirizzo destination	Indirizzo source	Porta destin.	Porta source	Azione
TCP	137.204.57.33	*	23	>1023	permit
TCP	137.204.57.32	*	25	>1023	permit
TCP	137.204.57.34	*	25	>1023	permit
TCP	137.204.57.31	137.2.5.30	119	>1023	permit
TCP	*	*	*	*	deny

Problemi

difficoltà in caso di

☹ servizi RPC

più interfacce

- difficoltà di specificare in modo compatto regole
- mancanza di logging

Application gateway

i problemi del **packet filtering** si possono superare con proxy

cioé gestori ad-hoc per consentire il trattamento solo di uno specifico servizio

proxy server

applicazione software col compito di mediare il traffico tra rete esterna ed interna e consentire accesso a un servizio specifico

vantaggi

ϑ filtra *servizi* e *protocolli*
supporta *autenticazione* robusta e *logging*
semplifica le regole del *filtering*
garantisce riservatezza alla rete interna
ϑ incide positivamente sul costo

i proxy devono essere concentrati sul solo firewall e non distribuiti su tutti gli host della rete

svantaggi

☹ connessioni con host interno a due passi

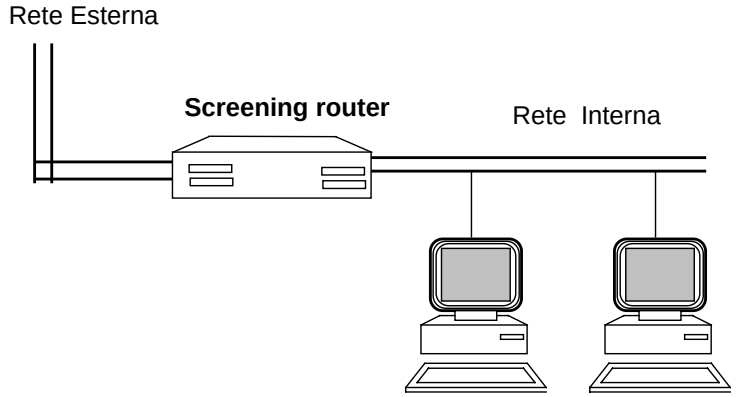
perdita di trasparenza del firewall

a meno di modificare i clienti per i servizi di rete più comuni

Screening router

*un **router** fa da filtro tra le **due reti** (interna ed esterna)*

- questo firewall usa il router per filtrare il traffico
- non necessita di proxy
- implementare la politica
  tutto ciò che non è espressamente permesso è proibito



problemi

☹ basso livello di sicurezza introdotto
ogni host necessita
di robuste misure di autenticazione==>
la zona di rischio è pari al numero di host della rete

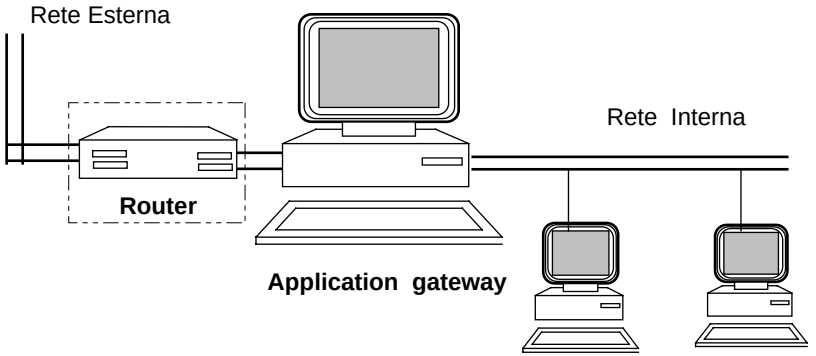
☹ regole di packet-filtering difficili da specificare sul router

☹ mancanza di logging

Dual homed gateway

***stazione** dotata di due **interfacce** di rete con effettiva separazione fisica tra rete interna ed esterna*

a volte si aggiunge anche un ***router*** sulla connessione esterna per packet-filtering



ϑ alto livello di privacy
misure robuste di autenticazione
logging facile

implementa politica di accesso più rigida
proxy per servizi standard: **telnet, ftp, e-mail**

mancanza di flessibilità in caso di modifiche di servizi e sovraccarico di lavoro concentrato sul gateway

gateway stesso come *zona di rischio* e come *collo di bottiglia*

Screened host firewall

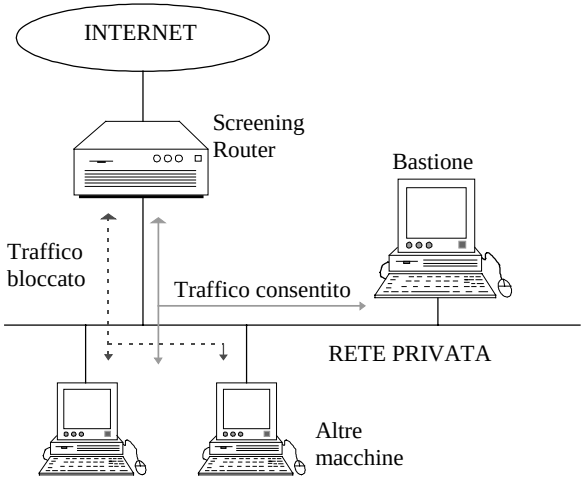
*costituito da un **bastion host** e da **una rete interna***

application-gateway sul bastione

==> si affaccia direttamente sulla rete interna e passa le informazioni all'interno

router

==> blocca i pacchetti dall'esterno/interno tranne quelli in arrivo/invio da application gateway



- flessibilità maggiore rispetto al dual-homed
- allenta il controllo su certi servizi/host
  implementa entrambe le politiche di autorizzazione

problemi

costo della soluzione

la rete interna non presenta ulteriori barriere di protezione a parte il gateway,

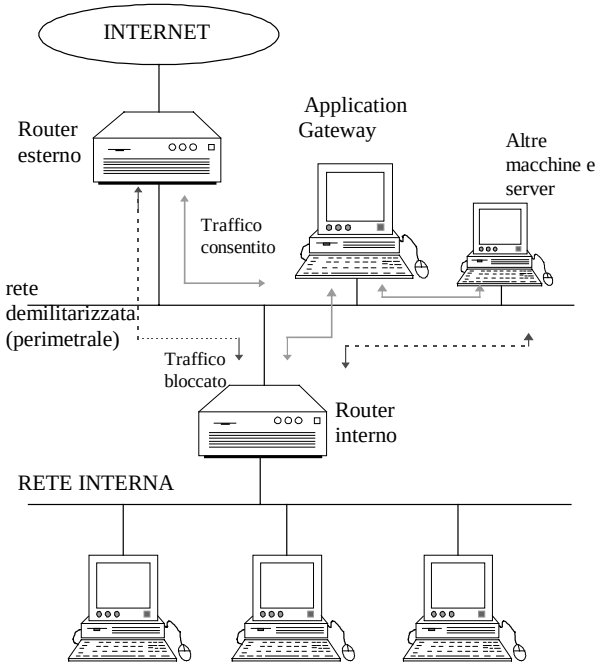
Screened Subnet Firewall

router per esterno

- inoltra traffico dall'esterno agli **application gateway**
  server e-mail e information server (amche host diversi)
- inoltra traffico dagli application gateway all'esterno
- *altro traffico rifiutato*

router per interno

- inoltra traffico dagli application gateway all'interno
- inoltra traffico ftp, gopher dal'interno agli information server della rete demilitarizzata
- *altro traffico rifiutato*



vantaggi:

non c'è alcun accesso al **sistema interno**

si garantisce elevato throughput considerando due router con intrinseca **ridondanza**

☺ anche **autenticazione avanzata** sugli application gateway

gestione più complessa delle risorse

VPN (Virtual Private Network)

Una VPN realizza una Intranet privata virtuale al di sopra di una rete pubblica (Internet).

Macchine di sottoreti diverse all'interno di una stessa organizzazione possono cooperare direttamente.

Integrazione di diversi Firewall e di macchine mobili.

Vantaggi VPN:

- Trasparenza per utenti
- Supporto alla mobilità utenti
- Economicità del collegamento

Tecnologie:

PPTP (Point to Point Tunneling Protocol) tipicamente collegato al RAS (Remote Access Services) di Win NT (che esegue autenticazione e cifratura).

Altavista tunnel della Digital.

Cisco PIX Firewall, soluzione HW, veloce ed efficiente ma scarso supporto utenti mobili.

Riferimenti su Internet Security

(da http://www-lia.deis.unibo.it/Staff/CesareStefanelli/Security.htm)

Libri

Applied Cryptography - Protocols, Algorithms and Aource code in C, Bruce Schneier, John Wiley & Sons, 1995
(schneier@counterpane.com www.counterpane.com)
Network Security, Kaufman, Perlman, Speciner, Prentice Hall, 1995.
Security in Computing, C. Pfleeger, Prentice Hall
Practical Unix Security, Garfinkel, Spafford, O'Reilly
Java Security, S. Oaks, O'Reilly, 1998.
Virtual Private Network, C. Scott, P. Wolfe, M. Erwin, O'Reilly, 1998.
"Computer Communications Security: Principles, standards, protocols and techniques" di Warwick Ford, Prentice Hall
"Handbook of applied cryptography" di A.J.Menezes, P.C.van Oorschot, S.A.Vanstone, CRC Press
Firewalls and Internet Security, Cheswick, Bellovin, Addison Wesley
Building Internet Firewalls, Chapman, Zwicky, O'Reilly
"Protecting your Web Site with Firewalls" di Marcus Goncalves, Prentice Hall
Trusted Computer System Evaluation Criteria. DOD 5200.28-STD, National Computer Security Center, December 1985. (Orange Book)
Trusted Database Management System Interpretation. NCSC-TG 021, April 1991. (Lavender Book)
Trusted Network Interpretation. NCSC-TG 005, National Computer Security Center, August 1990. (Red Book)
Information Technology Security Evaluation Criteria (ITSEC). Department of Trade and Industry, London, June 1991. Harmonized Criteria of France, Germany, the Netherlands, and the United Kingdom.

Site

www.cert.org : CERT (computer emergency response team) charter is to work with the Internet community to facilitate its response to computer security events involving Internet hosts
www.crypto.com cifrare o non cifrare?
http://www.zurich.ibm.com/Technology/Security/ IBM
http://www.zurich.ibm.com/Technology/Security/extern/internet/white-paper.html
http://www.nist.gov/ NIST (National Institute of Standards and Technology)
http://www.itl.nist.gov/div893/ NIST, Computer Security Division
www.swcp.com/~iacr/proceedings/alldata_byname.html (IACR conference proceedings, by author name);
www.swcp.com/~iacr/jofc/jofc.html (Journal of cryptology bibliography and table of contents, from IACR)
http://web.mit.edu/security/www/iso1.html
news: alt.security
news: sci.crypt

University sites:

thery.lcs.mit.edu/~rivest/crypto.bib (Ron Rivest's Crypto and Security bibliography)
Cambridge www.cl.cam.ac.uk/Research/Security
Purdue COAST project www.cs.purdue.edu/coast/coast.html
Carnegie Mellon www.ini.cmu.edu/netbill
Ross Anderson www.cl.cam.uk/users/rja14
Carl Ellison (www.clark.net/pub/cme/home.html)

Algoritmi crittografici

www.rsa.com RSA Data Security, Inc.
www.cs.berkeley.edu/~daw/ David Wagner, collabora con Schneier, ha messo su web molti lavori.
Su Quantum cryptography si veda http://www-dse.doc.ic.ac.uk/~nd/surprise_97/index.html e i lavori di Gilles Brassard
http: //www.cs.hut.fi/ssh/crypto
http: //www.ifi.uio.no/pgp

Protocolli crittografici

www.rsa.com per le PKCS (Public-Key Cryptography Standards)
Certification Authorities, PKI (Pubblic Key Infrastructure), etc.
www.entrust.com/library.htm (contiene white paper sia sul prodotto specifico sia di carattere generale sulla gestione
della fiducia in Internet; contiene anche tutti gli IETF draft relativi alle PKI)
www.public-key.com
http://www.valicert.com/
www.xcert.com Esempio di CA
www.steinroe.com Esempio di CA

Sistemi Firewall
www.tis.com (Trusted Information System)
www.data.com (sito con rsultati di test di performance sui firewall commerciali)
www.clark.net/pub/mjr (pagina web di Ranum con tutti i suoi articoli)
Fred Avolio’s entire set of slides for his talk on "Securing the Perimeter"
http://www.tis.com/docs/products/gauntlet/fwovervw/index.htm

Internet Mail
www.imc.org Internet Mail Consortium, Informazioni su RFC e Internet Draft relativi alla posta elettronica.

Commercio Elettronico
http: //www.digicash.com/
www.forrester.com Informazioni e stime relative al commercio elettronico
Gail Grant, "Understanding Digital signatures: Establishing Trst over the Internet and other networks"
http://www.betabooks.mcgraw-hill.com/grant/