Il Firewall 1

Università degli studi di Salerno

Corso di laurea in Informatica

Sistemi di elaborazione dell'informazione: Sicurezza su reti

A.A. 2000/2001

Prof A. De Santis

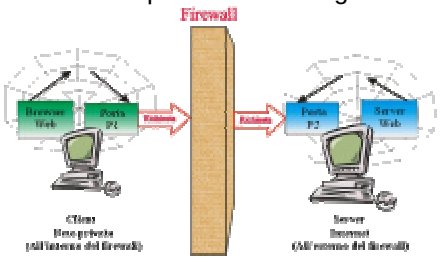
Dore Salvatore	matricola:56/000954
Jaquinta Ilaria	matricola:56/100372
Tedeschi Antonio	matricola:56/000874

Introduzione

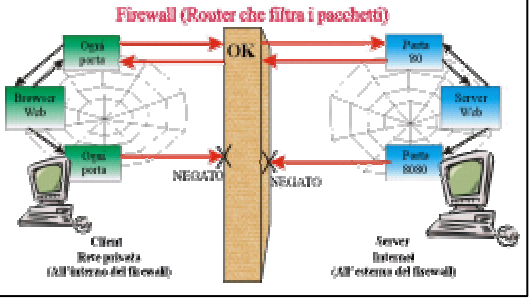
Con il termine *FIREWALL* si tende ad identificare in modo generico tutta una serie di funzioni e di apparecchiature che servono a proteggere un determinato dominio o rete privata

Introduzione

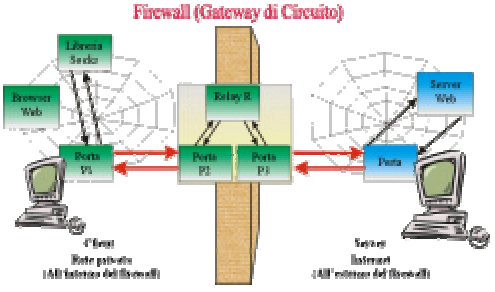
Vediamo un po' uno schema generico...



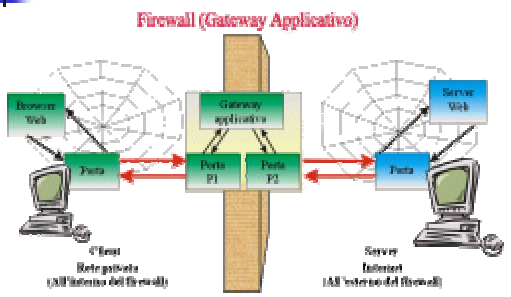
Tipologie di firewall più conosciute



Tipologie di firewall più conosciute



Tipologie di firewall più conosciute



Requisiti di un Firewall

Le decisioni di controllo richiedono che un firewall sia capace di accedere, analizzare e utilizzare i seguenti punti:

- Informazione delle comunicazioni
- Stato communication-derived
- Stato application-derived
- Manipolazione dell'informazione

Il Firewall 1

Il Firewall 1

Il ***VPN 1/Firewall 1*** è un firewall commercializzato dalla *CheckPoint®* sviluppato per la definizione e il mantenimento di politiche di sicurezza nell'ambito di reti complesse

L'attuale versione in commercio è la 4.1 rilasciata nel secondo semestre 2000

Il Firewall 1

VPN-1/ Firewall-1 é composto principalmente da due moduli:

Il ***FireWall Module*** che comprende:

- L'inspection Module

Il ***Management Module*** diviso in***:***

- Management server
- Gui client

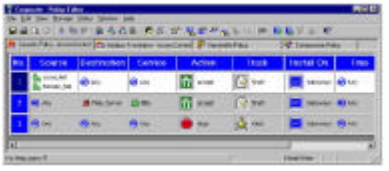
Ma vediamoli più in dettaglio...

Management Server

Con il ***Management Server*** vengono memorizzate le regole di sicurezza definite tramite GUI Client e mantenuti i databases di VPN-1/Firewall-1

GUI Client

Il ***GUI Client*** permette di definire e amministrare la propria politica di sicurezza (con un'interfaccia grafica)



FireWall Module

Il ***FireWall Module*** é situato sui gateway e su tutti gli altri punti di accesso alla rete e costituisce il modulo principale del FireWall 1

L'***Inspection Module*** esamina tutte le comunicazioni in accordo con la *Security Policy*

Piattaforme Supportate

Piattaforme supportate per l'installazione:

Modulo	Sistema Operativo
Gui Client	Windows 9x-ME, Windows NT 4.0 con Service Pack 4-6a, Windows 2000 su processori Intel o compatibili X Motif (Solaris, HP-UX 10.20, IBM AIX)
Management Module **VPN/FireWall Module**	Windows NT 4.0 con Service Pack 4-6a, Windows 2000 su processori Intel o compatibili Solaris 2.6, Solaris Operating Environment 7 (conosciuto come Solaris 2.7) SPARC and x86 HP-UX 10.20, 11.0 IBM AIX 4.2.1, 4.3.2, 4.3.3 Red Hat Linux 6.1 (Versione del kernel 2.2.x)

Stateful Inspection Technology

Caratteristica del *Firewall 1* è la Stateful Inspection Technology che permette la definizione e la gestione dei requisiti di sicurezza definiti in precedenza

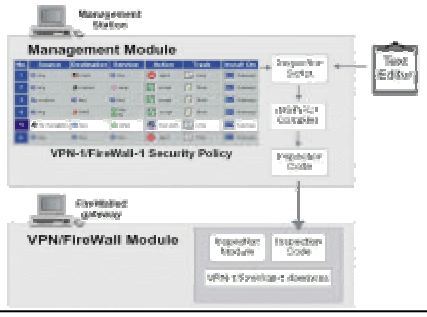
Capacità di un Firewall	Packet Filters	Application-Layers Gateway	Stateful Inspection
Informazione delle comunicazioni	Parziale	Parziale	*Si*
Stato Communication Derived	No	Parziale	*Si*
Stato application-Derived	No	Si	*Si*
Manipolazione dell'informazione	Parziale	Si	*Si*

Stateful Inspection Technology

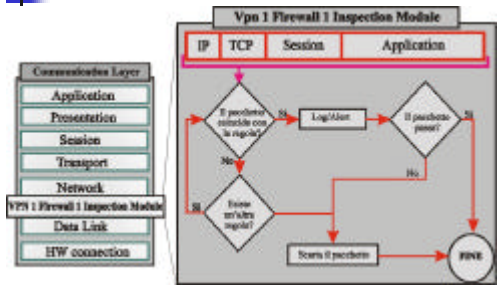
Il motore **Inspect :**

- osserva tutti i livelli di comunicazione ed estrae solo i dati rilevanti che vengono utilizzati per la protezione della rete
- programmabile usando il **linguaggio Inspect**

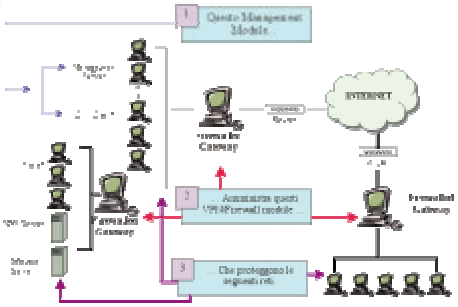
Schema Stateful Inspection Technology



VPN 1/Firewall 1 Inspection Module



Architettura Firewall 1

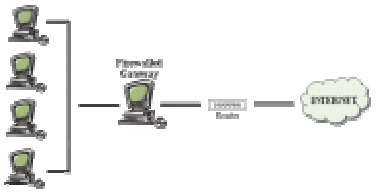


Installazione

Tramite il wizard d'installazione la procedura permette di scegliere dove e quali moduli installare in base alla topologia della rete

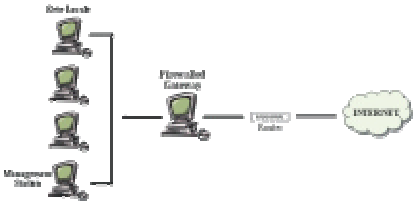
Esempi di Configurazione

Unico firewalled Gateway



- Tutti i moduli sono installati sulla stessa macchina
- Tutte le operazioni della politica di sicurezza sono gestite da un unico host
- Configurazione è adatta per la protezione di una singola rete locale, composta al più da *n* host

Un singolo Firewalled gateway e una separata Management Station



i differenti moduli devono essere installati su ognuna delle due macchine

Modello Client Server VPN 1/Firewall 1

- I due componenti del *Management Module* possono essere installati sulla stessa macchina o su due macchine differenti.
- Il Management Server gestisce gli amministratori e definire quali sono i client autorizzati a collegarsi con il Server.
- L'user, che lavora su Big Ben, ha la gestione della politica di sicurezza e del database che risiede su Tower.
- Il VPN / Firewall Module è istallato su London, Il Firewalled Gateway, che rafforza la politica di sicurezza e protegge la rete.

Interazione Client-Server

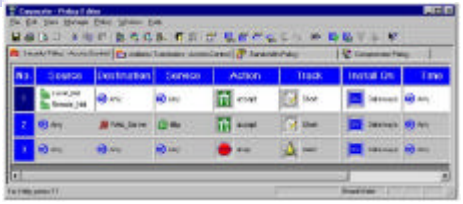
- La macchina su cui il GUI Client sta girando deve essere definita come un client autorizzato e quindi deve essere definito nel Management Server, al momento dell'installazione
- Si può aggiungere o eliminare un Client utilizzando l'apposita utility di configurazione (CPCONFIG)

Grafical User Interface

Per gestire il firewall ci sono due metodi:

- Tramite linee di comando (Inspect)
- Check point policy editor

Policy Editor



La finestra di policy editor è composta da:

- Security Policy che ci permette di stabilire la politica di sicurezza
- Address Tanslation che serve per il reindirizzamento degli indirizzi IP
- Compression Policy che riguarda le politiche per la compressione dei dati

Specifiche creazione delle regole

Source	Specifica la *sorgente* del pacchetto che può essere un qualsiasi element in contatto della rete (Es. reti, gateway, router)
Destination	Specifica la *destinazione* del pacchetto che può essere un qualsiasi elemento in contatto della rete
Services	Protocolli: TCP, HTTP, HTTPS, SMTP, UDP, RPC e ICMP
Action Time	Indica *l'intervallo di tempo* di validità della regola
Install On	Specifica su quale oggetto della rete bisogna installare la politica di accesso
Track	Indica se e in quale modo notificare all'amministratore il passaggio di un pacchetto soggetto ad una determinata regola di accesso

Network Objects Manager

In questa "categoria" sono inclusi : *workstations, gateways, routers, networks, switches, gateway clusters, and domains.*

E' possibile organizzare questi oggetti in gruppi, ai quali, applicare delle regole e definire delle proprietà.