

**Sistemi di elaborazione dell'informazione
(Sicurezza su Reti)**

Firewall Builder
Inbound
Protection
Outbound

a cura di: Flauti Nunzia, Colosimo Massimo, Sguelgia Paola

Anno Acc. 2003-2004 Prof. Alfredo De Santis

Introduzione

Guida all'installazione e configurazione del Software **Firewall Builder ver 2.0.2** (detto anche FWBuilder) distribuito dalla NetCitadel LLC sul sito www.fwbuilder.org.

- Questa release, rilasciata a cavallo tra il mese di agosto e settembre 2004, è stata sviluppata per vari sistemi operativi:
 - Linux (tutte le distribuzioni)
 - Windows
 - Mac Os
- Le **licenze d'uso** del pacchetto software sono due:
 - la GNU Public License (permette l'uso gratuito del software solo per sistemi operativi linux
 - Una prettamente "commerciale". (è possibile utilizzare il software per un periodo limitato di 30 giorni)

Ci occuperemo di:

⇒ **Il firewall in generale:** cos'è un firewall, a cosa serve e quali sono le sue caratteristiche principali

- **Descrizione di FWBuilder:** caratteristiche principali del software
- **Installazione di Firewall Builder:** procedura da seguire per installare correttamente il software
- **GUI e Configurazione di Firewall Builder:**
 - Analisi dell'interfaccia (GUI) che caratterizza Firewall Builder
 - Procedura per la configurazione del software
- **Esempio di utilizzo di FWBuilder:** descrive il comune funzionamento di FWBuilder installato su di un host

Che cos'è un Firewall?

Un **firewall** non è altro che un'applicazione il cui scopo è:

- **protezione** di un singolo sistema posto in rete, di un'intera rete o più reti interconnesse
- **consentire** il passaggio del solo traffico legittimo e bloccare quello illegittimo

Non bisogna però vederlo come una soluzione a tutti i possibili problemi !!

Perché usarlo?

Il firewall tiene traccia dei dati che passano attraverso la rete e ne controlla il flusso, decidendo che cosa accettare, rifiutare o ignorare

Esistono tre validi motivi per cui dovremmo filtrare i pacchetti che transitano attraverso la nostra rete:

- **Controllo:** permette di far transitare solo un certo tipo di traffico e vieta completamente l'entrata ad un altro tipo
- **Sicurezza:** Il sistema potrebbe diventare senza saperlo un server a disposizione di qualcun altro
- **Vigilanza:** si riferisce in particolar modo a problemi inerenti ad un'errata configurazione della nostra macchina che potrebbe inviare pacchetti sulla rete esterna senza farcene accorgere

Tipi di Firewall

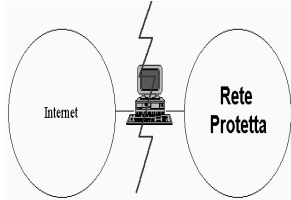
Application Proxy Firewall (o "Application Gateway")

- Implementano il concetto di firewalling a livello applicazione
- Il **proxy firewall** garantisce oppure blocca gli accessi tenendo conto di regole predefinite. Tali regole possono essere basate su indirizzi IP, protocolli o porte

Tipi di Firewall

Dual Homed Host

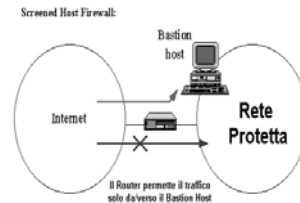
- Configurazione in cui l'Host che prevede la funzione di instradamento dei pacchetti (**routing function**), ha due distinte schede di rete
- Questa routing function può essere:
 - **attivata:** i pacchetti transitano regolarmente
 - **disattivata:** il dual-homed host effettua un vero e proprio isolamento tra i due segmenti di rete



Tipi di Firewall

Screened Host

- L'elemento principale è uno **screening router**:
 - permette il traffico da/verso il Bastion host che fornisce i servizi alla rete
- Il **bastion host**:
 - svolge funzioni di application gateway
 - ha una sola interfaccia di rete e tramite il router, filtra i pacchetti in maniera tale che solo lui possa aprire connessioni con la rete esterna e viceversa

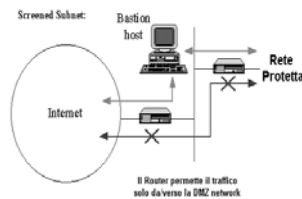


Tipi di Firewall

Screened Subnet

Viene creata una vera e propria rete isolata tra quella esterna e quella interna

- Non è ammesso alcun flusso diretto di dati tra la rete interna e quella esterna
- La rete isolata prende nome di **Screened Subnet** e spesso contiene al suo interno almeno due application-level gateway che svolgono la funzione di bastion host



Ci occuperemo di:



- Il **firewall in generale:** cos'è un firewall, a cosa serve e quali sono le sue caratteristiche principali
- ⇒ **Descrizione di FWBuilder:** caratteristiche principali del software
- **Installazione di Firewall Builder:** illustra la procedura da seguire per installare correttamente il software
- **GUI e Configurazione di Firewall Builder:**
 - Analisi dell'interfaccia (GUI) che caratterizza Firewall Builder
 - Procedura per la configurazione del software
- **Esempio di utilizzo di FWBuilder:** descrive il comune funzionamento di FWBuilder installato su di un host

Descrizione di Firewall Builder

Il punto di forza di Firewall Builder risiede nella sua progettazione

- **Object Oriented:** l'interfaccia permette una più semplice definizione delle politiche di sicurezza (*Policies*)
- **GUI intuitiva:** grazie a potenti Wizard è possibile configurare e amministrare host, reti e NAT in modo semplice e veloce
- Permette di mantenere un database di oggetti e l'editing preciso delle Policies mediante semplici operazioni drag-and-drop
- La **GUI** permette di definire e amministrare la propria politica di sicurezza con un'interfaccia grafica molto semplice

Descrizione di Firewall Builder

Firewall Builder: funzionalità

- **Accounting:** regole usate per tener traccia di tutti i pacchetti IP che vengono trasmessi o ricevuti tramite una delle interfacce di rete locali
- **Lista di ingresso (input):** regole che gestiscono l'accettazione di pacchetti entranti
- **Lista di uscita (output):** regole che definiscono i permessi per la trasmissione di pacchetti IP uscenti
- **Lista di inoltra (forward):** regole che definiscono i permessi per la ritrasmissione di pacchetti IP

Descrizione di Firewall Builder

Il "motore" di FWBuilder

- **"Packet Filtering"**: parte di software che, analizzando le intestazioni (header) dei pacchetti, ne decide la destinazione
 - scartare (**deny**) il pacchetto
 - accettarlo (**accept**)
 - scartarlo dando una notifica al mittente (**reject**)
- **Stateful Inspection**: tecnologia che permette di ottenere informazioni derivanti da tutti i livelli di comunicazione del protocollo TCP. Questa tecnologia permette al nostro software di soddisfare i seguenti requisiti di sicurezza:
 - **Informazione sullo stato della connessione**
 - **Stato derivato dalla comunicazione**
 - **Stato derivato dall'applicazione**

Ci occuperemo di:



- **Il firewall in generale**: cos'è un firewall, a cosa serve e quali sono le sue caratteristiche principali
- **Descrizione di FWBuilder**: caratteristiche principali del software
- **Installazione di Firewall Builder**: illustra la procedura da seguire per installare correttamente il software
- **GUI e Configurazione di Firewall Builder**:
 - Analisi dell'interfaccia (GUI) che caratterizza Firewall Builder
 - Procedura per la configurazione del software
- **Esempio di utilizzo di FWBuilder**: descrive il comune funzionamento di FWBuilder installato su di un host

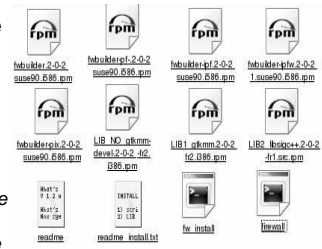
Requisiti minimi per l'installazione

Sistema Operativo	Distribuzione Linux con kernel 2.4 in poi
Processore	Intel /Amd
Spazio su disco	20 MBytes
Memoria	64 MBytes
Interfacce di rete	Tutte le interfacce supportate dal sistema operativo

Il sistema da noi scelto per l'installazione di Firewall Builder è basato sulla distribuzione **Linux Suse 9.0** con **kernel 2.4.21** ed interfaccia grafica KDE 3.1

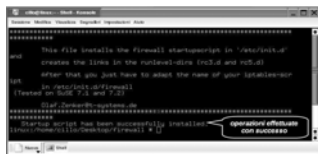
Il pacchetto software

- **File di installazione**
- **Librerie necessarie al corretto funzionamento del software stesso**
- **Due file di script che creano in automatico le directory di installazione**



Preparazione del sistema

- Prima di tutto, **creiamo la directory "firewall"** (sul desktop per esempio) che contiene tutti i sorgenti del pacchetto Firewall Builder
- Lanciamo lo **script fw_install** che si trova nella directory di installazione del programma denominata "firewall"
- Se tutto è andato a buon fine, appare la schermata seguente che ci conferma l'esattezza delle operazioni compiute fino ad ora



Installazione pacchetti

Cliccando su ogni pacchetto si aprirà la seguente finestra

- Sono elencate le caratteristiche del pacchetto
- Permette la sua installazione attraverso un semplice clic sul bottone **"Install package with YaST"**
- Grazie all'interfaccia intuitiva di YaST, sarà molto semplice portare a termine il setup ripetendo questa operazione per tutti i pacchetti



Primo avvio di Firewall Builder

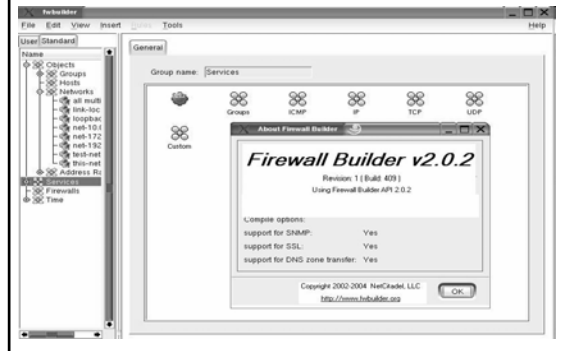
Dopo aver effettuato l'installazione di tutti i pacchetti cliccando sull'icona per la visualizzazione dei programmi, selezioniamo l'opzione "Esegui comando"



Inseriamo il comando "fwbuilder" e si aprirà l'applicazione



Primo avvio di Firewall Builder



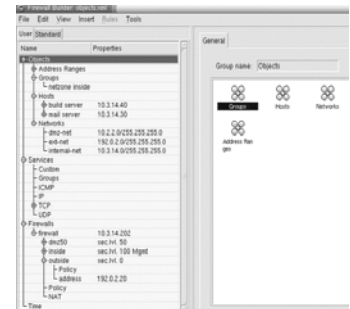
Ci occuperemo di:



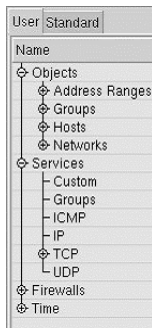
- **Il firewall in generale:** cos'è un firewall, a cosa serve e quali sono le sue caratteristiche principali
- **Descrizione di FWBuilder:** caratteristiche principali del software
- **Installazione di Firewall Builder:** illustra la procedura da seguire per installare correttamente il software
- ⇒ **GUI e Configurazione di Firewall Builder:**
 - Analisi dell'interfaccia (GUI) che caratterizza Firewall Builder
 - Procedura per la configurazione del software
- **Esempio di utilizzo di FWBuilder:** descrive il comune funzionamento di FWBuilder installato su di un host

GUI: finestra principale

- La finestra principale è divisa in due parti:
 - l'albero degli oggetti
 - l'area di dialogo
- Si può creare più di una finestra principale usando il menu principale "File"/"New Window"
- Tutte le finestre sono sincronizzate e lavorano sullo stesso albero degli oggetti
- Le modifiche fatte su un oggetto in una finestra si riflettono in tutte le altre finestre



La Struttura Standard dell'Albero



- L'**oggetto albero** permette di organizzare tutti i tipi di oggetti in una gerarchia
 - Il ramo "**Objects**" contiene i tipi corrispondenti agli oggetti della rete: host, spazi di indirizzi, reti, etc
 - Il ramo "**Services**" contiene invece tutti gli oggetti relativi ai servizi di rete: ICMP, IP, TCP, UDP, etc
- Gli **oggetti standard** rappresentano i protocolli e i servizi usati più di frequente

Oggetto Host con un' unica interfaccia e più indirizzi virtuali

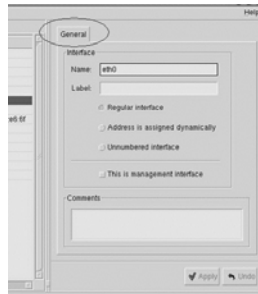
- L'host "test server" situato sulla LAN ha tre indirizzi IP virtuali che appartengono tutti alla stessa interfaccia "eth0"
- L'host "www.netcitadel.com" è remoto, ma ha anche tre indirizzi IP



Interface dell'Host

La finestra di dialogo per l'oggetto **host** ha soltanto la voce "**General**" che fornisce i seguenti comandi:

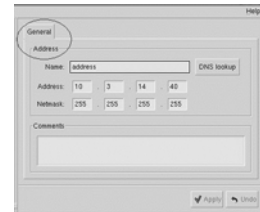
- **Name:** nome dell'interfaccia reale
- **Label:** voce descrittiva
- **"Regular Interface":** usata solo se l'interfaccia ha un indirizzo IP assegnato manualmente
- **"Address is assigned dynamically":** usata solo se l'interfaccia ha un indirizzo IP assegnato dinamicamente per mezzo di DHCP o PPA



Oggetto Address

L'**oggetto Address** definisce l'indirizzo IP dell'interfaccia e fornisce i seguenti campi:

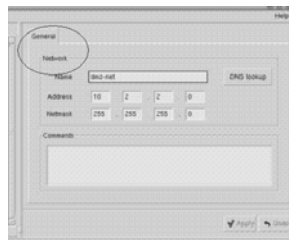
- **Name:** Si suggerisce di usare un nome descrittivo perché quando l'oggetto indirizzo è usato nella politica del firewall, viene identificato con questo nome
- **Address:** l'indirizzo IP dell'interfaccia
- **Netmask:** netmask assegnata all'interfaccia
- **Comment:** Campo testuale libero



Oggetto Network

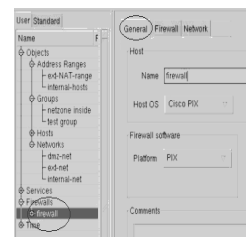
L'**oggetto Network** descrive una rete IP o una sottorete e fornisce i seguenti campi:

- **Name:** Il nome dell'oggetto Network
- **DNS Lookup:** cliccando su questo bottone si esegue una query DNS per ottenere un nome di riferimento
- **Address:** indirizzo della rete
- **Netmask:** la netmask, insieme all'Address, definisce la sottorete



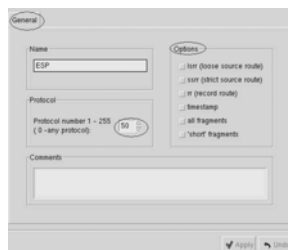
Oggetto Firewall

- L'oggetto Firewall rappresenta l'oggetto più complesso di FWBuilder
- La sua finestra di dialogo ha le seguenti voci:
 - 'General', 'Firewall' e 'Network'
- La voce **General** fornisce i seguenti comandi:
 - **Name:** Il nome dell'oggetto
 - **Host OS e Platform Firewall:** Definiscono i moduli che forniscono il supporto per il Sistema Operativo e la piattaforma in uso
- Le voci **'Firewall'** e **'Network'** forniscono i campi che specificano la piattaforma del firewall e le configurazioni scelte del Sistema Operativo



IP Service

- L'**oggetto IP service** aiuta a descrivere altri protocolli che non sono né ICMP né TCP né UDP
- La schermata riportata in figura, rappresenta l'oggetto ESP (Encapsulating Security Payload, una parte del protocollo IPSEC), il quale utilizza il protocollo IP numero 50
- Oltre al numero del protocollo, l'header del pacchetto IP ha anche un campo chiamato "**opzione**" che è una lista di lunghezza variabile contenente informazioni opzionali del pacchetto



Policy e Rule: Azioni

Le azioni delle policy possono essere di tre tipi:
Accept, Deny, Reject

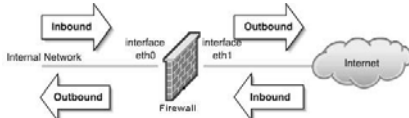
- Se l'azione è **Accept**, un pacchetto con l'indirizzo sorgente e destinazione o un servizio che rispetta la regola viene fatto passare
- Se l'azione è **Deny**, tale pacchetto viene bloccato senza l'invio di alcuna notifica
- Se l'azione è **Reject**, allora un pacchetto è bloccato e un appropriato messaggio ICMP viene spedito al mittente

Policy e Rule: Direzioni

La direzione dei pacchetti è definita considerando la politica di firewall, non la rete controllata da esso

Per esempio:

- I pacchetti che lasciano la rete interna, attraversando il firewall, sono considerati "inbound" nell'interfaccia interna del Firewall e "outbound" nell'interfaccia esterna
- I pacchetti provenienti da Internet sono "inbound" nell'interfaccia esterna del firewall e "outbound" nell'interfaccia interna



Ci occuperemo di:



- Il firewall in generale:** cos'è un firewall, a cosa serve e quali sono le sue caratteristiche principali
- Descrizione di FWBuilder:** caratteristiche principali del software
- Installazione di Firewall Builder:** illustra la procedura da seguire per installare correttamente il software
- GUI e Configurazione di Firewall Builder:**
 - Analisi dell'interfaccia (GUI) che caratterizza Firewall Builder
 - Procedura per la configurazione del software

→ Esempio di utilizzo di FWBuilder: descrive il comune funzionamento di FWBuilder installato su di un host

Esempio di utilizzo di FWBuilder

- Dopo aver lanciato in esecuzione il programma, ci troveremo di fronte alla schermata principale del software
- Cliccando sull'icona "New", si aprirà il seguente menù a tendina dal quale sceglieremo l'opzione "New Firewall" per creare un nuovo oggetto firewall



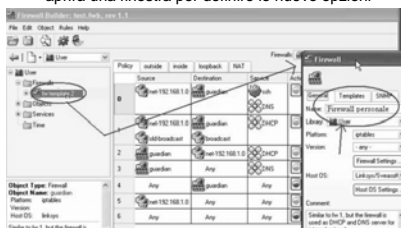
Esempio di utilizzo di FWBuilder

- Ora, scegliendo come configurazione di rete del nostro host "Firewall protects local host", ci presenteranno alcuni template standard da utilizzare successivamente per la configurazione del firewall stesso
- Scegliamo la **seconda opzione** che ci permetterà di configurare il nostro host e la sua interfaccia di rete
- Cliccando sul tasto "Finish", torneremo nella schermata principale



Esempio di utilizzo di FWBuilder

Con un doppio click sul nome dell'oggetto firewall appena creato, si aprirà una finestra per definire le nuove opzioni



Così facendo abbiamo rinominato il nostro firewall in "Firewall personale"

Esempio di utilizzo di FWBuilder

I parametri

- Source:** applicazione/host sorgente
- Destination:** applicazione/host di destinazione
- Service:** tipo di servizio in uso
- Action:** azione da associare all'applicazione

Policy	Interface	Source	Destination	Service	Action	Time	Options
0	eth0	any	any	any	Deny	Any	Remember this setting
1	eth0	any	any	any	Deny	Any	Remember this setting
2	eth0	any	any	any	Deny	Any	Remember this setting
3	eth0	any	any	any	Deny	Any	Remember this setting
4	eth0	any	any	any	Deny	Any	Remember this setting
5	eth0	any	any	any	Deny	Any	Remember this setting
6	eth0	any	any	any	Deny	Any	Remember this setting
7	eth0	any	any	any	Deny	Any	Remember this setting

Opzione "Remember this setting":

- se l'applicazione accede frequentemente alla rete, una semplice spunta sulla casella permette a FWBuilder di memorizzare la policy ad essa associata

Conclusioni...



- Vogliamo concludere questa nostra guida ricordando che per quanto un firewall possa essere affidabile, potrebbe anche non proteggerci adeguatamente perchè come abbiamo visto, siamo noi utenti a decidere quali applicazioni possono accedere alla rete
- Se non si è sicuri di un'applicazione, è sempre meglio bloccarla, documentarsi e poi permetterle l'accesso alla rete se realmente necessario!!

Speriamo solo che la nostra guida vi sia stata di aiuto!!

Grazie!