Firewall e

Port Forwarding

www.avm.de

Descrizione

Nelle reti di computer il Firewall è quell'elemento di difesa perimetrale che ha lo scopo di proteggere una rete (locale o privata) da accessi non autorizzati.
Un Firewall può permettere l'accesso ad una certa tipologia di traffico o bloccarla, basando la sua decisione su una serie di parametri come la destinazione della comunicazione e la tipologia della stessa.
Un Firewall tipicamente consente le connessioni verso la rete privata che deve proteggere solo se la richiesta è stata inizialmente originata dalla rete locale.
Ad esempio, attraverso un browser è possibile visualizzare delle pagine web perché la richiesta delle stesse parte dalla nostra rete locale.
Un Firewall in grado di operare un controllo sui pacchetti di dati che vengono scambiati tenendo traccia dello stato dei vecchi pacchetti viene identificato come *Stateful Packet Inspection* (SPI) Firewall.
Questa tipologia di Firewall consente di implementare un sistema in grado di applicare dei filtri alle connessioni, consentendo l'accesso alla nostra rete locale anche se la richiesta è originata da un'altra rete.
Il FRITZ!Box integra questa tipologia di Firewall Stateful Inspection, grazie al quale ad esempio consente l'accesso remoto all'interfaccia grafica di utente (GUI), come descritto nella mini-guida su "Dynamic DNS e Accesso Remoto".
Questo sistema di filtri viene tipicamente identificato con il meccanismo *di Port Forwarding*: con questa tecnica si fa riferimento quindi alla capacità di un router di riconoscere una certa tipologia di traffico, originato da una altra rete e destinato ad una applicazione o ad una porta di comunicazione nota, e di re-indirizzarlo verso una destinazione specifica della propria rete locale.

La funzionalità di Port Forwarding si rivela particolarmente utile quando nella propria rete locale sono presenti delle applicazioni o macchine che devono poter essere raggiunte anche da remoto come ad esempio un Mail Server, un Print Server, un sistema documentale con interfaccia web, ecc..; oppure ad esempio quando si desidera controllare una postazione terminale tramite applicativi di desktop remoto

Configurazione e utilizzo

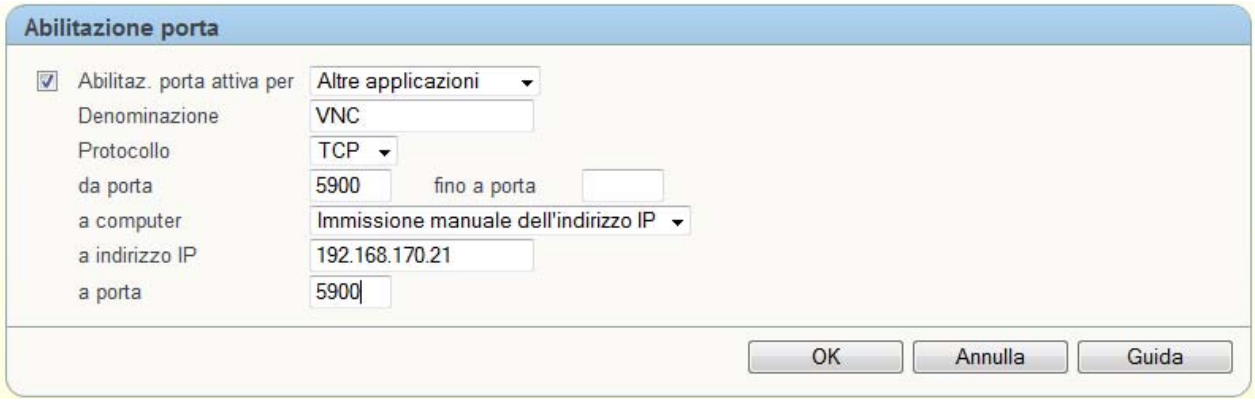
Per configurare delle regole di Port Forwading accediamo alla GUI del nostro FRITZ!Box utilizzando un browser e digitando nella barra degli indirizzi: *fritz.box*
Accediamo quindi al menu "Internet" → "Abilitazioni" → "Abilitazioni porte" e clicchiamo sul pulsante **Nuova abilitazione porta** per creare una nuova regola.

Il FRITZ!Box di default prevede già alcune regole relative ad applicazioni note e che sono preselezionabili, come ad esempio:

Server HTTP: filtra le richieste verso la porta tcp 80 di un client nella LAN
Server FTP: filtra le richiesta verso la porta tcp 21 di un client nella LAN

Le altre opzioni disponibili sono per le connessioni con emule su protocollo TCP e UDP, il Desktop Remoto di Microsoft, la funzionalità di *Exposed Host* che vedremo più avanti.

Per configurare una regola in maniera generale selezioniamo nel nostro caso l'opzione **Altre applicazioni:** la maschera di configurazione per i filtri da applicare sarà come quella in figura sotto e presenta diversi campi.



Nel dettaglio:

Denominazione: specifica il nome della regola da applicare
Protocollo: le opzioni possibili sono TCP, UDP oltre ad ESP e GRE[1]
da porta – fino a porta: specifica la porta o il range di porte da filtrare
a computer: seleziona un client, ad esempio un PC, già presente nella rete lan o consente di inserire manualmente l'indirizzo IP della destinazione
a porta: specifica la porta di destinazione (o il range di porte, se selezionato in precedenza)

Nell'esempio proposto in figura abilitiamo la connessione TCP verso la porta 5900 del PC con indirizzo IP 192.168.170.21: con questa regola abilitiamo l'accesso al Desktop Remoto del PC selezionato, tramite l'applicativo VNC.
Questo significa che collegandosi all'indirizzo IP pubblico del FRITZ!Box[2] sulla porta 5900 il nostro access gateway inoltrerà direttamente questa connessione verso la porta 5900 del PC che abbiamo configurato nella regola.

Selezionando la modalità di *Exposed Host* è possibile indicare verso quale client della rete locale devono essere destinate tutte le connessioni: in pratica è come se venisse disattivata la funzionalità del Firewall integrata nel FRITZ!Box.
Questa opzione può risultare utile in taluni scenari applicati, come ad esempio nell'utilizzo di un FRITZ!Box in combinazione con un Firewall specifico.

Link Video:

http://www.avm.de/de/Service/FRITZ_Clips/start_clip.php?clip=fritz_clip_firewall_en

[1] Utilizzati per applicazioni VPN passthrough

[2] Oppure tramite il nome DNS con Dynamic DNS