

16. DMZ

16.1 Firewall

Definition

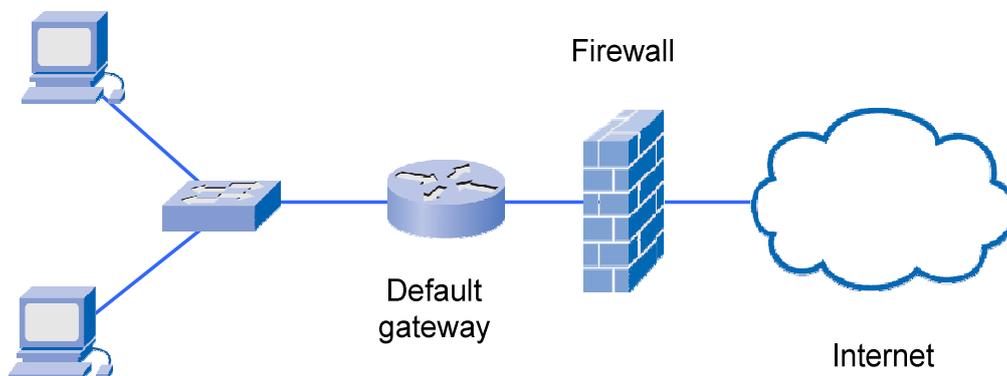
A firewall is a network security system that can block the incoming and the outgoing network traffic based on rules set within the firewall.

We can classify all firewalls into two types:

1. External firewalls
2. Personal firewalls

External firewall:

An external firewall is a hardware component switched between the router and the internet. The external firewall analyzes traffic to and from a whole network.



Personal firewall:

A personal firewall is a software installed on a host. The personal firewall analyzes the traffic to and from the host it is installed on. This software can be part of the operating system.

Functionalities

Simple firewalls operate on the transport layer (layer 4).

This fact tells us that a firewall is able to analyze from which or to which software / port number a frame is sent to. Thus all firewalls are able to distinguish between incoming and outgoing traffic. Under outgoing traffic we understand a request going out of our network including the incoming answer to the request.

Consequently under incoming traffic we understand a request coming in our network including the outgoing answer to the request.

Most firewalls for private networks are configured by default such that all outgoing traffic is allowed to pass the firewall, but all incoming traffic is blocked. This configuration is fine for most private networks only consisting of hosts requesting information from outside of the network.

If however a server application within the private network needs to be accessible for requests coming from the internet, e.g. private web servers or gaming server, then an exception to the general rule for incoming traffic has to be added. We say "a port has to be opened in the firewall". This exception rule will allow requests to pass the firewall that are addressed to the port number defined in the rule. The firewall rules can often be manipulated over a web-interface.

Example:

Freigaben

Portfreigaben Fernwartung Dynamic DNS VPN IPv6

An FRITZ!Box angeschlossene Computer sind sicher vor unerwünschten Zugriffen aus dem Internet. Für einige Anwendungen wie z.B. Online-Spiele oder das Filesharing-Programm eMule muss Ihr Computer jedoch für andere Teilnehmer des Internets erreichbar sein. Durch Portfreigaben erlauben Sie solche Verbindungen.

Liste der Portfreigaben

Aktiv	Bezeichnung	Protokoll	Port	an Computer	an Port	
<input checked="" type="checkbox"/>	eMule TCP	TCP	4662	192.168.1.20	4662	

Änderungen der Sicherheitseinstellungen über UPnP gestatten
Programme mit UPnP-Unterstützung können Sicherheitseinstellungen wie die Portfreigaberegeln der FRITZ!Box automatisch verändern. Aktivieren Sie diese Option aus Sicherheitsgründen nur, wenn Sie tatsächlich eingehende Verbindungen aus dem Internet gestatten möchten.

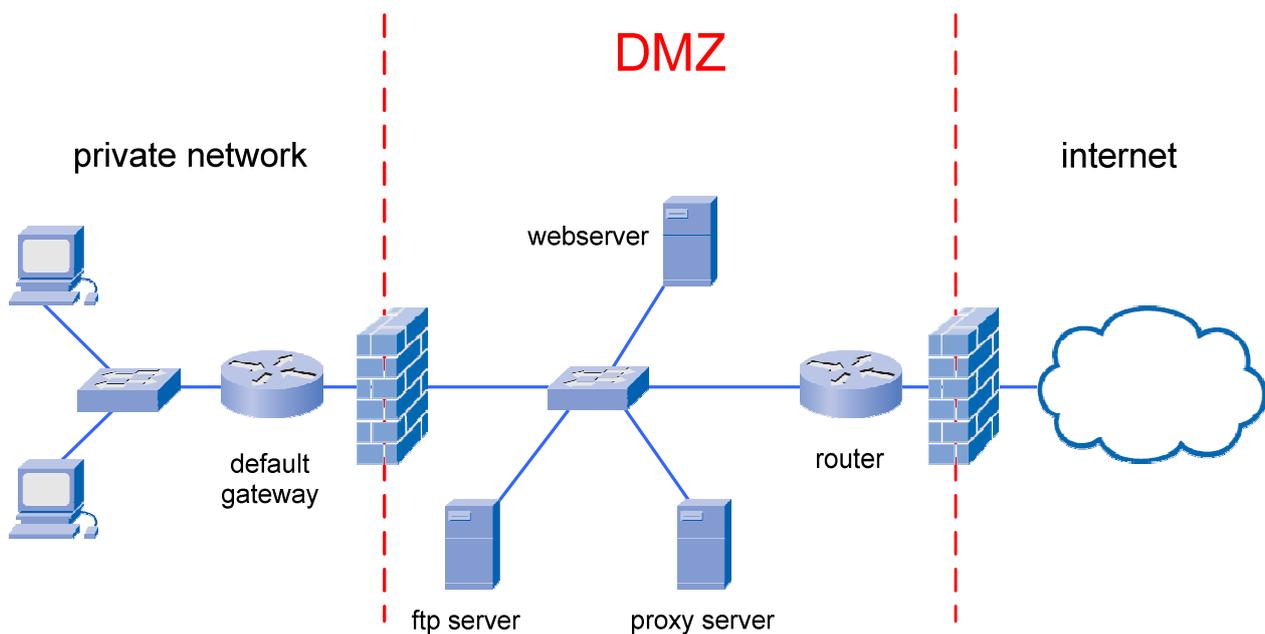
Neue Portfreigabe

Übernehmen Abbrechen Aktualisieren Hilfe

16.2 DMZ (demilitarized zone)

The weak point of the above shown network configuration is that if hackers detect a vulnerability (deut.: Verwundbarkeit) in the server software behind an open port, then attacks can be made to the whole network behind the firewall.

The current best practice is therefore to install a DMZ, which is a network portion between the private network and usually the internet. The DMZ is secured by two firewalls from the rest and contains the servers that should be accessible from the internet and the private network.



A request from the internet is passed through the first firewall to the servers.

All requests from the private network to the internet are sent first to the proxy server who forwards the requests to the internet.