How to Install a Demilitarized Zone for Your Servers

What is a Demilitarized Zone (DMZ)?

Common setups used for small and medium networks include a firewall that processes all the requests from the internal network (LAN) to the Internet and from the Internet to the LAN. This firewall is the only protection the internal network has in these setups and it handles any NAT (Network Address Translation), forwarding and filtering requests as necessary. In most cases, the firewall also runs public services accessible from the Internet, such as web services and e-mail services. Within such setups, the DMZ is thus installed on and limited, we may say, to the server.

Why use a DMZ?

A DMZ aims to secure the internal network from external access. It does so by isolating the public services (requiring any entity from the Internet to connect to your servers) from the local, private LAN machines in your network.

The most common method of implementing such a divider is by setting up a firewall with three network interfaces installed. The first one is used for the Internet connection, the second for the DMZ network and the third for the private LAN. Any inbound connections are automatically forwarded to the DMZ because the private LAN does not run any services and is not connectible. Therefore, setting up the DMZ helps isolate the LAN from any Internet attacks.

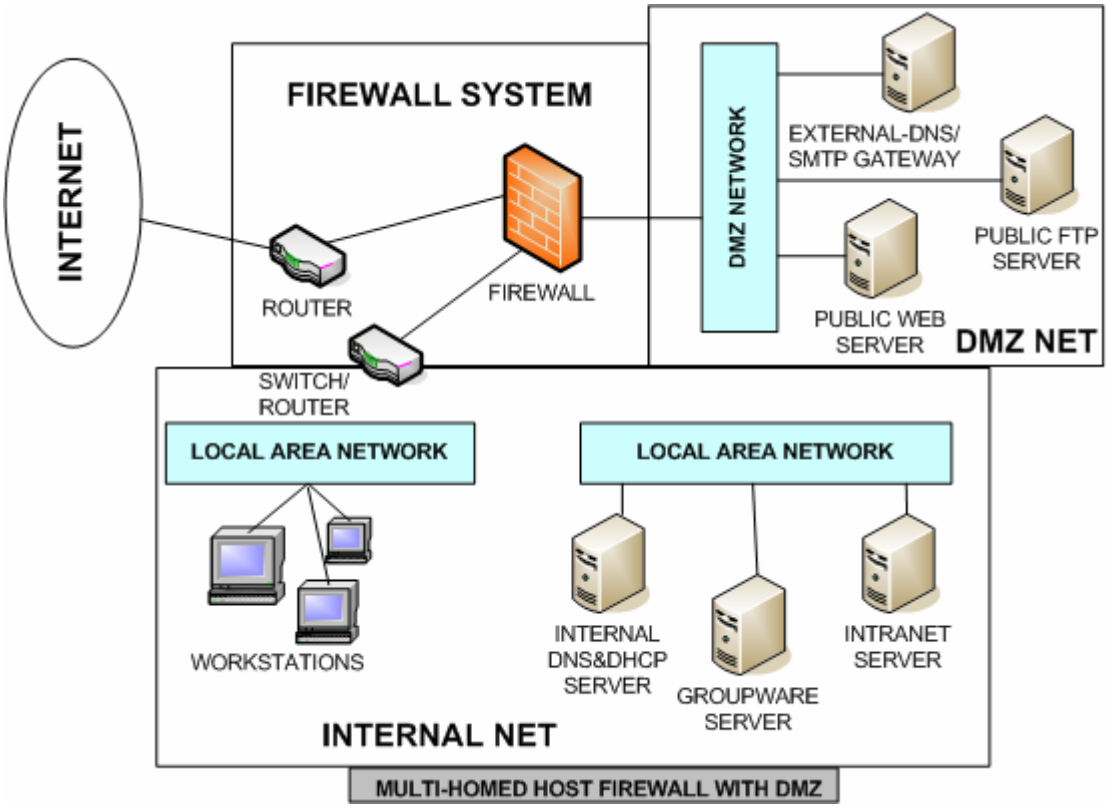
How to set a DMZ?

First of all, you need to decide what services will run on each machine. The DMZ is generally on a different network segment, both physically and logically. This means that you need to use a separate machine to host the services you want to make public (such as DNS, web, mail etc.). From the connectivity point of view, the DMZ will be located on a different subnet than the LAN.

All requests go through the firewall, so it has to be set up correctly. The success of a DMZ depends on the traffic management. No connections are to be forwarded to the LAN, as that is precisely the network segment that we aim to protect. Also, no connections should be initiated from the DMZ to either the protected network or the Internet, except the required services (like SMTP). As these services can easily be monitored, specific rules should be made in the firewall configuration to enforce the correct policy at all times.

Furthermore, NAT should be provided for the computers on the LAN in order to enable the Internet access for the client hosts. The clients should also be enabled to connect to the servers in the DMZ.

The final setup should look like this:



Hardening the DMZ machines

Computers in the DMZ obviously need to be hardened as much as possible given the fact that they will be in the first line, right behind the firewall. Their position will prevent attacks on the LAN, but it may also increas the risk to get compromised.

Here is a list of methods that you can use to increase the security of your DMZ systems:

- Disable all unnecessary services and dæmons;
- Run services chrooted whenever possible;
- Run services with unprivileged UIDs and GIDs whenever possible;
- Delete or disable unnecessary user accounts;
- Configure logging and check logs regularly;
- Use your firewall's security policy and anti-IP-spoofing features.

The DMZ infrastructure can also be improved by adding multiple demilitarized zones with different security levels, depending on the number of systems and services being deployed on the network. These zones can be assembled in a tier-like structure so that the information is passed from one DMZ to another.

This type of network infrastructure is not the most secure way of protecting the private perimeter, but it is sometimes required. An example of such situation would be when a web server placed in a DMZ requires access to a database server over a secured port (and that port only) placed in a second DMZ. This database server could ultimately access some data found on the private LAN systems, if there is such a requirement. This way, the database is secured from public exposure, while keeping the web server accessible and the private LAN, isolated.

Note: The above-listed methods apply to Linux/*NIX-type systems only.

What to keep in mind?

The simplicity of the DMZ concept makes it very powerful and prolific. A DMZ can be considered a safe-guard, although it is not a security measure by itself. However, with a tight and well-thought network infrastructure, IDS (intrusion detection systems) and IPS (intrusion prevention systems), it can become a barricade against attackers and unwanted or unneeded traffic.