



This is a non-technical introduction to the uses and configuration of firewalls and networks in a corporate environment. For more detailed and network technical information see other FAQs on <http://www.Xnet.com.pk/>

Basic Functions of a Firewall.

Firewalls primarily provide access control for connections between networks. Usually this will be the connection between a corporate network and the Internet. For our security purposes we classify networks as either

- 1 Trusted: this is usually the corporate LAN. It is assumed that all PCs and servers in the LAN are under your administrative control. If users are able to change their IP address and install software at will then
- 2 Untrusted: the Public Internet, the Firewall's WAN interface;
- 3 Partially trusted: the Firewall's DMZ interface. These are machines under our control, but freely accessible from the Internet. These are not fully trusted because it is assumed that being accessible they will be compromised or hacked at some time.

The LAN is allowed to access the WAN and DMZ on certain ports for certain services. These services are determined according to your security policies. Services not explicitly allowed are blocked.

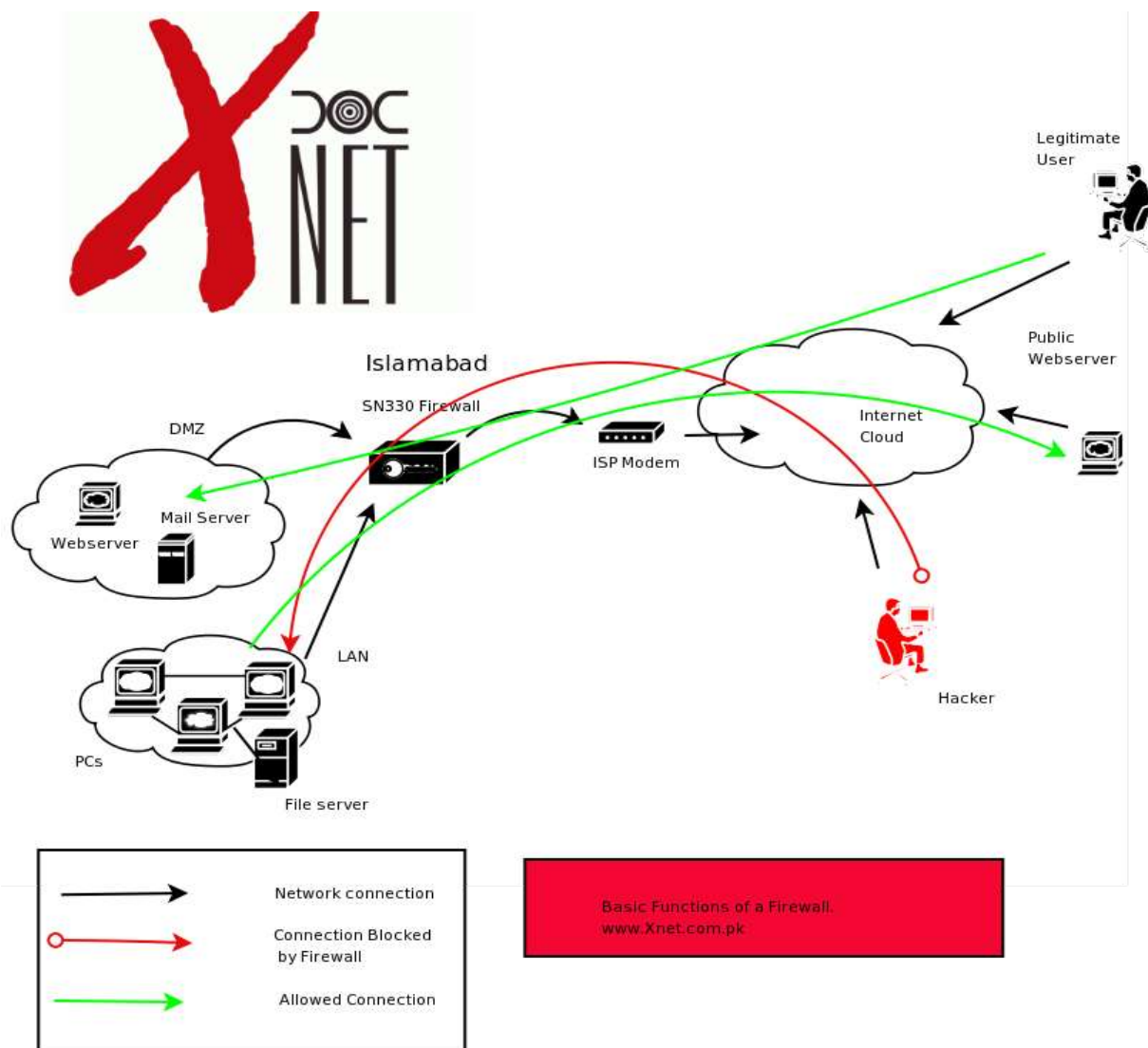


The WAN is allowed to access the WAN and DMZ on certain ports for certain services. These services are determined according to your security policies. Services not explicitly allowed are blocked. For example a Web server will only be accessible on port 80 reducing the possibility of a successful attack.

The DMZ is allowed to access the WAN on certain ports for certain services. These services are determined according to your security policies. Services not explicitly allowed are blocked. For example a Mail server in the DMZ may be allowed to access a few DNS servers on port 53 only; also it would be allowed outgoing access to any SMTP server on port 25. Incoming access would be on POP3, port 110.

A setup as described above provides

- excellent security from external threats
- controls the connections that LAN pcs are allowed out to the WAN
- proper utilisation of expensive bandwidth
- full speed access to internal and external resources



Here we see that the Legitimate user has access to the public servers (the Web server

and the Mail server). The Hacker that is trying to attack the LAN, has no access. Of course the Hacker has access to the public servers but only on selected ports so the possibility of a successful attack are minimised.

Xnet Solutions is a vendor and manufacturer of Network Appliances: the SN330 hardware firewall, the MX100 which is a mailserver and also a mail filter for existing mail servers. <http://www.xnet.com.pk/>

© Xnet Solutions, Karachi, Pakistan 2005, 2006.