



## TenStep Supplemental Paper

4 February 2008

### Firewalls for Security

Installing a firewall is the first and the chief step towards defending the security of any organization. However, just installing a firewall does not mean that the organization is entirely safe and secure from any attacks on the network. Once the firewall is installed, the rule set or policy file should be configured. A rule limits the boundaries against which each connection is compared, resulting in a resolution on the action to be taken for each connection. Also, a rule-set specifies the services that need to be let through the firewall and the ones that need to be kept out.

A rule, regardless of the kind of firewall installed, consists of a source address, a destination address, a service, and an associated action. In the table given below, the rule set of Feature1 and Feature2 could be any kind of advanced feature, such as time-sequence parameters, anti-virus parameters or intrusion-detection parameters.

SOURCE	DESTINATION	SERVICE	ACTION	FEATURE 1	FEATURE 2
Local-net	Anywhere	HTTP	Allow	Optional	Optional
VPN-clients	Anywhere	SMTP	Allow	Optional	Optional
VPN-clients	Radius Server	Telnet	Allow	Optional	Optional
Any	Any		Deny	Optional	Optional
Firewall	Demo-net	FTP	Allow	Optional	Optional
Customers					

A few firewalls, by default, come with their ports closed (automatic port blocking). However, again by default, sometimes the firewall comes with all the ports and services open. In such a case, the best way to start the rule-set configuration process is to close everything and open up only those services that are specifically required. The standard services that should be taken into consideration are:

- HTTP (Web surfing)
- HTTPS (Secure Web surfing)
- SMTP (e-mail)
- ICMP (Reporting services, Ping)
- Telnet (Bi-directional communication sessions)

Sometimes other types of traffic need to be let into the network. However, every additional service allowed through the firewall increases the risk of the network and systems being left open to security exploits. To avoid such problems, the more restrictive rules should be listed first, followed by the least restrictive rules. It is to be noted that if a less restrictive rule were placed before a more restrictive rule, the scrutiny would be stopped at the first rule itself. Mentioned below are a few time-tested best-practice firewall rules.



## TenStep Supplemental Paper

---

- Anything from inside the network is allowed out, enabling the users to have full control over the services needed.
- The total access to the firewall itself is blocked from the Internet. The system administrators are the only people with access to the firewall.
- SMTP messaging services for Internet and also the internal users are allowed to pass through the firewall in order to receive and send e-mail.
- ICMP services are turned off to prevent utilities such as ping to pass through the firewall. This does not allow hackers to break into the network.
- Telnet access to all the internal servers from the Internet is blocked. Also, Telnet access to the DNS server is blocked to avoid illegal zone transfers. If the internal users need to enter the network from outside the firewall, a VPN client or other secure authentication system should be used.
- If the Web server is situated outside the firewall, then HTTP should be blocked from reaching the internal networks. This way, when the Web servers are used from within the network, the services are visible to the outside Internet. However, if the Web server is behind the firewall, then HTTP or HTTPS should be allowed for total Internet viewing. Therefore, it is advisable to have the Web servers installed outside the firewall.

It should be understood that even the most restrictive firewall policies do not guarantee the systems being safe from attacks. However, a firewall, when properly configured, would surely reduce the risk of any major security hazard to the network and systems.