

Internet Security

Various forms of security for your network

- **Password/login Protection**

We ship all hardware with a default password and/or login. This should be changed during the initial installation of the hardware.

- **Packet Filters**

We do not ship routers with filters. Filters will allow you to specify which services you would like to block or allow, both to and from, your network. Our online filter builder at <http://www.support.ip.inter.net/support/fbuilder/index.html> can be used to generate a filter set specifically for your router.

- **Dividing Network Space**

Public Subnetwork: Servers and workstations that require public access.

Private Subnetwork: Servers and workstations that are for internal use only.

Possible attacks against your unprotected network

- **Smurf Attacks**

Pings sent to broadcast addresses which produce replies which in turn cause network congestion or network outages. The following web site includes descriptions of the **Attacker**, **Intermediary** and the **Victim** as well as tips on protecting your network against these attacks.

<http://www.quadrunner.com/~chuegen/smurf.cgi>

- **Spamming**

Relay spamming is done when an attacker uses someone else's mail server to relay mail, maybe in bulk amounts. This in turn steals the victim's network capacity, disk space and processing power. This can cause your entire network to crash, known as a **Denial-of-Service** attack. This is a big cause for concern because spammers now have tools to scan the Internet for open relays.

<http://maps.vix.com/tsi/ar-test.html> - To test your email server for vulnerability to these attacks.

<http://maps.vix.com/tsi/ar-fix.html> - Instructions to prevent these attacks.

CERT Coordination Center

CERT is an organization who is continually finding new attacks that can be made against your network and ways of protecting your network again these attacks.

<http://www.cert.org> - CERT web page

***Statement of Disclaimer:** All sites should perform a complete risk analysis with regard to their network and company security policies to determine exactly what additional security measures are required, or which are unnecessary. There is no such thing as perfect security under TCP/IP. This list of security measures will NOT guarantee any sort of security.