



24/7 network protection.

## Security/VPN

The PowerElf™ II was designed to provide networks with a wide variety of security options. The firewall protects your Internal network, while the VPN allows for the easy and secure communication of information from outside the network.

### Benefits of Stateful Packet Filtering?

#### Added Security

Adds security against port scanning by closing off ports until a connection for the port is requested.

#### Logging:

The firewall, logs all information related to a session in a state table. This information is then used, along with the rules outlined in the PowerElf™ II software, to make more informed policy decisions than a stateless firewall.

In addition to the stateful packet filtering implemented on the PowerElf™ II the following security features are used to protect your network. NAT (network address translation) is used to masquerade the internal network behind the PowerElf™ II. All traffic on the external (Internet) port is denied unless specifically permitted by the PowerElf™ II, protecting the internal network from attempts by intruders to gain access to the network through the external port.

### VPN

Businesses need a secure method of remotely connecting to the network. The PowerElf™ II provides this secure remote connection with support for both PPTP and IPSec VPN.

#### PPTP

PPTP allows remote users to securely and inexpensively access their corporate network from anywhere on the Internet.

PPTP uses a client-server model for establishing VPN connections.

#### IPSEC

IPSEC stands for "Internet Protocol SECurity". It uses strong cryptography to provide both authentication and encryption services. Authentication ensures that packets are from the right sender and have not been altered in transit. Encryption prevents unauthorized reading of packet content.

The PowerElf™ II implementation of IPSEC allows administrators to connect two networks together and create a secure passage for data between the two locations.



Prevent network attacks.

## Intrusion Detection System (IDS)

The IDS can be administered from the PowerElf™ II Manager. Features available in the Manager include:

- The ability to enable and disable the IDS.

- Choosing the type of IDS protection (reporting enabled or having a system that both logs and blocks suspected attacks).

What will IDS provide:

IDS will provide your network with real-time traffic analysis, logging and IP blocking. An Intrusion Detection Systems allows network administrators to stay informed of potential threats on their network.

IDS Analysis Console

The PowerElf™ II IDS provides an analysis report of your servers intrusion detection system. This report includes all alerts with detailed information including, the type activity that triggered the alert and information regarding origin of the threat. All the information available in the Analysis Console can also be exported to a graph. Graphing history can be a valuable tool in detecting patterns of attack and to help detect network vulnerabilities.

Benefits of using an IDS

- Provides real-time logging and alerts.

- Enhanced security for the PowerElf™ II, internal network computers and any other servers inside the network.

- Provides easy to understand reports with detailed information on attempted attacks.

- Provides peace of mind and security for the administrator.

The Advantage of the PowerElf™ II IDS

The PowerElf™ II server uses a combination of advanced firewall features, IDS and optional mail server anti-virus to provide your network with a complete security package.

The PowerElf™ II IDS is a bundled package of three applications to create a full Intrusion Detection “monitoring, logging, scanning and preventing” system on your network.

The PowerElf™ II IDS is powered by SNORT IDS, a leading IDS system with over 100,000 installations worldwide.