

### **What is Unified Threat Management?**

The SecPoint® Protector is an Unified Threat Management appliance. This includes many capabilities such as Anti Virus, Anti Spam, Anti Spyware, Anti VoIP, Instant Message Recording, Intrusion Prevention, and Content Filter all integrated in the same appliance. Previously all the functions were handled by multiple systems.

It is advantageous for the customer to have a centralized update point, reporting tool and control of the content on the traffic coming in and going out of the network.

### **What is the advantage of an Unified Threat Management?**

Unified Threat Management is a cost-effective solution to integrate multiple high tech technologies into a single appliance.

This also ensures you a higher level of security because you do not need to manage multiple appliances and keeping them up to date. With a Unified Threat Management appliance you have the following advantages: centralised management, less time used for maintenance, centralized updates multiple times daily, better performance, easier configuration and maintenance.

### **What does Unified Threat Management include?**

It is very important for an Unified Threat Management appliance to ensure the customers the highest quality and most up to date engines and databases 24/7.

SecPoint has chosen to use the strongest and most advanced technologies in each category:

**Anti-Spam:** Using the award winning SpamAssassin the latest version with the wide range of configuration possibilities to ensure the most accurate spam capture with more than 97% of all spam.

**Anti-Virus:** Multiple Award Winning Kaspersky labs Anti-Virus guarantees proven quickest virus definitions updates. As a backup ClamAV is also used to ensure the customer everything will be scanned twice. The protocol scanner allows scanning of services like, FTP, WEB, MSN, and other services for Virus.

**Anti-Spyware:** Scanning both incoming and outgoing traffic protects from infection from the Internet and prevents already infected systems from leaking sensitive information.

**Intrusion Prevention:** Updated multiple times a day and including intelligent Zero Day Protection that blocks for known and unknown vulnerabilities.

**Content-Filter:** Allows the user to control several elements on the network.

It includes: Anti-Free Mail to block public email sites, Anti-Game to block known network games such as Counter-Strike.

**Anti-VoIP:** With the Anti-VoIP you can block programs like Skype, Google Talk, Yahoo, VoIP Devices so you have full control of the traffic on your network and how your employees are communicating.

**Anti-P2P:** With the Anti-P2P you can ensure that your bandwidth is not being wasted or abused by the downloading and sharing of copyrighted materials.

The blockings include BitTorrent, GNUTella, Kazaa, Napster, eDonkey2000, Emule, Morpheus and more.

**Anti-Phishing:** Gives the customers clear warning about phishing attacks and the blocking of phishing websites.

**Web Blocker:** This allows for blocking of websites such as news sites. This can help you ensure that your employee's time is not wasted by browsing news websites.

