

## Unified Threat Management

Unified Threat Management (UTM) takes all the security monitoring and management tasks typically done by firewalls and various other security appliances, and includes them beneath one security umbrella. Grouping these services together saves your business money and ensures a unified approach to security within a single device. When managed by Alliance Technologies' security experts, this gives you quality service at an affordable price. We can either manage the on-site firewall device your business already owns or set up a new device for you.

### Features:

Most UTM devices include these services:

**Firewall Management, Logging, Alerting and Monitoring**—A firewall is often the first layer of security used to protect your network, but without logging, alerting and monitoring, it is not being fully utilized. These services allow managing of the firewall to quickly and appropriately respond to new security threats as they happen. On certain models, the logging can be extended to allow for monitoring of the servers the firewall is protecting.

**Intrusion Detection and Prevention**—Intrusion detection and prevention services (IDS/IPS) monitor traffic on your network to proactively identify malicious traffic and stop it at the source. In addition to monitoring for known attack types, some IPSs monitor traffic behavior to identify and prevent unknown threats. Due to the complexity of monitoring network signatures, most intrusion systems bundled in UTMs are effective, but are not a replacement for a dedicated IDS/IPS appliance.

**Web Content Filtering**—Employees used to be allowed to go wherever they liked on the web, since management figured that as long as the job got done, it didn't matter. However, modern attacks leveraging social media and online games have changed the threatscape. Web filtering has become a technology that is essential to protect your business from malware that can steal money right out of your bank account. While it is commonly used to block categories such as pornography or gambling, web content filtering can also block websites based on content and keywords.

**Antivirus**—End-point anti-malware software is the best solution for desktops and servers, but placing protection at the edges of your network can provide an excellent auxiliary layer of defense. This reduces the amount of malicious traffic reaching your end points, and frees up resources on those systems while reducing the attack surface.

**Data Loss Prevention**—Like IDS/IPS, a data loss prevention (DLP) service monitors network traffic; but instead of looking at incoming attacks, it analyzes outgoing data. If data is found to contain sensitive information such as credit card data, it can block or alert on the issue. Like IDS/IPS, the DLP service on a UTM is not a replacement for a dedicated DLP appliance.

### Pricing Model

The Alliance Technologies UTM solution includes three pieces: a hardware device, a yearly license and a monthly monitoring service. Please see the supplementary hardware sheet for hardware details to determine if your existing firewall can use the Alliance Technologies UTM management service.