Cyberoam CR25ia UTM

By Peter Nalika

The good: The Cyberoam CR25ia UTM provides security across the seven layers of the network protocol. Using identity-based policies, it offers multiple security zone firewalls from the data link layer to Layer 8 where the user sits. It supports Gigabyte Ethernet and IPv6 standards, among other nice networking features. The UTM device also comes with a USB port for updating its firmware, which takes the form of an embedded Linux operating system.

Its most interesting feature is its flexibility in managing web content. The CR25ia offers fine-grained levels of control, for example it can restrict what websites a user visits by time of day. Alternatively, access can be controlled by using groups, for instance only allowing sales persons access at certain time of the day while giving fulltime access to managers. Website access may also be controlled depending on the site's size. For instance an administrator may wish to restrict access to sites using IP addresses, and perhaps also limit user downloads to 100MB per day.

The bad: The CR25i requires a working Internet connection during the initial setup. Although its interface program does offer content filters, there are some drawbacks to the device such as some efforts are not being as steady as they should be, as well as the response time being slow when more than 2000 users are simultaneously connected to the device. Despite it having the ability to carry out HTTP inspection by scanning traffic for malware, viruses and trojans using the existing database, the CR25ia still offers little or no protection for new or unknown vulnerabilities like zero-day attacks.

The bottom line: The CR25ia is an advanced device from Cyberoam with excellent security features right from net work security, to content and administrative security. In addition, it provides an abundance of network connections via the VPN & 3G/WIMAX connectivity. It also guarantees continuity for enterprises using its multiple link-management features.

Being an improvement over the previous Cyberoam CR15i model, the CR25ia has greater capacities in terms of throughput for firewalls, antivirus, UTM and Intrusion Prevention System (IPS). It ensures link management with an automated load balancing feature that aids the distribution of traffic over multiple links. This feature alone greatly assists in optimizing the use of WAN links.

Compared to its peers, the CR25ia is not radically different, except for its extended performance and size. However, the built-in UTM firewall offers stateful deep-packet inspection for network inspection and user identity based security. This kind of feature protects organizations from increasingly common Denial of Service, (DoS) and IP spoofing attacks.

Other devices in the huge Cyberoam network security family, for instance the CR50i, have built-in double ISP configurations. This allows two links such as Jambonet and Safaricom to be terminated to the device at the same time. This offers the advantage of accessing and utilizing both lines simultaneously.

Design

Unfortunately, the CR25ia UTM device is no wallflower. It's certainly not pretty, it's not that compact, and its functions and inbuilt features- the WAN and LAN links and other multiple connections that should pass through it - all mean it is not the sort of device to sit on an office desk.

The device ships with a WAN port, which connects directly to the Internet. Now, this is usually not a trusted interface, and is therefore marked red. The LAN port connects to the local area network – it is trusted and therefore marked as a green interface. The CR25ia also has a useful extra LAN port in addition to the marked one.

The WAN and LAN ports are Gigabit–capable, meaning they support data throughput up to 1,000 Megabits per second (Mbps). At the back of the unit you will find the De-Militarized Zone (DMZ) port which connects to a server farm and helps segregate and stop devices that are directly Internet-accessible from intruding into the rest of the corporate LAN. The Cyberoam CR25ia has a USB port and a console. Both can be used to update its firmware, though you first need to understand how to use the command prompt in case you use the console option.

At the front the new CR25ia has the usual array of status LEDs. These are well labelled and light up in green when in full duplex mode, amber when in half duplex mode and solid red in case of a problem.

Like many other UTM devices, the CR25ia supports a wide range of standards among them 3DES, AES, Two fish, Blow fish and Serpent. It also supports the MD5 and SHA-1 algorithms.

Its interface is intelligent; it supports fusion technology by blending in security, connectivity, and productivity. Multiple features that control various security policies can be created through a single interface.

Performance

The Cyberoam CR25ia is amazing in terms of setting up internet policies that can be defined and tweaked by administrators to suit their individual needs. This is one area it scores highly when compared to some other UTM devices from other companies, for example those from Cisco Systems and Juniper Networks that offer little flexibility in terms of controlling Internet usage.

The Cyberoam CR25ia performs very well in terms of content filtering and traffic inspection, especially when compared to products from Juniper Networks, which are more of enterprise solutions geared towards large ISP's, telecommunication companies, and massive network installations.

In terms of throughput, i.e. the number of packets that can be handled at any given time, the CR25ia offers 225 Mbps firewall throughput and 50 Mbps UTM throughput - these metrics are fantastic for network connectivity. The device is thus up to the challenge of handling almost all traffic that may be thrown at it.

In this communication age where bandwidth is money, the Cyberoam CR25ia achieves better control over which web protocols access the network and how they are allowed to do so. The CR25ia's forte is its load balancing capability.

CIO East Africa gives this product a thumbs up