Unified Threat Management Applicance

Cyberoam CR 25iNG

'NG Series' or next generation series of Cyberoam UTMs when compared with older versions come with gigabyte ports and enhanced processing power, effected through the use of multithreaded software running on multi core processors

— Sandeep Koul

Price: INR 54,990/-

Key Specs: Layer 8 technology, multi-core appliance, multi-threaded application, application firewall

Pros: High on speed and performance

Cons: NA

Write to: pcquest@cybermedia.co.in for more info.

Before we discuss the results of the various tests we conducted to evaluate its performance, let's start by discussing its key features.

It also works as a firewall

It provides deep packet inspection, access control, user authentication, and network and application layer protection. In the web application firewall, you can protect websites and web-based applications from Application Layer (Layer 7) attacks like SQL injection, cross-site scripting (XSS), URL parameter tampering, session hijacking, buffer overflows, etc.

The product can work with Ipv6-based URLs. Its IPS provides protection against DoS attacks, backdoor activity, blended threats, etc while the gateway anti-virus and anti-spyware, lets you withstand viruses, worms and spyware from email protocols (HTTP, FTP, SMTP, POP3, IMAP) and IM traffic.

Provides spam protection

It has Gateway Anti-Spam with signature-less RPD technology that provides spam protection from both inbound as well as outbound spam. With VPN offerings you can have secure and remote connectivity across IPSec, PPTP, L2TP along with SSL VPN.

Supports content filtering

The device monitors indiscriminate surfing with a wideranging URL categorization database that has more than 82 categories. Instant Messenger Management allows archiving and customized security control over Yahoo & Windows Live Messengers. The Application Layer Management feature allows it to manage applications based on user, time and bandwidth to control their availability to users and offer benefits of productivity and cost containment by optimizing bandwidth consumed within the organization.

Side-by-side regular and instant reporting

With a revamped iView reporting tool, it gives inside visibility into all activities for maintaining security, data confidentiality and regulatory compliance. Its bifurcated dashboard provides side-by-side presentation of reports on traffic-related information and security-related alerts.

What's new

The device also provides application based firewalling where a particular application (like p2p applications) can be blocked. A dedicated team at Cyberoam keeps tab on upgrades or modifications to these applications and the UTM appliance is constantly updated to prevent any information leak. Other feature is the presence of a web application firewall and instant messaging control feature.

One also sees the introduction of 'user layer' or 'Layer 8'in the traditional OSI model, a feature that is quite relevant in today's world given increased interest in BYOD. By definition, Cyberoam UTM's Layer 8 Technology treats user identity the 8th layer or the "human layer" in the network protocol stack. This allows administrators to uniquely identify users, control Internet activity of these users on the network, and enable policy-setting and reporting by user name. This in turns ties a user instead of an IP or a MAC address to the policy, which is actually in sync with the BYOD philosophy.

How we tested

Setting up the appliance is fairly simple and you can do it in two modes: bridge and gateway. In our test setup we used the gateway mode. GUI is very simple with well-defined categories. If you want a quick setup, you can do so through a wizard-driven interface, which would configure your device with default settings. For our tests we created a network utilizing just two ports (LAN and WAN). The next important part is to register your product, which would synchronize your device with the Cyberoam servers for effective protection against latest signatures of viruses, spyware, spam, etc. For this, click on 'System>Maintenance> Licensing', and register with your credentials. There is one month free subscription available.

To check if each service is working properly, open the GUI on the dashboard, and under 'License Information' make sure there is an expiry date given in front of subscribed services. The other way around is to click on 'System> Maintenance> Services' from the page. Check if every service you've subscribed to is running properly. Now before we can check anti-virus and anti-spam blocking and reporting capabilities of CR 25iNG, we need to add the required policies. Start with clicking on 'Firewall>Rules.' At the top select 'Select Column' and check the option you want to configure.

To test anti-virus capabilities of this device, we created a Windows machine with Apache web server running on it and then dumped different types of viruses (macros, zipped files, etc). We tried to download these viruses from a machine behind CR 25iNG. For effective scanning and blocking, click on 'ANTI VIRUS>HTTP' (we used http protocol for downloading viruses) and change the scan mode to batch mode. Now while we tried to download viruses we found out that over 80% of those viruses were blocked, plus there was a custom message displayed stating that a particular URL had been blocked as it was harmful.

To test anti-spam capabilities we created a POP3 server using Microsoft Windows Server 2003, and created a test domain with a test user, and dumped spam mail in the mailbox (on the WAN side).

Next, we downloaded these mails from a mail client on the LAN side. But before doing this, we created a few rules by clicking on 'ANTI SPAM>Spam Rules'. Once we downloaded these mails we found that more than 90% of them were scanned and tagged by CR 25iNG. Another important point to note here is that, by default, if the mail size is more than 1 MB it is not scanned. To change the settings, go to 'ANTI SPAM> Configuration'.

Besides checking these capabilities, we also found that CR 25iNG was quite capable of blocking harmful web sites like porn sites. But no matter how good an enterprise class UTM is, it should provide elaborate reports on harmful activities. To check such activities, click on 'LOGS & REPORTS> View Reports.' This would redirect you to 'Cyberoam iVIEW.' Here log in and you can find all the necessary reports in a graphical manner for future analysis and immediate action.

Bottom Line: The NG series of UTMs not only show the old reliability of previous Cyberoam UTMs as far is network security is concerned, but also come with more useful features and faster processing power. □