The IPS continually cleanses the network at layers 2-7, checking both Internet and intranet traffic, eradicating threats and helping to prevent bandwidth hijacking and malicious traffic—spyware, worms, viruses, trojans, phishing attempts, VoIP threats and other harmful activities.

Statistical, protocol and application anomaly protection safeguards the network against traffic surges, buffer overflows and unknown attacks and vulnerabilities (zero-day threats).

To provide protection against new and evolving security threats, updated attack filters are incorporated into Digital Vaccine® Attack Filter Update Services, provided by TippingPoint, which are automatically distributed to all subscribing 3Com X5 and X506 devices, providing pre-emptive protection against new and zero-day vulnerabilities. The Digital Vaccine service offers this protection and prevention on a weekly (or more frequent) basis.
Recommended settings for IPS filters enable preconfigured policies that can automatically and accurately block attacks without any tuning, significantly reducing the time and resources required to protect and maintain a healthy network. This ensures that no “good” traffic is blocked and no “bad”’ traffic is permitted, with no security expertise or fine-tuning of settings required.

ADVANCED VPN CONNECTIONS

While most security implementations do not address security within a VPN connection, 3Com Unified Security platforms take a uniquely comprehensive approach to VPN-based security by providing the ability to look inside VPN IPSec tunnels for threats. This thorough inspection prevents propagation of exploits and other malware between sites and can also be used to provide protection from security risks that occur when laptop users terminate VPN connections while traveling.
Another unique feature is prioritization of bi-directional traffic inside the VPN tunnel, enabling high-quality secure VoIP services and optimizing other site-to-site applications. Threats that once gained access via a VPN tunnel are now eliminated by this unique approach, offering complete security protection, ensuring that remote VPN clients or branch offices cannot be used to propagate threats into the LAN.

APPLICATION PRIORITIZATION AND OPTIMIZATION

Using a single X5 or X506 device for application prioritization and optimization of network traffic, instead of separately managing multiple switches and routers, reduces complexity and cost while providing greater flexibility.

To control the amount of bandwidth allotted to applications and deliver the appropriate quality of service (QoS), 3Com X5 and X506 devices can throttle down non-critical applications such as FTP, and throttle up business-critical and latency-sensitive ones such as VoIP. Bandwidth can be allocated in both inbound and outbound directions for maximum control.

This policy-based traffic-shaping capability helps prevent network congestion, giving administrators a powerful tool for making sure that network services meet user expectations and adhere to the policies set by network managers.

IP MULTICAST WITH VPN

The 3Com X5 and X506 platforms perform the necessary prioritization for real-time applications such as IP telephony and video conferencing with an innovative tunneling approach that secures the traffic in both directions inside and outside VPN tunnels.

FLEXIBLE SECURITY ZONE CONTAINMENT

The flexible architecture of the 3Com X5 and X506 Unified Security Platforms allows the creation of multiple security zones-wired/wireless and student/teacher LANs and DMZs. Traffic between these security zones can then be fully inspected and prioritized using stateful packet inspection for access control and IPS for security control.

STATEFUL PACKET INSPECTION FIREWALL

3Com X5 and X506 platforms are equipped with a stateful packet inspection firewall which provides access control and also recognizes prioritized packet flows and helps maintain QoS. This firewall function replaces router- or switch-based access control lists that can lower performance in those devices.

SECURITY MANAGEMENT SYSTEM

In situations where there are multiple X5, X506 and other 3Com TippingPoint-based devices, the optional 3Com TippingPoint Security Management System (SMS) offers comprehensive management capabilities.

Delivered as a rack-mount appliance, SMS enables administrators to monitor, configure, diagnose and create reports for TippingPoint installations. With SMS, administrators can create IPS and firewall profiles, implement VPNs, manage bandwidth, set content filters and perform other tasks from a central location. SMS

comes with factory-installed software for simple installation, and is the only management system that provides high-availability HA/failover capabilities.

QUARANTINE PROTECTION

Often the most dangerous security threats emanate from within the corporate network. These threats may include worms from traveling laptops and visitor/guest PCs, or installation of unapproved applications such as peer-to-peer file sharing that can carry spyware.

X5 and X506 devices configured with SMS can automatically remove an infected PC from the network, or “move” the PC into quarantine VLAN where it can be safely repaired before being allowed back on the network. Quarantine protection will isolate infected devices from the network without the need for PC software agents, and transparently redirect web requests so users know they are infected or running applications which do not conform to corporate policies.