



## Features, Benefits & Specifications

**Comprehensive Security Solution: Powerful Protection, Simple Installation**

The 3Com® X5 Unified Security Platform delivers unprecedented threat protection for small businesses and organizations with several branch offices or numerous teleworkers— helping prevent business disruptions, revenue loss and damage to an organization's reputation caused by security breaches.

Built on the award-winning 3Com TippingPoint™ Intrusion Protection System (IPS) architecture, the X5 Unified Security Platform combines industry-leading IPS capabilities with virtual private network (VPN) support, stateful packet inspection firewall, application bandwidth management, audio/video IP multicast routing and web content filtering.

This comprehensive security solution safeguards the network from attacks and misuse, and delivers policy-based multisite connectivity for real-time business-critical applications such as Voice over IP (VoIP). High-availability features help ensure wirespeed traffic flow even in the event of network or internal device error or loss of power to the primary device.

A brief description of the many benefits of this solution are provided below. Please download the [data sheet](#) for complete information.

### **Proactive Network Security**

The 3Com X5 device leverages the best-in-class TippingPoint IPS Threat Suppression Engine currently used to protect thousands of enterprise-class networks throughout the world.

The IPS checks 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. Protection is also provided against traffic surges, buffer overflows and unknown attacks and vulnerabilities (zero-day threats).

To protect against new and evolving security threats, updated attack filters are incorporated into Digital Vaccine® Attack Filter Update Services, automatically distributed to all subscribing 3Com X5 devices on a weekly (or more frequent) basis.

### **Advanced VPN Connections**

While most security implementations do not address security within a VPN connection, the 3Com Unified Security platform takes 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. In addition, traffic inside the VPN tunnel can be prioritized, something not available with other solutions.

### **Application Prioritization and Optimization**

Use a single 3Com X5 device, instead of separately managing multiple switches and routers, to control the amount of bandwidth allotted to applications and deliver the appropriate quality of service (QoS).

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

### **IP Multicast with VPN**

The 3Com X5 platform performs 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.

### **Application Blocking and Web Filtering**

The platform enforces usage policies by blocking or rate limiting applications such as instant messaging (IM) and peer-to-peer file sharing that are not essential to business and can waste bandwidth.

3Com offers an optional integrated Web content filter subscription service that limits employee access to objectionable or unacceptable websites that could lower productivity or cause legal problems. This protection is kept current because content is filtered through a continually updated database.

### **Flexible Security Zone Containment**

The flexible architecture of the 3Com X5 Unified Security Platform allows the creation of multiple security zones— wired/wireless and student/teacher LANs and DMZs, for example— for greater IPS and firewall control of resources and networks. 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**

The 3Com X5 platform is 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.

This rack-mount appliance enables administrators to monitor, configure, diagnose and create reports, create IPS and firewall profiles, implement VPNs, manage bandwidth, set content filters and perform other tasks from a central location.

### **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 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.

The 3Com X5 Unified Security Platform offers many more benefits than what is described above. Please download the [data sheet](#) for complete information.

- A brief description of the many benefits of this solution are provided below; see the [data sheet](#) for complete information
- Comprehensive security solution for small businesses, supporting for an unlimited number of users
- Proactive intrusion prevention (IPS) based on award-winning TippingPoint Threat Suppression Engine
- Provides peace of mind by preventing business disruption, loss of revenue and damage to the organization's reputation caused by security breaches
- Continuously cleanses Internet and intranet traffic, eradicating threats and helping to prevent bandwidth hijacking
- Safeguards against traffic surges, buffer overflows, unknown attacks and vulnerabilities (zero-day threats)
- Quarantine protection isolates infected devices from the network without the need for PC software
- No security expertise or fine-tuning of settings is required
- High-speed, low-latency operation does not impact network performance
- Digital Vaccine Attack Filter Update Service automatically delivers new security filters that preemptively protect against new exploits
- Elimination of ad hoc patching and alert responses increases IT productivity and saves management costs
- Advanced VPN capabilities allows the Internet to be used as a secure connectivity mechanism for site-to-site connections and remote user connectivity
- Ability to apply IPS and traffic shaping inside VPN tunnels offers complete security protection and optimization

- Single, high-performance, resilient platform delivers application prioritization and optimization; reduces the number of devices that need to be managed
- Policy-based prioritization ensures QoS for business-critical applications and latency-sensitive services such as VoIP
- Enforce acceptable internet usage by blocking instant messaging (IM), file sharing and streaming applications
- Web content filtering reduces legal liability and security threats related to offensive or harmful Web content
- Flexible security zones and enforcement enables segmentation of the network into multiple zones, allowing greater IPS and firewall control between resources or networks
- See the [data sheet](#) for additional benefits

## Product Specifications

- Download: See the the [X5 and X506 Unified Security Platform data sheet](#) for complete specifications
- Ports: 6 auto-negotiating 10BASE-T/100BASE-TX configured as auto MDI/MDIX; 1 serial (RJ-45)
- Intrusion prevention method: TippingPoint Threat Suppression Engine
- IPS performance: 18 Mbps
- Concurrent IPS sessions: 60,000
- Attack filters: 2,300+ attack filters protecting against spyware, worms, viruses, trojans, phishing, VoIP threats, DoS, P2P, IM
- Attack filter updates: automatically distributed to all subscribing 3Com X5 devices through Digital Vaccine Attack Filter Update Service (see "*Please Note*", #1)
- Quarantine: isolates infected devices from the network without the need for PC software
- Firewall performance: 50 Mbps
- Firewall policies: 100
- Firewall security zones: 16
- VPN performance (168-bit DES): 40 Mbps
- Concurrent VPN client sessions: 128
- VPN encryption:: DES, 3DES, AES128, AES-192, AES-256
- VPN client support: native IPSec, L2TP/IPSec, PPTP/MPPE
- Web content filtering: 15+ million URLs filtered; 40 categories; custom URL black/white lists; onbox SurfControl subscription service (see "*Please Note*", #1)
- Traffic shaping: Inbound and outbound rate limiting; policy-based shaping; traffic shaping can be done inside VPN tunnels
- Security: RADIUS server and local database authentication; SNMP v1, 2 and 3
- Management: Web interface via HTTPS; command line interface via console, telnet, SSH; TippingPoint Security Management System (SMS) support
- Dimensions and weight: height: 4.3 cm (1.7 in); width: 29.5 cm (11.6 in); depth: 17.5 cm (6.9 in); weight: 1.1 kg (2.5 lb)
- More specifications: See the the [X5 and X506 Unified Security Platform data sheet](#) for complete specifications