3Com® X5 and X506 Unified Security Platforms

DATA SHEET

Enterprise-class unified security platform with best-of-breed performance, ideally suited for distributed Secure Converged Networks

OVERVIEW

Organizations of all sizes are having their networks attacked at an unprecedented rate. Attacks can be in the form of network outages; they can claim valuable bandwidth from productivity applications like Voice over IP (VoIP); they may even perpetrate the theft of company data and the personal and financial information of employees and customers.

Internal abuse of network resources—unauthorized file sharing, visiting inappropriate web sites, pervasive instant messaging—adds to the problem, resulting in an expanding threat environment which, left ignored, seriously impacts the delivery of information and services to customers, affecting the business's profitability.

Because of these attacks and abuses, businesses need comprehensive network protection along with multi-zone functionality allowing granular segmentation for better control over security policies and network traffic. Solutions up to now have included various security appliances that were not integrated and did not provide a single means of management.

3Com® X5 and X506 Unified Security Platforms deliver unprecedented threat protection for organizations with a single site, multiple branch offices, or remote workers—helping prevent business disruptions, revenue loss and damage to an organization's reputation caused by security breaches.

Built on best-of-breed services, including the award-winning 3Com TippingPoint® Intrusion Protection System (IPS) architecture, the X5 and X506 Unified Security Platforms combine industry-leading IPS capabilities with virtual private network (VPN) support, stateful packet inspection firewall, application bandwidth management, audio/video IP multicast routing, anti-spam 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. 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.

from left: 3Com X5 and X506 Unified Security Platforms

KEY BENEFITS

PROACTIVE NETWORK SECURITY

The 3Com X5 and X506 devices leverage the best-in-class TippingPoint IPS Threat Suppression Engine currently used to protect thousands of enterprise networks throughout the world.

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 ensure 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. 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.

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.

APPLICATION PRIORITIZATION AND OPTIMIZATION

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 for both inbound and outbound directions, both inside and outside VPN tunnels, to maximize 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.

APPLICATION BLOCKING AND WEB FILTERING

The platforms enforce 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.

Web filter policies can be customized to the site requirements, enforcing different access at a security zone or group/user basis. Advanced integration with directory services such as Windows Active Directory and Novell eDirectory allow fine grain per-user control.

KEY BENEFITS (CONTINUED)

SPAM EMAIL FILTERING

Unsolicited spam now comprises over 80% of all email traffic. Organizations continue to react with tactical fixes, but deterioration in the quality of service for valid network traffic remains. Email filtering in 3Com X5 and X506 platforms uses the best-of-breed GlobalView™ Mail Reputation Service, from Commtouch®, to fight spam and email-borne malware at the perimeter. The solution has been proven to reduce up to 80% of incoming spam email at the network entry-point, while providing the industry's lowest rate of false positives.

GlobalView offers a unique breadth of coverage, analysis and delivery of information in real-time. It utilizes global detection centers that analyze hundreds of millions of messages per day, providing visibility into network traffic in every location, globally. This critical mass of data is analyzed using patented technology, enabling the delivery of real-time classification for the source of each email received. In real time, the service determines if a particular address is sending spam and/or legitimate email, and if it has been compromised. These capabilities enable the solution to react to distributed spam attacks the moment they start.

IP MULTICAST WITH VPN

X5 and X506 devices enable organizations to deliver next-generation services such as distance learning, real-time training, and multimedia conferencing across the network using IP multicast in conjunction with VPN—two technologies which up until now have been mutually exclusive. Prioritized traffic shaping within a VPN tunnel can provide cost savings on long distance phone calls and leverages centralized business applications.

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, 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.

Security zone flexibility also extends to remote access users, who can have their VPN connection terminated to a specific zone, based on their identity, thanks to integration with authentication directory services. This capability enables flexible integration with network access control (NAC) products.

STATEFUL PACKET INSPECTION FIREWALL

3Com X5 and X506 platforms are equipped with a fully ICSA-certified stateful packet inspection firewall which provides access control and also recognizes prioritized packet flows and helps maintain QoS. Granular firewall rules allow the control of traffic down to an individual IP address, and fine-grain control of all security services.

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 and X506, as well as TippingPoint, security 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. With SMS, administrators can create IPS and firewall profiles, implement VPNs, manage bandwidth, setup web 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 device from the network, or "move" it to a quarantine VLAN where it can be safely repaired before being allowed back on the network. Quarantine protection isolates infected devices from the network without the need for client software, and transparently redirects web requests so users know they are infected or running applications which do not conform to corporate policies. Used in conjunction with network access control, this enables a fully-rounded pre- and post-access control solution.

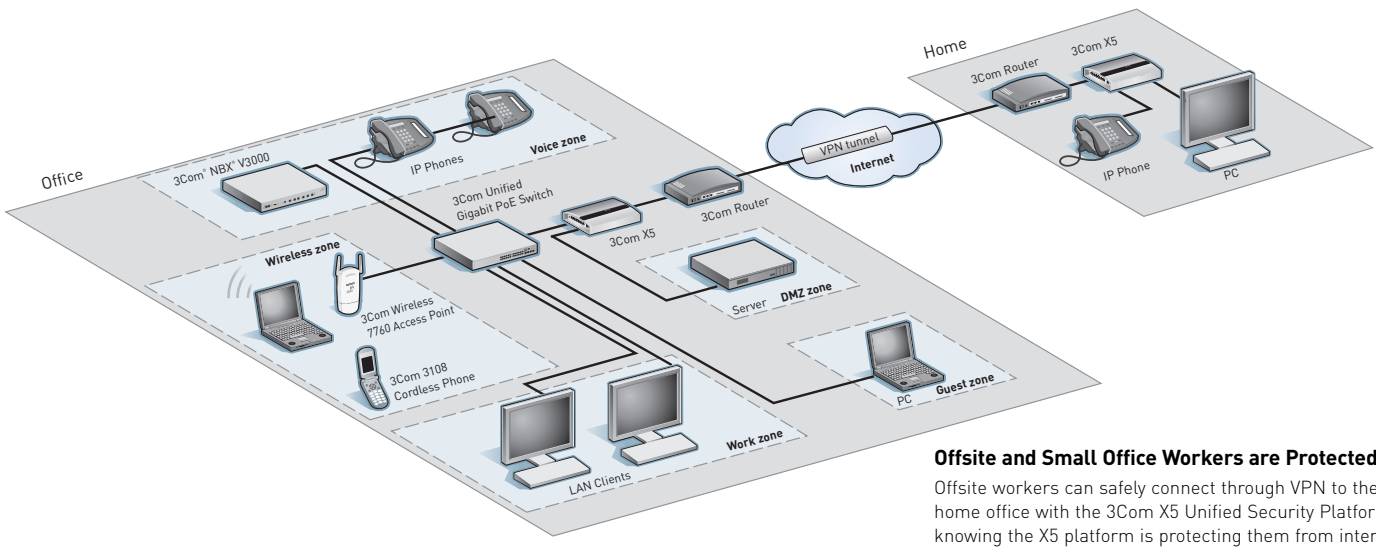
FEATURES HIGHLIGHTS

Feature	Description
PROACTIVE INTRUSION PREVENTION	
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.
Packet flow inspection for Layer 2 through Layer 7	Continuously cleanses Internet and intranet traffic, eradicating threats and helping to prevent bandwidth hijacking.
Statistical, protocol and application anomaly protection	Safeguards against traffic surges, buffer overflows, unknown attacks and unknown vulnerabilities (zero-day threats).
Quarantine protection	Isolates infected devices from the network without the need for client software; transparently redirects web requests so users know they are infected or running applications which do not conform to corporate policies.
Digital Vaccine Attack Filter Update Service	Automatically delivers new security filters that preemptively protect against new exploits; offers updated protection and prevention on a weekly (or more frequent) basis.
Recommended settings supplied with IPS filters in Digital Vaccine	Ensures that no "good" traffic is blocked and no "bad" traffic is permitted; no security expertise or fine-tuning of settings is required.
Traffic normalization	Eliminates malformed or illegal packets and performs TCP reassembly and IP defragmentation to increase bandwidth and detect evasions.
Elimination of ad hoc patching and alert responses	Increases IT productivity and saves management costs; continuously shields the network from application and infrastructure exploits while patches are being deployed.
ADVANCED VPN	
High-performance, low-latency IPSec VPN	Allows the Internet to be used as a secure connectivity mechanism for site-to-site connections and remote user connectivity.
Ability to apply IPS inside VPN tunnels	Offers complete security protection, ensuring that remote VPN clients or branch offices cannot be used to propagate threats into the LAN.
Terminate VPNs to different zones	Allows security policy to be controlled on a per user or per group basis and enables integration with network access control solutions to extend policy control to remote access users.
APPLICATION PRIORITIZATION AND OPTIMIZATION	
Single, high-performance, resilient platform	Reduces the number of devices that need to be managed and saves management costs; provides greater flexibility by integrating multiple functions (e.g., IPS in VPN tunnels).
Policy-based prioritization	Ensures QoS for business-critical applications and latency-sensitive services such as VoIP; makes sure network traffic adheres to policies set by management; improves users' productivity.
SIP/H323 application layer gateway and stateful traffic shaping	Provides ability to identify, prioritize and protect mission-critical applications, such as VoIP.
Traffic shaping inside VPN tunnels	Prioritizes site-to-site voice traffic across VPN tunnels, saving costs on long-distance phone calls and leveraging centralized business applications.
Support for PIM-DM multicast routing between sites over IPSec VPN	Enables next-generation applications such as distance-based learning, real-time training and conferencing and, at the same time, helps to preserve precious WAN bandwidth

FEATURES HIGHLIGHTS (CONTINUED)

Feature	Description
ENFORCE ACCEPTABLE INTERNET USAGE	
Block instant messages (IM), streaming applications	Improves employee productivity and preserves bandwidth by restricting peer-to-peer file sharing and access to unauthorized applications.
Web content filtering	Restricts access to non-business content, boosting employee productivity; helps reduce legal liability and security threats related to offensive or harmful web content.
Anti-Spam filtering	Stops unwanted email from reaching inboxes, improving employee productivity; helps reduce legal liability, security threats and the strain on IT infrastructure related to unsolicited emails containing offensive content, viruses or phishing attacks. As Spam is stopped at the connection layer, before it enters the network, LAN and WAN bandwidth and e-mail server resource requirements are significantly reduced.
Layer 4 through Layer 7 rate limiting	Provides the ability to limit the data rate of applications like IM and streaming video to maximize WAN bandwidth.
FLEXIBLE SECURITY ZONE CONTAINMENT	
Support for multiple DMZs	Lets administrators deploy one or more DMZs for greater security of publicly available resources.
Flexible security zones and enforcement	Enables segmentation of the network into multiple zones, allowing greater IPS and firewall control between resources or networks; allows creation of wired/wireless, student/teacher, and similar networks, for both local and remote access users.
Inter-LAN firewall and IPS	Allows segmentation and inspection between IEEE 802.1Q VLAN tagged networks.
Intrinsic high-availability and stateful network redundancy modes	Helps ensure maximum uptime and availability.
NETWORK TRANSPARENCY	
Seamless deployment	No IP or MAC address—and no changes needed to network configuration—simplifies installation, saves time, and helps eliminate the risk of hackers discovering devices on the network.
ENTERPRISE-CLASS HIGH AVAILABILITY	
Dual-box failover	Protects against loss of connectivity due to hardware failure, with automatic configuration synchronization to simplify administration and remove scope for errors.
Dual-WAN failover	Helps prevent loss of connectivity due to ISP WAN link failure.
Dual-WAN load-balancing	Enables increased WAN bandwidth for remote sites with the added benefit of protection against loss of connectivity due to ISP WAN Link failure.

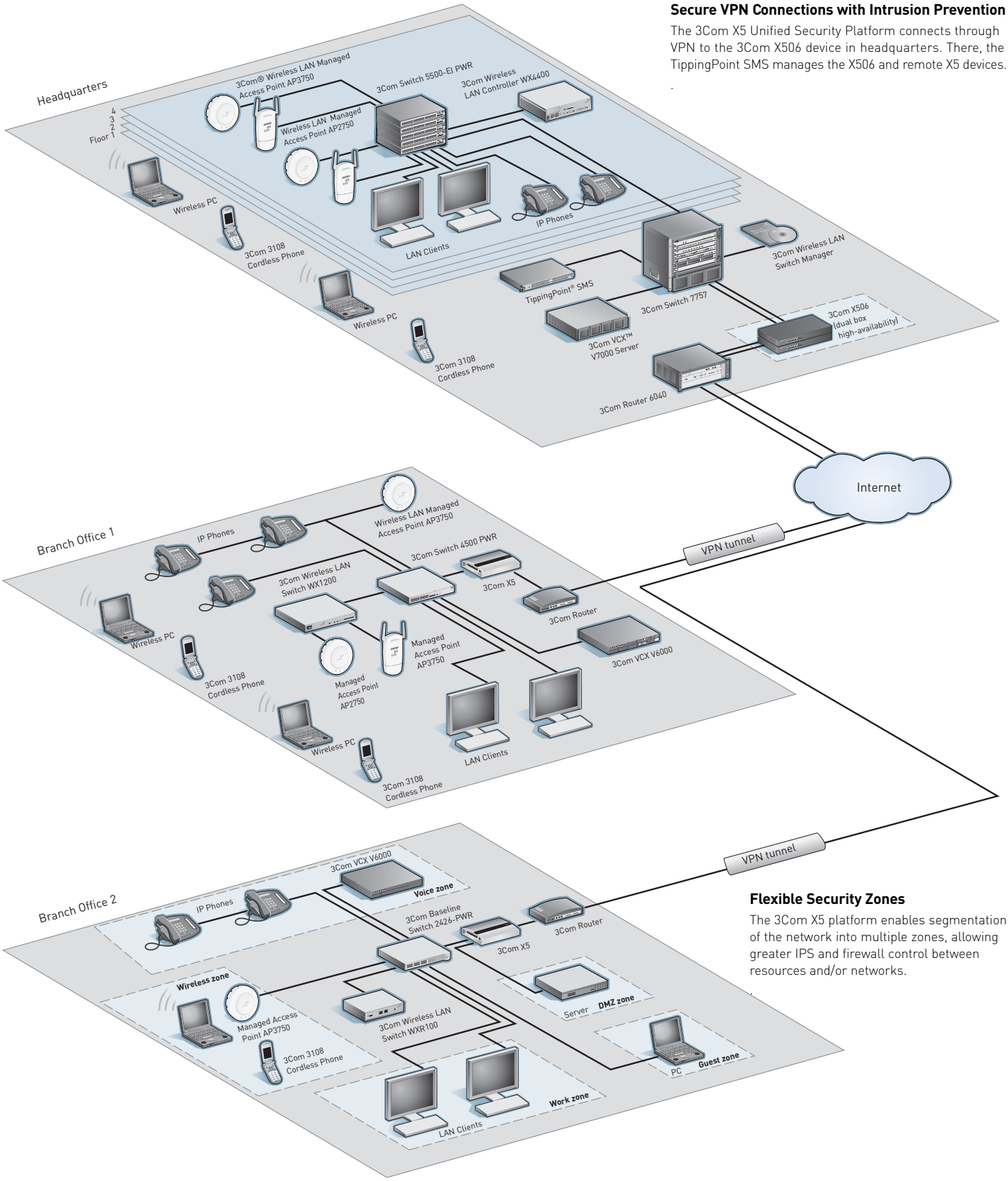
3COM X5 UNIFIED SECURITY PLATFORM: SMALL OFFICE AND TELEWORKER APPLICATION



Offsite and Small Office Workers are Protected

Offsite workers can safely connect through VPN to the home office with the 3Com X5 Unified Security Platform, knowing the X5 platform is protecting them from internet and intranet threats. At the office, the X5 device segments the network into multiple zones, allowing greater IPS and firewall control.

3COM X5 AND X506 UNIFIED SECURITY PLATFORMS: BRANCH OFFICE APPLICATION



Secure VPN Connections with Intrusion Prevention

The 3Com X5 Unified Security Platform connects through VPN to the 3Com X506 device in headquarters. There, the TippingPoint SMS manages the X506 and remote X5 devices.

.

Flexible Security Zones

The 3Com X5 platform enables segmentation of the network into multiple zones, allowing greater IPS and firewall control between resources and/or networks.

.

SPECIFICATIONS

Information in this section is relevant to all versions of the 3Com X5 and X506 Unified Security Platforms, unless stated otherwise.

CONNECTORS
6 auto-negotiating 10BASE-T/100BASE-TX configured as auto MDI/MDIX

1 serial (RJ-45)

CONCURRENT SESSIONS
3Com X5 (25 user license): 20,000

3Com X5 (unlimited license): 60,000

3Com X506 (unlimited license): 128,000

INTRUSION PREVENTION
TippingPoint Threat Suppression Engine

IPS performance:
- X5: 20 Mbps
- X506: 60 Mbps

Automated Digital Vaccine Attack Filter Update Service‡ by TippingPoint

Recommended settings for Intrusion Prevention System (IPS) filters

Zero-day filters

Level 4–7 rate limiting

Automatic quarantine

2,300+ attack filters protecting against spyware, worms, viruses, trojans, phishing, VoIP threats, DoS, P2P, IM

FIREWALL
Firewall performance:
- X5: 70 Mbps
- X506: 100 Mbps

Firewall policies:
- X5 (25 user): 50
- X5 (unlimited user): 100
- X506: 500

Security zones:
- X5: 16
- X506: 32

Virtual servers:
- X5: 25
- X506: 100

Time-based schedules

User authentication

VIRTUAL PRIVATE NETWORK (VPN)
VPN performance (168-bit DES):
- X5: 40 Mbps
- X506: 95 Mbps

Concurrent VPN client sessions:
- X5 (25 user): 50
- X5 (unlimited user): 128
- X506: 1,000

Security Associations:
- X5: 50
- X506: 512

Keying modes: manual key, IKE-PSK, IKE-X509

Encryption: DES, 3DES, AES128, AES-192, AES-256

VPN client support: native IPSec, L2TP/IPSec, PPTP/MPPE

User-based zone-specific VPN termination via LDAP

WEB CONTENT FILTERING
Annual subscription service*:
- Provider: WebSense; onbox subscription service*
- URLs filtered: 15+ million*
- Content filter categories: 40*

Custom URL black/white lists

User-based content filtering via LDAP

Keyword, wildcard, regular URL matching

ANTI-SPAM†
GlobalView Mail Reputation Service

Automated SMTP email Spam rating service

Greater than 80% detection rate

Industry's lowest false positives

TRAFFIC SHAPING
Inbound and outbound rate limiting

Policy-based shaping

Traffic shaping inside VPN tunnels

NETWORKING
Deployment modes: IP transparent, route, NAT

IP router interfaces:
- X5: 6
- X506: 32

IP address groups:
- X5: 25
- X506: 200

Static routes:
- X5: 100
- X506: 500

Dynamic routing RIP v1 and 2, OSPF v2 including NSSA

OSPF routes:
- X5: 50,000
- X506: 200,000

PPPoE, L2TP, PPTP IP assignment

DHCP client

IEEE 802.1Q VLAN support

Internal multi-scope DHCP server

DHCP relay over VPN

GRE tunneling

IP multicast routing PIM-DM

IGMP v1 and 2

HIGH AVAILABILITY
Dual-box active-standby pair

Dual-box automatic configuration synchronization

Dual WAN links in active-standby fail-over pair

Dual WAN links in active-active load-balancing pair

Primary and secondary VPN peers

Configurable load-balancing

SYSTEM AND ADMINISTRATION
Web interface via HTTPS

Command line interface via console, telnet, SSH

TippingPoint Security Management System (SMS) support

RADIUS server and local database authentication

DNS support for dynamic IP allocation

Configuration snapshot and restore

Software upgrade via web interface or SMS

Software rollback

SNMP v1, 2 and 3; SNMP Enterprise MIB

Fully-integrated AdventNet Firewall Analyzer support

DIMENSIONS
X5

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)

X506

Height: 4.3 cm (1.7 in)

Width: 44.5 cm (17.5 in)

Depth: 30.5 cm (12.0 in)

Weight: 4.1 kg (9.0 lb)

POWER SUPPLY
X5

100-240 VAC auto-ranging, 50/60 Hz

Current rating: 0.8-1.2 Amps, max

Power consumption: 30 W, max

X506

100-240 VAC auto-ranging, 50/60 Hz

Current rating: 1-2 Amps, max

Power consumption: 50 W, max

ENVIRONMENTAL REQUIREMENTS
Operating temperature: 0° to 40°C (32° to 104°F)

Storage temperature: -20° to 80°C (-4° to 176°F)

Humidity: 5% to 95% non-condensing

RELIABILITY
(MTBF @25°C)

X5: 22 years (193,000 hours)

X506: 13 years (115,000 hours)

EMISSIONS / AGENCY APPROVALS
FCC Part 15 Class B

EN 55022 Class B

ICES-003 Class B

VCCI Class B

EN 61000-3-2

EN 61000-3-3

IMMUNITY
Product conforms to EN 55024

SAFETY AGENCY CERTIFICATIONS
UL 60950-1

IEC 60950-1

EN 60950-1

CAN/CSA-C22.2 No. 60950-1-03

STANDARDS AND PROTOCOLS
IEEE standards

IEEE 802.1Q (VLANs)

IEEE 802.3 Ethernet

IEEE 802.3i (10BASE-T)

IEEE 802.3u (Fast Ethernet)

RFC standards

RFC 0768 (User Datagram Protocol)

RFC 0791 (Internet Protocol)

RFC 792, 950, 1256 (Internet Control Message Protocol)

RFC 0793 (Transmission Control Protocol)

RFC 1157 (Simple Network Management Protocol)

RFC 1213 (Management Information Base for Network Management of TCP/IP-based internets: MIB-II)

RFC 1722, 2082, 2453 (RIP)

RFC 2131 (DHCP)

RFC 2236 (IGMP)

RFC 2403 (Use of HMAC-MD5-96 within ESP and AH)

RFC 2404 (Use of HMAC-SHA-1-96 within ESP and AH)

RFC 2405 (ESP DES-CBC Cipher Algorithm With Explicit IV)

RFC 2410 (NULL Encryption Algorithm and Its Use With IPsec)

RFC 2516 (PPPoE)

RFC 2541 (ESP CBC-Mode Cipher Algorithms)

RFC 2637 (PPTP)

RFC 2661 (L2TP)

RFC 2784 (Generic Routing Encapsulation)

RFC 3022 (Network Address Translation)

RFC 3164 (Syslog)

RFC 3193 (Securing L2TP using IPsec)

RFC 3261 (SIP)

RFC 3947 (Negotiation of NAT-Traversal in the IKE)

RFC 3948 (UDP Encapsulation of IPsec ESP Packets)

RFC 3973 (PIM-DM)

RFC 4109 (Algorithms for Internet Key Exchange version 1)

RFC 4301 (Security Architecture for the Internet Protocol)

RFC 4302 (IP Authentication Header)

RFC 4303 (IP Encapsulating Security Payload)

PACKAGE CONTENTS
X5

3Com X5 Unified Security Platform

Power adapter

X506

3Com X506 Unified Security Platform

Power cord

WARRANTY
One Year Limited Hardware Warranty

Limited Software Warranty for 90 days

90 days free technical support

Refer to **www.3com.com/warranty** for details.

‡ 1 year of updates included with purchase of device; purchase additional licenses to extend protection

* 30-day trial included; requires purchase of content filter license for continued protection

† 30-day trial included; requires purchase of anti-Spam filter license for continued protection

ORDERING INFORMATION

PRODUCT DESCRIPTION	3COM SKU
3Com X5 Unified Security Platform *(25-user license; includes one year of Digital Vaccine updates)*	3CRX5DV-25-96
3Com X5 Unified Security Platform *(unrestricted user license; includes one year of Digital Vaccine updates)*	3CRX5DV-U-96
3Com X506 Unified Security Platform *(unrestricted user license; includes one year of Digital Vaccine updates)*	3CRX506DV-96
Product Options	
3Com X5 Digital Vaccine Attack Filter Update Service *(One year of Digital Vaccine IPS updates)*	3CX5-DV-E
3Com X506 Digital Vaccine Attack Filter Update Service *(One year of Digital Vaccine IPS updates)*	3CX506-DV-E
3Com X5 25-User to Unrestricted User Upgrade License *(Upgrades 3CRTPX5-25-96 to support unrestricted users)*	3CX5-25UPGU-E
3Com X5 Anti-Spam Filter Update Service *(One year of anti-Spam filtering)*	3CX5-AS-E
3Com X506 Anti-Spam Filter Update Service *(One year of anti-Spam filtering)*	3CX506-AS-E
3Com X5 Content Filter Update Service *(One year of Web content classification and filtering)*	3CX5-CF-E
3Com X506 Content Filter Update Service *(One year of Web content classification and filtering)*	3CX506-CF-E
3Com Global Services	
3Com Network Health Check, Installation Services, and Maintenance	www.3com.com/services_quote
3Com University Courses	www.3com.com/3comu

Visit www.3com.com for more information about 3Com secure converged network solutions.

3Com Corporation, Corporate Headquarters, 350 Campus Drive, Marlborough, MA 01752-3064
3Com is publicly traded on NASDAQ under the symbol COMS.

401013-008 06/08