

Comprehensive solution with a performance and price point making it affordable for branch offices to have best-of-breed enterprise-class security

OVERVIEW

Companies of all sizes are being attacked at an unprecedented rate. Most attacks are deliberate, but non-intentional ones do occur. They are, however, always serious and can be disastrous. Attacks can be in the form of network outages, they can claim valuable bandwidth from productivity applications and in some instances even perpetrate the theft of company or personal information from unwilling individuals.

Because of these attacks, networks today require 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 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 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 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.



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-class 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 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.

KEY BENEFITS (CONTINUED)

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.

Organizations can use this capability to deliver next-generation services such as distance learning and multi-media 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.

Support for Protocol Independent Multicast - Dense Mode (PIM-DM) routing between sites over an IPSec VPN enables next generation applications such as distance-based learning and real-time training and conferencing to be realized.

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.

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.

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.

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	Isolate infected devices from the network without the need for PC software agents; transparently redirect web requests so users know they are infected or running applications which do not conform to corporate policies.
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.
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.
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.

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 and prioritize mission-critical VoIP applications.
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

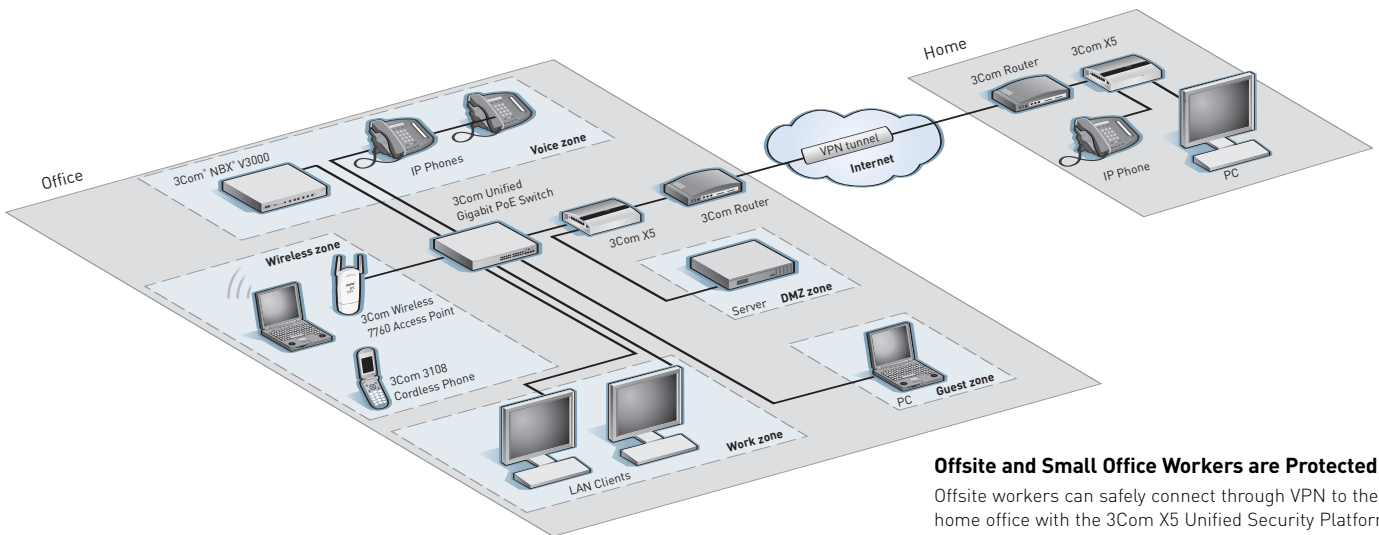
ENFORCE ACCEPTABLE INTERNET USAGE

Block instant messages (IM), peer-to-peer file sharing and streaming applications	Improves employee productivity and preserves bandwidth by restricting access to unauthorized applications.
Web content filtering	Reduces legal liability and security threats related to offensive or harmful Web content; boosts employee productivity by restricting access to non business content.
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.

FEATURES HIGHLIGHTS
(CONTINUED)

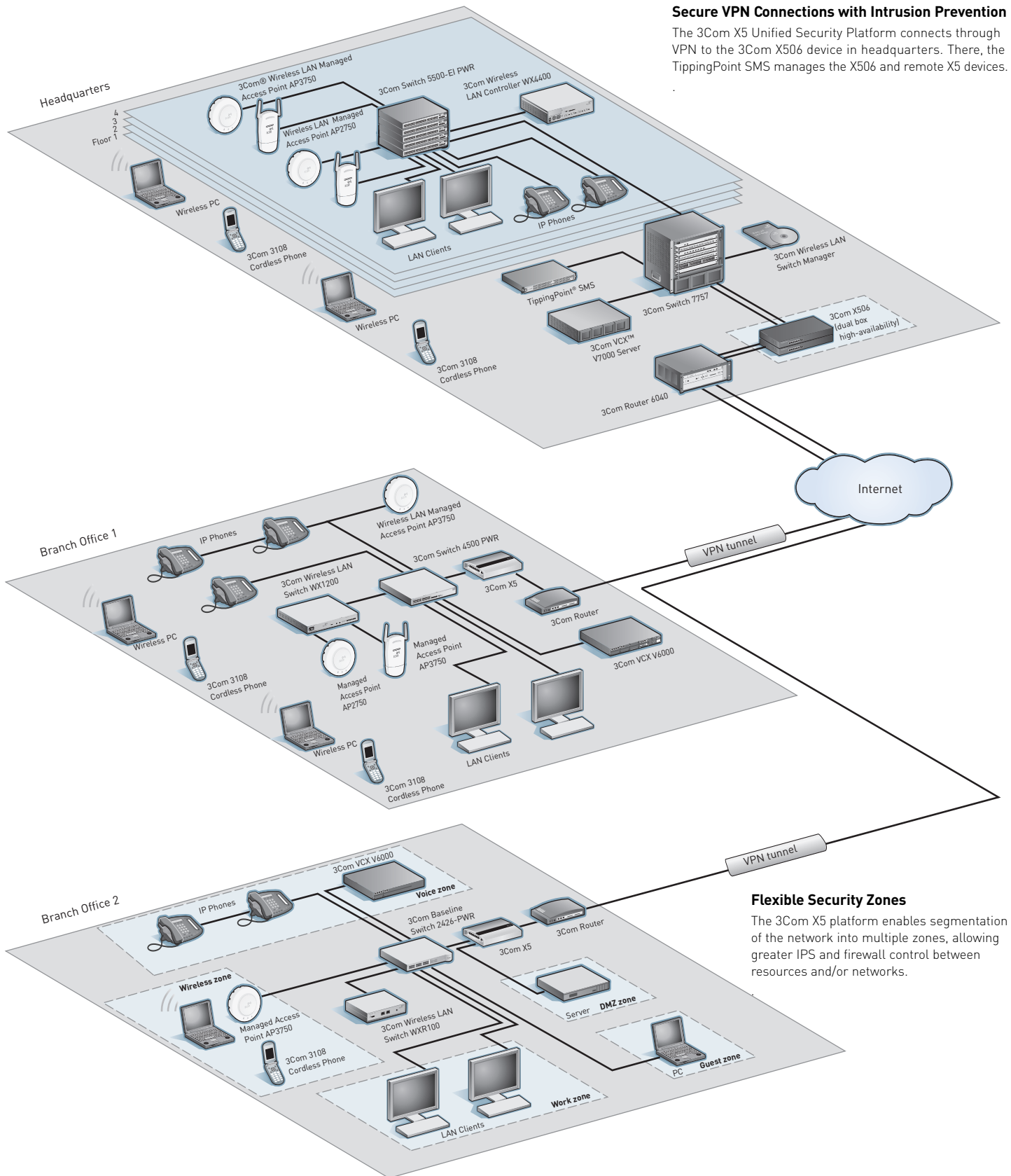
Feature	Description
FLEXIBLE SECURITY ZONE CONTAINMENT	
Support for multiple DMZs	Lets administrators deploy one or more DMZs for greater security of publicly available resources.
Flexible security zones and enforcement	Enables segmentation of the network into multiple zones, allowing greater IPS and firewall control between resources or networks; allows creation of wired/wireless, student/teacher, and similar networks.
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 and saves time; eliminates the risk of hackers discovering devices on the network.
High-speed, low-latency operation	Enables devices to be deployed without impacting performance; delivers high-quality convergence services.

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: 18 Mbps
- X506: 50 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: 50 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

WEB CONTENT FILTERING

URLs filtered: 15+ million

Content filter categories: 40

Custom URL black/white lists

Keyword, wildcard, regular expression
URL matching

Provider: SurfControl; onbox
subscription service*

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: 6

IP address groups:

- X5: 25
- X506: 200

Static routes:

- X5: 100
- X506: 500

PPPoE, L2TP, PPTP IP assignment

DHCP client

IEEE 802.1Q VLAN support

Internal multi-scope DHCP server

DHCP relay over VPN

GRE tunneling

Dynamic routing RIP v1 and 2

IP multicast routing PIM-DM

IGMP v1 and 2

SYSTEM AND ADMINISTRATION

Dual-box high availability

Web interface via HTTPS

Command line interface via console,
telnet, SSH

TippingPoint Security Management
System (SMS) support

RADIUS server and local database
authentication

Configuration snapshot and restore

Software upgrade via Web interface
or SMS

Software rollback

SNMP v1, 2 and 3; SNMP Enterprise
MIB

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

IEEE STANDARDS SUPPORTED

IEEE 802.1Q (VLANs)

IEEE 802.3 Ethernet

IEEE 802.3i (10BASE-T)

IEEE 802.3u (Fast Ethernet)

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

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

* 14-day trial included with purchase of X5 and X506

ORDERING INFORMATION



PRODUCT DESCRIPTION

	3COM SKU
3Com X5 Unified Security Platform <i>(25-user license)</i>	3CRTPX5-25-96
3Com X5 Unified Security Platform <i>(unlimited user license)</i>	3CRTPX5-U-96
3Com X506 Unified Security Platform <i>(unlimited user license)</i>	3CRX506-96

Product Options

3Com X5 Digital Vaccine Gold Attack Filter Update Service <i>(One year of Digital Vaccine IPS updates, web content filtering, telephone technical support, advance hardware replacement and software updates)</i>	3CTPX5-DVGOLD
3Com X506 Digital Vaccine Gold Attack Filter Update Service <i>(One year of Digital Vaccine IPS updates, web content filtering, telephone technical support, advance hardware replacement and software updates)</i>	3CX500-DVGOLD
3Com X5 Digital Vaccine Attack Filter Update Service with Support <i>(One year of Digital Vaccine IPS updates, telephone technical support, advance hardware replacement and software updates)</i>	3CTPX5-DV
3Com X506 Digital Vaccine Attack Filter Update Service with Support <i>(One year of Digital Vaccine IPS updates, telephone technical support, advance hardware replacement and software updates)</i>	3CX500-DV

3Com Global Services

3Com Network Health Check and Installation Services	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.

Copyright © 2007 3Com Corporation. All rights reserved. 3Com, the 3Com logo, and Digital Vaccine are registered trademarks, and TippingPoint is a trademark of 3Com Corporation or one of its subsidiaries. All other company and product names may be trademarks of their respective companies. While every effort is made to ensure the information given is accurate, 3Com does not accept liability for any errors or mistakes which may arise. All specifications are subject to change without notice.

401013-005 04/07

