

TippingPoint 200E Intrusion Prevention System

DATASHEET



Switch-Like Performance

- 200 Mbps Attack Filtering
- Typical Latency < 1 millisecond
- Real World TCP/UDP Traffic Mix
- 500,000 Simultaneous Sessions
 - TCP/UDP/ICMP
- 8,000+ Connections Per Second

Client and Server Protection

- Prevent Attacks on Vulnerable Applications and Operating Systems
- Eliminate Costly Ad-Hoc Patching
- Multiple Inspection Methods

Network Infrastructure Protection

- Protect Cisco IOS, DNS and Other Infrastructure
- Protect Against Traffic Anomaly and DoS
- Access Control Lists

Advanced DDoS Protection

- 450,000+ SYNs Per Second
- SYN Proxy
- SYN Flood
- Established Connection Flood
- Connection Per Second Flood

Advanced Threat Prevention

- VoIP
 - Phishing
- OS Vulnerabilities
 - DDoS
- Worms
 - P2P
- Spyware
 - Viruses
- Quarantine
 - ZDI

Application Performance Protection

- Increase Bandwidth, Router and Server Capacity
- Rate-Limit or Block Unwanted Traffic
 - Peer-to-Peer/Instant Messaging
 - Normalize Invalid Network Traffic

Digital Vaccine™ Real-Time Inoculation

- Protection Against Zero-Day Attacks
- Protection Against Undisclosed ZDI Vulnerabilities
- Automatic Distribution of Latest Filters

Dimensions

- 19" rack mountable
- Height: 2.0 in (51mm)
- Width: 17.25 in (438mm)
- Depth: 12.0 in (305mm)
- Weight: 12.7 lbs (5.8kg)

The Platform For Unrivaled Security and Performance

Protection has never been more powerful. TippingPoint is the industry's leading Intrusion Prevention System (IPS), unrivaled in security, performance, high availability and ease-of-use. As the only Intrusion Prevention System to receive the NSS Gold Award and Common Criteria certification, among many other awards, TippingPoint is the defining benchmark for network-based intrusion prevention.

Proactive Network Security

Organizations face an increasing challenge of securing their internal networks and remote offices. Organizations also face the monumental task of providing sufficient network speeds to retain high levels of productivity. With the TippingPoint IPS operating in-line in the network, malicious and unwanted traffic is blocked, while legitimate traffic passes unimpeded. TippingPoint optimizes network performance by continually cleansing the network and prioritizing applications that are mission critical. TippingPoint's high performance and extraordinary intrusion prevention accuracy have redefined network security, and fundamentally changed the way people protect their organization.

TippingPoint significantly reduces the amount of time and resources needed to maintain a healthy network. State of the art "Recommended Settings" allow instant deployment out-of-the-box with no tuning required. It is no longer necessary to clean up after cyber attacks. TippingPoint's vulnerability filters eliminate the need for ad-hoc and emergency patching. The Digital Vaccine Service ensures evergreen protection against emerging threats. TippingPoint's bandwidth management capabilities stop rogue applications like Peer-to-Peer and Instant Messaging from running rampant throughout the network.

Unparalleled Performance and Economics

TippingPoint is the best performing IPS in the industry. Traditional software and

appliance solutions are simply unable to perform without degrading network performance. The extremely high speed and low latency capabilities of the TippingPoint IPS enable deployment at the network edge or core, protecting from external as well as internal threats. TippingPoint enables traffic shaping to support critical applications and infrastructure, as well as provides attack isolation and network discovery of vulnerable devices. TippingPoint offers organizations the benefits of a comprehensive security solution at a competitive price.

Advanced Denial of Service Protection

TippingPoint's Advanced DDoS Protection utilizes a state-of-the-art hybrid approach with a combination of anomaly filters, SYN proxy, rate shaping, and statistical techniques. TippingPoint controls the number of new connection requests and established connections to limit the total number of connections and connection rates. This allows legitimate clients full access to protected resources while preventing attackers from flooding a server. TippingPoint also performs IP filtering to block attacks from malicious or spoofed IP addresses by validating the legitimacy of the packet and source before allowing the connection request to proceed. TippingPoint's security filters are able to block anomalous traffic that does not conform to normal traffic guidelines.

