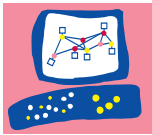


I-on-X Quick Guide

SECURED BY



CHECK POINT™

InterSpect

scan, block and quarantine for interior networks



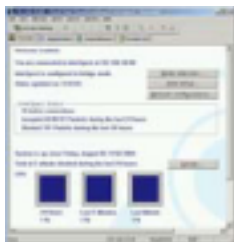
X45

up to 16 GE and 4000 VLANs



X80

up to 32 GE or 64 FE and 4000 VLANs



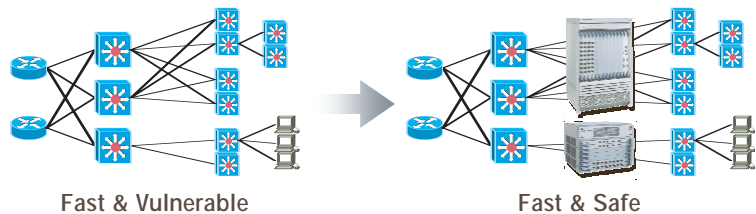
Management

simple policy administration and monitoring

InterSpect-on-X: Protecting the Core of Your Network

MONITORING THE INTERNAL NETWORK UNDER ATTACK Worms and viruses that spread inside corporate LANs cost more than any other type of attack. No complex mathematics are required to understand the numbers. Just multiply the number of compromised PCs by the time and dollars it takes your IT staff to clean and rebuild each one after a successful attack. In the case of attacks like Nachi/Welchia, the cost is greater still because they overwhelm network resources. Now the business can no longer operate effectively. This problem becomes exponentially worse for large networks: the larger the network, the more PCs, the greater the damage. Preventing this damage has become the number one issue for network security managers around the world.

BUT IS YOUR NETWORK DESIGNED FOR THE NETWORK UNDER ATTACK? In the words of Forrester Research, network managers are paid "to deliver bits, not to block them." The most popular architecture to "deliver bits" has been the three tier architecture of "Core Router – Distribution Switch – Access Switch" because it provides good throughput and port density cost effectively. It delivers bits fast. It also delivers attacks fast. Worms spread especially quickly on flat Layer 2 networks because there is nothing in the way to stop them. Even on a Layer 3 network, the network is neither secure nor scalable under attack. For instance, at the core router tier where Layer 3 operates, worms cause hundred and thousand-fold increases in the workgroup-to-workgroup routing being performed by the core routers. This is when "core meltdowns" occur. The routers can't keep up with these huge spikes in traffic.



CHECK POINT INTERSPECT ON CROSSBEAM X-SERIES PLATFORMS To address this problem, Check Point and Crossbeam Systems have partnered to offer InterSpect, Check Point's market-leading interior security technology, on Crossbeam X-Series security switches. The result is cost-effective, bulletproof segmentation and quarantining that delivers bits fast and blocks attacks fast. The InterSpect-on-X solution provides a single hardware device that seamlessly integrates at core, distribution or access layers. Its high port density allows many separate network segments to be protected and it can operate in bridge or switch mode for minimal to no network reconfiguration. InterSpect-on-X offers the highest scaling and highest availability solutions for interior network protection.

Deployment Architectures

Features

I-on-X Quick Tips

Quarantine:

Unlike network switches, InterSpect-on-X does not simply block traffic to and from an infected computer and the segment on which it resides. InterSpect isolates the segment into a secure quarantine zone to prevent propagation of the attack into other parts of the network, while still allowing IT to access the infected computer(s) for problem resolution.

End-to-End security:

In addition to securing network infrastructure, endpoints such as internal and remote PCs must also be secured with an integrated policy. Check Point's Integrity Endpoint Security solution is a natural complement to the InterSpect-on-X deployment to deliver the end-to-end security you require for your network.

BUILT FOR INTERNAL NETWORKS

Security and network operations groups are increasingly working together to keep up with performance, availability and security requirements. Crossbeam provides up to 8G of scanning with 99.999% availability and fail-open options while InterSpect ensures that LAN protocols, home-grown protocols and Internet-borne traffic are inspected at wire speed. Behavior-based block and quarantine assure that false positives are reduced to a minimum.

KEY FEATURES

- Up to 32 10/100/1000 or 64 10/100 interfaces
- Up to 4000 VLANs in one chassis
- Up to 8Gbps throughput in one chassis
- Dynamic capacity via simple addition of blades
- Automated SmartDefense updates
- Native LAN protocol scanning
- Bridge or switch modes supported

HOW INTERSPECT-ON-X WORKS

Crossbeam X-Series devices are purpose-built to run Check Point software better than any platform in the world. Crossbeam uses patent-pending technology that distributes network traffic across multiple blades running InterSpect. Traffic moves across a non-blocking, distributed switch fabric. X-Series devices provide millisecond time frame failover between InterSpect blades and interfaces and can operate in single or dual-box high availability modes.

KEY FEATURES

- High speed network processor-based flow handling
- Non-blocking switch fabric
- Millisecond failover for failed blades
- Fail open or fail closed
- Out of band management

DEPLOYMENT IN BOTH VLAN AND NON-VLAN NETWORKS

InterSpect-on-X slides transparently into networks built around both physical segments and VLANs. The high port density ensures physical segmentation with deployment either between core and distribution or between distribution and access layers. VLAN integration means that InterSpect-on-X switches can be deployed at any point in the network and offers interesting new possibilities for next-generation network architectures.

KEY FEATURES

- Supports 32 10/100/1000 ports or 64 10/100 ports
- Supports up to 4000 VLANs
- Can operate in bridge or switch mode



www.crossbeamsystems.com

Corporate Headquarters
200 Baker Avenue
Concord, MA 01742 USA
p: [+1] 978-318-7500
f: [+1] 978-287-4210

European Headquarters
Village d'Entreprises Green Side
400 Avenue Roumanille
F-06906, Sophia Antipolis Cedex
France
p: [+33] (0)4 93 00 88 00
f: [+33] (0)4 93 00 88 43

Asia Pacific Headquarters
17/F, Kai Ley Tower
16 Stanley Street
Central
Hong Kong
p: [+852] 2868 9797
f: [+852] 2314 0690