SENTRIANT *Rapid Threat Detection and Mitigation for Local Area Networks*

Sentriant™ is a security appliance that secures the network interior against rapidly propagating threats including Day-Zero attacks. Sentriant is designed to work in conjunction with Extreme Networks Security Rules Engine (CLEAR-Flow). Together, Sentriant and CLEAR-Flow provide:

- Continuous monitoring of all end-points as threat sources launching internal attacks
- Filtering out of basic attacks, such as denial of service (DoS) attacks, across multi-gigabit switched networks
- Deeper analysis of suspicious traffic without impacting the operation of live networks
- Enforcement of rapid security mitigation actions against specific threat sources across the enterprise

Sentriant uses behavior-based threat detection methods (no signatures, no heuristics) to detect threats – including new threats for which no signatures exist at the time of attack. It also includes a sophisticated early warning system that employs unused IP space to identify threats. Sentriant is not an in-line device, creates no performance impact to networks, and cannot jeopardize network availability – even while the network is under attack.

Sentriant incorporates a threat termination technology aggressive, protocol-independent, automated threat termination capability. This technology does not use software desktop agents, TCP resets, or switch-dependent VLAN shunting to compartmentalize an infected end-point.

Sentriant and the CLEAR-Flow Security Rules Engine are part of the Extreme Security Framework that is a comprehensive, scalable and easy to use network-based security solution.

TYPES OF THREATS

- **Denial of Service (DoS), Distributed DoS (DDoS): threats such as Attacks, Smurf attack, Ping of death, Ping sweep, Ping flood, Port sweep, TCP Flood (Syn, Syn-Ack, Ack, Fin, Xmas, Rst), Syn attack: RFC-2827**
- **Viruses and Worms (Welchia, Slammer, Blaster, MyDoom)**
- **Polymorphic viruses, Blended attacks, Day-Zero Threats (New attack on same day as vulnerability announcement)**

VIRTUALLY IN-LINE OPERATION

Detect and actively defend against threats without interfering with network traffic. Unlike firewalls and IDP systems that need to be in-line to mitigate threats and therefore can be bottlenecks or points of failure, Sentriant is “virtually” in-line

HYPER DETECTION & ACTIVE DECEPTION

Sentriant creates a network of “virtual decoys” in the unused IP address space in a broadcast domain. These virtual decoys create an “early warning system” that fires an alert when a virtual target is contacted.

By mimicking basic responses to TCP, UDP, and ICMP requests, Sentriant makes it difficult for a hacker to determine which devices are real and which are not – allowing valid machines to hide in the white noise of virtual decoys.

SURGICAL DEFENSE

This strategy, and the underlying technology allows Sentriant to isolate attackers and prevent them from communicating with the remainder of the network while allowing mission-critical data to continue to flow normally.

Extreme networks

VIRTUALLY IN-LINE OPERATION

Sentriant is commonly deployed on a mirror port on a switch, much like a network sniffer. However, unlike sniffers, Sentriant can actively engage, deter and terminate malicious behavior. This deployment model gives systems admin-istrators strong security control over the internal network without the latency or single point of failure risks associated with in-line devices.

HYPER DETECTION

On a typical network that uses private IP address space, as much as 80% of IP address space is unassigned. Sentriant uses this asset to identify threats.

Since most worms must conduct reconnaissance to spread, there is a high probability that worm activity will hit the virtual decoys in the unused IP address space. Therefore, administrators have a much better chance of being alerted to malicious activity quickly, giving them more time to respond.

ACTIVE DECEPTION

Sentriant provides false data about the network topology in order to deceive fingerprinting-malware designed to provide precise data about operating systems (OS) and application versions present on a network. This deception makes it difficult for the malware to attack the network effectively.

Sentriant can also actively engage an attacker during the network reconnaissance that generally precedes a threat, dramatically slowing the scanning process and giving administrators time to understand and thwart the attack. During this time, Sentriant will continue to provide false data to the scan itself, slowing or even stopping the attack and providing misleading information to the attacker.

SURGICAL DEFENSE

Sentriant can logically insert itself in-between one or more attackers and one or more target devices by redirecting communications streams from attackers to itself. Sentriant can then selectively pass or silently drop packets based on their threat potential, thereby, isolating infected computers while permitting all other communication to flow normally on a network. This process occurs at both Layer 2 and Layer 3 of the Open System Interconnection (OSI) reference model.

Surgical defense can be invoked either manually by an administrator or automatically by the product when a threat is detected. It represents a departure from previous network security systems by combining the best characteristics of an in-line protection system with the performance and reliability benefits of a passive device.

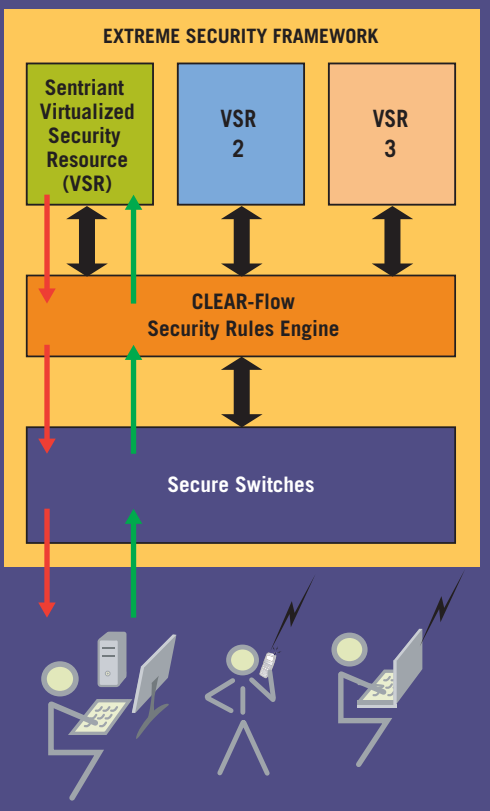
EXTREME SECURITY FRAMEWORK

Building on its proven expertise in delivering high-performance, highly available networks, Extreme Networks offers the Extreme Security Framework (ESF) that provides robust multi-gigabit security across all end-points.

ESF consists of Extreme Networks secure switches, CLEAR-Flow Security Rules Engine and Virtualized Security Resources (VSRs). The secure switches are packed with security features that help the network administrator to address operational necessities like user and usage policies, various security attacks, internal firewalling, and such. CLEAR-Flow Security Rules Engine provides first order threat detection and mitigation and mirrors traffic to VSRs for further analysis of suspicious traffic in the network. VSRs are the final piece in the ESF. VSRs are virtually available across the entire multi-gigabit network thus enabling cost-effective scalability of the security solution.

ESF enables end-point authentication and host-integrity checking, filters out DoS attacks at wire-speed, and enables threat-specific security solutions (termed as VSRs) to process mainly suspicious traffic.

As shown in the figure, multiple threat-specific VSRs can be integrated into the ESF while each VSR can be concurrently deployed to process individual threats. As an example, the Extreme Sentriant VSR is designed to detect, analyze and mitigate rapidly propagating threats such as virus or worm storms (ex. Slammer, Welchia and MyDoom).



DEPLOYMENT MODES

Sentriant can be deployed in two modes of operation – Stand-alone mode and Integrated mode.

Stand-alone mode

Sentriant can be connected to Extreme Networks core switches (BlackDiamond® 8800 series) via span ports. In this mode, Sentriant can monitor broadcast traffic from across thirty-two VLANs.

Integrated mode

Sentriant connected to the BlackDiamond 10808 (10K) switches offers the most benefits and is the recommended deployment mode. Benefits include:

- Greater performance: Since CLEAR-Flow detects and filters out DoS attacks, Sentriant can focus its resources on largely suspicious traffic, hence offering higher performance under load
- Broader range: Sentriant can analyze mirrored and span-port connected traffic. Access to all the mirrored traffic from threat-sources enables a quicker response time to potential attacks, as opposed to a narrower range of traffic presented via span-ports
- Dynamic Mitigation Control: Sentriant can add/modify the BlackDiamond 10K switch's CLEAR-Flow rules and ACLs to inspect additional traffic or change inspection thresholds – thereby allowing an automated system to fine-grain inspection rules in real-time

Sentriant provides a unique and differentiated set of benefits in the stand-alone and integrated deployment modes as summarized below.

THE ATTACK MITIGATION PROCESS TYPICALLY CONSISTS OF THE FOLLOWING STEPS

1. An infected source or malicious hacker launches a virus into the network.
2. BlackDiamond 10K static ACLs and CLEAR-Flow rules filter out DoS attacks, determine traffic class as 'suspicious' and selectively port-mirror traffic to Sentriant for further analysis.
3. The port-mirrored traffic is sent to Sentriant on a dedicated port. From here on, Sentriant controls the system in reference to the next steps.
4. Sentriant continues to watch suspicious traffic and uses its internal rules to escalate traffic-class from suspicious to the next alert level – yellow.
5. If needed, Sentriant also instantiates a dynamic ACL on BlackDiamond 10K to refine the flow criteria. BlackDiamond 10K applies the dynamic ACL in real- time and continues to port-mirror suspicious traffic conditioned on a new set of ACL rules. In parallel, if Sentriant determines that the threat is real it escalates threat-type from yellow to red alert, and sends the recommended mitigation action to EPICenter® and BlackDiamond 10K.
6. EPICenter works with the Extreme Secure Switch Infrastructure (core and edge switches) to enforce the security policy (mitigation action) in near-real time.

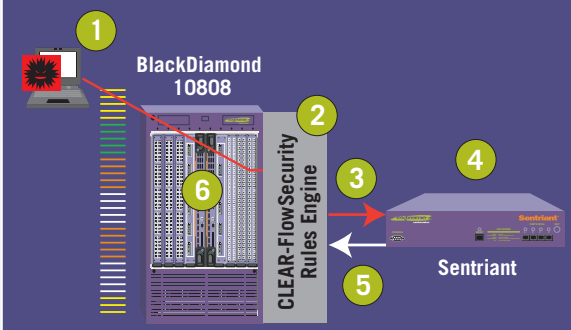


Figure 1: Attack detection and mitigation process, Integrated Deployment mode

DEPLOYMENT MODES

Sentriant is designed to operate seamlessly with perimeter and end-point security products in a stand-alone deployment mode. However, Sentriant offers the greatest benefits operating in an integrated mode within the Extreme Security Framework (ESF) as shown in the figure. Sentriant provides a unique and differentiated set of benefits in the stand-alone and integrated deployment modes as summarized below.

INTEGRATED DEPLOYMENT	STAND-ALONE DEPLOYMENT
Virtual visibility into all the end-points	Visibility limited to all end-points in the same broadcast domain.
More effective use of Sentriant resources acting on a reduced load filtered by the CLEAR-Flow security rules engine	Without CLEAR-Flow, the Sentriant needs to process the full load including DoS attacks
The Sentriant can dynamically refine filtering criteria using dynamic ACLs to the core switch	Sentriant criteria are not coupled with the switch ACLs by design; refinements can be made manually potentially affecting the system response times to attack
Inspection across a mirrored port at 1 Gbps, and across a SPAN-port at 1 Gbps possible. Mirrored traffic allows for a quicker detection and response.	Inspection across 4 Gigabit Ethernet span-ports allows access to broadcast traffic resulting in potentially slower response times
Unified Management Structure and CLEAR-Flow enable rich policy features (exxample: Role, Port, VLAN, QoS – based finer granularity for each detection or mitigation action)	Distinct device-level manager (Sentriant Console Manager) and without CLEAR-Flow, limited mitigation actions (example: No QoS-based throttling of suspicious traffic possible)

TECHNICAL SPECIFICATIONS

Performance	
Traffic Level (Inspection, Mitigation)	1 gigabit/sec aggregate traffic
Protected end-points	(Typical) 1000 end-points protected
Protected IP space	(Typical) 16K of used and unused IP addresses
Number of VLANs	Up to 32 VLANs
Appliance Internals	
Processors	Two Intel Xeon Processors (2.8 Ghz/ea)
Memory	2 GB of ECC DRAM
Hard Drive	40 GB
Network Interfaces	4 Intel 10/100/1000 NICS
Power Supply	Single 380W
Power Connection	120V/50/60Hz, US Connectivity (US cable only)
Cooling	Two 80mm Fans
Startup Access	Serial RJ45 Access
Operating System	Hardened Linux Kernel tuned for Sentriant
Chassis	
Height	2 RU (3.5 inches)
Depth	17.8 inches
Width	17.3 inches
Mounting	Bracket-based front mount
Certifications	UL 6950-1--IEC 6950-1 (US/Canada/Europe) FCC Part15/ISES003 Class A Emissions (US/Canada) CE (European Union) VCCI Class 1 ITE (Japan)
Sentriant Management System	
Platform Requirements	
Operating System	Windows XP / 2000 / Server 2003
Processor	Intel Pentium 4 (or equivalent)
Memory	512 MB
Hard Drive	1 GB (minimum)
Operation	
Access	Native application on client system
Security	Access IP and certificate-based security

ORDERING INFORMATION

Part Number	Description
70011	Sentriant Appliance (1 Gbps, 2RU chassis) includes:
	• Sentriant Console Manager
	• Sentriant MOC (Management Operations Console)
	• CLEAR-Flow security policy files library (Software package for Sentriant in (Integrated Deployment Mode)

Note:
Ordering information for Extreme Switches that work in conjunction with Sentriant are as follows:
Stand-alone mode: BlackDiamond 8800 Switches, www.extremenetworks.com/products/BlackDiamond_8800_DS.pdf
Integrated mode: BlackDiamond 10808 Switches, www.extremenetworks.com/products/BlackDiamond_10808_DS.pdf

3585 Monroe Street Santa Clara, CA 95051-1450 Phone +1 408 579 2800 Fax +1 408 579 3000
Email info@extremenetworks.com Web www.extremenetworks.com