Sentriant® NG300

Sentriant NG300 protects your network from rapidly propagating Day-Zero threats.

Detect and Deceive Threats Early

- Create a network of virtual decoys in the unused IP address space as an early warning system that alerts you when a virtual decoy is contacted
- Mimic basic responses to TCP, UDP, and ICMP requests, and make it difficult for a hacker to determine which devices are real and which are not—allowing valid machines to hide among virtual decoys

Mitigate and Slow Down Threats Precisely

- Isolate the source of attacks and prevent them from communicating with the remainder of the network
- Actively engage an attacker during the network reconnaissance that generally precedes a threat and dramatically slow down the attack

High Availability Multi-Gigabit Coverage

- CLEAR-Flow technology in ExtremeXOS® switches detects and mirrors just the threatening traffic to Sentriant NG300, allowing higher line rates of inspection and mitigation
- Detect and actively defend against threats without interfering with network traffic; Sentriant NG300 is not an inline device, therefore cannot be a bandwidth bottleneck or point of failure

Sentriant NG300 is a security appliance that complements existing perimeter and endpoint security solutions in securing the network interior against rapidly propagating threats including Day-Zero attacks. Sentriant NG300 is designed to provide:

- Continuous monitoring of all endpoints as threat sources launching internal attacks
- Deep analysis of suspicious traffic without impacting the operation of live networks
- Rapid enforcement of mitigation actions against threat sources across the Enterprise

Sentriant NG300 uses behavior-based threat detection methods (no signatures, no traffic sampling as in sFlow®) 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 NG300 incorporates an aggressive protocol—independent, automated threat termination technology. This technology does not use software desktop agents, TCP resets, or switch-dependent VLAN shunting to isolate an infected endpoint. Sentriant NG300 is a powerful threat detection and mitigation solution on its own. And when it is used with CLEAR-Flow Security Rules Engine available in ExtremeXOS switches, a single Sentriant NG300 can protect multi-gigabit networks.

Sentriant NG300 is not an inline device, creates no performance impact to networks, and cannot jeopardize network availability—even while the network is under attack.

Protect your network from:

- Viruses/Worms: Zotob, Sasser, Welchia, SQL Slammer, Blaster MyDoom and others
- Denial of Service (DoS): IP spoofing, MAC spoofing, smurf, ping of death, ping sweep, ping flood, port sweep, SYN Flood, TCP Xmas, Syn/Fin, Null, All Flags
- Day-Zero, Multi-Vector, blended attacks, polymorphic viruses
- Targeted attacks on IP Telephony devices

Detect and Deceive Threats Early

Delivers fast detection with a network of virtual decoys creating an early warning system that fires an alert when a virtual target is contacted.

Detect Threats Early

On a typical network that uses private IP address space, as much as 80% of IP address space is unassigned. Sentriant NG300 uses this asset to identify threats as shown in Figure 1. 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.

Sentriant NG300 listens to packet activity within a broadcast domain and uses its real-time map to verify packets are only sent between known, real hosts. Reconnaissance packets sent by an attacker always "miss" some real host IP addresses. The packets sent to unused IP addresses generate ARP requests by the host or gateway. If ARP requests are detected but ARP replies are not, this indicates reconnaissance. Sentriant NG300 tracks requests to unused IP addresses and assesses their source for threat potential.

Active Deception

Active Deception is a unique technology that Sentriant NG300 employs with the unused IP address space. Sentriant NG300 pre-populates the network with "virtual decoys" that occupy the unused IP address space. Using these virtual decoys, Sentriant NG300 will respond to attack traffic sent to a virtual decoy with legitimate responses. Threats waste valuable time trying to infect computers that are not really there. Meanwhile, Sentriant NG300 gathers valuable information about the nature of the attack, the ports and protocols it uses, the type of service it is trying to exploit, and the source of the attack packets and reports this information in the Sentriant Console Manager.

Sentriant NG300 also provides false data about the network topology in order to deceive fingerprinting-malware designed to provide precise data about operating systems and application versions present on a network. This deception makes it difficult for the malware to attack the network effectively.

Behavior Based Threat Detection

Sentriant NG300 uses behavior-based threat detection methods (no signatures, no traffic sampling as in sFlow) to detect threats—including new threats for which no signatures exist at the time of attack. Sentriant NG300 ships with a set of behavioral rules that are used to detect reconnaissance, bad packets, Denial of Service (DoS) attacks, targeted attacks against IP Telephony devices and protocol violations. Administrators can create additional custom rules in their environment if required. The combination of virtual decoys, active deception and continuous traffic monitoring against the behavioral rules results in very fast detection of threats in the network.

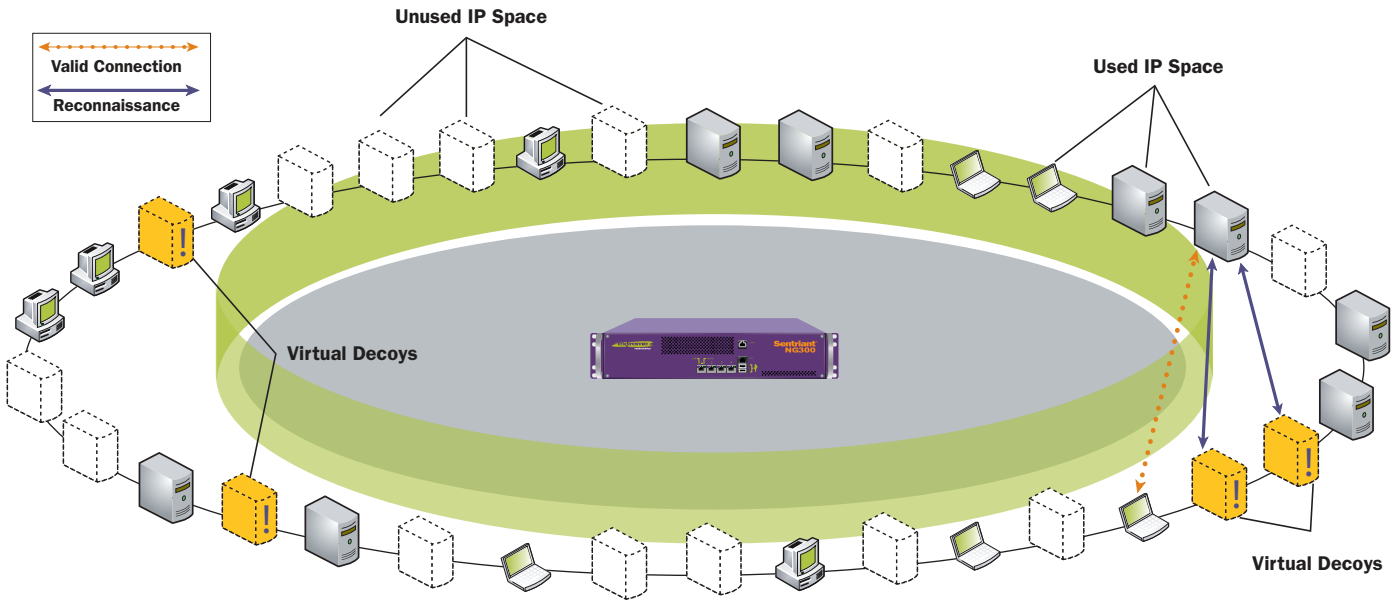


Figure 1: Unused IP Space Becomes an Early Warning System to Identify Threats

Mitigate and Slow Down Threats Precisely

Isolate the source of attacks and prevent them from communicating with the remainder of the network.

Cloaking

Sentriant NG300 can logically insert itself in between one or more attackers and one or more target devices by redirecting communication streams from the attackers to itself. Sentriant NG300 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 called Cloaking occurs at both Layer 2 and Layer 3 of the Open System Interconnection (OSI) reference model.

What makes the Cloaking unique among all other threat prevention technologies in the security networking marketplace, is that it is fundamentally a Layer 2 detection and mitigation technology. Cloaking works by using the ARP protocol, to force attacking computers to redirect attack packets to Sentriant NG300 and away from their intended targets. Cloaking is transparent to the network because it works with any type of Ethernet connected device. Cloaking is client-less because it requires no endpoint software to operate.

All Sentriant NG300 rules define a response action of either Track or Cloak. Track allows manual cloaking through the Sentriant Console Manager and Cloak performs automatic cloaking when the rule triggers.

Snaring/Slow Scan

Sentriant NG300 can also actively engage an attacker during the network reconnaissance that generally precedes a threat, dramatically slowing the scanning process as shown in Figure 2. This gives administrators enough time to understand and thwart the attack.

Snaring/Slow Scan is one of the unique technologies that Sentriant NG300 uses to stop rapidly propagating threats. Once detected, Sentriant NG300 "snares" the threat by engaging it in a legitimate protocol exchange.

Snaring operates by engaging in the TCP 3-way handshake during a connection attempt of an attacking thread. Sentriant NG300 sends responses from virtual decoys that set the TCP window size to zero, forcing attackers to send only one packet at a time, thus stopping the attacker from bursting attacks packets onto the wire. Sentriant NG300 also limits the packet size by setting a small Maximum Segment Size (MSS) to size 10. This keeps the amount of bandwidth used down to a minimum.

Slow Scan then puts the attacking thread on hold for the maximum allowed time according to the TCP protocol, of four minutes. When the attacking thread sends a "Window Probe" to the target, or virtual decoy in this case, responds and re-engages the Snaring/Slow Scan handshake.

Snaring/Slow Scan has the net effect of "holding" an attacker's attack threads, preventing that thread from being reused by the OS. Since computers have a finite number of attack threads, Snaring/Slow Scan will eventually consume all of them, stopping the attack dead in its track.

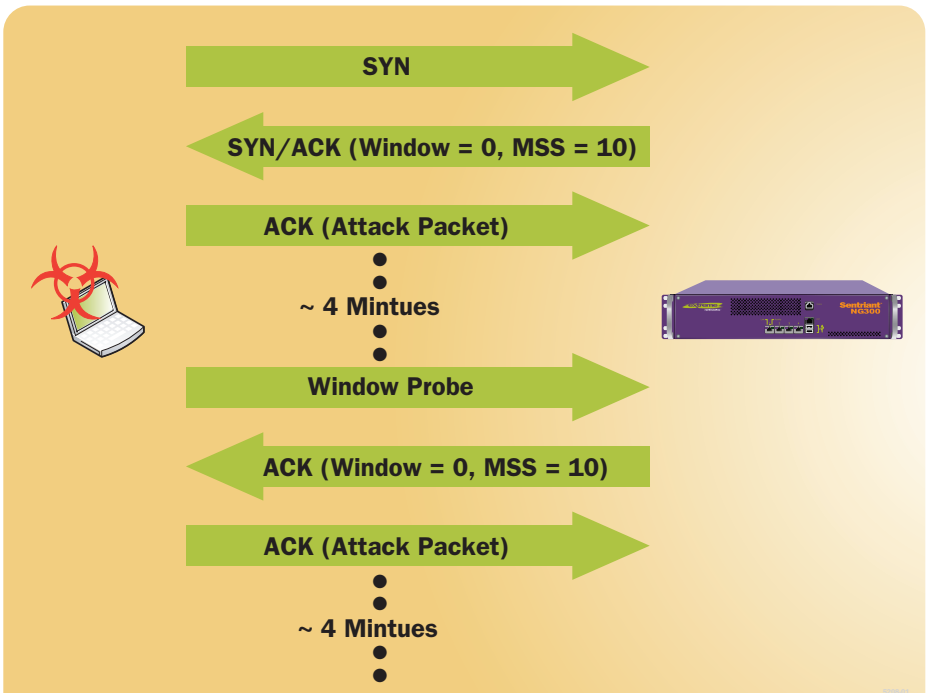


Figure 2: Slowing Down a Threat Using Snaring and Slow Scan

High Availability Multi-Gigabit Coverage

Sentriant NG300 can be integrated with CLEAR-Flow Security Rules Engine available in ExtremeXOS® switches to allow mult-gigabit rates of inspection and mitigation. Sentriant NG300 is not an inline device, therefore cannot be a bandwidth bottleneck or point of failure.

Protecting More of Your Network

Sentriant NG300 can be connected to any vendors' switches from via mirror or span ports in its standalone deployment mode. In this mode, Sentriant NG300 can monitor up to 1 gigabit per second of broadcast traffic across up to 64 VLANs. Sentriant NG300 is designed to operate seamlessly with perimeter and endpoint security products in the standalone deployment mode.

Sentriant NG300 can be deployed in a second mode called the integrated mode when it is deployed with ExtremeXOS switches from Extreme Networks that support the CLEAR-Flow Security Rules Engine. In this mode a single Sentriant NG300 can protect multi-gigabit networks.

Sentriant NG300 provides a unique and differentiated set of features in both standalone and integrated deployment modes. The major difference is the amount of traffic that it can monitor for threats.

CLEAR-Flow Integration

When integrated with ExtremeXOS switches that support CLEAR-Flow Security Rules Engine as shown in Figure 3, Sentriant NG300 offers the following benefits:

- **Greater performance:** Since CLEAR-Flow detects and filters out DoS attacks, Sentriant NG300 can focus its resources on just suspicious traffic alone, and cover of the network than in standalone mode
- **Broader range**: Sentriant NG300 can analyze mirrored traffic. Access to mirrored traffic from all the 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 NG300 can add/modify 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

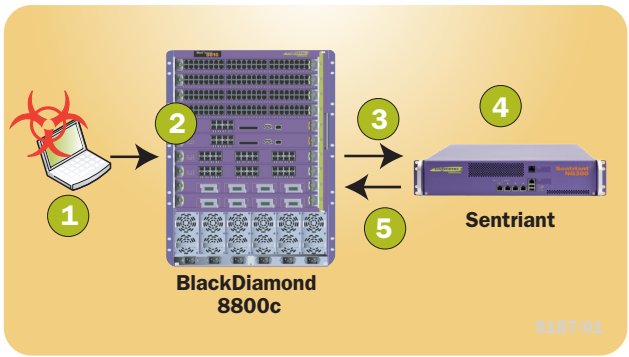
No Impact on Network Availability

Sentriant NG300 is commonly deployed on a mirror port on a switch, much like a network sniffer. However, unlike sniffers, Sentriant NG300 can actively engage, deter and terminate malicious behavior using Snaring/Slow Scan and Cloaking technologies. This deployment model gives systems administrators strong security control over the internal network without the latency or single point of failure risks associated with inline devices.

Snaring/Slow Scan and Cloaking represents a departure from previous network security systems by combining the best characteristics of an inline protection system with the performance and reliability benefits of a passive device.

Automated Attack Mitigation in Integrated Deployment Mode

1. An infected source enters the network.
2. ExtremeXOS static ACLs and CLEAR-Flow rules filter out DoS attacks, determine traffic class as 'suspicious'.
3. Selectively port-mirror traffic to Sentriant NG300 for further analysis.
4. Sentriant NG300 continues to watch suspicious traffic and uses its internal rules to escalate traffic-class from suspicious to high level alert.
5. Sentriant NG300 initiates a dynamic ACL on the ExtremeXOS switch*. The switch applies the dynamic ACL in real-time and continues to port mirror suspicious traffic.



* Summit X450a series, BlackDiamond® 8800c series, BlackDiamond 10808, and BlackDiamond 12800 series switches.

Technical Specifications

Performance

Traffic Level (Inspection, Mitigation)	1 gigabit/sec aggregate traffic
Protected Endpoints	1000 end-points protected (Typical)
Protected IP Space	16K of used and unused IP addresses (Typical)
Number of VLANs	Up to 64 VLANs

Appliance Internals

Processor	Two Intel® Xeon Processors (2.8 Ghz/ea)
Memory	2GB of ECC DRAM
Hard Drive	80GB
Network Interfaces	Four 10/100/1000BASE-T Ports One 10/100BASE-T Management Port
Power Supply	Single 400W Power Supply
Power Connection	120V/50/60Hz, U.S. Connectivity (U.S. cable only)
Startup Access	Serial RJ-45 Access

Chassis

Height	2RU (3.5 inches)
Depth	20.5 inches
Width	17.0 inches
Mounting	Bracket-based front mount
Certifications	UL 6950-1–IEC 6950 (U.S./Canada/Europe) FCC Part15/ISES003 Class A Emissions —(U.S./Canada) CE (European Union VCCI Class 1 ITE (Japan)

Sentriant NG300 Operations Console (SOC)

Platform Requirements	Operating System: Windows XP/2000/Server 2003 Processor: Intel Pentium 4 (or equivalent) Memory: 512 MB Hard Drive Space: 1 GB (minimum)

Sentriant NG300 Warranty

Hardware	Limited 1-year

Technical Specifications

Ordering Information

Part Number	Description
72051	Sentriant NG300 Apliance (1 Gbps, 2RU chassis) includes:
	• Sentriant NG300 Console Manager
	• Sentriant NG300 SOC (Sentriant Operations Console)
	• CLEAR-Flow security policy files library (Software package for Sentriant NG300 in Integrated Deployment Mode)
90534	Onsite Installation for Sentriant NG

www.extremenetworks.com email: info@extremenetworks.com

Corporate and North America
Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, CA 95051 USA
Phone +1 408 579 2800

Europe, Middle East, Africa and South America
Phone +31 30 800 5100

Asia Pacific
Phone +852 2517 1123

Japan
Phone +81 3 5842 4011