Carrier-class technologies. Outstanding support.

Feature comparisons & competitive analysis in DoS, DDoS and DrDoS mitigation solutions market

Analyzed competitors

Cisco
RadWare
Top Layer
RioRey
IntruGuard

January 2009

Cristian Velciov
ceo@andrisoft.com
(+40) 721 250246

Andrisoft Solution

WANGuard Platform is an enterprise-grade **Linux-based software solution** that delivers the functionality NOC, IT & Security teams need to effectively monitor and protect their network through a single, integrated package. WANGuard Platform is designed to protect organizations from inbound and outbound DoS, DDoS and DrDoS (such as TCP SYN flood, UDP flood, ICMP flood), but it can also be used for traffic monitoring and accounting, reacting to traffic anomalies and more.

WANGuard Platform has three main components:

1. **WANGuard Sensor** is an advanced Linux-based software created for both incoming and outgoing **traffic monitoring, accounting and analysis**. The supported traffic capturing methods are: Port Mirroring (SPAN), Cisco NetFlow®, Huawei NetStream® and In-line Deployment. At it's core, WANGuard Sensor has a highly scalable traffic correlation engine capable of continuously monitoring hundred of thousands of IP addresses. Complex statistical algorithms integrate traffic data to build accurate and detailed picture of real-time and historical traffic flows across the network.

2. **WANGuard Filter** is an advanced Linux-based software designed to **protect organizations** from internal and external threats (availability attacks on DNS, VoIP, Mail and similar services, unauthorized traffic resulting in network congestion), botnet-based attacks, zero-day worm and virus outbreaks. WANGuard Filter includes sophisticated algorithms that are able to detect, divert and drop the malicious traffic.

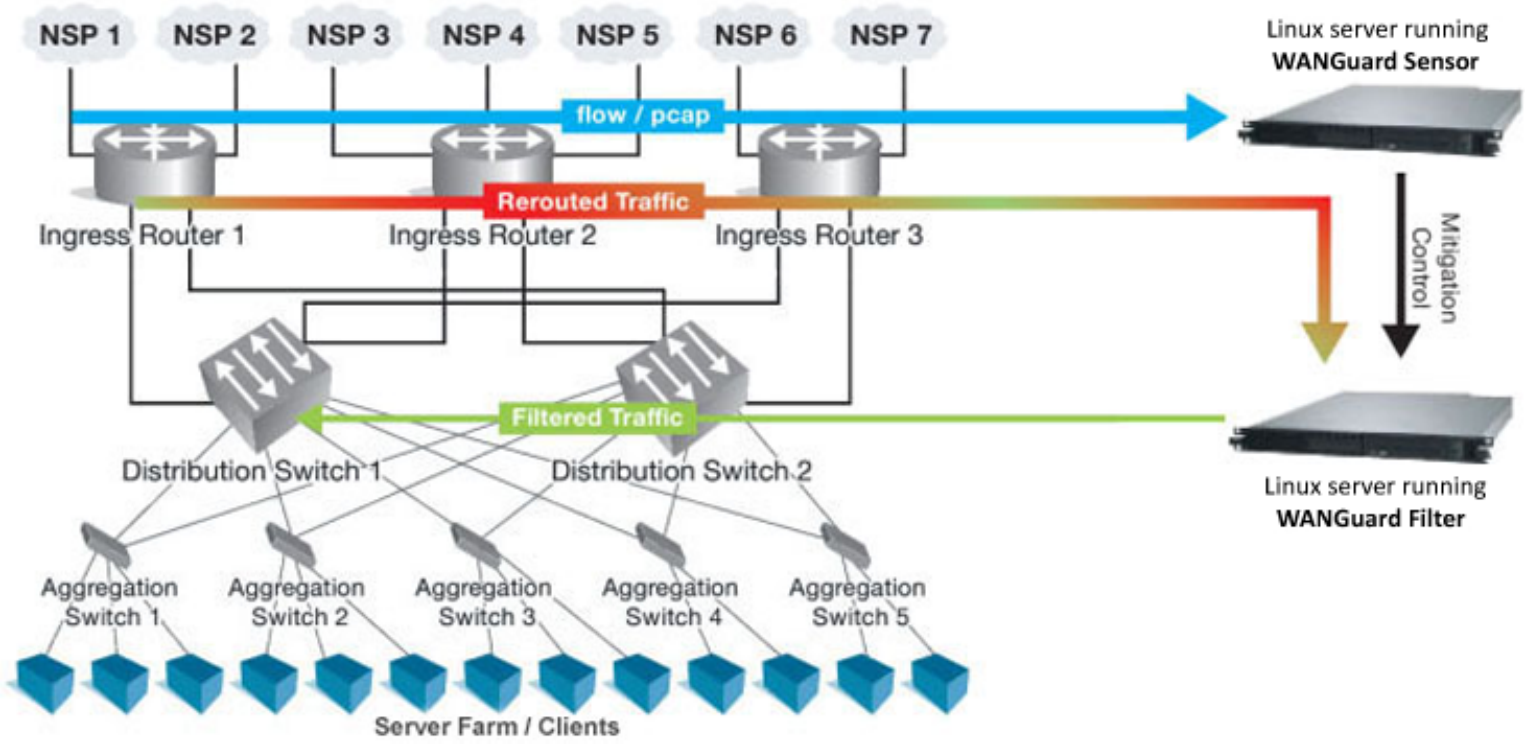
3. **WANGuard Console** provides the user with a tightly integrated and highly graphical, interactive **web interface** for all aspects of network protection and IP traffic monitoring, accounting and analysis. Included with WANGuard Console is the advanced graphing engine that provides quick and easy ad-hoc graphing functionality. WANGuard Console offers single-point management and reporting, by consolidating data received from all WANGuard Sensor and WANGuard Filter systems deployed within the network.

WANGuard Filter specifications

- Quickly see detailed live and historical information about traffic anomalies in your network from any location by accessing WANGuard Console with your web browser
- Defends against known, unknown and evolving attack patterns
- Recognizes and drops malicious traffic in under 5 seconds
- Does not block/blacklist valid customer traffic
- WANGuard Filter can be deployed in-line or out-of-line by diverting the malicious traffic towards the server running it. The cleaned traffic can be re-injected back to the network using Static Routing or GRE / IPIP tunneling
- Per endpoint flexible threat management tools and an easy to use API for scripting the reaction to attack patterns:
  - alert the NOC staff by email using user-defined email templates
  - alert the ISPs of the attackers via email using user-defined email templates
  - send custom syslog messages to remote log servers
  - execute custom scripts that extend the built-in capabilities, such as:
    - configure ACLs or execute PIX "shun" command to filter attack patterns
    - filter attacking IP addresses by executing “route blackhole” commands
    - send SNMP TRAP messages to SNMP monitoring stations
- Does not require network baseline training and operator intervention
- Easy and non-disruptive installation on common server hardware
- The most cost-effective DoS, DDoS and DrDoS mitigation and traffic policy enforcement solution on the market

WANGuard Platform deployment

To deploy WANGuard Platform in your organization you must install WANGuard Sensor server(s) near your upstream provider edges and one or more WANGuard Filter servers. You may install both components together if you have powerful servers with 3 ore more NICs. A simple deployment scenario involving two dedicated servers:



DoS, DDoS and DrDoS detection requirements for analyzing 1 Gbit NI

WANGuard Sensor Type:	WANGuard Sniff	WANGuard Flow
Traffic Capturing Technology:	Port Mirroring, Network TAP, In-line Deployment	NetFlow® or NetStream® v.5 enabled network devices
Maximum Traffic Capacity:	10 GigE , > 150,000 endpoints	10 GigE, < 100,000 endpoints
Traffic Parameters Accuracy:	Highest (5 seconds averages)	High
Traffic Anomalies Detection Time:	< 5 seconds	< flow export time + 5 seconds
Traffic Validation Options:	IP Subnets, MAC addresses, VLANs	IP Subnets, Interfaces, AS Number
Architecture:	x86 (32 or 64 bit)	x86 (32 or 64 bit)
CPU:	1 x Pentium IV 2.0 GHz	1 x Pentium IV 1.6 GHz
RAM:	500 Mbytes	3 GBytes
Network Cards:	1 x Gigabit Ethernet (with NAPI Support) 1 x Fast Ethernet	1 x Fast Ethernet
Operating System:	Red Hat Enterprise 5, CentOS 4, CentOS 5, OpenSuSE 10, SUSE Linux Enterprise 10, Debian Linux 4, Ubuntu Linux Server 8	Red Hat Enterprise 5, CentOS 4, CentOS 5, OpenSuSE 10, SUSE Linux Enterprise 10, Debian Linux 4, Ubuntu Linux Server 8
Installed Packages:	tcpdump, WANGuard-Sensor 3.0, WANGuard-Controller 3.0	WANGuard-Sensor 3.0, WANGuard-Controller 3.0
Disk Space:	5 GB (including OS)	5 GB (including OS)

Comparing Cisco Detector + Cisco Guard and WANGuard Platform

Feature	Cisco Detector + Guard	WANGuard Platform
Packet Inspection Technology	Multi-verification technology using network processors.	Granular Packet Inspection / NetFlow, Continuous, Adaptive rate limiting, using CPUs.
Detection and Mitigation	Two independent appliances (Detector and Guard).	One or two appliances (Sensor and Filter), can be deployed inline or configured for traffic diversion.
Attack Protection	Spoofed and non-spoofed attacks: TCP (syns, syn-acks, acks, fins, fragments),UDP (random port floods, fragments), ICMP (unreachable, echo, fragments), DNS, Client Attacks, Inactive and total connections, HTTP Get flood, BGP attacks.	Spoofed and non-spoofed attacks: Protocol (all 256 including TCP, UDP, ICMP, IPSec, BGP, …), Source, Destination, IP options (ToS,TTL, Length), TCP ports (all 64k incl. HTTP, SSL, DNS etc.), UDP ports (all 64k incl. DNS), ICMP Type/Code (all 64k), SYN, Excessive connection/source, Excessive connections/destination, BGP blackholing.
Multi-verification process (MVP)	Dynamic Filtering, Active Verification, Anomaly Recognition, Protocol Analysis, Rate Limiting.	Dynamic Filtering, Active Verification, Anomaly Recognition, Protocol Analysis, Rate Limiting, White/ Blacklist, Stealth Attack filtering,Source Tracking, Actions per attack.
Deployment	Complex due to traffic diversion.	From simple inline-deployment to complex traffic diversion deployment.
Management	Web-based GUI, CLI, SNMP, TACACS+.	Web-based GUI.
Baseline Self-Learning	Yes.	No.
Throughput / Latency	> 1 Gbps / Unknown.	10 Gbps / < 1 ms.

Competitive analysis with Cisco Detector + Cisco Guard

High level summary:

- Cisco is the biggest player in the networking market and during the last years has acquired multiple small companies to keep up with the perimeter security field.
- The Cisco solution and WANGuard Platform are created to solve exactly the same DDoS attacks problem. Both solutions don't rely on content-based mitigation and focus on detecting behavior anomalies. Both solutions deliver multi-gigabit performance to protect the largest enterprises, and don't sit in the main datapath.
- Besides being multiple times more affordable, WANGuard Platform delivers increased deployment and configuration flexibility, and provides a per-IP/ subnet traffic graphing and accounting system.

Comparing RadWare Defense Pro DP-1020 and WANGuard Platform

Feature	RadWare Defense Pro DP-1020	WANGuard Platform
Packet Inspection Technology	Deep packet inspection, stateful firewall, based on FPGA. DDoS shield mechanism based on sampling mechanism in CPUs.	Granular Packet Inspection / NetFlow, Continuous, Adaptive rate limiting, using CPUs.
Detection and Mitigation	One inline deployed appliance.	One or two appliances (Sensor and Filter), can be deployed inline or configured for traffic diversion.
Attack Protection	Source IP, Destination IP, Source Port, Destination Port, Packet ID, Packet size, TTL (Time to Live), ToS (Type of Service), IP Checksum, TCP Sequence Number, TCP Checksum, TCP Flags, ICMP Checksum, UDP Checksum, ICMP Message Type, DNS Query, DNS Query ID, HTTP request URI.	Spoofed and non-spoofed attacks: Protocol (all 256 including TCP, UDP, ICMP, IPSec, BGP, …), Source, Destination, IP options (ToS,TTL, Length), TCP ports (all 64k incl. HTTP, SSL, DNS etc.), UDP ports (all 64k incl. DNS), ICMP Type/Code (all 64k), SYN, Excessive connection/source, Excessive connections/destination, BGP blackholing.
Multi-verification process (MVP)	Traffic Anomaly (DoS), SYN Protection, Stateful Inspection, Intrusion Detection, Bandwidth Scheduling, White/Black list, Attack Signatures, Adaptive Smart Dynamic Filters, Proxy-based SYN Cookies, TCP Connection Resetting, Connection Blocking, Dynamic Source IP Blocking, Connection Rate Limit, Actions per Attack.	Dynamic Filtering, Active Verification, Anomaly Recognition, Protocol Analysis, Rate Limiting, White/Blacklist, Stealth Attack filtering,Source Tracking,Actions per attack.
Baseline Self-Learning	No.	No.
Throughput / Latency	8x1Gbps / < 200ms.	10 Gbps / < 1 ms.

Competitive analysis with RadWare Defense Pro DP-1020

High level summary:

- The DDoS mitigation solution from RadWare comes from an acquired company named V-Secure.
- RadWare Defense Pro DP-1020 must be deployed in the main datapath causing redundancy problems and up to 200 ms delay to the traffic. WANGuard Platform's non-distruptive and flexible installation ensures no delay to the traffic during worst attacks.
- WANGuard Platform can detect DDoS attacks using NetFlow, it can analyze 10 Gbps network links, and provides a per-IP/subnet traffic graphing and accounting system.
- By installing Snort on the WANGuard Sensor server, most of the IDS features will be supported at a fraction of the cost.

Comparing Top Layer IPS 5500-1000 and WANGuard Platform

Feature	Top Layer IPS 5500-1000	WANGuard Platform
Packet Inspection Technology	Deep packet inspection, stateful firewall, based on FPGA.	Granular Packet Inspection / NetFlow, Continuous, Adaptive rate limiting, using CPUs.
Detection and Mitigation	One inline deployed appliance.	One or two appliances (Sensor and Filter), can be deployed inline or configured for traffic diversion.
Attack Protection	Rate limiting on limited number of Dimensions, DDoS Mitigation from high rate attacks such as SYN floods and other network and application based DDoS attacks. (Limited DDoS protection).	Spoofed and non-spoofed attacks: Protocol (all 256 including TCP, UDP, ICMP, IPSec, BGP, …), Source, Destination, IP options (ToS,TTL, Length), TCP ports (all 64k incl. HTTP, SSL, DNS etc.), UDP ports (all 64k incl. DNS), ICMP Type/Code (all 64k), SYN, Excessive connection/source, Excessive connections/destination, BGP blackholing.
Multi-verificationprocess (MVP)	SYN Flood, SYN/Source, Normal / Suspicious / Malicious Monitor, Proxy, Drop connections.	Dynamic Filtering, Active Verification, Anomaly Recognition, Protocol Analysis, Rate Limiting, White/ Blacklist, Stealth Attack filtering,Source Tracking,Actions per attack.
Management	Java-based Web GUI, Windows App, CLI.	Web-based GUI.
Baseline Self-Learning	No.	No.
Throughput / Latency	4x1Gbps / < 1ms.	10 Gbps / < 1 ms.
Prevention Time	N/A	<10 seconds for Port Mirroring or <10 seconds + flow export time for NetFlow.

Competitive analysis with Top Layer IPS 5500-1000

High level summary:

- Top Layer started as a HTTP load balancer company and they extended their products with very limited DDoS mitigation capabilities.
- Top Layer IPS 5500-1000 must be deployed in the main datapath causing redundancy problems. WANGuard Platform's non-distruptive and flexible installation ensures no redundancy problems and no delay to the traffic during worst attacks.
- WANGuard Platform can detect DDoS attacks using NetFlow, it can analyze 10 Gbps network links, and provides a per-IP/subnet traffic graphing and accounting system.
- By installing Snort on the WANGuard Sensor server, most of the IDS features will be supported at a fraction of the cost.

Comparing RioRey NI-3000 and WANGuard Platform

Feature	RioRey NI-3000	WANGuard Platform
Packet Inspection Technology	Packet inspection, stateful firewall, based on CPU.	Granular Packet Inspection / NetFlow, Continuous, Adaptive rate limiting, using CPUs.
Detection and Mitigation	One inline deployed appliance.	One or two appliances (Sensor and Filter), can be deployed inline or configured for traffic diversion.
Attack Protection	Protocol, Fragmented, TOS, IP Option, Source, Destination, TCP Option, TCP Port, UDP Port, ICMP, SYN.	Spoofed and non-spoofed attacks: Protocol (all 256 including TCP, UDP, ICMP, IPSec, BGP, …), Source, Destination, IP options (ToS,TTL, Length), TCP ports (all 64k incl. HTTP, SSL, DNS etc.), UDP ports (all 64k incl. DNS), ICMP Type/Code (all 64k), SYN, Excessive connection/source, Excessive connections/destination, BGP blackholing.
Multi-verificationprocess (MVP)	Traffic Anomaly (DoS), SYN Protection, Stateful Inspection, Bandwidth Scheduling, White/Black list.	Dynamic Filtering, Active Verification, Anomaly Recognition, Protocol Analysis, Rate Limiting, White/ Blacklist, Stealth Attack filtering,Source Tracking,Actions per attack.
Management	Windows-based GUI.	Web-based GUI.
Baseline Self-Learning	Yes.	No.
Throughput / Latency	100 Mbps / < 1ms.	10 Gbps / < 1 ms.
Prevention Time	<90 seconds.	<10 seconds for Port Mirroring or <10 seconds + flow export time for NetFlow.

Competitive analysis with RioRey NI-3000

High level summary:

- Riorey technology is based on mathematical research conducted at the University of Maryland. This research led RioRey to the development of algorithms that can distinguish traffic that communicates in a valid manner from traffic that does not.
- RioRey NI-3000 must be deployed in the main datapath causing redundancy problems. WANGuard Platform's non-distruptive and flexible installation ensures no redundancy problems and no delay to the traffic during the worst DDoS attacks.
- WANGuard Platform can detect DDoS attacks using NetFlow, it can analyze 10 Gbps network links, and provides a per-IP/subnet traffic graphing and accounting system.

Comparing IntruGuard and WANGuard Platform

Feature	IntruGuard	WANGuard Platform
Packet Inspection Technology	Granular Packet Inspection, Stateful Analysis Firewall Chip(ASIC, FPGA), Continuous, Adaptive rate limiting.	Granular Packet Inspection / NetFlow, Continuous, Adaptive rate limiting, using CPUs.
Detection and Mitigation	One inline deployed appliance.	One or two appliances (Sensor and Filter), can be deployed inline or configured for traffic diversion.
Attack Protection	ARP, RARP, Multicast, Broadcast, VLAN, Double Encapsulated VLAN, Protocol (all 256 including TCP, UDP, ICMP, IPSec, BGP, …), Options (32), Fragment, Source, Destination, TOS (all 256), Network Scan, Dark Address Scan, TCP Ports (all 64K including HTTP, SSL, DNS,…), UDP Ports (all 64K), ICMP Type/ Codes (all 64K), TCP Options (32), SYN, Zombie, Excessive Connection/Source, Excessive Connections/ Destination, TCP State violation.	Spoofed and non-spoofed attacks: Protocol (all 256 including TCP, UDP, ICMP, IPSec, BGP, …), Source, Destination, IP options (ToS,TTL, Length), TCP ports (all 64k incl. HTTP, SSL, DNS etc.), UDP ports (all 64k incl. DNS), ICMP Type/Code (all 64k), SYN, Excessive connection/source, Excessive connections/ destination, BGP blackholing.
Multi-verificationprocess (MVP)	Dynamic Filtering, Active Verification, Anomaly Recognition, Protocol Analysis, Rate Limiting, State Anomaly Recognition, Stealth Attack filtering, Dark address scan prevention, White/Black list, Non-tracked Sources, Source Tracking, Legitimate IP address Matching (for anti-spoofing).	Dynamic Filtering, Active Verification, Anomaly Recognition, Protocol Analysis, Rate Limiting, White/Blacklist, Stealth Attack filtering,Source Tracking,Actions per attack.
Management	SSL Management, CLI	Web-based GUI.
Baseline Self-Learning	Yes.	No.
Throughput / Latency	1Gbps / < 50ms.	10 Gbps / < 1 ms.

Competitive analysis with IntruGuard

High level summary:

- IntruGuard is a company that actively promotes their own DDoS detection & mitigation appliance.
- IntruGuard must be deployed in the main datapath causing redundancy problems and up to 50 ms delay to the traffic. WANGuard Platform's non-distruptive and flexible installation ensures no delay to the traffic even during the worst DDoS attacks.
- IntruGuard's protection against layer 2 attacks has no relevance for IP-based, routed networks.
- WANGuard Platform can detect DDoS attacks using NetFlow, it can analyze 10 Gbps network links, and provides a per-IP/subnet traffic graphing and accounting system.