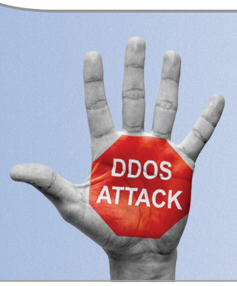
Product Data Sheet | WANGUARD 5.4

Carrier-grade DDoS detection and mitigation system

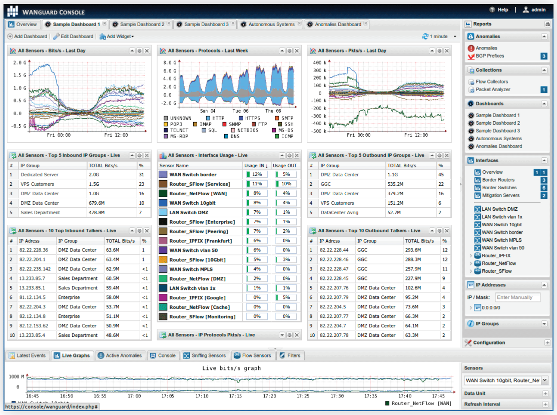
Andrisoft WANGUARD

On-premise anti-DDoS solution



OVERVIEW

Unforeseen traffic patterns affect user satisfaction, pressure over-subscription plans, and clog costly transit links. Providing a high performance level and reliable network services is central to the success of today's organizations. As the business cost of network malfunctions continues to increase, rapid identification and mitigation of threats to network performance and reliability becomes critical in order to meet expected SLAs and network availability requirements. Such threats can include Distributed denial-of-service attacks (spoofed SYN floods, NTP amplification attacks, generic UDP floods etc.), propagating worms, botnet attacks, misuse of services, and interference of best-effort traffic with critical traffic. WANGUARD's network-wide surveillance of complex, multilayer, switched and routed environments, together with its unique combination of features, is specifically designed to meet the challenge of pin-pointing and resolving any such threats.



All Sensors - Top 5 Inbound IP Groups - Live

#	IP Group	TOTAL Bits/s	%
1	Dedicated Server	2.0G	31
2	VPS Customers	1.5G	23
3	DMZ Data Center	1.0G	16
4	DMZ Data Center	679.6M	10
5	Sales Department	478.8M	7

All Sensors - Interface Usage - Live

Sensor Name	Usage IN ↓	Usage OUT
WAN Switch border	12%	5%
Router_SFlow [Services]	11%	10%
Router_NetFlow [WAN]	8%	4%
WAN Switch 10gbit	8%	4%
LAN Switch DMZ	7%	1%
Router_SFlow [Enterprise]	7%	1%
Router_SFlow [Peering]	7%	2%
Router_IPFIX [Frankfurt]	6%	0%
WAN Switch vlan 50	6%	0%
Router_SFlow [10Gbit]	5%	3%
WAN Switch MPLS	4%	0%
Router_NetFlow [DMZ]	2%	0%
LAN Switch vlan 1x	1%	1%
Router_IPFIX [Google]	0%	5%
Router_NetFlow [Cache]	0%	0%
Router_SFlow [Monitoring]	0%	0%

All Sensors - Top 5 Outbound IP Groups - Live

#	IP Group	TOTAL Bits/s	%
1	DMZ Data Center	1.1G	45
2	GGC	535.2M	22
3	DMZ Data Center	379.2M	16
4	VPS Customers	151.2M	6
5	DataCenter Avrig	52.7M	2

All Sensors - 10 Top Inbound Talkers - Live

#	IP Adress	IP Group	TOTAL Bits/s	%
1	82.22.228.36	DMZ Data Center	63.6M	1
2	82.22.204.1	DMZ Data Center	63.4M	1
3	82.22.235.142	DMZ Data Center	62.9M	<1
4	13.233.85.7	Sales Department	60.5M	<1
5	13.233.85.1	Sales Department	59.4M	<1
6	81.12.134.5	Enterprise	58.0M	<1
7	82.22.204.3	DMZ Data Center	53.7M	<1
8	82.12.134.8	Enterprise	51.1M	<1
9	82.12.153.62	DMZ Data Center	50.9M	<1
10	13.233.85.4	Sales Department	48.6M	<1

All Sensors - Top 10 Outbound Talkers - Live

#	IP Adress	IP Group	TOTAL Bits/s	%
1	82.22.228.44	GGC	293.6M	12
2	82.22.228.46	GGC	288.3M	12
3	82.22.228.47	GGC	257.9M	11
4	82.22.228.45	GGC	227.9M	9
5	82.22.207.76	DMZ Data Center	102.6M	4
6	82.22.207.79	DMZ Data Center	95.2M	4
7	82.22.204.5	DMZ Data Center	73.6M	3
8	82.22.207.77	DMZ Data Center	66.3M	2
9	82.22.204.7	DMZ Data Center	64.1M	2
10	82.22.207.78	DMZ Data Center	63.3M	2

Central Console for Network and Threat Management

KEY FEATURES AND BENEFITS

- **FULL NETWORK VISIBILITY** – Supports the latest IP traffic monitoring technologies: packet sniffing at 10 Gbps; NetFlow v5, v7 and v9; sFlow, IPFIX, NetStream, jFlow, cflowd.
- **DDOS DETECTION** – A fast traffic anomaly detection engine detects volumetric attacks by profiling the online behavior of users and by comparing over 120 live traffic parameters against user-defined thresholds.
- **DDOS MITIGATION** – Protects networks and services by detecting and cleaning malicious traffic on packet-scrubbing servers deployed in-line or out-of-line, or by using BGP black hole routing.
- **POWERFUL REACTION TOOLS** – Automate responses to threats using predefined or custom actions: send notification emails, announce prefixes in BGP, generate SNMP traps, modify ACLs, execute your own scripts with access to over 70 operational parameters through an easy-to-use API, etc.
- **DETAILED FORENSICS** – Samples of packets and flows for each attack are captured for forensic investigation. Detailed attack reports can be emailed to you, to affected customers or to attacker's ISP.
- **ADVANCED WEB CONSOLE** – Consolidated management and reporting through a single, interactive and configurable HTML5 web portal with customizable dashboards, user roles, remote authentication, etc.
- **PACKET SNIFFER** – Includes a distributed packet sniffer that can save packet dumps from different parts of the network. View packet details in a Wireshark-like web interface.
- **FLOW COLLECTOR** – Provides a fully featured NetFlow, sFlow, IPFIX Analyzer and Collector that saves flows in a compressed format for long term storage. Flows can easily be searched, filtered, sorted and exported.
- **COMPLEX ANALYTICS** – Generates the most complex reports with aggregated data for hosts, departments, interfaces, applications, ports, protocols, countries, autonomous systems, and more.
- **REAL-TIME REPORTING** – Bandwidth graphs are animated and have a short-term accuracy of just 5 seconds.
- **HISTORICAL REPORTING** – You can view reports from the last 5 seconds to the last 10 years by selecting any custom time period. Bandwidth histograms contain 95th-percentile values for burstable billing.
- **SCHEDULED REPORTING** – Any report can be generated automatically and emailed to interested parties at preconfigured intervals of time.
- **FAST & SCALABLE** – The software was designed to run on commodity hardware. Its components can be distributed on clustered servers.
- **THE LOWEST T.C.O.** – The most affordable on-premise DDoS protection solution on the market!

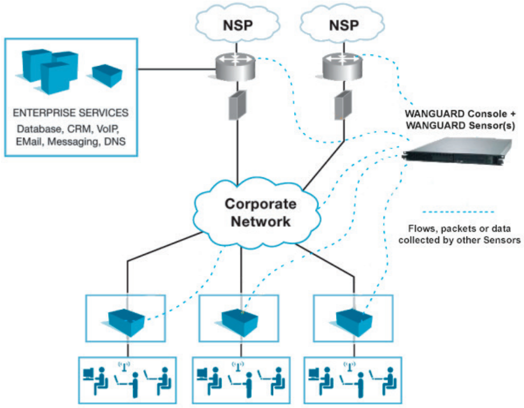
WANGUARD Sensor

OVERVIEW

The Sensor provided by WANGUARD does IP traffic monitoring by processing packets or flows, detects DoS, DDoS and other volumetric attacks, collects in-depth traffic analysis and accounting data.

The collected information enables you to generate complex IP traffic reports, graphs and tops; instantly pin down the cause of network incidents; understand patterns in application performance and make the right capacity-planning decisions.

At its core, the Sensor contains a highly scalable traffic correlation engine capable of continuously monitoring hundreds of thousands of IP addresses. Complex statistical algorithms integrate traffic data to build an accurate and detailed picture of real-time and historical traffic flows across the network.


NSP
NSP
ENTERPRISE SERVICES
Database, CRM, VoIP, EMail, Messaging, DNS
WANGUARD Console + WANGUARD Sensor(s)
Corporate Network
Flows, packets or data collected by other Sensors

KEY FEATURES AND BENEFITS

- The Sensor contains a completely scalable IP traffic analysis engine able to monitor tens of thousands of IPv4 and IPv6 addresses and IP blocks in real time
- Management and reporting are done from a single web-based Console with a unified, holistic presentation
- Detects all bandwidth-related traffic anomalies:
  - Distributed Denial of Service (DDoS) attacks, unknown volumetric DoS attacks
  - NTP amplification attacks, generic UDP floods, ICMP floods, SMURF attacks
  - SYN floods, TCP/UDP port 0, LOIC, peer-to-peer attacks, etc.
  - Scans and worms sending traffic to illegal or unallocated addresses, missing traffic to critical services
- Per-endpoint flexible threat reaction options:
  - Activate WANGUARD Filter for DDoS attack mitigation
  - Send remotely-triggered black hole announcements, BGP off-/on-ramp traffic diversion announcements
  - Alert the NOC staff by email using user-defined email templates
  - Send custom Syslog messages to remote log servers or SIEM systems
  - Capture a sample of traffic for forensic investigation
  - Extend the built-in capabilities with customized scripts that can access an easy-to-use API
- Provides traffic accounting reports and per-IP / subnet / IP Group graphs for each of the following traffic types: total, tcp, tcp+syn, udp, icmp, other, bad, flows, flows+syn, http, https, ssl, mail, dns, sip, ntp, rdp, snmp, ssh, ipsec, facebook, youtube, netflix, hulu, and more to come
- Generates tops and graphs for talkers, external IPs, IP groups, autonomous systems, countries, TCP or UDP ports, IP protocols, and more
- The short-term accuracy of bandwidth graphs can be set between 5 seconds and 10 minutes
- Users can save individual flows and packet dumps for forensic investigation or for aiding network troubleshooting. Flows can easily be searched, filtered, sorted and exported. Packet dumps can be downloaded or viewed online in a Wireshark-like interface
- Supports running in a clustered mode with collected data aggregated from multiple Sniffing Sensors or Flow Sensor interfaces. Instances can be load-balanced on different CPU cores or servers
- Any number of instances can be deployed on servers across the network
- Can use PF_RING/DNA for packet sniffing on 10 Gbit interfaces with no packet losses
- Easy and non-disruptive installation on commodity hardware

SYSTEM REQUIREMENTS

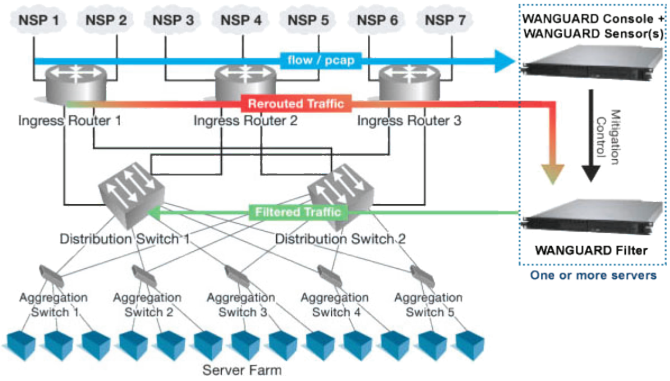
	Packet Sniffing Sensor	Flow Sensor
Traffic Capturing Technology:	In-line Appliance, Port Mirroring, Network TAP	NetFlow® v5 v7 v9, sFlow® v4 v5, IPFIX
DDoS Detection Time	< 5 seconds	< flow export time + 5 seconds
Capacity / Sensor Instance:	1 x 10 Gigabit Ethernet interface	1 flow exporter with tens of 10 GbE interfaces
CPU & RAM:	2.8 GHz quad-core Xeon, 2 GB RAM	2.0 GHz dual-core Xeon, 4 GB RAM
Network Cards:	1 x 10 GbE (Intel 82599 chipset recommended)	1 x Gigabit Ethernet
Operating System:	RHEL / CentOS 5 or 6, Debian 6 or 7, Ubuntu Server 12 or 13, OpenSuSE 12 or 13	RHEL / CentOS 5 or 6, Debian 6 or 7, Ubuntu Server 12 or 13, OpenSuSE 12 or 13

WANGUARD Filter

OVERVIEW

The Filter provided by WANGUARD detects attack patterns and generates filtering rules that scrub off anomalous traffic in a granular manner, without impacting the user experience or resulting in downtime.

DEPLOYMENT SCENARIOS



- **Out-of-line server** – In the image on the right, the Filter sends a BGP routing update to the ingress border router that will set the Filter's server as the next hop for the suspect traffic. The Filter then blocks the malicious traffic, and the cleaned traffic is routed back into the network. This technique, used to send only the traffic received by attacked destinations to the filtering server for cleaning, is called traffic diversion, BGP off-/on-ramping, sink hole routing or side filtering.
- **In-line server configured as router** – The Filter runs on a server that resides in the main data-path, configured to be a Linux router.
- **In-line server configured as network bridge** – The Filter runs on a server that resides in the main data-path, configured to be an OSI Layer 2 network bridge.
- **Server connected to a network tap or mirroring port** – The Filter runs on a server that receives a copy of packets from a network tap or mirroring port. Direct filtering is not possible, but the Filter is still able to generate filtering rules that improve the visibility of attacks and can be applied to other in-line appliances or firewalls.

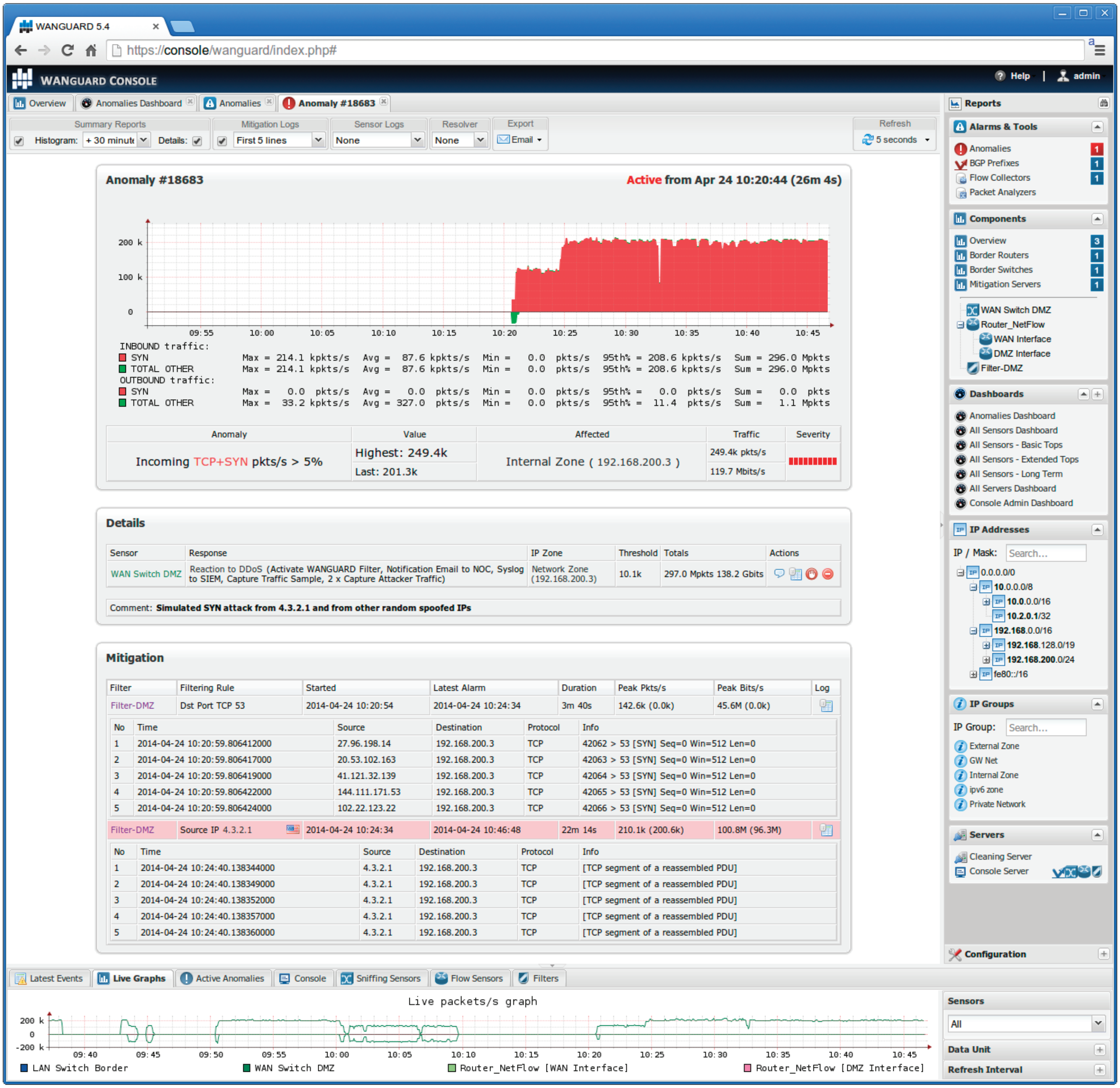
KEY FEATURES AND BENEFITS

- Defends against known, unknown and evolving DoS, DDoS and other volumetric attacks by filtering dynamically any combination of: source or destination IP addresses (IPv4 or IPv6), source or destination TCP ports, source or destination UDP ports, IP protocols, invalid IP packets, ICMP types, Time To Live, packet lengths, and more
- Recognises and blocks malicious traffic in under 5 seconds
- Does not block or blacklist valid customer traffic
- Does not require network baseline training or operator intervention
- Per endpoint flexible threat management tools and an easy to use API for scripting the reaction to attack patterns:
  - Alert your NOC staff or the ISP of the attacker using user-defined email templates
  - Send custom syslog messages to remote log servers or SIEM systems
  - Capture a sample of the attacker's traffic for forensic investigation and legal evidence
  - Execute your own scripts that extend the built-in capabilities: configure ACLs or execute PIX "shun" commands on routers or firewalls, filter attacking IP addresses by executing "route blackhole" commands on Linux servers, send SNMP TRAP messages to SNMP monitoring stations, etc.
- Supports multiple packet filtering backends:
  - Software filtering using the NetFilter framework provided by the Linux kernel
  - Hardware-based filtering on 1 or 10 Gbps network cards with Intel's 82599 chipset (Intel X520 NIC, Intel X540 NIC, HP 560 NIC, other vendors), or better
  - Dedicated firewalls and IPSes using helper scripts
- The cleaning server can be deployed in-line or can scrub the malicious traffic with BGP off-/on-ramping
- The cleaned traffic can be re-injected downstream into the network with Static Routing or GRE tunnelling
- Easy and non-disruptive installation on common server hardware

SYSTEM REQUIREMENTS

	1 Gbps mitigation	10 Gbps mitigation
Deployment Type:	In-line or out-of-line deployment	Out-of-line deployment recommended
CPU & RAM:	2.5 GHz dual-core Xeon,2 GB RAM	2.8 GHz quad-core Xeon, 4 GB RAM
Network Cards:	2 x Gigabit Ethernet	1 x 10 GbE NIC with Intel 82599 chipset or better, 1 x Gigabit Ethernet
Operating System:	RHEL / CentOS 5 or 6, Debian 6 or 7, Ubuntu Server 12 or 13, OpenSuSE 12 or 13	RHEL / CentOS 5 or 6, Debian 6 or 7, Ubuntu Server 12 or 13, OpenSuSE 12 or 13

DDoS Attack Report



☑ Histogram: + 30 minute Details: ☑ | ☑ First 5 lines | None | None | Email | 5 seconds

Anomaly #18683 — **Active from Apr 24 10:20:44 (26m 4s)**

```
INBOUND traffic:
🟥 SYN            Max = 214.1 kpkts/s   Avg =  87.6 kpkts/s   Min =   0.0  pkts/s   95th% = 208.6 kpkts/s   Sum = 296.0 Mpkts
🟩 TOTAL OTHER    Max = 214.1 kpkts/s   Avg =  87.6 kpkts/s   Min =   0.0  pkts/s   95th% = 208.6 kpkts/s   Sum = 296.0 Mpkts
OUTBOUND traffic:
🟥 SYN            Max =   0.0  pkts/s   Avg =   0.0  pkts/s   Min =   0.0  pkts/s   95th% =   0.0  pkts/s   Sum =   0.0  pkts
🟩 TOTAL OTHER    Max =  33.2 kpkts/s   Avg = 327.0  pkts/s   Min =   0.0  pkts/s   95th% =  11.4  pkts/s   Sum =   1.1 Mpkts
```

Anomaly	Value	Affected	Traffic	Severity
Incoming TCP+SYN pkts/s > 5%	Highest: 249.4k Last: 201.3k	Internal Zone (192.168.200.3)	249.4k pkts/s 119.7 Mbits/s	▮▮▮▮▮▮▮▮▮▮

Details

Sensor	Response	IP Zone	Threshold	Totals	Actions
WAN Switch DMZ	Reaction to DDoS (Activate WANGUARD Filter, Notification Email to NOC, Syslog to SIEM, Capture Traffic Sample, 2 x Capture Attacker Traffic)	Network Zone (192.168.200.3)	10.1k	297.0 Mpkts 138.2 Gbits	

Comment: **Simulated SYN attack from 4.3.2.1 and from other random spoofed IPs**

Mitigation

Filter	Filtering Rule	Started	Latest Alarm	Duration	Peak Pkts/s	Peak Bits/s	Log
Filter-DMZ	Dst Port TCP 53	2014-04-24 10:20:54	2014-04-24 10:24:34	3m 40s	142.6k (0.0k)	45.6M (0.0k)	

No	Time	Source	Destination	Protocol	Info
1	2014-04-24 10:20:59.806412000	27.96.198.14	192.168.200.3	TCP	42062 > 53 [SYN] Seq=0 Win=512 Len=0
2	2014-04-24 10:20:59.806417000	20.53.102.163	192.168.200.3	TCP	42063 > 53 [SYN] Seq=0 Win=512 Len=0
3	2014-04-24 10:20:59.806419000	41.121.32.139	192.168.200.3	TCP	42064 > 53 [SYN] Seq=0 Win=512 Len=0
4	2014-04-24 10:20:59.806422000	144.111.171.53	192.168.200.3	TCP	42065 > 53 [SYN] Seq=0 Win=512 Len=0
5	2014-04-24 10:20:59.806424000	102.22.123.22	192.168.200.3	TCP	42066 > 53 [SYN] Seq=0 Win=512 Len=0

Filter	Filtering Rule	Started	Latest Alarm	Duration	Peak Pkts/s	Peak Bits/s	Log
Filter-DMZ	Source IP 4.3.2.1	2014-04-24 10:24:34	2014-04-24 10:46:48	22m 14s	210.1k (200.6k)	100.8M (96.3M)	

No	Time	Source	Destination	Protocol	Info
1	2014-04-24 10:24:40.138344000	4.3.2.1	192.168.200.3	TCP	[TCP segment of a reassembled PDU]
2	2014-04-24 10:24:40.138349000	4.3.2.1	192.168.200.3	TCP	[TCP segment of a reassembled PDU]
3	2014-04-24 10:24:40.138352000	4.3.2.1	192.168.200.3	TCP	[TCP segment of a reassembled PDU]
4	2014-04-24 10:24:40.138357000	4.3.2.1	192.168.200.3	TCP	[TCP segment of a reassembled PDU]
5	2014-04-24 10:24:40.138360000	4.3.2.1	192.168.200.3	TCP	[TCP segment of a reassembled PDU]

DOWNLOAD A FREE 30-DAY TRIAL
www.andrisoft.com/trial

WAN GUARD

Website: www.andrisoft.com | Email: sales@andrisoft.com | Twitter: twitter.com/andrisoft | LinkedIn: www.linkedin.com/company/andrisoft
Address: Str. Dorobantilor 20, ap. 21, 300298 Timisoara, Romania.
Phone: +40721250246 (10-16 GMT)