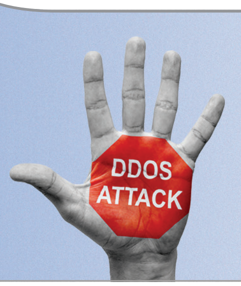
Carrier-grade DDoS detection and mitigation software

Andrisoft WanGuard

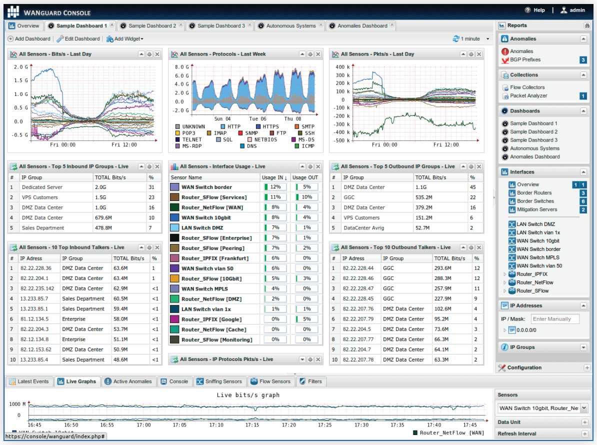
On-premise anti-DDoS solution



OVERVIEW

Andrisoft WanGuard is enterprise-grade software that delivers to NOC, IT and Security teams the functionality needed for effectively monitoring and protecting WAN networks through a single integrated package.

Unforeseen traffic patterns affect user satisfaction and clog costly transit links. Providing reliable network services is imperative 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. WanGuard's network-wide surveillance of complex, multilayer, switched or 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 - 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 - 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 - 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

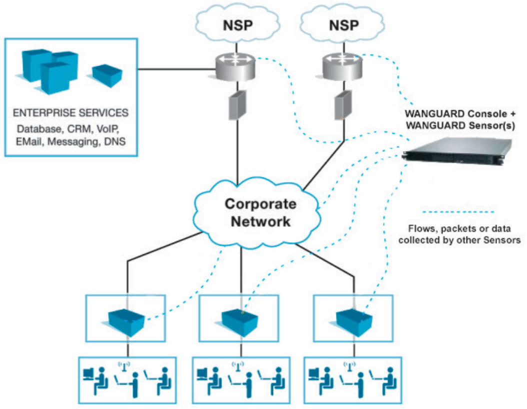
KEY FEATURES AND BENEFITS

- **FULL NETWORK VISIBILITY** – Supports all major IP traffic monitoring technologies: 10 GbE packet sniffing, NetFlow version 5,7 and 9; sFlow version 4 and 5; IPFIX and SNMP.
- **COMPREHENSIVE DDOS DETECTION** – Leverages an innovative traffic anomaly detection engine that quickly detects volumetric attacks by profiling the online behavior of users and by comparing over 130 live traffic parameters against user-defined thresholds.
- **ON-PREMISE DDOS MITIGATION** – Protects networks by using BGP black hole announcements or FlowSpec; protects services by cleaning malicious traffic on packet-scrubbing servers deployed in-line or out-of-line.
- **FAST, SCALABLE & ROBUST** – The software was designed to run on commodity hardware by leveraging high-speed packet capturing technologies such as Myricom Sniffer10G, PF_RING Vanilla, PF_RING ZC or Netmap. Can run as a cluster with its software components distributed across multiple servers.
- **POWERFUL REACTION TOOLS** – Executes predefined actions that automate the responses to attacks: sends notification emails, announces prefixes in BGP, generates SNMP traps, modifies ACLs, and executes scripts that have access through an easy-to-use API to over 80 internal parameters.
- **DETAILED FORENSICS** – Samples of packets and flows are captured for forensic investigation during each attack. Detailed attack reports can be emailed to you, affected customers or to the attacker's ISP.
- **ADVANCED WEB CONSOLE** – Consolidated management and reporting through a single, interactive and highly-configurable HTML5 web portal with customizable dashboards, user roles and remote authentication.
- **PACKET SNIFFER** – A distributed packet sniffer that saves packet dumps from different network entry points. View packet details in a Wireshark-like web interface.
- **FLOW COLLECTOR** – A fully featured NetFlow, sFlow, and 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 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.

WanGuard Sensor

OVERVIEW

The Sensor component of WanGuard uses an extremely fast and highly innovative traffic anomaly detection engine that detects volumetric attacks by profiling the on-line behaviour of users and by comparing over 130 live traffic parameters against user-defined thresholds. It collects information that allows you to generate complex traffic reports, graphs and tops; instantly pin down the cause of network incidents; automate the reaction to threats; understand patterns in application performance and make the right capacity planning decisions. You can automate the reaction to attacks by using predefined action modules that send notification emails, announce prefixes in BGP, generate SNMP traps, modify ACLs and execute custom scripts with access to an easy-to-use API exposing 80+ internal parameters.


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

- Contains a completely scalable traffic analysis engine able to monitor, in real time, tens of thousands of IPv4 and IPv6 addresses and ranges
- Management and reporting through an advanced web-based Console with a unified, holistic presentation
- Detects all bandwidth-related traffic anomalies, such as:
  - 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
  - Scans and worms sending traffic to illegal/unallocated addresses, missing traffic to/from critical services
- Per-endpoint flexible threat reaction options, such as:
  - Activate on-premise DDoS attack mitigation with WanGuard Filter
  - Send BGP black hole routing updates with FlowSpec (RFC 5575) or null-routing communities
  - Send BGP off-/on-ramp traffic diversion routing updates to on-premise/on-cloud DDoS mitigation services
  - Email alerts with user-defined dynamic 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 by executing your own scripts with access to 70+ operational parameters through an easy-to-use API
- Provides traffic accounting reports and per-IP/subnet/IP group graphs for each of the following decoders (classes): tcp, tcp+syn, tcp+rst, tcp+ack, tcp+syn+ack, tcp-null, udp, icmp, other, bad, flows, http, https, ssl, mail, dns, sip, ntp, rdp, snmp, ssh, ipsec, ssdp, facebook, youtube, netflix, hulu. Supports custom decoders
- Generates tops and graphs for talkers, external IPs, IP groups, autonomous systems, countries (based on GeoIP or ASN), 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 by aggregating data collected by multiple Sensors, load-balanced on different CPU cores or servers
- Easy installation on commodity hardware. Any number of instances can be deployed across the network

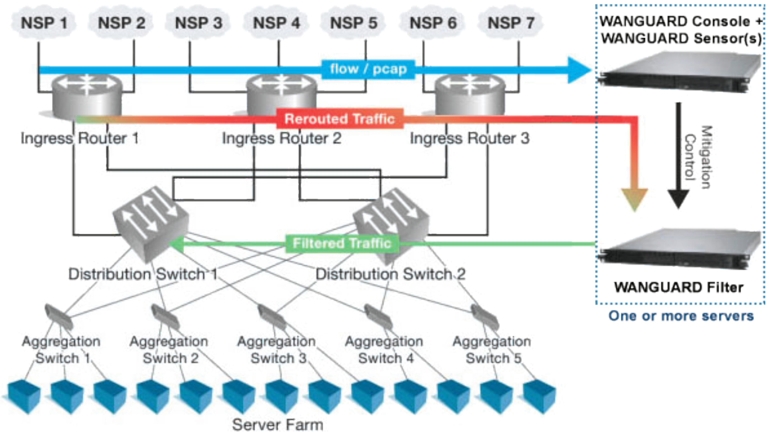
SYSTEM REQUIREMENTS

	Packet Sensor	Flow Sensor
IP Monitoring 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 per Sensor:	10 GbE (supports PF_RING, Sniffer10G, Netmap)	1 flow exporter with tens of 10 GbE interfaces
CPU & RAM:	3.2 GHz quad-core Xeon, 3 GB RAM	2.0 GHz dual-core Xeon, 4 GB RAM
Network Cards:	1 x 10 GbE	1 x Gigabit Ethernet
Operating System:	RHEL / CentOS 6 or 7; Debian 6, 7 or 8; Ubuntu Server 12 or 14; OpenSuSE 13	RHEL / CentOS 6 or 7, Debian 6, 7 or 8; Ubuntu Server 12 or 14; OpenSuSE 13

WanGuard Filter

OVERVIEW

The Filter component of WanGuard ensures zero downtime for customers and services during Distributed Denial of Service attacks, without requiring an operator intervention. It defends against DDoS attacks by cleaning the malicious traffic on-premise (when the upstream links are not congested), and notifies the attacker's ISP when the attack is not spoofed. The malicious packets are blocked using intelligent, dynamic filtering rules that are applied on stateless software or hardware firewalls and on BGP FlowSpec-capable routers. Dedicated packet scrubbing servers can be deployed in the main data path, or can perform side-filtering with BGP off-ramping.



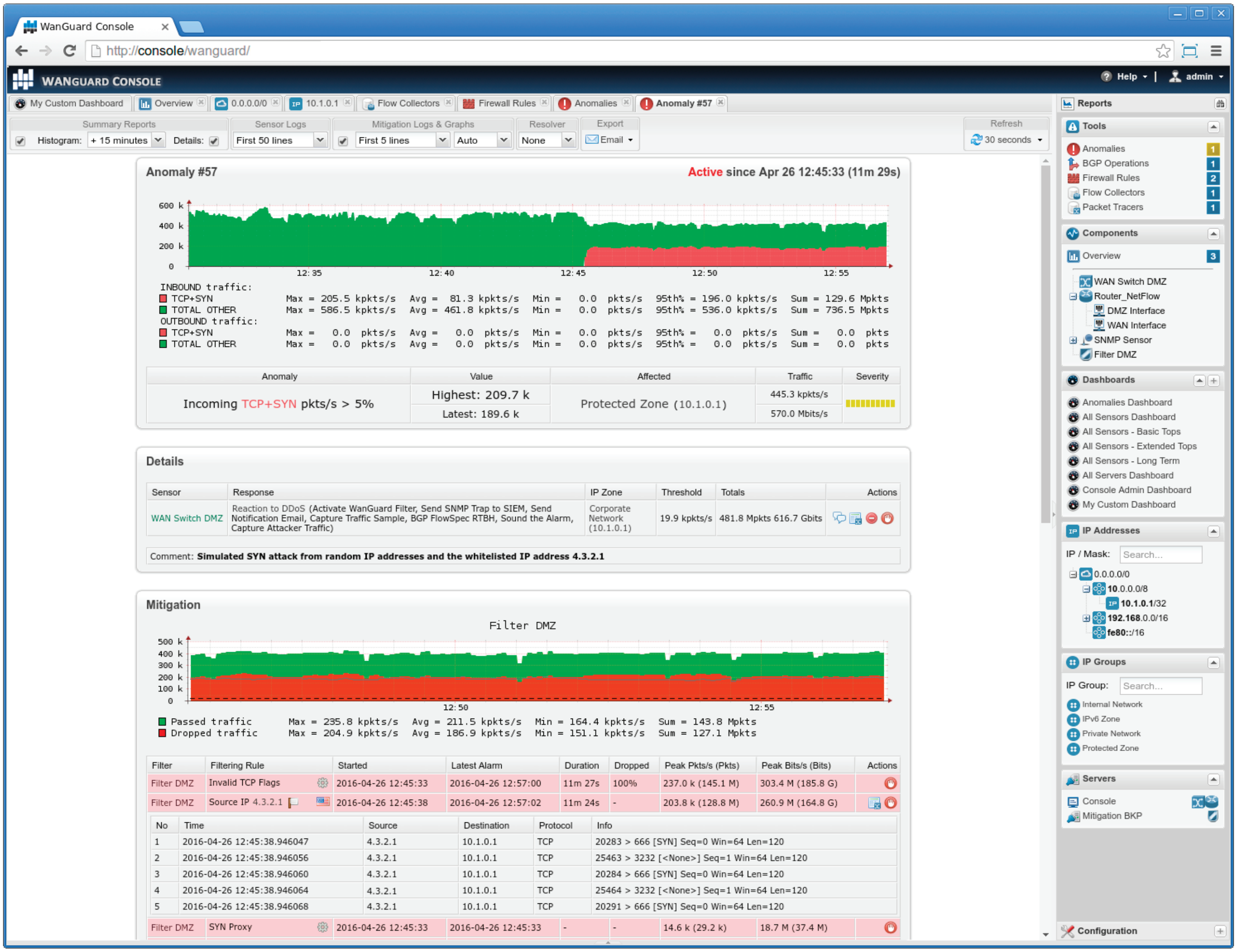
KEY FEATURES AND BENEFITS

- Defends against known, unknown and evolving DoS, DDoS and other volumetric attacks by smart filtering any combination of source and destination IPv4 or IPv6 addresses, source and destination TCP ports, source and destination UDP ports, IP protocols, invalid IP headers, ICMP types, common Time To Live values, packet lengths, country, DNS Transaction ID, etc.
- Recognises and blocks malicious traffic in under 5 seconds
- Stateless operation designed to work with asymmetric routing
- Uses SYN Proxy to protect against spoofed SYN, SYN-ACK and ACK attacks
- Does not require network baseline training or operator intervention
- Per-endpoint threat management tools and an easy-to-use API for scripting the reaction to attack vectors:
  - Alert the NOC, customer or ISP of the attacker with 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, execute "shun" commands on routers and 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 10/40 Gbps Chelsio T5 NICs, or 1/10 Gbps NICs with Intel 82599 chipset
  - BGP FlowSpec-capable routers
  - Third-party dedicated firewalls and IPSes controlled by helper scripts
- Cleaning servers can be deployed in-line or can scrub malicious traffic by BGP off-/on-ramping (sink hole routing), S/RTBH or FlowSpec
- Easy and non-disruptive installation on commodity server hardware

SYSTEM REQUIREMENTS

DDoS Mitigation Capacity:	1 Gbit/s – 1,400,000 packets/s	10 Gbit/s – 14,000,000 packets/s
Deployment Type:	In-line or out-of-line	Out-of-line (using BGP redirect) recommended
CPU & RAM:	2.4 GHz dual-core Xeon, 2 GB RAM	3.2 GHz quad-core Xeon, 8 GB RAM
Network Cards:	2 x Gigabit Ethernet	1 x 10 GbE NIC (Chelsio T4/T5 or Intel 82599 chipset recommended), 1 x Gigabit Ethernet
Operating System:	RHEL / CentOS 6 or 7; Debian 6, 7 or 8; Ubuntu Server 12 or 14; OpenSuSE 13	RHEL / CentOS 6 or 7; Debian 6, 7 or 8; Ubuntu Server 12 or 14; OpenSuSE 13

DDoS Report Sample



Anomaly #57 — Active since Apr 26 12:45:33 (11m 29s)

```
INBOUND traffic:
🟥 TCP+SYN       Max = 205.5 kpkts/s  Avg =  81.3 kpkts/s  Min =   0.0  pkts/s  95th% = 196.0 kpkts/s  Sum = 129.6 Mpkts
🟩 TOTAL OTHER   Max = 586.5 kpkts/s  Avg = 461.8 kpkts/s  Min =   0.0  pkts/s  95th% = 536.0 kpkts/s  Sum = 736.5 Mpkts
OUTBOUND traffic:
🟥 TCP+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 =   0.0  pkts/s  Avg =   0.0  pkts/s  Min =   0.0  pkts/s  95th% =   0.0  pkts/s  Sum =   0.0  pkts
```

Anomaly	Value	Affected	Traffic	Severity
Incoming TCP+SYN pkts/s > 5%	Highest: 209.7 k Latest: 189.6 k	Protected Zone (10.1.0.1)	445.3 kpkts/s 570.0 Mbits/s	▮▮▮▮▮▮▮▮▮▮

Details

Sensor	Response	IP Zone	Threshold	Totals	Actions
WAN Switch DMZ	Reaction to DDoS (Activate WanGuard Filter, Send SNMP Trap to SIEM, Send Notification Email, Capture Traffic Sample, BGP FlowSpec RTBH, Sound the Alarm, Capture Attacker Traffic)	Corporate Network (10.1.0.1)	19.9 kpkts/s	481.8 Mpkts 616.7 Gbits	

Comment: **Simulated SYN attack from random IP addresses and the whitelisted IP address 4.3.2.1**

Mitigation

Filter DMZ

```
🟩 Passed traffic    Max = 235.8 kpkts/s  Avg = 211.5 kpkts/s  Min = 164.4 kpkts/s  Sum = 143.8 Mpkts
🟥 Dropped traffic   Max = 204.9 kpkts/s  Avg = 186.9 kpkts/s  Min = 151.1 kpkts/s  Sum = 127.1 Mpkts
```

Filter	Filtering Rule	Started	Latest Alarm	Duration	Dropped	Peak Pkts/s (Pkts)	Peak Bits/s (Bits)	Actions
Filter DMZ	Invalid TCP Flags	2016-04-26 12:45:33	2016-04-26 12:57:00	11m 27s	100%	237.0 k (145.1 M)	303.4 M (185.8 G)	
Filter DMZ	Source IP 4.3.2.1	2016-04-26 12:45:38	2016-04-26 12:57:02	11m 24s	-	203.8 k (128.8 M)	260.9 M (164.8 G)	

No	Time	Source	Destination	Protocol	Info
1	2016-04-26 12:45:38.946047	4.3.2.1	10.1.0.1	TCP	20283 > 666 [SYN] Seq=0 Win=64 Len=120
2	2016-04-26 12:45:38.946056	4.3.2.1	10.1.0.1	TCP	25463 > 3232 [<None>] Seq=1 Win=64 Len=120
3	2016-04-26 12:45:38.946060	4.3.2.1	10.1.0.1	TCP	20284 > 666 [SYN] Seq=0 Win=64 Len=120
4	2016-04-26 12:45:38.946064	4.3.2.1	10.1.0.1	TCP	25464 > 3232 [<None>] Seq=1 Win=64 Len=120
5	2016-04-26 12:45:38.946068	4.3.2.1	10.1.0.1	TCP	20291 > 666 [SYN] Seq=0 Win=64 Len=120

Filter	Filtering Rule	Started	Latest Alarm	Duration	Dropped	Peak Pkts/s (Pkts)	Peak Bits/s (Bits)	Actions
Filter DMZ	SYN Proxy	2016-04-26 12:45:33	2016-04-26 12:45:33	-	-	14.6 k (29.2 k)	18.7 M (37.4 M)	

Website: www.andrisoft.com | Email: sales@andrisoft.com | Twitter: twitter.com/andrisoft | LinkedIn: www.linkedin.com/company/andrisoft
Address: City Business Centre, E Building Ground Floor, Str. Coriolan Brediceanu, Nr. 10, 300011 Timisoara, Timis, Romania.
Phone: +40721250246 (10:00 - 16:00 GMT)