corero [NETWORK SECURITY]

SECUREWATCH® ANALYTICS _

Unlock the Power of Multisite Traffic Monitoring

Your network spans multiple locations, and you can't afford any blind spots. That's why complete visibility across all sites is essential. Our multisite analytics solution simplifies managing a dispersed network by providing clear insights and quickly resolving service availability issues. With a unified dashboard, you can monitor, analyze, and protect your entire network, no matter the size.

Get powerful security with intuitive, easy-to-read dashboards that deliver actionable intelligence before, during, and after a DDoS attack—without needing specialized expertise. Plus, traffic data is stored for as long as you need, enabling you to identify trends, respond to threats faster, and keep services running smoothly.

Benefits That Make Business Sense

Optimize Network Resources:

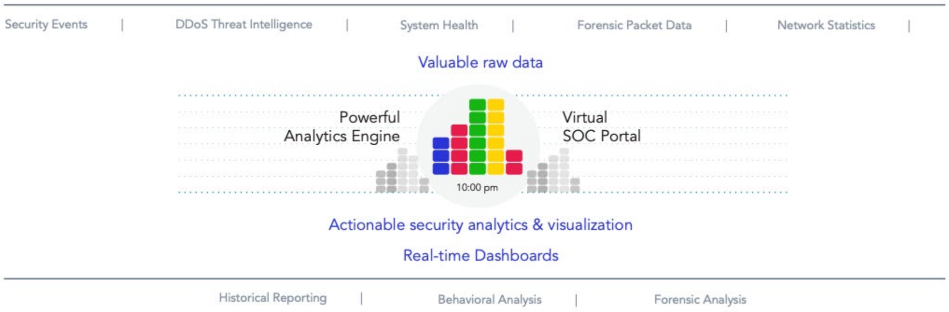
Leverage detailed traffic and geographic reports to efficiently manage network traffic, reduce costs, and plan intelligently for future growth.

Fuel Business Expansion

Unlock insights from our built-in traffic reports to streamline the provisioning, delivery, and maintenance of new services—boosting customer satisfaction and driving business growth.

Minimize Downtime

Stay ahead of potential disruptions by proactively detecting threats like misconfigurations, DDoS attacks, or sudden traffic spikes. Our real-time analytics portal lets you respond quickly and mitigate risks before they impact your service availability.


Security Events | DDoS Threat Intelligence | System Health | Forensic Packet Data | Network Statistics |
Valuable raw data
Powerful Analytics Engine
Virtual SOC Portal
10:00 pm
Actionable security analytics & visualization
Real-time Dashboards
Historical Reporting | Behavioral Analysis | Forensic Analysis

SecureWatch Analytics is included as a key component of Corero's SmartWall ONE™ real-time, automatic, DDoS defense solutions. It transforms DDoS tailored security feeds from SmartWall ONE deployments into autonomic defense actions and dashboards of actionable security intelligence, exposing:

1. Volumetric DDoS – reflection, amplification, & flooding attacks
2. Under the radar non-saturating attacks
3. Targeted resource exhaustion attacks
4. Victim servers, ports, and services
5. Malicious IP addresses and botnets

Empowered by this enhanced visibility, organizations can utilize SecureWatch Analytics as a single pane of glass to visualize DDoS attacks and help ensure uninterrupted business continuity for their Internet facing services.

Key Service Benefits

Monitor and Optimize Traffic Across Multiple Locations

Get a complete view of traffic patterns across all your geographical locations. This allows you to monitor network performance and ensure smooth, uninterrupted operations wherever you're located.

Prioritize High-Traffic Areas for Efficiency

Easily identify which sites are experiencing the most traffic, so you can allocate resources efficiently and focus your attention where it's needed most.

Make Confident, Data-Driven Decisions

Empower your team with detailed traffic analysis tools. Whether you're focusing on specific assets or identifying trends across multiple locations, real-time data helps you detect anomalies, spot potential threats, and make informed decisions that enhance security and network performance.

Forensic-Level Insights into DDoS Attacks

Stay ahead of potential threats with forensic-level visibility before, during, and after DDoS events. Our intuitive dashboards provide clear, actionable insights that help you quickly troubleshoot and respond to attacks.

Stay Ahead with Comprehensive, Real-Time Monitoring

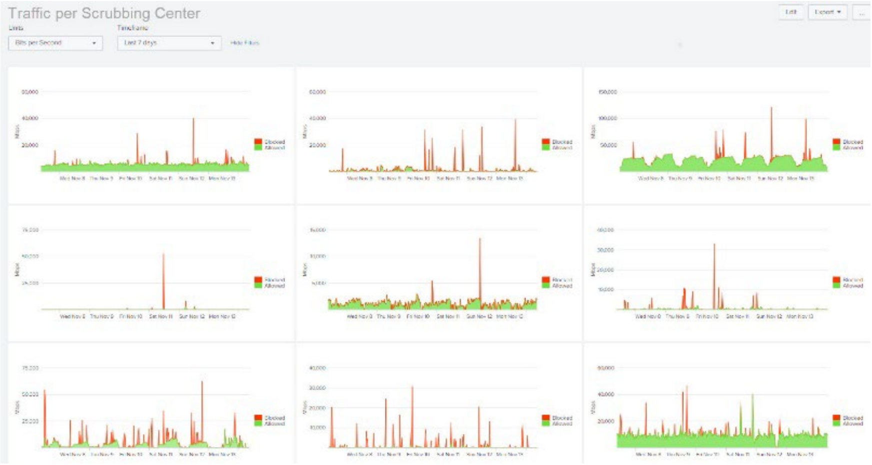
Get real-time visibility into your network's DDoS activity from a single dashboard. Whether you're viewing the overall network health or drilling down into individual site data, you'll have the information you need to respond swiftly and effectively.

Detailed Breakdown of Threats

Easily drill down into attack specifics—right down to the IP address, protocol, or port—enabling faster, more targeted responses to any threat.

Multi-User NOC/SOC Dashboards

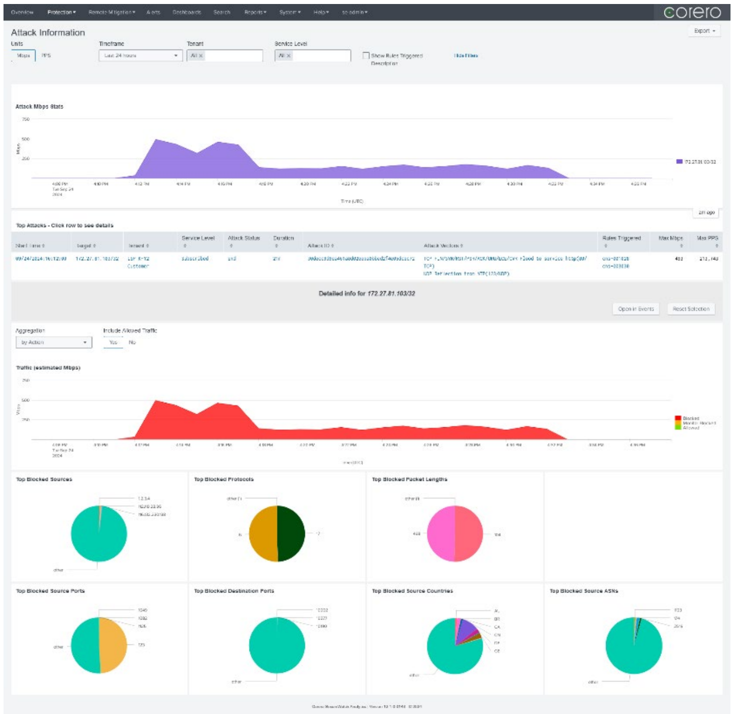
SecureWatch Analytics (SWA) is accessible from any browser, providing real-time and historical dashboard views that give a clear summary of network and DDoS activity. Analysts can view data at a specific site level or across multiple locations for a consolidated security overview. SWA helps analysts quickly assess the size, profile, and specific attack vectors in real-time, offering a complete, "single-pane-of-glass" view of system health and protection status.



Traffic per Scrubbing Center

Units: Bits per Second

Timeframe: Last 7 days



Attack Information

Units: Mbps | PPS
Timeframe: Last 24 hours
Tenant: All ×
Service Level: All ×
□ Show Rules Triggered Description

Top Attacks - Click row to see details

Start Time	Target	Tenant	Service Level	Attack Status	Duration	Attack ID	Attack Vectors	Rules Triggered	Max Mbps	Max PPS
09/24/2024 16:12:00	172.27.81.103/32	ISP K-12 Customer	subscribed	end	21m	[illegible]	TCP FLAG/SYN/RST/PSH/ACK/URG/ECE/CWR Flood to service http(80/TCP) UDP Reflection from NTP(123/UDP)	cns-001038 cns-003038	483	213,748

Detailed info for *172.27.81.103/32*

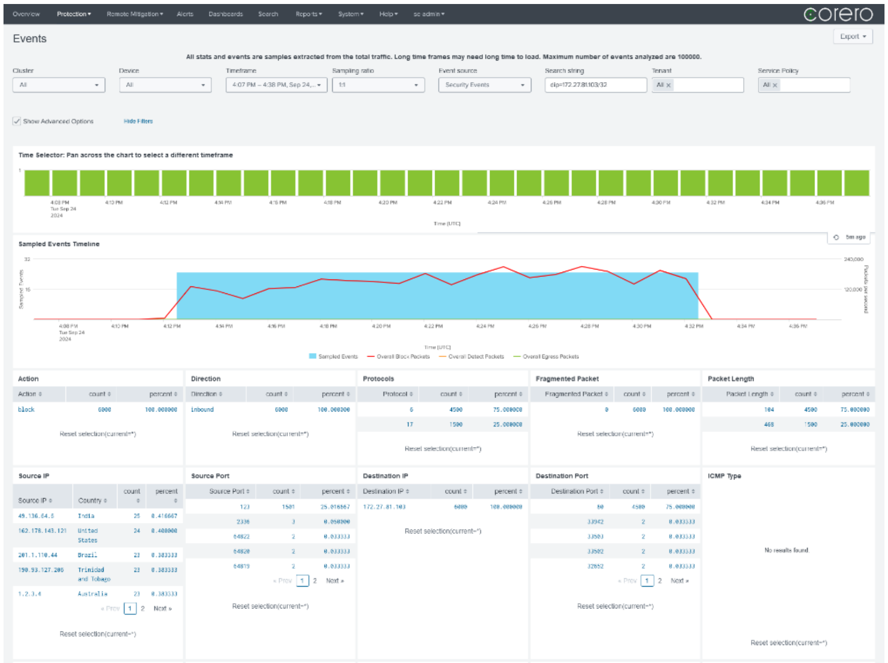
Aggregation: by Action
Include Allowed Traffic: Yes | No

Drill Down on Attacks

SecureWatch Analytics presents a detailed statistical view of inbound traffic using IP sFlow samples from SmartWall ONE DDoS protection solution. Reports cover key metrics like source and destination IPs, ports, protocols, TTL (time-to-live), packet lengths, and fragments. These insights provide valuable data to help refine security policies and optimize network performance when needed.

Detailed Traffic Statistics

It is critical to know the details when you are under attack. SecureWatch Analytics gives you the ability to immediately drill down to see the offending addresses, ports, protocols and other key insight into the attackers targeting your infrastructure. These can then easily be reported on or incorporated into ACLs and blacklists to permanently or temporarily block access for devices with no legitimate reason to be accessing your network.



Events

All stats and events are samples extracted from the total traffic. Long time frames may need long time to load. Maximum number of events analyzed are 100000.

Cluster: All
Device: All
Timeframe: 4:07 PM – 4:38 PM, Sep 24,...
Sampling ratio: 1:1
Event source: Security Events
Search string: dip=172.27.81.103/32
Tenant: All ×
Service Policy: All ×

☑ Show Advanced Options

Action

Action	count	percent
block	6000	100.000000

Reset selection(current=*)

Direction

Direction	count	percent
inbound	6000	100.000000

Reset selection(current=*)

Protocols

Protocol	count	percent
6	4500	75.000000
17	1500	25.000000

Reset selection(current=*)

Fragmented Packet

Fragmented Packet	count	percent
0	6000	100.000000

Reset selection(current=*)

Packet Length

Packet Length	count	percent
104	4500	75.000000
468	1500	25.000000

Reset selection(current=*)

Source IP

Source IP	Country	count	percent
49.136.64.5	India	25	0.416667
162.178.143.121	United States	24	0.400000
201.1.110.44	Brazil	23	0.383333
190.93.127.206	Trinidad and Tobago	23	0.383333
1.2.3.4	Australia	23	0.383333

« Prev 1 2 Next »

Reset selection(current=*)

Source Port

Source Port	count	percent
123	1501	25.016667
2336	3	0.050000
64822	2	0.033333
64820	2	0.033333
64819	2	0.033333

« Prev 1 2 Next »

Reset selection(current=*)

Destination IP

Destination IP	count	percent
172.27.81.103	6000	100.000000

Reset selection(current=*)

Destination Port

Destination Port	count	percent
80	4500	75.000000
33942	2	0.033333
33503	2	0.033333
33502	2	0.033333
32652	2	0.033333

« Prev 1 2 Next »

Reset selection(current=*)

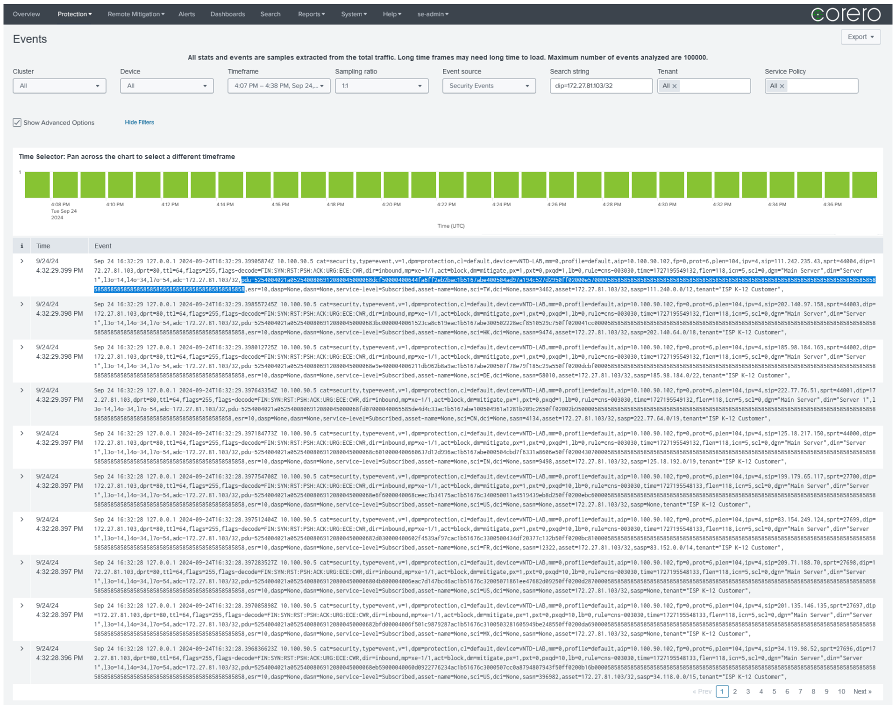
ICMP Type

No results found.

Reset selection(current=*)

Packet-Level Forensics

SecureWatch Analytics archives security event data down to the power distribution unit (PDU) level, enabling forensic analysis of ongoing and past threats for greater intelligence and compliance reporting on security activity. Authorized Users can analyze event data based on preset timescales (e.g., last day, week, or month) or select a very specific timeframe when investigating past events, for example.



Events

All stats and events are samples extracted from the total traffic. Long time frames may need long time to load. Maximum number of events analyzed are 100000.

Cluster	Device	Timeframe	Sampling ratio	Event source	Search string	Tenant	Service Policy
All	All	4:07 PM – 4:38 PM, Sep 24,...	1:1	Security Events	dip=172.27.81.103/32	All ×	All ×

☑ Show Advanced Options

Hide Filters

Time Selector: Pan across the chart to select a different timeframe

```
i  Time             Event
>  9/24/24          Sep 24 16:32:29 127.0.0.1 2024-09-24T16:32:29.39905874Z 10.100.90.5 cat=security,type=event,v=1,dpm=protection,cl=default,device=vNTD-LAB,mm=0,profile=default,aip=10.100.90.102,fp=0,prot=6,plen=104,ipv=4,sip=111.242.235.43,sprt=44004,dip=1
   4:32:29.399 PM   72.27.81.103,dprt=80,ttl=64,flags=255,flags-decode=FIN:SYN:RST:PSH:ACK:URG:ECE:CWR,dir=inbound,mp=xe-1/1,act=block,dm=mitigate,px=1,pxt=0,pxqd=1,lb=0,rule=cns-003030,time=1727195549132,flen=118,icn=5,scl=0,dgn="Main Server",din="Server
                    1",l3o=14,l4o=34,l7o=54,adc=172.27.81.103/32,pdu=5254004021a0525400806912080045000068dcf50000400644fa6ff2eb2bac1b5167abe400504ad97a194c527d2950ff02000e57000058585858585858585858585858585858585858585858585858585858585858585858585858585858585858
                    5858585858585858585858585858585858585858585858,esr=10,dasp=None,dasn=None,service-level=Subscribed,asset-name=None,sci=TW,dci=None,sasn=3462,asset=172.27.81.103/32,sasp=111.240.0.0/12,tenant="ISP K-12 Customer",
>  9/24/24          Sep 24 16:32:29 127.0.0.1 2024-09-24T16:32:29.398557245Z 10.100.90.5 cat=security,type=event,v=1,dpm=protection,cl=default,device=vNTD-LAB,mm=0,profile=default,aip=10.100.90.102,fp=0,prot=6,plen=104,ipv=4,sip=202.140.97.158,sprt=44003,dip=
   4:32:29.398 PM   172.27.81.103,dprt=80,ttl=64,flags=255,flags-decode=FIN:SYN:RST:PSH:ACK:URG:ECE:CWR,dir=inbound,mp=xe-1/1,act=block,dm=mitigate,px=1,pxt=0,pxqd=1,lb=0,rule=cns-003030,time=1727195549132,flen=118,icn=5,scl=0,dgn="Main Server",din="Server
                    1",l3o=14,l4o=34,l7o=54,adc=172.27.81.103/32,pdu=5254004021a05254008069120800450000683bc0000040061523ca8c619eac1b5167abe300502228ecf8510529c750ff020041cc000058585858585858585858585858585858585858585858585858585858585858585858585858585858585858
                    5858585858585858585858585858585858585858585858,esr=10,dasp=None,dasn=None,service-level=Subscribed,asset-name=None,sci=HK,dci=None,sasn=9474,asset=172.27.81.103/32,sasp=202.140.64.0/18,tenant="ISP K-12 Customer",
>  9/24/24          Sep 24 16:32:29 127.0.0.1 2024-09-24T16:32:29.398012725Z 10.100.90.5 cat=security,type=event,v=1,dpm=protection,cl=default,device=vNTD-LAB,mm=0,profile=default,aip=10.100.90.102,fp=0,prot=6,plen=104,ipv=4,sip=185.98.184.169,sprt=44002,dip=
   4:32:29.398 PM   172.27.81.103,dprt=80,ttl=64,flags=255,flags-decode=FIN:SYN:RST:PSH:ACK:URG:ECE:CWR,dir=inbound,mp=xe-1/1,act=block,dm=mitigate,px=1,pxt=0,pxqd=1,lb=0,rule=cns-003030,time=1727195549132,flen=118,icn=5,scl=0,dgn="Main Server",din="Server
                    1",l3o=14,l4o=34,l7o=54,adc=172.27.81.103/32,pdu=5254004021a052540080691208004500068e9e400004006211db962b8a9ac1b5167abe200507f78e79f185c29a550ff0200dcbf000058585858585858585858585858585858585858585858585858585858585858585858585858585858585858
                    5858585858585858585858585858585858585858585858,esr=10,dasp=None,dasn=None,service-level=Subscribed,asset-name=None,sci=DE,dci=None,sasn=58010,asset=172.27.81.103/32,sasp=185.98.184.0/22,tenant="ISP K-12 Customer",
>  9/24/24          Sep 24 16:32:29 127.0.0.1 2024-09-24T16:32:29.397643354Z 10.100.90.5 cat=security,type=event,v=1,dpm=protection,cl=default,device=vNTD-LAB,mm=0,profile=default,aip=10.100.90.102,fp=0,prot=6,plen=104,ipv=4,sip=222.77.76.51,sprt=44001,dip=17
   4:32:29.397 PM   2.27.81.103,dprt=80,ttl=64,flags=255,flags-decode=FIN:SYN:RST:PSH:ACK:URG:ECE:CWR,dir=inbound,mp=xe-1/1,act=block,dm=mitigate,px=1,pxt=0,pxqd=1,lb=0,rule=cns-003030,time=1727195549132,flen=118,icn=5,scl=0,dgn="Main Server",din="Server 1",l
                    3o=14,l4o=34,l7o=54,adc=172.27.81.103/32,pdu=5254004021a0525400806912080045000068fd07000040065585de4d4c33ac1b5167abe100504961a1281b209c2650ff02002b950000585858585858585858585858585858585858585858585858585858585858585858585858585858585858585858585858
                    585858585858585858585858585858585858585858,esr=10,dasp=None,dasn=None,service-level=Subscribed,asset-name=None,sci=CN,dci=None,sasn=4134,asset=172.27.81.103/32,sasp=222.77.64.0/19,tenant="ISP K-12 Customer",
>  9/24/24          Sep 24 16:32:29 127.0.0.1 2024-09-24T16:32:29.397184773Z 10.100.90.5 cat=security,type=event,v=1,dpm=protection,cl=default,device=vNTD-LAB,mm=0,profile=default,aip=10.100.90.102,fp=0,prot=6,plen=104,ipv=4,sip=125.18.217.150,sprt=44000,dip=
   4:32:29.397 PM   172.27.81.103,dprt=80,ttl=64,flags=255,flags-decode=FIN:SYN:RST:PSH:ACK:URG:ECE:CWR,dir=inbound,mp=xe-1/1,act=block,dm=mitigate,px=1,pxt=0,pxqd=1,lb=0,rule=cns-003030,time=1727195549132,flen=118,icn=5,scl=0,dgn="Main Server",din="Server
                    1",l3o=14,l4o=34,l7o=54,adc=172.27.81.103/32,pdu=5254004021a0525400806912080045000068c6010000400660637d12d996ac1b5167abe000504cbd7f6331a8606e50ff020043070000585858585858585858585858585858585858585858585858585858585858585858585858585858585858585858
                    5858585858585858585858585858585858585858585858,esr=10,dasp=None,dasn=None,service-level=Subscribed,asset-name=None,sci=IN,dci=None,sasn=9498,asset=172.27.81.103/32,sasp=125.18.192.0/19,tenant="ISP K-12 Customer",
>  9/24/24          Sep 24 16:32:28 127.0.0.1 2024-09-24T16:32:28.397754708Z 10.100.90.5 cat=security,type=event,v=1,dpm=protection,cl=default,device=vNTD-LAB,mm=0,profile=default,aip=10.100.90.102,fp=0,prot=6,plen=104,ipv=4,sip=199.179.65.117,sprt=27700,dip=
   4:32:28.397 PM   172.27.81.103,dprt=80,ttl=64,flags=255,flags-decode=FIN:SYN:RST:PSH:ACK:URG:ECE:CWR,dir=inbound,mp=xe-1/1,act=block,dm=mitigate,px=1,pxt=0,pxqd=10,lb=0,rule=cns-003030,time=1727195548133,flen=118,icn=5,scl=0,dgn="Main Server",din="Server
                    1",l3o=14,l4o=34,l7o=54,adc=172.27.81.103/32,pdu=5254004021a0525400806912080045000068e6f6000040068ceec7b34175ac1b51676c340050011a4519439eb8d250ff0200ebc6000058585858585858585858585858585858585858585858585858585858585858585858585858585858585858
                    5858585858585858585858585858585858585858585858,esr=10,dasp=None,dasn=None,service-level=Subscribed,asset-name=None,sci=US,dci=None,sasn=None,asset=172.27.81.103/32,sasp=None,tenant="ISP K-12 Customer",
>  9/24/24          Sep 24 16:32:28 127.0.0.1 2024-09-24T16:32:28.397512404Z 10.100.90.5 cat=security,type=event,v=1,dpm=protection,cl=default,device=vNTD-LAB,mm=0,profile=default,aip=10.100.90.102,fp=0,prot=6,plen=104,ipv=4,sip=83.154.249.124,sprt=27699,dip=
   4:32:28.397 PM   172.27.81.103,dprt=80,ttl=64,flags=255,flags-decode=FIN:SYN:RST:PSH:ACK:URG:ECE:CWR,dir=inbound,mp=xe-1/1,act=block,dm=mitigate,px=1,pxt=0,pxqd=10,lb=0,rule=cns-003030,time=1727195548133,flen=118,icn=5,scl=0,dgn="Main Server",din="Server
                    1",l3o=14,l4o=34,l7o=54,adc=172.27.81.103/32,pdu=5254004021a0525400806912080045000682d030000400602f4539af97cac1b51676c3300500434df20377c132b50ff0200bc81000058585858585858585858585858585858585858585858585858585858585858585858585858585858585858
                    5858585858585858585858585858585858585858585858,esr=10,dasp=None,dasn=None,service-level=Subscribed,asset-name=None,sci=FR,dci=None,sasn=12322,asset=172.27.81.103/32,sasp=83.152.0.0/14,tenant="ISP K-12 Customer",
>  9/24/24          Sep 24 16:32:28 127.0.0.1 2024-09-24T16:32:28.397283527Z 10.100.90.5 cat=security,type=event,v=1,dpm=protection,cl=default,device=vNTD-LAB,mm=0,profile=default,aip=10.100.90.102,fp=0,prot=6,plen=104,ipv=4,sip=209.71.188.70,sprt=27698,dip=1
   4:32:28.397 PM   72.27.81.103,dprt=80,ttl=64,flags=255,flags-decode=FIN:SYN:RST:PSH:ACK:URG:ECE:CWR,dir=inbound,mp=xe-1/1,act=block,dm=mitigate,px=1,pxt=0,pxqd=10,lb=0,rule=cns-003030,time=1727195548133,flen=118,icn=5,scl=0,dgn="Main Server",din="Server
                    1",l3o=14,l4o=34,l7o=54,adc=172.27.81.103/32,pdu=5254004021a05254008069120800450000006804b800004006eac7d147bc46ac1b51676c32005071861ee47682d09250ff0200d287000058585858585858585858585858585858585858585858585858585858585858585858585858585858585858
                    5858585858585858585858585858585858585858585858,esr=10,dasp=None,dasn=None,service-level=Subscribed,asset-name=None,sci=US,dci=None,sasn=None,asset=172.27.81.103/32,sasp=None,tenant="ISP K-12 Customer",
>  9/24/24          Sep 24 16:32:28 127.0.0.1 2024-09-24T16:32:28.397085898Z 10.100.90.5 cat=security,type=event,v=1,dpm=protection,cl=default,device=vNTD-LAB,mm=0,profile=default,aip=10.100.90.102,fp=0,prot=6,plen=104,ipv=4,sip=201.135.146.135,sprt=27697,dip
   4:32:28.397 PM   =172.27.81.103,dprt=80,ttl=64,flags=255,flags-decode=FIN:SYN:RST:PSH:ACK:URG:ECE:CWR,dir=inbound,mp=xe-1/1,act=block,dm=mitigate,px=1,pxt=0,pxqd=10,lb=0,rule=cns-003030,time=1727195548133,flen=118,icn=5,scl=0,dgn="Main Server",din="Server
                    1",l3o=14,l4o=34,l7o=54,adc=172.27.81.103/32,pdu=5254004021a05254008069120800450000682bfd00004006f501c9879287ac1b51676c3100503281605949be248550ff0200da69000058585858585858585858585858585858585858585858585858585858585858585858585858585858585858
                    5858585858585858585858585858585858585858585858,esr=10,dasp=None,dasn=None,service-level=Subscribed,asset-name=None,sci=MX,dci=None,sasn=None,asset=172.27.81.103/32,sasp=None,tenant="ISP K-12 Customer",
>  9/24/24          Sep 24 16:32:28 127.0.0.1 2024-09-24T16:32:28.396836623Z 10.100.90.5 cat=security,type=event,v=1,dpm=protection,cl=default,device=vNTD-LAB,mm=0,profile=default,aip=10.100.90.102,fp=0,prot=6,plen=104,ipv=4,sip=34.119.98.52,sprt=27696,dip=17
   4:32:28.396 PM   2.27.81.103,dprt=80,ttl=64,flags=255,flags-decode=FIN:SYN:RST:PSH:ACK:URG:ECE:CWR,dir=inbound,mp=xe-1/1,act=block,dm=mitigate,px=1,pxt=0,pxqd=10,lb=0,rule=cns-003030,time=1727195548133,flen=118,icn=5,scl=0,dgn="Main Server",din="Server
                    1",l3o=14,l4o=34,l7o=54,adc=172.27.81.103/32,pdu=5254004021a0525400806912080045000068eb59000040060d0922776234ac1b51676c3000507cc0a8794807943f50ff0200b16b000058585858585858585858585858585858585858585858585858585858585858585858585858585858585858
                    5858585858585858585858585858585858585858585858,esr=10,dasp=None,dasn=None,service-level=Subscribed,asset-name=None,sci=US,dci=None,sasn=396982,asset=172.27.81.103/32,sasp=34.118.0.0/15,tenant="ISP K-12 Customer",
```

Events include all the metadata extracted by the SmartWall ONE system as well as the first 200 bytes of the packet which the attack comprised of. In addition, PDU data from security and sFlow events can be extracted to a file for import to third-party applications, such as Wireshark for further forensic analysis.

Open Integration

SecureWatch Analytics (SWA) leverages the APIs and JSON formatted syslog event feeds of SmartWall ONE's open architecture to deliver forensic-level attack analysis and closed-loop autonomic protection. It is built on top of a self-contained Splunk instance, which is included with every SmartWall ONE solution, to deliver its powerful, flexible and easily customizable attack analysis and reporting.

Users with their own Splunk Enterprise instance can leverage that directly by running the SWA application on it and consuming the SmartWall ONE feeds directly. Users with a SIEM or other security platform can directly consume the SmartWall ONE JSON formatted syslog feed which delivers all the same detailed information which is available from SWA.

Technical Specifications

Management		
Web-Based GUI	Programmatic API	Secure Authentication
HTTPS Access through Portal Login Page	JSON-Based REST	Role-Based Access via LDAP
Physical Environmental		
Hypervisors	Minimum Requirements	
KVM running on Red Hat Enterprise Linux 7+, CentOS, Ubuntu 20.04+, Debian 11+, Rocky 9+ or Alma 9+ VMware ESXi 7+	8 Cores, 32GB Memory, 310GB Disk	

Learn more About SecureWatch Analytics

SecureWatch Analytics was developed with the deep security experience and knowledge of Corero's security analysts that deliver our market leading SecureWatch service. SecureWatch Managed is a comprehensive suite of DDoS configuration optimization, monitoring and response services. As a trusted advisor, Corero extends this security expertise to our customers and partners to better defend against cyber-crime.

About Corero Network Security

Corero Network Security leads in adaptive, cost-effective DDoS protection, ensuring uninterrupted availability for critical online services. Unlike conventional approaches, our software-defined solution mitigates threats in real-time directly in the data path, using high-speed processing and predictive automation, validated by a 24x7 SOC. With flexible hybrid deployment options, Corero offers superior protection at lower costs without extensive technical expertise. Our real-time threat intelligence and proactive mitigation provide unparalleled visibility and security, allowing businesses to focus on their core operations.