Network Security

Protect your network infrastructure and its users from online threats, and build a network that fights back

Sandvine's Network Security product delivers carrier-grade protection of subscribers and network resources at scale, with the flexibility to be deployed as a virtualized system, and advanced network threat deception capabilities that materially increase the costs of malicious network activities for the actor making an attack on the network or subscribers less economically feasible.

With capabilities delivered through three unique feature sets: Network Protection, Subscriber Protection, and Web Content Intelligence, Sandvine's Network Security product enables communications service providers (CSPs) to address a wide array of network threats, infections, and vulnerabilities.

Additionally, Sandvine's Network Security product includes several features to protect your network, and your subscribers from online threats and malicious activity, including:

Accuracy

Sandvine's traffic classification technology emphasizes zero false positives to ensure no harmful impact to the network or users when you enable mitigation/defenses.

Asymmetry Aware Detection

Detects attacks in networks where asymmetric traffic is prevalent; when the inbound traffic is seen by one Policy Traffic Switch (PTS) element, and the outbound traffic is handled by another Policy Traffic Switch (PTS) element.

Attack Traffic Protection

Provides protection for single-origin or distributed denial of service attacks: SYN flood, flow flood, bandwidth flood, fragmented SYN, and reflector attack detection and mitigation.

Behavioral Signatures

Detects threats based on traffic behaviors, and is not reliant on specific attack signatures (so the network is always protected against zero-day attacks):

- Multi-factor analysis: Detections include analysis of measurements of source IPs, source ports, destination IPs, destination ports, and transport protocol; different attack detections rely on different thresholds and ratios applied to different factors; outbound email detection is based on analysis of a multitude of email-specific factors.
- Sampling thresholds: Configurable sampling thresholds, over configurable periods of time, and intelligence normalization.

Carrier-Grade Performance

Network Security is specifically designed to perform in carrier-grade environments, and can handle large-volume attacks greater than 1 terabit per second; since the Sandvine platform scales to support the world's largest networks, your network-based filtering works no matter your bandwidth volume.

CSP-Defined Filtering Lists

Define your own white/black/grey lists of up to 150 million URLs, depending on your network's unique requirements.

EMS/NMS Alarms

Trigger SNMP alarms based on detections that alert an EMS or NMS systems (as well as the operator) to a network threat.

Network-Based Filtering/Defense

Since content filtering and threat mitigation actions are performed in the network, without any dependency on client device, software, or operating system, they are very difficult to bypass.

Network Processing Unit (NPU) Mitigation

Sandvine delivers detection and mitigation at the hardware level using the Network Processing Unit (NPU) for large scale, volumetric attacks beyond 400Gbps.

Mitigation and Enforcement Flexibility

Once threats or requests for harmful or restricted content are detected, a range of actions can be taken, including: log, report, notify, block, flow rate-limit, BGP flow spec (well-suited for 'scrubbing' use cases), mark, divert, and tee to file. These can be applied with varying degrees of automation:

- Alarm: notify operations personnel about threatening activity.
- Manually block: monitor detected threats in real time and selectively block as needed.
- Automatically block: automatically take action to limit or block detected threats.

QuickSand

Provide malicious actors with deceptive information that materially increases the costs of malicious network activities to the attacker, making network attacks less economically feasible. This feature uses multiple network threat deception techniques:

- Network Scale Tarpitting: Slows down the propagation of attacks, and malicious activity by acknowledging requests made by malicious actors with information that falsely suggests progress while the attack is actually being mitigated.
- Dynamic Vulnerability Masking: Identifies users and servers that are running vulnerable software versions, and leverages Sandvine's SandScript capabilities to dynamically mask this information, making it appear that the vulnerable software is running a version which does not contain the vulnerability, deceiving the attacker into not proceeding.

Real-Time Threat Visibility, Historical Reporting, and Audit Records

Security events are logged and can be used for audit purposes or examined for business and operational intelligence. Historic reports are available within Sandvine's Network Demographics reporting interface, and Sandvine's Control Center provides real-time visibility into ongoing threats for operational analysis.

Sandvine Policy Engine

- Subscriber awareness: Subscriber-specific policies integrated with Sandvine behavioral policies, threat intelligence feeds from reputable third-party sources, and any variety of additional conditions and actions, to enable stateful cyber security use cases and revenue-generating services.
- Automatic updates: Threat intelligence feeds from reputable third-party sources are automatically updated four times a day, so your network is always current without any manual intervention.
- Zero latency: Threat detection and policy enforcement response occurs in microseconds.

Threat and Infection Notifications

- The Sandvine platform is completely subscriber-aware, allowing CSPs to engage subscribers with personalized security notifications to prevent scams and infections. Advanced notifications can be achieved by linking Network Security with Sandvine OutReach.

NETWORK PROTECTION

Sandvine's Network Protection capability allows operators to identify a wide range of network threats in real time for reporting and mitigation to provide specialized protection.

Address and Port Scan Protection

Detects and prevents address-scans, which are commonly conducted by machines infected with malware.

Bandwidth Flood Prevention

Provides protection for bandwidth floods by detecting when a subscriber's received traffic exceeds a threshold that is configured to be the max of what it could possibly generate legitimately.

DNS Cache Poisoning Protection

Leverages Sandvine's DNS analyzer to ensure the correct DNS information is returned by the DNS server to prevent an infected server from spoofing the DNS request and redirecting an unsuspecting user to a malicious site.

Flow Flood Prevention

Provides protection for flow flood attacks that attempt to overwhelm the target's flow state memory.

Fragmentation Attack Detection/Mitigation

Enables operators to detect and mitigate fragmentation attacks (a form of DOS attack in which the actor looks to overwhelm the network by exploiting the datagram fragmentation mechanisms – a necessary component of data transmission), increasing their level of protection against a greater number of potential network threats.

Malware Scanning Protection

IP Address and port scanning detection and mitigation.

Outbound Spam Protection

Stops outbound email spam by combining 12 metrics and measurements in configurable and customizable ways to address the uniqueness of the network while achieving the desired level of network security vigilance according to the CSP's operational/security objectives.

Precision DoS/DDoS Attack Prevention

The Sandvine platform inspects every subscriber flow, without flow sampling to detect and mitigate large volumetric attacks as well as the more precision, or surgical DDoS attacks and stop them in real-time.

Reflector Attack Prevention

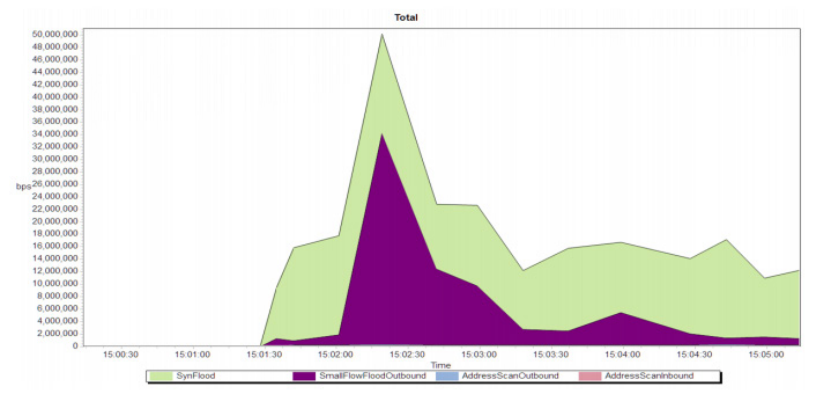
Uses precisely-tuned, behavior-based algorithms to stop reflector attacks that attempt to overwhelm a victim by spoofing their IP address and sending many queries to Domain Name Servers (DNS) or NTP elements, subsequently flooding the victim with an avalanche of responses.

SYN Flood Prevention

SYN floods overwhelm the target's ability to process SYN packets. Sandvine's Network Protection feature detects symptoms exhibited by a server under a DDoS attack by analyzing the ratio of aborted flows to total flows.

Figure 1

This screenshot from Control Center's PowerView feature displays a real-time report for SYN flood and address scan activity that shows a SYN flood attack occurring in real time. The same real-time detections that power this chart serve as conditions within the Sandvine Policy Engine – conditions that can be linked to mitigation actions.



SUBSCRIBER PROTECTION

Sandvine's Subscriber Protection feature enables operators to identify a wide range of subscriber cyber security threats in real-time for reporting and mitigation.

Botnet Detection and Disruption

Detects devices that are part of a botnet, blocking communication with botnet command and control (C&C) servers.

Malware Infection Protection

Detects malware download and infection attempts from known malicious sources in real-time.

Spoofing and Phishing Prevention

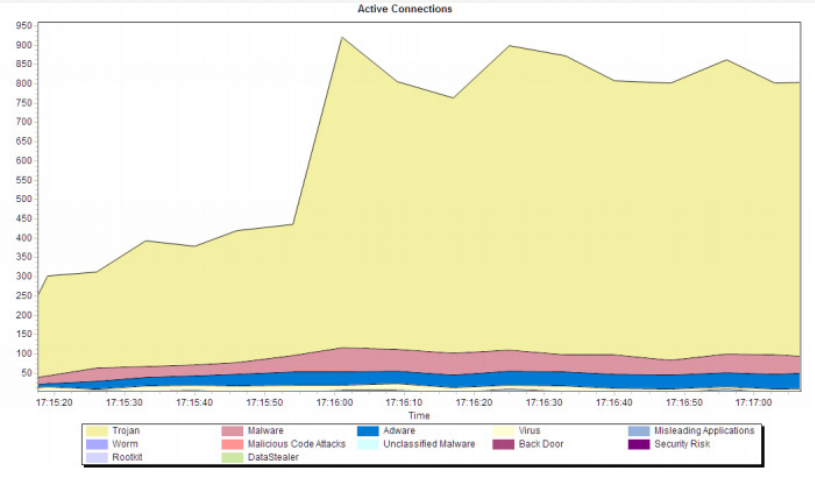
Automatically detects attempts to access known phishing websites and can detect and prevent attempts to spoof DNS responses, IPs or ports.

Threat and Infection Notifications

When combined with Sandvine's Subscriber Engagement product, OutReach, threat and infection notifications can be sent automatically to subscribers when malicious traffic or known vulnerabilities are detected.

Figure 2

This screenshot from Control Center's PowerView shows a real-time view of active malware a small CSP's network. The same real-time detections that power this chart serve as conditions within the Sandvine Policy Engine – conditions that can be linked to mitigation and remediation actions.



WEB CONTENT INTELLIGENCE

Sandvine Web Content Intelligence enables operators to implement network-based filtering of web browsing content, with filtering based on URL and/or topic-based categories.

Parental Controls

Provides dynamic categorization, keyword blocking, user- and page-level granularity, and other advanced features drive a positive user experience and enhanced revenue opportunities across business and residential customers.

URL Access Control Provides network-based web filtering for more than 150-million URLs.

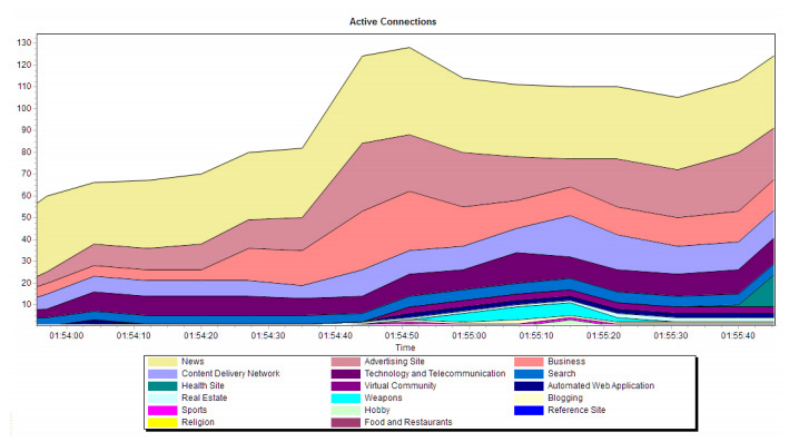
Web Filtering Service Delivery Flexibility

Enables CSPs to deliver web filtering services that align with their strategy; for example:

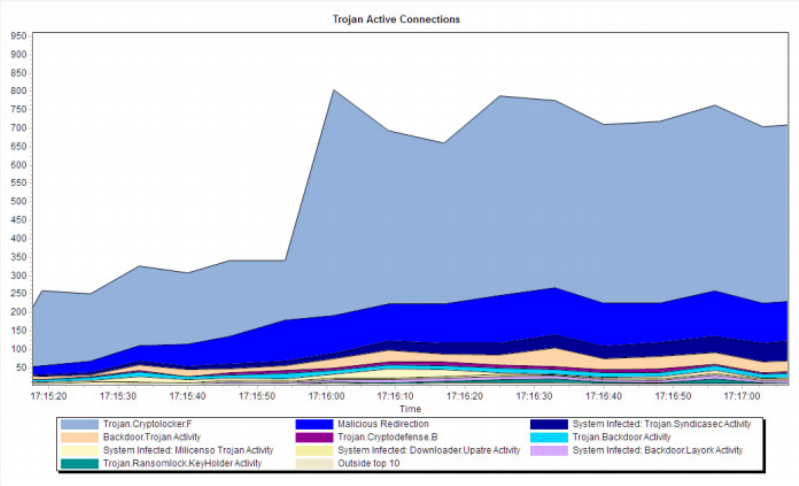
- A global policy applied to all network users.
- Pre-configured policies offered to consumers and/or businesses on an opt-in basis.

Figure 3

This screenshot from Control Center's PowerView shows a real-time view of active connections to Web Content Intelligence categorized flows. The same real-time detections that power this chart serve as conditions that trigger filtering of web content for regulatory and service creation use cases.



This screenshot from Control Center's PowerView shows a real-time view of active Trojans on a small CSP network. The same real-time detections that power this chart serve as conditions within the Sandvine Policy Engine – conditions that can be linked to mitigation and remediation actions.



v20180124

ABOUT SANDVINE

Sandvine helps organizations run world-class networks with Active Network Intelligence, leveraging machine learning analytics and closed-loop automation to identify and adapt to network behavior in real-time. With Sandvine, organizations have the power of a highly automated platform from a single vendor that delivers a deep understanding of their network data to drive faster, better decisions. For more information, visit **sandvine.com** or follow Sandvine on Twitter at **@Sandvine.**

SANDVINE

USA
47448 Fremont Blvd,
Fremont,
CA 94538,
USA
T. +1 510.230.2777

EUROPE
Birger Svenssons Väg
28D
432 40 Varberg,
Sweden
T. +46 (0)340.48 38 00

CANADA
408 Albert Street,
Waterloo,
Ontario N2L 3V3,
Canada
T. +1 (0)519.880.2600

ASIA
Ardash Palm Retreat,
Bellandur, Bangalore,
Karnataka 560103,
India
T. +91 80677.43333