Executive Summary
The term cyber security describes a wide range of issues and solutions related to protecting communications service providers (CSPs), residential subscribers and business customers from malicious Internet activity and harmful content. Examples of cyber security threats include:

- Illegal and harmful web content
- Phishing scams
- Malware infections and scanning activity
- Distributed Denial of Service (DDoS) attacks
- Outbound spam
- Botnets

While CSPs are stuck with the cost of transporting ‘bad packets’ and fielding support calls from frustrated subscribers with infected devices, the business market is demanding what Frost & Sullivan call ‘secure pipes’ through a carrier-grade cyber security solution embedded at the heart of CSP network. This paper provides a comprehensive guide to Sandvine’s ‘secure pipes’ solution for CSPs - our Network Security product.
Introduction to Secure Pipes

The CSP’s network itself is often overlooked as a valuable layer of protection against cyber security threats. The concept of ‘clean Pipes’ is about removing DDoS attack traffic from the CSP network while allowing everything legitimate to pass through. While most agree that less DDoS hitting residential subscribers and businesses is a good thing, the challenge has been how to achieve this goal for all cyber threats (not just DDoS) in a cost-effective manner for CSP networks of all sizes. In a January 2015 Executive Brief titled “Secure Pipes: Changing the Expectation of Your Internet Service Providers”, Frost & Sullivan renews the call for CSPs to take a central role in implementing the next generation of cyber security for the public Internet, which they call secure pipes:

> Essentially, the concept behind a Secure Pipe is to build rather than to bolt-on security into the communication services and, with this pivot, change the expectations around what Internet service providers (ISPs) deliver. Why should an organization apply security at its business locations and Web properties when the ISP can examine and filter incoming traffic before landing at the doorsteps of its customers? Water is filtered and cleaned before it reaches consumers’ taps. We expect electricity to be safe and reliable at the flip of a switch. Why would we not have the same expectation in the flow of Internet traffic?

Network Layers - Private and Public

Cyber security solutions are primarily concerned with reducing or filtering out ‘all of the bad stuff’ that could cross the boundary between the untrusted public Internet and a trusted private network (e.g., a residential subscriber’s home network or the private network of a business). Much of the historic focus in dealing with this challenge has been on solutions that sit at the ‘front door’ of a private network and act as gatekeeper/protector between that which is ‘untrusted’ and that which is ‘trusted’. Frost & Sullivan argue that the market is demanding a paradigm shift from the fractured kaleidoscope of traditional approaches that present an ‘every solution for itself’ mentality focused on the doorstep of a private network to a complementary approach that puts the CSP center-stage as a critical cyber-defender.

---

1 See this article, which summarizes the Frost & Sullivan report.
Network Security

Sandvine’s Network Security product recognizes and responds to costly threats as they appear in real-time for the following benefits:

- **Lower Support Costs:** reduce support calls and retain existing subscribers by blocking attack traffic, infection rates, and harmful content, and by initiating stateful remediation workflows.
- **Increased Revenue:** Offer value-added ‘secure pipes’ services and attract new subscribers to a CSP that emphasizes a safe Internet experience.
- **Valuable Insight:** Understand the threat landscape with detailed historic and real-time cyber security reporting.
- **Regulatory Compliance:** Quickly and cost-effectively comply with filtering regulations.

![Diagram of Network Security](image)

Clean and Secure Pipes From Within the CSP Network

Reduce the cost of transporting bad packets while preventing threats from ever reaching the subscriber’s front door. With Network Security, CSPs can rapidly implement a wide range of valuable cyber security use cases for both residential and business customers, including:

- DDoS attack protection
- Botnet disruption
- Outbound email spam protection
- Malware scanning protection
- Malware prevention
- Phishing prevention
- Regulatory URL filtering
- Web filtering services
- Subscriber notification
- Infection remediation support
- Cyber security analytics
  - Real-time malicious traffic monitoring
  - Detailed operational reporting and auditing
Secure Pipes with Network Security

Behavioral Threat Detection
Using behavioral policies that can be tailored for individual subscribers and subscriber classes, Network Security detects a range of threats including:

- Single-origin or distributed denial of service attacks: SYN flood, flow flood, bandwidth flood, and refector attack
- Malware scanning: Address and port scan detection and mitigation
- Outbound email spam: Mitigation of email spam using the CSP’s mail servers (protocol-based port locks can also be applied to prevent connections to remote email servers)

DDoS Attack Protection
Sandvine’s Network Security product delivers a third-generation clean pipe technology to automatically identify and eliminates Layer-3/4 DDoS attacks like SYN floods, flow floods, and bandwidth floods, as well as IP-spoofing reflector attacks (e.g., DNS, NTP) that trick network resources into attacking subscribers. This inline solution uses behavioral heuristics to detect high-volume attacks for reporting and alarm notification, with both manual and automatic mitigation options.

Example – flow flood mitigation
A flow flood is a Layer-3/4 attack typically directed towards a specific host and port (subscriber device port). To detect a flow flood, a policy might measure the absolute number of completed new flows per second per period to a single target. For example:

- Block unsolicited inbound flows towards the destination port
- Since a flow flood attempts to overload a single target with completed TCP connections, the source can also be used.
- Allow traffic destined to other ports
- Allow subscriber-initiated traffic

Figure 3 - How Behavioral Threat Detection Works
Example - SYN flood mitigation

SYN floods are also typically directed at a specific host address and port, and are often part of a flow flood exhaustion attack. A behavioral policy can isolate true attacks from normal Internet traffic without false positives or the missed positives associated with signature-based approach. As just one example, to detect a SYN flood a policy might:

- Measure the ratio of failed connection attempts to total connection attempts on a specific target (applies to singular DoS attacks and coordinated DDoS attacks):
  - 70 percent of initiated connections must not be completed per 15 second period
  - Before this threshold is applied, a minimum of 15 packets per second must be observed
- Determine if the SYN Floods is part of a larger attack flow flood attack.
- Specify residential or business subscribers exempt from the policy

To block these kinds of attacks based on source is inapplicable because the attack does not rely upon a completed connection. To mitigate a SYN flood, a policy might:

- Block SYN packets directed at a specific destination address and port
- Mitigate by stopping the over-arching flow flood attack the SYN flood is supporting

Reflector Attack Protection

A reflector attack spoofs the victim’s IP in many queries to Domain Name Server (DNS) elements or NTP elements both inside and outside your network, and then the elements send an avalanche of DNS replies to the intended victim to overwhelm subscriber computers and frustrate their service experience. Behavioral Intelligence can inspect DNS and NTP traffic and detect the tell-tale signs of a reflector attack. Once detected, reflector attacks can be mitigated by blocking unsolicited traffic inbound to the subscriber (attack target) while leaving outbound traffic untouched.

Malware Scanning Protection

Malware programs scan network addresses and ports to find vulnerable connected devices, and then use an exploit to infect the target. Sandvine’s malware scanning protection solution recognizes malware scanning behavior in real-time and can limit or block the activity, thereby disrupting the formation of botnets, preventing subscriber infections and protecting the network infrastructure.

Example behavioral policy

- For outbound scanning, 15 IPs scanned per second adds the source to a short-list of suspected malware scanners
- For inbound scanning, 10 IPs scanning per second, adds the source to a shortlist of suspected malware scanners
- For a group of address scans to be considered an attack, they must appear in at least 40 percent of a 30-second sample
- The activity will be considered an attack until at least 5 minutes have passed during which the thresholds are not met

Outbound Spam Protection

For many communications service providers (CSPs), the top security problem is outbound email spam: watchdog groups blacklist entire networks when the spam problem is considered severe, resulting in email disruption for all of the network’s subscribers. Sandvine’s use of highly-tunable behavioral policy
Secure Pipes with Network Security

overcomes the shortcomings of Bayesian filters and port lockdowns, and identifies spammers based on behavioral characteristics rather than content specifics. CSPs are able to mitigate spam, including blocking or rate-limting SMTP connections from spammers and presenting infected subscribers with a message notifying them of the problem and a path to removing spam-causing threats.

Behavioral Threat Analytics

Behavioral Intelligence reporting includes detailed, real-time threat monitoring with the ability to selectively block observed threats, and historic reporting for auditing and analysis.

![Graph showing real-time monitoring of DDoS, Malware Scanning, and Outbound Spam](image)

**Figure 4 - Real-time Monitoring of DDoS, Malware Scanning, and Outbound Spam**

Subscriber Protection

Subscriber Protection allows CSPs to deploy a solution that prevents malware infections and phishing scams while also disrupting the operations of botnet command and control servers.

![Diagram showing how Subscriber Protection Works](image)

**Figure 5 - How Subscriber Protection Works**
Secure Pipes with Network Security

**Malware Infection Prevention**

For the residential subscriber, the only protection from malware threats has been traditional anti-virus software for their devices. IT security experts manage a wide range of solutions to protect their private networks, including intrusion detection and prevention solutions, firewalls, unified threat management systems, and security information and event management solutions. All of these solutions are designed to detect and block threats as they arrive at the boundary between the public Internet and a private network, or well after they’ve installed themselves and begun to do damage.

**Stop malware from ever reaching the customer’s front door**

Sandvine’s malware prevention solution complements existing endpoint and private network security solutions by automatically detecting malware download and infection attempts in real time, and before infection can take place. Upon detecting threatening browsing activity, including both solicited and unsolicited malicious software downloads, Sandvine can proactively notify subscribers that they are at risk and/or block the malicious software from traversing the network.

**Phishing Prevention**

If you’re reacting to a phishing attack, it means the damage is likely already done and the cost and stress are related solely to the cleanup effort. Sandvine’s phishing prevention solution automatically detects attempts to access known phishing websites. Upon detecting threatening browsing activity, the solution can notify subscribers that they are at risk and/or block access to a known phishing site.

**Botnet Disruption**

This solution allows CSPs to strike at the heart of botnet operations by detecting devices that are part of a botnet, blocking communication with botnet command and control, and getting in touch with subscribers to initiate a solution.

**Subscriber Protection Analytics**

Subscriber Protection reporting includes detailed, real-time threat monitoring with the ability to selectively block observed threats, and historic reporting for auditing and analysis.

![Figure 6 - Real-time Monitoring of Active Trojan Connections](image-url)
Web Content Intelligence

Web Content Intelligence allows CSPs to quickly comply with web filtering regulations. The solution also allows CSPs to deploy cost-saving web filtering services for residential subscribers, and revenue-generating web filtering services for business subscribers.

Figure 7 - How Contextual Intelligence Works

Regulatory Web Filtering

Most countries have strict regulatory requirements that require CSPs to block a blacklist of illegal URLs (websites). In many places, public institutions such as schools and libraries are encouraged to block specific subjects with the promise of government funding subsidies. Similarly, many business organizations that offer public WiFi (e.g., hotels, airports, coffee shops, etc.) need to enable public access to the Internet without worrying about being liable for inappropriate content.

With Sandvine, CSPs can block specific URLs and allows businesses and subscribers to manage access to over 100 web browsing subjects to enable full compliance with regulations.

Examples of categories that can be filtered include blocking child pornography sites or blocking subjects like “drugs”, “weapons”, and “violence”.

Web Filtering Services

CSPs, businesses, and subscribers have various reasons for wanting to filter out specific URLs and categories of web content. These include increasing employee productivity, protecting employees from content not appropriate for the workplace, protecting general subscribers in specific cultures and locales from offensive content, and offering parents the power to control what their children see online. In addition, endpoint solutions can be bypassed by the device user, which is something many businesses and parents would like to prevent. Sandvine allows CSPs to deploy a network-side solution for businesses and subscribers to block URLs and filter over 100 web browsing subjects that cannot be bypassed, and with no need for end-client software.

---

2 CSPs can define their own white/black/grey lists of up to 150 million URLs.
Sandvine allows CSPs to deliver network-based web filtering services as:

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

**Web Content Intelligence Analytics**

Web Content Intelligence reporting includes detailed, real-time monitoring of subscriber browsing activity and historic reporting for marketing profiling and analysis.

---

**Figure 8 - Offer Pre-Configured, Network-based Web Filtering Services**

**Figure 9 - Real-time Monitoring of Subscriber Browsing Preferences by Subscriber or Network-wide**
Secure Pipes Example - Destroying Botnets

Sandvine’s support for preventative and threat recognition and mitigation policies helps squeeze botnets and their negative effects out of carrier networks, including malware infection prevention, phishing prevention, malware scanning protection, DDoS attack protection, and outbound spam mitigation.

![Diagram of Network Security](image)

**Figure 10 - Destroying a Botnet**

Additional Network Security Features

Network Security supports the following additional features:

**Sandvine Policy Engine**

The Sandvine Policy Engine platform offers the following key features in the context of Network Security.

- **Subscriber awareness**: Subscriber-specific policies integrated with Symantec intelligence feeds, Sandvine behavioral policies, and any variety of additional conditions and actions, to enable stateful cyber security use cases and revenue-generating services
- **Zero latency**: Threat detection (including harmful content) and policy enforcement response occurs in microseconds
- **Automatic database updates**: Symantec intelligence feeds are automatically updated four times a day, so your network is always current without any manual intervention

**Enforcement Flexibility**

Once threats and requests for illegal or harmful 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
Carrier-Grade Performance and Accuracy
The Sandvine platform scales to support the world’s largest networks, so your network-based filtering works no matter your bandwidth volume. Network Security is specifically designed to perform in carrier-grade environments, and can handle large-volume attacks greater than 1 terabit per second. Sandvine’s traffic classification technology emphasizes zero false positives to ensure no harmful impact to network users.

Subscriber Notification and Remediation
The Sandvine platform is completely subscriber-aware, allowing CSPs to engage subscribers with personalized security notifications. Advanced notifications (e.g., self-service for remediation) can be achieved by linking Network Security with Sandvine OutReach.
Conclusion

Sandvine’s Network Security solution is embedded inside public network layers to address a broad range of cyber security issues inside the CSP network, including malware and phishing, harmful content, malware scanning, DDoS attacks and outbound spam.

Network Security offers a single scalable and completely centralized point of control for detecting and managing threats. Whether offered as a paid service or deployed globally across the network, the ability to stop harmful traffic before it ever gets to the subscriber’s front door through secure pipes is a win for everyone involved.

Related Resources

For a comprehensive overview of cyber security and concept of secure pipes, please see the Sandvine whitepaper “Cyber Security Considerations and Techniques for Network-based Protection.”