

Network Protection

Protecting your Infrastructure Investment

Broadband providers invest heavily in their networks, enabling subscribers to benefit from the promises of the Internet. Media streaming, rich and interactive communication, online gaming, content acquisition and distribution - these services are all delivered over today's networks. Subscribers have embraced these applications and are increasingly reliant on them as valued components of daily life.

A minority of Internet users have found other ways in which to put the network to work: launching debilitating attacks at networks and specific targets, delivering billions of unwanted e-mails, hijacking the computers of other subscribers - these are only a few examples of the malicious uses of broadband networks.

The cost of this misuse is staggering, both in terms of money and the human impact. Service providers, especially, are faced with the financial burdens created by malicious use of their network resources, including:

- Support calls resulting from symptoms of infection and attack
- Addressing complications arising from e-mail and IP blacklisting, major contributors to subscriber churn
- Operational expenses to protect and restore network services
- Campaigns to contact and educate infected subscribers

Each of these cost centers could be significantly reduced by introducing a layer of intelligence in the network to recognize and respond to threats as they appear in real-time, and to specifically contact only those subscribers who are infected with or impacted by malicious activities.

Many network operators are familiar with defenses such as firewalls, intrusion prevention systems, and anti-virus software, all of which are important elements in an over-all strategy of preserving network integrity; however, none of these technologies is designed to specifically address security issues and the requirement for immediate response facing today's service providers at the scale of modern networks.

Network Defense on the Policy Traffic Switch

Sandvine's Network Protection product is different. By working exclusively with Internet service providers to understand the security issues they face, Sandvine has designed a security product that is ideally suited to identifying and mitigating the unique set of threats that exist on broadband networks.

A defense strategy built on Sandvine's Policy Traffic Switch scales to any network size and any number of asymmetric links, allowing the solution to focus on the tasks at hand:

- Identifying and blocking sources of outbound e-mail spam
- Preventing worms from spreading on the network
- Detecting and blocking Denial of Service attacks

Furthermore, the subscriber-awareness native to the Policy Traffic Switch allows providers to identify subscribers who have fallen victim to malicious software, regardless of dynamic IP addresses. When coupled with Sandvine's web redirection capabilities this intelligence enables targeted communication with infected subscribers, ensuring that they land on a branded education page or a similar portal.

Key Benefits

- Reduces operational costs resulting from security incidents
- Protects infrastructure investment by preserving the network's capacity to deliver services
- Prevents blacklisting by identifying and blocking sources of e-mail spam
- Mitigates zero-day attacks - never wait for a signature update again
- Enables targeted interaction with infected subscribers, lowering the cost and guaranteeing your message and brand are seen

Protecting your Infrastructure Investment

Sandvine recognized early on that the security challenges facing broadband Internet providers are unlike those faced by Enterprises, Universities, or any other organizations. The network itself is vastly different in terms of scale, trust, and operational restrictions; the users place different demands; and the mix of traffic is much more diverse.

Sandvine pioneered the behavioral approach to network protection that is gaining widespread acceptance as the only realistic defense against modern malware. By building a layer of intelligence into the network itself, a layer that is capable of catching diverse and zero-day threats, we believe that a service provider can dramatically reduce the expenses associated with protecting a network's operational integrity.

Never wait for a signature update

Historically, network security placed an emphasis on signatures. How many do you have? How many can you apply? How fast can you deliver updates? The reality is that signatures are hopelessly ineffective against a rapidly evolving threat. A library of tens of thousands of signatures is useless against the worm released 15 minutes ago. How long is too long to wait for a signature update, and when you get one will the new signatures be effective?

The algorithms at the heart of Sandvine's Network Protection product examine the behavior exhibited by network traffic, not the specific patterns of 1s and 0s, in order to identify the tell-tale signs of infection. Until worms stop trying to scan for vulnerable hosts, or spammers stop trying to send e-mail, behavioral algorithms will remain effective against zero-day and known threats.

How much spam is leaving your network?

By applying patented behavioral algorithms to all outbound mail traffic, regardless of port or destination, and by identifying or locking down popular evasive mechanisms such as spam relays, Sandvine can identify abusive machines on the network and block or limit their mail traffic.

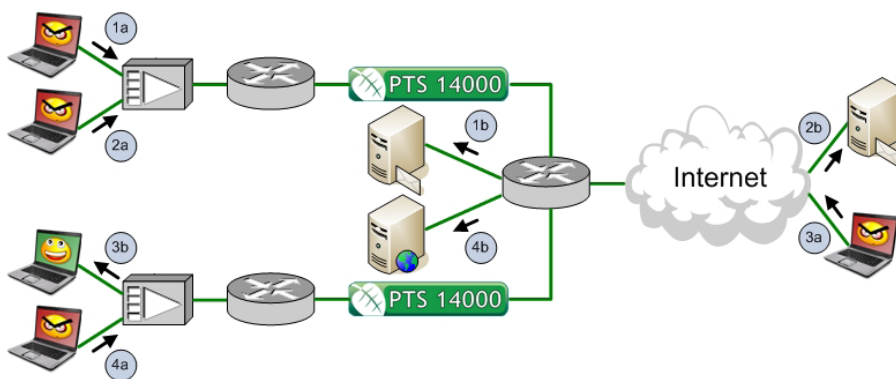
Other advantages of Sandvine's behavioral spam identification algorithms include:

- Advanced protocol detection identifies all mail traffic, regardless of port and destination
- Deployment is possible anywhere in the network where mail traffic is carried
- Behavioral algorithms are content-agnostic and fully customizable, and never play the catch-up game

Build brand loyalty by engaging with subscribers

The Policy Traffic Switch can redirect web sessions to specific destinations based on definable variables. When combined with the per-subscriber awareness and the threat detection capabilities of the Network Protection product, this feature allows service providers to engage with specific subscribers. For example, a service provider can:

- Quarantine infected subscribers on a landing page providing information about a malware infection, links to software updates and educational resources
- Redirect subscribers impacted by an attack to a care portal describing the incident and detailing the provider's efforts to resolve the situation



1. A spam Trojan (1a) connecting to the local mail server (1b)
2. A spam Trojan (2a) connecting to a foreign mail server (2b)
3. An external user (3a) attacking a local subscriber (3b)
4. An infected subscriber (4a) being redirected to a custom landing portal (4b)