Cyber Security: Considerations and Techniques for Network-Based Protection

Contents

An Industry Whitepaper

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 describes the wide variety of solutions that CSPs and enterprise Internet security professionals are juggling today, and explains the many advantages of using network policy control to deliver secure pipes to residential subscribers and business customers.

Version 2.0

sandvine
Intelligent Broadband Networks

Introduction to Cyber Security

The term cyber security describes a wide range of issues and solutions related to protecting communications service providers (CSPs), businesses and subscribers from malicious Internet activity and harmful content. Cyber attackers are enjoying a renaissance with the increasing availability of bandwidth, connected devices, and affordable attack tools that allow them to launch ever-more complex and potent attacks against a CSP's residential subscribers and businesses.[1]

Companies reported an average of $1.5 million in costs related to DDoS over the past 12 months, with 82% of survey respondents saying attacks have shut down all or part of their data center and that the main consequence beyond revenue loss is reputation damage.[2] Malware alone was a $491 billion cost to residential subscribers and businesses in 2014[3] and phishing attacks are on the rise, with more than 70000 unique scams reported in 2012 as compared to 320000 in 2014.[4] The botnet – a network of thousands to millions of compromised 'zombie' machines used to conduct attacks - is the over-arching menace that reinforces and sustains these damaging threats.

Secure Pipes – the CSP as Cyber Protector

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[5], 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.[6] 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?*[7]

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 to

---

[1] See this article detailing how the threat landscape is expected to continue to evolve in 2016.
[2] An independent report on the cost of DDoS from the Poneman Institute is available here.
[3] Figures are based on a report by SC Magazine.
[4] According to the Anti-Phishing Working Group report accessible here.
[5] In his book *Cyber War: The Next Threat to National Security and What to Do About It*, former White House cyber security czar Richard Clarke argues for the deployment of deep-packet inspection systems (network policy control) in Tier 1 service providers to block malware prior to reaching end-customer networks.
[6] This article acknowledges the need for CSPs to strive for clean pipes but questions the ability of network-based intrusion detection and prevention solutions to achieve the goal without the high false-positives for which these solutions are notorious.
[7] See this article, which summarizes the Frost & Sullivan report.

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. This paper will show that the answer to this market need and today's cyber security challenges is a comprehensive approach to cyber security where CSPs use network policy control to deliver cost-reducing and revenue-generating cyber security services in the public Internet for the benefit of their residential and business customers.

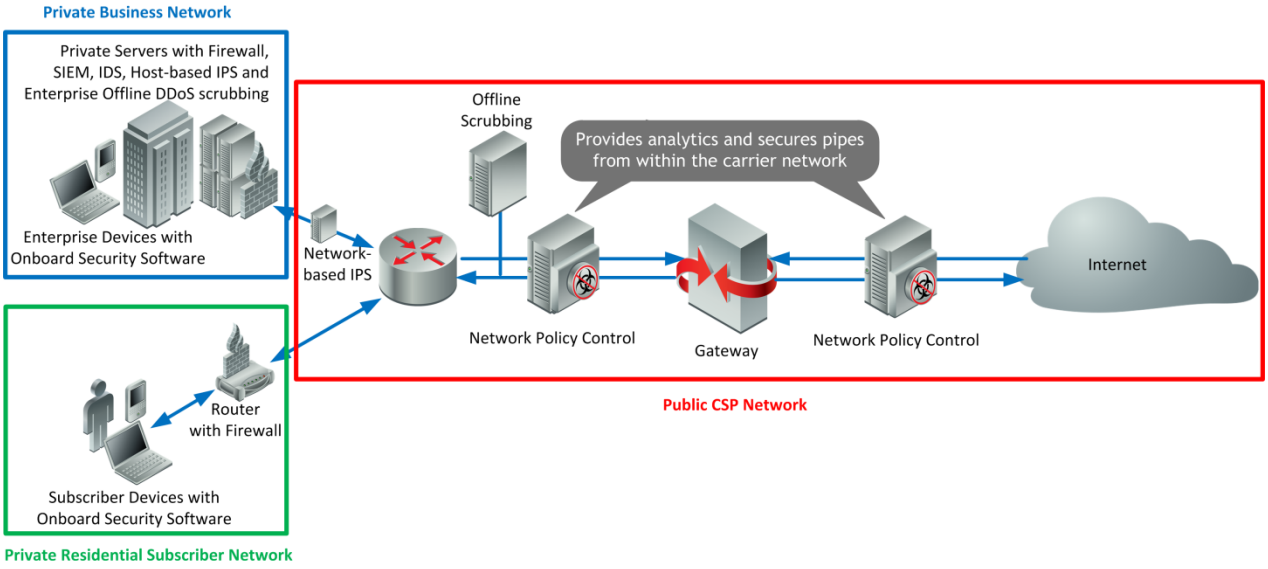

Figure 1 - Cyber Security Solutions both Public and Private

Cyber Security Threat Considerations

Cyber security threats come in all shapes and sizes, including illegal and harmful content, protocol abuse, malware infections, spam and DDoS attack traffic. This section identifies and summarizes the landscape of key cyber security threats facing CSP customers.

Botnets – A Landscape of Threats

Botnets are armies of remote-controlled devices used for the purpose of sending spam (including phishing scams), propagating malware and launching DDoS attacks. Botnets are the master-mover of most cyber security threats in terms of the scope of damage they cause in CSP networks across the globe.

Zombies

'Zombies' are the obedient foot-soldiers of the botnet army, and are typically a residential subscriber or business employee device that has been infected by malware specifically designed for control by a remote party. That remote party is a botnet command and control (C&C) device that can conduct malicious activity using many thousands to millions of computers.[8]

In most cases, subscribers generating malicious traffic on the network are unwillingly doing so as a part of a botnet because their device has unknowingly become infected with malicious software. Not only is the network being abused, but infected subscribers are often unaware of the root cause of the symptoms that appear and erroneously blame the network provider.

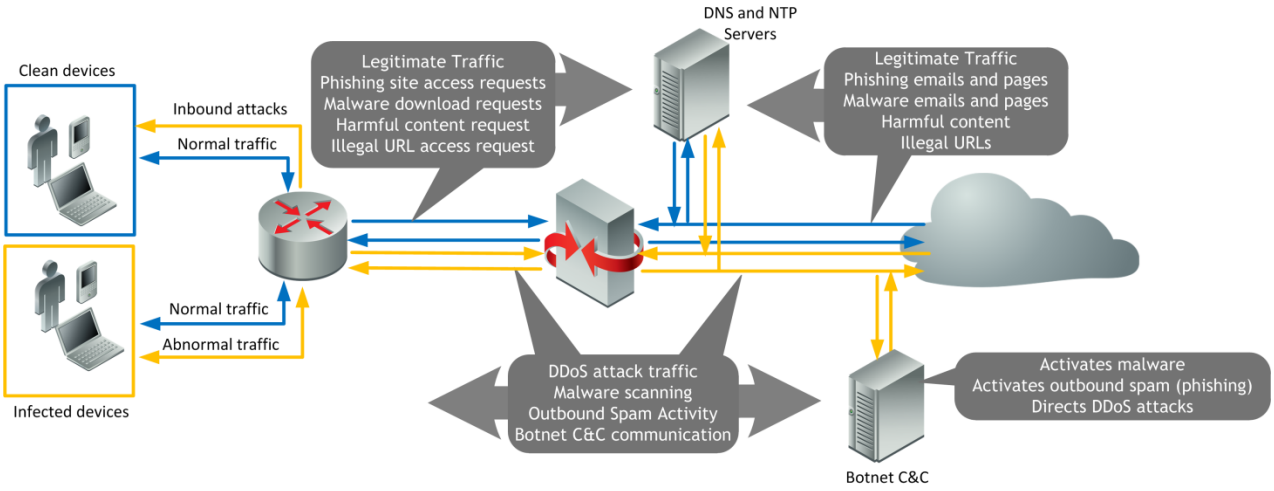

Figure 2 -Botnets Represent a Landscape of Cyber Security Threats

Phishing Scams

A phishing scam is an attempt to acquire information such as usernames, passwords, and sensitive financial information by masquerading as a trustworthy entity in an electronic communication. The user thinks they are accessing a legitimate website when they enter an incorrect URL in their browser, or click on a link in their browser, an email, or instant message, which prompts them to reveal sensitive information. A main source of phishing spam emails are botnets engaged in spamming activity.

[8] This article details the damage done by none high-profile botnets over the past few years that were able to control thousands and even millions of compromised 'zombie' devices to send spam and conduct attacks.

Once identity and authentication information has been stolen, criminals use it to make fraudulent purchases, send spam, propagate malicious software, and conduct various other activities that are bad for both CSPs and their customers.[9]

Malware

Malware is malicious software that is unwittingly installed or self-propagates onto end user devices. A device can be infected with malware when a subscriber opens an email attachment, clicks a download link or visits a web page that installs the malicious software program. Once installed, malware frequently turns healthy subscriber computers into compromised 'zombies' that can be controlled by a remote host as part of a botnet to launch DDoS attacks and send spam (including phishing scams). Many malware programs also use their infected host to scan the network's addresses and the ports of vulnerable devices before using an 'exploit' to infect more machines.

DDoS Attacks

The intent of DDoS attack traffic is to make a computer resource or network unavailable. By targeting a company's computers and its network connection, an attacker can cause costly disruptions to operations and damage to reputation and trustworthiness. CSP networks are both targets of and attack vectors for DDoS attacks that disrupt service and hurt subscriber Quality of Experience (QoE).[10]

Layer-3/4 attacks

The majority of DDoS attacks focus on targeting the transport and network layers with shear volume, aiming to overwhelm the target machine, denying or consuming resources until the server goes offline. These attacks can also saturate the entire network with malicious traffic until it is rendered temporarily unusable. There are three types of Layer-3/4 attacks.

- A SYN flood overwhelms the target's ability to process SYN packets
- A flow flood overwhelms the target's flow state memory
- A bandwidth flood overwhelms the target with shear bandwidth volume

Reflector attacks

IP-spoofing reflector attacks (e.g., DNS, NTP) trick network resources into attacking subscribers. Reflector attacks direct NTP and DNS servers to flood a target with traffic, and they can make the attack even worse through 'amplification'. These attacks can be amplified by using server protocol request/response features to elicit a server response towards the intended target that is disproportionate to the original request. An example is an NTP protocol command called "monlist" (or sometimes MON_GETLIST) which can be sent to an NTP server to return the addresses of the last 600 machines with which the NTP server interacted. Because this response is much bigger than the request sent, it is ideal for amplifying a reflector attack.

[9] Phishing costs the average large enterprise $3.7 million per year according to CSOonline.

[10] This article notes that Akamai's *State of the Internet* report for Q2 2015 found DDoS attacks reached a record high in 2015, with the largest attack spanning 13 hours at a sustained rate of 240Gbps.

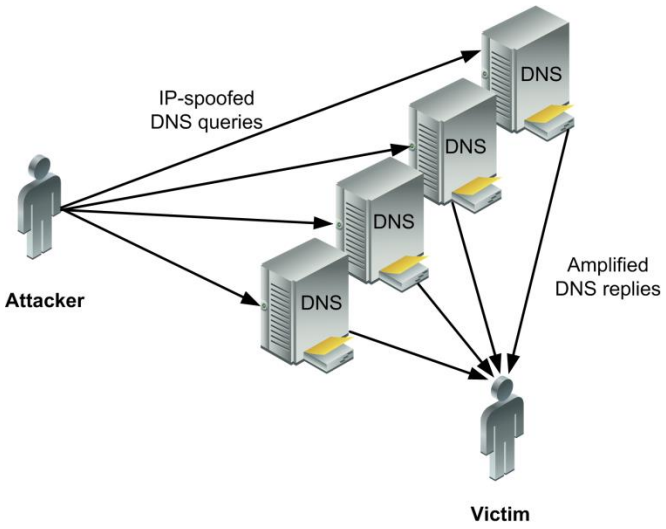

Figure 3 – Reflector DDoS Attack (DNS Amplification)

Layer-7 attacks

Layer 7 DDoS attacks are more difficult to detect and mitigate because they mimic human behavior as they interact with the application user interface. These are typically 'low and slow' attacks where apparently legitimate Layer-7 transactions occur at rates below the thresholds typically set to detect and mitigate high volume Layer-3/4 attacks.

A sophisticated Layer-7 DDoS attack may consist of thousands of devices all attempting to download the banner of a target website, or a file stored on its servers, or make endless queries, or send the content of a form very slowly, all with the goal of exhausting a server by repeatedly straining its resources. Because it mimics human behavior by manipulating application-layer features and functionality, these attacks are difficult to separate from normal traffic.[11]

Outbound Spam

Outbound spam is a problem for CSPs because it can lead to blacklisting by watchdog groups if the spam problem is considered severe, resulting in email disruption for all of the network's subscribers. The support costs and brand damage that result from blacklisting are severe as subscribers report non-delivery of e-mail and significant operational resources are expended investigating and resolving individual blacklisting incidents.

A lot of spam consists of botnets emailing phishing scams, which further victimize Internet subscribers while costing businesses billions each year that remediate financial charges related to identify theft.

The Negative Impact of Botnets

Malicious software and traffic are a cost to CSPs, residential subscribers and business customers.

The cost to CSPs

CSPs incur the cost of transporting abnormal or bad traffic all the way across their networks to the residential subscriber or business customer's front door. CSPs have to pay for support calls from angry

[11] Attack tools such as Slowloris, Sockstress, and R.U.D.Y. produce legitimate packets at a slow rate, allowing the packets to pass traditional detection techniques that look at volume-based characteristics at layers 3 and 4. For a complete overview of various DDoS attack techniques see "Attack Techniques" on the Wikipedia page for DDoS.

residential subscribers who do not understand that their devices are behaving abnormally or poorly because they are infected. When the problem becomes severe, a CSP must deal with the reputational issues that stem from being associated with a threat-heavy service.

The cost to a CSP's residential subscribers

Subscribers on pay-for-data plans end up paying the CSP for a bunch of traffic that ruins QoE and device performance at the very least, and ruins their lives via identify theft and destruction of their data and software property at the very most.

The cost to a CSP's business customers

The enormous cost of DDoS attacks, malware infections and phishing scams for businesses of all sizes is well-understood by all. Businesses spend a lot to deploy and maintain a complex array of solutions designed to protect their private networks from all of the 'bad stuff' that exists on the public Internet; threats that can intrude into their employee devices and critical business systems to disrupt operations, steal sensitive data and generally wreak havoc.

As the frequency and intensity of attacks and intrusions increase exponentially, and the various solutions to defend the private network from these threats become increasingly unwieldy, Frost & Sullivan argue that businesses are reaching a point of exhaustion and demanding a new paradigm that offers badly-needed relief.

Harmful Web Content

The actual content that is available to subscribers through Internet browsing has emerged as a threat as parents, schools and businesses seek to filter out the bad while protecting the good.

Regulatory Pressures

CSPs are compelled to filter web content based on public pressure, local regulations and government incentives. One example is the filtering of known sources of child pornography based on a URL blacklist maintained by the Internet Watch Foundation (IWF).

There is an emerging need for a more nuanced approach to the management of web content that goes beyond simple URL blacklisting to filter entire topics, regardless of URL. For example, the Children's Internet Protection Act (CIPA) requires schools and libraries in the United States to bar access to specific categories of content before they can receive government funding. Example categories that could be filtered include:

- alcohol
- blog
- entertainment
- gambling
- hate
- pornography
- weapons

Social and Parental Pressures

Going beyond regulations, various cultures and individuals have a vested interest in filtering out what they perceive as harmful or offensive material while browsing the internet.

Cyber Security Threat Mitigation Techniques

Given the sheer variety of cyber security solutions at play in the market, from endpoint anti-virus software, to firewalls, to host- and network-based IDS/IPS solutions, the "security professionals (of enterprises and businesses) must feel, at times, less like they are managing and more like they are herding cats."[12]

To help illustrate this point, let's briefly review the various private and public network cyber security solutions available today before deep diving into how network policy control can address the many problems by securing pipes from within the CSP network.

Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is typically installed behind a firewall, offline, and is focused on the detecting and logging security events that affect the private network of a business.

The IDS primarily reports on anomalies and known threats detected within the private network, and comes with a group of 'signatures' that use bit patterns (1s and 0s) and RFC application compliance to detect known malware threats. IDS solutions can also be linked to access control and management systems to detect unauthorized access and activity. The IDS is purely a reporting tool:

> *A good analogy is to compare an IDS with a protocol analyzer. A protocol analyzer is a tool that a network engineer uses to look deep into the network and see what is happening, in sometimes excruciating detail. An IDS is a "protocol analyzer" for the security engineer. The IDS looks deep into the network and sees what is happening from the security point of view.*
>
> *An IDS provides a window into the network for security analysts (to gain insight into):*
>
> - *Security policy violations, such as systems or users who are running applications against policy*
> - *Infections, such as viruses or Trojan horses that have partial or full control of systems*
> - *Information leakage, such as running spyware and key loggers*
> - *Configuration errors, such as applications, systems or firewalls with incorrect security settings*
> - *Unauthorized clients and servers*[13]

This increased visibility into the security posture of the network is what characterizes IDS products, and which differentiates the visibility function of an IDS from the control function of an Intrusion Prevention System. [14]

SIEM Solutions

Security experts at the SANS Institute describe a Security Information and Event Management (SIEM) system as "a hybrid solution coming from two distinct security-related products: Security Information Management (SIM) systems, technologies focused upon policy and standards compliance through the consolidation of logs, the analysis of data and the reporting of findings; and Security Event Management (SEM) systems, which provide technical support in the management of threats, events and security incidents in real time."[15] TechTarget describes the SIEM as a reporting enhancement with visual dashboards that helps automate the analysis of security event logs generated by an IDS.[16]

---

[12] See this article, which summarizes the Frost & Sullivan report.
[13] See this page, which provides a detailed comparison of firewalls, IDS and IPS solutions.
[14] Ibid.
[15] See this article from the SANS Institute for a detailed description of SIEM.
[16] See this TechTarget article that explains the difference between SIEM and IDS.

Device Cyber Security Software

Many vendors sell anti-virus software that can be installed on endpoint devices like desktop PCs, laptops, tablets and smartphones. These products are typically the last opportunity to detect an inbound threat, and are also used to scan devices for threatening software that has already been installed. Network-based security solutions do not compete with, but are complementary to, endpoint anti-virus software solutions in that they seek to prevent bad packets from ever arriving at business or subscriber premise.

Firewalls

Network firewalls filter traffic between an untrusted public network (typically the CSP's network) and a trusted private network, and host-based firewalls control traffic in and out of a single machine (e.g., between the untrusted public Internet and a residential subscriber's device, or as a redundant layer of defense protecting business devices that sit behind a private network firewall). A firewall typically consists of an ordered hierarchy of rules, and for every packet the system sees it starts at the top of the rules list and proceeds to each subsequent rule until the conditions are satisfied and the rule is executed. Most of these rules are pass rules, as in 'allow the traffic through'. Thus, the firewall gets a packet off the wire and starts looking for an allow rule. If it gets to the end of the list and no such rule exists, then there's a final deny rule, as in 'drop everything else'.[17] Firewalls have several limitations, including:

- Pattern recognition based on signatures is easy to exploit if any bot or hacker is observing the data packet patterns. It becomes easy for the hacker to create fake packets containing a 'trusted source IP' to hack a computer/network.
- Firewalls cannot stop internal users from accessing external websites with malicious code.
- Firewalls cannot stop internal users from accessing external websites running phishing scams.
- Firewalls cannot detect or block malware scanning activity that spread malware and overwhelm resources from within a private network.
- Firewalls do nothing to help address infected subscriber machines.
- Pure firewall solutions are limited in their ability to report on and analyze packets that are blocked for not matching a rule.

Intrusion Prevention System (IPS)

An IPS is essentially an IDS that is installed inline and can take action based on what it detects. Critically, the IDS is designed to be deployed at the boundary between different levels of trust (for instance, a high-trust private network and an untrusted public network). It's like a firewall, but inside-out because it has a set of mostly 'deny' rules as in 'block this known security problem'. When a packet shows up at the IPS, the IPS looks through its list for a rule indicating it should drop the packet. At the end of the list, though, is an implicit 'pass' rule. Just as with the IDS, the IPS detects malware threats through the use of binary signatures, logs security events and looks for patterns of behavior indicating violations to a private network's security policy. An IPS has traditionally been oriented towards detecting and stopping attempts to compromise a host rather than network-level attacks, although some solutions include some rate-limiting functions to address DDoS attacks targeted at the enterprise network.

Host-based IPS

A host-based IPS protects individual devices such as enterprise workstations, servers and smartphones from unauthorized access and malware coming from the untrusted public Internet. As such, they fall

[17] See this page, which provides a detailed comparison of firewalls, IDS and IPS solutions.

squarely into the realm of endpoint protection and, when tuned properly to the specific workstation, application, user role and workflow, can work very well. Unfortunately, echoing the findings of Frost & Sullivan, this expert reports on TechTarget that he rarely sees a host-based IPS in the field:

> *The interesting thing I've seen regarding host-based IPSes is that they're rarely used. This is likely because of the complexity and frustration involved; they're challenging for IT and security staff to configure properly without creating bottlenecks or negatively impacting network traffic, and it can be frustrating if they're set up in a way that prevents the user from getting his or her work done. Furthermore, the last thing that users want to deal with is a bunch of annoying pop-up windows asking if it's okay to allow unknown traffic to communicate to and from the computer. This brings up another interesting caveat: Users are often in control of their local security policies, which can actually negate any perceived benefits of the host-based IPS.*[18]

Network-based IPS

A network-based IPS is placed in front of the private network firewall to face the public internet. It does the same job as a host-based IPS but for an entire business or enterprise private network. In recent years, vendors have been offering IPS solutions to block threats identified within the CSP's public network. As they move towards more public network solutions, traditional IPS solutions have significant limitations to overcome:

- The most commonly reported problem with IPS solutions is a very high rate of false positives.[19] A fact of life perhaps for enterprise security professionals, in any carrier network false-positives are a death-knell for both subscriber QoE and the CSP's reputation.
- Because they are migrating from the enterprise market, stateful IPS solutions typically fall prey to failure and increased latency under the heavy load of large volume attacks, which are very common in CSP networks.[20]
- IPS solutions require large investment in security expertise to continuously monitor and tune IPS signatures and configurations to keep pace with a changing landscape of threats.

To further confuse the issue, some vendors entering the cyber security market with network-based, proprietary solutions for CSPs are using the term IPS when their solutions actually operator more like traditional network policy control devices (e.g., the PCEF or TDF in 3GPP).

Unified Threat Management (UTM)

Unified Threat Management (UTM) is an integration of the firewall, IDP and IPS into one seamless solution for enterprise networks.[21] UTMs are an attempt to consolidate a fractured array of solutions addressing individual use cases into one single, more manageable entity that protects the enterprise network. One reported drawback of UTM solutions is that they lack the granular tuning typical of traditional IDS and IPS solutions.[22]

---

[18] This TechTarget article discusses the difference between host-based and network-based IDS/IPS solutions.

[19] False-positives are such a common occurrence with IDS/IPS systems that there is a standardized method of reporting them, explained here. False-positives are reported by multiple independent sources as the main issue with IDS/IPS solutions – see pages here, here, here, here, and here.

[20] See this article imploring those considering an IPS to make sure it fails open due to the high likelihood of being overwhelmed by the sheer of large attacks volume.

[21] See a full description of UTM here.

[22] This article describes the limitations of UTM solutions.

Scrubbing Centers

A scrubbing center is a vast improvement over the first-generation DDoS mitigation methods that used null routing to 'blackhole' all traffic destined for a particular IP suspected of being under attack. The problem with the null routing approach was that it blocked all traffic destined for suspected victims, mainly to protect the network from overload, which means a victim would cease receiving any Internet traffic at all (the actual intent of the attack).

With a second-generation scrubbing center solution, high-volume Layer-3/4 attacks coming from or directed at a specific IP are first identified and, once the 'victim' IPs have been isolated, all of the traffic destined for the 'victim' is redirected to a bank of appliances that 'scrub' out the DDoS attack traffic before reinserting legitimate traffic back into the network. The obvious advantage of this approach is that it eliminates the attack traffic while allowing everything else to proceed to the intended destination. Scrubbing center solutions offer a genuine, network-based solution for DDoS that can contribute significantly to the concept of 'clean pipes' (i.e., business and residential subscriber traffic is 'cleaned' of DDoS).

For CSPs, the main drawback to scrubbing center solutions is the enormous expense associated with diverting huge volumes of Internet traffic to an offline system for the sole purpose of removing DDoS packets and nothing else. The approach introduces latency, requires a significant capital investment and a large budge for operational maintenance. The 'mitigation' aspect is often a manual exercise, where an operator must be notified of a potential attack, investigate, and manually confirm redirection to the scrubbing center. The method typically will only address the 'next flow' when an attack is detected, which means if the attack is a bandwidth flood or advanced Layer-7 attack it will not be mitigated.

The operational cost of running a scrubbing center can be prohibitive for smaller CSPs and enterprises that cannot afford the people resources required to constantly monitor and confirm redirection of suspected attacks. Scrubbing centers are also typically only designed to clean DDoS attacks, and only DDoS attacks, before data arrives at the boundary of a private network. This single use case limitation means that, although such solutions cleanse Internet pipes, they fall short of delivering the comprehensive, next generation 'secure pipes' called for by Frost & Sullivan.

Secure Pipes with Network Policy Control

Cyber security services can be delivered by CSPs using an inline network policy control solution either globally across their networks or as a specific service for individual residential and business subscribers. There are several advantages to managing cyber security threats from within the CSP network:

- Content filtering can be mandated by regulation, forcing CSPs to respond with a global, network-based solution
- These solutions do not depend on up-to-date end-client software and local databases installed on a device that must be maintained to remain effective
- Cyber-security driven by network policy control can lower the cost of data delivery by reducing the reach and associated burden of transporting bad packets
- Cyber protection use cases can generate revenue when sold as a managed security service to businesses subscribers that are in desperate need of a more simplified and effective approach
- A CSP cyber security solution with freeform policy capabilities offers highly-tunable, zero-day threat detection and automatic mitigation based on traffic behaviors observed in real time that cannot be bypassed

Why Network Policy Control?

The main argument for network policy control as the best way to offer a secure pipes solution is that it is already designed to operate within the carrier-sized, untrusted environment of the public Internet. Cyber security solutions designed to protect private networks serve as a boundary between layers of trust, and therefore are designed to 'default block', but this is not a feasible approach for a carrier-grade solution. Private network solutions can be forgiven for a high rate of false-positives (accidently blocking or altering something that should have been left alone) because the focus is to protect the pristine environment of the private network that sits behind the IPS, IDS, and firewall.

The rule of thumb for network policy control solutions designed for carrier networks is to 'default allow', always taking special care to avoid unacceptable false positives. These solutions are also designed to handle the incredible volume of traffic that a carrier-grade network generates as they intersect, inspect, and make decisions about every packet and flow.

Why Should a CSP Step into the Fray?

A CSP might question the value or incentive of deploying a network-based secure pipes solution for their residential subscribers and business customers, but there are many benefits.

Reducing support costs and attracting residential subscribers

Subscriber devices have well-developed endpoint anti-virus solutions already installed, and it's important to note that network-based solutions are complementary. The following three factors suggest a real benefit for CSPs that commit to a global, network-based secure pipes solution for residential subscribers:

1. Reduces the amount of bad (or 'abnormal') traffic that CSPs incur the cost of transporting all the way across their networks to the residential subscriber's front door.
2. Reduces the cost of support calls to CSPs from angry residential subscribers who do not understand that their devices are behaving abnormally or poorly because they are infected.
3. Generates revenue as residential subscribers are attracted to purchase Internet service from a CSP that advertises a dramatic reduction in malware and attack traffic via secure pipes.

A secure pipes solution for the public internet 'secures' traffic as much as possible before it reaches subscriber devices. In doing so, these solutions do not replace but complement the endpoint device solutions residential subscribers already have in place.

Generating revenue from business customers

A CSP's business customers are very well-informed about the cause of and damage done by cyber security threats that breach the entry point of their private networks. This paper has shown that Internet security experts trying to protect the private network of a business are already spending their valuable time and money juggle a wide variety of complex solutions that seek to identify and stop threats as they arrive at the front door.

The market need is clear: Instead of having enterprise-oriented solutions shoulder the entire burden of protecting sensitive private networks, these solutions should rather be a 'last line of defense' at the threshold between the private network and a public CSP network that has already been secured as much as possible by the CSP.

Once again, we can see how a solution installed in the public-layer Internet complements rather than replaces the private network solutions businesses already have in place. In their 2015 report on secure pipes, Frost & Sullivan define the following benefits:

> *Secure pipes changes the way security is managed. Network technicians and security professionals can now share the responsibilities of security. Coordination and cooperation create a holistic approach to integrated network security. Perimeter defenses placed at the edge (LAN-WAN demarcation) of an integrated network security architecture can be sized to be smaller (less traffic to process), and have policies that are complementary and more surgical than the policies used in the "pipe. Additionally, secure pipes reduces the required security responsibility of in-house security staff and network administrators. Security professionals are less likely to need to be experts in all aspects of security, allowing them to optimize or re-prioritize their attention on the many important and urgent tasks and initiatives pulling at their time and talent."*

To reap the rewards of this enormous benefit, a CSP's business customers are ready and willing to pay for a solution that secures public Internet traffic as much as possible before it arrives at the front door.

A consolidation of protective services that meet performance requirements

Most importantly, CSPs equipped with the right solution are in the best possible position to clean out the bad while protecting the good across the entire carrier network. According the Frost & Sullivan, secure pipes are similar to UTM, where best-of-breed firewall, IDS and IPS have been unified into one platform for individual residential and business subscribers. A solution for secure pipes combines the following key technologies and capabilities into one platform positioned at the heart of the CSP network to prevent bad packets from ever arriving at the subscriber premise:

- Network firewall and intrusion detection and prevention systems (IDPS)[23]
- Distributed-Denial-of-Service (DDoS) Protection and Mitigation
- Email and Web filtering
- Advanced Analytics – Applying "Big Data" principles with state of the art analytics[24]

[23] It is critical to note Frost & Sullivan's use of the term IDPS "services". Here Frost & Sullivan is not proposing the deployment of traditional IPS solutions deep in the CSP network, but are asking for equivalent functions to what an enterprise security expert would recognize as an IPS. The paper argues that network policy control is the solution to this market need.

Of course, secure pipe solutions have capabilities that go beyond the traditional UTM, including third-generation, carrier-grade DDoS protection and other functions enterprise security experts would recognize as being similar to a Web Application Firewall (WAF), IDS, or IPS (malware infection and phishing prevention, botnet disruption and malware exploit scanning protection across the entire CSP network or as a service for individual businesses).[25]

Frost & Sullivan emphasizes the "effectiveness benefit as security is applied at light speeds. Breaches and data exfiltration time is measured in minutes and sometimes seconds. Applying security at line rates within the carrier network provides an additional layer of security, extending defense in-depth and refining the network perimeter."[26]

Cyber Security Analytics

In their Executive Brief on Secure pipes, Frost & Sullivan emphasize that the ability to expose unknown cyber security threats is directly related to a solution's scope of visibility, and no solution has a better vantage point than a network policy control platform collecting data and performing analysis from within the CSP network:

> *Expose is the stage in which the advantages of applying security in the network come to light. The ability to expose unknown malicious traffic is directly correlated to how much can be seen, or the scope of visibility. Even the largest enterprises have only tens of thousands of endpoints. Having the visibility of millions, tens of millions or hundreds of millions of endpoints provides visibility benefits that cannot be replicated by a single enterprise.*

Using the operational and strategic reporting tools embedded in network policy control solutions, CSPs can leverage the following use cases:

- Anomaly Detection – Monitor network traffic, establish a baseline of what is normal, and detect anomalous traffic that is indicative of malicious activity
- Behavioral Analysis – Analyze traffic for known behaviors that indicate improper activity
- Flow Data Comparison – Monitor traffic flows for activity that is not congruent with legitimate known good patterns
- Gain extremely valuable insight into cyber threats through real-time monitoring and historic threat analysis

Subscriber Protection Intelligence

Traditional security solutions, although effective against known threats when kept current, are still being bypassed by attacks which morph or contain zero-day exploits resulting in a security posture that is predominantly reactive. A source of threat intelligence data feeds can deliver automated real-time flows of threat intelligence data to the network policy control solution covering reputation (IP, Domain/URL), security risks (including malicious code, spyware, and adware), and vulnerabilities.

The network policy control solution can respond to detected network traffic and subscriber behaviors based on the real-time threat intelligence database to protect subscribers from phishing scams, prevent malware infections, and disrupt the communications of botnet command and control servers.

---

[24] See the Frost & Sullivan report on secure pipes, pages 5 and 6.
[25] See the Frost & Sullivan report on secure pipes, page 6.
[26] See the Frost & Sullivan report on secure pipes, page 4.

Malware and Phishing Prevention

When the threat intelligence databases commonly found in end-user anti-virus software products for devices are integrated with a network policy decision engine located at the heart of the network, CSPs gain real-time visibility into the global threat landscape and the ability to secure their public network against these threats. This allows CSPs to respond with proactive policies that prevent security threats from ever reaching the front door of a residential subscriber or private business network.

The network policy control solution registers subscriber web requests and checks them against the threat intelligence database to block or warn residential subscribers and business employees at risk of becoming duped for their sensitive information or infected with malware. This approach allows the CSP to shift from a reactive to a proactive security policy without incurring additional IT management overhead, while keeping abreast of the rapidly changing threat environment.

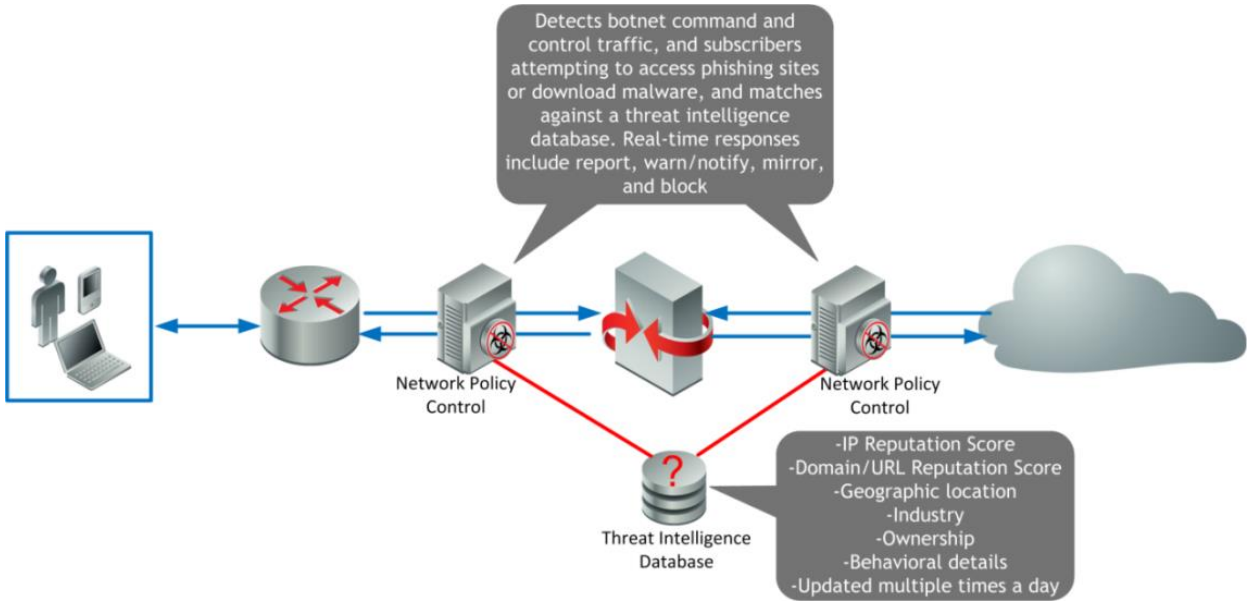

Figure 4 – Network Policy Control Integrated with Network Threat Intelligence

Behavioral Threat Intelligence

With the increasing prevalence of traffic encryption, the need for zero-day protection and the danger of false positives, it has become much less effective to rely on signatures to detect and block malware scanning activity, DDoS activity and outbound spam. DPI-based network policy control solutions are uniquely positioned to analyze and respond to traffic behaviors that deviate from a 'normal' profile. The same behavioral policies that enable powerful reports can also underlie the real-time decision process that determines whether traffic inspected at line rate is 'abnormal or 'normal', 'good' or 'bad'.

'Abnormal' traffic could include things such as high traffic volume coming from or to a single IP, many IPs sending a certain pattern of traffic to one IP, abnormal DNS behavior, abnormal scanning activity, abnormal flow or SYN rates, known botnet C&C IP communications, etc. Based on this real-time analysis of traffic behavior, a network policy control solution can recognize an attack as it is occurring and can notify subscribers and throttle, block or disrupt attack traffic using a precisely-tailored policy defined by the CSP.

This means that even if it's not precisely clear what tool, technologies, or motives are in play during an attack, it can still be detected and automatically mitigated in real time. Solutions can also be configured to only detect and notify about attacks, with decision to mitigate made manually by the monitoring operator.

Malware Scanning Protection

Self-propagating malware can be detected by analyzing the behavior of malicious software as it conducts ICMP scans to find vulnerable hosts. Malware will scan vast swathes of IP ranges, and the ports of likely infection candidates, in its search for vulnerable targets. This scanning activity, which can be considered an attack all by itself since it has the potential to exhaust network elements, has a specific behavioral profile that can be detected using behavioral policies. Behavior-based policies are highly tunable and extremely adept at accurately recognizing threat-based scanning activity without false positives.

DDoS Attack Traffic Mitigation

An inline network policy control solution represents the third generation of DDoS detection and mitigation.[27] Network policy control offers the necessary additional layer of behavioral traffic analysis to recognize and instantly respond automatically to threats as they are detected in real-time, without redirection to an array of scrubbing center appliances.

Layer-3/4 attack protection

The tools and methods available to DDoS attackers render the use of static signatures for detection and mitigation completely ineffective for detect Layer-3/4 attacks. Effective inline solutions use behavioral heuristics to identify the tell-tale signs of a flood, SYN, or bandwidth flood.[28]

Reflector attack protection

Detecting a reflector attack is made easier if the network policy control solution can analyze DNS and NTP protocol traffic and recognize anomalies. Once detected, reflector attacks can be mitigated by blocking unsolicited traffic inbound to the subscriber (attack target) while leaving outbound traffic untouched.

Layer-7 Attack Protection

Because Layer-7 attacks use automated scripts to mimic the web browsing behavior of actual humans, a network policy control solution that supports behavioral traffic analysis is ideally suited to detecting and mitigating application-based DDoS. The solution's Layer-7 reporting capabilities can help establish a baseline traffic profile for 'normal' browsing behavior. A policy can be written to compare this profile against any 'anomalous' behaviors detected by the DPI solution.

Detection criteria can include a 'challenge and response' prompt that requires a suspected automated bot to enter a Captcha response that cannot be scripted or reproduced artificially.

Once behavioral analysis has determined a Layer-7 attack is occurring, mitigation can include blocking, slowing or even tar-pitting[29] the attack traffic.

---

[27] The first generation of DDoS protection was QoE-destroying null-routing. The second generation of DDoS protection uses redirection of suspected attacks to scrubbing centers.

[28] For examples of Layer-3/4 DDoS behavioral mitigation policies, see the Sandvine technology showcase "*Secure Pipes with Network Security*".

[29] More information on tar-pitting can be found here.

Outbound Spam Mitigation

Unlike anti-spam solutions that look at specific ports or email content, a network-based solution allows CSPs to apply policies that analyze real-time packet and traffic behaviors to detect outbound spammers. The real-time decision engine can consider dozens of variables with policies distinctly applied to both residential subscribers and business customers. Such real-time analysis and decision-making capabilities require adequate processing power and memory, and have become important with the emergence of encryption. Any time a signature is impossible or simply not accurate enough, behavioral traffic analysis offers accurate solutions if the cyber security solution has the horsepower.

CSPs are able to mitigate outbound spam by blocking, rate-limiting SMTP connections, or even tar-pitting traffic from spammers and presenting infected subscribers with a message notifying them of the problem. The ideal solution should include detection, mitigation, and notification functions to:

- Instantly recognize and respond to spam
- Identify households sending spam
- Notify infected household
- Assist with guided self-remediation

Recognizing that those subscribers who are spamming are almost always doing so unknowingly as part of a botnet, CSPs can chose a collaborative approach to solving the issue:

- When a household is identified as a source of spam, rather than blocking email traffic outright, the operator could implement a rate-limiting policy to stem the flow of spam
- Next, the subscriber could be redirected to a landing portal that provided an advice-of-infection notification and detailed instructions and resources to remove the malicious software

Web Browsing Content Intelligence

A major challenge today is ensuring a safe web environment for users and companies without impacting their web experience. Integrating the contextual intelligence database of an endpoint parental control solution with real-time network policy control allows CSPs to offer URL and web categorization filtering for:

- Parental controls
- Web Analytics
- Acceptable use enforcement (e.g., Wi-Fi hotspots, business web filtering, etc.)

Web Filtering Based on URL

In a global implementation, CSPs use network policy control to check subscriber access requests against a prepackaged ‘blacklist’ of restricted URLs. Attempts to access blacklisted URLs are detected and blocked by the network policy control appliance, and users are informed that the content they are attempting to access is restricted.

CSPs can also use network policy control to define custom URL blacklists and whitelists for the entire network or for specific subscribers and businesses. These can be tied to additional policy conditions such as “time-of-day” and can specify exclusions for specific subscribers and groups.

Web Filtering Based on Topic Categories

Although it can be driven by regulatory incentives (e.g., CIPA in the United States), the need to filter out specific categories of web browsing topics presents an opportunity to offer new network-based

filtering services to both businesses and subscribers. As one example, CSPs can provide their business customers with a preconfigured solution that filters employee access to specific categories of content during specific times of day (e.g., no gambling or social media from 9 am to 5 pm).

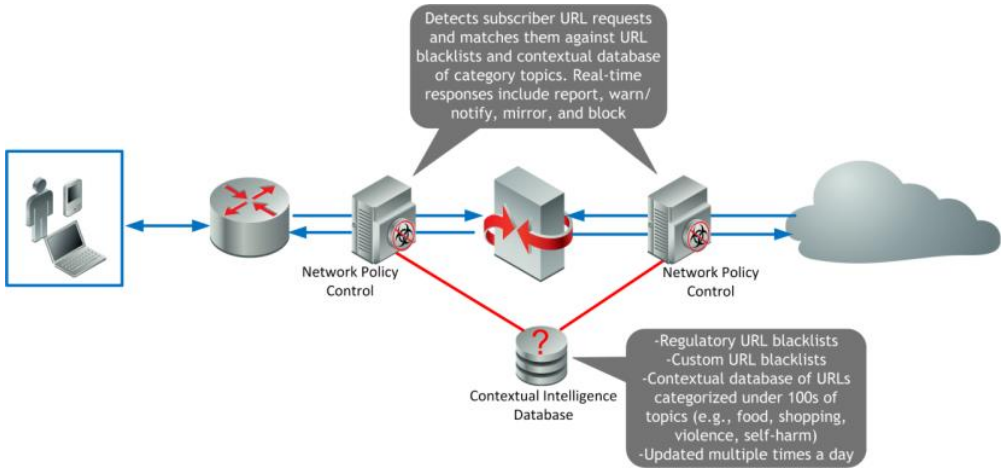

Figure 5 – Network Policy Control integrated with Contextual Web Intelligence

Use Case Example – Destroying Botnets

The use case example of detecting botnets, mitigating their effects and disrupting their operation illustrates a broad range of benefits associated with network policy control-based cyber security.

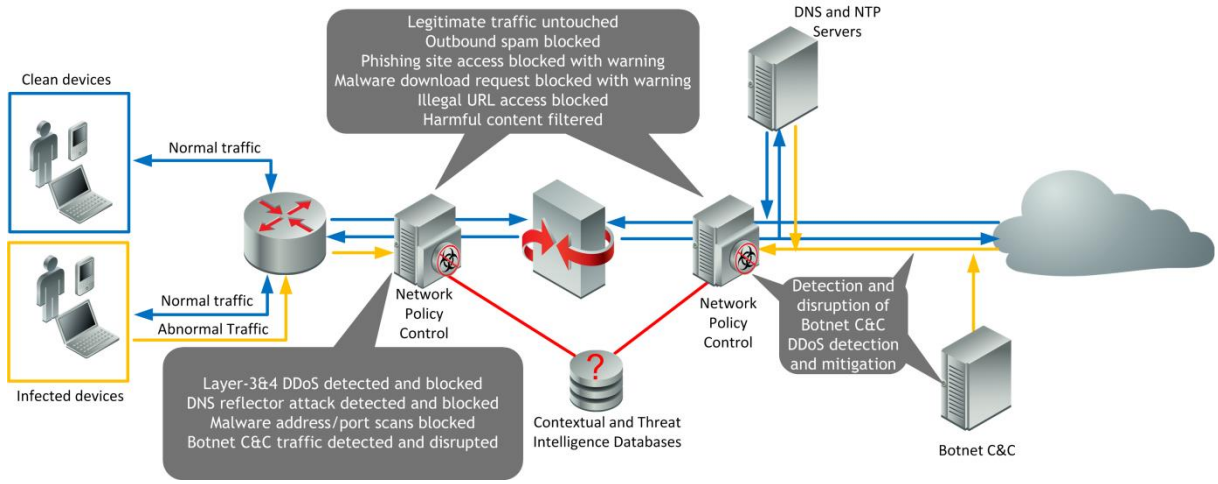

Figure 6 – Botnet Destruction – Mitigating a Landscape of Threats

Conclusions

The focus of this paper has been on demonstrating how CSPs can deploy a solution today to meet the incredible subscriber demand for secure pipes. A secure pipes solution embedded inside public network layers addresses a broad range of cyber security issues inside the CSP network, including malware and phishing, harmful content, malware scanning, DDoS attacks and spam.

A network policy control solution 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.

Summary Table

The following table summarizes the landscape of threat visibility and management approaches.

Cyber Security Solution	Description and Use Cases
IDS	*Location* Behind the private network firewall *Use Case* Monitor and log network security events
SIEM	*Location* Behind the private network firewall *Use Cases* -Monitors and provides a visual representation of security events -Integrates with access control systems to manage security events
Device Security Software	*Location* Installed on an end-user device *Use Cases* -Malware and Phishing prevention at the host interface on a private network -Anti-virus and anti-spyware host scanning, detection and cleaning
Firewall	*Location* -Network-based - on the boundary between the public Internet and a private network -Host-based – controls traffic in an out of a single device *Use Case* Block everything except that which has been specifically authorized

IPS	*Locations* -Network-based - immediately in front of the private network firewall -Host-based – behind the network firewall, in front of host firewall *Use Cases* -Allow everything except known threats via static signatures -Some limited rate-limiting policy capabilities for localized DDoS
UTM	*Location* On the boundary between the public Internet and a private network *Use Cases* – combines the following systems into one platform -Firewall -Web Application Filter -IDS -IPS
Scrubbing Centers	*Location* Offline – tap to CSP's public core or access network *Use Case* Removal of Layer-3/4 DDoS attack traffic (clean pipes)
Network Policy Control	*Location* Inline – intersects all traffic in CSP's public core or access network *Use Cases* Secure Pipes -Cyber security analytics -Botnet disruption -Malware prevention -Phishing prevention -DDoS removal (clean pipes) -Malware scanning disruption -Outbound spam mitigation -Web filtering

Related Resources

For specific information about Sandvine's secure pipes solution, Network Security, please see the technology showcase "*Secure Pipes with Network Security*".

Invitation to Provide Feedback

Thank you for taking the time to read this whitepaper. We hope that you found it useful, and that it contributed to a greater understanding of network policy control. If you have any feedback at all, then please get in touch with us at whitepapers@sandvine.com.

Headquarters
Sandvine Incorporated ULC
Waterloo, Ontario Canada
Phone: +1 519 880 2600
Email: sales@sandvine.com

European Offices
Sandvine Limited
Basingstoke, UK
Phone: +44 0 1256 698021
Email: sales@sandvine.co.uk

Copyright ©2016 Sandvine Incorporated ULC. Sandvine and the Sandvine logo are registered trademarks of Sandvine Incorporated ULC. All rights reserved.

sandvine®
Intelligent Broadband Networks