

*Protect Your Network from **Threats**
Before They **Impact**
Your Business*

Managed Intrusion Prevention Services
Proactive Network Protection

Virtela™ 
a global network solutions company

Table of Contents

- 1** Introduction
- 1** The Threat Landscape
- 2** IPS vs IDS
- 4** Managed IPS
- 5** About Virtela

Introduction

As business processes evolve to require anywhere/anytime access for mobile employees, partners, suppliers and customers, maintaining data security is becoming significantly more complex. This complexity, when combined with IT's day-to-day challenge to identify and stay ahead of the 'vulnerability curve', requires a new approach to securing enterprise assets. Historically, firewalls have established the security perimeter; however, by its very nature the firewall must allow certain applications to pass through unencumbered. The result is that attacks continually evolve through various methods of subversion taking advantage of this basic premise. Intrusion Detection Systems (IDS) attempted to solve the porous firewall problem, monitoring permitted traffic and notifying if it was not "clean." But the IDS is not 'in-line' and therefore is reactive, and for many the most rapid reaction possible considering the number of IDS alerts received is generally 15 to 30 minutes with dedicated staff. Considering the SQL Slammer virus blanketed the globe in less time than this, a more immediate reaction is necessary.

Intrusion Prevention Systems (IPS) couple the intelligence of an IDS, with an in-line network design that is capable of actively reacting to security events. Through the use of Managed Intrusion Prevention Services ensuring proper tuning and active monitoring, reaction windows can be dropped to milliseconds. Considering the increasing number of threats, and the speed with which these threats proliferate, Virtela believes Managed Intrusion Prevention Services are a mandatory addition to any security conscious enterprise network.

This brief will highlight shifts in the threat landscape, the capabilities of IPS, and finally the benefits in terms of constant vigilance through the use of Managed IPS Services provided by Virtela.

The Threat Landscape

Virus Proliferation

On average, approximately 30 new viruses appear each and every day. Worms introduced years ago, such as Nimble, Sasser, and even Melissa are still "in the wild". In fact, the average life of an unprotected Windows PC on the Internet is less than 20 minutes (SANS). A life-expectancy that can be expected to decrease as more and more attacks emerge.

Criminal Intent

The virus writer's motive is migrating from mischief to profit as an increasing number of viruses are now designed to abstract valuable information such as credit card and online banking data. Whether through a virus, spyware, worm or real-time activity, hackers who can leave "backdoors" open in user, or even corporate systems, can sell that access to the highest bidder. The transition of crime from the physical world to the online world is a logical progression—referencing Willie Sutton's famously quoted response to the question "Why do you rob banks?" – "because that's where the money is".

User Mobility

Security challenges are exacerbated by the mobility of today's users. Laptops, PDA's, and even cell-phones allow users to connect to corporate resources from nearly anywhere. Wireless coffee-shops, airports, kiosk PC's, unprotected home networks, and now entire metro wireless networks represent a potential breeding ground for malicious activity. Maintaining consistent security on all the end points connecting to these environments is a daunting task, and therefore requires the means to rapidly identify and respond to inevitable threats.

Government Regulation

The Government has realized that information must be protected both within and beyond the corporate network. Regulatory acts such as California Senate Bill 1386, HIPAA and Sarbanes-Oxley define guidelines around requirements to protect data and also mandate the disclosure of security breaches. The latter often being the most costly effect of a security failure in terms of customer or partner confidence in maintaining an ongoing relationship.

IPS vs IDS

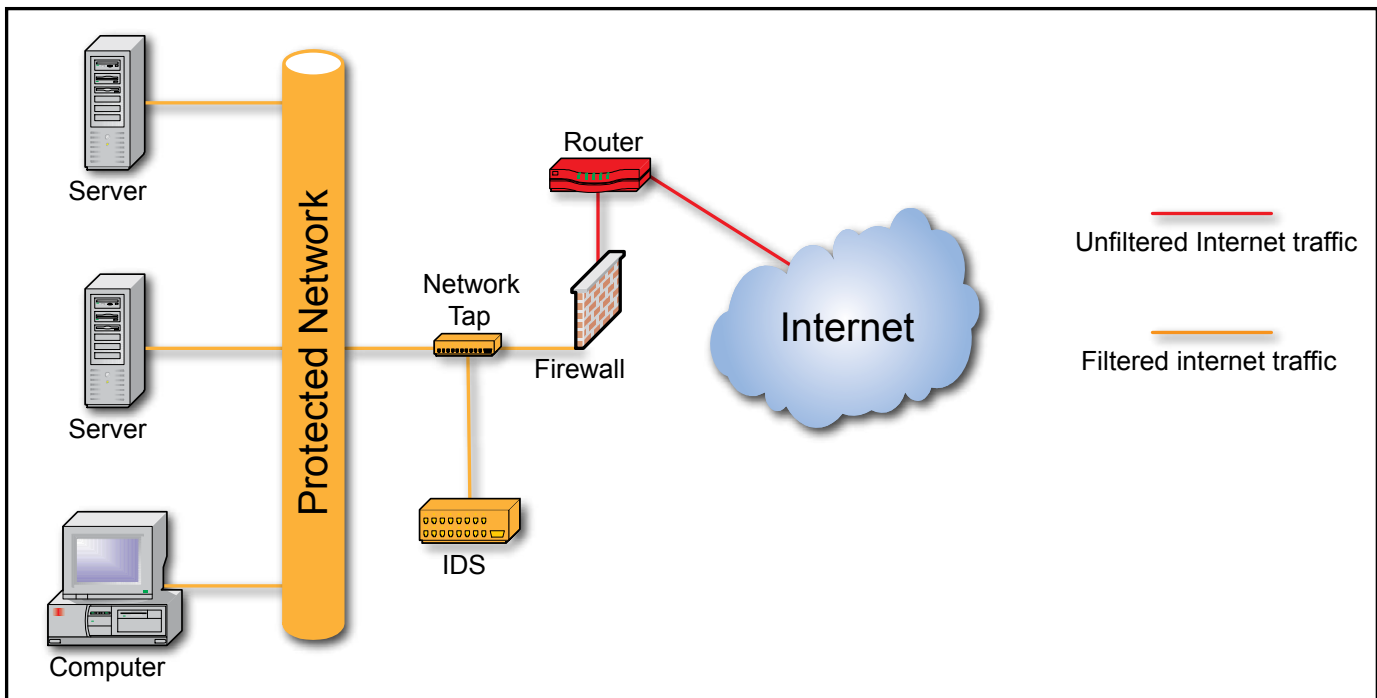
Intrusion Prevention has reached maturity in terms of technology readiness and manageability. It is a “best of both worlds” approach in that it performs deep packet inspection, like an IDS, but is placed in-line of the communication flow so that it enables an immediate reaction to threats. This results in a proactive protection security posture for the enterprise.

Intrusion Detection

The diagram below reflects a basic deployment and highlights the minimum connectivity required for secured Internet access using a firewall and IDS solution. Traffic is filtered at the firewall based upon the defined rules the firewall applies. Firewalls do an extremely good job of applying these rules, but the rules do not recognize repeated attack attempts or specific attack signatures that are eventually able to find their way past the firewall.

The IDS is trusted to identify these particular attacks and raise the alarm. However, since the IDS is not in-line and does not have any response capabilities, that alarm must be manually validated before any action is taken. Once validated, a security engineer updates the firewall rules to prevent the attack from continuing, hopefully before any significant damage has been done.

Intrusion Detection Network Design

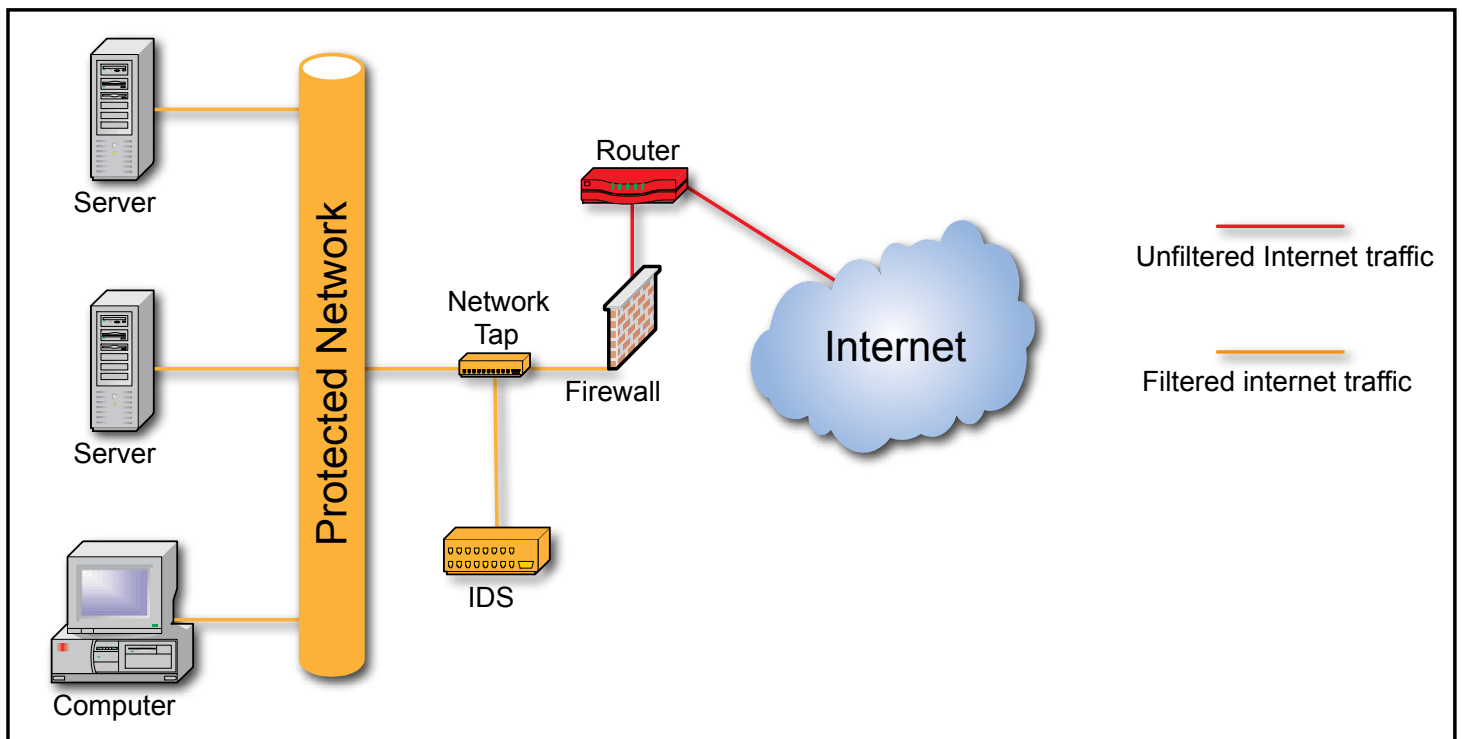


Intrusion Prevention

In the next diagram, Intrusion Prevention Sensors with the ability to actively block attacks are placed in-line. Well-qualified attacks by the IPS result in an immediate response to prevent damage, while questionable activity generates an alert for engineer validation. Similar to a firewall Intrusion Prevention Sensors should be deployed in alignment with critical corporate resources and between internal transit points. Proper placement of Intrusion Prevention Sensors allows for rapid quarantine of affected networks and mitigates the damage of virus outbreaks when users unknowingly bring infected systems into the corporate environment.

The pro-active nature of these devices allows a real-time response to qualified threats. This results in significant reductions in the time and resources required to respond. This efficiency greatly reduces costs associated with the remediation required when a virus or worm wreaks havoc within a network. Intrusion Prevention Sensors are a major step forward against the malicious threats found on the Internet.

Intrusion Prevention Network Design



Managed Intrusion Prevention Services

Ensuring the maximum effectiveness of IPS technology requires a thorough understanding of network services, network baseline behaviors, the security landscape and best practices, and constant vigilance. The unfortunate result of overburdened staffs is often a “set it and forget it” method of deployment—hoping that the technology will simply take care of itself and the organization. In fact, more than 80% of firewalls are not touched 90 days after installation. Such a mindset results in the protection quickly becoming the vulnerability. An unpatched firewall is just as likely an access point into a network as a web or database server. IPS's are less likely than firewalls to be accessed unaware, but without constant vigilance regarding new patches, updates, best-practices, and threshold rules, they too can quickly become more of a burden than benefit. In addition, the stereotype of IDS's generating massive amounts of data and events for analysis holds true for IPS. Properly configuring an IPS, matching that configuration to a particular environment, then maintaining that configuration as the network and security landscape changes is the ongoing challenge when utilizing IPS.

Virtela's Managed Solution

Virtela has been offering Managed IPS Services since the first IPS devices came to market through the equipment vendors. Its team of highly skilled security engineers works to

understand a customer's specific network design and then strategically place IPS hardware in locations that maximize the investment. Virtela then “tunes” the equipment to match the security needs of the specific customer's environment—maintaining that the most important requirement of IPS services is first to “do no harm”. Due to the IPS sitting in-line with network communications, it has the potential to block good traffic mistaken as a threat if not tuned properly. For example, denying corporate users access to the Internet or to the corporate network and applications. Virtela's experience and implementation process with IPS eliminates this concern.

24x7 monitoring, constant tuning, vigilance in reviewing SANS and CERT advisories and recommendations, internal cross-customer knowledge, and the application of security best-practices allow Virtela to offer unmatched capabilities in terms of management of IPS devices. Combined with Virtela's global coverage, award-winning Managed VPN Portfolio, and its robust Managed Security Service's suite, such as Firewall, Vulnerability Scanning, Secure eMail, and event correlation capabilities, Virtela provides world-class secure global networking infrastructures for today's enterprise.



About Virtela

Virtela Communications Inc. delivers award-winning network and security solutions to many of the world's largest and fastest-growing multinational companies. Currently serving customers across six continents, Virtela's network reach spans more than 190 countries. Virtela's unique Internet Protocol Service Fabric (IPSF) and MPLS Service Fabric (MPLS-SF) offer the foundation for delivering all critical business applications via the company's acclaimed service methodology, with a services suite that includes IP-based Virtual Private Networks (VPNs), security services, Voice over IP, Video over IP, and network consulting services. Virtela is headquartered in Denver, Colorado, with a second Network/Security Operations Center in Mumbai, India.

Corporate Headquarters

Virtela Communications, Inc.
5680 Greenwood Plaza Blvd.
Greenwood Village, CO 80111

Phone: +1 (720) 475-4000
Toll Free: (877) 803-9629
Fax: +1 (720) 475-4001

Sales and Product Information

Phone: +1 (720) 475-4445
Toll Free: (866) 261-4607
Fax: +1 (720) 475-4305
www.virtela.com
e-mail: info@virtela.com

Copyright 2005 Virtela Communications, Inc. All Rights Reserved.

"Virtela" and the Virtela logo are registered service marks of Virtela Communications, Inc. All products and service names, marks and slogans of Virtela Communications, Inc. are trademarks or service marks of Virtela Communications, Inc. Products, service names, marks and slogans of third parties may be trademarks or service marks of their respective companies.

VirtelaTM 
a global network solutions company