TECHNOLOGY BRIEF

THE ROLE OF IPS IN THE TELECOMMUNICATIONS AND MOBILE SERVICE PROVIDER INDUSTRY

SOURCEfire®

INTRODUCTION

Telecommunications (telecom) services providers, both fixed line and mobile operators, face common challenges when implementing network-based intrusion prevention. In order to attract customers, businesses must provide the services that those customers demand. To retain those customers, providers must ensure services are secure and available. In order to maintain profit margins, providers must ensure the costs of delivering and securing services are sustainable. Any organization that has a reputation for not providing services, being too expensive, or providing insecure services will lose customers to better-prepared competition.

In this technology brief, we will delve into the business drivers that govern telecommunications providers, explore the technical environment and security challenges that naturally follow, and share use cases where the Sourcefire 3D® System has helped organizations in the telecommunications sector meet their security and business goals.

BUSINESS AND OPERATIONAL DRIVERS

As an industry, a broad mix of often conflicting desires and demands drives telecommunications. Customers, for example, seek out the latest and most stylish smartphones, a broad portfolio of services, and the best coverage—all at the lowest possible price.

The business, in turn, works to provide those service elements while maximizing ARPU (Average Revenue per User) and reducing customer churn. It tries to do so by providing value-added services over and above the basics, delivering reliable and affordable connectivity, and minimizing the impact of service problems.

The operations team faces its own challenges, including the requirement to deliver services in a way that minimizes capital costs and operational overheads. By running a common network infrastructure and using the right software to automate processes as efficiently as possible, staff can concentrate on longer-term objectives—while still responding swiftly to correct problems that impact service levels.

At the proverbial end of the line, the security team is effectively driven by other parts of the business. Business drivers dictate the required services that then dictate the required infrastructure. In turn, the security team is driven to adapt to ensure security policy requirements are met and assets are protected. Consumers, of course, can be quite fickle. Demand can change very rapidly and dramatically. That places the security team—with all of its responsibilities—at the tail end of a process that aims to hit a moving target. Change—sometimes with warning, but more often without—is inevitable, thus requiring the security team to maintain agility and flexibility.

THE TECHNICAL ENVIRONMENT

While they might seem different, fixed and mobile infrastructures share a common high-level approach. Customers connect to the provider backbone network via fixed lines (DS1, cable, leased lines) or mobile networks (GSM/GPRS, 3G, WiFi/WiMax). The endpoint, be it a laptop with a 3G card, a smartphone, a home computer, or any other type of device, is assigned an IP address. Depending on the type of connection, an interface device (DSLAM, MPLS router, SGSN) will transmit IP traffic to the backbone network, performing any necessary translation of the underlying transport mechanisms (fiber, copper, radio, etc.). In most cases, an MPLS network is the primary backbone—it offers huge advantages to the operator in minimizing deployment costs, configuration overhead, and operational support while maintaining the illusion of a secure private network for the customer. Essentially, the MPLS network is a "cloud" to which the provider attaches various other networks and provides Internet access at various points.

On the customer side of the network, there are limited associated security issues. It is relatively straightforward to segregate individual endpoints so they have no visibility of each other, and to route all traffic that crosses the core network directly to and from the Internet. The risk to the provider infrastructure is very low. However, this does not stop endpoints from being used as attack vectors against other systems or networks connected to the Internet—either knowingly through traditional network-based attacks, or unknowingly as part of a botnet.

That is only the beginning of the risks. Networks attached to the backbone provide various other services, some of which are for customers; some of which are for the configuration, management, and maintenance of the network itself; and some of which support the provider's business—it is, after all, an enterprise in its own right.

Customer-accessible services, such as account management portals, are open to the general customer population. Consequently, they must be protected as if they were attached directly to the Internet. Since these systems are also attached to other, more sensitive, provider networks, if customer-facing services are breached it is likely an attacker would then be able to leapfrog to the more sensitive networks, resulting in fraud or unauthorized access to data.

Operational Support System (OSS) networks (typically including CRM, billing, and network and systems management applications) are used to ensure the infrastructure on which services are deployed is properly built, maintained, and managed, and—of ultimate importance to the provider—that proper billing information is collected. The data held on these systems typically includes sensitive customer data, full details on a provider's network and server assets (right down to patch and installed software versions), and in some cases login credentials for network devices and servers. It would not be overstating the case to say that this data must be protected at all costs. Best practice would dictate this, and various control or privacy requirements mandated by regulatory bodies are likely to be in place.

TELECOM AND MOBILE SERVICE PROVIDER SECURITY CHALLENGES

In an ideal world, the security team would have proper input into the design of new and upgraded services, would be forewarned of changes to infrastructure, and yet would be able to react rapidly to unforeseen changes. Sadly, this is not an ideal world. All too often, security is not yet seen as the business enabler it represents, but rather as more of an inhibitor. Even with the best of intentions, service changes may demand infrastructure modifications that are only communicated to the security team as—or after—they happen.

Nor is the security team itself—and the systems which support it—exempt from the need for rapid changes on occasion. With the pace of change imposed by many IPS (intrusion prevention system) and security products, the security team itself can require a huge number of people to ensure security systems are kept up-to-date with changes. Given the cost and time restraints, it makes sense to select security solutions which adapt to such changes with minimal human intervention. Otherwise, costs become unmanageable, human error and omission introduce points of weakness, and the business risk increases because of reduced visibility and awareness of the infrastructure.

Any IPS solution is capable of generating large numbers of intrusion events. It is easy to block these events, and this most basic of capabilities is found in all major IPS solutions.

However, real attacks may yet be lost in all the noise, and security staff may be unaware of the extent of any real attack or compromise. Without context, it is difficult to sort through events and work out which are relevant. Sourcefire's passive network analysis capability (Real-time Network Awareness) provides the information required—such as operating systems and applications in use—to understand the context of an event. In addition to expediting the evaluation of events by individuals, that contextual data can be used to match attacks to individual resources and to automatically determine if an event is relevant. A further benefit is the ability to automatically modify in-use rulesets to precisely reflect the actual configuration of a network.

Even with the best security systems in the world, breaches sometimes do occur. After a compromise, the typical IPS is useless. However, Sourcefire's real-time ability to determine that something has changed in the environment assures that the Sourcefire 3D System maintains its relevance and utility. As was the case with attacks, we continue to grapple with the issue that detection software is capable of generating a massive number of alerts. The challenge here is less in identifying the activity, but in determining which activities are inappropriate or that violate policy.

The necessary element here is policy, the ability to define what activities are permissible in a given environment. If we can combine these two elements—policy definitions and deep insight into the network environment, we leverage the combined abilities of humans and automation to tell us things about our environment that we need to know—not to mention the development of reflexes that are, quite literally, inhumanly fast.

NETWORK IPS USE CASES

The following network IPS use cases are taken from actual Sourcefire customers. In each case, Sourcefire has provided the highest possible protection to the customer, meeting the business, technical, and security requirements while ensuring that the operational and financial overheads are contained.

Protecting Service Platforms

A major mobile provider has deployed service platforms, such as weather forecasts, news, and account management services, in a multi-tiered DMZ accessible to mobile phone users. These services, providing light, rapidly-downloaded web pages, are designed for customers with phones. However, they are also visible to attackers with more sophisticated computing devices and attack tools. Network IPS has been deployed on several of the most visible DMZ layers as a defense against attackers.

The business may require that service capabilities in the DMZ be scaled up, changed, or modified completely to keep up with the changing business and competitive environment. Traditional IPS environments need constant tuning of rulesets and other settings to ensure the right protection is in place and false positives are reduced. This provider has opted to deploy Sourcefire RNA® (Real-time Network Awareness) and Sourcefire IPS™ to support this requirement. RNA's ability to passively identify operating systems and applications provides two major benefits to this customer. First, events generated by the IPS can be automatically viewed in context. For example, if a Unix system is attacked with a Windows exploit, then the event is ignored. However, the same attack against a susceptible operating system is marked as requiring further investigation. Sourcefire customers routinely see reductions of between 95 to 99 percent in the volume of events requiring analysis by a human operator. Secondly, the real-time, all-the-time knowledge of assets and applications can be used to tune the IPS ruleset automatically, with complete confidence that the correct rules are deployed. This reduction in effort of the two most burdensome tasks in IPS use—tuning and event analysis—allows IT security staff to concentrate on strategic goals, rather than firefighting.

In this instance, the business benefit is both the reduction in effort and cost required to maintain the IPS solution, and the increase in business visibility to potential risk through the reduction in the number of events to be analyzed.

Fraud Prevention and Detection

A large mobile operator deployed Sourcefire IPS sensors at points where traffic from its mobile radio networks is converted to IP traffic (i.e., near the GGSN). Vulnerabilities in the protocols used for signaling and transport of traffic mean they are susceptible to fraud if attackers can frame the traffic properly.

The Sourcefire 3D System protects this environment with a combination of "out-of-the-box" detection capabilities, combined with the customization made possible by the underlying IPS detection engine—Snort®. In this case, rulesets to examine mobile-specific traffic protocols at the GGSN have been developed and implemented by the customer.

The ability to detect and stop attempts to exploit vulnerabilities in network protocols specific to the mobile environment is a significant benefit to the operator, since it prevents revenue loss through fraudulent avoidance of proper billing.

Ensuring Outsourcer Compliance

Service providers, as is common in other industries, use external organizations to assist in the tasks of developing, maintaining, and operating software. Contracts between a provider and outsourcers often include provisions relating to the protocols to be used to connect to the contracting company's network. These arrangements typically dictate the use of a protected VPN, while forbidding the use of potentially risky network protocols, such as RSH, Telnet, and others. While the VPN provides a level of protection, especially when combined with other routine contract provisions dictating "air gaps" between outsourcer systems used to connect to the contractor's network and other networks, it still falls to the contractor to "trust, but verify."

One large provider has just such a contract in place with an external software developer. To reduce operational burdens and provide increased support responsiveness—with the goal of ensuring that the provider's customers are properly serviced—the software developer is allowed to support the software remotely. The contract specifies, among other provisions, that "in the clear" protocols, such as Telnet, FTP, and Rlogin, are not to be used. The provider implemented Sourcefire IPS and RNA inside their network, after the VPN entry point, in order to verify the compliance of the outsourcer with the contract terms. The goals were to ensure that the provider systems were protected by attack (deliberate or inadvertent; for example, by virus infection) and to monitor the protocols used by the outsourcer. RNA can make use of the data gathered passively about operating systems and applications it sees to match against policies. In this case, a "white list" specifies which applications and operating systems are allowed on specific segments of the network—the discovery of anything not matched in the white list generates a compliance violation event.

As might be expected, within days of implementation it was discovered that the outsourcer was, in fact, using Telnet to access the systems it was maintaining. The discovery provided the contractor with the opportunity to remind the outsourcer of its contractual obligations. This enabled the company to reduce its exposure to any additional risk introduced by allowing an external organization access to its critical internal systems.

Monitoring Mobile Endpoint Activity

Monitoring customer activity on provider's networks poses a complex legal and ethical challenge. There is often a regulatory requirement to ensure customers are protected from attack or infection by other mobile endpoints, in combination with a business need to reduce liability and improve the quality of service offerings. As a result, there is a desire to monitor traffic from mobile endpoints as it traverses internal networks to and from the Internet. However, there are also privacy constraints limiting the ability of service providers to examine customer network activity. This tension is heightened, since many jurisdictions enforce different standards in this regard. Thus, in the United States, for example, individual states have differing laws and regulations regarding the monitoring of private communications. A similar problem exists for pan-European operators where some countries, notably Germany, prohibit the interception of traffic—while others do not.

The challenge for network operators is obvious—to provide relevant protections to the consumer, by deploying IPS sensors and policies that protect both themselves and the prospective customers, while still complying with local laws and regulations.

One network provider chose the Sourcefire 3D System to address these issues for several reasons—the level of protection afforded and ease-of-use being chief among them. In addition, the 3D System's architecture and centralized management through Sourcefire Defense Center® allows for easy management of multiple, different policies on multiple, different IPS sensors. This capability uniquely provides both a cost-effective and efficient solution to this challenge. Policy Layering, for example, allows for a standard policy to be developed that covers the security policy for the business as a whole. That base policy is then used as a starting point, where country-specific policy definitions can be added to turn specific protection features on or off, according to local requirements. If changes are made to the base policy, the country-specific layers will have a higher precedence, overriding changes resulting in a breach of regulations.

The benefit to this customer in choosing the Sourcefire solution was the elimination of the management overhead introduced by the complex web of local laws and regulations. The Policy Layering feature, combined with the distributed management capabilities of the Sourcefire 3D System, allowed this operator to give local legal and operational staff the ability to monitor deployed policy to ensure local compliance, all the while maintaining the highest possible global security posture and providing a consolidated view of the IPS operations.

Protecting Operational Support Systems

Proper deployment, configuration, and management tools are essential to ensure network services are built correctly, infrastructure failures are detected and rectified properly, and correct data is gathered relating to customer activities to ensure accurate billing. These activities, of course, are the province of Operational Support Systems. OSS-generated data is, in turn, often passed to CRM systems that contain customer-specific data and which may be subject to the PCI DSS (Payment Card Industry Data Security Standard), or other standards subject to auditing, security, or privacy.

OSS tools themselves may well contain vulnerabilities that would allow unauthorized remote access. The tools routinely collect large amounts of sensitive data—IP addresses, network equipment and server operating system and application software versions, personally identifiable information (PII) relating to customers, and in some cases server and network device account names and passwords. Access to this sort of data would enable a malicious intruder to cause untold damage to the infrastructure, or to gather large amounts of sensitive data.

Traditionally, OSS systems used to build and manage telecommunications environments have been accessed by authorized staff through protected networks. Increasingly, though, these systems have links to other networks added to perform their primary functions more efficiently. In addition, customer self-service initiatives have prompted broader access to these sensitive systems. Regardless of the innate security of the added networks, each link provides an attack vector which can be used to reach highly sensitive systems.

The placement of Sourcefire IPS at the interface where OSS tools connect to their managed elements or additional networks will provide enhanced security in similar cases. In addition, using RNA to monitor running services allows the provider to prove compliance based on RNA's white list functionality. This technique can also be used to ensure newly-installed systems meet the baseline configuration and would catch accidental misconfigurations early enough to allow rectification.

The business benefit in this case is to reduce the business exposure due to undiscovered vulnerabilities in complex software essential to the operational running of the network. By securing those systems independently of any vendor-supplied controls, an extra level of assurance is provided.

Protecting the Internal IT Environment

We cannot forget that the service provider is also a business in its own right. Therefore, in addition to all the components specific to supporting a provider's business, it needs all the tools that other enterprises need—Human Resources, e-mail, Intranet, and so on. There is also a need to deploy IPS systems in more traditional ways—to protect DMZs, data centers, and the IT assets used by employees in the normal course of business.

A service provider implemented the Sourcefire 3D System in its internal network, protecting its data centers. One of their employees returned to the office carrying a work-issued laptop that had been infected by Conficker. Sourcefire was able to detect the laptop's attempts to infect other systems and to communicate externally, and was able to block them in real time. Sourcefire RUA™ (Real-time User Awareness) was also able to link the IP address of the infected system with the actual user's name in real time, allowing the infected system to be quarantined within minutes of events being detected.

There is a clear business benefit here in reducing the time taken to respond to a security incident and the ability to contain an infection to a minimal number of systems. As a side effect, the laptop was disinfected and returned to the user within a day or so, allowing the employee to continue working normally in a shorter time than would have otherwise been possible.

SUMMARY AND CONCLUSIONS

Dramatic changes in the topology and structure of telecommunications networks have introduced a number of completely new security issues, while reinforcing more traditional concerns that have existed for years. The broad reach of standard, out-of-the-box security capabilities delivered by the Sourcefire 3D System—along with extensive customization capabilities—has been shown to provide a robust and efficient solution for these demanding security environments.

In this technology brief, we have briefly discussed these environments and demonstrated ways that the 3D System is uniquely capable of addressing the specific network security needs of telecommunications providers. Although the 3D System offers extensive customization and integration capabilities, with one exception, organizations realized these benefits simply through out-of-the-box product capabilities.

The key benefits telecommunication provider customers have realized after adopting the Sourcefire 3D System are:

- Reduced operational management overhead and cost
- Increased staff productivity through reduced time to identify and remediate ongoing security incidents
- Reduced risk profile through increased security around critical systems and improved monitoring of external connections to critical systems
- Reduced risk through reduction in failure to comply with local regulations
- Reduction in billing losses through mobile environment-specific fraud prevention

To learn more about the Sourcefire 3D System, visit our website at www.sourcefire.com or contact Sourcefire or a member of the Sourcefire Global Security Alliance today.

Acronym Glossary

3G: 3rd Generation, International Mobile Telecommunications (IMT-2000)

ARPU: Average Revenue per User

CRM: Customer Relationship Management

DS1: Digital Signal 1

DSLAM: Digital Subscriber Line Access Multiplexer

GGSN: Gateway GPRS Support Node

GSM: Global System for Mobile Communications

GSN: GPRS Support Node

GPRS: General Packet Radio Service

MPLS: Multi Protocol Label Switching

OSS: Operational Support System

PII: Personally Identifiable Information

RSH: Really Simple History

SGSN: Serving GPRS Support Node

WiMax: Worldwide Interoperability for Microwave Access