How Software-Defined Firewalls/WAFs Enable Communications Companies to Secure Networks, Grow Revenue and Comply with Regulations

INDIGO SOFTWARE

WHITEPAPER

EXECUTIVE SUMMARY

Compared with most businesses, today's communications service providers (CSPs) face much larger challenges, which often include managing nationwide networks and millions of users. An increasingly complex regulatory environment and an expanding legislative agenda creates additional hurdles for CSPs and their security teams. Government regulations range from banning the use of encrypted messaging and VoIP over telco networks to requiring cloud service providers and device manufacturers to drop support for virtual private networks (VPNs). In addition, CSPs must protect themselves and their service provider and enterprise customers from risks such as fraud, malware, and distributed denial of service (DDoS) attacks. If they do not, their reputations could be irreparably harmed.

Ponemon INSTITUTE

The cost of non-compliance, including fines, business disruption and losses in productivity and revenue, currently stands at around $14.82 million.

Coping with this increased scrutiny and more stringent accountability—not to mention increasingly sophisticated bad actors—means communications companies must enhance their control, monitoring, reporting and compliance capabilities. This challenges network operator SOC teams to achieve full visibility into network traffic. It may also require controlling prohibited traffic such as VoIP or encrypted apps as well as retaining data for compliance audits.

However, the need to block or control certain types of traffic potentially creates a "Catch-22" for CSPs because they typically depend on bandwidth usage to generate revenue. In other words, considering the boundless creativity of people who want to circumvent controls, how can security teams achieve two mutually exclusive goals: limiting "bad" traffic without limiting access to the "good" services that subscribers want. Unless they deploy the right technology solution, this could essentially require shutting down access to large swaths of the Internet in order to control access and comply with government regulations.

Gartner

Over 70% of security vulnerabilities exist at the application layer, not the network layer.

But the cost of not deploying adequate security solutions is enormous. According to a December 2017 study by the Ponemon Institute, the cost of non-compliance, including fines, business disruption and losses in productivity and revenue, currently stands at around $14.82 million per incident. And for CSPs, the loss of revenue due to reduced subscriber bandwidth usage caused by inadvertently blocking popular Internet services can run as high as 20% of revenue or more. So security teams at CSPs find themselves tasked with trying to balance the significant risk of non-compliance with business needs for revenue generation and customer satisfaction. Plus, the challenge has become amplified by today's bad actors who use sophisticated techniques—such as mimicking Google or AWS addresses—to circumvent controls. Constantly evolving efforts by dedicated hackers also make it very difficult to comply with regulations without limiting subscribers' access to key communications and Internet services.

Bad actors present other threats to CSPs, such as DDoS attacks on their networks and on the hosted websites of their customers. ISPs and other communications network operators also need to protect their customers from malware and APTs. They further need to protect their networks from web application layer attacks, which can penetrate back-end systems to cause mayhem or steal valuable and often confidential data. This creates a huge vulnerability because most firewalls are designed to protect the network. However, according to Gartner, over 70 percent of security vulnerabilities exist at the application layer, not the network layer.

All these risks also need to be considered in context of scale. CSP companies typically operate networks that are many times larger than the typical enterprise, often spanning entire countries, which makes their security challenges exponentially larger. CSPs have other unique needs when compared with enterprises, such as requirements for security measures to work with carrier-grade reliability, at line speed, and without causing downtime or otherwise negatively impacting the customer experience.

This white paper looks at the security and compliance requirements of CSPs and ISPs. It also takes a close look at one of the first next-generation firewall and web application firewall (WAF) solutions designed to provide network and application layer security on a very large scale.

Unique needs and challenges of network operators

Corporate security teams face huge challenges to maintaining the security and availability of enterprise networks that may serve thousands or tens of thousands of employees. But SOC teams at communications network operators must keep sometimes millions of customers or even an entire country secure and satisfied. Operators of such large-scale communications networks include:

- Telcos
- Mobile network operators
- Fixed ISPs
- Wi-Fi operators
- Satellite Internet providers
- Cloud hosting providers

Governments want to prevent terrorists and criminals from hiding communications

In many countries these CSPs also face unique regulatory challenges as well. For example, governments may want to block secure messaging apps like Signal, which could be used by terror groups or criminal elements. For instance, in early 2018, media regulators in Russia mandated network operators block the Telegram encrypted messaging app, citing the need to monitor potential terrorists. Russia's main security agency had claimed the bomber who killed 15 people in the St. Petersburg subway in 2017 used the app to communicate with accomplices. They went so far as to call Telegram "the messenger of choice for international terrorist organizations in Russia".

Regulators protect incumbents by stopping the free ride of OTT services

'Over-the-top' (OTT) services—applications that use the Internet and IP protocol—have also caught scrutiny from government regulators. IP has separated network carriage from content and allowed content and applications providers to deal directly with end users over networks whose owners and operators are excluded from these transactions. Internet telephony, or Voice over the Internet Protocol (VoIP), for example, has major implications for the business models of both fixed and mobile network operator incumbents and national carriers. Even text messages, encrypted or not, are often carried for free over communications networks, which can impact the revenues of fixed and mobile operators. Therefore, some governments have passed regulations requiring the blocking of these services to prevent the destabilization of existing industries, including government-owned carriers. Compliance with these laws can mean blocking VoIP calling and videoconferencing services like Skype or Line that compete with traditionally telephony.

ABOVE AND BEYOND ENTERPRISE FIREWALLS – A SOLUTION DESIGNED SPECIFICALLY FOR LARGE-SCALE NETWORK OPERATORS

This regulatory environment—as well as privacy laws and other increasingly stiff regulations—puts network operator SOC teams in a tough spot. Sophisticated obfuscation techniques make it difficult to block VoIP and messaging traffic without shutting down access to essential Internet destinations and services like Google search. One popular tactic is called Domain Fronting. According to Amazon, "Domain Fronting is when a non-standard client makes a TLS/SSL connection to a certain name, but then makes a HTTPS request for an unrelated name. For example, the TLS connection may connect to 'www.example.com' but then issue a request for 'www.example.org'. In certain circumstances this is normal and expected. For example, browsers can re-use persistent connections for any domain that is listed in the same SSL Certificate, and these are considered related domains. But in other cases, tools including malware can use this technique between completely unrelated domains to evade restrictions and blocks that can be imposed at the TLS/SSL layer."

Domain fronting and other obfuscation techniques allow legitimate and illegitimate users of prohibited services to masquerade as popular web services. From a revenue and customer satisfaction perspective, blocking these services is not practical. Consequently, SOC and compliance teams need a new type of tool that goes beyond the next-generation firewalls that are de rigueur among today's enterprise security teams. And while Google and Amazon disabled some aspects of domain fronting in April 2018 in response to pressure from Russia, hackers and illicit users are constantly evolving their tradecraft. This means any solution must have the flexibility and capability to detect and block new techniques or new apps. Meeting all these large-scale network operator challenges requires a solution that provides:

- Real-time decoding capability
- Ability to detect the newest applications (encrypted or unencrypted)
- Automated controls and methods for establishing policies
- Granular visibility that enables SOC teams to solve issues on the individual subscriber or service level
- Minimal false positives
- Real-time inspection of traffic that does not degrade network performance

Communications network operators also face many of the threats common to enterprises. DDoS attacks are increasing in frequency and scope—the latest involving Botnet armies of hijacked IoT devices. And ISPs need to protect not only their own networks from outages caused by these attacks but also the hosted services of their subscribers. In addition, Network operators need to protect their own web servers as well as their subscribers' web servers from increasingly sophisticated application layer attacks—e.g., hackers can take down a website or provide a pathway for attacks such as SQL injections into vital backend systems to cause malicious damage or steal confidential or personal protected data. Malware, including hard-to-detect zero-days and APTs, can also cause a breach.

Of course, any attack that exposes personal and private customer data brings on serious compliance issues regarding privacy regulations. This has always been a major concern but has grown in importance with the advent in May 2018 of the European Union's General Data Protection Regulation (GDPR), which carries huge fines (up to 4% of global revenue) for noncompliance and impacts companies far beyond European borders.

HOW THE INDIGO SOFTWARE-DEFINED FIREWALL/WAF MEETS THE REQUIREMENTS OF LARGE-SCALE NETWORK OPERATORS

Recognizing these unique needs, Indigo Software spent years of research and development creating a next-generation firewall and web application firewall solution designed specifically for large-scale network operators.

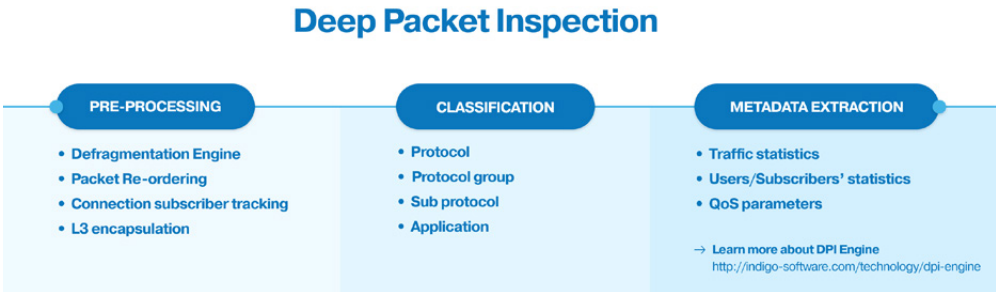
The Indigo Software-Defined Firewall (SDF) / WAF combines next-generation firewall capabilities such as data leakage prevention (DLP) with deep packet inspection (DPI) and advanced scripting engines—all within a software—defined architecture that gives SOC teams unparalleled flexibility and agility. It also receives weekly protocol and application signature updates to enable real-time visibility into applications traffic over large-scale networks with high—throughput and carrier-grade reliability. SOC teams can easily integrate the solution with existing infrastructure without the need for extensive custom development and maintenance. And as an inline appliance, it easily and transparently deploys within days and with zero network downtime.

ROHDE&SCHWARZ
Cybersecurity

Rohde & Schwarz Cybersecurity is a leading vendor of deep packet inspection software that adds protocol and application classification capabilities to network analytics, traffic management and cybersecurity solutions.

Industry-leading DPI engine for real-time visibility

Deep packet inspection is an advanced form of packet filtering that examines and manages network traffic. Unlike conventional packet filtering, which examines only packet headers, DPI looks in detail at the contents of the data packets traversing a network. It identifies, classifies and detects packets with data payloads that hackers have obfuscated—e.g., executables concealed in an HTTP request—or for other reasons traditional packet analysis cannot detect. These capabilities make DPI a critical tool for SOC teams seeking to not only gain more thorough visibility into their networks but also control unwanted or potentially malicious traffic.



The Indigo SDF embeds the R&S® PACE2 DPI engine from leading German cybersecurity partner Rohde & Schwarz. It provides powerful and extremely reliable detection and classification of thousands of applications and protocols by combining DPI and behavioral traffic analysis—regardless of whether the protocols use advanced obfuscation, port hopping techniques or encryption. The Indigo SDF restores visibility into network traffic made opaque by encrypted applications and obfuscated or masked by traffic path techniques such as Domain Fronting.

Embedding DPI technology also results in far more detailed logs, providing valuable information when dealing with security incidents, policy implementation, and compliance audits. In this way, SOC teams can accept or deny specific application requests or commands, giving them a far greater degree of granular control over network traffic.

In addition, the DPI engine meets network operators' increasing needs for fast performance, high application and protocol classification accuracy, and a very low memory footprint of the DPI engine. The R&S® PACE 2 solutions also includes an easy-to-integrate software library that operates in real time at up to 32 GBps per core—the industry's fastest performance.

WAF capabilities designed for large-scale communications networks and ISPs

With the embedded DPI technology in the Indigo Software application-layer filtering system, the firewall can be deployed as a WAF with the ability to reach beyond network addresses and ports. Its advanced traffic analytics capabilities make it possible to carefully examine the entire communication between clients and web applications and make it more secure. Indigo WAF capabilities include:

- Virtual patching
- IP reputation
- Web-based malware detection
- Webshell/backdoor detection
- DDoS detection
- Botnet attack detection
- Anti-Virus scanning of file attachments

Software-defined architecture enables flexibility and agility

Indigo also developed a software-defined architecture that includes a breakthrough scripting engine—employing a modern scripting language—that offers SOC teams extreme flexibility and agility when establishing policies. These policies can control subscriber activity such as use of VoIP and encrypted messaging apps or access to prohibited or malicious URLs, and SOC teams have granular control down to the individual subscriber, application, or site level.

Indigo SDF policies are written as scripts based on the Lua programming language.

Indigo SDF policies are written as scripts based on the Lua programming language and provide the following features:

- **Flexibility:** Policy rules, lists and objects can be integrated with external systems (RADIUS, SQL, HTTP, etc.) and data feeds (IP reputation database and malware hash lists); data can be arbitrarily processed (JSON, XML, CSV, etc.).
- **Just-in-time compiler:** Scripts are compiled to native x86 machine code for optimal performance.
- **Dynamic reload:** Scripts can be reloaded live in production without restarting the firewall, and all state information is retained.
- **Sandbox:** Scripts are memory-safe and sandboxed; errors in scripts cannot crash the main firewall processes.

In addition, an Elastic/Kibana (ELK stack) integration enables greater visibility of metadata and logs, while further simplifying management and speeding incident response time. The powerful open-source capabilities of the ELK stack offer another key benefit for budget-constrained security teams—eliminating the need for a costly SIEM.

Provides core next-generation firewall capabilities

The Indigo SDF provides all of the integrated next-generation security of a next-generation firewall along with centralized management. WAF capabilities also defend against SQL injection and other application layer attacks, while anti-DDoS protects the availability of not only your network infrastructure but also subscribers' hosted services. Core capabilities include:

- Network security monitoring
- Intrusion detection system
- Intrusion prevention system
- Data leakage protection
- Web application protection
- DDoS protection
- Historic and real-time threat reporting

NETWORK OPERATOR BENEFITS

The Indigo SDF is specifically designed to streamline compliance while enabling network operators to instantly increase achieve business benefits by reducing false positives. CSPs can boost subscriber bandwidth usage—and revenue—by enabling uninterrupted access to popular Internet services. They can also quickly and cost-effectively comply with government mandates such as monitoring and controlling apps and access to harmful websites or blocking IP telephony (VoIP). Capabilities include:

- Easier data retention and recall
- Governs access to websites / URLs
- Governs applications traffic — including encrypted messaging
- Blocks protocols / proxies / VPNs
- Controls prohibited traffic without hindering access to key communications and Internet services
- Increases network operator revenue by minimizing false positives
- Eliminates need to for custom development and maintenance with regular application and protocol updates

Case in Point — One of the World's Largest Mobile Operators

The Indigo SDF Is currently in-line at large-scale deployments such as monitoring and controlling traffic at national telecom companies or powering the entire Internet infrastructure of a country. It was deployed by Russia's largest mobile operator, which has some 70 million subscribers in Russia and more than 35 million subscribers in several Central Asia countries.

elastic

Creators of Elasticsearch, Kibana, Beats, and Logstash — the Elastic Stack. Securely and reliably search, analyze, and visualize your data.

For this Indigo customer, blocking unwanted traffic such as secure messaging apps, which can circumvent security measures by using domain fronting, was a challenge. As described earlier in this paper, many popular services like Google and content delivery networks (CDNs) such as Amazon Cloudfront, Azure and Akamai can mask secure messaging traffic with techniques that make it look indistinguishable from other "normal" traffic. In other words, when a Signal or Telegram user, for example, sends a message it may look like a normal HTTPS request to www.google.com. So shutting down secure messaging traffic would essentially shut down the Internet, which would have unacceptable consequences because, like many mobile operators, this customer depends on satisfied mobile subscribers and charging for bandwidth usage.

As a result of deploying the Indigo SDF / WAF, subscriber satisfaction greatly increased. More important, the customer instantly saw significant improvements in revenue—20% or greater. Prior to deploying the Indigo Software solution, the unacceptable number of false positives in previous vendors' products made it difficult to balance compliance with revenue-generating access to online services.

CONCLUSION

Mobile, fixed-line telco, satellite Internet and cloud services providers as well as ISPs face unique challenges. Next-generation firewalls designed for enterprises are not up to the task of protecting their large-scale networks because they cannot provide the real-time visibility into encrypted and unencrypted app traffic on the level of a nation-state. They lack the throughput to support millions of users or flexible and agile means for SOC teams to establish policies as well as other must-have capabilities. More important, these enterprise network firewalls, WAFs, and other solutions such as open source security measures also deliver too many false positives, which reduces revenue due to decreased bandwidth charges.

The Indigo SDF is a multi-vendor solution designed specifically for network operator Security Teams that need a customized, personalized Firewall / WAF solution to address today's complex security and compliance concerns. It combines next-generation firewall features with a software-defined architecture to simplify complex security management. The industry's highest-performing DPI engine also provides near-real-time visibility into network traffic.

Plus, it gives mobile, fixed telecom, satellite data and ISP SOC teams the flexibility to establish policies for controlling applications and user access to URLs using a modern scripting language. An Elastic Stack integration, which includes the Kibana dashboard, further simplifies management and speeds incident response time. The Indigo SDF is also designed from the ground up as a carrier-grade security technology, enabling it to deliver line-speed performance and high availability. These capabilities range from 10G wire-speed throughput to hot standby to minimal latency.

The result is easier, more effective compliance, fewer false positives (which translates into more subscriber revenue), greater customer satisfaction and fewer burdens on SOC teams.

INDIGO SOFTWARE

Address:
15-01 Valley Point
491B River Valley Road, Singapore 248373

Voicemail:
+65 3158 1070

E-mail:
info@indigo-software.com