

Providing managed security services on a global basis



iPolicy Networks' Intrusion Prevention Firewall and iPolicy Security Manager provide a powerful suite of tools for service providers who are seeking to offer high-value managed security services on a geographically distributed scale.

Case Study

EXECUTIVE SUMMARY

Industry:
Telecommunications

Environment:
Headquartered in Overland Park, Kansas, Sprint is one of the world's largest global telecom carriers serving high-speed data, networking and managed security services to corporate customers in more than 100 countries.

Key Business Challenge:

- Best-of-breed URL/content filtering and Firewall capabilities
- Scalability of the managed security service to serve hundreds of customers
- High availability and reliability of the managed security service

Key Business Solution:

- Deployed iPolicy IPF solutions with Stateful Firewall and URL filtering capabilities.
- Implemented iPolicy ISM security management solutions to provide centralized management with distributed control, allowing end-customers to manage their security settings and view/generate reports

Key Business Benefit:
Sprint has added a valued new service offering that provides end-customers with a flexible, scalable and easily managed URL filtering and stateful firewall solution.

▶ iPolicy Networks solutions enable Sprint, one of the world's largest global telecom carriers, to provide managed security services to safeguard its customer networks.

Background

Carriers the world over are seeking to transform their existing broadband network investments into additional profit-generating models. Given the importance of restricting questionable content and optimizing traffic for enterprise customers, a network-hosted and managed security service offering can be a valued added service by helping these organizations increase their workforce productivity and decrease labor, legal and bandwidth costs.

Challenge

Sprint, headquartered in Overland Park, Kansas, provides a broad range of communications services to domestic and international businesses, from multinational corporations to smaller businesses. Like many progressive service providers, Sprint was interested in leveraging its extensive network infrastructure, deep knowledge of networking, and operational support infrastructure to provide value-added services that would counteract the commoditization of other services such as bandwidth. Network security as a hosted, or managed, service leverages these key strengths to deliver a highly valued service for Sprint's customers because a) network security is relatively complex, and requires knowledge and expertise to manage; b) the ever changing nature of network threats requires frequent updates and modifications, which in turn add management and employee overhead; and c) a service provider's vantage position in the core of the network allows faster response to current and new threats, and delivers cleaner "pipes" to the end-customer

The MSSP Model Protects Confidential Information

As a managed security services provider (MSSP), Sprint can offer its customers several advantages in its managed URL Screening and Firewall service offering: a) Customers benefit from complete control over their Web traffic by enforcing corporate policies and the service secures outbound flows of information to reduce risk of unauthorized communication; b) The service can protect against information breaches and unauthorized access to confidential digital assets (e.g. patents, intellectual property, credit card information); c) Regulatory and internal privacy policies are more easily enforced, protecting customer or patient information from breaches or access in violation of Sarbanes-Oxley, HIPAA and Gramm-Leach-Bliley; d) The service can prevent access to restricted or offensive content, such as pornography or copyrighted material.

Solution

iPolicy Intrusion Prevention Firewalls (IPFs) are deployed at strategic points of presence (POPs) across Sprint's network to offer the managed security services. The systems are interconnected with the aggregation routers, which use a combination of Virtual Routing technology and Policy-Based Routing to direct Web traffic from the customer networks to the IPFs. All Intrusion Prevention Firewalls have a corresponding 'virtual IPF' for each customer who is subscribed to the URL Screening and Firewall service. The aggregation routers tag each customer's Web traffic with a unique VLAN, which is used to uniquely identify and enforce customer-specific policies on the network traffic. Customer traffic identification helps the IPFs generate reports and logs on a per-customer basis.



Results

The key advantages that iPolicy offers to MSSPs (managed security service providers) are:

An architecture based on the patented Single Pass Architecture™ that allows carriers to scale across three critical dimensions while maintaining line-rate security and minimal latency: (i) number of security applications supported per appliance; (ii) number of policies per security application; and (iii) number of customers supported per appliance.

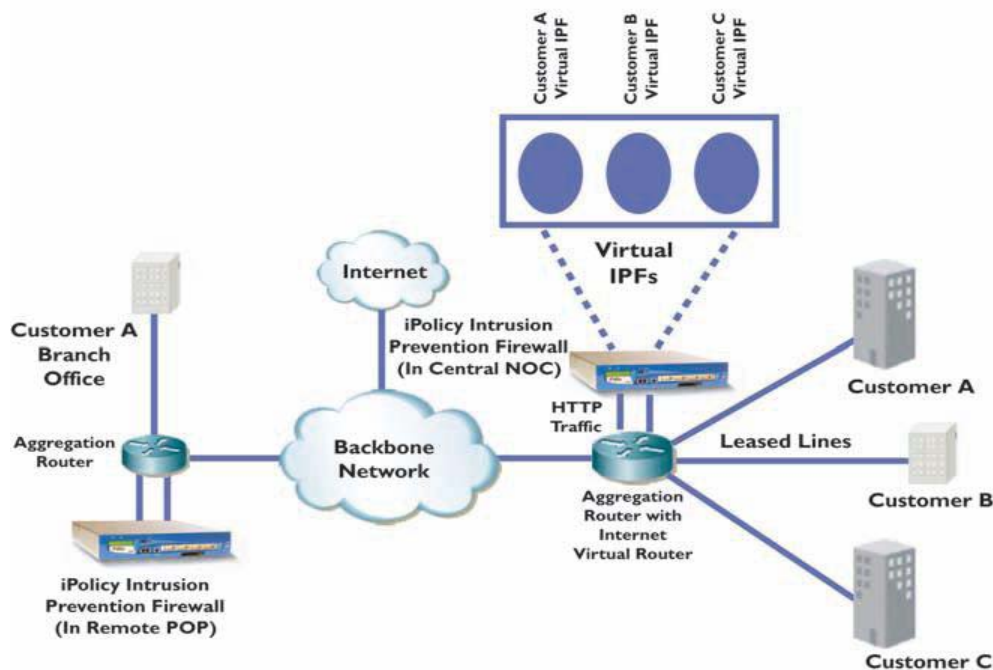
Centralized security management with distributed control. The iPolicy Security Manager allows a service provider to configure security applications and policies for new customers, minimize management of updates and service changes for existing customers, and provide detailed security information to their customers via reports. The ISM achieves its industry-leading scalability through the ability to allow individual components of the ISM to be distributed across several machines.

Customer co-management rights for enterprise administrators are provided through the iPolicy ISM. This capability can be offered as a premium service, and also helps offload routine, day-to-day management tasks to the business end-customer.

Sprint can scale the iPolicy solution globally by deploying multiple IPFs across its regional POPs, providing geographical proximity to enterprise customers who have offices dispersed around the world. Localized presence helps improve response time and the overall user experience. Even though enterprises are globally distributed, Sprint can continue to manage its customers' security services with the centralized iPolicy Security Manager.

The ISM supports Security Domain™ technology, which allows Sprint to group multiple virtual IPFs together and enforce policies, and generate reports and logs, on a per-customer basis, thus reducing the overhead of managing enterprises with hundreds of locations across different IPFs. An enterprise with multiple locations can be managed as a single Security Domain, while maintaining consistent security policies throughout with a centralized reporting and logging infrastructure. The ISM also supports co-management capabilities, whereby customers can log into the management system (controlled by access rights) to view and generate reports, view logs and/or edit policies across one or multiple locations.

Figure 1 - Network diagram showing deployment of iPolicy's Intrusion Prevention Firewalls in the central Network Operations Center (as virtual Intrusion Prevention Firewalls) and in a Remote Point of Presence.



Summary

Through the iPolicy integrated network security solutions, Sprint has leveraged its network infrastructure to provide a valued managed security service to its customers. iPolicy's virtualization capabilities allow Sprint to minimize the number of devices to deploy and manage, providing a distinct advantage in serving customers while significantly lowering the total cost of ownership.