

# Security “in the cloud”

Carrier A provides enterprise-class managed security services



*iPolicy Networks' Intrusion Prevention Firewall provides services providers and telcos with carrier-grade managed security services that protect their customers from worms, viruses, Trojans, DoS/DDoS attacks and blended attacks.*

Case Study

## EXECUTIVE SUMMARY

**Industry:**  
Telecommunications

### Environment:

The carrier is headquartered in North America, sells to virtually all the Fortune 1000 companies, and is a household name throughout the world. The carrier is known for its leadership in offering value-added services to its business customers.

### Key Business Challenge:

- To leverage the existing network to offer value-added services that would increase ARPU
- 24 x 7 uptime

### Key Business Solution:

- Implemented iPolicy IPF solutions with Stateful Firewall, IDS/IPS, and URL filtering capabilities
- Implemented iPolicy ISM security management solutions to provide centralized management with distributed control

### Key Business Benefit:

The carrier has added a compelling security service offering that generates much more revenue per month per leased line, and achieved positive ROI in less than a year.

**➤ iPolicy Networks solutions are helping one of the largest telecommunications carriers in the world to deliver managed security services that protect its corporate customers from current and emerging network threats.**

## Background

Worldwide, carriers are looking for ways to leverage their existing networks to offer value-added services. Given the importance of security to enterprise customers, a managed security service allows the carrier to transition from simply selling bandwidth to selling “clean” and secure bandwidth. In so doing, the carrier increased revenues per leased line by a factor of three to six.

## Challenge

As carriers see their average revenue per customer (ARPU) declining and bandwidth increasingly becomes a commodity, progressive service providers are looking to offer value-added services that leverage their large networks, proficiency in IP networks, and expertise in operations. Network security is an ideal service for a network-hosted offering because a) it is complex and requires significant expertise to manage; b) it is dynamic, requiring regular updates to various security modules, a process that can be expensive for an enterprise to manage, and c) it can be offered more effectively from within the service-provider network as opposed to the perimeter of an enterprise network. It was, therefore, a natural progression for Carrier A to issue an industry-wide RFP in 2001 to select a vendor for its managed security service offering.

## A Compelling Value Proposition

Carrier A offers several advantages in offering a managed security service from within the network: a) Economies of scale that allow the service provider to amortize the cost of equipment that is needed at the edge of the network to inspect each and every packet from Layer 3 through 7, while providing line-rate security and introducing minimal latency. b) Knowledge of IP networks, qualified personnel and operations. c) The ‘power of many’ that allows a service provider to leverage knowledge of attacks accruing from their large network across many individual customers, protecting them proactively. d) The ability to offer a range of security and network services. e) Benefits arising from thwarting attacks at the edge of the service-provider network with no impact to WAN connectivity for the customer.

## Solution

After evaluating the RFP responses, the carrier rigorously tested equipment from multiple vendors and selected iPolicy’s Intrusion Prevention Firewall (IPF) advanced integrated network security appliances. The carrier selected iPolicy Networks based on its robust platform, depth and breadth of security services, and security granularity as well as the scalable iPolicy Security Manager (ISM) security management platform. The carrier has installed more than a dozen iPolicy IPF systems, and serves hundreds of medium- to large-sized enterprise customers worldwide with iPolicy-based managed security services.



The iPolicy IPF appliances are installed in multiple data centers and network points of presence (POPs). Today, the carrier's managed security services include managed stateful firewall, IDS/IPS and URL filtering. Examples of some of the large, multi-location customers that are being served by the carrier using the iPolicy solution include a large IT infrastructure consulting company with about 100 locations worldwide; a 5,000 employee manufacturing company with 30 factories; and a large online travel services company.

The iPolicy ISM has enabled the carrier to manage a lights-out security system installation with a reasonably small team of experts due in large part to two capabilities unique to the ISM: a) The ISM enables security service management, as opposed to device management, and b) the ISM provides co-management capabilities from multiple administration points into a single centralized system. The iPolicy Intrusion Prevention Firewalls are installed in the POPS, while the ISM is installed in the Security Operations Center (SOC) in major cities. For 24x7 non-disruptive reliability, each iPolicy IPF installation is configured in a fully redundant active-active configuration and the ISM is also deployed in a redundant mode.

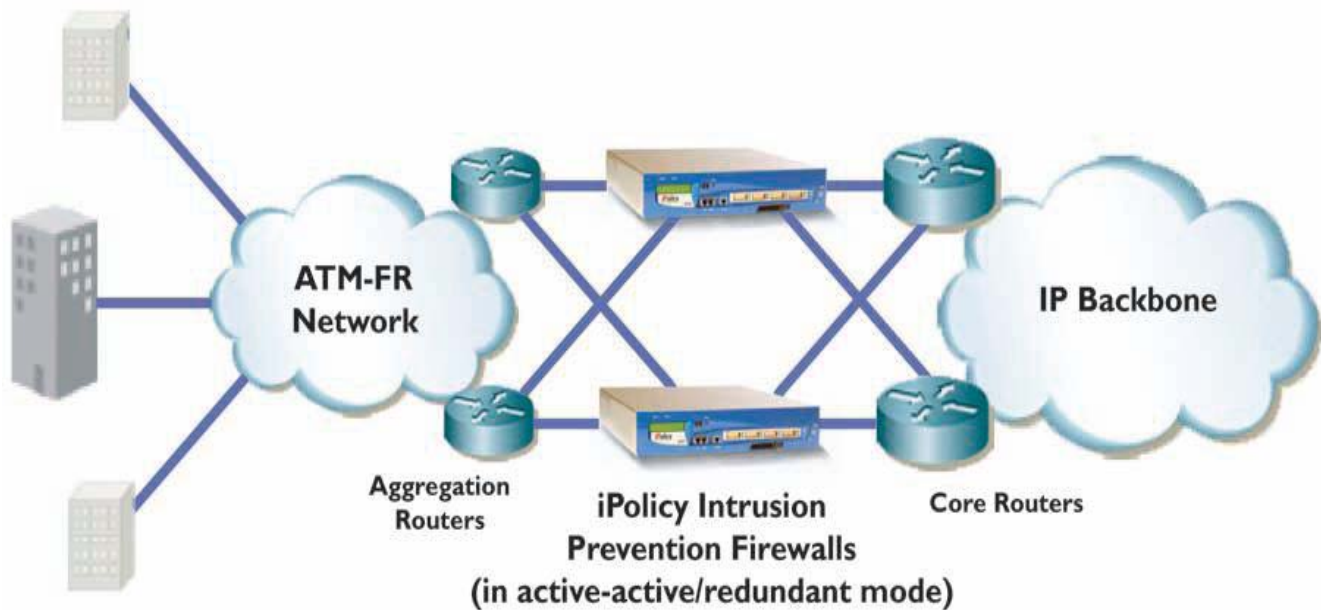
## Results

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.

The iPolicy Security Manager is the most scalable and feature-rich security management system in the industry. The ISM 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 scalability through the ability to allow individual components of the ISM to be distributed across several machines.

**Figure 1** - Network diagram showing deployment of iPolicy's Intrusion Prevention Firewalls



## Summary

Given its compelling managed security service offering, the carrier is able to charge 3 to 6 times the revenue per month for a leased line. Through this deployment, the carrier achieved a positive return on investment within a year, even when the iPolicy IPF appliances were merely 10% loaded.