



White Paper

IP Next-Generation Network Security for Service Providers

In the Cisco® IP Next-Generation Network (NGN) architecture, security features can be integrated and activated in the network fabric at all levels. Security is pervasive in technologies, policies, monitoring, and enforcement features from service provider networks to end-user devices. These evolving security solutions will enable service providers to enhance their current offerings, provide new offerings for new revenue generation, and give customers the protection and confidence they require in an environment of multifaceted and blended security threats, where multiple attack techniques are combined and used together. Security is embedded into the foundation of the Cisco IP NGN architecture and designed to mitigate the broad range of network threats that exist today and that will challenge networks tomorrow.

This paper highlights some of the most prevalent security threats to service delivery and business continuity while detailing how Cisco IP NGN security protects against these threats. The Cisco IP NGN security architecture includes an operational process model for end-to-end security assessment, design, and implementation. This model also helps to establish the economic and operational value of security services, and can be used to promote the introduction of managed security services through technologies that embed security capabilities in the fabric of the network and solutions built at the systems level for integrated, collaborative, and adaptive security.

Summary

The primary challenge faced by today's service providers is maintaining service predictability in the presence of an outbreak of malicious traffic sourced from multiple endpoints spread across multiple network boundaries. In today's terms, this type of behavior has been identified with threats such as distributed-denial-of-service (DDoS) attacks, turbo worms, e-mail spam, phishing, and viruses. The amount of traffic generated by infections and subsequent outbreaks can disrupt the normal operation of a network and adds risk to the supporting devices that are responsible for even basic routing and switching of packets.

Security has become a critical characteristic of all services and is essential to the profit line of service providers. Today, to maintain heightened network security, operations departments must transition from the traditional reactive stance to an incrementally proactive stance by reducing windows of vulnerability, improving reaction times, and effectively mitigating attacks. However, security professionals and meshed correlative security systems that provide comprehensive views of entire networks are in short supply.

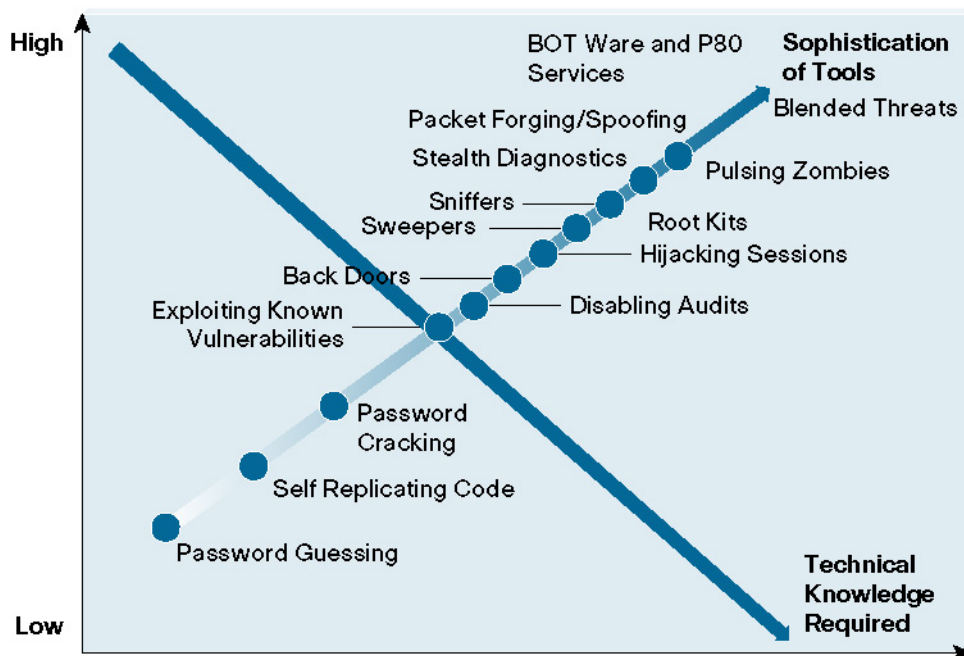
The time to begin improving security operations is now. More advanced security capabilities and solutions will evolve as the service provider undergoes the IP transformation. Effective network security is a multifaceted challenge that Cisco Systems® is helping to define and implement in methodologies, standards, technologies, products, and solutions within the IP NGN architecture.

Challenge

Malicious traffic is becoming more prevalent because of readily available and ever more sophisticated attack tools, and motivations are becoming increasingly varied and malicious. We have witnessed a transformation in the miscreant economy – the community that engages in cyber crime-related activities for financial reward. This transformation and its financial ramifications now require that service providers offer more defined value propositions for protecting networks and services. Service providers must enhance the value perceptions of the general marketplace toward managed security-enabled services and present significant, increasing service and value guarantees to their customers.

In the early years of cyber crime, knowledgeable system administrators often developed and published vulnerability detection and validation tools. These tools were used by systems administrators seeking fixes for specific vulnerabilities and by hackers who adapted the tools for use in attacks. However, these tools were generally regarded as a positive contribution to the security protection effort. In more recent history, however, many more cyber criminals have been able to freely obtain copies of these tools and have developed methods to join their capabilities with automated attack routines. Methods have matured in the past few years to include intelligence-gathering routines to create truly complex blended threats that propagate in a highly redundant and automated manner. This evolution is depicted in Figure 1. Today, the hacker's job is getting easier and the job of protecting the network is becoming more complicated.

Figure 1
Network Attacks Growing in Sophistication and Ease of Deployment



While attacks were once primarily the work of hackers who wanted to temporarily take well-known sites offline to get media attention, they are increasingly being used as the foundation of elaborate extortion schemes or are motivated by political or economic objectives, costing businesses and service providers millions of dollars each year.

Evolution of Service Provider Security

Today, customers are asking their service providers to implement security measures to combat malicious traffic and worms. Customers need end-to-end and automatic protection. Solutions that require large quantities of dedicated customer premises equipment (CPE) to be deployed and network topologies to be massively reworked are not feasible because of increased costs, increased operational constraints, increased use of encryption to hide attacks, added complexity and risks, and scalability issues. Customers want their service providers to be accountable for endpoint behavior, where the service provider currently does not have enough visibility, control, or the appropriate infrastructure to support endpoint software distribution, maintenance, and troubleshooting.

Security is no longer just about a single appliance or a dedicated service. Security is at the heart of the network's future. We have moved from an Internet of implicit trust to an Internet of pervasive distrust, where security policies are the arbiter and no packet, service, or device can be

Cisco Systems, Inc.

trusted until it is inspected. Hence, security can no longer be a specialized practice or a dedicated function. It must be absorbed within the fabric of the service provider environment and operational support processes, and it must be viewed as a critical requirement to sustain:

- Service availability and reliability
- Business continuity
- Service-level agreements (SLAs)
- Customer trust and loyalty

Integration of security requires a fundamental operational process model and a secure infrastructure to provide the foundation for service delivery and business continuity. All the elements of the network fabric must have knowledge about what is relevant. The network fabric must itself become a pervasive, proactive policy monitoring and enforcement environment. This implies tight collaboration, in business and technology, between service providers and their business customers, and creates opportunities for service provider-managed security services.

Solution

End-to-End Security Architectures

Security at Cisco is regarded as a major pillar in the IP NGN architecture and as one of the most fundamental requirements for service delivery and business continuity. The end-to-end Cisco security methodology provides an effective guide to developing a security architecture by helping to create a plan for defining, maintaining, and implementing security programs throughout the network. The resulting architecture can then be applied to the service provider's security program through policies, procedures, and technologies. Cisco has devised modern IP threat definitions and provides a practical operational process model to create revenue-generating services for service providers. Cisco has defined these modern threats to include:

- **Reconnaissance threats** – Hackers scan network topologies to identify vulnerable devices (such as open ports, lack of password requirements, OS vulnerabilities) and attack them.
- **Distributed-denial-of-service (DDoS) and infrastructure attacks** – These are IP packet-based attacks launched at the network infrastructure to compromise network performance and reliability.
- **Break-ins and device takeover** – These usually follow a reconnaissance and are the unauthorized access to a given device with the intention to compromise device security.
- **Theft of service and fraud** – This threat category pertains to the unauthorized use of network resources.

Once the threats are identified, combating them requires the understanding of three basic principles, which include the following:

- **Prevention** is the act of preparing a known defensive posture to prevent known threats. Prevention includes patching vulnerable systems, implementing standard and hardened system images, and implementing firewalls or other access control technologies.
- **Monitoring** is the act of detecting potentially malicious and exploitative activities and differentiating between truly malicious activity and nuisance activity to understand the real-world threats that are encountered at key aggregation points. It involves deploying intrusion-monitoring technologies, conducting log analysis of servers and firewalls, and actively monitoring OS calls.
- **Response** is the ability to act on the information discerned to control the impact of a confirmed real-world threat in near real-time. Methods include dynamic access controlling, black-holing, shunning, resetting sessions, and interrupting invalid system calls.

It is important to understand that these principles traverse all layers of operation, applications, and the entire infrastructure.

To mitigate emerging threats when scaling to multigigabit rates of traffic, service provider requirements have now shifted from using standalone security appliances to integrating security into the network infrastructure. Integrated security provides:

- Protection without affecting overall network performance
- Operation with existing high-availability services
- The ability to identify, classify, and trace back anomalous behavior across the network
- The ability to increase the overall security posture of the network
- The ability to distribute countermeasures to multiple points of the network

Cisco helps service providers to apply a security program that encompasses the various aggregation points for all known threats and threat perspectives.

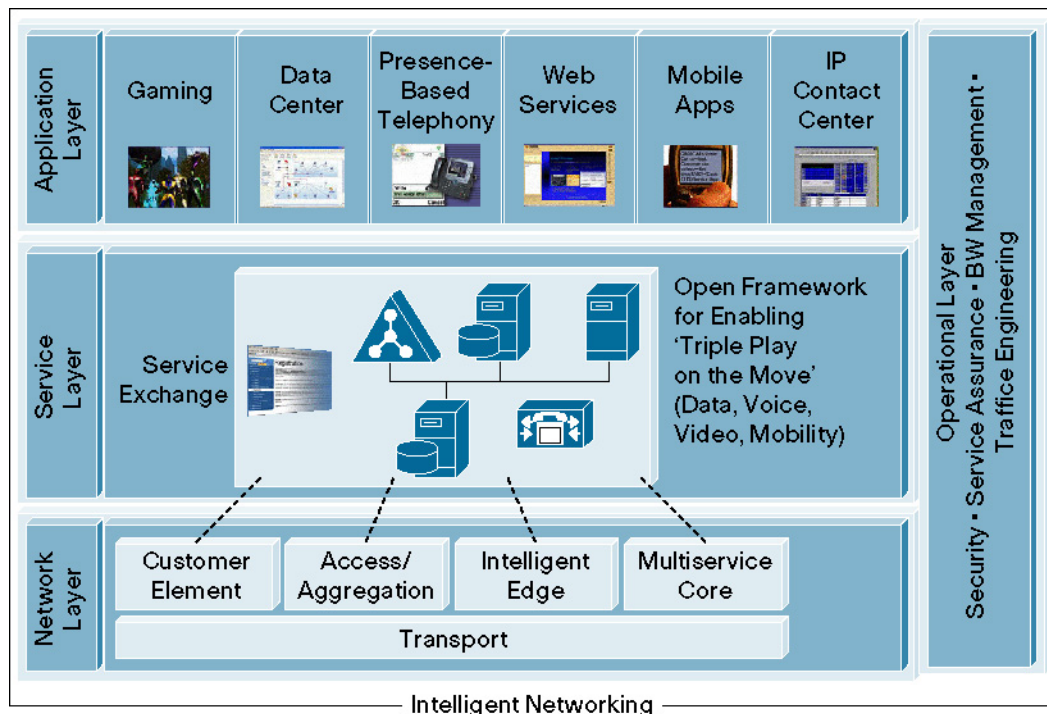
Cisco IP NGN Security


The Cisco IP NGN is a vision and an architecture designed to deliver a broad, sweeping transformation of the service provider network and business. It provides a sustainable competitive advantage and profits by helping service providers develop and plan for the future of their organizations, network architectures, and business models.

In the IP NGN architecture, security is fundamental to a service provider’s ability to protect the infrastructure, deliver services in a manner that complies with specific service levels, and control its business. Security is resident in all four layers of the IP NGN architecture (Figure 2). Cisco IP NGN security solutions help create an environment where service providers can extend more services for new revenue generation and differentiation, achieve greater efficiencies with highly available service and minimum downtime, and apply better control for network and business success.

Figure 2

Cisco IP NGN Architecture





In the operational layer, security spans the entire IP NGN architecture, protecting a service throughout the network to maintain service availability in the event of an attack. In the network layer, security is built into the foundation of the infrastructure and its hardware and operating systems to secure the transport of services. In the service layer – part of the Cisco Service Exchange Framework – security plays a role in creating services and service features to generate revenue and service differentiation. In the application layer, security is resident in the applications themselves and in the links to the service layer to secure the integrity of the applications as they interface with the network.

The intelligent operational layer operates through and helps connect the three IP NGN convergence layers – network, service, and application – and makes intranetwork and internetwork communications as efficient and productive as possible. Intelligent networking simplifies the operation of an IP NGN by making it more resilient, integrated, and adaptive. Together, the three convergence layers, the cohesive operational layer, and intelligent networking allow Cisco to build integrated features that are consistent across product lines and that enable products to function as a global system – an IP Next-Generation Network. Security is fundamental to the IP NGN, implemented through a combination of *processes, technologies, and solutions*.

Cisco Operational Process Model for Service Provider Security

The Cisco Operational Process Model for Service Provider Security addresses how a service provider can effectively deliver more services with better efficiencies and greater control. It has relevance to both business and technology groups throughout a service provider's organization, putting the focus both on maintaining service availability and reliability and on enabling new revenue opportunities.

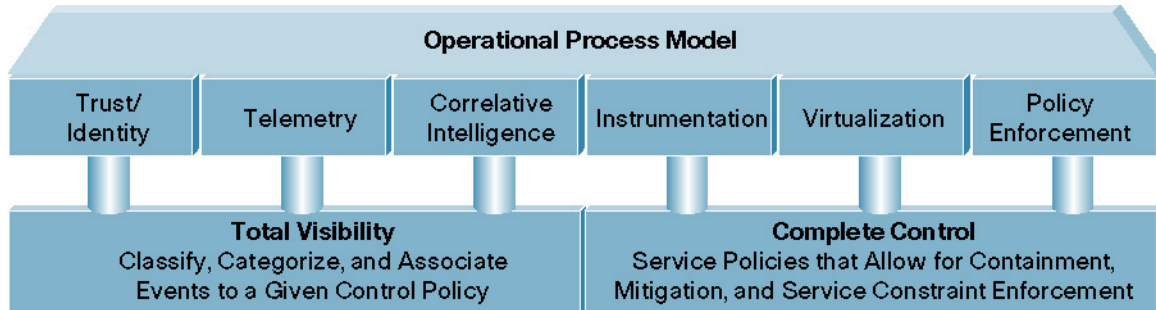
Critical elements of this model are available today to combat service disruption and mitigate exploits targeted at the service provider infrastructure. Executing and scaling the process model requires comprehensive integration of multiple security systems into the service provider network's fabric. Cisco is committed to pioneering the integration and adoption of the entire model, not simply as it pertains to a security facet, device, or subsystem built to combat a single type of problem.

The Cisco Operational Process Model for Service Provider Security is designed specifically for service providers. This proactive threat-mitigation approach goes beyond a single box or technology, anticipates the shortage of operational security expertise, and helps minimize threats that cannot be completely controlled while controlling those that can. This approach is also aimed at decreasing the operational expenses of both the service provider and the enterprise customer.

This operational strategy relies on telemetry to gain total visibility and complete control of network and systems elements to maintain services and business continuity in an environment of continual security exposures. The model is used to implement security networkwide without reliance on a single technology. Multiple technologies and features are used throughout the network to obtain visibility into network behavior and to exert control over questionable network behavior.

The model is used to implement visibility and control across an IP infrastructure (Figure 3). The IP NGN design works within a sustainable operational model, supporting both network and security operations. All pillars of this model work together as a whole, providing a secure system of defense.

Figure 3
Cisco Operational Process Model for Service Provider Security



Security in the IP NGN includes total visibility and complete control, based upon:

- **Identity and trust** – Identification of devices accessing the network and inspection of credentials required to identify the state of trust
- **Telemetry** – Monitoring the effectiveness of security policies
- **Correlative intelligence** – Interpreting and transforming large data flows into meaningful operational information, which involves the contextualization of seemingly unrelated changes in posture, methods for determining violations of policies, or any combination of changes to posture that could affect guaranteed service delivery
- **Instrumentation** – Presenting the intelligence derived from audit logs, event monitoring, fault knowledge, and health and status information, and graphically displaying that understanding in near real time
- **Virtualization** – Defining and interpreting policies for a logical device to a required posture
- **Policy enforcement** – Enforcing policies in response to an observation and how the policy defines the action required when that observation is contextualized

Primary benefits of the Cisco Operational Process Model for Service Provider Security include the integration of telemetry information, intelligent and collaborative management systems, cost efficiencies through virtualization, and a proactive and adaptive orientation for readiness against threats. It is a holistic approach that accelerates service deployment and is built to scale.

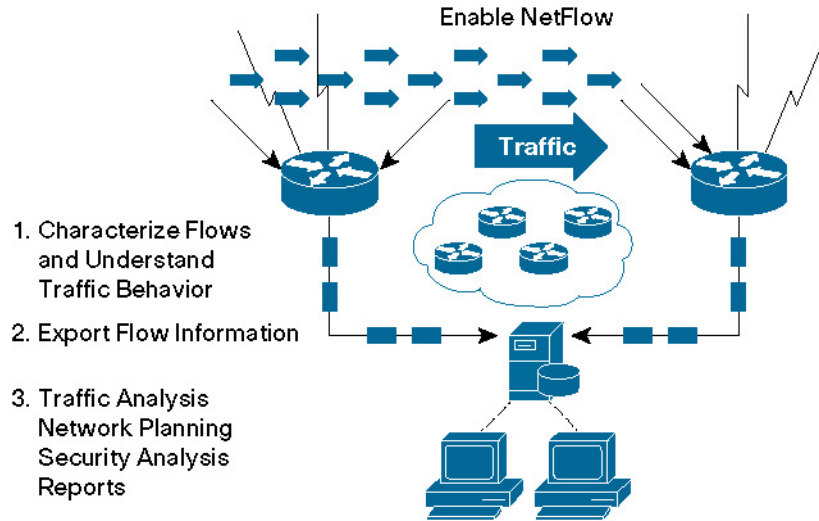
Security Technologies Integrated in Products

Cisco routers and switches feature embedded security capabilities to protect and harden the service provider network in its fabric. These features – Cisco NetFlow and Cisco Network Foundation Protection – work together to mitigate most baseline threats and attacks, providing foundational security.

Cisco NetFlow

Cisco NetFlow technology in Cisco IOS® Software efficiently delivers a set of services for IP applications, including network traffic accounting, usage-based network billing, network planning, security, DoS monitoring capabilities, and general network and traffic monitoring (Figure 4). NetFlow provides valuable telemetry information about network users and applications, peak usage times, and traffic routing. Cisco invented NetFlow and is the leader in IP traffic-flow technology, establishing NetFlow as a standard for acquiring IP network and operational data.

Figure 4
Cisco NetFlow Operation



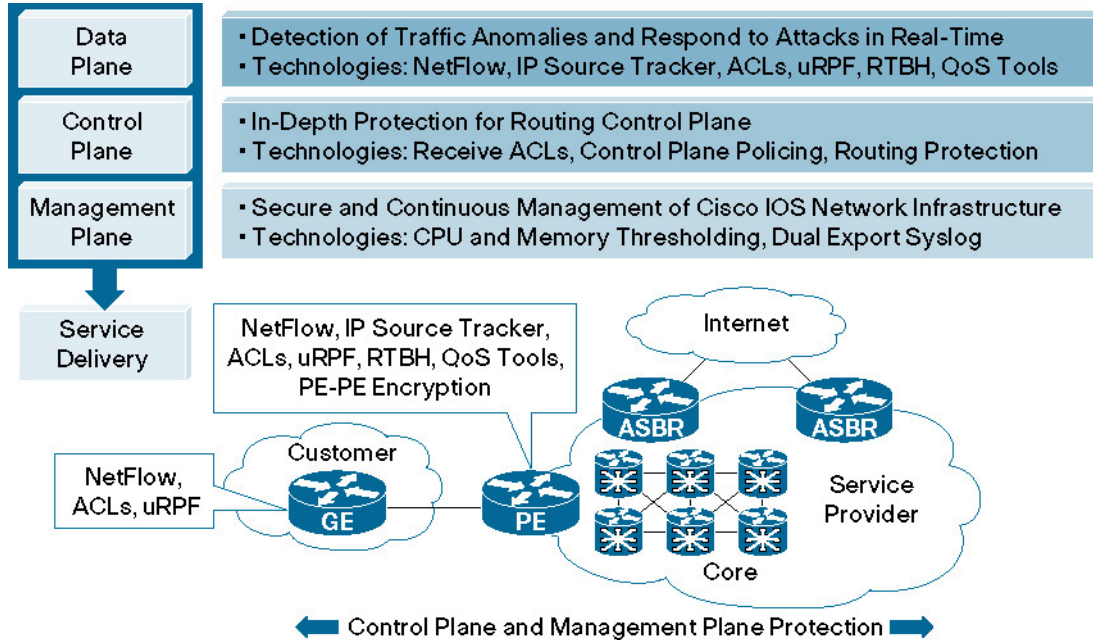
Cisco NetFlow helps network administrators to detect and classify security incidents, to understand the impact of network changes and services, and to improve network usage and application performance. With Cisco NetFlow, service providers can also reduce IP service and application costs and better optimize network costs.

Cisco Network Foundation Protection

Cisco Network Foundation Protection (NFP) in Cisco IOS Software protects network devices, routing and forwarding of control information, and the management of traffic bounded to the network devices (Figure 5). Cisco NFP is built into the very fabric of Cisco routers and switches.

Figure 5

Cisco Network Foundation Protection



Legend:

- Access Control List (ACL)
- Remote Triggered Black Holing (RTBH)
- unicast Reverse Path Forwarding (uRPF)
- Provider Edge (PE)

Cisco NFP hardens the data, control, and management planes of the network infrastructure against a wide variety of security threats. It helps protect network devices not only from DDoS attacks but also from threat vectors like reconnaissance, network device break-ins, and theft of service. It helps minimize the vulnerability of critical services such as Domain Name System (DNS), e-mail, Web access, and voice over IP (VoIP). Making use of network telemetry such as NetFlow, NFP studies traffic patterns in real time, creates traffic baselines, detects anomalies and misuse, and characterizes affected interfaces. Anomalies can be compared across the network to provide traceback and determine an attack’s point of ingress. Complementing the Cisco DDoS protection solution, NFP also mitigates primitive DDoS attacks, freeing the capacity of the Cisco Guard – an essential element in the Cisco DDoS Protection solution – to fight more sophisticated attacks in a scalable manner.


Solutions for Systems-Based Security

The Cisco security portfolio includes system-built security solutions that have been successfully deployed by major service providers and have generated new revenue for them. The following system-built solutions give service providers ample opportunities to create managed security services to offer their customers.

DDoS and “Inbound” Traffic Protection

Cisco DDoS protection delivers “clean pipes” capabilities to service providers. The solution uses NetFlow and NFP capabilities in Cisco IOS Software, which embed comprehensive security features in Cisco switches and routers to lock down services and routing protocols, secure

Cisco Systems, Inc.



access for management and instrumentation, and protect data forwarding through the devices. Additionally, the solution uses Cisco DDoS protection and third-party products to perform detection, mitigation, and traffic diversion and injection functions to protect networks from increasingly complex DDoS attacks. Cisco DDoS protection helps enable service providers to sell connectivity and last-mile bandwidth services to customers while hardening their own network infrastructure.

Service Control and Outbound Traffic Protection

The Cisco service control suite protects outbound traffic coming from service provider customers and provides the capability to quarantine specific users. Network quarantine is a technique used to identify and contain the spread of potential threats within a service provider domain by segregating all traffic from infected hosts to an isolated network that is specially designed to empower the end user to recognize and resolve threats themselves. Network quarantine is not intended as a security measure to keep out attackers. It is intended as a fail-safe measure to ensure that legitimate users are in compliance with the service provider's policies and are not a threat to other users or network resources. The goal of service control is to greatly reduce customer support and help desk costs by enabling customers to mitigate attacks themselves. This can be achieved through software upgrades or the use of dedicated software to remove viruses, worms, or other malicious code from a host.

Network-Based Virtual Private Network

Cisco network-based IP VPN solutions allow service providers to offer a secure, ubiquitous, and fully integrated IP VPN service to enterprises and small and medium-sized businesses (SMBs). It is a cost-effective and scalable VPN solution that takes full advantage of a service provider's existing Multiprotocol Label Switching (MPLS) network to introduce new revenue-generating service options, such as class-of-service (CoS) priorities for individual applications and users and SLAs. New VPN customers can be added without installing additional interfaces or reconfiguring the customer's edge routers. A major revenue opportunity for service providers is to provide managed access to and from such VPNs. For example, managed remote access to VPNs from Internet-attached clients using IPSec or Secure Socket Layer (SSL) or managed secure Internet access provide firewalled access to the Internet from a VPN.

Managed Customer Premise Equipment and Customer Edge Security

The Cisco Managed Customer Premise Equipment/Customer Equipment (CPE/CE) Security bundle is a collection of market and service management best practices organized by marketable solution. It helps service providers to design, develop, and deliver remote management services using Cisco technologies on service providers' customer premises. These best practices provide guidance in designing the support infrastructure and planning for a functional go-to-market strategy for managed CPE using Cisco technologies. The remote management facets that are addressed in these best practices include: system management, incident detection, isolation, and resolution techniques; configuration and change-management methodologies; and security-event reporting, analysis, and mitigation concepts. All remote management techniques and concepts are designed to optimize the end customer's service availability, reliability, and fault tolerance when faced with technological failure or security attack scenarios.

Border Control

Next-generation service provider peering architectures stress new levels of security in the seamless delivery of voice, video, and multimedia services. Border Control is designed to provide security, service assurance, and meet regulatory demands – such as legal intercept requirements like the Communications Assistance for Law Enforcement Act (CALEA) – across IP network borders. Border Control features offer a layered peering model segmenting device functions to control and derive new revenue from the interconnect between service providers. These features include interprovider QoS, security on the border between providers, and the enforcement of interprovider SLAs.

Conclusion

Integrated, collaborative, and adaptive security in the evolving Cisco IP NGN architecture is built into the fabric of the service provider's network infrastructure and integrated with other network elements. Integration means that every element in the network incorporates security technologies and acts as a point of defense. Collaborative security means that network components work together to provide new types of protection. It involves cooperation between endpoints, network elements, and policy enforcement. Adaptive features encompass behavioral methods that recognize new types of threats as they arise. This broadens threat-recognition capabilities and addresses threats at multiple layers of the network.

Cisco Systems not only provides a comprehensive security product portfolio, it also assists service providers in developing revenue-generating managed security services from concept to implementation and marketing. Security is not perceived as an afterthought at Cisco, but as a fundamental part of the service provider's business that impacts all services. Cisco has developed a modular approach to the creation of managed security services for the enterprise and SMB. This approach allows service providers to build customized service bundles quickly and easily to meet the needs of different types of customers and vertical market requirements. The richness of features and the modularity of Cisco platforms allow for truly comprehensive managed security services that can generate significant revenues for service providers and deliver valuable protection to end customers.

The IP NGN involves creation of an intelligent infrastructure from which application-aware services are securely delivered by service-aware networks. This intelligence directly benefits efforts to proactively secure networks against existing and ever-changing threats while offering service providers a major competitive advantage.

For More Information

Cisco Network Foundation Protection: <http://www.cisco.com/go/nfp>

Cisco NetFlow: <http://www.cisco.com/go/netflow>

Cisco Network-Based VPN: http://www.cisco.com/en/US/netsol/ns587/networking_solutions_sub_solution.html

Cisco Distributed-Denial-of-Service Protection Solution: <http://www.cisco.com/go/cleanpipes>

**Corporate Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica
Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR
Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico
The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia
Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R) KL/LW10135 01/06