Data Center Security That Accelerates Your Business

Business today runs at a breakneck pace. Customers want exceptional service, and workers expect instant access to their job tools, from any location. IT managers have turned to virtualization and automation to deploy applications and services efficiently to meet changing business requirements. New applications can be enabled more quickly than ever before, and data center provisioning times have dropped from months to minutes.

Even so, this speed is being throttled by users' insatiable appetite for network bandwidth and by unprecedented security threats. Consider this:

- By the end of 2013, the number of mobile-connected devices will exceed the number of people on the planet.[1]
- Application traffic and network connections are predicted to increase 3000 percent by 2015.
- More than 100,000 new security threats are identified every day.

IT managers struggle to balance the delivery of anytime, anywhere access to applications, websites, and devices with the imperatives to protect the business from attacks and to maintain regulatory compliance.

Conventional Approaches to Data Center Security Are Failing

In many of today's data centers, applications, servers, storage, and networks are secured in "silos" for different business units and departments. Physical and virtual infrastructures are secured separately. The technology, people, and processes needed to secure data center services operate in isolation.

This sort of piecemeal, "bolted on" security increases cost and complexity, but cannot secure data that is in constant motion across devices and networks. Nor can it scale to meet the massive performance demands of the cloud.

[1] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012-2017.

To realize the full benefits of data center and cloud innovation, IT managers need to be able to deploy new services rapidly and securely. Security must be automated, highly adaptive, and instantly responsive. Security policies must be applied in the context of usage, and must follow the user, application, device, and virtual workload, no matter where or how they move.

To enable data center innovation, IT organizations must adopt three measures:

1. Speed deployment of new, secure services from weeks to hours to meet rapidly evolving business requirements.
2. Maximize network performance to scale to today's increasing workloads and application traffic.
3. Establish pervasive protection that creates a secure chain of trust from the user to the application.

Built-In Security That Scales with Your Data Center Needs

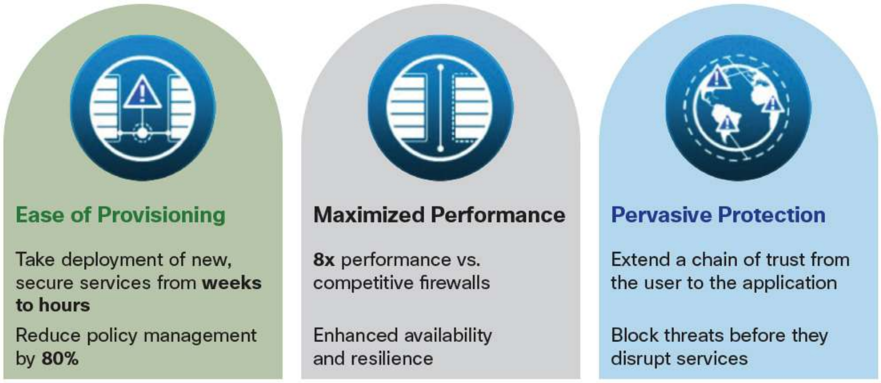
Cisco builds security into every aspect of the network and compute infrastructure, enabling you to apply security policies within the business context. As a result, you can speed the delivery of secure, on-demand elastic services from your data centers, private cloud, or hybrid cloud.

With Cisco® data center security solutions, you can:

- Accelerate the provisioning of secure applications and services
- Maximize network performance
- Rely on pervasive protection that protects against evolving threats

Cisco® ASA 5500-X Series Next-Generation Firewalls are the foundation of protection for enterprises and cloud providers around the world. The Cisco ASA 5585-X Next-Generation Firewall and ASA 1000V Cloud Firewall work in concert with the Cisco Nexus® 7000 Series Switch to simplify data center provisioning, maximize network performance and scale. Cisco Security Intelligence Operations (SIO) and Cisco Intrusion Protection provide superior protection with lower operating expenses (Figure 1). And, Cisco TrustSec® automates security policy and enables rapid provisioning of new services. The Cisco Virtual Services Gateway delivers strong Intra-tenant security and is ideal for multi-tenant clouds.

Figure 1. Cisco Data Center Security Accelerates Your Business



Ease of Provisioning

Take deployment of new, secure services from **weeks to hours**

Reduce policy management by **80%**

Maximized Performance

8x performance vs. competitive firewalls

Enhanced availability and resilience

Pervasive Protection

Extend a chain of trust from the user to the application

Block threats before they disrupt services

Ease of Provisioning

Cut deployment time for new services from weeks to hours. Provisioning new virtual workloads eliminates the time-consuming, error-prone manual configuration of data center firewall policies.

Case Study

Consider a global bank where 24 people were responsible for managing more than a half million firewall rules. When the bank moved to Cisco ASA Next-Generation Firewalls, it needed only 50 server rules, 10 firewall rules, and 6 people to manage data center security. It gained comprehensive threat protection at a lower cost.

With Cisco ASA Next-Generation Firewalls, provisioning is automated across both physical and virtual infrastructures. When a new workload is provisioned, the firewalls automatically apply the appropriate security policies. Real-time policy provisioning is enabled via Security Group Tags (SGTs), which automate security policies across routers, switches, firewalls, and intrusion prevention systems. Security rules are applied in the context of the users and devices, so IT managers can, for example, enforce different access policies for finance employees using iPads in Europe than for finance employees in China.

Data center security is integrated across physical and virtual domains with Cisco Virtual Network Management Center (VNMC). VNMC provides policy management for Cisco network virtual services, so IT can automate the process of generating a tenant and its applications, including governing which applications and services may communicate with each other across a virtual infrastructure.

Maximized Performance

With Cisco, strong security does not come at the price of network performance. Compared to competitors' firewalls, Cisco ASA Next-Generation Firewalls deliver:

- Eight times the performance
- Eighty-four percent less power consumption
- Eighty-seven percent less rack space

Cisco ASA firewalls can support up to 1.9 million new connections per second and a total of 80 million connections per second.

In addition, Cisco Unified Fabric technologies, including Virtual Port Channel (vPC) and FabricPath, enhance network resiliency and deliver the massive scale needed for the cloud. Using vPC on Cisco Nexus 7000 Series switches maximizes data center network performance. vPC extends link aggregation across two physical switches to use all of the available uplink bandwidth and to support Layer 2 multipathing to increase network availability.

Cisco FabricPath is the foundation for a massively scalable data center fabric. FabricPath provides optimal bandwidth between any two switch ports, regardless of their physical locations. Any application can be deployed to any server, so businesses gain the flexibility they need to support virtual workload mobility across data centers and the cloud.

Pervasive Protection

IT managers no longer have to take security risks to gain the benefits of virtual workloads. With Cisco, IT managers gain full visibility into network activity in a virtualized data center so they can enforce acceptable use policies. Policies can be applied in context and differentiated by users, devices, and applications. IT managers have visibility into who is connecting to the network and can tightly control what they can do and where they can go based on identity and usage context.

You can proactively block advanced threats before they disrupt services - and your business. Cisco Security Intelligence Operations (SIO) gives you early warning intelligence, threat, and vulnerability solutions by correlating and analyzing 75 terabytes of threat data and more than 5500 IPS signatures each day. With SIO's reputation-based protection, your business is protected long before a threat can take hold.

A Broad Portfolio of Data Center Security Solutions

Your business needs security without compromise. Cisco's next-generation data center security solutions eliminate the tradeoff between security and agility for data centers, private clouds, and hybrid clouds. Businesses can accelerate the pace of business when innovative security is built into their data center infrastructure.

Cisco offers a broad portfolio of solutions, whether your focus is on consolidating and virtualizing data centers or automating service delivery for the cloud. Wherever you are on the road to virtualization and the cloud, when you deploy Nexus 7000 Series switches and ASA Next-Generation Firewalls together, you can harness the full power of Cisco's data center security innovation, reduce data center costs, and gracefully scale your infrastructure as your business needs grow and change.

By the Numbers

- Global data center traffic is expected to quadruple over the next five years.[2]
- By 2016, global cloud traffic will make up nearly two-thirds of total data center traffic.[3]
- Forty percent of millennial workers say that company policy forbids using company-owned devices for personal activities, yet 75 percent say they don't obey the policies.[4]
- Thirty-two percent of IT professionals believe big data complicates security requirements and protection of data and networks.[5]
- In 2012, data center security threats increased nearly 20 percent over 2011.[6]

Summary

Cisco builds security into next-generation data centers to accelerate the provisioning of secure services. Through shared protocols, Cisco uniquely automates security policies for new levels of operational efficiency, reducing manual rule sets by 80 percent. Next-generation datacenters benefit from 8x performance gains versus competitor solutions and maximized scalability and availability through innovations such as FabricPath and Virtual Port Channel.

With Cisco TrustSec®, security extends from the user to the application. Threats are blocked before they can disrupt data center services through actionable security intelligence and next-generation intrusion prevention. IT can accelerate secure, elastic, on-demand services and can connect policies across physical, virtual, and cloud locations using validated designs that further ensure proven and scalable deployments.

To learn more about the Cisco Secure Data Center Solution, visit http://www.cisco.com/go/securedatacenter.

[2] 2013 Cisco Annual Security Report.

[3] 2013 Cisco Annual Security Report.

[4] 2012 Cisco Connected World Technology Report.

[5] 2012 Cisco Connected World Technology Report.

[6] 2013 Cisco Annual Security Report.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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