White Paper

Cisco Cloud Security Accelerates Cloud Adoption

Introduction

Cloud computing is gaining customer attention at a fascinating pace. An Infonetics research report published in early 2011 noted a significant increase in customers' interest in cloud computing between 2009 and 2010—most of respondents indicated interest in 2010, up from only 10% in 2009. Many studies have concluded that software as a service (SaaS) and infrastructure as a service (IaaS) are leading the way in adopting cloud computing. Meanwhile according to an April 2011 Forrester report, the third largest cloud category, platform as a service (PaaS) is predicted to surpass IaaS to become the second largest cloud category by 2014.

According to Forrester, security is one of the top barriers to cloud computing. While cloud computing increases business agility, scalability, and efficiency, it also introduces new security risks and concerns. The challenges are complex because they involve not only technology issues but also substantial process changes due to the new business computing models. Following are some common security concerns for cloud computing.

- **Increased attack surface.** New technologies introduce new vulnerabilities. Virtualization, for instance, is a foundational technology for cloud computing. The virtual access layer adds a new dimension for threat vectors. Offline virtual machines (VMs) can carry unnoticed vulnerabilities if brought back online without a rigorous patching process. Administrative and application access by cloud subscribers across the Internet raises the risk level due to the exposed public interfaces.
- **Ownership and responsibilities.** Cloud service providers are expected to deliver a high level of security assurance, but the line can be blurred between providers and subscribers. For example, IaaS subscribers may need to be largely responsible for deploying cloud security resources for their cloud operations. PaaS and SaaS subscribers, on the other hand, may not need to manage security infrastructure components themselves, but they still need to collaborate closely with their cloud service provider on security, especially in areas such as identity and access management.
- **Shared environments (multi-tenancy).** Traditional security demands physical separation when highly sensitive data is involved. In cloud environments, however, subscribers typically share infrastructure, applications, and other resources. Threats to the network and computing resources can be amplified when sharing with unknown outside co-subscribers who might have poor security practices or even malicious intent.

Cisco cloud security offerings help customers take a strategic and architectural approach to cloud adoption. Cisco cloud security solutions dovetail with Cisco data center and Borderless Networks services to deliver high performance and operational simplicity. Cisco cloud security solutions comprise three key areas:

1. In-depth capabilities to help public cloud service providers, subscribers, and private/hybrid cloud practioners secure their cloud infrastructure.
2. Cloud-based email, web, and threat intelligence security for customers.
3. Secure cloud access capabilities to help organizations better control access to SaaS applications and to enable a trusted cloud environment.

Governance

Cloud computing represents a dramatic shift to new technologies and new business computing models. Providers and subscribers need to ensure that their organizational governance is up to date to support these changes. Specifically, they need to update their related policies, procedures, and standards. Subscribers need to review information offered by their cloud provider to ensure that they help achieve compliance, trust, and privacy. They should demand transparency so that they can gain insight on how providers manage application development, infrastructure design, security architecture, and implementation, as well as monitoring, auditing, and security incident response processes. Subscribers should also insist on a strong service-level agreement (SLA) that specifies requirements for data confidentiality, integrity, and availability. In addition, they should also discuss their rights to audit. Security is not a responsibility for cloud providers only. If a subscriber does not have sound governance and a strong security posture to start with, moving to the cloud will not solve their security challenges.

Governance considerations can also heavily influence cloud deployment decisions. Compliance requirements play a major role as customers select their cloud deployment models, namely public, private, or hybrid. Industries with substantial compliance regulations, such as financial services, healthcare, and government, have not adopted public clouds, but some of them have pushed forward with private cloud deployments.

From a technology perspective, cloud governance necessitates an increase in visibility and auditing capabilities. In-depth knowledge and contextual information about users and their activities help with not only better policy decisions but also compliance efforts.

Architecture

The cloud computing architecture generally includes the underlying infrastructure, various service components, and certain pervasive functions such as security and resiliency. Furthermore, cloud security has its own architectural structure. We discuss some key considerations below.

Logical separation. A key cloud computing benefit is its “elastic” computing capabilities, meaning that computing power can be ramped up or dialed down rapidly based on demand. To support such a dynamic business computing model, security should be provisioned in a similar manner. Static and physically oriented security configurations such as VLAN-based security are labor-intensive and can hardly keep up with the fast pace. New approaches are needed to achieve logical separation to secure dynamic and shared environments such as multi-tenancy.

Policy consistency. An overarching and consistent policy framework is critical for successful cloud security implementation. For example, an excellent design to achieve reliable and dynamic logical separation is to apply zone-based and policy-driven security enforcement. A zone is a group of attributes that may include traditional networking parameters such as IP addresses, network protocols, and port numbers. The zone may also contain information such as virtual machine (VM) and custom attributes. Approaches such as this help ensure policy consistency in a dynamic cloud environment where VMs typically move around.

Automation. A core tenet of the cloud computing business model is pay-per-use, meaning that elasticity is not only reflected in the infrastructure and computing power, but also in the cost structure. Costs for IaaS subscribers, for instance, are associated with their consumption rate, which may go up or down depending on demand. From a security perspective, automation presents two challenges: 1) how to secure an automated environment and 2) how security service provisioning can be automated. As an example, a centralized security policy framework with automated push mechanisms can greatly improve business efficiencies by mapping a security policy to a technical implementation.

Scalability and performance. Closely tied to automation, scalability and performance are requirements for cloud security because of the potentially massive workloads and stringent security requirements involved. Innovative technologies that can help boost performance while maintaining a high security standard are critical to cloud security implementation.

Authentication and access control. As previously discussed, cloud security is a shared responsibility between cloud service providers and subscribers. Access control to the cloud is one of the key cloud security areas and is a good example to demonstrate the shared responsibility concept. PaaS and SaaS providers, for instance, can provide authentication for cloud application developers and users. On the other hand, opportunities exist for cloud subscribers to take ownership of authentication and access control to cloud for tighter integration with their identity and access management systems. For IaaS subscribers, client-side access control is an integral component of their cloud security strategy.

Cisco Cloud Security Solutions

Cisco cloud security begins with governance considerations. The Cisco Privacy and Security Compliance Journey website provides detailed discussions about Cisco's vision for cloud computing. It contains information about how Cisco helps customers realize their business objectives by balancing the benefits and risks as they embark on their cloud journey. The information offers insight and clarity on how Cisco conducts business for more transparency, which is the cornerstone of a robust compliance program. Helping customers fulfill compliance requirements and providing trusted cloud products and services are top priorities for Cisco.

Cisco® SecureX. Cisco SecureX is an integral part of several key Cisco architectures, including Cisco Borderless Networks, Data Center/Cloud, and Collaboration Architectures. Cisco SecureX is a context-aware security framework that meets customer needs as they embrace a mobile, dynamic, and cloud-based working environment. The framework is a solid foundation composed of technologies that ensure a trusted network infrastructure. Cisco SecureX is led by context aware policy that allows customers to easily define and manage business relevant security policies. It provides further security enforcement elements in the form of appliances, modules, and cloud services.

Cisco cloud security consists of three key solution components that are direct implementation of Cisco SecureX:

- Secure Cloud Infrastructure
- Cloud Security Services
- Secure Cloud Access

Secure Cloud Infrastructure. Cisco provides a powerful cloud security solution to help secure private, public or hybrid clouds. The Cisco product portfolio includes the following components:

- Cisco ASA 5585-X Appliance and Cisco Catalyst® 6500 Series ASA Services Module
- Cisco Nexus® 1000V Series Switches
- Cisco Virtual Security Gateway (VSG)
- Cisco IPS 4200 Series Sensors

The Cisco ASA 5585-X appliance is uniquely positioned to provide high-performance security to protect the new virtualized data center and extended cloud with firewall and intrusion prevention (IPS) capabilities. The ASA 5585-X deployment at the cloud data center distribution layer provides strong protection for high-valued cloud resources and services. The ASA 5585-X supports advanced virtual data center technologies, such as Cisco virtual PortChannel (vPC), Cisco Catalyst 6500 Virtual Switching System (VSS), and Cisco Nexus 7000 Series virtual

device contexts (VDCs). These technologies enable high scalability and performance for cloud environments. Furthermore, the ASA 5585-X supports multiple security contexts that enable efficient logical separation to keep all customer traffic separate and secure in a multi-tenant environment.

The Cisco ASA 5585-X appliance features MultiScale™ performance, which provides rapid connections per second, an abundance of concurrent sessions, and accelerated throughput, and enables multiple security services for exceptional flexibility. The ASA 5585-X can offer up to 20 Gbps of real-world HTTP traffic and up to 35 Gbps of large packet traffic. It supports up to 350,000 connections per second and a total of up to two million simultaneous connections initially.

The Cisco ASA Services Module provides similar high performance, but is deployed as a plug-in module for Cisco Catalyst 6500 Series Switches. Cisco also provides another IPS deployment option with IPS sensors to enable distributed and intelligent detection with precision response to network attacks.

The Cisco Virtual Security Gateway works with Cisco Nexus 1000V switches to provide zone-based and policy-driven security at the virtual machine level, extending existing security policies into virtual and cloud environments. The Virtual Security Gateway provides secure segmentation to achieve logical separation at the VM level. Because the Virtual Security Gateway uses security-zone-based policy implementation rather than static IP addresses, it can consistently enforce security policies even as VMs move from one physical host to another. This support of VM mobility is critical to ensure policy consistency in an automated cloud environment where workloads can be processed anywhere in the cloud.

Furthermore, the Virtual Security Gateway logs all traffic permissions and denies for auditing and visibility purposes. The Cisco Nexus 1000V adds additional security and monitoring capabilities at the access layer, including PVLAN, IP Source Guard, DHCP Snooping, ARP inspection, and NetFlow. The vPath traffic steering mechanism in a Cisco Nexus 1000V switch can collaborate intelligently with the Virtual Security Gateway to offload destination traffic processing directly to the hypervisor after the initial packet of a flow has gone through Virtual Security Gateway policy enforcement. Such intelligent processing significantly increases processing efficiency and performance. Finally, a single Virtual Security Gateway can support multiple physical hosts due the distributed virtual switch design of Cisco Nexus 1000V switches. Such flexibility greatly increases the scalability of Cisco cloud security as more VMs are added to commissioned and non-commissioned pools of resources.

The Virtual Security Gateway is managed through the Cisco Virtual Network Management Center, which supports both built-in GUI and transparent operation management through an XML API. This XML API enables programmatic integration with third-party management and orchestration tools. Such capability is critical to enable cloud security service automation.

Together with the Cisco ASA 5585-X, ASA Services Module, and IPS sensors, the Cisco Virtual Security Gateway and Cisco Nexus 1000V switches enable in-depth cloud security for logical separation, policy consistency, automation, and access control in the cloud infrastructure. The Cisco solution helps secure multi-tenancy in public and hybrid cloud environments, and provides network traffic and activity visibility to help customers and service providers alike improve their cloud governance processes.

Cloud Security Services. Cisco offers email, web, and threat intelligence security via the cloud to help customers increase protection and scalability and reduce costs. These public and hybrid cloud security services include the following components:

- Cisco ScanSafe Web Security and Web Filtering
- Cisco IronPort™ Cloud, Managed, and Hybrid Email Security
- Cisco Registered Envelope Service for Email Encryption
- Cisco Security Intelligence Operations

Cisco ScanSafe Web Security redirects end-user web traffic directly to the ScanSafe cloud infrastructure, with access to more than 20 data centers around the globe. The service provides multiple layers of antivirus and antimalware scanning to prevent clients from accessing compromised web objects or pages, and incorporates additional security to prevent zero-day threats. The system analyzes every piece of web content accessed, including HTML, images, scripts, and Flash content. Each piece is analyzed using artificial-intelligence-based "scanlets" to build a detailed view of each web request and its associated security risk. The service also includes acceptable use controls to block users from specific websites and categories. Cisco ScanSafe Web Filtering includes Web Intelligence Reporting (WIRe), the world's most advanced web usage reporting system, which provides full visibility into how users are using the web and details the threats that Cisco ScanSafe blocks. The cloud service delivers a pervasive, high-performance, and scalable web security shield for end users whether they are in office, on the road, or working remotely.

Cisco ISR Web Security with Cisco ScanSafe is a new hybrid cloud security service delivered via the Cisco Integrated Services Router Generation 2 (ISR G2) product portfolio and Cisco ScanSafe. The system enables branch offices to intelligently redirect web traffic to the cloud to enforce granular security and control policy over dynamic Web 2.0 content, protecting branch office users from malware and enforcing a centralized policy. All resource-intensive operations, from content analysis to global reporting, are cloud-based. As a result, the web security functionality does not impact the performance of the other ISR G2 services such as firewall, intrusion prevention, and VPN.

Cisco offers multiple deployment options for email security, including onsite, hybrid, cloud, or managed. With the onsite model, customers manage their on-premises email security appliances and operations. With the hybrid model, customers can choose any cloud services while they manage their own on-premises services. For example, Cisco can provide cloud-based email filtering to remove spam and viruses while customers use on-premises Cisco IronPort C-Series Email Security Appliances for additional services such as data loss prevention, encryption, image analysis, and acceptable use filtering. The cloud services support full email security capabilities plus a special web-based management and monitoring interface for customers to have complete control over their gateways. Cisco IronPort Managed Email Security is a managed service offering that uses on-premises appliances.

Cisco offers two options for email encryption. An on-premises key server called the Cisco IronPort Encryption Appliance can manage envelope encryption keys for large organizations. But encryption customers that do not want to manage day-to-day operational issues prefer to use Cisco Registered Envelope Service, a cloud-based key management service. If an email message requires encryption, the email gateway (either on-premises or cloud-based) contacts the Cisco Registered Envelope Service. An encryption key is provided to the gateway, which then encrypts the message using this key. Recipients can open the message by interacting with the key server, even though the actual message and envelope are never stored in the cloud.

Cisco Security Intelligence Operations (SIO) is a cloud-based security service with three operational components:

1. Cisco SensorBase: The world's largest threat monitoring network that captures global threat telemetry data from an exhaustive footprint of Cisco devices and services.
2. Cisco Threat Operations Center: A global team of security analysts and automated systems who extract actionable intelligence from SensorBase data.
3. Dynamic updates: Real-time updates are automatically delivered to security devices worldwide.

Cisco SIO compiles real-time data that comes from web gateways, email gateways, probes, IPS sensors, routers with NetFlow at large ISPs, and Cisco AnyConnect™ endpoints. Cisco SIO has visibility into around 35% of global email traffic, 20 billion web requests per day, more than 30,000 IPS signatures that are triggered daily, and also feedback from over 150 million endpoints and almost 1 million devices deployed on customer locations around the world. This data is stored in Cisco SensorBase, where it is analyzed by sophisticated algorithms and Cisco SIO threat engineers. When new threats are detected, Cisco SIO generates new rule sets and reputation scores to rapidly distribute them to Cisco security systems that customers are using worldwide, including Cisco IronPort Email/Web Security Appliances, Cisco ScanSafe Web Security Cloud, Cisco ASA 5500 Series Appliances, and Cisco IPS 4200 Series Sensor Appliances. With frequent updates every few minutes, Cisco SIO dynamically keeps customers protected from potential threats, including zero-day attacks.

Overall, Cisco cloud security services enable customers to reduce their equipment management tasks; increase savings in floor and rack space, electricity consumption, and cooling power; and achieve a higher level of security.

Secure Cloud Access. The Cisco Secure Cloud Access solution component supports a multi-dimensional defense strategy that includes secure SaaS access and secure network access.

Cisco cloud security provides a critical SaaS Revocation evocation capability that enables secure access to cloud-based SaaS applications. When a SaaS user changes their role within an organization or leaves the job permanently, their access to SaaS applications must be adjusted or terminated immediately. Without a seamlessly implemented business process and HR database synchronization, the SaaS service provider may have a time delay to execute access updates, which may become a potential security vulnerability. The Cisco SaaS Revocation capability is delivered by the Cisco IronPort S-Series Web Security Appliances to provide high performance and scalable access control to SaaS applications. When this capability is enabled, no direct access to SaaS applications is permitted. Instead, SaaS users are authenticated at a central place within the SaaS cloud subscriber organization. After successful authentication, Security Assertion Markup Language (SAML) is used to authorize access to SAML-enabled SaaS applications.

IT administrators retain full control over authentication and authorization of SaaS application users, and users benefit from ease of use due to a single corporate sign-on for all of their SaaS-based activities. Furthermore, by denying direct access, cloud subscribers greatly reduce the attack surface associated with the exposed public interface of their cloud applications. A single authentication server, such as the Cisco Identity Services Engine, can provide access control for SaaS applications, VPN connectivity, and web proxy authentication. Cisco now supports corporate directory integration for many SaaS applications, with policy and access controls.

Securing network access adds one more security layer for cloud subscribers. Network-level access control, for example, allows IaaS subscribers to secure their own network to ensure data transfer and communications with the cloud are not compromised internally. For SaaS subscribers, network access to their own network greatly improves their overall cloud security if they also implement the SaaS Revocation capability. Cisco TrustSec® extends context awareness through policy-based access control for users and devices seeking access to the

distributed network. Cisco Identity Services Engine, which is the policy engine for Cisco TrustSec, enables policy consistency so that no matter how users are connecting to the network (wired connections, wireless connections, or remote access) they are always meeting a consistent set of policy requirements.

The combined Cisco Secure Cloud Access capabilities deliver policy consistency, high performance, and trusted access to the dynamic cloud environment today.

Summary

Cisco cloud security is a key part of the Cisco cloud strategy, which provides cloud solutions today for private, public, and hybrid clouds. Cisco cloud security contains three key areas:

1. In-depth capabilities to help public cloud service providers, subscribers, and private/hybrid cloud practioners secure their cloud infrastructure.
2. Cloud-based email, web, and threat intelligence security for customers.
3. Secure cloud access capabilities for organizations to better control access to SaaS applications and to enable a trusted cloud environment.

As customers embark on their cloud journey, Cisco cloud security helps them reduce their risks with consistent policies and enforcement, up-to-date threat intelligence, greater scalability, and improved performance. Cisco cloud security, in collaboration with many industry partners, helps remove cloud barriers so that customers can achieve the economies of scale and efficiency of cloud computing.

For More Information

Cisco ASA 5500 Series Adaptive Security Appliances: http://www.cisco.com/go/asa

Cisco AnyConnect: http://www.cisco.com/en/US/netsol/ns1049/index.html

Cisco Cloud Security: http://www.cisco.com/en/US/netsol/ns1066/index.html

Cisco Identity Services Engine: http://www.cisco.com/go/ise

Cisco secure virtual applications and data centers: http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns224/ns1097/white_paper_c11-652663.html

Cisco ScanSafe: http://www.cisco.com/go/scansafe

Cisco TrustSec: http://www.cisco.com/go/trustsec

Cisco Virtualization Security: http://www.cisco.com/go/vsec

Cisco Virtual Services Gateway: http://www.cisco.com/go/vsg

References

Gartner 2011 CIO Survey: Almost half of all CIOs expect to operate their applications and infrastructures via cloud technologies within the next five years.
http://www.gartner.com/technology/cio-priorities/2011-cio-survey.jsp

Forrester 2011 Report: Sizing The Cloud: Understanding And Quantifying The Future Of Cloud Computing.
http://www.forrester.com/rb/Research/sizing_cloud/q/id/58161/t/2

NIST Cloud Computing Reference Architecture.
http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/ReferenceArchitectureTaxonomy/NIST_CC_Reference_Architecture_v1_March_30_2011.pdf

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.**

Printed in USA C11-674558-00 06/11