

Cisco Cloud Security Overview

Borderless Network Security: Cloud Computing

Cloud computing is the ability to move infrastructure, services and applications into a data center (cloud) environment that is managed by someone else. There are several compelling reasons to move certain applications and services into the cloud. Providers can pass along the lower costs from streamlined, high-volume operations. Organizations can save on floor space and rack space, as well as cooling and electricity costs. And outsourcing certain parts of the system's management provides time and resource savings as well.

How significant are these savings? A recent IDC study on messaging security found that 25 percent of North American organizations have adopted a hybrid mix of on-premises and cloud messaging security services. Even more interesting is that the highest degree of adoption (38 percent) was found in large enterprise environments with more than 10,000 employees. This is clear evidence that cloud messaging security services are no longer just an SMB solution.

PRODUCT OVERVIEW

Cisco offers a wide range of products and solutions that can help businesses take advantage of cloud computing, including:

- Cisco® WebEx Mail
- Cisco WebEx® Meeting Center and WebEx Collaboration Cloud
- Cisco ScanSafe Web Security
- Cisco IronPort® Cloud Email Security, Hybrid Email Security and Managed Email Security
- Cisco Registered Envelope Service
- Cisco AnyConnect Secure Mobility Solution
- Cisco Security Intelligence Operations
- Cisco Nexus® and Unified Computing System platforms with Unified Service Delivery

Some of these offerings are used by service providers as part of their platform; others are used by enterprises in their private cloud infrastructure. For a growing number of organizations, cloud computing means outsourcing particular functions or adopting specific hosted applications.

Hosted services can take on many forms. Following are some examples:

- Software as a service, in which applications are delivered over the network on a subscription basis (Salesforce.com, for example).
- Platform as a service, in which Windows, Linux, or Solaris servers are rented by the month. Examples include application development, testing, hosting, database integration, storage and persistence. These services are often provisioned as an integrated solution over the Internet.
- Infrastructure as a service, in which computing, network, and storage services are delivered over the network on a pay-as-you-go basis (Amazon EC2, for example).



SECURITY CHALLENGES WITH CLOUD COMPUTING

Many organizations want the savings and efficiency benefits of cloud computing, but don't want to sacrifice traditional levels of control and security. Security is traditionally applied at the network perimeter; this disappears in cloud-based computing, in which borderless networks connect many types of users with enterprise private data centers and cloud-based resources. Some transactions, such as a remote worker accessing Salesforce.com, don't even pass through the corporate network or scanning systems.

The Cisco Borderless Network architecture addresses this challenge, securing cloud computing by placing intelligent control points and endpoints throughout the network. Figure 1 provides an example of how Cisco's on-premises and cloud-based security systems work together.

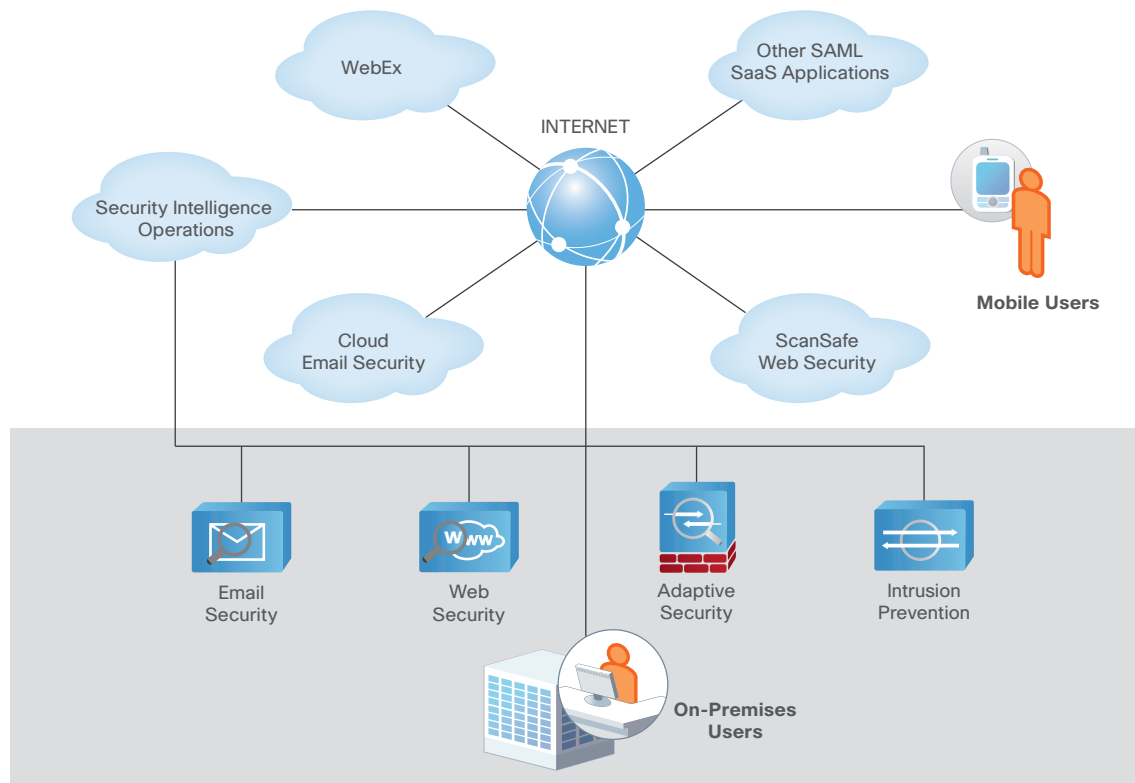


Figure 1: Cisco Secure Borderless Network architecture Cloud and Hybrid components in action.

CLOUD SECURITY COMPONENTS

This section describes Cisco's security-related software-as-a-service (SaaS) offerings. Cisco hosts these applications in the cloud, enabling customers to reduce or eliminate the number of on-premises security systems they have to maintain. For information about Cisco WebEx SaaS applications, please visit www.webex.com. For information about Cisco Nexus and Unified Computing System platforms, please visit www.cisco.com/unifieddatacenter.

Cisco ScanSafe Web Security



In 2009, Cisco acquired ScanSafe, a leading cloud-based web security provider. ScanSafe offers consistent, enforceable, high performance web security and policy regardless of where or how users access the Internet. With numerous data center locations spread around the globe, ScanSafe Web Security is both scalable and reliable. Every day the ScanSafe service scans billions of web requests and has a track record of seven years continuous uptime.

ScanSafe is proven to block more malware than traditional web security solutions and focuses on preventing zero-day malware threats. This is achieved using the wide visibility into web content gained by the solution's position in the cloud and also integration with Cisco Security Intelligence Operations (SIO), discussed below.

ScanSafe also includes web filtering and control capabilities as well as advanced cloud-based reporting visibility. This offers complete visibility and flexibility into web usage to identify issues and influence policy enhancements.

Cisco IronPort Cloud, Managed and Hybrid Email Security

The Cisco IronPort Hybrid Email Security service is currently available for email filtering. In many cases, customers use the cloud-based service to remove spam and viruses, but use on-premises Cisco IronPort C-Series Email Security Appliances for services such as data loss prevention, encryption, image analysis, and acceptable use filtering. The cloud services include a special web-based management and monitoring interface for customers who need complete control over their gateways. Cisco IronPort Managed Email Security is a managed service offering that uses on-premises appliances and is available for customers who prefer a hands-off approach. Unlike competing services, Cisco IronPort Cloud and Hybrid Email Security provide maximum data protection in the cloud with private infrastructures.

Cisco Registered Envelope Service for Email Encryption

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 most encryption customers prefer to use Cisco's cloud-based key management service, Cisco Registered Envelope Service. If a 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 AnyConnect Secure Mobility Solution

The Cisco AnyConnect Secure Mobility Solution delivers advanced, "always-on" protection for mobile workers. The solution comprises three Cisco products: the Cisco IronPort S-Series Web Security Appliance provides web filtering, the Cisco ASA 5500 Series Adaptive Security Appliance provides VPN head-end functions, and the Cisco AnyConnect VPN Client provides VPN connection management and other functions. The solution supports desktops, laptops, tablets, and smart phones with popular operating systems. As users roam between public and private (enterprise) networks, their VPN automatically reconnects and redirects traffic to Cisco IronPort S-Series appliances.

The Cisco AnyConnect Secure Mobility Solution has two enhancements specifically for cloud-based computing: Dynamic Context Routing and SaaS Revocation.

Dynamic Context Routing When a roaming user accesses the Internet, all traffic is tunneled and backhauled to one or more scanning elements within the enterprise. If the content is high-volume (such as YouTube streaming media) and the basic header and response checks show no security or acceptable use risks, the client is permitted to fetch the content directly. This increases the performance and efficiency of high-bandwidth applications. Administrators can control this intelligent split tunnel without sacrificing security.

SaaS Revocation This feature addresses a critical problem with hosted SaaS applications such as WebEx. When a user ends employment with an organization, the enterprise security team must disable that person's access in every SaaS account he or she used. When there are multiple SaaS applications, such as Salesforce.com and Google Apps, this becomes a time-consuming and error-prone process. Users also have separate passwords for each SaaS application; forgetting these results in frequent password reset requests.

The Cisco IronPort S-Series now supports SaaS Revocation, in which authentication to Security Assertion Markup Language (SAML)-enabled SaaS applications is proxied. With a single click, an administrator can grant or revoke access for specific users or groups, for multiple applications. A single authentication server, such as Cisco Secure Access Control



Server (ACS), can provide access control for SaaS applications, VPN connectivity, web proxy authentication, and more. Cisco now supports corporate directory integration for many SaaS applications, with policy and access controls.

The Cisco AnyConnect Secure Mobility Solution puts security filtering in the cloud, protecting the user's choice of endpoint devices without relying on client-based anti-virus or regular OS patches.

Cisco Security Intelligence Operations

Cisco Security Intelligence Operations (SIO) is a cloud-based service that gathers data about Internet traffic, servers, and compromised PCs—anywhere in the world. The data comes from web crawlers, email gateways, probes, IPS sensors, routers with NetFlow at large ISPs, and other sources. This data is stored in SensorBase, where it is analyzed by sophisticated algorithms and threat engineers. When new threats are detected, Cisco SIO generates new rule sets and reputation scores that are used by Cisco security products, including:

- Cisco IronPort C-Series Email Security Appliances
- Cisco IronPort S-Series Web Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco IPS 4200 Series Sensor Appliances

Cisco devices access these rule updates every few minutes, which helps to protect Cisco customers from zero-day threats. For more information about Cisco SIO, please visit www.cisco.com/go/sio or download the SIO-To-Go iPhone application.

SUMMARY

Traditional network borders are breaking down at the same time that security threats are increasing. Cisco offers a wide range of cohesive cloud-based security applications and services, enabling customers to choose the combination of on-premises and/or cloud services that meet their individual requirements and business demands. Part of the Secure Borderless Network initiative, Cisco cloud-based offerings can help to secure your organization, now and into the future.

For more information about Cisco Secure Borderless Networks, please visit www.cisco.com/go/borderless.



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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco-Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document 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. (1002R)

Many of the products and features described in this document remain in varying stages of development and will be offered when and if they are available. This roadmap is subject to change at the sole discretion of Cisco, and Cisco will have no liability for delay in the delivery of, or failure to deliver, any of the products or features set forth in this document.