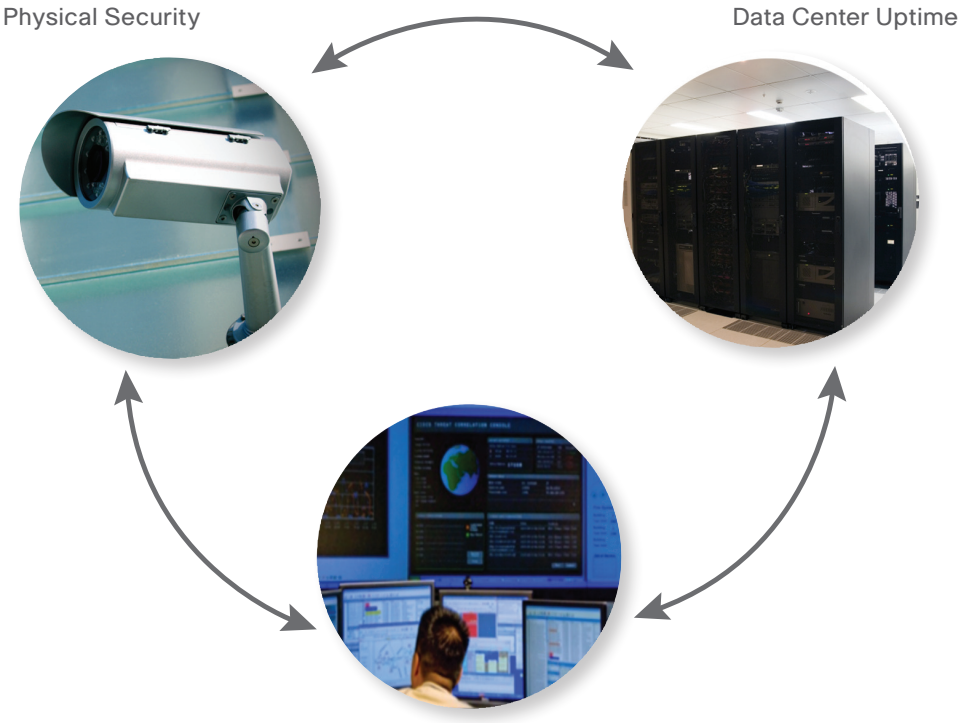
Infrastructure Security Overview

Cisco IronPort Hosted Email Security

Cisco® IronPort Hosted Email Security combines best-of-breed technologies to provide the most scalable and sophisticated email protection available today. Based on the same industry-leading technology that protects 40 percent of Fortune 1000 companies from inbound and outbound email threats, Cisco IronPort Hosted Email Security allows customers to reduce their on-site data center footprint and out task the management of their email security to trusted security experts. It provides a dedicated email security infrastructure in multiple, resilient data centers to enable the highest levels of service availability and data protection.

Cisco IronPort Email Security solutions are designed to ensure the highest levels of security and availability of the hosted infrastructure – from both a physical and logical access perspective. The design spans aspects like access controls to data center buildings, processes to protect access to customer data, and the availability of the hardware infrastructure. The figure below highlights these aspects.



PHYSICAL SECURITY

Physical security of the data center is the foundation of a vigilant security infrastructure. Data center security is supported by state-of-the-art surveillance systems, backed by security personnel to ensure the highest levels of physical infrastructure security. This includes:

1. Surveillance System

   Along with Cisco's onsite presence, a digital video surveillance system provides for an automated surveillance interface. All fixed cameras are high-resolution color, with auto low-light switching capable of viewing to .01 lux. Pan/tilt/zoom (PTZ) cameras are used on the exterior and areas of sensitivity. All PTZs use up-the-coax protocol for immediate relocation to any current fixed camera location.

   Video is recorded at 720x240 pixels at 15 IPS upon motion or 30 IPS upon operator command. Most video channels synchronously record audio. Video is retained for approximately 100 days. The data center deploys an active surveillance system with 24x7 officers operating the camera system using IOU (Identify, Observe and Understand) methodology. The use of IOU increases attentiveness to the monitors and provides a superior video product for investigations. Executive team members have remote access to video via PDA and VPN laptop access. All video is archived in M-JPEG format for a minimum of 90 days.

2. Access Control/Intrusion Detection

   All entrances are centrally monitored 24x7x365. The exterior doors were designed and installed for additional protection. They include detection devices, access control and can be independently viewed by fixed cameras. Exterior access points are kept to a minimum, and (in most cases) only one door at each facility can be used for entry or exit. These doors lead into specially-engineered mantraps, constructed of 12 gauge stainless steel and strapped by ¼" aluminum. All access points off the mantrap require the additional biometric authentication of the card holder and mantrap relay logic. Additionally, the mantraps are fitted with a minimum of one fixed camera and audio surveillance of the space.

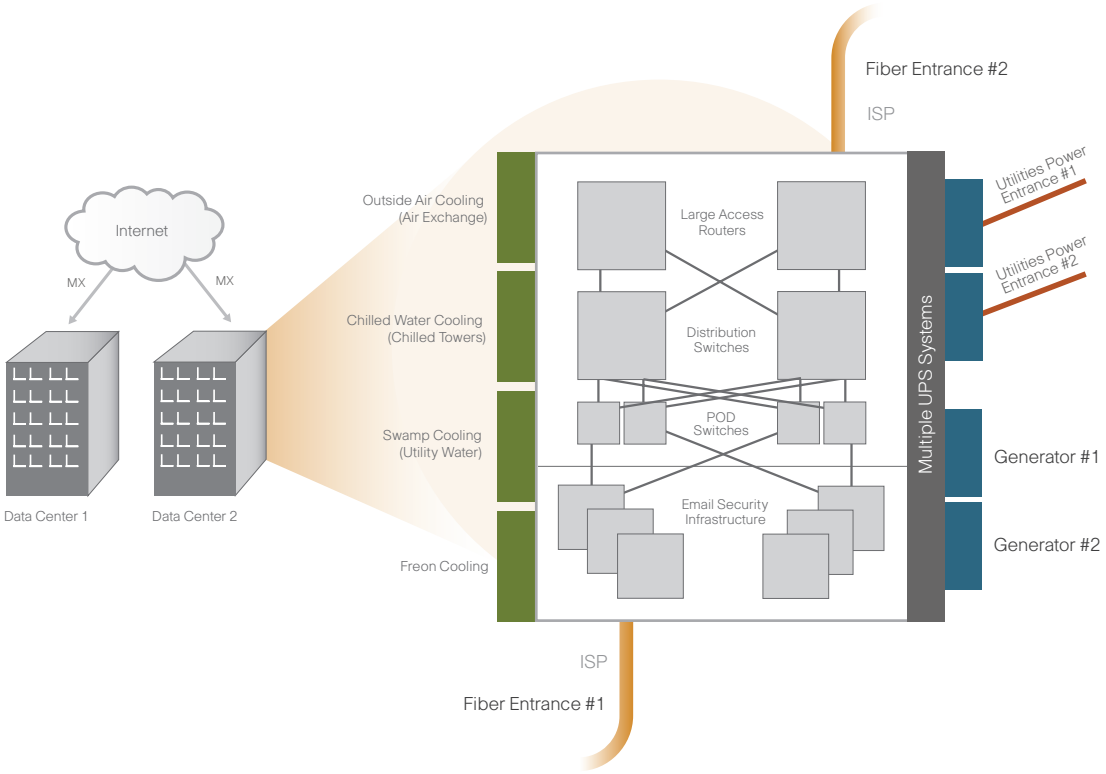
DATA CENTER UPTIME

The figure on page 3 describes the architecture of the Cisco IronPort Hosted Email Security solution. Highlights of this solution include:

1. Geographically-diverse data centers for disaster recovery
2. SAS 70 Type II certified data centers
3. Network connectivity, power, cooling and bandwidth redundancy within each data center
4. Bandwidth to process up to 20 Gb/sec of network traffic

DATA CENTER UPTIME (CONTINUED)

Cisco IronPort Hosted Email Security employs multiple SAS 70 Type II data centers in an active-active deployment architecture. By pointing multiple MX records to these data centers the solution provides email continuity, even in the event of an unforeseen disaster at one of the data centers. The architecture, which includes multiple data centers, ensures the highest level of availability for the Cisco IronPort Hosted Email Security service.



Cisco IronPort Hosted Email Security Data Center Architecture

Each of the data centers has multiple levels of redundancy built into the infrastructure. The first is the network infrastructure that has multiple carrier-grade access routers, distribution switches and POD switches – ensuring that there is no single point of failure. Behind this highly-redundant networking infrastructure, the solution employs multiple dedicated Cisco IronPort email security hardware that is used for mail processing, reporting, tracking and more. To prevent failure and ensure connectivity in the event of an unexpected incident which impacts one of the inputs, the data centers utilize two separate fiber inputs that are physically separated. Additionally, these data centers have the bandwidth capacity to process up to 20 Gb/sec of network traffic.

Most data centers today are faced with severe issues resulting from improper management and control of equipment-generated heat. The data centers are designed with the most advanced designs for space and power in the industry. They have 100 percent power availability, delivered via a very sophisticated power grid architecture that includes primary power circuits and failover power connections, both of which come from two completely separate N+2 power systems. Each of these systems has separate UPS batteries, generators, PDUs, and RPPs, and are delivered to each rack via color-coded receptacles. This ensures consistent uptime for the email security infrastructure that is plugged into the system.

DATA CENTER UPTIME (CONTINUED)

As server densities have increased, the demand on cooling systems has grown significantly. Each data center facility has enough primary and backup cooling to ensure that the heat generated by the email security infrastructure is appropriately dissipated and ample backup cooling is available in case of a failure with one of the cooling systems. The cooling infrastructure is delivered through Freon, swamp, chilled water and outside air mechanisms.

Specifications of the infrastructure at work in powering the data center are listed below.

1. Power Specifications

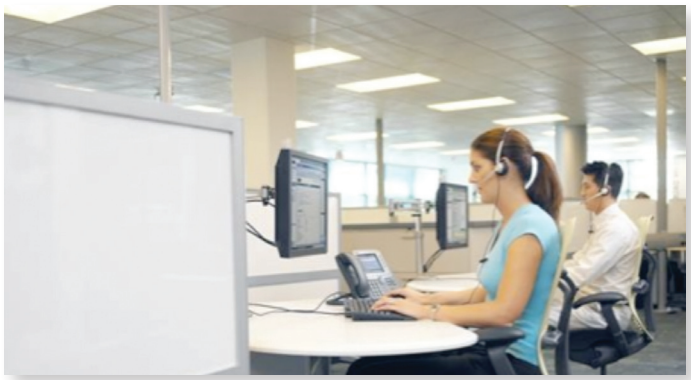
17 KiloWatts Power and cooling per rack	UPS backup power
120/208V AC and -48V DC available	Voltage output 480 transformed to 120/208 V
100% generator backup	-48 Volt DC Battery Plant
Generator capacity designed to multiple 1 to 2 MgWatt generators	1200 amp expandable to 10,000 amp
Size of fuel tank 1,000 to 2,000 gallons	2-hour battery reserve non-redundant, 4 hours redundant
Generator both auto start and auto transfer. Isolation bypass feature on automatic transfer switch.	True A/B power feeds
Minimum 24-hour run time fuel capacity	Grounding in accordance with NFPA 70
Two-hour response for fuel delivery	

2. Environmental Controls

Under-floor cooling provided by computer-room grade equipment	Cooling not less than 200 BTU/h per square foot with an N+1 redundancy
Temperature maintained at 72 degrees F dry bulb at ASHRAE 1%	In the event of a power interruption, HVAC systems (and entire facility) operate on diesel generators.
30% to 60% humidity non-condensing. Humidity control delivered through ATS/Liebert units via infrared humidifier.	

SECURITY OPERATIONS CENTER

The Cisco Security Operations Center (SOC) is run by the Cisco Remote Operations Services (ROS) organization. In order to ensure a world-class level of security oversight, Cisco ROS implements continual management and internal auditing of employees, processes and tools. This helps deliver peace of mind to Cisco customers, as well as the highest level of secure service delivery standards.



Cisco Security Operations Center Help Desk

1. Network Security

With a combination of security devices and applications, adding to a defense-in-depth design, the Cisco SOC uses a layered approach to security. Additional layers include multiple firewalls to control inbound access to Cisco ROS. This strategy allows users to only access information that is legitimate to their purpose (least privilege).

Intrusion detection systems (acting as sensors) are strategically placed throughout the network to monitor traffic and detect security events. Detected events are managed by the Cisco Security Management Service. Intrusion detection is used at various points within the network, monitoring the traffic between the service delivery network and customer networks for suspicious or malicious patterns.

A security event manager provides event and threat correlation of the security devices throughout the service delivery network. Digital certificates are used to secure access to customer web portals and systems that require both internal and external access.

2. Systems Security

Cisco ROS uses multiple controls to ensure the security of managed systems. These include both physical controls and vulnerability detection scans.

a. Physical Controls

Cisco provides photo identification to all employees and contractors, which must be worn visibly within the building. All visitors must obtain a visitor's badge and be escorted within the building.

Entrances to controlled data centers and wiring closets are accessible only from internal corporate space. Access is granted based on a business need. Corporate space is also controlled, requiring proper badge access to enter.

Video cameras are located at each building entry and monitored and managed by the 24x7 Security Facilities Operation Center.

Primary power to the facility is provided by the local utility. Backup power is provided to critical areas by standby UPS systems and generators. Backup power systems are routinely checked and tested. Preventive maintenance is performed quarterly and full load tests are conducted annually.

b. Vulnerability Scans

The Cisco ROS service delivery network is routinely scanned to assess risks and vulnerabilities. Results from these assessments are used to create internal IT incident cases for necessary remediation.

SECURITY OPERATIONS CENTER (CONTINUED)

3. Human Controls

Information security, and the protection of informational assets and intellectual property, begins with awareness and education. To develop and preserve a culture of security, successful organizations recognize that responsibility and accountability resides with all employees.

At Cisco, the executive team has embedded security into corporate initiatives and its code of business conduct, and employees are assimilating security in their daily activities. With employees educated about the importance of security awareness throughout the organization, everyone works together toward the common goal of keeping the company (and its partners and customers) secure.

Human controls are becoming an important aspect of data center security. The aim for these controls is to protect customer data against security threats that may arise from within the service provider. Cisco ROS has a number of different controls in place that help ensure customer data security. Cisco conducts background screenings as part of the hiring process for all full-time and contract employees. Job descriptions outline roles and responsibilities within Cisco ROS, and the rule of least privilege is applied to ensure proper access to customer networks and information.

Additional human controls utilized by Cisco ROS include:

a. Auditing and Testing

Cisco ROS employs a five-step process to mitigate exposure to network-based threats. This process includes utilizing a defined security policy, assessing compliance, monitoring for policy violations, and routinely testing the policy to minimize exposure. The final step includes a routine overview of all identified threats and exposures to improve the overall security of the network.

b. Change Control

Change control is critical to the operation of any IT environment and Cisco ROS service delivery teams. Cisco ROS change control is a partnership with customers to establish proper authorization for requesting, scheduling, implementing and validating all changes within the customer environment.

CONCLUSION

Cisco IronPort Hosted Email Security is backed by state-of-the-art data centers that enable the highest available physical, utility and data redundancy under one roof. The support of the Cisco Security Operations Center provides an additional layer of security, ensuring secure service delivery. Through these means, Cisco is able to offer the highest levels of service availability and data protection.

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**.

P/N 435-0255-1 6/09