SAFE Architecture Guide

Places in the Network: Secure Data Center

April 2018

SAFE
SIMPLIFIES SECURITY

Contents

Overview

The Secure Data Center is a place in the network (PIN) where a company centralizes data and performs services for business. Data centers contain hundreds to thousands of physical and virtual servers that are segmented by applications, zones, and other methods. This guide addresses data center business flows and the security used to defend them.

The Secure Data Center is one of the six places in the network within SAFE. SAFE is a holistic approach in which Secure PINs model the physical infrastructure and Secure Domains represent the operational aspects of a network.

The Secure Data Center architecture guide provides:

- Business flows for the data center
- Data center threats and security capabilities
- Business flow security architecture
- Design examples and a parts list

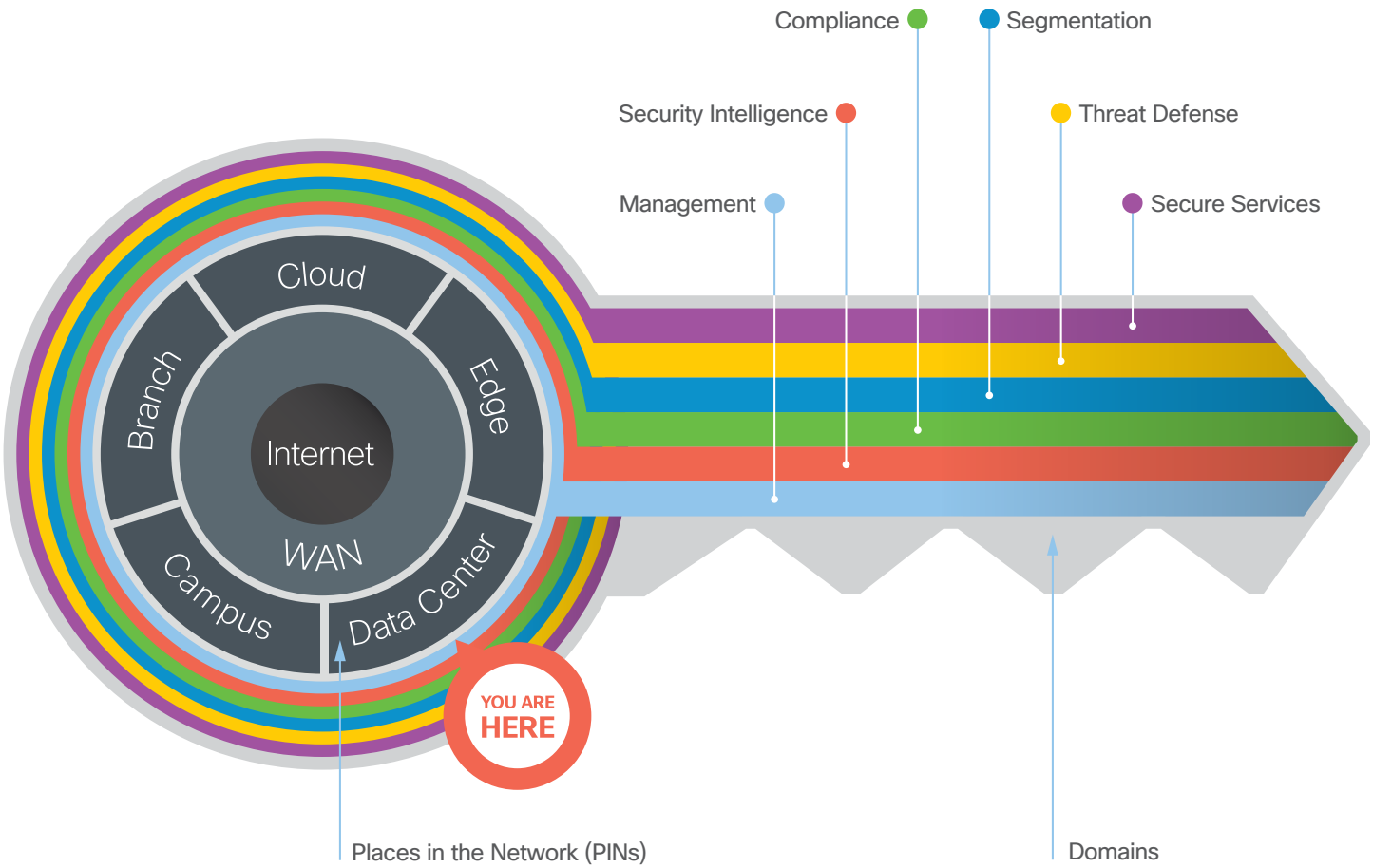


Figure 1 ***The Key to SAFE.*** *SAFE provides the Key to simplify cybersecurity into Secure Places in the Network (PINs) for infrastructure and Secure Domains for operational guidance.*

Return to Contents

SAFE simplifies security by starting with business flows, then addressing their respective threats with corresponding security capabilities, architectures, and designs. SAFE provides guidance that is holistic and understandable.

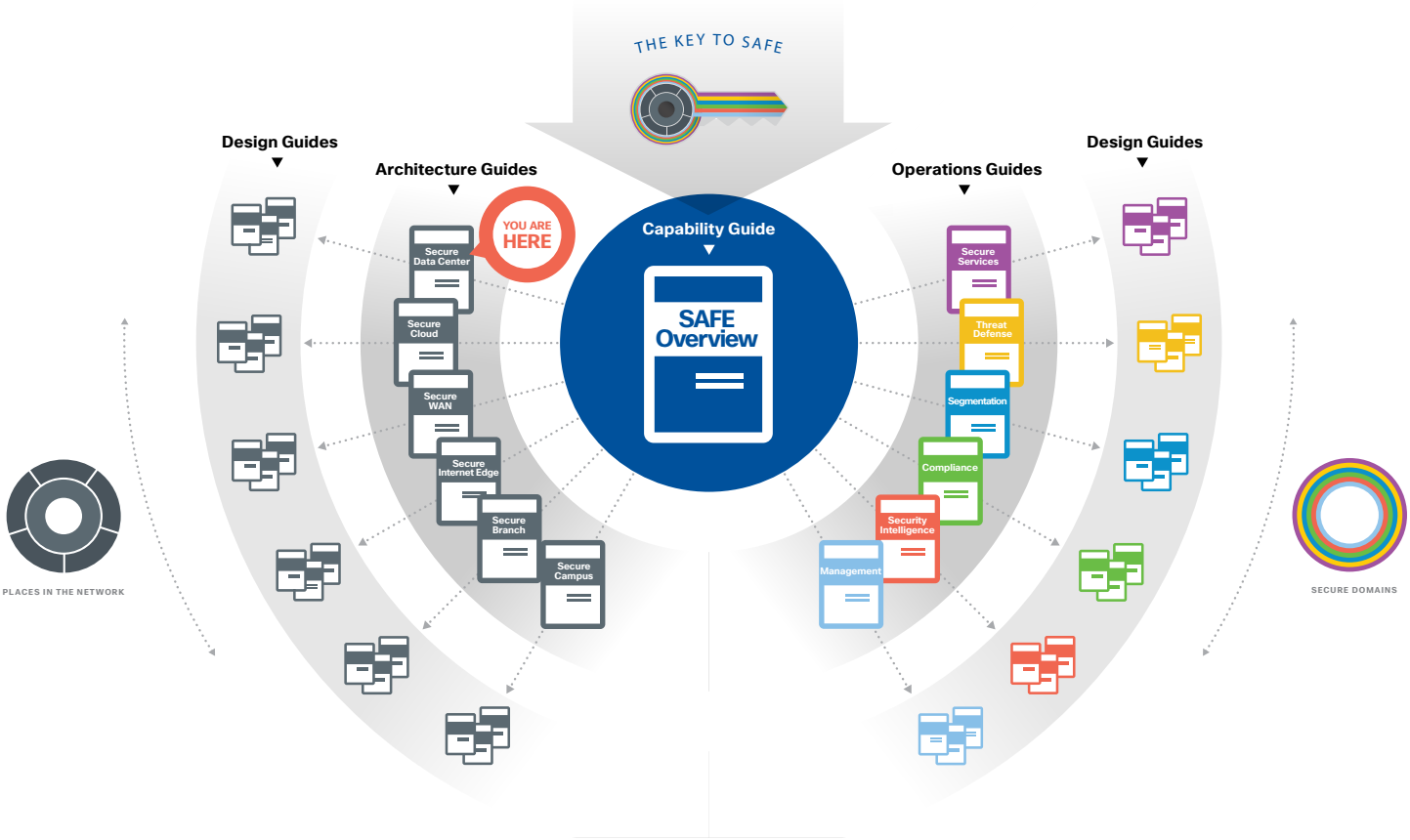


Figure 2 *SAFE Guidance Hierarchy*

Return to Contents

Business Flows

The Secure Data Center provides business services to the company's users. It is the central destination and transit area that ties the company business flows together.

- Internally, employees in the branch, campus, and remote locations require access to applications, collaboration services (voice, video, email), and the Internet. Systems communicate east/west within and between data centers.
- Third parties, such as service providers and partners, require remote access to applications and devices.
- Customer guest traffic transits the network en route to the Internet edge.

Figure 3 *Data center business use cases are color coded to define where they flow.*

Return to Contents

Functional Controls

Functional controls are common security considerations that are derived from the technical aspects of the business flows.

Secure Applications	Applications require sufficient security controls for protection.
Secure Access	Servers and devices securely accessing the network.
Secure East/West Traffic	Data moves securely; internally, externally, or to third-party resources.
Secure Remote Access	Secure remote access for employees and third-party partners that are external to the company network.
Secure Communications	Email, voice, and video communications connect to potential threats outside of company control and must be secured.

Figure 4 *Data center business flows map to functional controls based on the types of risk they present.*

Return to Contents

Capability Groups

Data center security is simplified by grouping capabilities into three groups which align to the functional controls: Foundational, Business, and Access.

Each flow requires the access and foundational groups. Business activity risks require appropriate capabilities to control or mitigate them as shown in Figure 5, which often reside within the data center. User clients and devices also require security, but are non-data center capabilities.

For more information regarding capability groups and functional controls, refer to the SAFE overview guide.

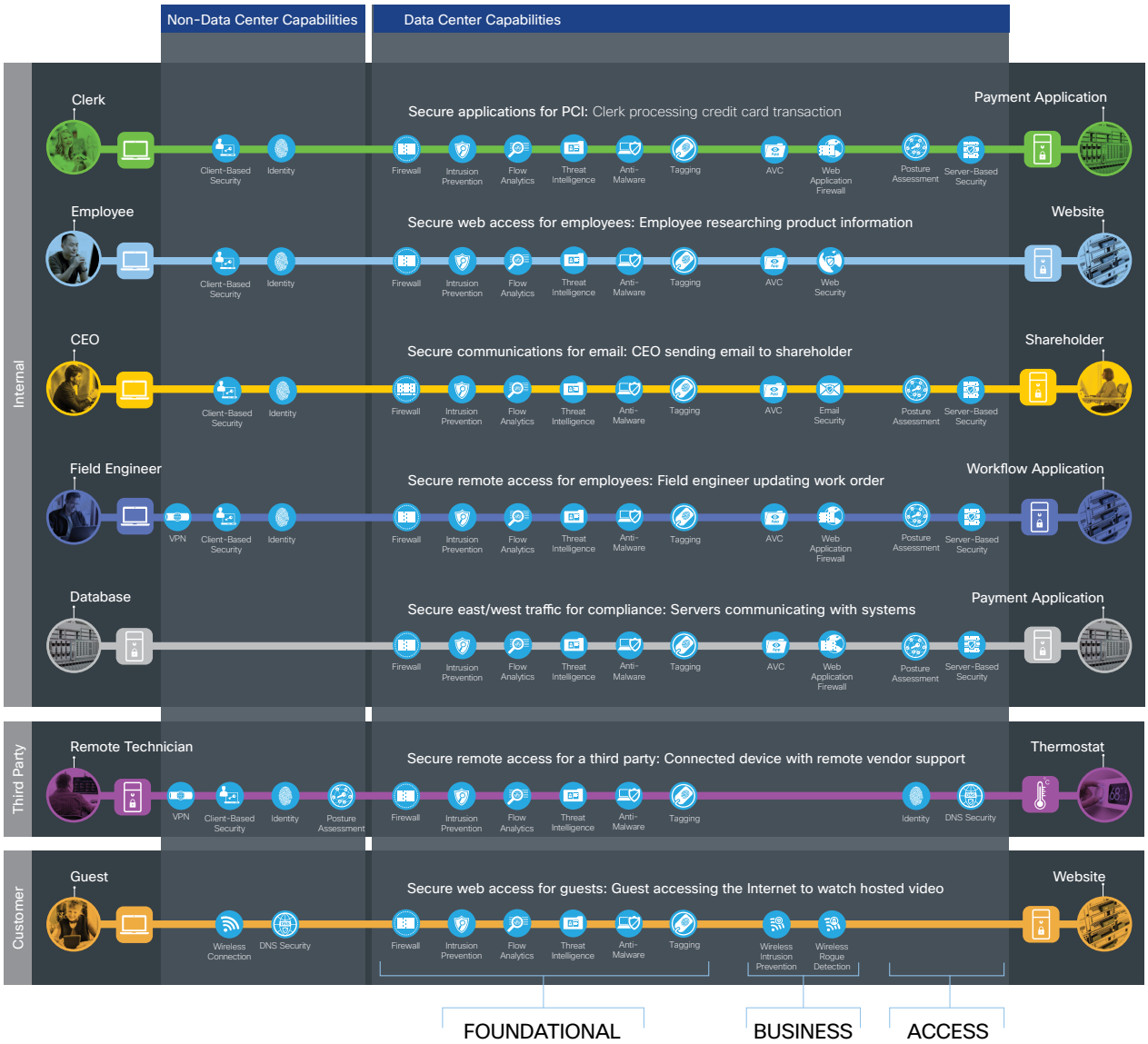


Figure 5 *The Secure Data Center Business Flow Capability Diagram*

Secure Data Center threats and capabilities are defined in the following sections.

Return to Contents

Threats

Data centers contain the majority of business information assets and intellectual property. These are the primary goals of targeted attacks and require the highest level of investment to secure. The data center has four primary threats:

Data extraction (data loss)

The unauthorized ex-filtration or theft of a company's intellectual property, innovation, and proprietary company data.

Unauthorized network access

Unauthorized access gives attackers the potential to cause damage, such as deleting sensitive files from a host, planting a virus, and hindering network performance with a flood of illegitimate packets.

Malware propagation

Assets in the data center are targets for east/west contamination between servers, and north/south from employees, partners, or customer devices on the network. Applications that process credit card transactions and Internet of Things devices are the most prevalent targets.

Botnet cultivation

The resources of a server farm are a valuable target for botnet cultivation.

Botnets are networks made up of remote-controlled computers, or "bots." They are used to steal data, send spam, or perform other attacks.

The defense is explained throughout the rest of the document.

Return to Contents

Security Capabilities

The attack surface of the data center is defined by the business flows, and includes the people and the technology present. The security capabilities that are needed to respond to the threats are mapped in Figure 6. The data center security capabilities are listed in Table 1. The placement of these capabilities are discussed in the architecture section.

Figure 6 *Secure Data Center Attack Surface and Security Capabilities*

Return to Contents

Table 1 *Secure Data Center Attack Surface, Security Capability, and Threat Mapping*
Products that implement these capabilities can be found in Table 2.

Data Center Attack Surface			
Human	**Security Capability**		**Threat**
Users: Employees, third parties, customers, and administrators.	**Identity:** Identity-based access.		Attackers or disgruntled admins accessing restricted information resources.
Devices	**Security Capability**		**Threat**
Clients: Devices such as PCs, laptops, smartphones, tablets.	**N/A:** Addressed in other PINS where clients reside.		Compromised administrator systems obtaining elevated access.
Voice/Video: Phone and teleconferencing.	**N/A:** Covered in Secure Services domain.		Attackers accessing private information.
Autonomous Device: Building controls.	**N/A:** Covered in IoT Threat Defense.		Attackers taking over systems.
Network	**Security Capability**		**Threat**
Wired Network: Physical network infrastructure; routers, switches, used to connect access, distribution, core, and services layers together.	**Firewall:** Stateful filtering and protocol inspection between segments in the data center.		Unauthorized access and malformed packets between and within the data center.
	Intrusion Prevention: Blocking of attacks by signatures and anomaly analysis.		Attacks using worms, viruses, or other techniques.
	Tagging: Software-based segmentation using EPG's/TrustSec/VLANs		Unauthorized access and malicious traffic between segments.
Wireless Network: Branches vary from having robust local wireless controller security services to a central, cost-efficient model.	**N/A:** Covered in Branch and Campus PINS.		Attacks on the infrastructure via wireless technology.

Return to Contents

Network (continued)	Security Capability	Threat
Analysis: Analysis of network traffic within the campus.	**Anti-Malware:** Identify, block, and analyze malicious files and transmissions.	Malware distribution across networks or between servers and devices.
	Threat Intelligence: Contextual knowledge of existing and emerging hazards.	Zero-day malware and attacks.
	Flow Analytics: Network traffic metadata identifying security incidents.	Traffic, telemetry, and data exfiltration from successful attacks.
WAN: Public and untrusted Wide Area Networks that connect to the company, such as the Internet.	**N/A:** Covered in Branch, Campus, WAN, and Edge PINS.	Exposed services and data theft of remote workers and third parties.
Cloud	**N/A:** Covered in Branch, Campus, Edge and Cloud PINS.	Unauthorized access and malformed packets connecting to services.
Applications	**Security Capability**	**Threat**
Applications: Management, servers, database, load balancer.	**Application Visibility Control:** Inspects network communications.	Unauthorized access and malformed packets connecting to services.
	Central Management: Company-wide management, monitoring, and controls.	Single target for complete company control and destruction.
	Malware Sandbox: Inspects and analyzes suspicious files.	Zero-day malware and attacks.
	TLS Encryption Offload: Accelerated encryption of data services.	Theft of unencrypted traffic.
	Web Application Firewalling: Advanced application inspection and monitoring.	Attacks against poorly developed applications and website vulnerabilities.
Storage: Drives, databases, media.	**Disk Encryption:** Encryption of data at rest.	Theft of unencrypted data.

Return to Contents

Applications (continued)	Security Capability	Threat
 Servers	 **Server-based Security:** Security software for servers with the following capabilities:	
	 **Anti-Malware:** Identify, block, and analyze malicious files and transmissions.	 Malware distribution across servers.
	 **Anti-Virus**	 Viruses compromising systems.
	 **Cloud Security:** Security services from the cloud.	 Redirection of session to malicious website.
	 **Host-based Firewall:** Provides micro-segmentation.	 Unauthorized access and malformed packets connecting to server.
	 **Posture Assessment:** Server compliance verification, authorization, and patching.	 Targeted attacks taking advantage of known vulnerabilities.
	 **Disk Encryption:** Protect information at rest.	 Unauthorized access to system-stored data.

Return to Contents

Management	Security Capability	Threat
 Management, Control, and Monitoring	 **Analysis/Correlation:** Security event management of real-time information.	 Diverse and polymorphic attacks.
	 **Anomaly Detection:** Identification of infected hosts scanning for other vulnerable hosts.	 Worm traffic that exhibits scanning behavior.
	 **Identity/Authorization:** Centralized identity and administration policy.	 Single target for complete company control and destruction.
	 **Logging/Reporting:** Centralized event information collection.	 Unauthorized network access or configuration.
	 **Monitoring:** Network traffic inspection.	 Traffic, telemetry, and data ex-filtration from successful attacks.
	 **Policy/Configuration:** Unified infrastructure management and compliance verification.	 Seizure of infrastructure or devices.
	 **Time Synchronization:** Device clock calibration.	 Misdirection and correlation of attacks.
	 **Vulnerability Management:** Continuous scanning, patching, and reporting of infrastructure.	 Malicious device connected to infrastructure.

Return to Contents

Architecture

SAFE underscores the challenges of securing the business. It enhances traditional network diagrams to include a security-centric view of the company business. The Secure Data Center architecture is a logical grouping of security and network technology that supports data center business use cases. It implements a traditional access/distribution/core network architecture as well as application-centric server farm.

SAFE business flow security architecture depicts a security focus. Traditional design diagrams that depict cabling, redundancy, interface addressing, and specificity are depicted in SAFE design diagrams. Note that a SAFE logical architecture can have many different physical designs.

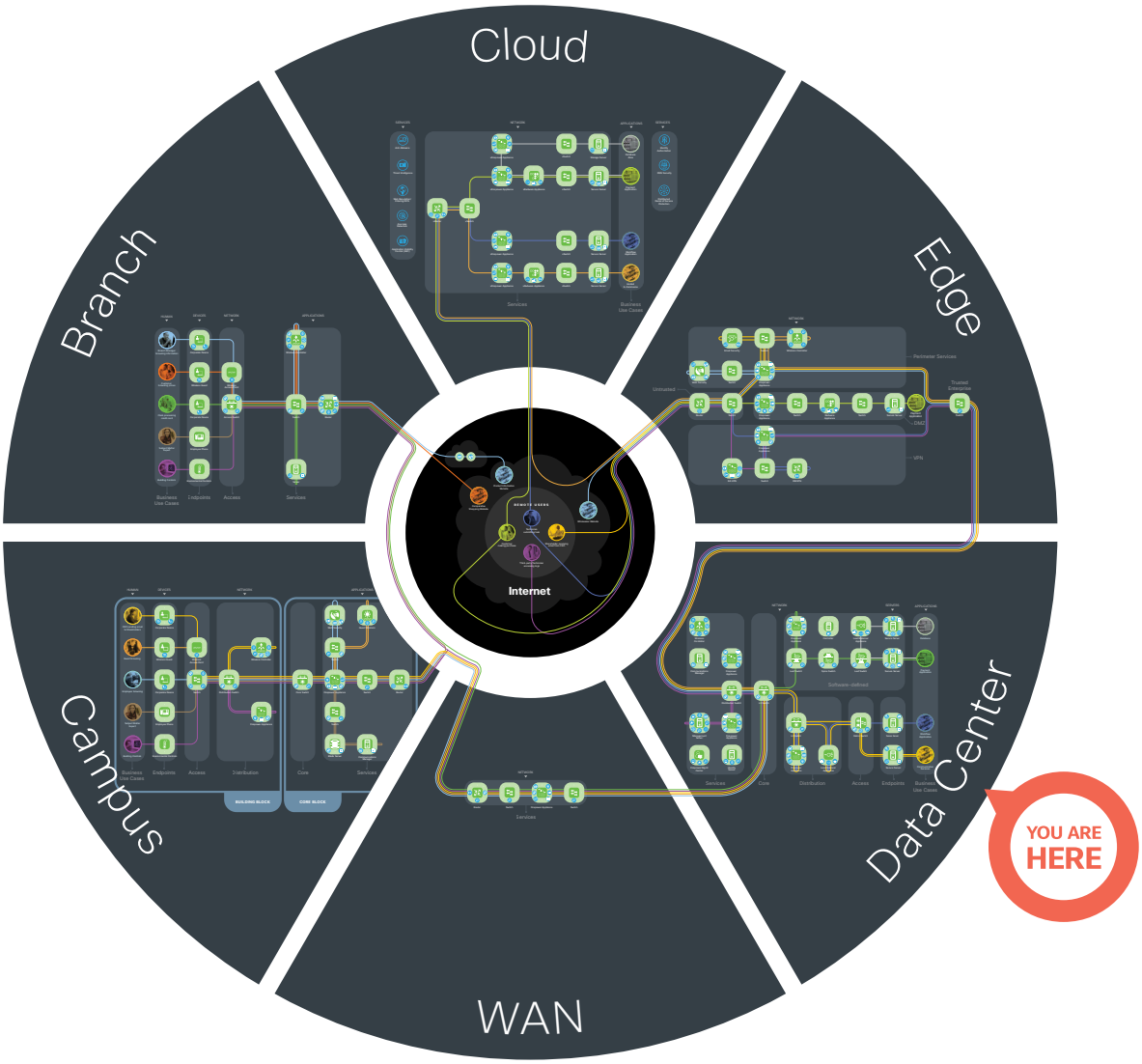


Figure 7 ***SAFE Model.*** *The SAFE Model simplifies complexity across a business by using Places in the Network (PINs) that it must secure.*

Return to Contents

Secure Data Center

The Secure Data Center architecture has the following characteristics:

- Visibility with centralized management, analytics, and shared services
- A core connecting distribution and application-centric layers
- Redundant high-performance appliances for availability and maximum uptime
- Modular access and distribution layers which dynamically segment applications
- Software-defined network segmentation, orchestration
- Software-defined application segmentation
- Physical and virtual servers requiring secure network access connectivity

Humans and devices are part of the attack surface, but are not part of the architecture within the data center. Data centers are often deployed within a campus or corporate headquarters.

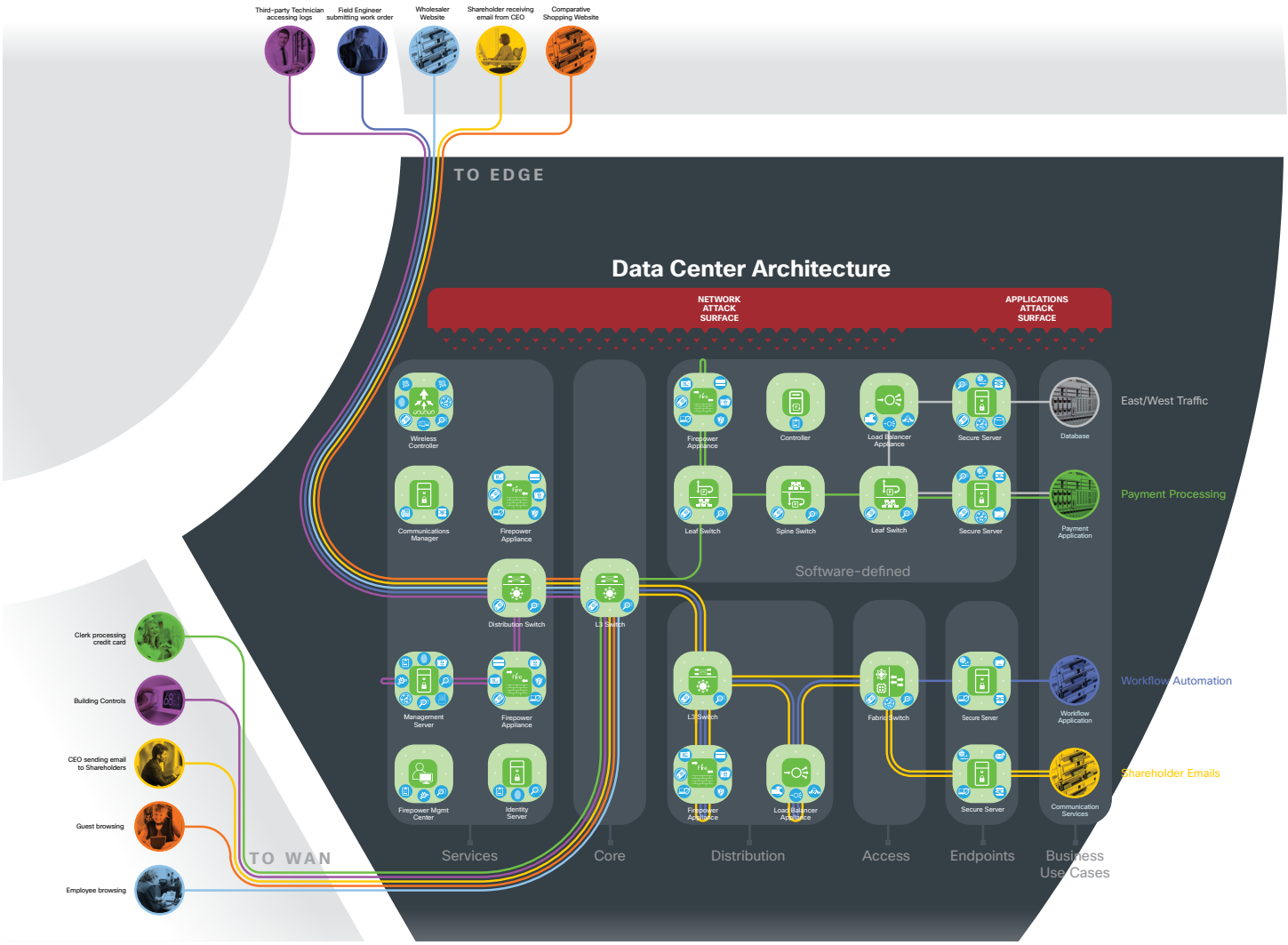


Figure 8 ***Secure Data Center.*** *The Secure Data Center business flows and security capabilities are arranged into a logical architecture. The colored business use cases flow through the green architecture icons with the required blue security capabilities.*

Return to Contents

Attack Surface

The Secure Data Center attack surface (Figure 6) consists of Humans, Devices, Network, and Applications. A successful breach gives an attacker the "keys to the kingdom." Security includes these considerations:

- Human administrators are located outside of the data center
- Devices are autonomous vs. operated by users
- Network security is enhanced by comprehensive physical security
- Applications and data contain vital company information
- Hosted by company-wide, centralized management
- Application orchestration centralizes control of security, network, and server elements into a single critical target

The sections below discuss the security capability that defends the threats associated with each part of the surface.

Humans

Typically, humans in the data center are administrators. No amount of technology can prevent successful attacks if the administrators themselves are compromised.

Administrators that are disgruntled (fired, demoted, bullied, ideology), compromised (blackmail, threats, bribery), or have had their credentials stolen (phishing, key logger, password reuse) are the single biggest risk in the security of a company.

Administrators have a higher level of access than normal users which requires additional controls:

- Two-factor authentication
- Limited access to job function
- Logging of administrator changes
- Dedicated, restricted workstations
- Removal of old administrator accounts

Server farms that host Virtual Desktops (VDI) enable remote users to access shared resources for everyday applications and should be segmented appropriately.

Primary Security Capability

Identity

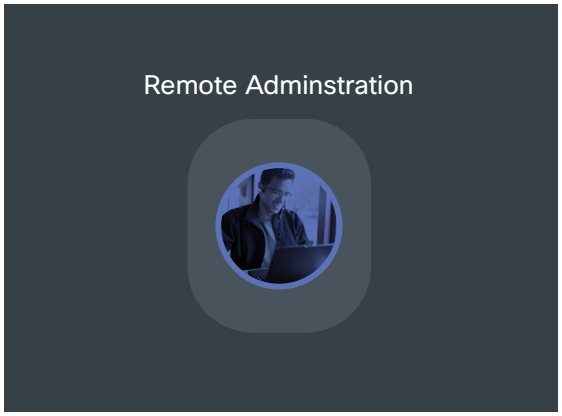


Figure 9 *Business Use Case – Humans*

Return to Contents

Devices

The devices for the data center are tools that administrators use to control and monitor systems that maintain and secure the data center.

Remote administrators connect to centralized management systems using secure connectivity with strong encryption (SSH, TLS, VPN) and multi-factor authentication from a variety of devices.

Control and monitoring systems (e.g., HVAC, power distribution, fire control) provide services to the data center and attach in the services layer.

Administrator systems and autonomous IoT devices connect to the services layer or the adjacent campus network, not in the server farm of the data center. Capabilities provided there must implement posture assessments, patching, and enhanced security controls which should be enforced for these devices. Access policies that must be applied to administrator devices include time of day, geography, and role.

Compromising these systems is a direct threat to the data center (e.g., if you turn off the A/C, you will burn up the servers—a Denial of Service attack).

The capabilities to protect these devices are found in the associated campus network that the data center is deployed within.

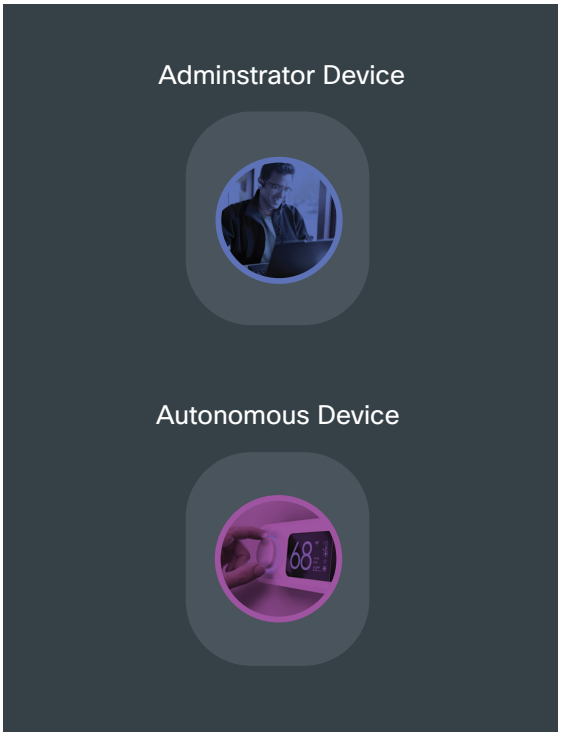


Figure 10 *Data Center Devices*

Network

The access/distribution/core is classic network hierarchy. These layers provide a method which discretely separates services for business-based traffic into flows, and allows scale as services are moved, added, or changed. Application-centric infrastructure enhances policy enforcement through orchestrated, software-defined segmentation across a flat topology. These organizations simplify network troubleshooting and segment traffic for security. Visibility into these flows using flow analytics provides insight to protect against data extraction.

Access Layer

The access layer is where servers are attached to the network. Its purpose is to enforce compliance to policy and prevent unauthorized network access.

Flow analytics provide visibility to network traffic and enable the identification of anomalies. Anomalous behavior and other attacks can then be quarantined appropriately.

This layer connects to the distribution layer.

Distribution Layer

Distribution layers segregate network traffic between the access layer and the core layer.

They provide scalable services to the access layer and endpoints (e.g., firewall, intrusion prevention, load balancing, TLS offload). High-speed access and availability are the primary design considerations.

Primary Security Capability

- Firewall
- Flow Analytics
- Intrusion Prevention
- Anti-Malware
- Tagging
- Threat Intelligence

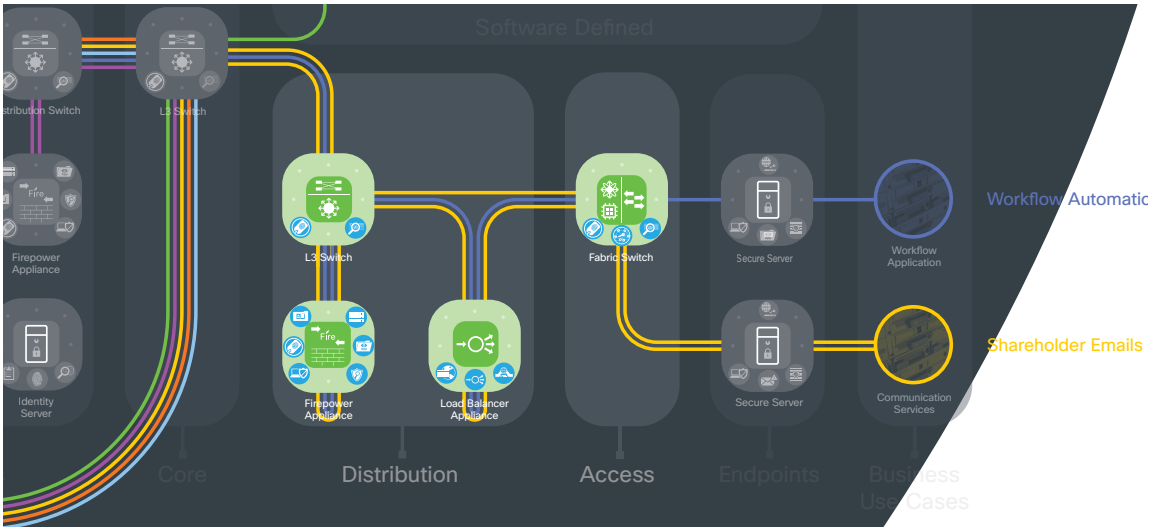


Figure 11 *Distribution and Access Layers*

Return to Contents

Software-defined Layer

The Software-defined Data Center (SDDC) is a layer in the data center with an open, programmable fabric which enables automation, agility, security, and analytics. It integrates virtual and physical workloads in a multi-hypervisor fabric to build a multi-service, hybrid, or cloud data center. The configurable fabric consists of discrete components that operate as compute, storage, networking, security, and availability, but is provisioned and monitored as a single entity. It enhances policy enforcement through orchestrated, software-defined segmentation across a flat topology, enabling better business agility.

Segmentation is implemented by grouping endpoints, and services are applied to traffic between groups using contracts to prevent unauthorized network access.

Leaf and spine layers connect the core to the servers. These provide a distribution method of services that discretely separates business-based traffic into flows based on applications, and allows scale as services are moved, added, or changed.

Primary Security Capability

- Firewall
- Flow Analytics
- Intrusion Prevention
- Tagging
- Anti-Malware
- Threat Intelligence

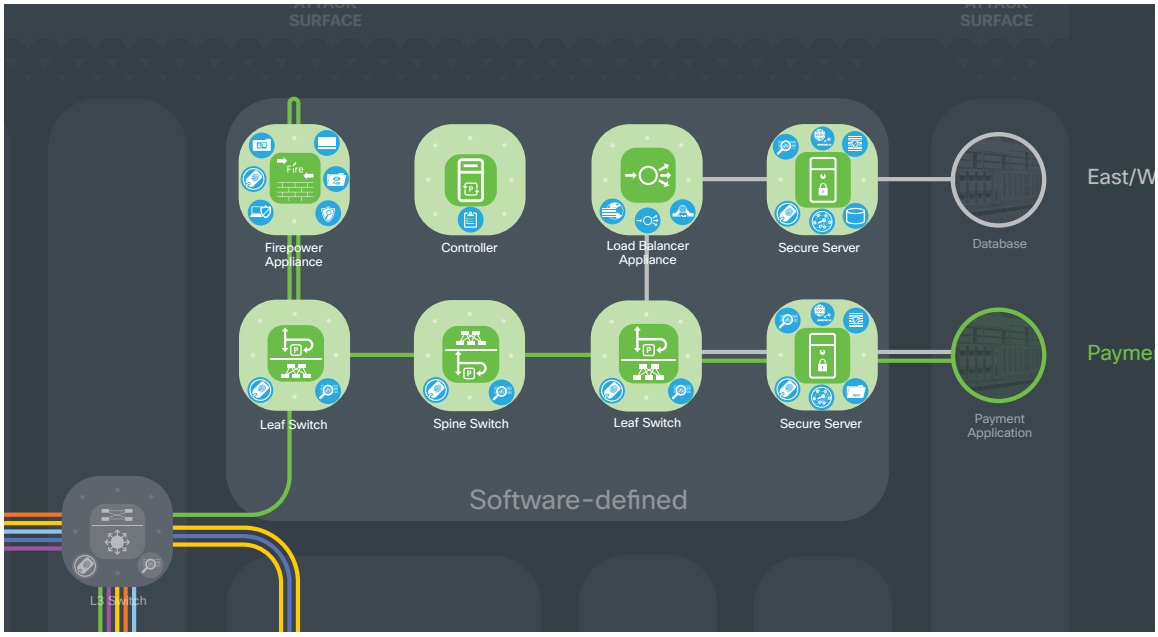


Figure 12 *Application-Centric Infrastructure Leaf and Spine*

Return to Contents

Core Layer

The core network provides high-speed, highly redundant connectivity to route packets between distribution-layer devices and different areas of the network.

The location of deployment varies from small to large companies, where the data center is deployed within a campus or independently of other PINs.

The core layer requires flow analytics for visibility, and tagging for segmentation.

Primary Security Capability

Flow Analytics

Tagging

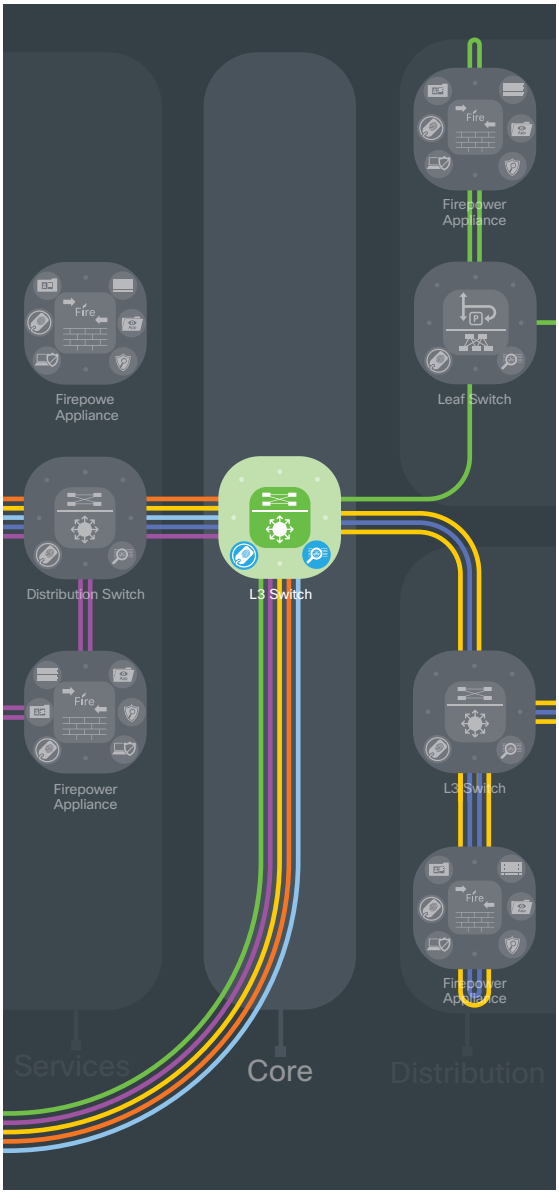


Figure 13 *Core Layer*

Applications

Services Layer

The services layer is a special collapsed distribution and access layer within a data center. It hosts supporting capability services for the data center and other places in the network. A high-security section contains the management, monitoring, and communications infrastructure. Unified wireless controllers, WIPS, and voice systems are also centrally managed for other PIN locations.

Independent management networks and data center devices connect here (e.g., HVAC, security cameras, power control systems).

Primary Security Capability

Foundational Security Services

- Firewall
- IPS
- Threat Intelligence
- Anti-Malware
- Flow Analytics
- Tagging

Business-based Security

- Application Visibility Control
- Malware Sandbox
- TLS Offload
- WAF
- WIPS for Branches
- Wireless Rogue Detection for Branches

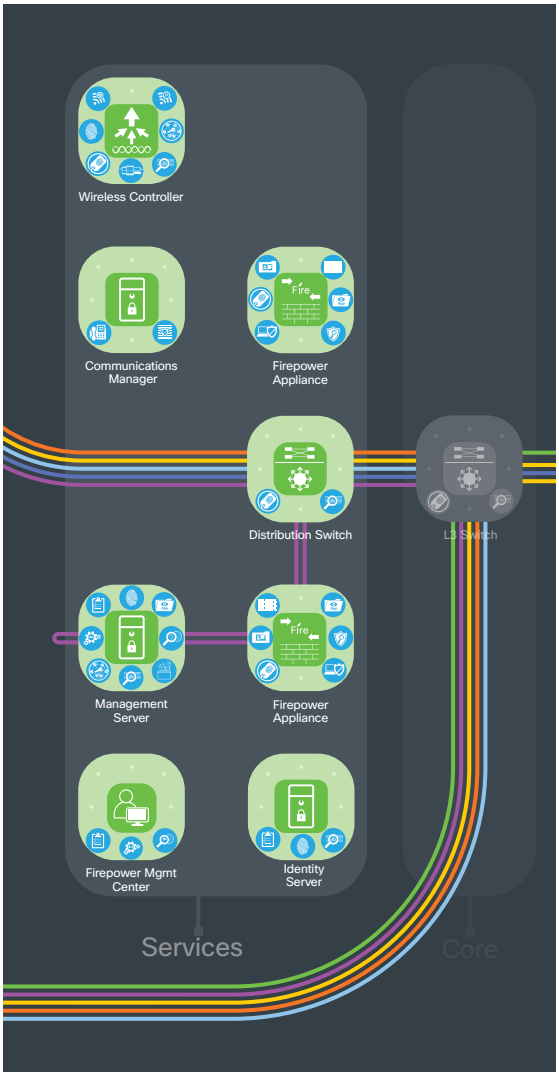


Figure 14 *Services Layer*

Return to Contents

Common Services Layer

The services layer also hosts many common services utilized across the company. Identity management using products like Cisco Identity Services Engine (ISE) is integrated with common identity platforms such as Microsoft Active Directory to better manage identity-based access and control policies. Network devices use protocols such as RADIUS and TACACS to securely authenticate administrators to these services when managing infrastructure.

Time synchronization within a company is a fundamental necessity for security certificate exchange and accurate log/event correlation.

Host and domain name resolution services are often directed to the Internet in branch locations. But in the data center, local servers are deployed for security and speed of replies.

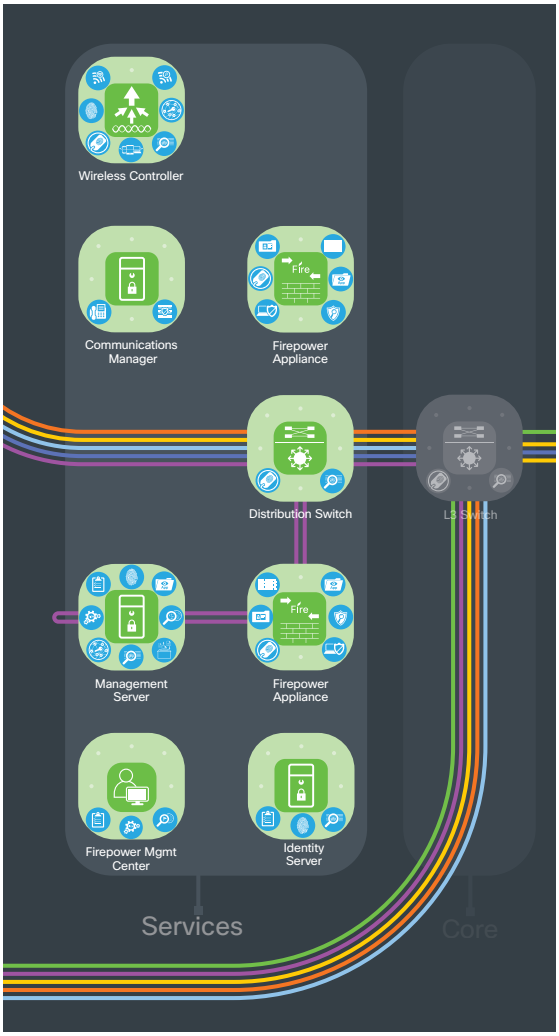


Figure 14 *Services Layer*

Endpoints Layer

Servers are the business flow endpoints in a data center that host web services, applications, and databases. Collectively these clusters or farms provide capabilities beyond a single machine, and often consist of thousands of computers. To ensure reliability they include redundancy with automatic fail-over and rapid re-configuration.

Malware propagation, botnet infestation, and a large attack surface are threats targeting servers.

Server-based security is achieved through deployment of host-based firewalls, anti-malware, and anti-virus products in addition to software sensors which add visibility, enforcement, and package management such as Cisco Tetration.

East/west traffic refers to the communication between servers within an application tier (web, application, database) as seen in Figure 15. This workload traffic pattern can be secured by policies between them which implement application micro-segmentation, behavior baselining/analysis, vulnerability detection, and intrusion prevention, which are tuned to meet the application requirements.

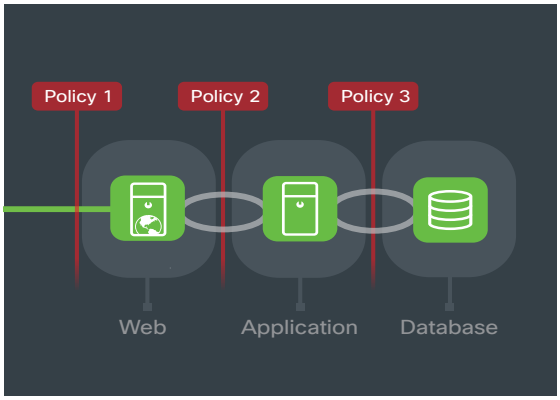
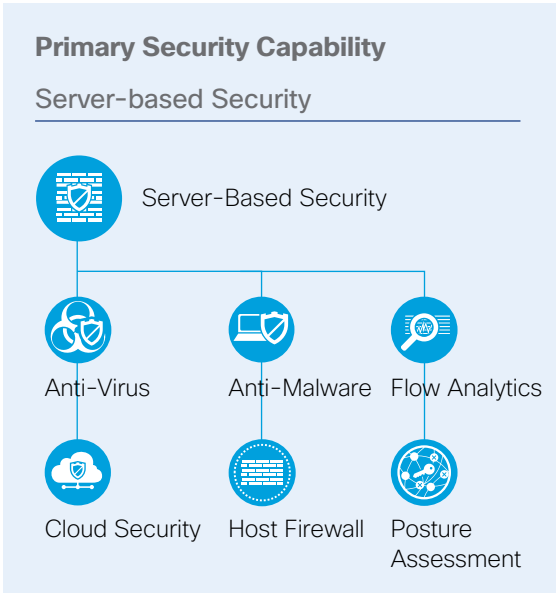


Figure 15 *Data Center Application Tiers*



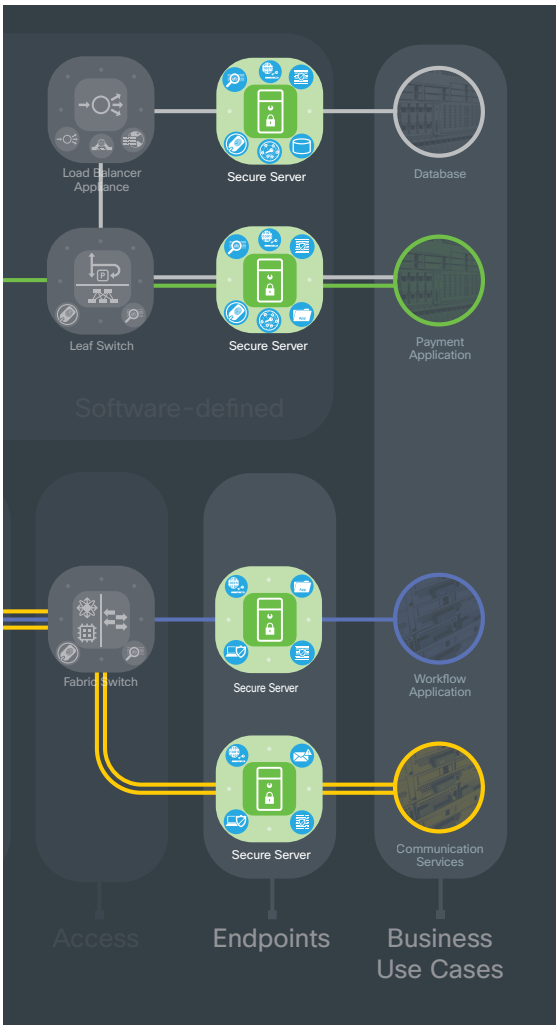


Figure 16 *Data Center Endpoints*

Return to Contents

Multi-site Data Center

The Secure Data Center is complemented by a redundant data center where workloads are distributed. Alternatively, infrastructure can be ready in a warm standby data center or a cold data center where full backups are ready to deploy in the event of a complete failure.

Centralized management and shared services are the most common applications deployed in both, enabling full active/active redundancy. Connectivity between data centers is achieved via the WAN PIN or dedicated fiber connections to the cores when within the same metro area.

As the cost of cloud services decreases, many companies are deploying services in public service provider environments such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform.

Application mobility to this infrastructure, shared services from this infrastructure, and dynamic scaling enable a hybrid data center architecture. Administration and monitoring must be secured using encryption (e.g., Cisco AnyConnect) and Cloud Access Security Broker (CASB) services such as Cisco Cloudlock.

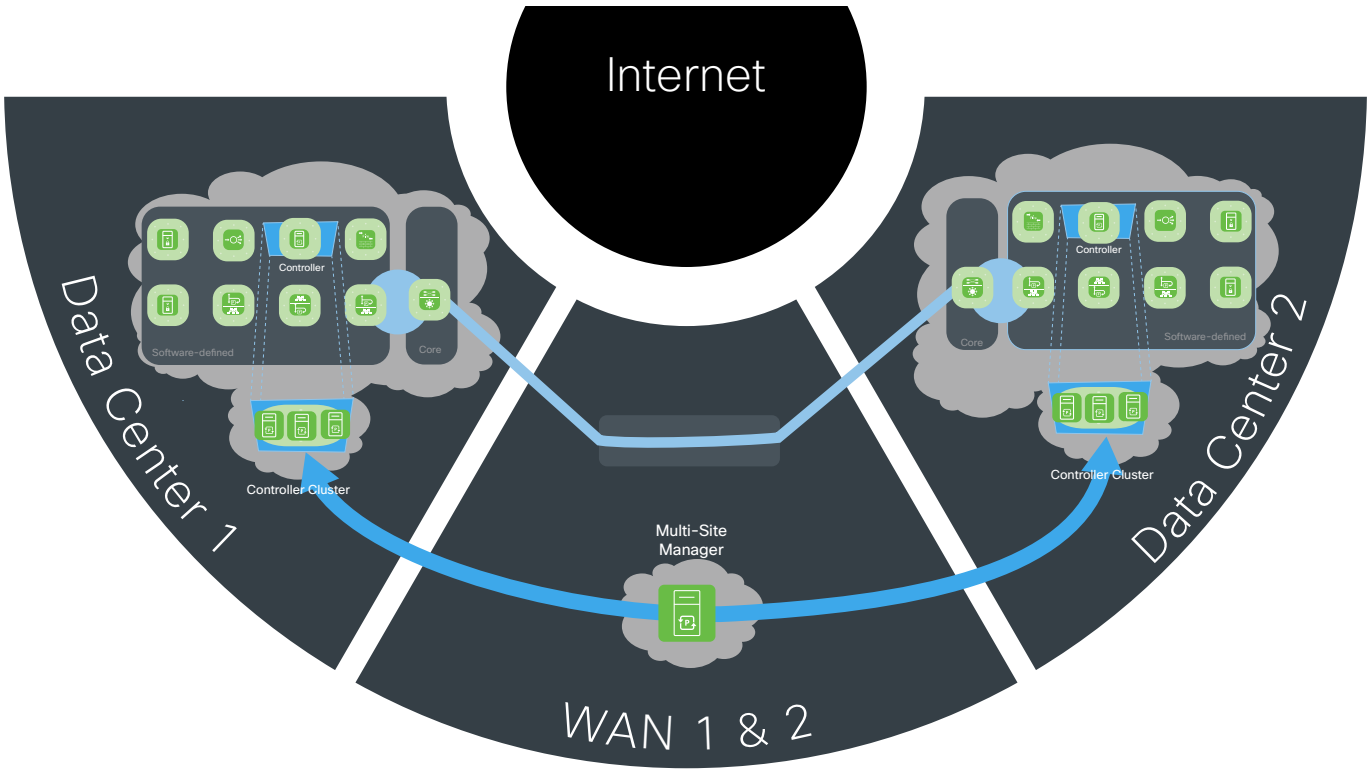


Figure 17 ***Multi-site Data Center.*** *This model shows how multiple data center connectivity is secured across the PINs.*

Return to Contents

Summary

Today's companies are threatened by increasingly sophisticated attacks. Data centers are targeted because they store all of a company's data across increasingly complicated systems.

Cisco's Secure Data Center architecture and solutions defend the business against corresponding threats using an architectural approach that overcomes the limitations of a point product offering.

SAFE is Cisco's security reference architecture that simplifies the security challenges of today and prepares for the threats of tomorrow.

Return to Contents

Appendix

A Proposed Design

The Secure Data Center has been deployed in Cisco's laboratories. Portions of the design have been validated and documentation is available on Cisco Design Zone.

Figures 18 and 19 depict the specific products that were selected within Cisco's laboratories. It is important to note that the Secure Data Center architecture can produce many designs based on performance, redundancy, scale, and other factors. The architecture provides the required logical orientation of security capabilities that must be considered when selecting products to ensure that the documented business flows, threats, and requirements are met.

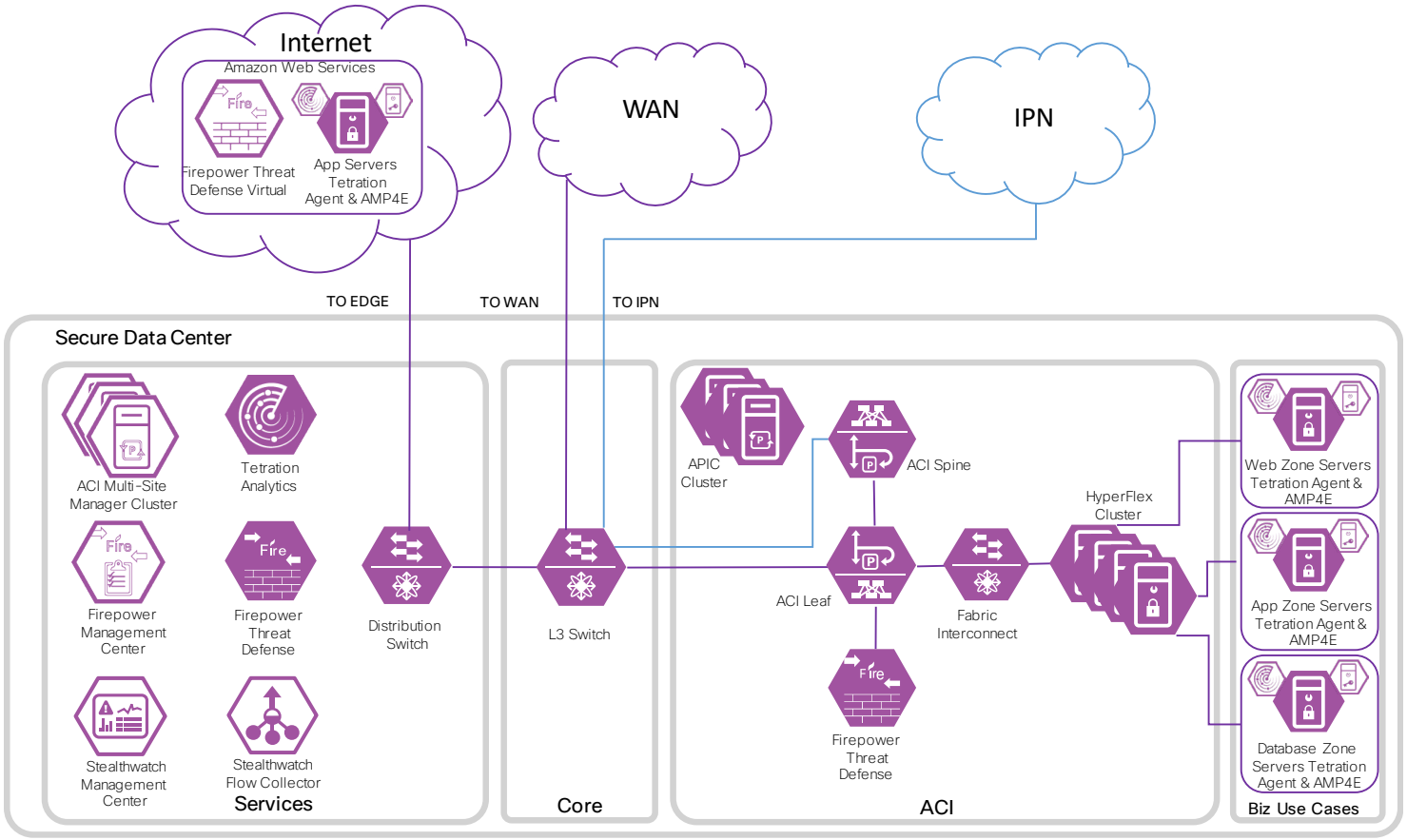


Figure 18 *Secure Data Center Proposed Design, single site*

Return to Contents

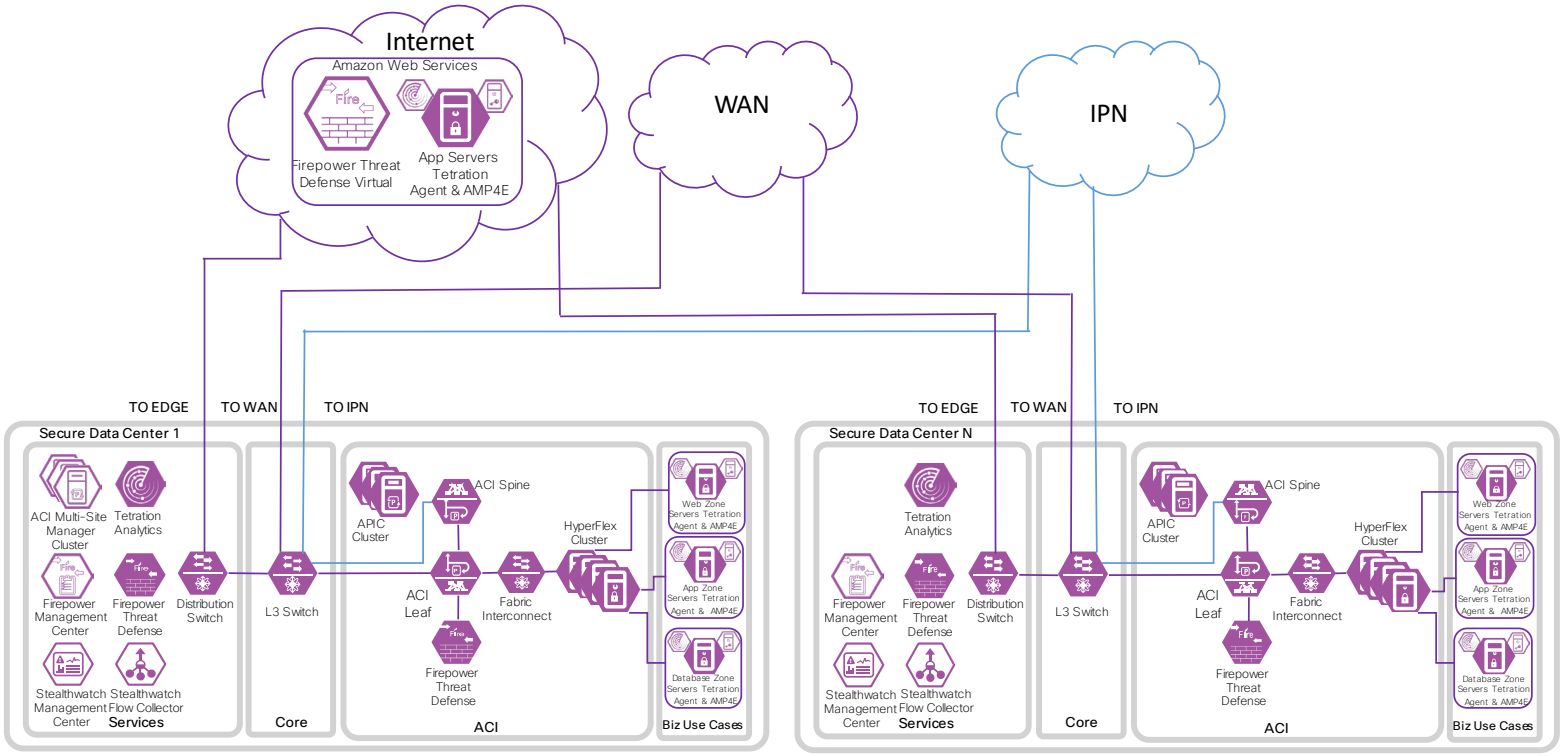


Figure 19 *Secure Data Center Proposed Design, multi-site*

Suggested Components

Table 2 *SAFE Design Components for Secure Data Center*

Campus Attack Surface		Campus Security	Suggested Cisco Components
Human	Users	 Identity	Identity Services Engine Meraki Management
Devices	Endpoints	 Client-Based Security	Advanced Malware Protection (AMP) for Endpoints Cisco Umbrella AnyConnect
		 Posture Assessment	AnyConnect Agent Identity Services Engine (ISE) Meraki Mobile Device Management
Network	Wired Network	 Firewall	Firepower Appliance, Adaptive Security Appliance (ASA)
		 Intrusion Prevention	Firepower Appliance
		 Tagging	Nexus/Catalyst Switch VLANs Centralized Identity Services Engine TrustSec Application Centric Infrastructure (ACI) Endpoint Group (EPG)
	Wireless Network Branch centralized services	 Wireless Rogue Detection	Meraki Wireless Mobility Services Engines (MSE) Wireless APs Wireless LAN Controller
		 Wireless Intrusion Prevention (WIPS)	

Return to Contents

Table 2 *SAFE Design Components for Secure Data Center (continued)*

Campus Attack Surface		Campus Security	Suggested Cisco Components
Network continued	Analysis	 Anti-Malware	Advanced Malware Protection (AMP) for Endpoints Advanced Malware Protection (AMP) for Networks Stealthwatch ThreatGrid
		 Threat Intelligence	Cisco Collective Security Intelligence Talos Security Intelligence ThreatGrid Cognitive Threat Analytics (CTA)
		 Flow Analytics	Cisco Tetration Adaptive Security Appliance Catalyst Switches Nexus Switches Stealthwatch (Flow Sensor and Collectors) Wireless LAN Controller
	Cloud	 Cloud Security	Cisco Umbrella Secure Internet Gateway(SIG) Cisco Cloudlock
		 DNS Security	Cisco Umbrella Secure Internet Gateway (SIG)
		 Cloud-based Firewall	Cisco Umbrella Secure Internet Gateway (SIG)
		 Software-defined Perimeter (SDP/SD-WAN)	AnyConnect Agent Cisco Viptela Meraki MX
		 **Web Security:** Internet access integrity and protections.	Firepower URL Filtering Cisco Umbrella Secure Internet Gateway (SIG)
		 **Web Reputation/ Filtering:** Tracking against URL-based threats.	Cloud Web Security Firepower Threat Defense Meraki MX Web Security Appliance
		 Cloud Access Security Broker (CASB)	Cloudlock
Applications	Service	 Server-based Security	Advanced Malware Protection (AMP) for Endpoints Cisco Tetration Cisco Umbrella

Return to Contents

For more information on SAFE, see www.cisco.com/go/SAFE.

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**