

SAFE Architecture Guide

Places in the Network: Secure Edge

January 2023

Contents

Overview	3
Business Flows	4
Functional Controls	5
Capability Groups	6
Threats	7
Security Capabilities	8
Human Attack Surface	9
Network Attack Surface - Wired Network	9
Network Attack Surface - Analysis	10
Network Attack Surface - WAN	11
Network Attack Surface - Cloud	12
Applications Attack Surface - Applications	12
Applications Attack Surface - Servers	13
Management	14
Architecture	15
Secure Edge	16
Attack Surface	17
Untrusted Layer	17
Perimeter Services Layer	19
Demilitarized Layer	22
VPN Layer	23
Trusted Layer	25
Summary	26
Appendix	26
Appendix A - A Proposed Design	26
Appendix B - Suggested Components	28
Appendix C - Feedback	30

Overview

The Secure Edge is a place in the network (PIN) where a company connects to the public Internet, service providers, partners, and customers. As internal company users reach out to websites, use email and other collaboration tools, and as remote workers and customers reach in, the services of the network must remain both accessible and secure.

The Secure Edge is one of the seven 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 Edge architecture guide provides:

- Business flows typical for cloud edge and data center edge locations
- Edge threats and security capabilities
- Business flow security architecture
- Design examples and a parts list

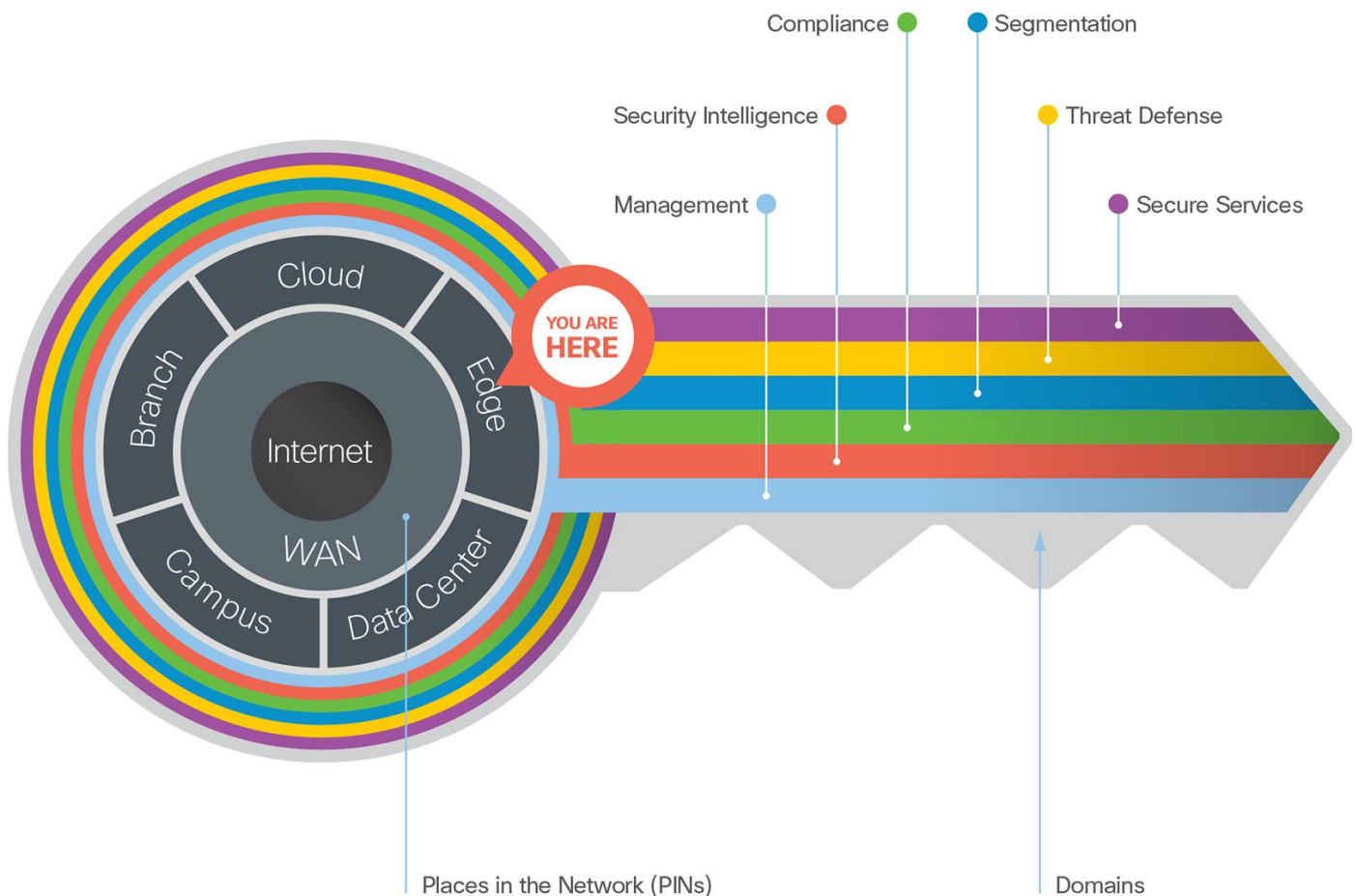


Figure 1. SAFE provides the Key to simplify cybersecurity into Secure Places in the Network (PINs) for infrastructure and Secure Domains for operational guidance.

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.

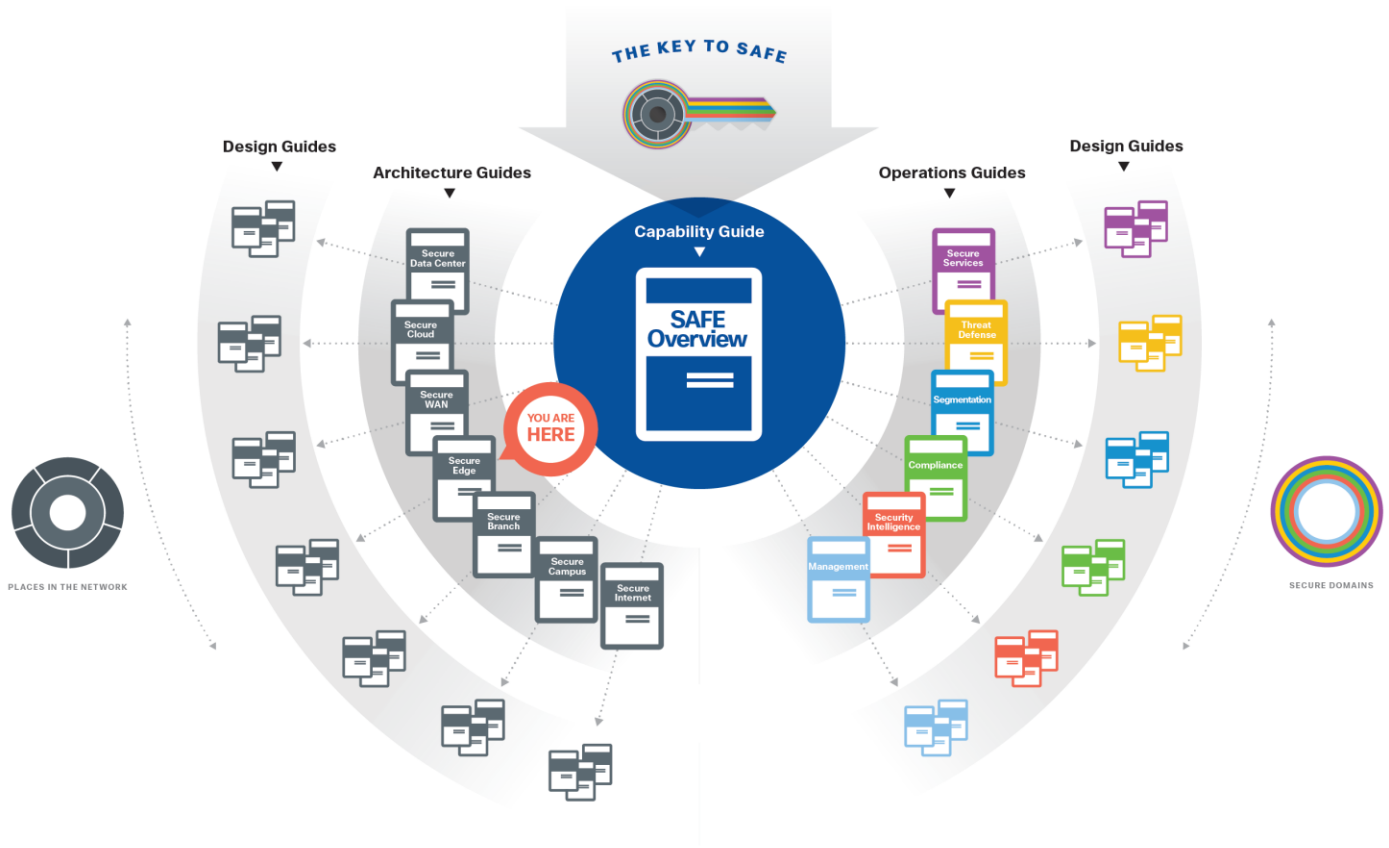


Figure 2. SAFE Guidance Hierarchy

Business Flows

The Secure Edge does not have local users; it is the main security choke point between the internal company and external users.

- Internally, employees located in campus or branch locations require access to external application services (voice, video, email) and the Internet.
- Third parties, such as service providers and partners, require remote access to applications and devices.
- Customers access portals to their personal or financial information.



Figure 3. Edge business use cases are color coded to define where they flow

Functional Controls

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

Functional Control	Definition
Secure Applications	Applications require sufficient security controls for protection.
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.
Secure Web Access	Web access controls enforce usage policy and help prevent network infection.



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

Capability Groups

Edge security is simplified using foundational, access and business capability groups. Each flow requires the foundational group. Additional business activity risks require appropriate controls as shown in figure 5.

User and Device capabilities are located where the flow originates within the Campus, Branch or external locations (Non-Edge Capabilities).

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



Figure 5. The Secure Edge Business Flow Capability Diagram

Secure Edge threats and capabilities are defined in the following sections.

Threats

The Edge connects the internal company to the external world and all its associated dangers. Employees, partner and customer users use a combination of services such as email, browse the web, and collaborate. The attack surface is particularly dangerous as most threats originate or coordinate services exposed from the Internet.

The Secure Edge has four primary threats.

Web server vulnerabilities

Web servers with poorly coded applications are susceptible to threats such as SQL Injections, Cross Site Scripting (XSS) and Request Forgery. These allow an attacker to read, alter, or delete data. Compromised

servers enable attackers to execute scripts in the victim's browser which can hijack user sessions, deface websites, or redirect the user to other malicious sites.

Distributed denial of service (DDoS)

An attack utilizing multiple sources of traffic which overwhelms the capabilities of a system. These connections overload systems and stop all normal operation.

Data loss

The Data Center or Cloud Edge is a choke point for traffic exiting the company. Data theft via email and compromised web sessions occurs commonly through these flows.

Man-in-the-Middle (MitM)

An attacker inserts themselves in to the communications between the company and their partners or customers. Compromised email, web proxies, or DNS name services enable traffic interception and redirection with out the knowledge of the parties.



Security Capabilities

The attack surface of the Edge is defined by the business flow, which includes the people and the technology present. The security capabilities that are needed to respond to the threats are mapped in Figure 6. The placement of these capabilities are discussed in the architecture section.

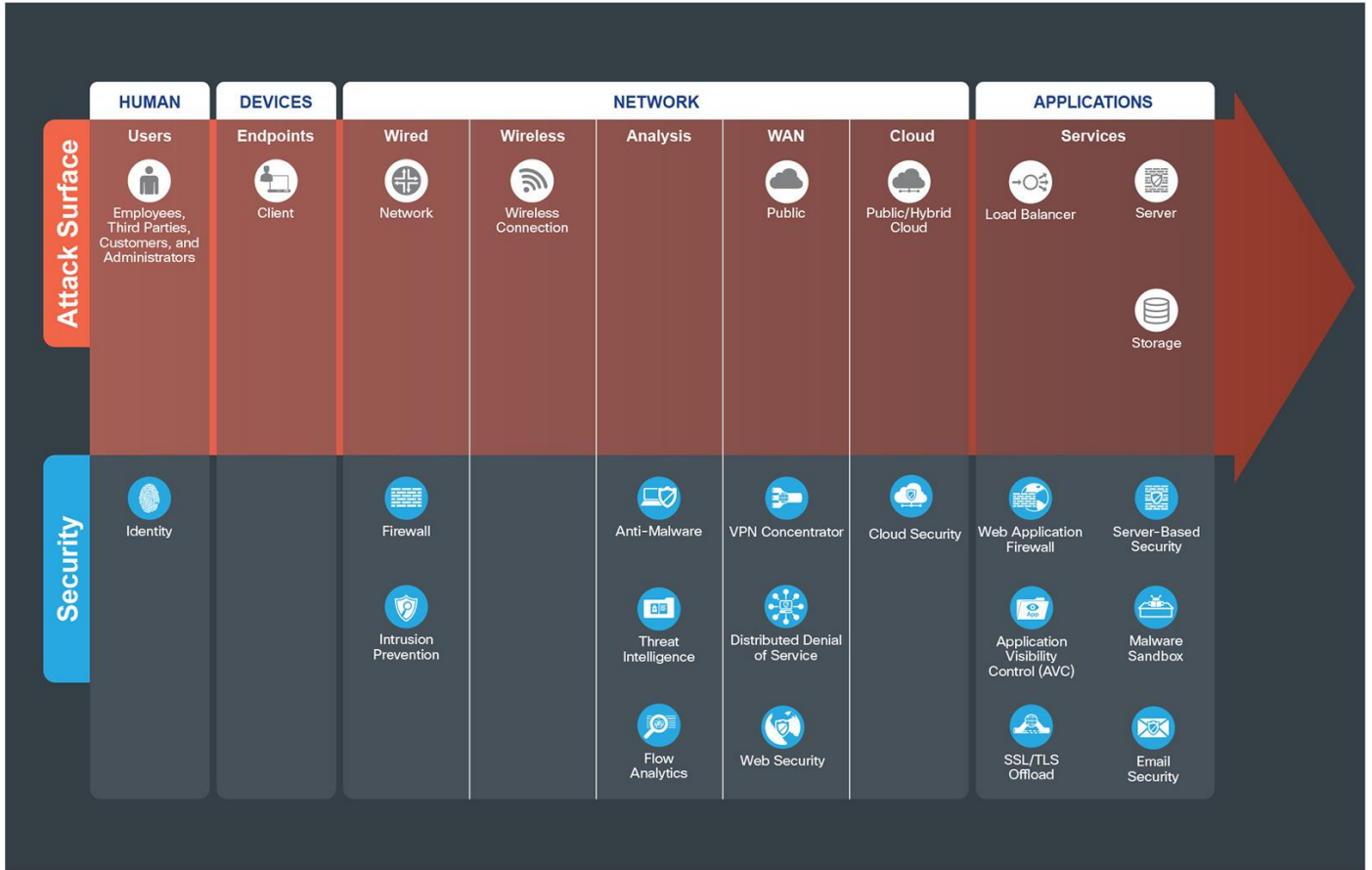


Figure 6. Secure Edger Attack Surface and Security Capabilities

The suggested products that implement these capabilities can be found in Appendix B.

Human Attack Surface









Users: Remote employees, third parties, customers and administrators.

Security Capability		Threat	
	Identity: Identity-based access.		Attackers or disgruntled admins accessing restricted information resources.

Network Attack Surface - Wired Network









Wired Network: Physical network infrastructure; routers, switches, used to connect access, distribution, core, and services layers together.

Security Capability		Threat	
	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 Endpoint Groups (EPGs)/TrustSec/VLANs.		Unauthorized access and malicious traffic between segments.

Network Attack Surface - Analysis











Analysis: Analysis of network traffic within the edge layers.

Security Capability		Threat	
	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.

Network Attack Surface - WAN



Security Capability		Threat	
	Virtual Private Network (VPN) or SD-WAN: Encrypted communication tunnels.		Easily collecting information and identities.
	VPN Gateway or Concentrator: Encrypted remote access.		Exposed services and data theft.
	DDoS Protection: Protection against scaled attack forms.		Massively scaled attacks that overwhelm services.
	Web Security: Web, DNS, and IP-layer security and control for the branch.		Attacks from malware, viruses, and redirection to malicious URLs.

Network Attack Surface - Cloud



Security Capability		Threat	
	Cloud Security: Web, DNS, and IP-layer security and control in the cloud for the campus.		Attacks from malware, viruses, and redirection to malicious URLs
	DNS Security		Redirection of user to malicious website.
	Cloud-based Firewall		Unauthorized access and malformed packets connecting to services.
	Software-Defined Perimeter (SDP/SD-WAN)		Easily collecting information and identities.
	Web Security		Infiltration and exfiltration via HTTP.
	Web Reputation/Filtering: Tracking against URL-based threats.		Attacks directing to a malicious URL.
	Cloud Access Security Broker (CASB)		Unauthorized access and data loss.

Applications Attack Surface - Applications








Applications: Servers, database, load balancer.

Security Capability		Threat	
	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 Firewall: Advanced application inspection and monitoring.		Attacks against poorly developed applications and website vulnerabilities.
	Email Security: Messaging integrity and protections		Infiltration or exfiltration attacks via email.

Applications Attack Surface - Servers



Security Capability		Threat	
	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.

Security Capability		Threat	
	Cloud Security: Security services from the cloud		Redirection of session to malicious website.
	Host-based Firewall: Provides micro-segmentation and policy enforcement.		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: Encryption of data at rest.		Theft of unencrypted data.
	Flow Analytics: Network traffic metadata identifying security incidents.		Traffic, telemetry, and data exfiltration from successful attacks.
	Application Dependency Mapping:		Exploiting a misconfigured firewall policy.
	Vulnerability Assessment and Software Inventory:		Exploiting unpatched or outdated applications.
	Process Anomaly Detection & Forensics:		Exploiting privileged access to run shell code.
	Tagging: Grouping for Software Defined Policy		Unauthorized access and malicious traffic between segments.
	Policy Generation, Audit, and Change Management:		Targeted attacks taking advantage of known vulnerabilities.

Management



Management, Control, and Monitoring.

Security Capability		Threat	
	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.		Unauthorized access to system-stored data.

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 Edge architecture is a logical grouping of security and network technology that supports the Data Center Edge and Cloud Edge business use cases.

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.

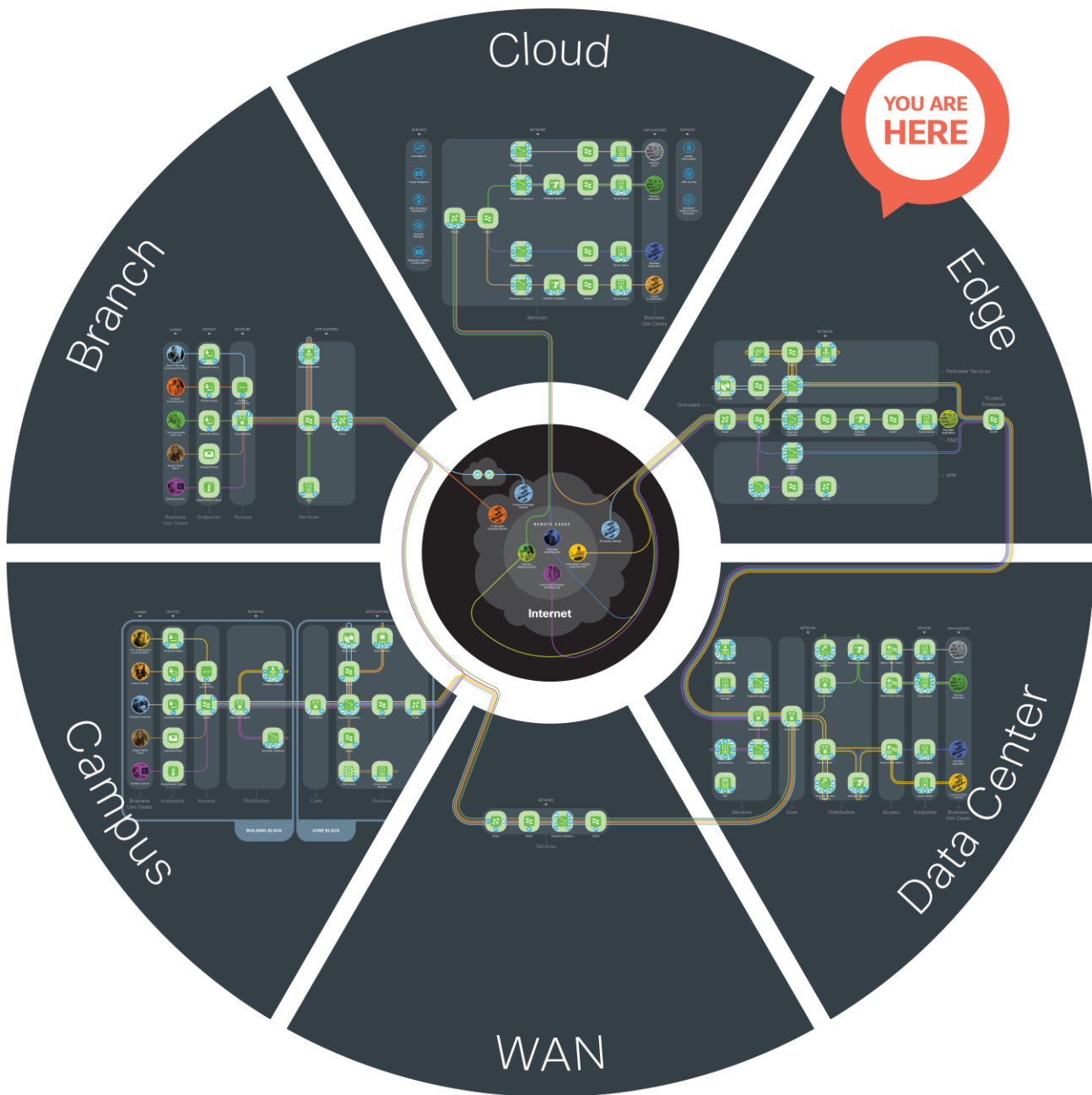


Figure 7. SAFE Model. The SAFE Model simplifies complexity across a business by using Places in the Network (PINs) that it must secure.

Secure Edge

The Secure Edge architecture is logically arranged into five layers to provide a company with several lines of defense from the threats that exist in public networks. It connects the dangers of the untrusted Internet to the trusted internal company; certain cautionary layers are used to protect public-facing services without exposing the internal company directly. Each of these layers supports the different business functions and security control points. They are separated because of the need for layered defense that provides more security in the event of

one compromise point, scalability concerns when one layer needs growth or change, and tailored security controls. These could be consolidated into fewer systems initially that can be increased as the needs grow.

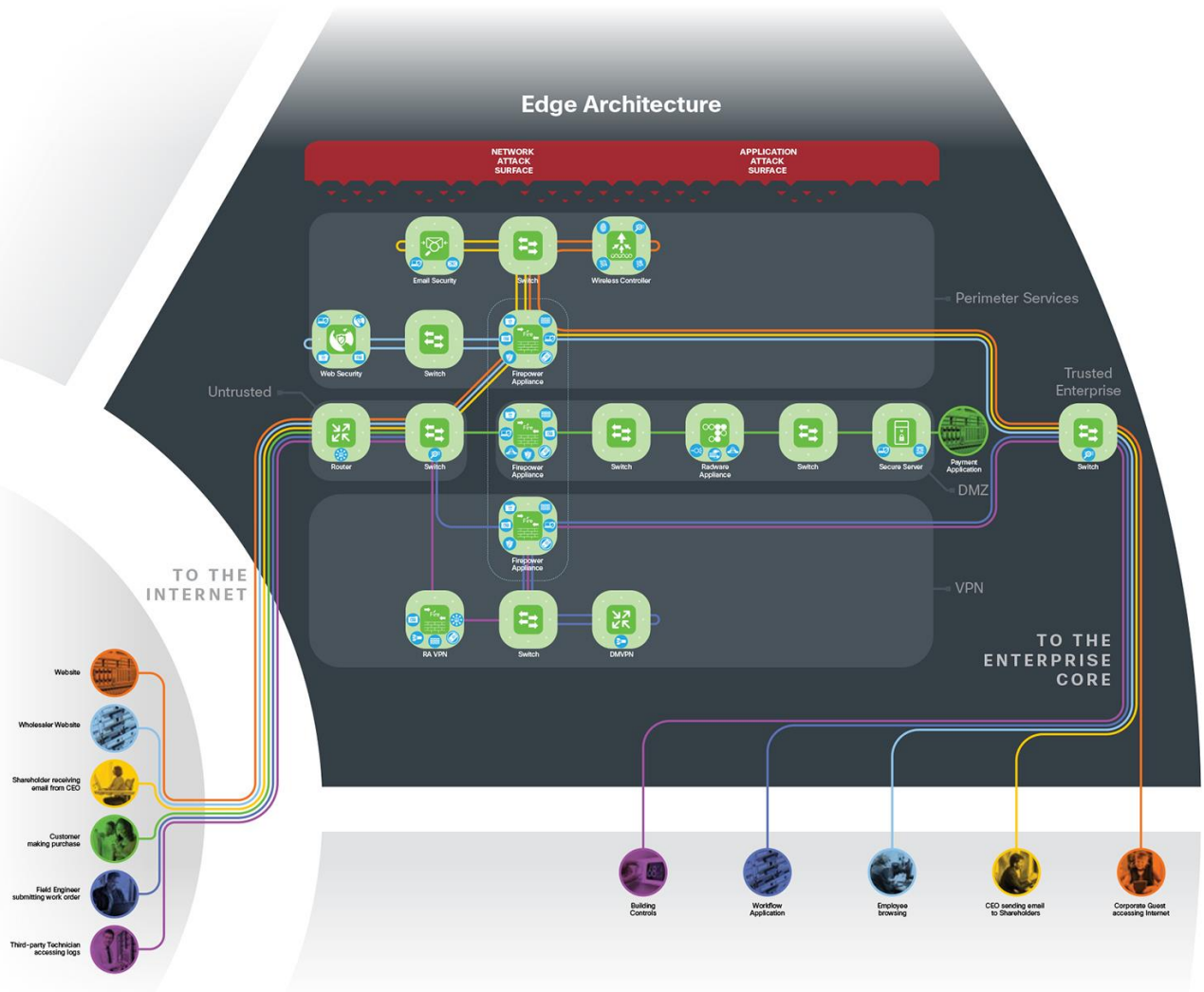


Figure 8. Secure Edge Architecture. The Secure Edge business flows and security capabilities are arranged into a logical architecture. The colored business use cases flow through the green architecture icons with the required blue security capabilities.

Attack Surface

The Secure Edge attack surface consists of Network and Applications. The sections below discuss the security capability that defends the threats associated with each layer of the surface. Note that the capability might be a service that is supplied from another PIN. For example, the Identity service is prompted to a human, on a user’s device, enforced at the switch, and served from the Data Center. However, for the sake of simplifying, Identity is depicted logically where the risk exists.

Untrusted Layer

The untrusted layer connects the Internet, partners, service providers, and customers directly to the company. It connects service providers using routers that demark where the public domain ends and the internal company begins. All public traffic can access these edge routers, making this layer susceptible to threats such as

volume-based denial of service attacks (DDoS). Switching infrastructure connects the untrusted layer to the perimeter services, DMZ, and VPN layers, providing visibility into the traffic using analytics.

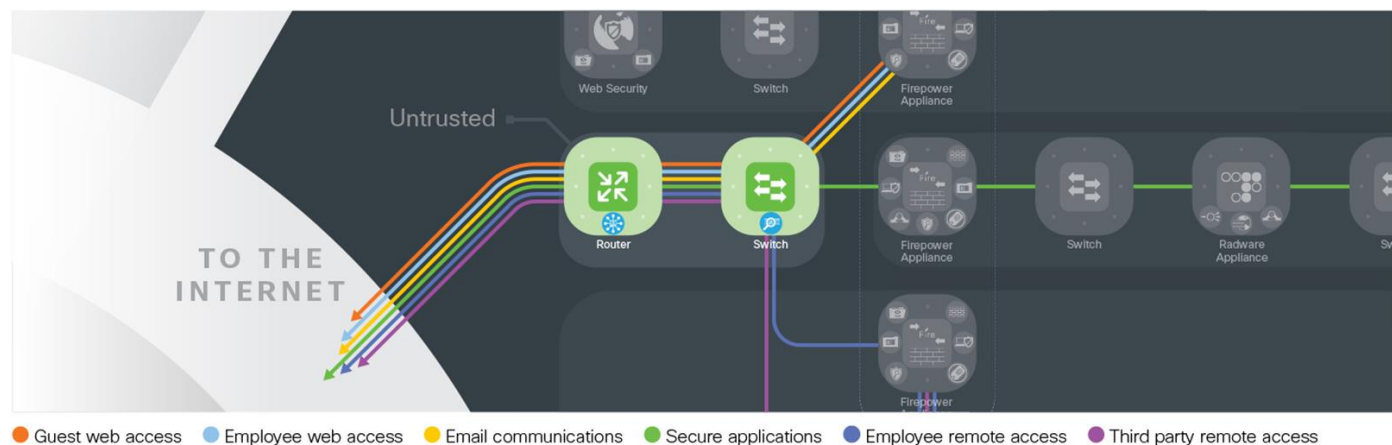





Figure 9. Untrusted Layer

Business Flows/Functional Controls	Primary Security Capability
<ul style="list-style-type: none"> Secure email Secure outbound web access Corporate employee remote access Guest wireless access External corporate VPN Hosted applications 	<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;">  <p>DDoS</p> </div> <div style="text-align: center;">  <p>Filtering- Router ACLs</p> </div> <div style="text-align: center;">  <p>Flow Analytics</p> </div> </div>

Design Considerations for the Untrusted Layer

- Implement out-of-band management for all systems in the edge using dedicated management interfaces and Virtual Route Forwarding (VRF) or console access for high-security implementations
- Segment the untrusted layer from all other edge layers by implementing separate physical switches which are used to connect each of the layers for common egress
- Implement edge DDoS capabilities in conjunction with service provider DDoS services for offloading volumetric attacks

Edge Routers

- Contains the edge routing capability and forms the first layer of defense for the Edge
- Implement authenticated routing protocols
- Use physical versus virtual segmentation
- Implement infrastructure access control list filtering for all inbound and outbound packets allowing only public addresses

- Block spoofed packet flows with Unicast Reverse Path Forwarding (RPF)

BGP Considerations

- Use Border Gateway Protocol (BGP) with authentication as the routing protocol for all dynamic routing—both between the border routers and between the border routers and the service provider or partner
- Have an independent autonomous system number. This will give the flexibility of advertising your Internet prefix to different service providers and partners, optimizing communications
- BGP TTL security check – The BGP support for the time-to-live (TTL) security check feature introduces a lightweight security mechanism to protect eBGP peering sessions from CPU utilization-based attacks. These types of attacks are typically brute-force DoS attacks that attempt to disable the network by flooding the network with IP packets that contain forged source and destination IP addresses

Perimeter Services Layer

The perimeter services layer segments the connections of the other layers and has all of the core security and inspection capabilities necessary to protect. Man in the Middle attacks and data loss via exfiltration are mitigated at the perimeter.

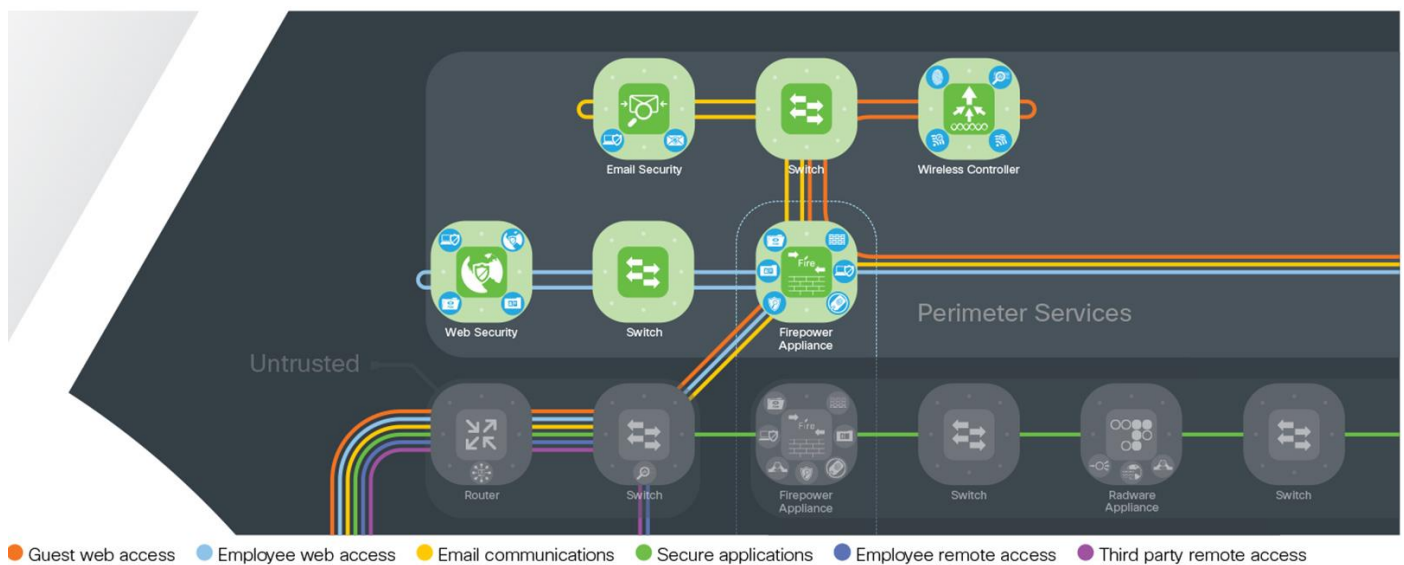


Figure 10. Perimeter Services Layer

Design Considerations for the Perimeter Services Layer

The perimeter services layer contains the wired, email, web, and wireless security platforms.

Wired Security

The perimeter security is enforced by next-generation firewalling and intrusion prevention.

The corporate access policies are enforced by edge firewalls in this layer. Multiple appliances should be used to provide redundancy and implemented in active/standby mode. This simplifies inspection capabilities and ensures that no traffic loss occurs in the event of a failover.

Business Flows

- Secure email
- Guest wireless access
- Secure outbound web access

Primary Security Capability



Firewall



IPS



Anti-
Malware



Threat
Intelligence



Flow
Analytics

Key objectives of firewall requirements:

- All users and guests must be able to access the Internet
- All HTTP/HTTPS traffic must pass through web security
- Allow only authorized DNS queries
- Only web, email, and some Internet Control Message Protocol (ICMP) traffic are allowed into the network
- Firewalls should be hardened and configured for redundancy
- Secure device access by limiting accessible ports, authentication for access, specifying policy for permitted action for different groups of people, and proper logging of events
- Disable Telnet and HTTP; allow only secure shell (SSH) and HTTPS
- Secure firewall routing protocols by implementing Message Digest 5 (MD5) authentication

Email Security

Email is a critical communication service used by corporate business people including the CEO, which makes it an attractive target for hackers. The two major threats to email systems are spam and malicious email.

Primary Security Capability



Email Security



Anti-Malware

If spam is not properly filtered, its sheer volume can consume valuable resources such as bandwidth and storage, and require network users to waste time manually filtering messages. Legitimate messages may be discarded, potentially disrupting business operations. Failing to protect an email service against spam and malicious attacks can result in a loss of data and network user productivity.

Logically, the email security appliance acts as a Mail Transfer Agent (MTA) within the email delivery chain. There are multiple deployment approaches for the security appliance depending on the number of interfaces used. The best practice is for the email security appliance to be deployed with a single physical interface to transfer emails to and from both the Internet and the internal mail servers. The edge firewalls should be configured to allow incoming mail from the Internet, and outgoing mail from specific servers in the company.

Other recommendations and best practices for email security deployment:

- A static address must be defined on the firewall to translate a publicly accessible IP address for the email server to a private IP address used by the email security appliance
- The email security appliance should be configured to access a DNS in the outside network, rather than the internal DNS. This means that the firewall must allow it to perform DNS queries and receive DNS replies
- The email security appliance downloads the latest threat intelligence information through HTTP/HTTPS connections. Firewall rules must allow HTTP/HTTPS traffic from the email security appliance
- SMTP routes must be set to point to inside email servers
- Either the same interface or a separate interface can be used for incoming or outgoing mail. If the same interface is used, mail must be relayed on the interface
- Use a separate interface to connect to the management network

Web Security

Web access is a requirement for the day-to-day functions of most organizations. Companies must maintain appropriate web access while minimizing the impact of unacceptable or risky use.

Primary Security Capability



Cloud Web
Security



Web Security
Appliance

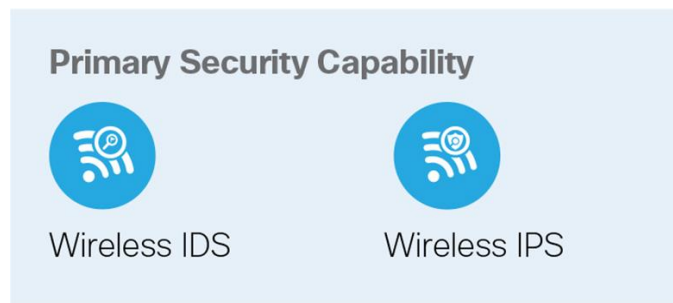
Implement policy-based web access to help users work effectively, and to ensure that personal web activity does not waste bandwidth, affect productivity, or expose the organization to undue risk, such as very broad threats of viruses and Trojans. The web security appliance is logically placed in the path between corporate web users and the Internet. In effect, it acts as a web proxy for the corporate users residing inside the network.

Other recommendations and best practices for web security deployment:

- Specify policies for handling HTTPS traffic
- Configure the policies and actions to be taken for the different ranges in the web reputation score based on the reputation score, pass, monitor, or dropped web traffic
- The edge firewalls should be configured to allow only outgoing HTTP or Hypertext Transfer Protocol over SSL (HTTPS) connections sourced from the web security appliance to prevent users from bypassing it in order to directly connect to the Internet
- Use separate interfaces for management
- Disable unnecessary services (such as Telnet, HTTP) to prevent users from taking advantage of open ports

Wireless Network

The wireless controller terminates guest wireless communications.



Demilitarized Layer

The demilitarized zone (DMZ) is a restricted layer containing both internal and public-facing services. The DMZ has the all of the core security and inspection capabilities necessary to protect the enterprise.

DMZ threats like Web server vulnerability attacks are protected by the following architectural guidance.

Design Considerations for the Demilitarized Layer

Wired Security

The perimeter security is enforced by firewalling and intrusion prevention.

Corporate access policies are enforced by edge firewalls in this layer. Multiple appliances should be used to provide redundancy and should be implemented in active/standby mode. This simplifies inspection capabilities and ensures that no traffic loss occurs in the event of a failover.

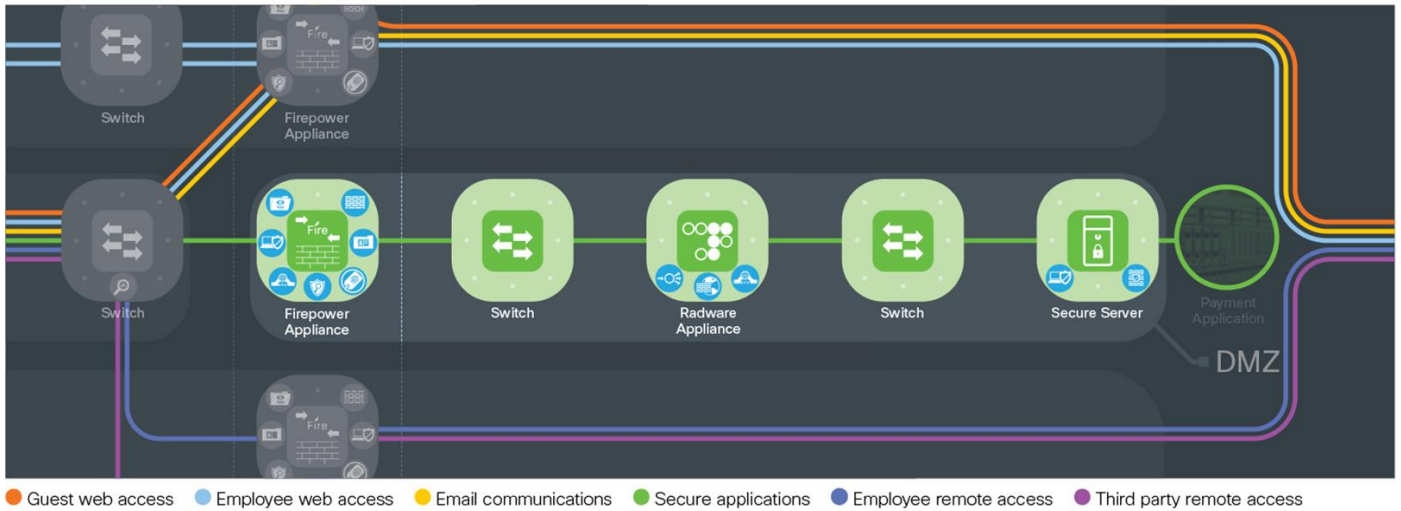
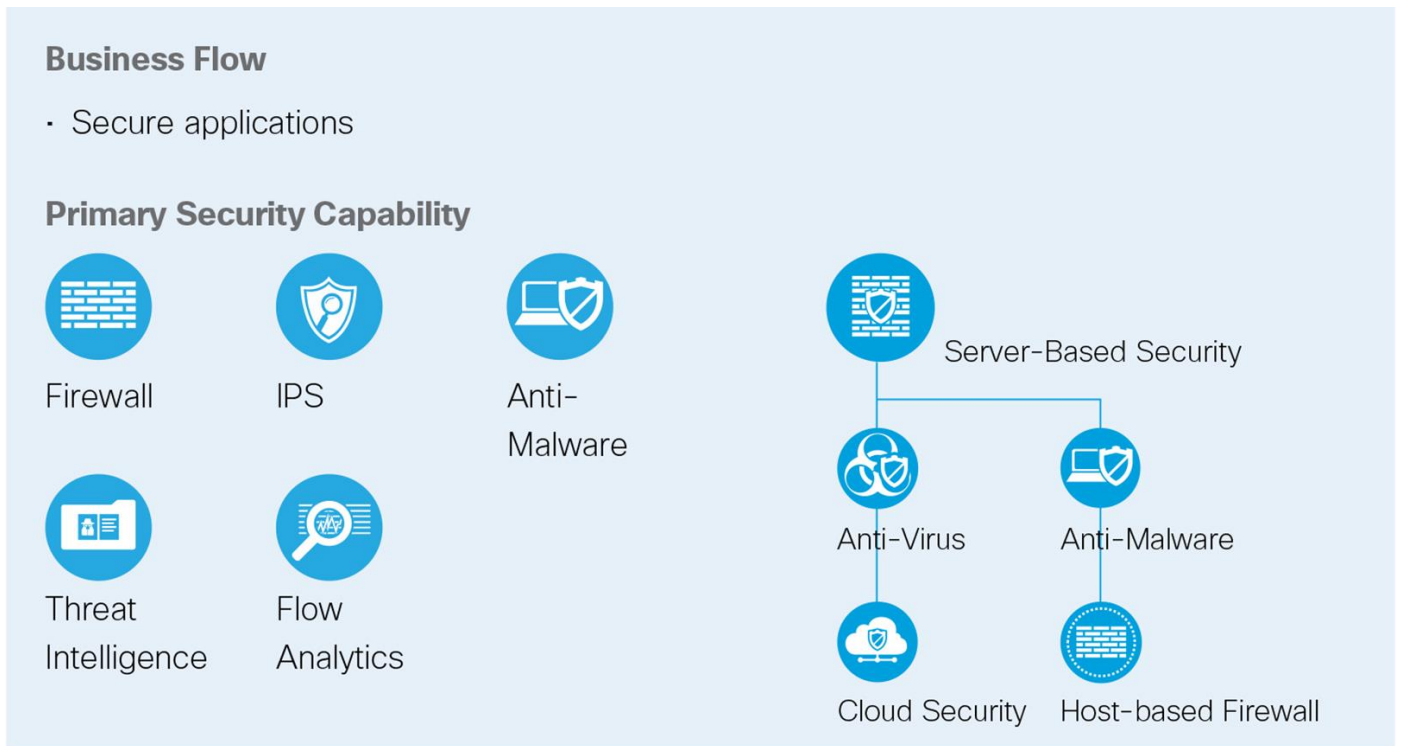


Figure 11. Demilitarized Layer



VPN Layer

The Virtual Private Network (VPN) layer connects to the remote places and people who are using untrusted public connections, and requires encryption technology to secure it.

There are two types of VPN connections: site-to-site and remote access.

The VPN layer has the all of the core security and inspection capabilities necessary to protect the company.

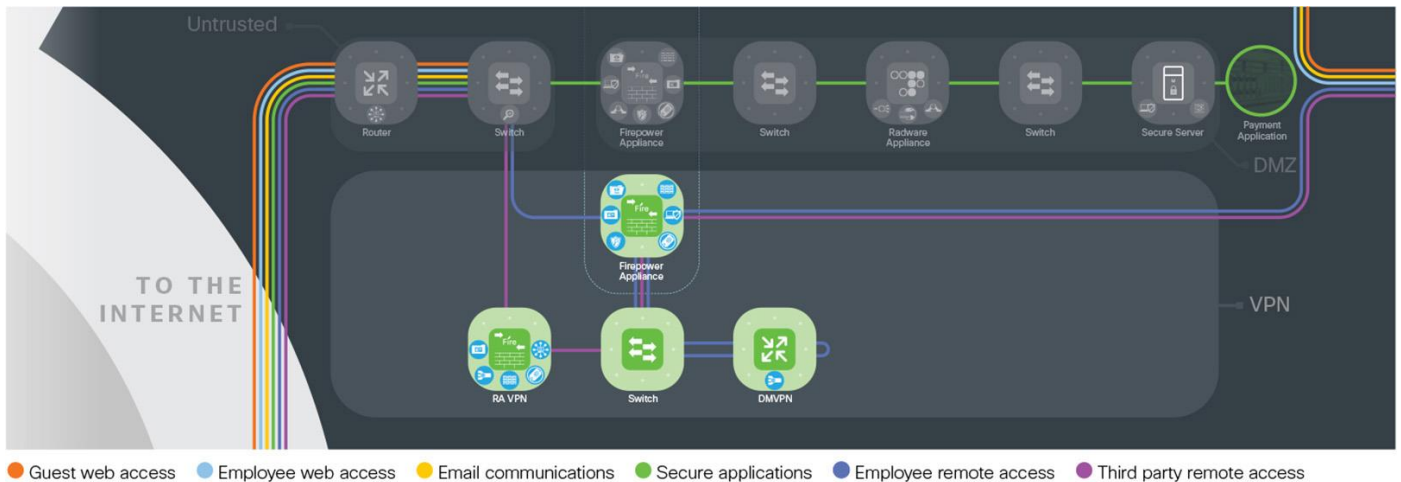


Figure 12. VPN Layer

Business Flows





- Corporate employee remote access
- External corporate VPN

Design Considerations for the VPN Layer

Wired Security

The perimeter security is enforced by firewalling and intrusion prevention.

Primary Security Capability

 Firewall	 IPS	 Anti-Malware
 Threat Intelligence	 Flow Analytics	

The corporate access policies are enforced by edge firewalls in this layer. Multiple appliances should be used to provide redundancy and should be implemented in active/standby mode. This simplifies inspection capabilities and ensures that no traffic loss occurs in the event of a failover.

Site-to-Site VPN

Site-to-site VPN secures connections between the edge and other company PINs, employee home offices, and third-party partners.

Primary Security Capability



DMVPN Router

Remote Access VPN

The remote access virtual private network (RA VPN) layer implements dedicated resources to connect remote users. Employees, contractors, and partners often need to access the network when traveling or working from home or other off-site locations. Many organizations therefore need to provide users in remote locations with network connectivity to data resources.

Primary Security Capability



VPN Concentrator

Secure connectivity to the Edge requires:

- Support for a wide variety of endpoint devices
- Seamless access to networked data resources
- Authentication and policy control that integrates with the authentication resources used by the organization
- Cryptographic security to prevent sensitive data from exposure to unauthorized parties who accidentally or intentionally intercept the data

Trusted Layer

The trusted layer connects the edge to the rest of the internal company network. Typically, this is the data center core that contains core services needed to securely implement, manage, monitor, and operate the Edge.

Design Considerations for the Trusted Layer

Infrastructure protection plays an important role in the Edge trusted layer. These best practices are recommended:

- All infrastructure protection hardening, such as management access control lists (ACL), authentication, control plane policing, or Layer-2 hardening, must be implemented on the inner switches
- Routing protocols between switches and Cisco Firepower and core routers must be authenticated

- Implement NetFlow generation, or attach flow generators to span ports to collect detailed traffic telemetry

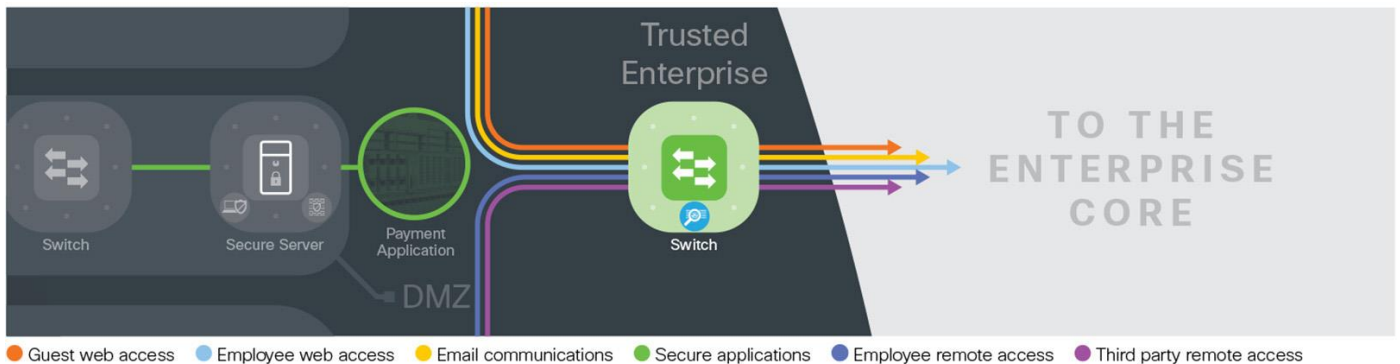



Figure 13. Trusted Layer

Business Flows	Primary Security Capability
<ul style="list-style-type: none"> • Secure email • Secure outbound web access • Corporate employee remote access • Guest wireless access • External corporate VPN 	 <p>Flow Analytics</p>

Summary

Today’s networks extend to wherever employees are, wherever data is, and wherever data can be accessed. The Edge is often the first point of attack and is subsequently the first line of defense.

As a result, technologies must be applied that focus on detecting, understanding, and stopping threats. Attacks can render a company inaccessible from the Internet and prevent employees from being productive.

Cisco’s Secure Edge architecture and solutions defend the business against corresponding threats.

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

Appendix

Appendix A - A Proposed Design

The Secure Edge has been deployed in Cisco’s laboratories. Portions of the design have been validated and documentation is available on [Cisco Design Zone](#).

Figure 14 depicts the specific products that were selected within Cisco’s laboratories. It is important to note that the Secure Edge 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.

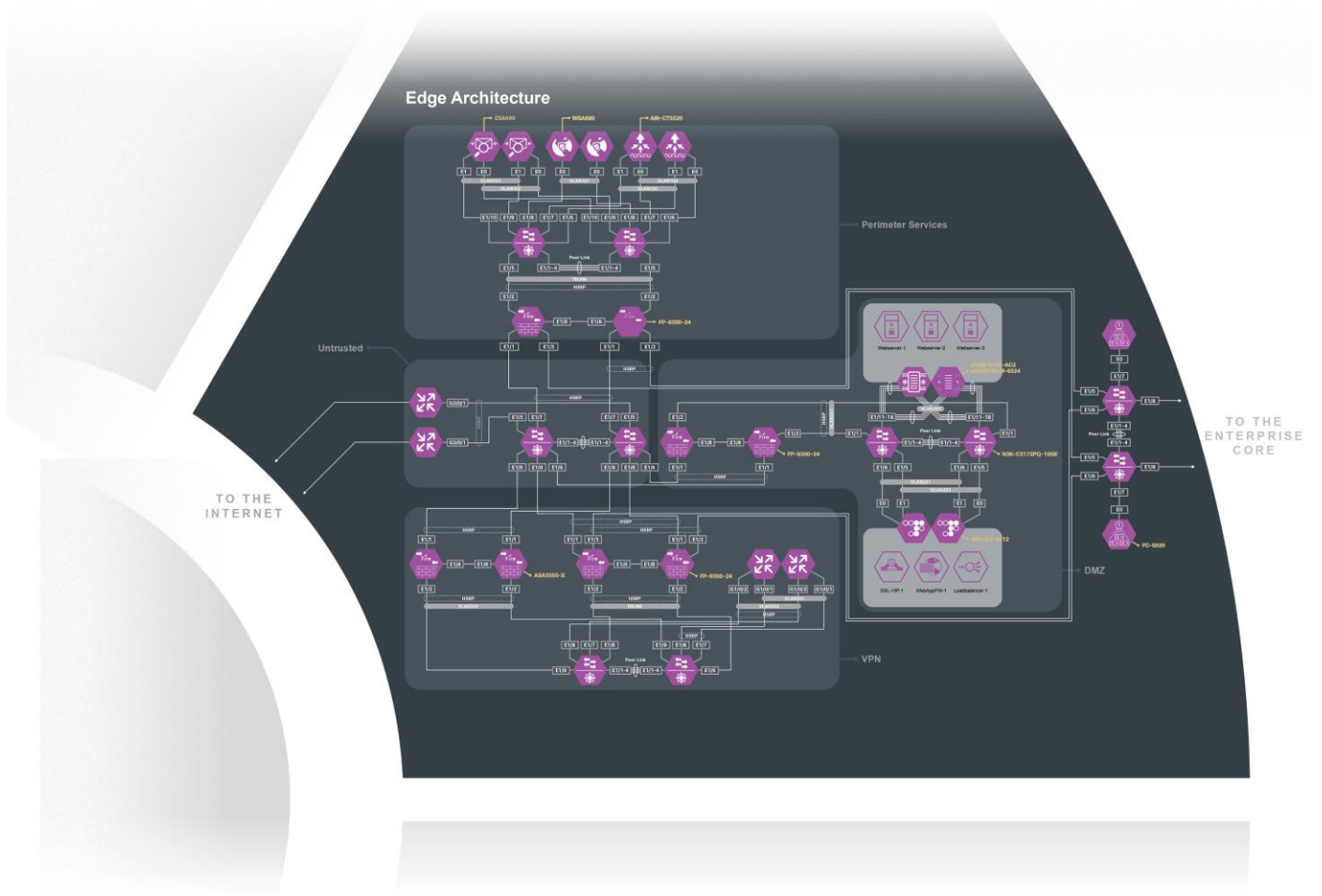














Figure 14. Secure Edge Proposed Design

Appendix B - Suggested Components

Edge Attack Surface		Security Capability		Suggested Cisco Components
Human	Administrators: Typically, no humans are physically present.		Identity	Cisco Identity Services Engine (ISE) Cisco Secure Access by Duo
Network	Wired Network: Routers, switches.		Firewall	Cisco Secure Firewall Cisco Secure Firewall Threat Defense Virtual (FTDv) Cisco Adaptive Security Appliance Virtual (ASAv) Cisco Cloud Services Router (CSR)
			Intrusion Prevention System	Cisco Secure Firewall Cisco Secure Firewall Threat Defense Virtual Cisco Secure IPS Virtual
			Tagging	Nexus/Catalyst/Meraki Switch VLANs TrustSec
			Anti-Malware	Cisco Secure Endpoint
	Analysis		Threat Intelligence	Talos Threat Intelligence
			Flow Analytics	Cisco Secure Network Analytics Cisco Secure Cloud Analytics
		WAN		VPN Site to Site, SD-WAN
			VPN Gateway, Remote Access VPN	Cisco Secure Firewall Cisco Adaptive Security Appliance Cisco Meraki

Edge Attack Surface		Security Capability		Suggested Cisco Components
			DDoS Protection	Cisco Secure DDoS
			Web Security	Cisco Secure Web Appliance
Applications	Application		Application Visibility Control	Cisco Secure Workload Cisco Secure Firewall Cloud Native Cisco Secure Firewall Threat Defense Virtual Cisco Adaptive Security Appliance Virtual Cisco Meraki Virtual MX
				
			Web Application Firewall	Cisco Secure WAF
			Malware Sandbox	Cisco Secure Malware Analytics
			TLS Encryption Offload	Cisco Secure Application Delivery Controller (ADC)
	Storage		Disk Encryption	Cloud Storage Provider
	Server-Based Security		Anti-Malware	Cisco Secure Endpoint
			Anti-Virus	Cisco Secure Endpoint
			Cloud Security	Cisco Umbrella
			Host-based Firewall	Cisco Secure Workload

Edge Attack Surface		Security Capability	Suggested Cisco Components
		 Posture Assessment	Cisco Secure Endpoint Cisco Secure Access by Duo
		 Disk Encryption	Cisco Unified Computing System (UCS) Cisco Hyperflex
		 Flow Analytics	Cisco Secure Cloud Analytics Cisco Secure Workload
		 Application Dependency Mapping	Cisco Secure Workload
		 Vulnerability Assessment and Software Inventory	Cisco Secure Workload
		 Process Anomaly Detection & Forensics:	Cisco Secure Workload
		 Tagging: Grouping for Software Defined Policy	Cisco Secure Workload
		 Policy Generation, Audit, and Change Management:	Cisco Secure Workload

Appendix C - Feedback

If you have feedback on this design guide or any of the Cisco Security design guides, please send an email to ask-security-cvd@cisco.com.

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 <https://www.cisco.com/go/offices>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned 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. (1110R)