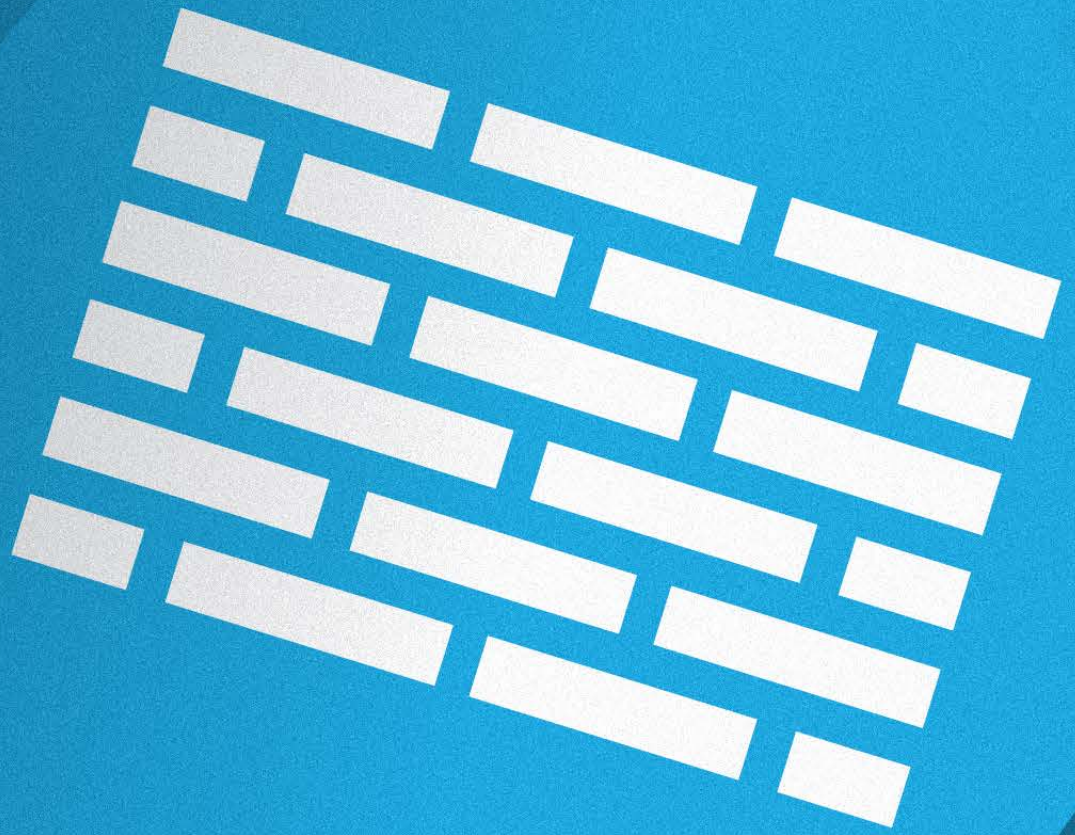
SAFE Security Architecture Toolkit



July 2018

SAFE Security Architecture Toolkit Table of Contents

- SAFE Toolkit Overview
- Capabilities Flows and Endpoints
- Architectures
- Designs
- SAFE Icon Library
- Tools, Rules and Techniques
- Contact

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

SAFE Toolkit Overview

Cisco SAFE simplifies security so your conversations can focus on the needs of a business. By mapping the flows of the business, specific threats can be addressed with corresponding security capabilities, architectures, and designs.

The SAFE Toolkit includes the elements required to facilitate security discussions. You can use the items on these slides to build presentations using SAFE best-practice illustrations and diagrams. And you can customize the diagrams to suit your business.

This toolkit complements the SAFE Overview, Architecture and Design Guides which can be found at www.cisco.com/go/safe

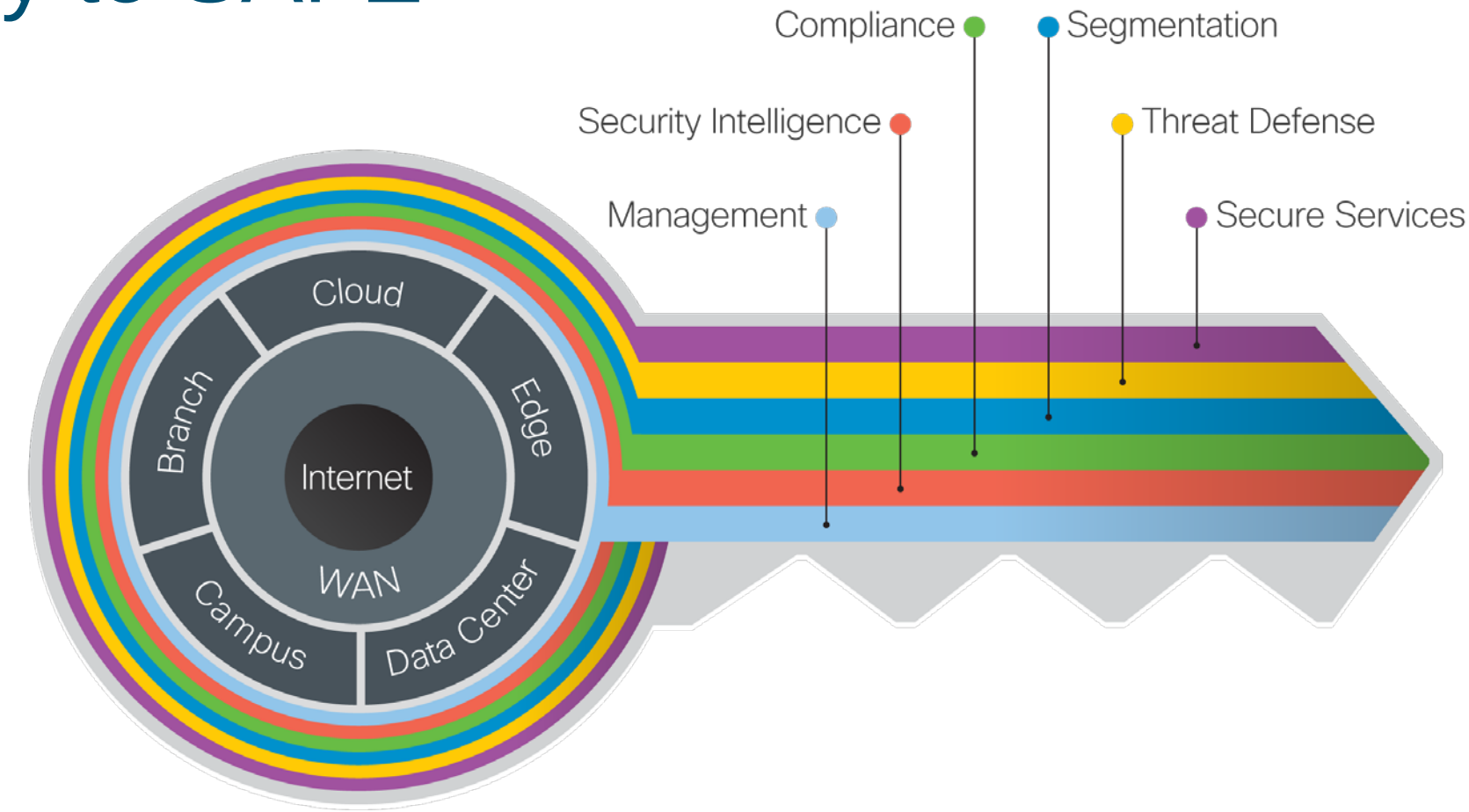
© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

High-level SAFE Graphics

The following slides contain graphics that you can use to introduce SAFE and explain SAFE concepts and components.

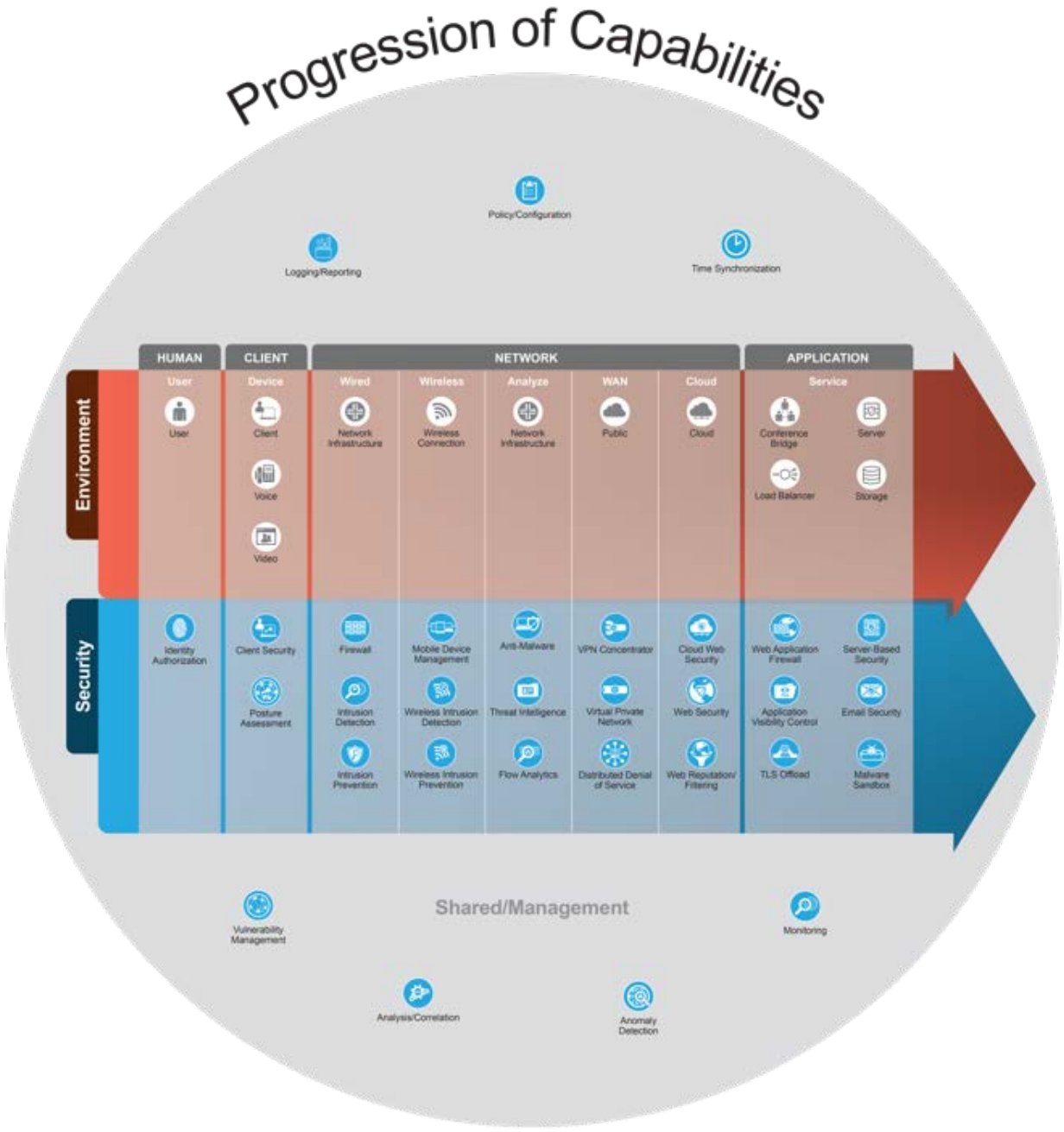
© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public

The Key to SAFE



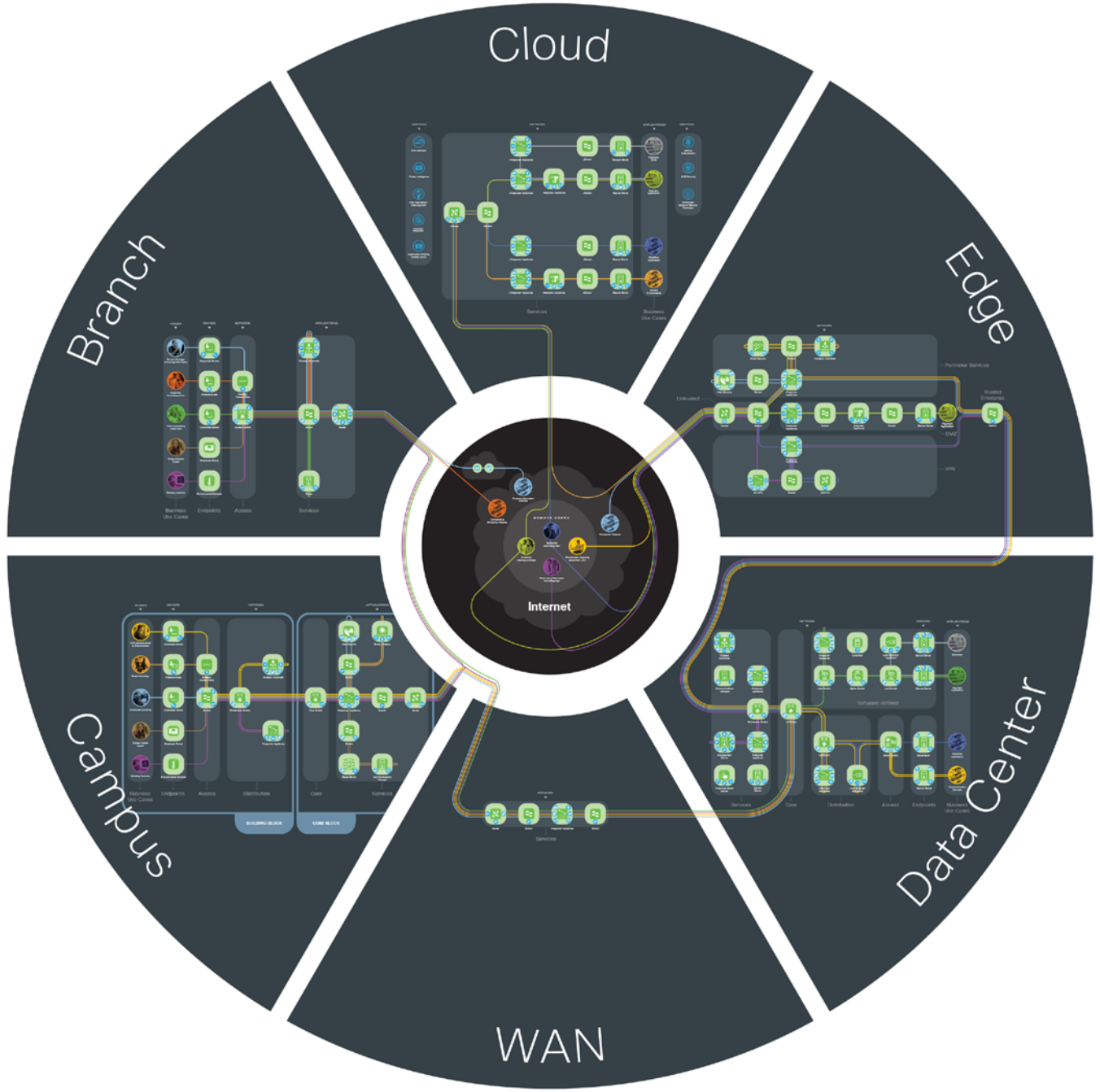
© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

SAFE Progression of Capabilities



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

SAFE Architecture Wheel



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

SAFE Capabilities Flows and Endpoints

First, identify the capabilities your customer needs their network to provide to the business.

Next, you can use the endpoints and capabilities icons to map the business flows.

Mapping the threats the customer faces onto the capabilities is the key to SAFE.

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public

SAFE Master Capabilities Flows

Internal Business Flows:

Secure communications for email: CEO sending email to shareholder

Secure applications for PCI: Clerk processing credit card transaction

Secure web access for employees: Employee researching product information

Secure communications for collaboration: Subject matter expert consultation

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

SAFE Master Capabilities Flows

Third-Party Business Flows:

Secure remote access for third party: Connected device with remote vendor support

Secure remote access for employees: Field engineer updating work order

Secure east-west traffic for compliance: PCI compliance for financial transactions

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

SAFE Master Capabilities Flows

Customer Business Flows:

Secure web access for guests: Guest accessing the Internet for comparative shopping

Secure web access for guests: Guest accessing the Internet to watch hosted video

Secure applications for PCI: Customer making purchase

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

SAFE Master Endpoints

Use these endpoints to further customize your SAFE capabilities flows. Industry-specific endpoints are provided on the following slides.

CEO

Shareholder

Guest

Server

Manager

Manager

Salesperson

Technician

Server

Subject Matter Expert

Remote Colleague

Remote Employee

Video Surveillance

Server

Video Camera

Technician

Remote Technician

Automated Process

Server

Building Controls

Building Controls

Customer

Guest

Salesperson

Shareholder

Server

Server

Automated Process

Clerk

Server

Customer

Technician

Remote Employee

Server

Building Controls

CEO

Shareholder

Customer

Manager

Clerk

Guest

Subject Matter Expert

Remote Employee

Secure Partner

Server

Server

Building Controls

Building Controls

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

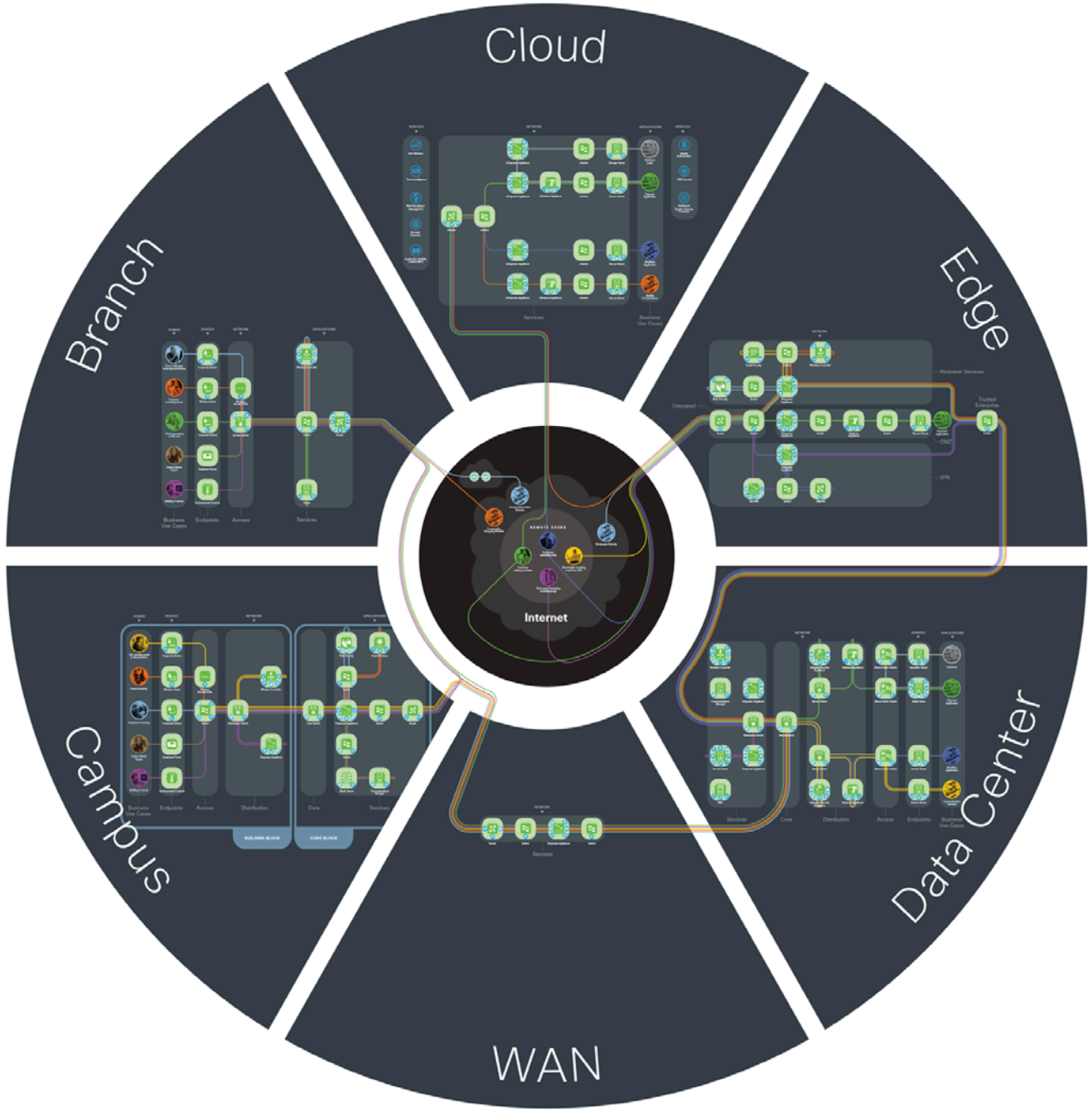
SAFE Architecture Diagrams

SAFE architecture diagrams convey the network structure at a high level without naming specific products. Architectures can also reference capabilities.

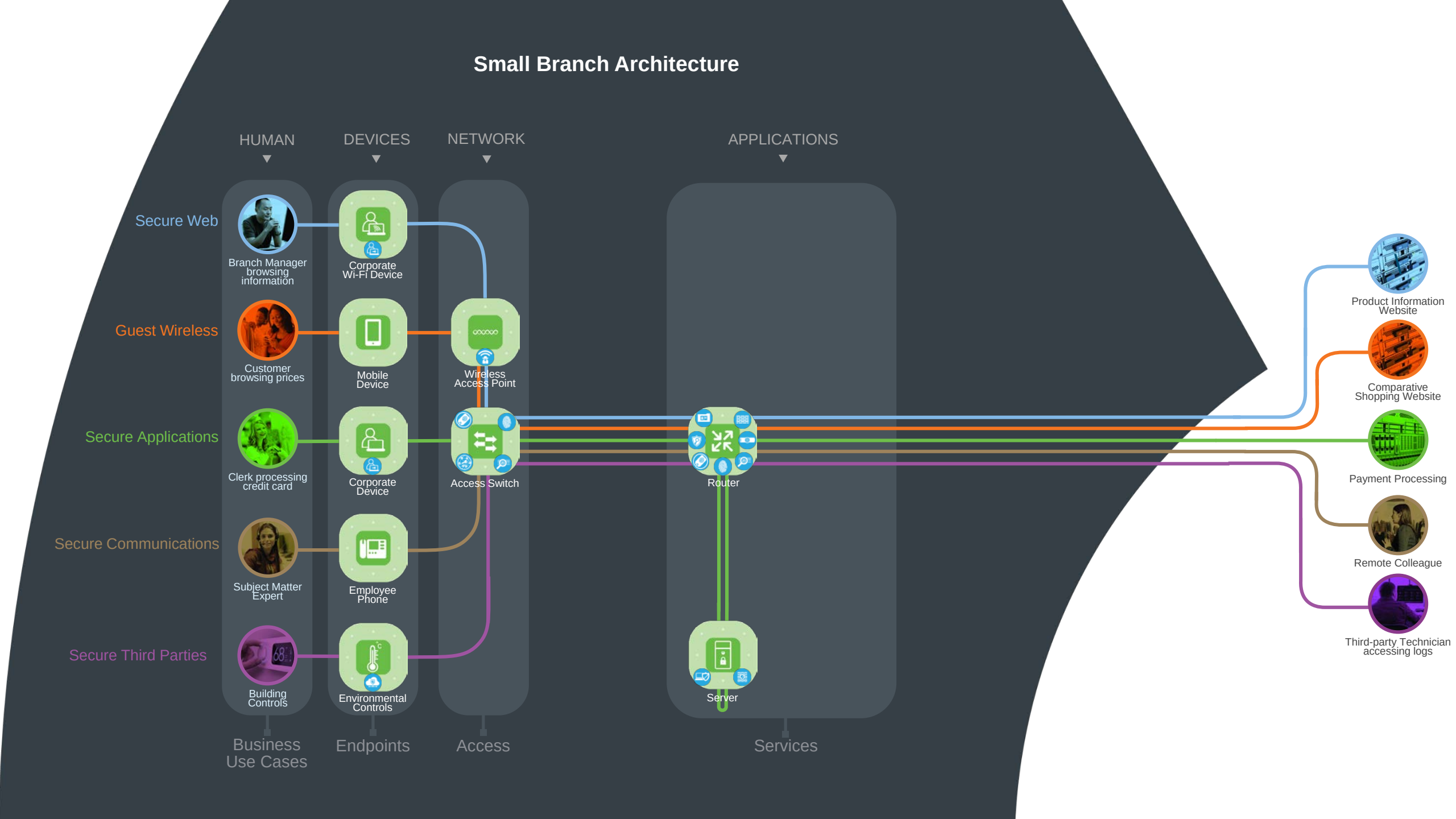
© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public

The following architecture diagrams are best-practice references for each Place in the Network (PIN).

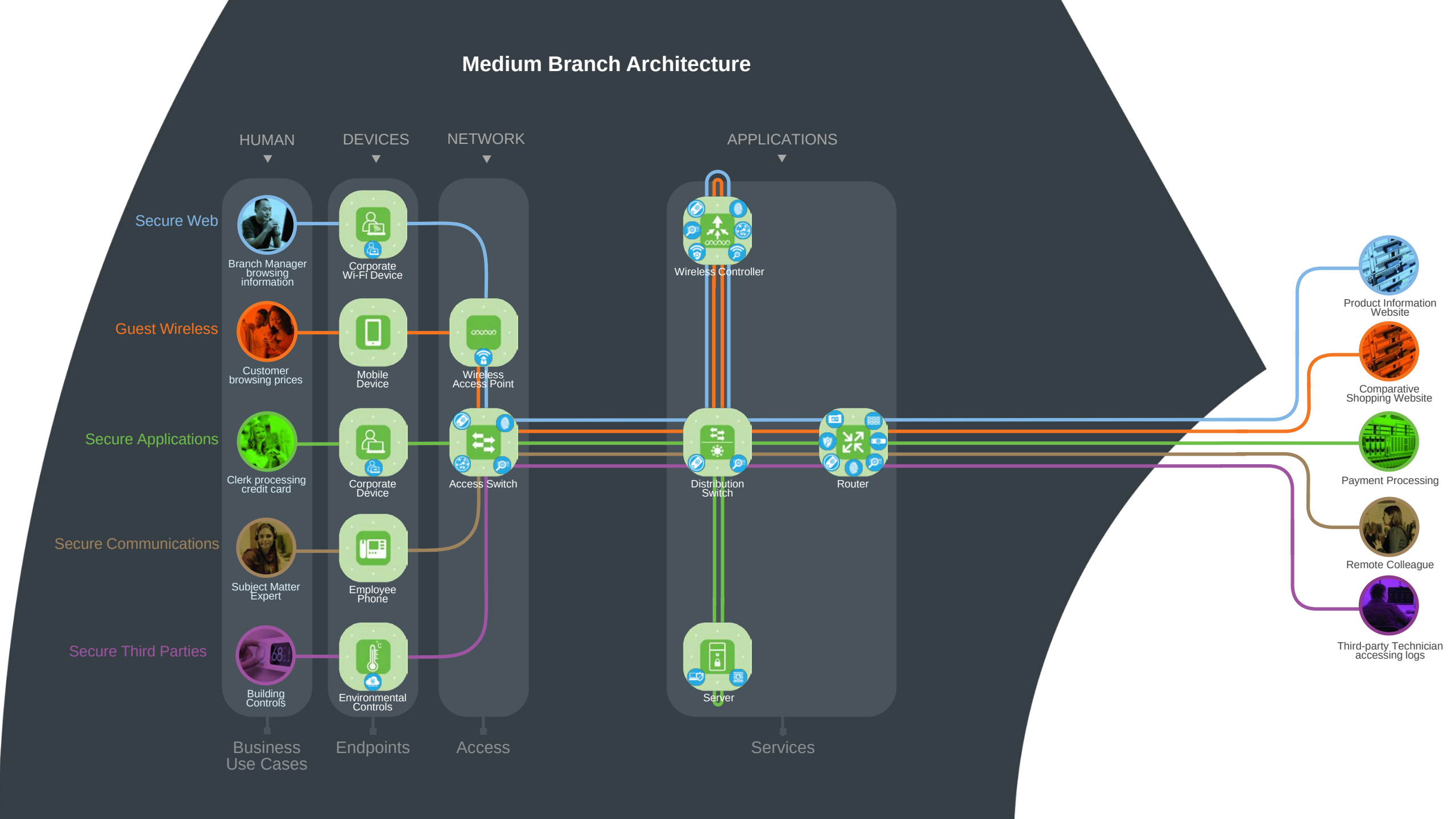
They may be used as is or you may customize them. Customization instructions are in the Tools and Rules section beginning on slide 38.



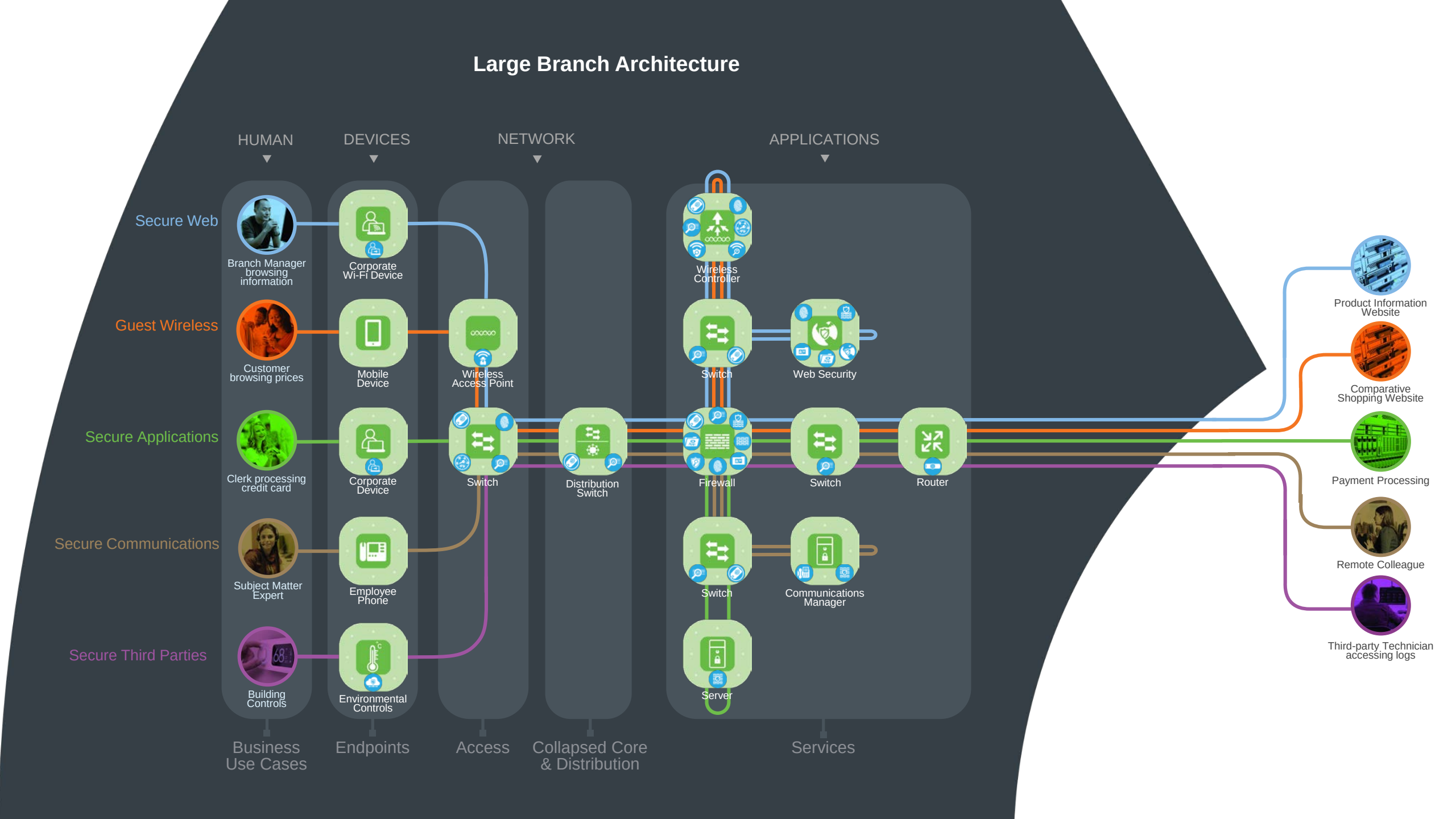
© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public


Small Branch Architecture
HUMAN
DEVICES
NETWORK
APPLICATIONS
Secure Web
Guest Wireless
Secure Applications
Secure Communications
Secure Third Parties
Branch Manager browsing information
Corporate Wi-Fi Device
Customer browsing prices
Mobile Device
Wireless Access Point
Clerk processing credit card
Corporate Device
Access Switch
Router
Subject Matter Expert
Employee Phone
Building Controls
Environmental Controls
Server
Product Information Website
Comparative Shopping Website
Payment Processing
Remote Colleague
Third-party Technician accessing logs
Business Use Cases
Endpoints
Access
Services

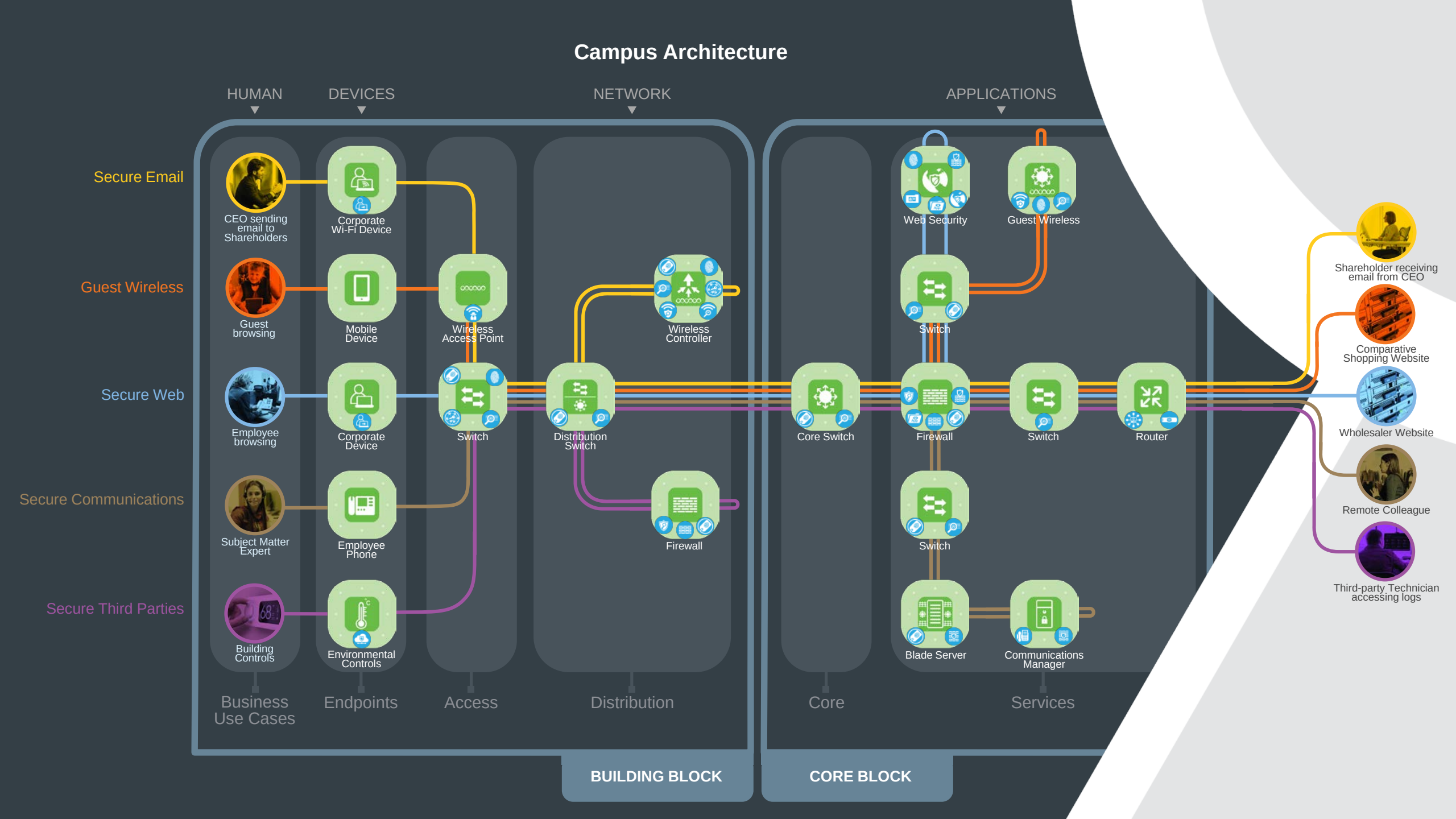
Medium Branch Architecture

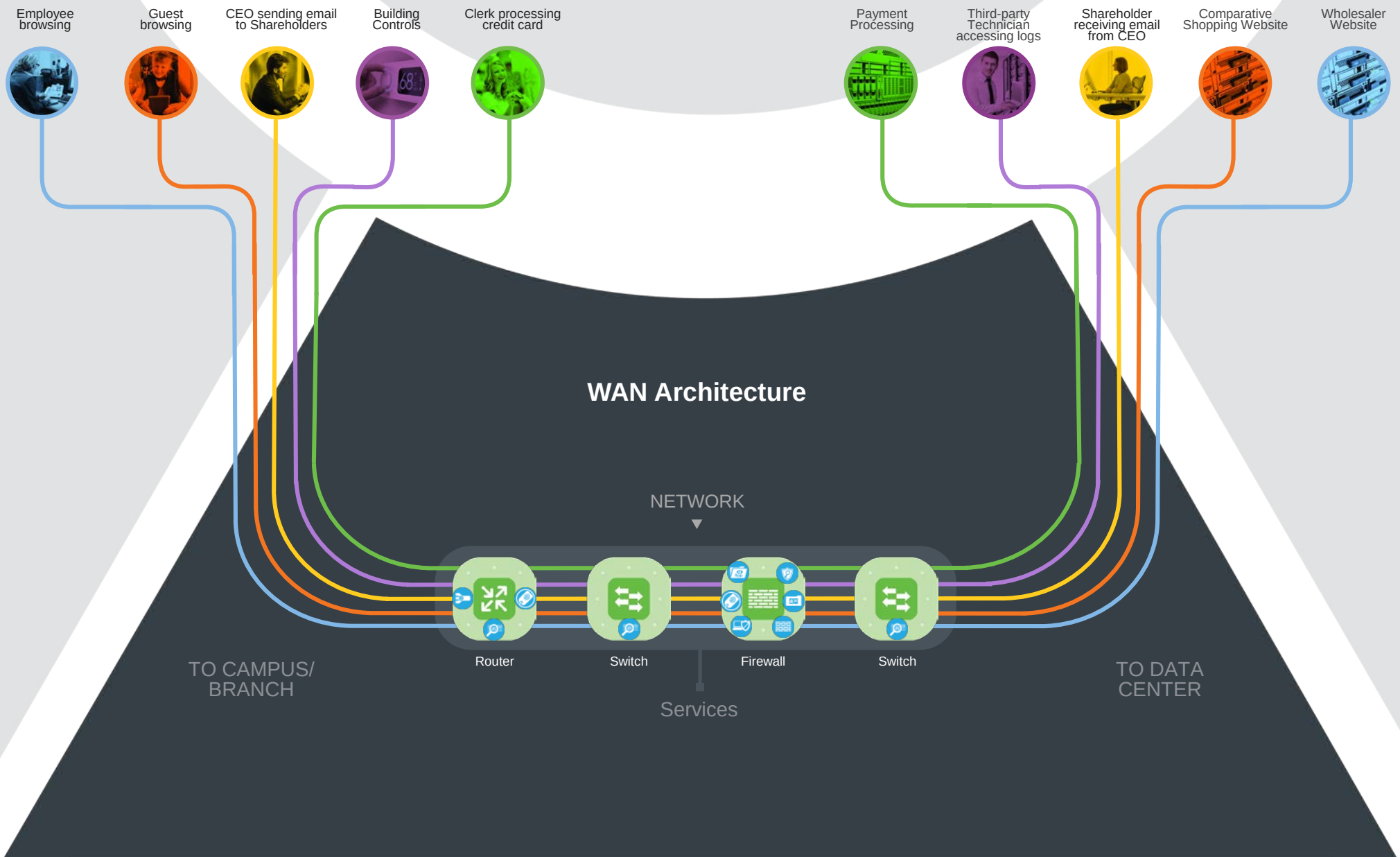


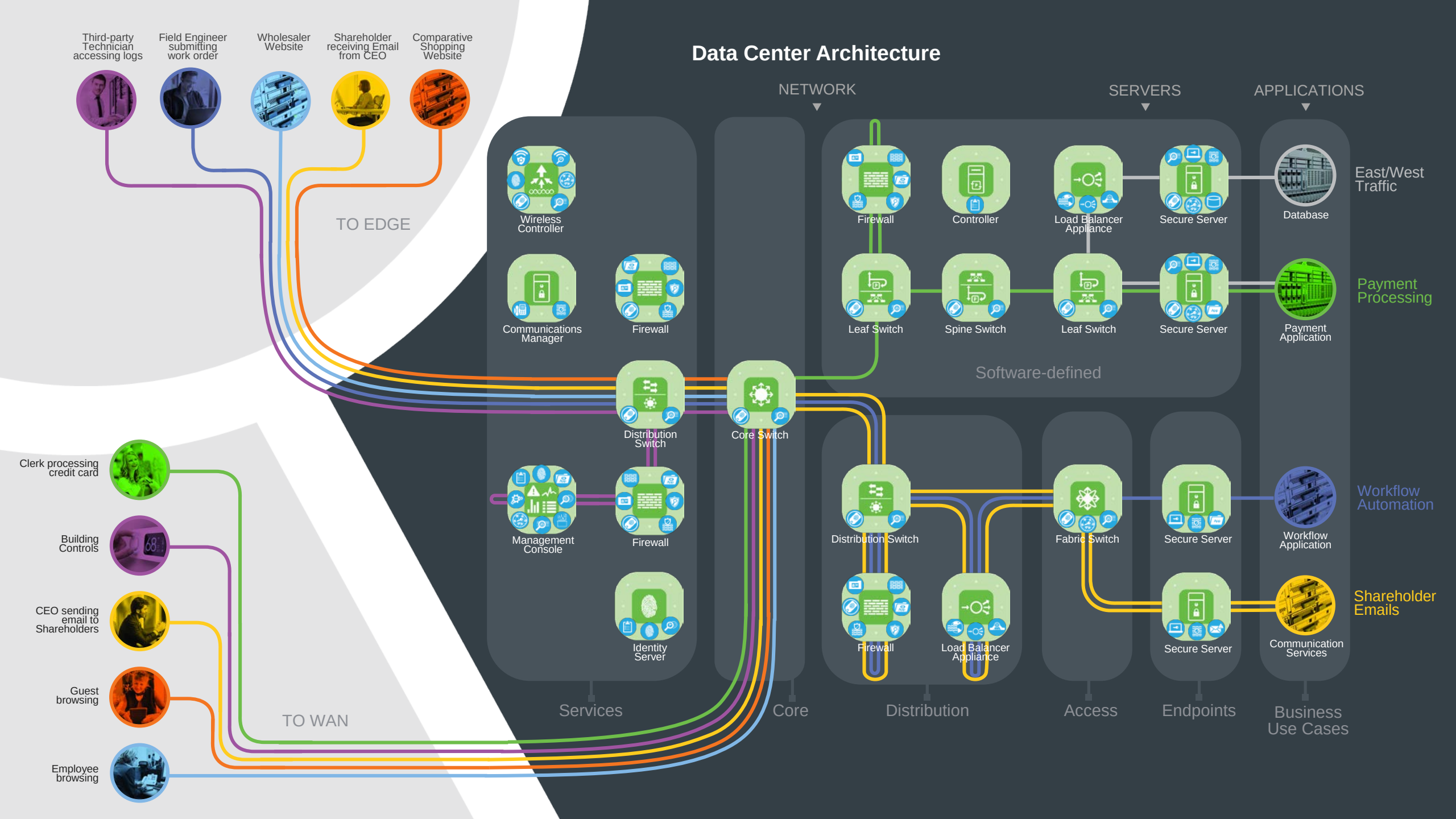
Large Branch Architecture



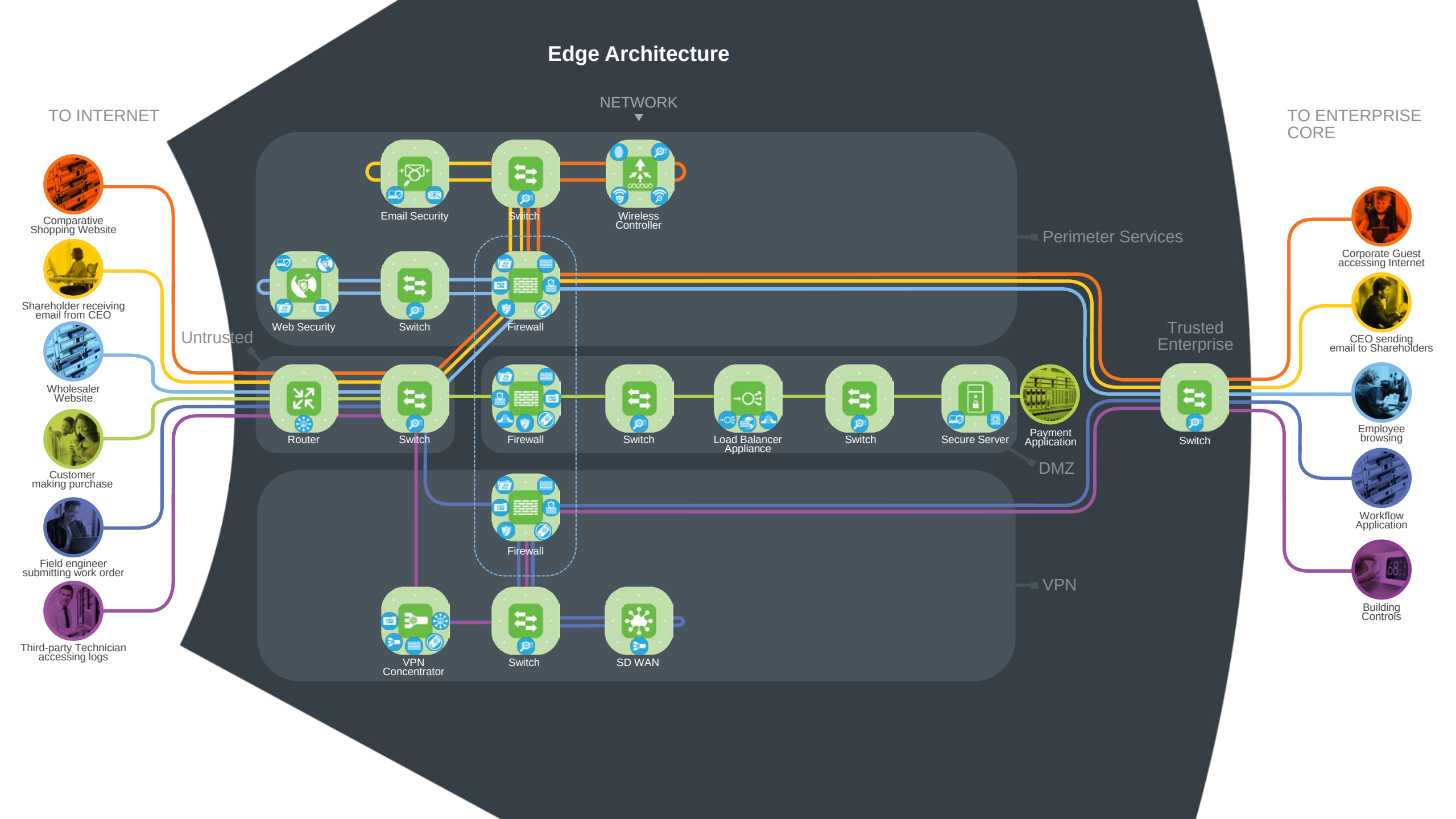
Campus Architecture



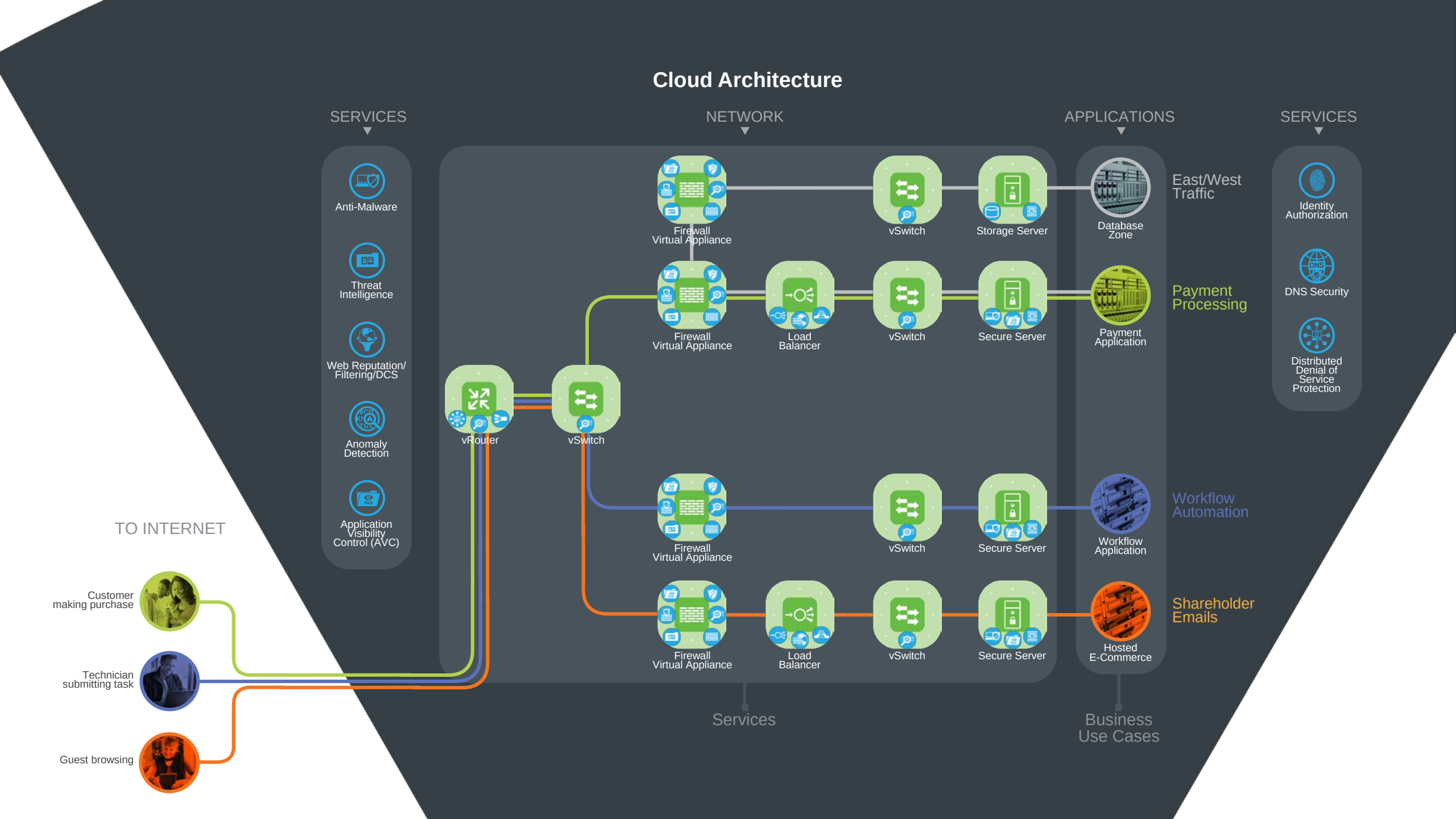

Employee browsing
Guest browsing
CEO sending email to Shareholders
Building Controls
Clerk processing credit card
Payment Processing
Third-party Technician accessing logs
Shareholder receiving email from CEO
Comparative Shopping Website
Wholesaler Website
WAN Architecture
NETWORK
Router
Switch
Firewall
Switch
Services
TO CAMPUS/ BRANCH
TO DATA CENTER


Third-party Technician accessing logs
Field Engineer submitting work order
Wholesaler Website
Shareholder receiving Email from CEO
Comparative Shopping Website
Data Center Architecture
NETWORK
SERVERS
APPLICATIONS
TO EDGE
Wireless Controller
Communications Manager
Firewall
Firewall
Controller
Load Balancer Appliance
Secure Server
Database
East/West Traffic
Leaf Switch
Spine Switch
Leaf Switch
Secure Server
Payment Application
Payment Processing
Software-defined
Distribution Switch
Core Switch
Management Console
Firewall
Identity Server
Distribution Switch
Fabric Switch
Secure Server
Workflow Application
Workflow Automation
Firewall
Load Balancer Appliance
Secure Server
Communication Services
Shareholder Emails
Clerk processing credit card
Building Controls
CEO sending email to Shareholders
Guest browsing
Employee browsing
TO WAN
Services
Core
Distribution
Access
Endpoints
Business Use Cases

Edge Architecture



Cloud Architecture

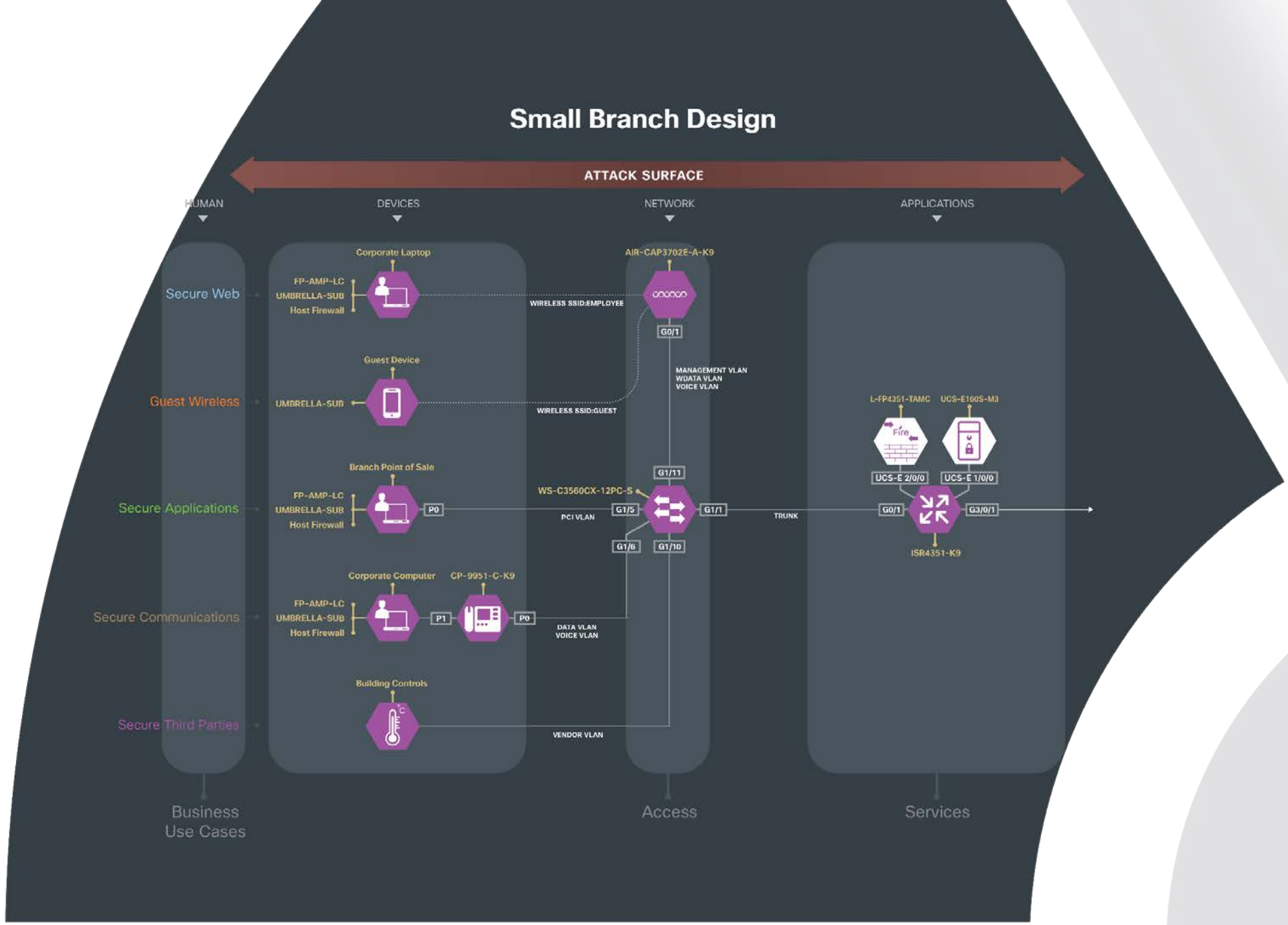


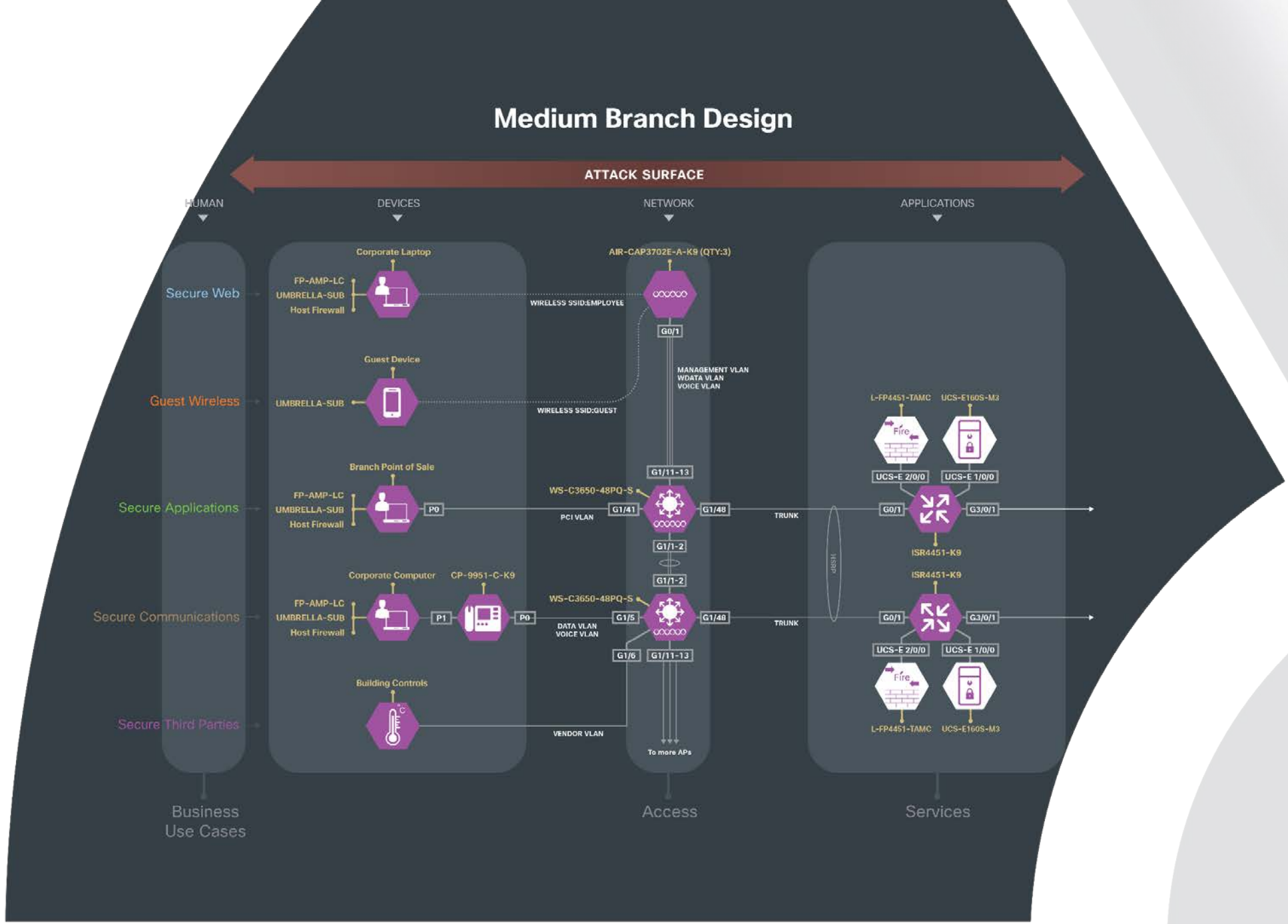
SAFE Design Diagrams

SAFE design diagrams show the specific products and flow/ structure needed to satisfy the desired security capabilities of a particular network.

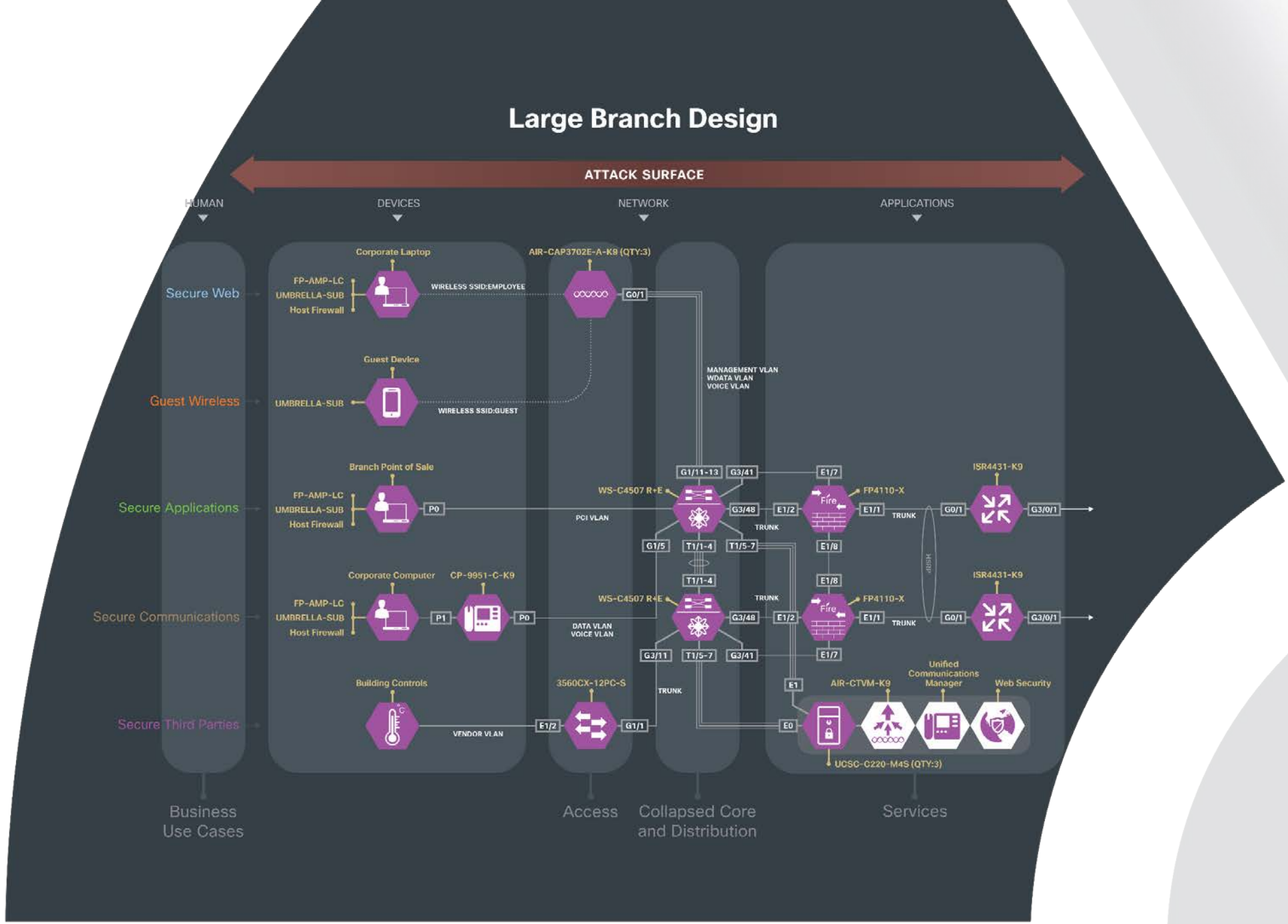
The following design diagrams are best-practice references for selected Places in the Network (PINs). Contact the Cisco SAFE Team for assistance in building customized SAFE designs in Visio.

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public


Small Branch Design
ATTACK SURFACE
HUMAN
DEVICES
NETWORK
APPLICATIONS
Secure Web
Guest Wireless
Secure Applications
Secure Communications
Secure Third Parties
Corporate Laptop
FP-AMP-LC
UMBRELLA-SUB
Host Firewall
Guest Device
UMBRELLA-SUB
Branch Point of Sale
FP-AMP-LC
UMBRELLA-SUB
Host Firewall
P0
Corporate Computer
CP-9951-C-K9
FP-AMP-LC
UMBRELLA-SUB
Host Firewall
P1
P0
Building Controls
VENDOR VLAN
AIR-CAP3702E-A-K9
WIRELESS SSID:EMPLOYEE
G0/1
MANAGEMENT VLAN
WDATA VLAN
VOICE VLAN
WIRELESS SSID:GUEST
WS-C3560CX-12PC-S
G1/11
G1/5
G1/1
G1/6
G1/10
PCI VLAN
TRUNK
DATA VLAN
VOICE VLAN
L-FP4351-TAMC
UCS-E160S-M3
UCS-E 2/0/0
UCS-E 1/0/0
G0/1
G3/0/1
ISR4351-K9
Business
Use Cases
Access
Services


Medium Branch Design
ATTACK SURFACE
HUMAN
DEVICES
NETWORK
APPLICATIONS
Secure Web
Guest Wireless
Secure Applications
Secure Communications
Secure Third Parties
Corporate Laptop
FP-AMP-LC
UMBRELLA-SUB
Host Firewall
Guest Device
UMBRELLA-SUB
Branch Point of Sale
FP-AMP-LC
UMBRELLA-SUB
Host Firewall
P0
Corporate Computer
CP-9951-C-K9
FP-AMP-LC
UMBRELLA-SUB
Host Firewall
P1
P0
Building Controls
AIR-CAP3702E-A-K9 (QTY:3)
WIRELESS SSID:EMPLOYEE
G0/1
MANAGEMENT VLAN
WDATA VLAN
VOICE VLAN
WIRELESS SSID:GUEST
G1/11-13
WS-C3650-48PQ-S
G1/41
PCI VLAN
G1/48
TRUNK
G1/1-2
G1/1-2
WS-C3650-48PQ-S
G1/5
DATA VLAN
VOICE VLAN
G1/48
TRUNK
G1/6
G1/11-13
VENDOR VLAN
To more APs
HSRP
L-FP4451-TAMC
UCS-E160S-M3
UCS-E 2/0/0
UCS-E 1/0/0
G0/1
G3/0/1
ISR4451-K9
ISR4451-K9
G0/1
G3/0/1
UCS-E 2/0/0
UCS-E 1/0/0
L-FP4451-TAMC
UCS-E160S-M3
Business Use Cases
Access
Services

Large Branch Design



SAFE Icon Library

If you need to customize SAFE capabilities flows or architectures, you'll find the icons on the following slides.

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public

Human Icons

To maintain your library, copy (do not cut) icons from this grid.

Attack Surface	Threat	Capability Icons	Architecture Icons	Cisco Product
Users: Employees, third parties, customers, and administrators. 	Rogue: Attackers accessing restricted information resources. 	Identity: Identity-based access. Identity 	Identity Directory Identity Directory	• Cisco Identity Services Engine Appliance • Cisco Identity Services Engine Virtual Appliance

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Additional Humans Icons

To maintain your library, copy (do not cut) icons from this grid.

Optional Endpoints

CEO

Clerk

Customer

Expert

Guest

Manager

Remote Employee

Secure Partner

Shareholder

Identity Directory

Identity Directory

Identity Directory

Generic Icons

Person

People

Third-Party Icons

Other Icons

MS Active Directory

MS Active Directory

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Devices Icons

To maintain your library, copy (do not cut) icons from this grid.

Attack Surface	Threat	Capability Icons	Architecture Icons	Cisco Product
Clients: Devices such as PCs, laptops, smartphones, tablets. Workstation	Malware: Viruses, malware, and attacks that compromise systems. 	Client-Based Security: This capability represents multiple types of security software to protect clients. Client-Based Security 	Corporate Device Corporate Device	• Cisco Advanced Malware Protection for Endpoints • Cisco Umbrella • Cisco AnyConnect • Built-in OS Firewall or Partner Products
	Malware: Viruses, malware, and attacks that compromise systems. 	Anti-Malware Anti-Malware 		• Cisco Advanced Malware Protection for Endpoints
	Virus: Viruses compromising systems. 	Anti-Virus Anti-Virus 		• Cisco Advanced Malware Protection for Endpoints (TETRA)

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Devices Icons

To maintain your library, copy (do not cut) icons from this grid.

Attack Surface	Threat	Capability Icons	Architecture Icons	Cisco Product
Clients: Devices such as PCs, laptops, smartphones, tablets. Workstation	Exploit Redirection: Unauthorized access and malformed packets connecting to client. 	Personal Firewall Firewall 	Corporate Device Corporate Device	• Built-in OS Firewall • Partner Products
	Phish Link: Redirection of user to malicious web site. 	Cloud Security: Combination icon representing several security capabilities provided by the cloud. Cloud Security 		• Cisco Umbrella - Secure Internet Gateway (SIG) • Cisco AnyConnect Agent • Cisco Cloudlock • Cisco Web Security Appliance • Cisco Meraki MX • Cisco Firepower with URL Filtering • Cisco Viptela SD-WAN
	Botnets DDOS: Compromised devices connecting to infrastructure. 	Posture Assessment: Client endpoint compliance verification and authorization. Posture Assessment 		• Cisco AnyConnect Agent • Cisco Identity Services Engine • Cisco Meraki MDM

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Devices Icons

To maintain your library, copy (do not cut) icons from this grid.

Attack Surface	Threat	Capability Icons	Architecture Icons	Cisco Product
Voice: Phone phone	Rogue: Attacker accessing private information. 		Phone Phone	• Cisco Unified Communications • Cisco IP Phones
Video: Displays, collaboration, smartboards. Video Endpoint	Rogue: Attacker accessing private information. 		Video Endpoint Video Endpoint	• Cisco Unified Communications • Cisco Telepresence • Cisco WebEx Teams • Cisco IP Phones
Autonomous Device: Building controls, manufacturing systems, automation. sensor	Rogue: Attacker accessing private information. 		Environmental Controls Environmental Controls	• Partner devices and controllers

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Additional Devices Icons

To maintain your library, copy (do not cut) icons from this grid.

Optional Endpoints

Server

Building Controls

Server

Camera

Building Controls

Corporate Device

Corporate Wireless Device

Mobile

Phone

Video Endpoint

Actuator

Sensor

Automated System

Corporate Device

Corporate Wireless Device

Mobile

Phone

Video Endpoint

Actuator

Sensor

Automated System

Phone

Video Endpoint

Automated System

Generic Icons

Third-Party Icons

Other Icons

Standardized System Images

Infrastructure Redundancy

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Network Icons

To maintain your library, copy (do not cut) icons from this grid.

Attack Surface	Threat	Capability Icons	Architecture Icons	Cisco Product
Wired Network: Physical network infrastructure; routers, switches, used to connect access, distribution, core, and services layers together 	Exploit Redirection: Unauthorized access and malformed packets connecting to client. 	Firewall: Stateful filtering and protocol inspection. 	Firewall 	• Cisco Adaptive Security Appliance (ASA) • Cisco Firepower Appliance • Cisco Next Generation Firewall • Cisco Next Generation Firewall Virtual
Exploit Redirection: Attacks using worms, viruses, or other techniques. 	Intrusion Prevention: Blocking of attacks by signatures and anomaly analysis. 	Intrusion Prevention 	• Cisco Adaptive Security Appliance (ASA) • Cisco Firepower Appliance • Cisco Next Generation Intrusion Prevention System • Cisco Next Generation Intrusion Prevention System Virtual	
Unauthorized Network Access: Lateral spread of infiltration. 	Tagging: Policy-based, software-defined segmentation. 	Switch 	• Cisco Adaptive Security Appliance (ASA) • Cisco Firepower Appliance • Cisco Catalyst Switches • Cisco Wireless Controller and Access Points • Cisco Identity Services Engine • Cisco Integrated Services Routers • Cisco Aggregation Services Routers • Cisco Nexus Switches • Cisco ACI Fabric • Cisco DNA Fabric • Cisco Tetration	

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Network Icons

To maintain your library, copy (do not cut) icons from this grid.

Attack Surface	Threat	Capability Icons	Architecture Icons	Cisco Product
Wireless Network: Physical network infrastructure; access points and controllers used to connect mobile devices to the access layer. Wireless	Malware: Compromised devices connecting to infrastructure. 	Mobile Device Management (MDM): Endpoint access control based on policies. Mobile Device Management (MDM) 	MDM Appliance MDM Appliance	• Cisco Identity Services Engine • Cisco Meraki Mobile Device Management
Rogue: Unauthorized access and disruption of wireless network. 	Wireless Rogue Detection: Detection and containment of malicious wireless devices not controlled by the company. Wireless Rogue Detection 	Wireless LAN Controller Wireless LAN Controller	• Cisco Catalyst Switches with Unified Access • Cisco Wireless Controller and Access Points • Cisco Mobility Services Engine
Rogue: Attacks on the infrastructure via wireless technology. 	Wireless Intrusion Prevention (WIPS): Blocking of wireless attacks by signatures and anomaly analysis. Wireless Intrusion Prevention (WIPS) 	Wireless Access Point Wireless Access Point	• Cisco Catalyst Switches with Unified Access • Cisco Wireless Controller and Access Points

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Network Icons

To maintain your library, copy (do not cut) icons from this grid.

Attack Surface	Threat	Capability Icons	Architecture Icons	Cisco Product
Analysis: Telemetry and analysis of traffic across the enterprise. Analytic Engine	Malware: Malware distribution across networks or between servers and devices. 	Anti-Malware for Networks: Identify, block, and analyze malicious files and transmissions. Network Anti-Malware 	Firewall Firewall	• Cisco Advanced Malware Protection for Networks • Cisco Next Generation Firewall • Cisco Next Generation Firewall Virtual • Cisco Next Generation Intrusion Prevention System • Cisco Next Generation Intrusion Prevention System Virtual
	Advanced Threat: Zero-day malware and attacks. 	Threat Intelligence: Contextual knowledge of emerging hazards. Threat Intelligence 	Threat Intelligence is a capability leveraged by many systems and not deployed separately; there is no dedicated architecture icon.	• Cisco Collective Security Intelligence • Cisco Global Threat Analytics and Encrypted Traffic Analytics • Cisco Talos Security Intelligence • Cisco Firepower Management Center • Cisco Umbrella Investigate • Cisco AMP Console – Telemetry • Cisco Stealthwatch Management Console
	Exfiltration: Traffic, telemetry, and data exfiltration from successful attacks. 	Flow Analytics: Network traffic metadata identifying security Incidents. Flow Analytics 	Flow Sensor Flow Sensor	Flow Sensors and Collectors: • Cisco Integrated Services Router • Cisco Adaptive Security Appliance • Cisco Wireless LAN Controller • Cisco Catalyst Switch • Cisco Nexus Switch • Cisco NetFlow Generation Appliance • Cisco Stealthwatch Flow Sensor Analysis: • Cisco Stealthwatch Management Console • Cisco Stealthwatch Cloud

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Network Icons

To maintain your library, copy (do not cut) icons from this grid.

Attack Surface	Threat	Capability Icons	Architecture Icons	Cisco Product
WAN: Public and untrusted Wide Area Networks that connect to the company, such as the Internet. WAN	Exfiltration: Traffic, telemetry, and data exfiltration from successful attacks. 	VPN Concentrator: Encrypted remote access. VPN Concentrator	VPN Concentrator VPN Concentrator	• Cisco Adaptive Security Appliance (ASA) • Cisco Firepower Appliance • Cisco Next Generation Firewall • Cisco Next Generation Firewall Virtual
	Man-in-the-Middle: Connection of information and identities. 	Virtual Private Network (VPN): Encrypted communication tunnels. Virtual Private Network (VPN)	SD WAN SD WAN	• Cisco Adaptive Security Appliance (ASA) • Cisco Aggregation Services Routers • Cisco Cloud Services Router • Cisco Integrated Services Router • Cisco Firepower Appliance • Cisco Meraki SD-WAN • Cisco IWAN • Cisco Next Generation Firewall • Cisco Next Generation Firewall Virtual • Cisco Viptela SD-WAN vEdge
	Botnets DDOS: Massively scaled attacks that overwhelm services. 	DDOS Protection: Protection against scaled attack forms. Distributed Denial of Service Protection	DDOS Protection Appliance DDOS Protection Appliance	• Cisco Aggregation Services Routers with Radware • Cisco Firepower Appliance with Radware • Distributed Denial of Service Technology Partner

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Network Icons

To maintain your library, copy (do not cut) icons from this grid.

Attack Surface	Threat	Capability Icons	Architecture Icons	Cisco Product
Cloud: Security services from the cloud. Cloud	Phish Link: Attacks from malware, viruses, and malicious URLs. 	Cloud Security: Combination icon representing several security capabilities provided by the cloud. Cloud Security 	VPN Concentrator Cloud Security	• Cisco Umbrella - Secure Internet Gateway (SIG) • Cisco AnyConnect Agent • Cisco Cloudlock • Cisco Cloud Services Router • Cisco Web Security Appliance • Cisco Meraki MX • Cisco Firepower with URL Filtering • Cisco Viptela SD-WAN
	Phish Link: Redirection of user to malicious website. 	DNS Security: Name resolution filtering. DNS Security 	Secure DNS Secure DNS	• Cisco Umbrella
	Rogue: Unauthorized access to cloud SaaS services, data loss. 	Cloud Access Security Broker (CASB): Monitor and protect SaaS services. CASB 		• Cisco CloudLock

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Network Icons

To maintain your library, copy (do not cut) icons from this grid.

Attack Surface	Threat	Capability Icons	Architecture Icons	Cisco Product
Cloud: Security services from the cloud. Cloud	Redirect Link: Infiltration and exfiltration via Web protocols. 	Web Security: Internet access integrity and protections. Web Security 	Web Security Web Security	• Cisco Umbrella - Secure Internet Gateway (SIG) • Cisco Web Security Virtual Appliance • Cisco Meraki URL Filtering
	Malware C2: Attacks directing to a malicious URL. 	Web Reputation/Filtering: Tracking against URL-based threats. Web Reputation/ Filtering/DCS 	Web Reputation Filtering Web Filtering	• Cisco Umbrella - Secure Internet Gateway (SIG) • Cisco Web Security Virtual Appliance • Cisco Meraki URL Filtering
	Redirect Link: Unauthorized access and malformed packets connecting to services. 	Cloud-based Firewall: Filter and inspect traffic via the cloud. Firewall 		• Cisco Adaptive Security Virtual Appliance (ASAv) • Cisco Cloud Services Router • Cisco Next Generation Firewall Virtual (NGFWv)

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Additional Network Icons

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Additional Network Icons

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Additional Network Icons

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Applications Icons

To maintain your library, copy (do not cut) icons from this grid.

Attack Surface	Threat	Capability Icons	Architecture Icons	Cisco Product
Applications: Application-specific security services. Application	Redirect Link: Attacks against poorly-developed applications. 	Web Application Firewalling: Advanced application inspection and monitoring. Web Application Firewall 	Web Application Firewall Web Application Firewall	• Web Application Firewall Technology Partner
	C2 Sites: Attack tools hiding in permitted applications. 	Application Visibility Control (AVC): Deep packet inspection of application flows. Application Visibility Control (AVC) 		• Cisco Aggregation Services Router • Cisco Cloud Services Router • Cisco Integrated Services Router • Cisco Next Generation Firewall • Cisco Next Generation Firewall Virtual
	Spying: Theft of unencrypted traffic. 	TLS Encryption Offload: Accelerated encryption/ decryption of data services. TLS Offload 	TLS Appliance TLS Appliance	• Cisco Next Generation Firewall • Transport Layer Security Offload Technology Partner

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Applications Icons

To maintain your library, copy (do not cut) icons from this grid.

Attack Surface	Threat	Capability Icons	Architecture Icons	Cisco Product
Applications: Application-specific security services. Application	Phishing: Infiltration and exfiltration via email. 	Email Security: Messaging integrity and protections. Email Security 	Email Security Email Security	• Cisco Email Security Appliance • Cisco Cloud Email Security
	Malware: Polymorphic threats. 	Malware Sandbox: Detonation and analysis of file behavior. Malware Sandbox 	Sandbox Appliance Sandbox Appliance	• Cisco Threatgrid
Storage: Drives, databases, media. Storage	Spying: Theft of unencrypted traffic. 	Disk Encryption: Encryption of data at rest. Disk Encryption 		• Disk Encryption Technology Partner

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Applications Icons

To maintain your library, copy (do not cut) icons from this grid.

Attack Surface	Threat	Capability Icons	Architecture Icons	Cisco Product
Servers: Application hosting operation systems. Secure Server Load Balancer	Malware: Viruses, malware and attacks that compromise systems. 	Server-based Security: Combination icon representing several security capabilities to secure the server. Server-Based Security 	Secure Server Secure Server	• Cisco Advanced Malware Protection for Endpoint • Cisco Umbrella • Cisco Tetration • Built-in OS Firewall or Partner Products

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Additional Applications Icons

To maintain your library, copy (do not cut) icons from this grid.

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Management Icons

To maintain your library, copy (do not cut) icons from this grid.

Attack Surface	Threat	Capability Icons	Architecture Icons	Cisco Product
Management: Infrastructure systems management and orchestration. Central Management		Analysis/Correlation: Security event management of real-time information. Analysis/ Correlation	SIEM SIEM	• Cisco Stealthwatch • Cisco Stealthwatch Cloud • Cisco Visibility • SIEM Technology Partner Products
		Anomaly Detection: Identification of infected hosts scanning for other vulnerable hosts. Anomaly Detection		• Cisco Identity Services Engine • Cisco Meraki • Cisco Tetration • Cisco Stealthwatch
		Identity/Authorization: Centralized identity and administration policy. Identity/ Authorization	Identity Directory Identity Directory	• Cisco Identity Services Engine

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Management Icons

To maintain your library, copy (do not cut) icons from this grid.

Attack Surface	Threat	Capability Icons	Architecture Icons	Cisco Product
Management: Infrastructure systems management and orchestration. Central Management		Logging/Reporting: Centralized event information collection. Logging/ Reporting 	Log Collector Log Collector	• Cisco Stealthwatch • Logging Technology Partner Products
		Monitoring: Network traffic inspection. Monitoring 	Monitoring Monitoring	• Cisco Stealthwatch • Cisco Stealthwatch Cloud • Cisco Tetration
		Name Resolution: Centralized DNS Services Name Resolution 	Secure DNS Secure DNS	• Cisco Umbrella

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Management Icons

To maintain your library, copy (do not cut) icons from this grid.

Attack Surface	Threat	Capability Icons	Architecture Icons	Cisco Product
Management: Infrastructure systems management and orchestration. Central Management		Policy/Configuration: Unified infrastructure management and compliance verification. Policy/ Configuration 	Policy Policy	• Cisco Firepower Management Center • Cisco Identity Services Engine • Cisco DNA Center • Cisco ACI APIC • Cisco Stealthwatch Management Console • Cisco Advanced Malware Protection Console • Cisco Defense Orchestrator • Cisco Tetration • Cisco Security Manager • Cisco Prime LMS
		Time Synchronization: Device clock calibration for accurate event correlation. Time Synchronization 	NTP NTP	• Cisco Firewalls, Routers, and Switches
		Vulnerability Management: Continuous scanning, patching, and reporting of infrastructure. Vulnerability Management 	Vulnerability Management Vulnerability Management	• Endpoint Technology Partner

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Additional Management Icons

To maintain your library, copy (do not cut) icons from this grid.

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Tools and Rules

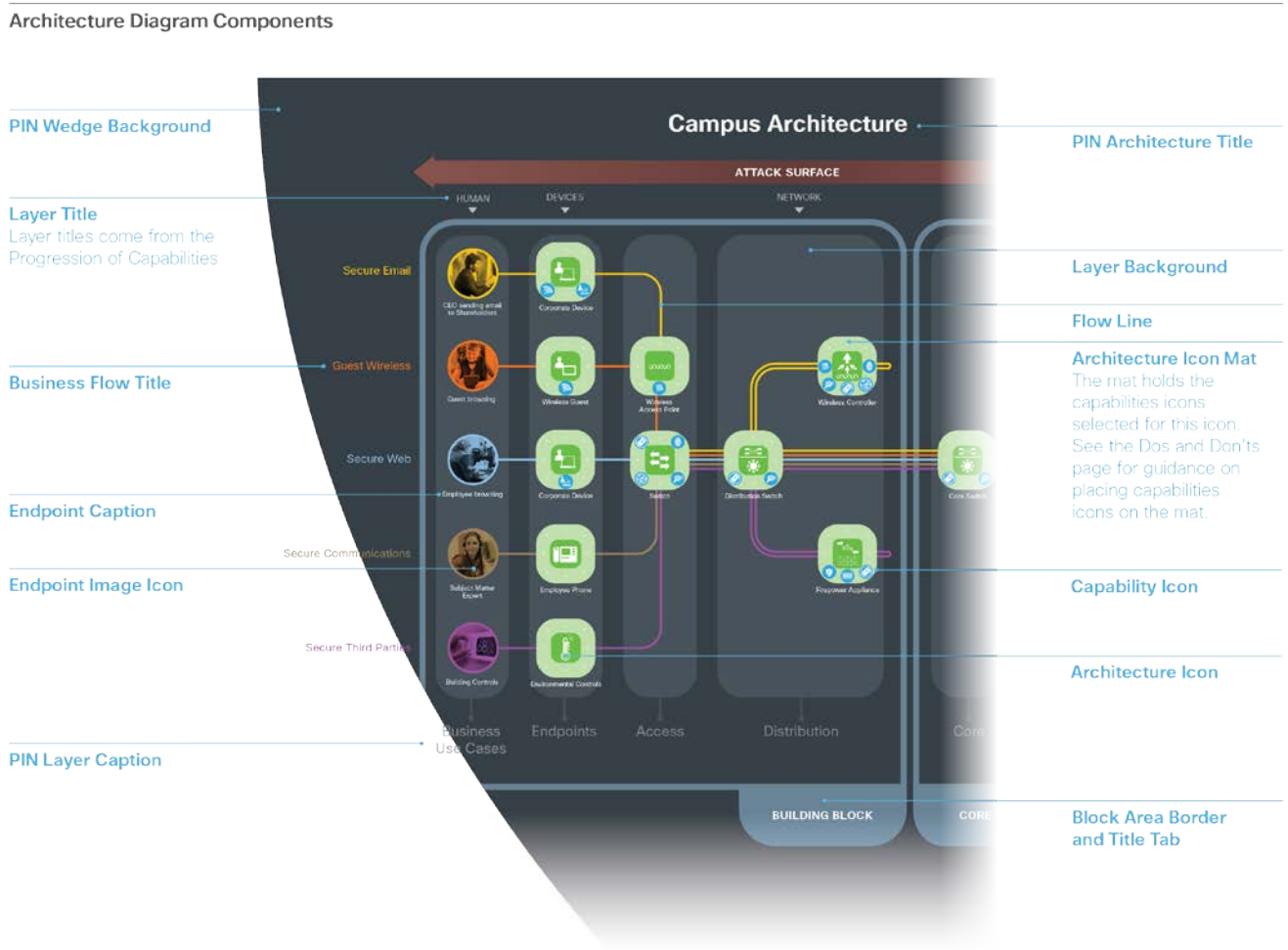
Please refer to the guidelines and helpful elements on these pages to ensure that your diagrams and presentations are SAFE!

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public

Building SAFE Architectures

To customize one of the architecture diagrams on slides 20-27, or to build one, please refer to this key as well as the Architecture Toolkit and the Dos and Don’ts information on the following slides.

For assistance, contact Christian Janoff.
chjanoff@cisco.com



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Architecture Toolkit

All architecture diagrams must be created from the elements found on this page and pages 23-25. Do not alter the elements in any way except as noted next to each element.

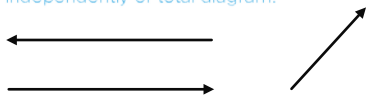
Be sure to review the Dos and Don'ts of Building a Diagram found on page 7 of this document.

Network Border
Border may be extended in width or heighth. Do not scale radius corner or line thickness independently of the entire diagram.

Network Title
Use 22.5pt in either Arial or Cisco Sans Extra Light, 100% Black. Do not alter size unless it is being scaled with the entire diagram.

Title Example

Network Flow Line with Directional Arrow Endcap
Length can be extended. Do not scale line thickness independently of total diagram.



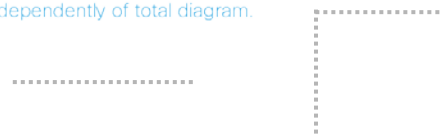
Management Icons
A complete list can be found on page 20 of this document.

Area
Area can be extended in width or heighth. Do not scale radius corner.

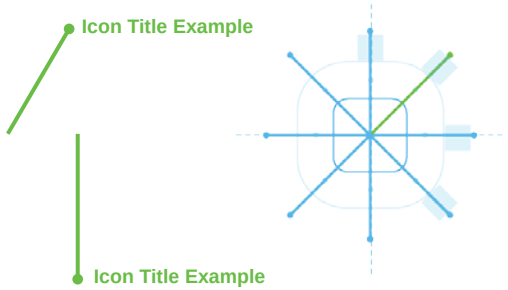
Area Title
Use 11pt in either Arial or Cisco Sans Extra Light, 100% Black. Do not alter size unless it is being scaled with the entire diagram.

Area Title Example

Wireless Connection Line
Length can be extended. Do not scale line thickness independently of total diagram.

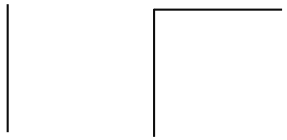


Architecture Icon Name and Rule with Dotted Endcap
Use 5pt in either Arial Bold or Cisco Sans Bold, **R**105, **G**188, **B**70 equivalent. Do not alter size unless it is being scaled with the entire diagram.



Internet/Cloud
Size can be independently reduced and enlarged proportionally as needed.

Network Flow Line
Length can be extended. Do not scale line thickness independently of total diagram.



Architecture Icon with Mini Capability Band
A complete list can be found on pages 23-35 of this document. Do not scale icons independently of the entire diagram. Mini capability icons can be found on pages 27-28 of this document. When placing various numbers of mini icons within the band, refer to the prefered position examples below.

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Dos and Don'ts

Do

Show all flow lines butting up to the icon.

Keep all like icons at a consistent size.

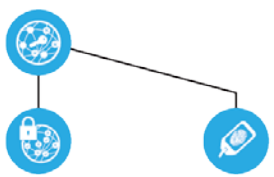
Keep all flow rules at vertical or horizontal alignments.

Make all right angles out of a single rule, keeping corners sharp.

Don't

Don't allow flow lines to overlap icon.

Don't vary the size of the icons.

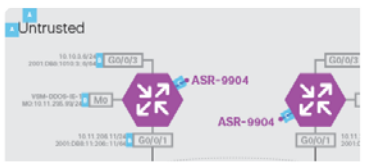


Don't angle the flow lines.

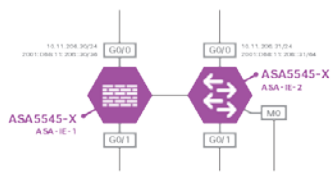
Don't make right angles out of more than one rule.

Do

Use the elements from the toolkit as they have been provided. If elements need to be reduced or enlarged, apply the same reduction/ enlargement over the entire diagram unless otherwise noted in the toolkit.



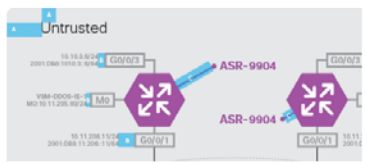
Keep spacing between elements consistent as much as possible.



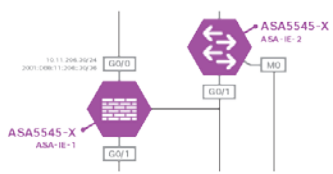
Keep elements aligned as much as possible.

Don't

Don't alter the toolkit elements or create additional components.



Don't vary gaps between elements or length of callout lines if possible.



Don't use arbitrary placement of objects without alignment to other objects within the diagram if possible.

Do

Center mini capability icons on the guide markers per the instructions provided in the Architecture Toolkit.

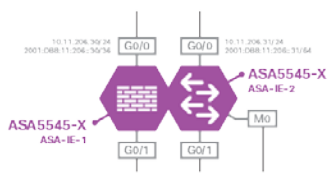
Maintain colors as provided in the toolkit.

Keep space between elements.

Don't

Don't place the mini capability icons outside of the Mini Capability Icon Band or in a position that is inconsistent with the guidelines provided in the toolkit.

Do not alter or add colors to the elements.



Don't overlap elements.

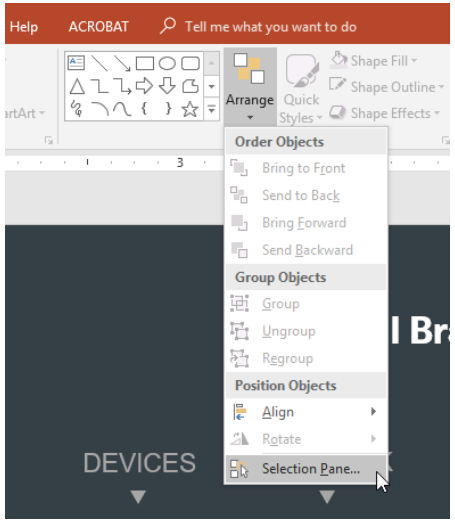
© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Using Selection Pane

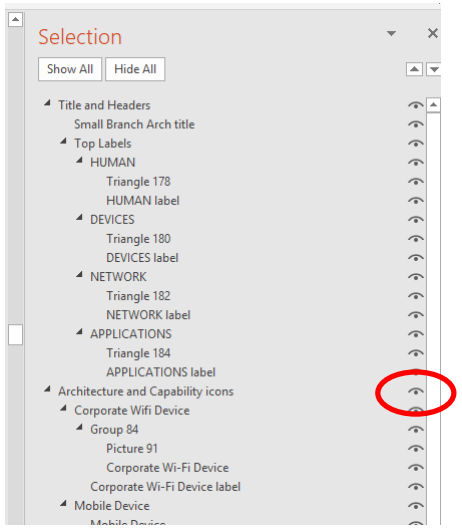
The Selection Pane enables you to view and access layers easily

1. Turn on the Selection Pane
2. Each object in the pane is listed in the hierarchical order (depth) that it is on the slide.
3. Click the eye to make them invisible/visible so you can access objects below them without having to move them from their position
4. By clicking on an object or group name you can select objects that are hard to grab
5. Once selected, you can change their order via the Arrange menu, or move them with cursor keys

1

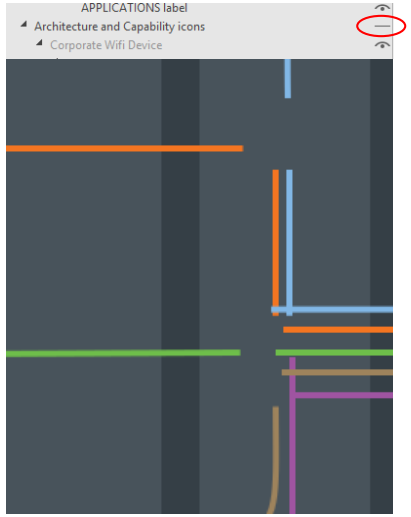


2

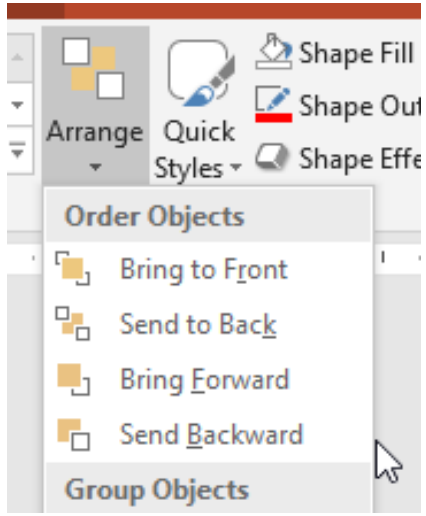


3

4



5

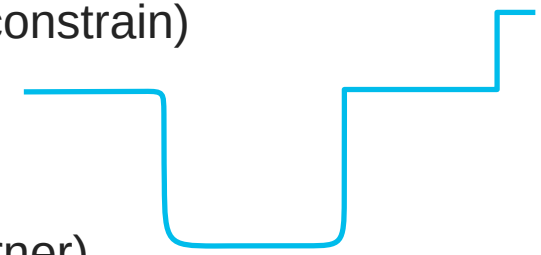


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

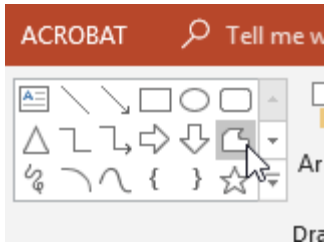
How to draw smooth business flows

By editing the points of a freeform shape you can create smooth consistent corners (steps 1-8).

- Make the line with square turns, click and drag to make each segment (hold shift to constrain)
- Select Edit Shape then Edit Points from the Drawing Tools menu
- Using the gridlines from the View menu, add points before and after (Ctrl+click)
- After adding the new points, then select and delete the corner point
- Stretch handles as appropriate (back to where the corner point was, and the next corner) to create a smooth arching corner

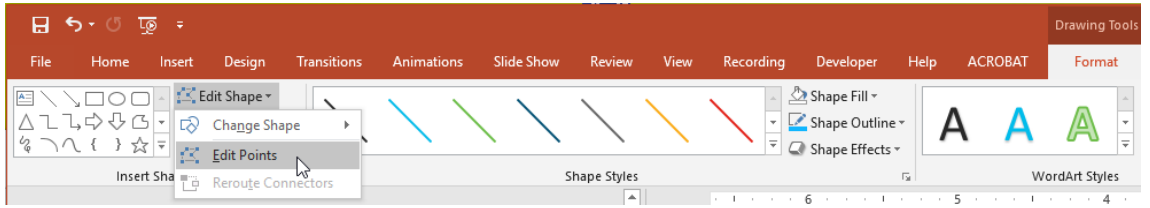


1

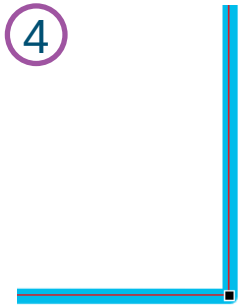


2

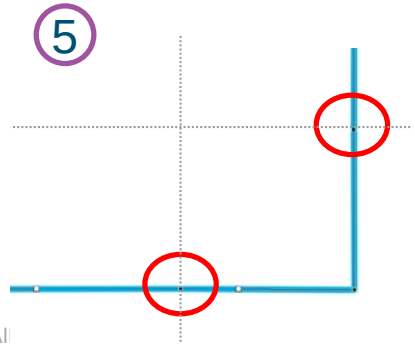
3



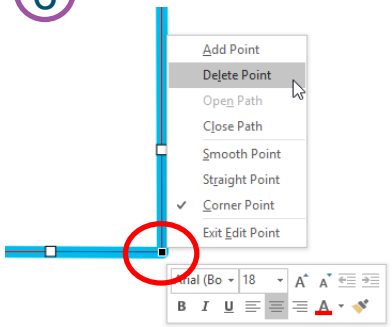
4



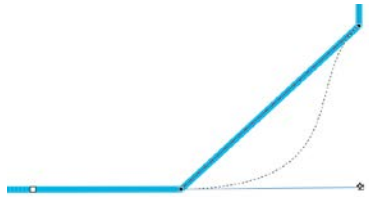
5



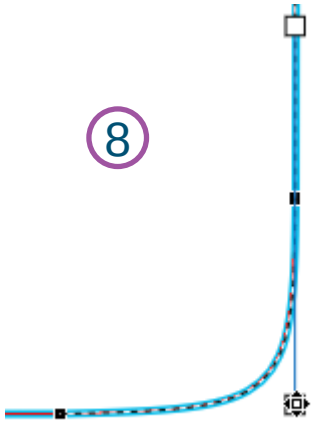
6



7

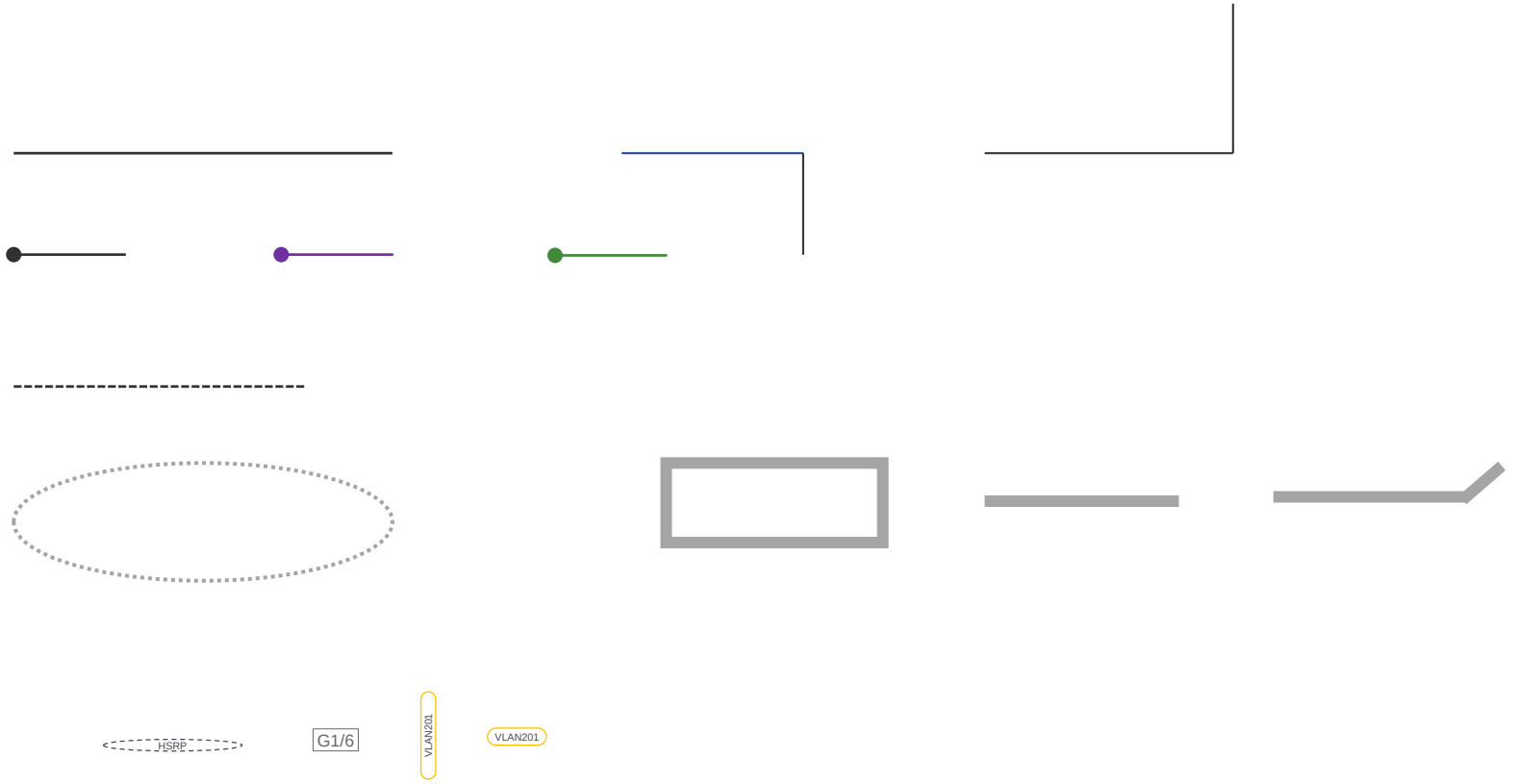


8



ffiliates. Al

Design/Drawing Elements



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

If you have questions about SAFE and constructing SAFE architectures with the resources in this toolkit, contact Christian Janoff. chjanoff@cisco.com

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

CISCO