SAFE Architecture Guide
Places in the Network: Secure Internet Edge

January 2018
Contents

3  Overview
5  Business Flows
8  Threats
9  Security Capabilities
13  Architecture
   Secure Internet Edge 14
15  Attack Surface
   Untrusted Layer 2
   Perimeter Services Layer 17
   Demilitarized Layer 20
   VPN Layer 21
   Trusted Layer 23
24  Summary
25  Appendix
   A Proposed Design 25
26  Suggested Components
Overview

The Secure Internet 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 Internet Edge 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 Internet Edge architecture guide provides:
- Business flows typical for edge locations
- Edge 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.
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 Internet 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

Edge business flows direct the type of functional controls that are used to secure them.

<table>
<thead>
<tr>
<th>Secure Applications</th>
<th>Applications require sufficient security controls for protection.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Remote Access</td>
<td>Secure remote access for employees and third-party partners that are external to the company network.</td>
</tr>
<tr>
<td>Secure Communications</td>
<td>Email, voice, and video communications connect to potential threats outside of company control and must be secured.</td>
</tr>
<tr>
<td>Secure Web Access</td>
<td>Web access controls enforce usage policy and help prevent network infection.</td>
</tr>
</tbody>
</table>

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

Internet 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-internet Edge Capabilities).

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

Figure 5 The Secure Internet Edge Business Flow Capability Diagram

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

The Internet 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 Internet 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 overwhemles the capabilities of a system. These connections overload systems and stops all normal operation.

Data loss

The internet 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 without the knowledge of the parties.

The defense is explained throughout the rest of the document.
Security Capabilities

The attack surface of the internet 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 and defined in Table 1. The placement of these capabilities are discussed in the architecture section.

Figure 6 Secure Internet Edge Attack Surface and Security Capabilities
### Table 1 Secure Internet Edge Attack Surface, Security Capability, and Threat Mapping

<table>
<thead>
<tr>
<th>Internet Edge Attack Surface</th>
<th>Security Capability</th>
<th>Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Human</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users: Remote employees, third parties, customers and administrators.</td>
<td><strong>Identity:</strong> Identity-based access.</td>
<td>Attackers accessing restricted information resources.</td>
</tr>
<tr>
<td><strong>Devices</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clients: N/A Typically, user devices are not physically present within the Internet Edge.</td>
<td><strong>N/A:</strong> Relevant to the policy of the remote user.</td>
<td>Dependent on the environment of remote user, customer, or partner.</td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wired Network: Physical network infrastructure; routers, switches, used to connect trusted, untrusted, perimeter services, VPN, and service layers together.</td>
<td><strong>Firewall:</strong> Stateful filtering and protocol inspection between Internet Edge layers.</td>
<td>Unauthorized access and malformed packets between layers of the Internet Edge.</td>
</tr>
<tr>
<td>Wireless Network: The Internet Edge is used to anchor guest traffic from other PINs to centralize insecure traffic.</td>
<td><strong>Intrusion Prevention:</strong> Blocking of attacks by signatures and anomaly analysis.</td>
<td>Attacks using worms, viruses, or other techniques.</td>
</tr>
<tr>
<td>Analysis: Analysis of network traffic within the Internet Edge layers.</td>
<td><strong>Anti-Malware:</strong> Identify, block, and analyze malicious files and transmissions.</td>
<td>Malware distribution across networks or between servers and devices.</td>
</tr>
<tr>
<td><strong>Threat Intelligence:</strong> Contextual knowledge of existing and emerging hazards.</td>
<td><strong>Flow Analytics:</strong> Network traffic metadata identifying security incidents.</td>
<td>Zero-day malware and attacks.</td>
</tr>
<tr>
<td><strong>Analysis:</strong> Analysis of network traffic within the Internet Edge layers.</td>
<td><strong>Threat Intelligence:</strong> Contextual knowledge of existing and emerging hazards.</td>
<td>Zero-day malware and attacks.</td>
</tr>
<tr>
<td><strong>Flow Analytics:</strong> Network traffic metadata identifying security incidents.</td>
<td><strong>Flow Analytics:</strong> Traffic, telemetry, and data exfiltration from successful attacks.</td>
<td>Traffic, telemetry, and data exfiltration from successful attacks.</td>
</tr>
<tr>
<td>Network (cont.)</td>
<td>Security Capability</td>
<td>Threat</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------</td>
<td>--------</td>
</tr>
<tr>
<td>WAN: Public and untrusted Wide Area Networks that connect to the company, such as the Internet.</td>
<td>DDoS Protection: Protection against scaled attack forms.</td>
<td>Massively scaled attacks that overwhelm services.</td>
</tr>
<tr>
<td></td>
<td>VPN Concentrator: The Internet Edge consolidates remote users for encrypted remote access.</td>
<td>Exposed services and data theft of remote workers and third parties.</td>
</tr>
<tr>
<td></td>
<td>Web Security Appliance: Advanced analysis and filtering of web communications.</td>
<td>Redirection to malicious URLs and data loss.</td>
</tr>
<tr>
<td>Cloud</td>
<td>Cloud Security: Web, DNS, and IP-layer security and control in the cloud for the campus.</td>
<td>Attacks from malware, viruses, and redirection to malicious URLs.</td>
</tr>
<tr>
<td></td>
<td>DNS Security</td>
<td>Redirection of user to malicious website.</td>
</tr>
<tr>
<td></td>
<td>Cloud-based Firewall</td>
<td>Unauthorized access and malformed packets connecting to services.</td>
</tr>
<tr>
<td></td>
<td>Software-Defined Perimeter (SDP/SD-WAN):</td>
<td>Easily collecting information and identities.</td>
</tr>
<tr>
<td></td>
<td>Web Security: Internet access integrity and protections.</td>
<td>Infiltration and ex-filtration via HTTP.</td>
</tr>
<tr>
<td></td>
<td>Web Reputation/Filtering: Tracking against URL-based threats.</td>
<td>Attacks directing to a malicious URL.</td>
</tr>
<tr>
<td></td>
<td>Cloud Access Security Broker (CASB)</td>
<td>Unauthorized access and Data loss.</td>
</tr>
<tr>
<td>Applications</td>
<td>Security Capability</td>
<td>Threat</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------</td>
<td>--------</td>
</tr>
<tr>
<td></td>
<td><strong>Server-Based Security: Anti-virus, anti-malware, firewall, DNS security.</strong></td>
<td>Viruses or malware compromising systems.</td>
</tr>
<tr>
<td></td>
<td><strong>Anti-Malware: Identify, block, and analyze malicious files and transmissions.</strong></td>
<td>Malware distribution across servers.</td>
</tr>
<tr>
<td></td>
<td><strong>Anti-Virus</strong></td>
<td>Viruses compromising systems.</td>
</tr>
<tr>
<td></td>
<td><strong>Cloud Security</strong></td>
<td>Redirection of session to malicious website.</td>
</tr>
<tr>
<td></td>
<td><strong>Host-based Firewall</strong></td>
<td>Unauthorized access and malformed packets connecting to server.</td>
</tr>
<tr>
<td></td>
<td><strong>Email Security: Inspects email communications.</strong></td>
<td>Phishing, MitM, malicious attachments, and data loss.</td>
</tr>
<tr>
<td></td>
<td><strong>TLS Encryption Offload: Accelerated encryption of data services.</strong></td>
<td>Theft of unencrypted traffic.</td>
</tr>
<tr>
<td></td>
<td><strong>Web Application Firewailing: Advanced application inspection and monitoring.</strong></td>
<td>Attacks against poorly developed applications and website vulnerabilities.</td>
</tr>
</tbody>
</table>

**Management**

<table>
<thead>
<tr>
<th>Security Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>These security capabilities are required across all PINs:</td>
</tr>
<tr>
<td>• Identity/authorization</td>
</tr>
<tr>
<td>• Policy/configuration</td>
</tr>
<tr>
<td>• Analysis/correlation</td>
</tr>
<tr>
<td>• Monitoring</td>
</tr>
<tr>
<td>• Vulnerability management</td>
</tr>
<tr>
<td>• Logging/reporting</td>
</tr>
<tr>
<td>• Time synchronization/NTP</td>
</tr>
</tbody>
</table>

Get details on these management security capabilities in the SAFE Management Architecture Guide.
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 Internet Edge architecture is a logical grouping of security and network technology that supports Internet 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 Internet Edge

The Secure Internet 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 Internet Edge Architecture. The Secure Internet 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.
Attacks Surface

The Secure Internet 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.

Business Flows/Functional Controls

- Secure email
- Secure outbound web access
- Corporate employee remote access
- Guest wireless access
- External corporate VPN
- Hosted applications

Primary Security Capability

- DDoS
- Filtering-Router ACLs
- Flow Analytics
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 Internet 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.

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.

Business Flows

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

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 implemented in active/standby mode. This simplifies inspection capabilities and ensures that no traffic loss occurs in the event of a failover.

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.
- Implement an appropriate policy for intrusion prevention, such as Security over Connectivity.
• 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.
• Enable firewall network telemetry functionality by using features such as Network Time Protocol (NTP), logging, and NetFlow.

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.

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.

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.

Guest wireless termination within the Internet edge is detailed in the Campus Wireless LAN Technology Design Guide: http://cvddocs.com/fw/355-14b
Demilitarized Layer

The demilitarized zone (DMZ) is a restricted layer containing both internal and public-facing services. The DMZ has 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 firewalls 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.

Business Flow

- Secure applications

Primary Security Capability

<table>
<thead>
<tr>
<th>Firewall</th>
<th>IPS</th>
<th>Anti-Malware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Intelligence</td>
<td>Flow Analytics</td>
<td>Server-Based Security</td>
</tr>
<tr>
<td>Anti-Virus</td>
<td>Anti-Malware</td>
<td>Cloud Security</td>
</tr>
<tr>
<td>Host-based Firewall</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.

![Diagram showing network components and flows](image)

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.

Remote Access VPN

<table>
<thead>
<tr>
<th>Primary Security Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
</tr>
<tr>
<td>Threat Intelligence</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Primary Security Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMVPN Router</td>
</tr>
</tbody>
</table>

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

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.

Secure connectivity to the Internet 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 Internet 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 Internet edge.

**Design Considerations for the Trusted Layer**

Infrastructure protection plays an important role in the Internet 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](image-url)

**Business Flows**

- Secure email
- Secure outbound web access
- Corporate employee remote access
- Guest wireless access
- External corporate VPN

**Primary Security Capability**

Flow Analytics
Summary

Today’s networks extend to wherever employees are, wherever data is, and wherever data can be accessed. The Internet 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 Internet 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

A Proposed Design

The Secure Internet 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 Internet 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.
Suggested Components

Table 2 SAFE Design Components for Secure Internet Edge

<table>
<thead>
<tr>
<th>Internet Edge Attack Surface</th>
<th>Internet Edge Security</th>
<th>Suggested Components</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Human</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administrators</td>
<td>Identity</td>
<td>Identity Services Engine</td>
</tr>
<tr>
<td>Typically, no humans are physically present in Internet Edge.</td>
<td>Remote Access VPN</td>
<td>AnyConnect</td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wired Network</td>
<td>Firewall</td>
<td>Firepower Appliance</td>
</tr>
<tr>
<td>Routers, Switches</td>
<td></td>
<td>Adaptive Security Appliance</td>
</tr>
<tr>
<td></td>
<td>Intrusion Prevention</td>
<td>Firepower Appliance</td>
</tr>
<tr>
<td>Analysis</td>
<td>Anti-Malware</td>
<td>Advanced Malware Protection for Endpoints</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Advanced Malware Protection for Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Advanced Malware Protection for Email Security Appliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Advanced Malware Protection for Web Security Appliance</td>
</tr>
<tr>
<td>WAN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DDoS Protection</td>
<td>Threat Intelligence</td>
<td>Firepower Appliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Adaptive Security Appliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Aggregation Services Router</td>
</tr>
<tr>
<td>VPN Concentrator</td>
<td>Flow Analytics</td>
<td>Nexus and Catalyst Switch</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Integrated Services Router</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Aggregation Services Router</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cisco Partner</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Integrated Services Router</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Aggregation Services Router</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Firepower Appliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Adaptive Security Appliance</td>
</tr>
<tr>
<td>Internet Edge Attack Surface</td>
<td>Edge Security</td>
<td>Suggested Components</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------</td>
<td>----------------------</td>
</tr>
</tbody>
</table>
| Network (cont.)             | 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 |
|                             | Web Security: Internet access integrity and protections. | Firepower virtual URL  
Cisco Umbrella Secure Internet Gateway (SIG) |
|                             | Web Reputation/Filtering: Tracking against URL-based threats. | Web Security Appliance  
Cloud Web Security  
Meraki |
|                             | Cloud Access Security Broker (CASB) | Cloudlock |
| Applications                | Web Security | Firepower URL  
Web Security Appliance  
Umbrella Secure Internet Gateway (SIG) |
| Service                     | Server-Based Security | Cisco AMP  
Cisco Umbrella |
|                             | Web Application Firewalling | Cisco Partner |
|                             | TLS Encryption Offload | Cisco Partner |
|                             | Email Security | Email Security Appliance |
For more information on SAFE, see www.cisco.com/go/SAFE.