SAFE Security Architecture Toolkit

Table of Contents

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

The following slides contain graphics that you can use to introduce SAFE and explain SAFE concepts and components.
The Key to SAFE
SAFE Progression of Capabilities
SAFE Architecture Wheel
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.
SAFE Master Capabilities Flows

Third-Party Business Flows:

**Secure remote access for third party:** Connected device with remote vendor support
- Thermostat
- Thermo
- Secure remote access for third party
- Thermostat
- Connected device with remote vendor support
- Virtual Private Network
- Posture Assessment
- Identity
- Remote Technician

**Secure remote access for employees:** Field engineer updating work order
- Engineer
- Secure remote access for employees
- Field engineer updating work order
- Virtual Private Network
- Posture Assessment
- Identity
- Workflow Application

**Secure east-west traffic for compliance:** PCI compliance for financial transactions
- Database
- Secure east-west traffic for compliance
- PCI compliance for financial transactions
- Firewall
- Intrusion Prevention
- Flow Analytics
- Threat Intelligence
- Anti-Malware
- Tagging
- Distributed Denial of Service Protection
- Web Application Firewall
- Server-Based Security
- Payment Application

© 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.
SAFE Architecture Diagrams

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

HUMAN

Secure Email
- CEO sending email to Shareholders

Guest Wireless
- Guest browsing
- Employee Phone

Secure Web
- Employee browsing

Secure Communications
- Subject Matter Expert

Secure Third Parties
- Building Controls

APPLICATIONS

WEB SECURITY
- Web Security
- Guest Wireless

Router
- Wholesaler Website
- Comparative Shopping Website
- Third-party Technician accessing logs

Wholesaler Website
- Employee browsing

Comparative Shopping Website
- Guest browsing

Wholesale Website
- Shareholder receiving email from CEO
- CEO sending email to Shareholders

Router
- Secure Email
- Secure Web
- Secure Communications
- Secure Third Parties

Router
- Corporate Wi-Fi Device

Router
- Corporate Device

Router
- Mobile Device

Router
- Wireless Access Point

Router
- Wireless Controller

Router
- Firewall

Router
- Switch

Router
- Core Switch

Router
- Blade Server

Router
- Communications Manager

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Wireless

Router
- Wireless Access Point

Router
- Wireless Controller

Router
- Firewall

Router
- Switch

Router
- Core Switch

Router
- Blade Server

Router
- Communications Manager

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core

Router
- Services

Router
- Distribution

Router
- Core
TO CAMPUS/BRANCH TO DATA CENTER

Services

Payment Processing
Third-party Technician accessing logs
Shareholder receiving email from CEO
Comparative Shopping Website
Wholesaler Website

CEO sending email to Shareholders
Building Controls
Clerk processing credit card

Switch Firewall Switch

Router

WAN Architecture

Guest browsing
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

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

Switch Firewall Switch

Router

NETWORK

TO CAMPUS/BRANCH TO DATA CENTER
Data Center Architecture

APPLICATIONS
-东/西流量
-支付处理
-工作流应用
-股东通讯服务

SERVERS
-数据库
-安全服务器
-支付应用
-工作流自动化
-股东通讯服务

APPLICATIONS
-数据中心架构
-网络
-服务器
-应用

NETWORK
-无线控制器
-防火墙
-通信管理器
-核心交换机
-分布交换机
-安全服务器
-负载均衡器
-控制器
-堆叠交换机
-防火墙
-核心交换机
-身份服务器
-分布式交换机
-防火墙
-核心交换机
-管理控制台
-无线控制器
-分配器
-交换机
-防火墙
-分配器
-交换机
-防火墙

TO EDGE
-第三方技术员访问日志
-批发商网站
-股东收到CEO的电子邮件
-比较商城

TO WAN
- BPMN
-数据中心架构
-网络
-服务器
-应用

TO EDGE
-客户处理信用卡
-建筑控制系统
-CEO发送股东电子邮件
-员工浏览

TO WAN
- BPMN
-数据中心架构
-网络
-服务器
-应用

TO EDGE
-客户处理信用卡
-建筑控制系统
-CEO发送股东电子邮件
-员工浏览

TO WAN
- BPMN
-数据中心架构
-网络
-服务器
-应用
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.
SAFE Icon Library

If you need to customize SAFE capabilities flows or architectures, you’ll find the icons on the following slides.
## Human Icons

<table>
<thead>
<tr>
<th>Attack Surface</th>
<th>Threat</th>
<th>Capability Icons</th>
<th>Architecture Icons</th>
<th>Cisco Product</th>
</tr>
</thead>
</table>
• Cisco Identity Services Engine Virtual Appliance |
# Additional Humans Icons

## Optional Endpoints

<table>
<thead>
<tr>
<th>Role</th>
<th>Icon</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEO</td>
<td></td>
</tr>
<tr>
<td>Clerk</td>
<td></td>
</tr>
<tr>
<td>Customer</td>
<td></td>
</tr>
<tr>
<td>Expert</td>
<td></td>
</tr>
<tr>
<td>Guest</td>
<td></td>
</tr>
<tr>
<td>Manager</td>
<td></td>
</tr>
<tr>
<td>Remote Employee</td>
<td></td>
</tr>
<tr>
<td>Secure Partner</td>
<td></td>
</tr>
<tr>
<td>Shareholder</td>
<td></td>
</tr>
</tbody>
</table>

## Identity Directory

- Identity Directory
- Identity Directory
- Identity Directory

## Generic Icons

- People
- People

## Third-Party Icons

- MS Active Directory
- MS Active Directory

## Other Icons

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

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

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
<table>
<thead>
<tr>
<th>Attack Surface</th>
<th>Threat</th>
<th>Capability Icons</th>
<th>Architecture Icons</th>
<th>Cisco Product</th>
</tr>
</thead>
</table>
| Voice: Phone          | Rogue: Attacker accessing private information. | ![phone](phone.png) | ![Phone](phone.png) | • Cisco Unified Communications  
  • Cisco IP Phones            |
| Video: Displays, collaboration, smartboards. | Rogue: Attacker accessing private information. | ![Video Endpoint](video_endpoint.png) | ![Video Endpoint](video_endpoint.png) | • Cisco Unified Communications  
  • Cisco Telepresence  
  • Cisco WebEx Teams  
  • Cisco IP Phones            |
| Autonomous Device: Building controls, manufacturing systems, automation. | Rogue: Attacker accessing private information. | ![sensor](sensor.png) | ![Environmental Controls](environmental_controls.png) | • Partner devices and controllers |
## Additional Devices Icons

### Optional Endpoints

- Corporate Device
- Corporate Wireless Device
- Mobile
- Phone
- Video Endpoint
- Actuator
- Sensor
- Automated System

### Generic Icons

- Server
- Building Controls
- Server
- Camera
- Building Controls

### Third-Party Icons

- Corporate Device
- Corporate Wireless Device
- Mobile
- Phone
- Video Endpoint
- Actuator
- Sensor
- Automated System

### Other Icons

- Standardized System Images
- Infrastructure Redundancy
## Network Icons

<table>
<thead>
<tr>
<th>Attack Surface</th>
<th>Threat</th>
<th>Capability Icons</th>
<th>Architecture Icons</th>
<th>Cisco Product</th>
</tr>
</thead>
</table>
| 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 |
• 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 |
### Network Icons

<table>
<thead>
<tr>
<th>Attack Surface</th>
<th>Threat</th>
<th>Capability Icons</th>
<th>Architecture Icons</th>
<th>Cisco Product</th>
</tr>
</thead>
</table>
| Wireless Network: Physical network infrastructure; access points and controllers used to connect mobile devices to the access layer. | Malware: Compromised devices connecting to infrastructure. | Mobile Device Management (MDM): Endpoint access control based on policies. | MDM Appliance | - Cisco Identity Services Engine  
- Cisco Meraki Mobile Device Management |
- Cisco Wireless Controller and Access Points  
- Cisco Mobility Services Engine |
- Cisco Wireless Controller and Access Points |
# Network Icons

<table>
<thead>
<tr>
<th>Attack Surface</th>
<th>Threat</th>
<th>Capability Icons</th>
<th>Architecture Icons</th>
<th>Cisco Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analysis: Telemetry and analysis of traffic across the enterprise.</td>
<td>Malware: Malware distribution across networks or between servers and devices.</td>
<td>Anti-Malware for Networks: Identify, block, and analyze malicious files and transmissions.</td>
<td>Firewall</td>
<td>• Cisco Advanced Malware Protection for Networks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Cisco Next Generation Firewall</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Cisco Next Generation Firewall Virtual</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Cisco Next Generation Intrusion Prevention System</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Cisco Next Generation Intrusion Prevention System Virtual</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Advanced Threat: Zero-day malware and attacks.</td>
<td>Threat Intelligence: Contextual knowledge of emerging hazards.</td>
<td>Threat Intelligence</td>
<td>• Cisco Collective Security Intelligence</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Cisco Global Threat Analytics and Encrypted Traffic Analytics</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Cisco Talos Security Intelligence</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Cisco Firepower Management Center</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Cisco Umbrella Investigate</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Cisco AMP Console – Telemetry</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Cisco Stealthwatch Management Console</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Cisco Stealthwatch Flow Sensor Analysis:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Cisco Stealthwatch Management Console</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Cisco Stealthwatch Cloud</td>
</tr>
</tbody>
</table>

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
<table>
<thead>
<tr>
<th>Attack Surface</th>
<th>Threat</th>
<th>Capability Icons</th>
<th>Architecture Icons</th>
<th>Cisco Product</th>
</tr>
</thead>
</table>
| WAN: Public and untrusted Wide Area Networks that connect to the company, such as the Internet. | Exfiltration: Traffic, telemetry, and data exfiltration from successful attacks. | VPN Concentrator: Encrypted remote access. | 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. | 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. | DDOS Protection Appliance | • Cisco Aggregation Services Routers with Radware  
• Cisco Firepower Appliance with Radware  
• Distributed Denial of Service Technology Partner |
## Network Icons

<table>
<thead>
<tr>
<th>Attack Surface</th>
<th>Threat</th>
<th>Capability Icons</th>
<th>Architecture Icons</th>
<th>Cisco Product</th>
</tr>
</thead>
</table>
| Cloud: Security services from the cloud. | Phish Link: Attacks from malware, viruses, and malicious URLs. | Cloud Security: Combination icon representing several security capabilities provided by the cloud. | VPN Concentrator | • 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 |
<p>| Phish Link: Redirection of user to malicious website. | DNS Security: Name resolution filtering. | Secure DNS | Secure DNS |
| Rogue: Unauthorized access to cloud SaaS services, data loss. | Cloud Access Security Broker (CASB): Monitor and protect SaaS services. | CASB | • Cisco CloudLock |</p>
<table>
<thead>
<tr>
<th>Attack Surface</th>
<th>Threat</th>
<th>Capability Icons</th>
<th>Architecture Icons</th>
<th>Cisco Product</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Cisco Web Security Virtual Appliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Cisco Meraki URL Filtering</td>
</tr>
<tr>
<td></td>
<td>Malware C2: Attacks directing to a malicious URL.</td>
<td>Web Reputation/Filtering: Tracking against URL-based threats.</td>
<td>Web Reputation Filtering</td>
<td>• Cisco Umbrella - Secure Internet Gateway (SIG)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Cisco Web Security Virtual Appliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Cisco Meraki URL Filtering</td>
</tr>
<tr>
<td></td>
<td>Redirect Link: Unauthorized access and malformed packets connecting to services.</td>
<td>Cloud-based Firewall: Filter and inspect traffic via the cloud.</td>
<td></td>
<td>• Cisco Adaptive Security Virtual Appliance (ASAv)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Cisco Cloud Services Router</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Cisco Next Generation Firewall Virtual (NGFWv)</td>
</tr>
</tbody>
</table>
Additional Network Icons

<table>
<thead>
<tr>
<th>Firewall</th>
<th>Intrusion Prevention</th>
<th>Router</th>
<th>VPN Concentrator</th>
<th>DDOS Protection</th>
<th>Identity Directory</th>
<th>Web Security</th>
<th>Web Filtering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>IPS</td>
<td>Router</td>
<td>VPN Concentrator</td>
<td>DDOS Protection</td>
<td>Identity Directory</td>
<td>Web Security</td>
<td>Web Filtering</td>
</tr>
</tbody>
</table>

Generic Icons | Third-Party Icons | Other Icons

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Additional Network Icons
Additional Network Icons
# Applications Icons

<table>
<thead>
<tr>
<th>Attack Surface</th>
<th>Threat</th>
<th>Capability Icons</th>
<th>Architecture Icons</th>
<th>Cisco Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications: Application-specific security services.</td>
<td>Redirect Link: Attacks against poorly-developed applications.</td>
<td>Web Application Firewalling: Advanced application inspection and monitoring.</td>
<td>Web Application Firewall</td>
<td>• Web Application Firewall Technology Partner</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| C2 Sites: Attack tools hiding in permitted applications. | Application Visibility Control (AVC): Deep packet inspection of application flows. | | | • 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 Appliance | | • Cisco Next Generation Firewall
• Transport Layer Security Offload Technology Partner |
### Applications Icons

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

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

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

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

Generic Icons | Third-Party Icons | Other Icons
---|---|---
[Generic Appliance] | [Cisco Appliance] | [Cisco AnyConnect]
[Radware Appliance] | [Radware Appliance] | [Cisco Alerter]
## Management Icons

<table>
<thead>
<tr>
<th>Attack Surface</th>
<th>Threat</th>
<th>Capability Icons</th>
<th>Architecture Icons</th>
<th>Cisco Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management: Infrastructure systems management and orchestration.</td>
<td>Analysis/Correlation: Security event management of real-time information.</td>
<td>SIEM</td>
<td>SIEM</td>
<td>• Cisco Stealthwatch&lt;br&gt;• Cisco Stealthwatch Cloud&lt;br&gt;• Cisco Visibility&lt;br&gt;• SIEM Technology Partner Products</td>
</tr>
<tr>
<td>Anomaly Detection: Identification of infected hosts scanning for other vulnerable hosts.</td>
<td>Anomaly Detection</td>
<td></td>
<td></td>
<td>• Cisco Identity Services Engine&lt;br&gt;• Cisco Meraki&lt;br&gt;• Cisco Tetration&lt;br&gt;• Cisco Stealthwatch</td>
</tr>
<tr>
<td>Identity/Authorization: Centralized identity and administration policy.</td>
<td>Identity/Authorization</td>
<td></td>
<td>Identity Directory</td>
<td>• Cisco Identity Services Engine</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Attack Surface</th>
<th>Threat</th>
<th>Capability Icons</th>
<th>Architecture Icons</th>
<th>Cisco Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management: Infrastructure</td>
<td>Management and orchestration.</td>
<td>Logging/Reporting: Centralized event information collection.</td>
<td>Log Collector</td>
<td>• Cisco Stealthwatch</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Logging Technology Partner Products</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name Resolution:</td>
<td>Centralized DNS Services</td>
<td>Secure DNS</td>
<td>Secure DNS</td>
<td>• Cisco Umbrella</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Management Icons

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

|------------|-----|------------|--------------------------|--------|--------------|------|-------------------|

Generic Icons | Third-Party Icons | Other Icons
---|---|---
Generic Appliance | | |
Tools and Rules

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

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

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.

Do

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.

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.

Do

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.
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.
How to draw smooth business flows

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

1. Make the line with square turns, click and drag to make each segment (hold shift to constrain)
2. Select Edit Shape then Edit Points from the Drawing Tools menu
3. Using the gridlines from the View menu, add points before and after (Ctrl+click)
4. After adding the new points, then select and delete the corner point
5. Stretch handles as appropriate (back to where the corner point was, and the next corner) to create a smooth arching corner
If you have questions about SAFE and constructing SAFE architectures with the resources in this toolkit, contact Christian Janoff. chjanoff@cisco.com