SAFE Operations Guide
Domain: Segmentation

July 2019
Contents

3 The Challenge

4 Overview

6 Segmentation Defined
   Entity Segmentation 7
   Data Segmentation 8
   Traffic Segmentation 9

10 Attack Surface and Segmentation Capabilities
   Humans 11
   Devices 12
   Network 13
   Applications 14

15 Segmentation Considerations

16 Business Flows
   PCI Use Case Example 16

23 Summary

24 Suggested Components

26 References
The Challenge

Cybercriminals are stealing company intellectual property, resources, and money. These valuable assets are like jewels and need protection.

Segmentation is the act of creating barriers around these assets to guard them.

Segmentation, Then and Now

In the past, threats were considered external. Building a security perimeter was good enough to protect a company’s property and resources.

That mindset has rapidly evolved along with the severity of today’s cyber threats. Now the challenge of connecting any user on any device across any network to any application increases the complexity of segmentation.

Applying these basic concepts protects an organization’s attack surface:

- The identity of every human must be authenticated based on the permissions of their individual role.
- Every device or thing on the network must be authenticated and policies applied based on its identity and posture.
- The network is assumed to be hostile from internal as well as external threats.
- Application enforcement happens across services, sessions, transactions, and storage.
- Asset protection using automated policy enforcement is a sign of mature and successful segmentation.
Overview

Segmentation is one of the six Operational Domains within SAFE. SAFE is a holistic approach where Operational Domains represent the functioning aspects of the physical infrastructure modeled by the Secure Places in the Network (PINs).

Although SAFE recommends that these operational layers be thought of as a progression stack, it is important to realize that all of these domains are active concurrently and heavily interdependent.

The SAFE Key illustrates how segmentation supports an overall threat defense of a company:

- First, Management identifies humans, devices, networks, and applications.
- Second, Visibility observes threats on the network.
- Segmentation creates secure partitions across entities, data, and traffic. These partitions restrict access based on role, function, and policy.
- Threat Defense provides accurate and timely threat response to reinforce segmentation policy dynamically, as reputations are augmented by the visibility of new threats.

There is no silver bullet for segmentation; as a practice and concept, it is maturing from static to automated.

The SAFE Segmentation operations guide provides:

- A segmentation model
- Technical considerations
- A business use case
- Recommended products

Figure 1 The Key to SAFE. SAFE provides the Key to simplify cybersecurity into Secure Places in the Network (PINs) for infrastructure and SAFE Operational Domains for 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. The SAFE Overview Guide introduces the SAFE model and method. It supports the Architecture, Design, and Operations Guides that provide specific guidance in each area.
Segmentation Defined

Segmentation creates secure partitions for entities, data, and traffic on the network.

Segmentation can be simplified by thinking about these three classifications:

- **Entities** are humans, devices, networks, and applications.
- **Data** is information *at rest* on devices, networks, and applications.
- **Traffic** is data *in motion* between devices, networks, and applications.

Figure 3 The SAFE Segmentation Model. Entities, Data, and Traffic must be securely partitioned across the attack surface.
Entity Segmentation

Entities are humans, devices, networks, and applications which represent the attackable surface.

Entity segmentation comprises identity and posture assessment according to policy:

- The identity of a person or device is established using authentication and authorization.
- Posture assessments verify that the system is policy-compliant, properly patched to participate in the appropriate segments, and not infected.

Examples of entities:

**HUMAN**
- Doctors
- Clerks
- Managers
- Administrators
- Employees

**DEVICES**
- Laptops
- Smartphones
- Tablets
- Sensors
- Servers

**NETWORK**
- Firewalls
- Routers
- Switches
- Access Points
- Cloud IaaS

**APPLICATIONS**
- Payments
- Payroll
- Workforce Automation
- E-commerce
- Email

*Figure 4 Entity segmentation securely partitions Humans, Devices, Networks, and Applications based on policy.*
Data Segmentation

Data is information at rest that is segmented on devices, networks, and applications.

Data segmentation techniques can be logical or physical:

• Data can be segmented logically or physically.
• Logical separation allows segmented utilization of shared resources (e.g., disk encryption, virtual storage device, data store, drive partition, encrypted tables).
• Physical separation relies on dedicated hardware for each data storage need (e.g., multiple hard drives).

Figure 5 Data Segmentation secures data at rest on Devices, Networks, and Applications.
Traffic Segmentation

Traffic is data in motion between devices, networks and applications.

Traffic best practices:

- Companies must ensure separation of traffic flows (line of business, role-based, physical, etc.) for many purposes, including regulating information movement, network resource consumption, and threat reduction.
- Classify traffic (e.g., TCP/UDP port, packet header, IP address) and apply a particular policy to manipulate traffic physically or logically (e.g., allow traffic to go from A to B, but not A to C).
- Multiple policies are used consistently in different parts of the network by leveraging traffic classification conveyed via explicit marking, flow tables, state tables (e.g., group tagging, VLAN, ACL, VPN).
- Implement controls to facilitate appropriate differentiated entity access using enforcement mechanisms (e.g., VLANs, subnets, firewall rules).
Attack Surface and Segmentation Capabilities

SAFE maps segmentation types to the attack surface. The attack surface is defined by the business flow and the entities present across it. The security capabilities needed to segment these flows are mapped in Figure 7.

Segmentation security capabilities are listed throughout the sections below. The placement of these capabilities are discussed in the architecture section.
Human

Humans are entities such as employees, customers, and remote access users such as partners who provide assigned identity information to their devices for access.

All people must be considered potentially bad actors. Exploitation of Trust attacks happen most frequently at this layer through credential theft. Credential management of employees, partners, and customers with effective role-based segmentation helps minimize the risk of this threat.

Administrators have more authority than normal users. The systems they access must require additional controls like two-factor authentication, limited access to job function, and logging of their changes.

Humans with access to sensitive data should also be required to use similar added controls when identifying themselves following the policy of least-privilege access.

<table>
<thead>
<tr>
<th>Organization Attack Surface</th>
<th>Segmentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human</td>
<td>Type</td>
</tr>
<tr>
<td></td>
<td>Entity</td>
</tr>
</tbody>
</table>

Users: Employees, third parties, customers, and administrators.

Multi-Factor Authentication in addition to passwords (something the user knows), i.e., something the user is (fingerprint) or something the user has (push notification code).
Devices

Device entities include laptops, smart phones, tablets, sensors, and servers.

In contrast to Humans who can only be classified as entities, a device can store data and transmit/receive traffic. Devices participate in all three areas of segmentation as illustrated in Figure 9.

Segmentation at the device level is necessary to prevent the spread of threats across the network from an infected system by a zero-day attack. For example, administrators must separate building control systems from user devices.

Table 2 Devices

<table>
<thead>
<tr>
<th>Organization Attack Surface</th>
<th>Segmentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices</td>
<td></td>
</tr>
<tr>
<td><strong>Endpoints</strong></td>
<td><strong>Type</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Capability</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Identity:</strong> Device-specific identity information and context.</td>
</tr>
<tr>
<td></td>
<td><strong>Posture Assessment:</strong> Client endpoint compliance verification and authorization.</td>
</tr>
<tr>
<td></td>
<td><strong>Data:</strong> Disk Encryption: Encryption of data at rest.</td>
</tr>
<tr>
<td></td>
<td><strong>Traffic:</strong> VPN: Encrypted communication tunnels between entities.</td>
</tr>
<tr>
<td></td>
<td><strong>Traffic:</strong> Host Firewall: Stateful filtering and protocol inspection between entities.</td>
</tr>
</tbody>
</table>

Figure 9 Devices can be segmented by Entity, Data, and Traffic based on their activity.
Network

Network entities include firewalls, routers switches, wireless, cloud IaaS, and other devices that send and receive traffic. Network devices are entities that can store data and transmit/receive traffic, and therefore participate in all three areas of segmentation as illustrated in Figure 10.

Table 3 Network

<table>
<thead>
<tr>
<th>Organization Attack Surface</th>
<th>Segmentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td></td>
</tr>
<tr>
<td>Wired Network: Physical network infrastructure; routers, switches, used to connect access, distribution, core, and services layers together.</td>
<td>Entity</td>
</tr>
<tr>
<td>Mobile Device Management (MDM): Evaluation of the state of the device.</td>
<td>Entity</td>
</tr>
<tr>
<td>Cloud Access Security Broker (CASB): Contextual policy enforcement for cloud services.</td>
<td>Entity</td>
</tr>
<tr>
<td>Disk Encryption: Encryption of data at rest.</td>
<td>Data</td>
</tr>
<tr>
<td>Tagging: Software-based segmentation using EPGs/SGT/VLANs.</td>
<td>Traffic</td>
</tr>
<tr>
<td>Firewall: Stateful filtering and protocol inspection between entities.</td>
<td>Traffic</td>
</tr>
<tr>
<td>Software-Defined Perimeter (SDP/SD-WAN): Dynamic, multi-point encrypted communications fabric.</td>
<td>Traffic</td>
</tr>
</tbody>
</table>

Segmentation at the network level is necessary to prevent the spread of threats across the network as well as to separate different classifications of data and their business-relevant value from each other.

For example, administrators must separate payment and financial systems from personal identifiable information or proprietary intellectual property.
Applications

Examples of Applications entities are payments, payroll, workforce automation, e-commerce, email, etc.

Applications are entities on servers that can both store data and transmit/receive traffic, and therefore participate in all three areas of segmentation as illustrated in Figure 11.

Table 4 Application

<table>
<thead>
<tr>
<th>Organization Attack Surface</th>
<th>Segmentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td></td>
</tr>
<tr>
<td><strong>Entity</strong></td>
<td><strong>Identity</strong>: Identity-based access.</td>
</tr>
<tr>
<td><strong>Posture Assessment</strong></td>
<td><strong>Server compliance verification, authorization, and patching.</strong></td>
</tr>
<tr>
<td><strong>Data</strong></td>
<td><strong>Storage Encryption</strong>: Encryption of data at rest in tables and databases.</td>
</tr>
<tr>
<td><strong>Traffic</strong></td>
<td><strong>Traffic Encryption Offload</strong>: Accelerated encryption of traffic services.</td>
</tr>
<tr>
<td><strong>Application Firewalling</strong></td>
<td><strong>Web Application Firewalling</strong>: Advanced application inspection and monitoring.</td>
</tr>
</tbody>
</table>

Segmentation of applications at the session level is necessary to ensure the attack surface is minimized. If not supported by the application natively, a web application firewall (WAF) can add this capability.

Storage of application data must be encrypted to protect it in local and cloud deployments. Techniques for reducing the attack surface include proper key management and rotation.

For example, payment card security requires each transaction session to be encrypted plus all data at rest must be encrypted.
Segmentation Considerations

The industry is moving away from manual segmentation and toward segmentation that is automated, adaptive, and holistically coordinated.

Cisco recommends a tiered approach to trusted segmented access:

1. Verify identity for any user; verify hygiene for any device.
3. Grant easier, safer access to specific workload apps.
4. Segment the network via software-defined access.
5. Implement consistent data access policy management.
6. Remediate network, cloud, and endpoint threats or Common Vulnerabilities and Exposures (CVE).
Business Flows

PCI Use Case Example

Segmentation should restrict the flow of data. You can place appropriate controls for your particular use case by identifying where the source and destination of each flow of data traverses, tracking its journey from the Humans to Devices to the Network and to Applications.

For example, consider the secure business flow for PCI applications below. The data flow must be isolated from end to end: from the human clerk, the payment card device within a branch, across the WAN, and into the data center, ending in the payment application.

Figure 14 The PCI Business Flow

After isolating the data flow, apply the capabilities that are appropriate for your use case across the entities, data, and traffic. Using this method, you can ensure controls are in place as the flow traverses to restrict the scope of the data (as described in Figure 13).

Figure 15 Segmentation capabilities for the PCI business flow.
Segmentation Across the Enterprise

Everything in your organization is open to attack without segmentation. Without segmentation controls, all humans, devices, networks, and applications that are compromised by an attack can be used to compromise everything else.

![Diagram of SAFE architecture and all business flows.](image1)

*Figure 16* The SAFE architecture and all business flows.

However, when you use segmentation across your entities, devices, networks, and applications, you can isolate the business flow from the rest of your network to defend it.

![Diagram of PCI business flow segmented from the rest of the network.](image2)

*Figure 17* The PCI business flow segmented from the rest of the network.
The Branch to the Data Center

The PCI business flow begins with the humans in the branch.

Figure 18 The Human Clerk is the source of the PCI business flow.

To segment the human entity, use appropriate controls such as user name and password to identify employees with access to credit card devices.

Figure 19 Identity controls are used to segment the Human Entity.
Next, the payment device require all three segmentation controls: identity for the device entity, encryption for the data at rest, and host-based firewall for traffic to and from the device.

![Figure 20 Payment card device segmentation for Entity, Data, and Traffic.](image)

The network in the branch assures the payment device conforms to policy using a posture assessment from the switch. The network entities are segmented using identity controls. Firewalls and tagging assure the PCI business flow does not co-mingle with other business flows by putting the PCI traffic onto its own subnet/VLAN, enforced by firewalling and tagging.

![Figure 21 The branch network segmented for Entity, Data, and Traffic.](image)
Leaving the branch, the PCI traffic flow moves to the Wide Area Network (WAN) as it travels to the data center.

![Diagram showing traffic flow from branch to data center](image)

**Figure 22** The PCI business flow travels from the branch to the WAN.

The WAN entities are segmented using identity controls. Firewalls and tagging assure the PCI business flow does not co-mingle with other business flows by putting the PCI traffic onto its own subnet/VLAN.

![Diagram showing segmentation of WAN entities](image)

**Figure 23** The WAN is segmented using identity and traffic controls.
Leaving the WAN, the PCI traffic flow enters the data center.

The virtualized data center is segmented using the same methodology as the branch with its physical equipment. The network in the data center assures the payment system conforms to policy using a posture assessment from the switch. The network entities are segmented using identity controls. Firewalls and tagging assure the PCI business flow does not co-mingle with other business flows by putting the PCI traffic onto its own subnet/VLAN, enforced by firewalls and tagging.
Finally, the application data is encrypted.

![Diagram](image)

**Figure 26** Data from the PCI flow is encrypted at the application data layer.

When isolated and segmented using these best practices, the data within your business flows will be protected.

![Diagram](image)

**Figure 27** The PCI business flow segmented from the rest of the network.
Summary

Segmentation is evolving. In the past, businesses focused primarily on the network perimeter. Today they’re looking for a holistic model that applies controls to their users, devices, networks, applications, and application processes. Although a comprehensive zero-trust design may not be achievable yet, this SAFE Segmentation Operations Guide provides the concepts and capabilities that can help your organization develop an appropriate segmentation solution.

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

<table>
<thead>
<tr>
<th>Segmentation Attack Surface</th>
<th>Segmentation Capability</th>
<th>Suggested Cisco Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human</td>
<td>Users</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Identity</td>
<td>Identity Services Engine</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Meraki Management</td>
</tr>
<tr>
<td></td>
<td>Multi-Factor Authentication</td>
<td>Cisco Duo</td>
</tr>
<tr>
<td>Devices</td>
<td>Endpoints</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Identity</td>
<td>Identity Services Engine (ISE)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Industrial Network Director</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AnyConnect Agent</td>
</tr>
<tr>
<td></td>
<td>Host Firewall</td>
<td>Cisco Tetration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device OS</td>
</tr>
<tr>
<td></td>
<td>VPN</td>
<td>AnyConnect Agent</td>
</tr>
<tr>
<td></td>
<td>Disk Encryption</td>
<td>Device OS</td>
</tr>
<tr>
<td></td>
<td>Posture Assessment</td>
<td>AnyConnect Agent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Identity Services Engine (ISE)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Meraki Mobile Device</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Management</td>
</tr>
</tbody>
</table>
### Table 5 SAFE Design Components for Segmentation (continued)

<table>
<thead>
<tr>
<th>Segmentation Attack Surface</th>
<th>Segmentation Capability</th>
<th>Suggested Cisco Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Network Systems</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Firewall</td>
<td>Firepower Appliance, Adaptive Security Appliance (ASA)</td>
</tr>
<tr>
<td></td>
<td>Tagging</td>
<td>Nexus/Catalyst Switch VLANs Centralized Identity Services Engine TrustSec Application Centric Infrastructure (ACI) Endpoint Group (EPG)</td>
</tr>
<tr>
<td></td>
<td>Mobile Device Management (MDM)</td>
<td>Meraki Device Manager Identity Services Engine (ISE)</td>
</tr>
<tr>
<td></td>
<td>Cloud Access Broker</td>
<td>Cisco Cloudlock</td>
</tr>
<tr>
<td></td>
<td>Disk Encryption</td>
<td>Web Security Appliance (WAS) Email Security Appliance (ESA) Content Delivery (CDA)</td>
</tr>
<tr>
<td></td>
<td>Software-Defined Perimeter (SDP/SD-WAN)</td>
<td>AnyConnect Agent Cisco Viptela Meraki MX</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Applications</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>TLS Encryption Offload</td>
</tr>
<tr>
<td></td>
<td>Web Application Firewalls</td>
</tr>
<tr>
<td></td>
<td>Identity</td>
</tr>
<tr>
<td></td>
<td>Host Firewall</td>
</tr>
<tr>
<td></td>
<td>Disk Encryption</td>
</tr>
<tr>
<td></td>
<td>Posture Assessment</td>
</tr>
</tbody>
</table>
References

A Framework to Protect Data Through Segmentation


Cisco TrustSec—Software-Defined Segmentation

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