Device Access Security

Privilege Level Passwords

Privilege Level Passwords

Level 0:

- Most restricted
- 5 available commands

Level 1 (User Level):

- Read-only commands

Level 15 (Privileged Level):

- Complete device control

Privilege Level Passwords

Least Privilege Principle:

Users should only have the minimum level of access necessary to perform their job duties.

- Helpdesk support staff
- Junior admins
- Senior engineers

Line Passwords

CTY Line:

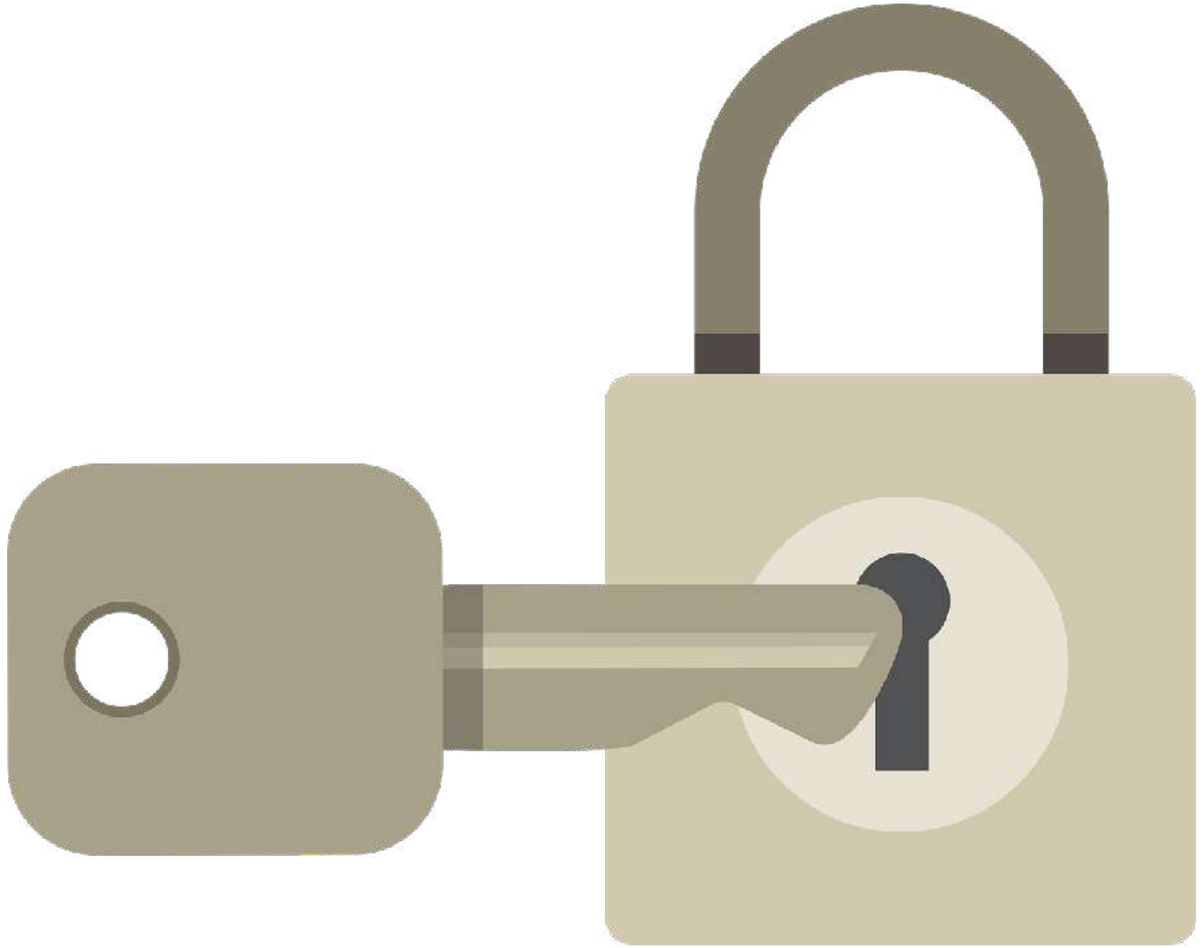
- Console port
- Initial configuration

AUX Line:

- Auxiliary port
- Backup console port

VTY Lines:

- Virtual terminal connections
- Inbound telnet control



AAA with a Local Database

Authentication:

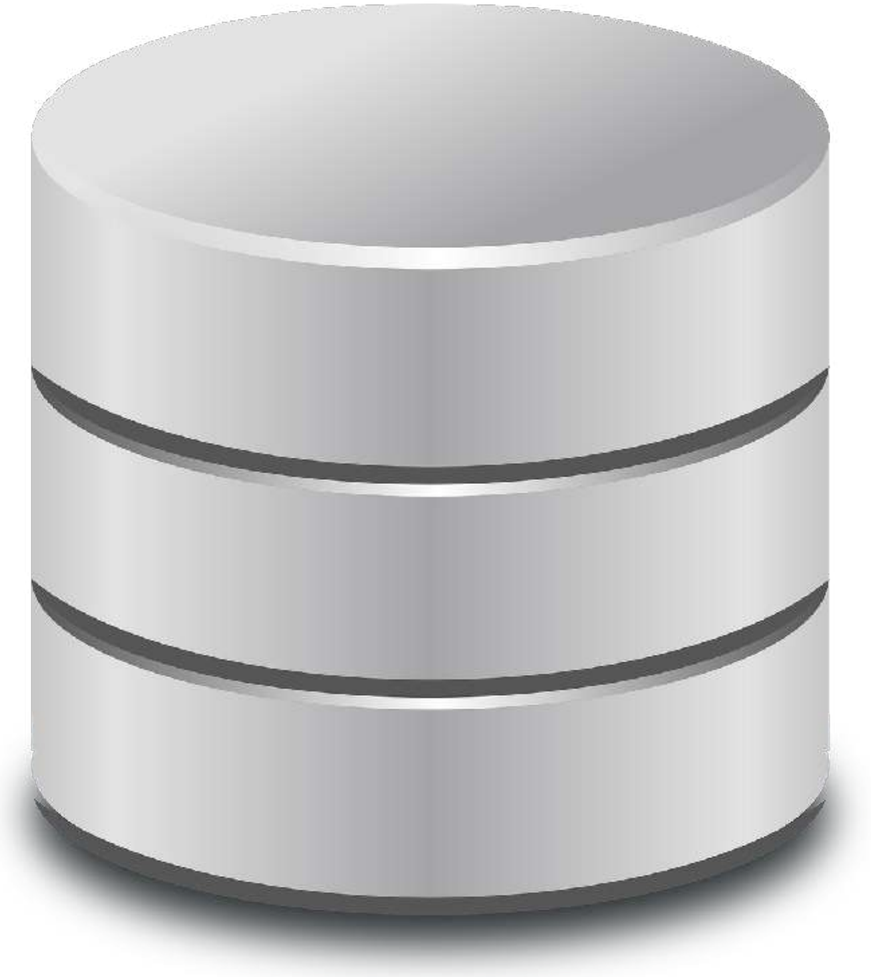
- Proof of identity
- Username/password

Authorization:

- Privileges and restrictions
- Authentication does not ensure authorization

Accounting:

- Record of user actions
- Log files



AAA with a Local Database

External AAA:

- RADIUS
- TACACS+

RADIUS:

- IETF open standard
- UDP ports 1812/1813
- Encrypts password field only
- Network access

TACACS+:

- Cisco-proprietary
- Encrypts entire payload
- TCP port 49
- Device administration

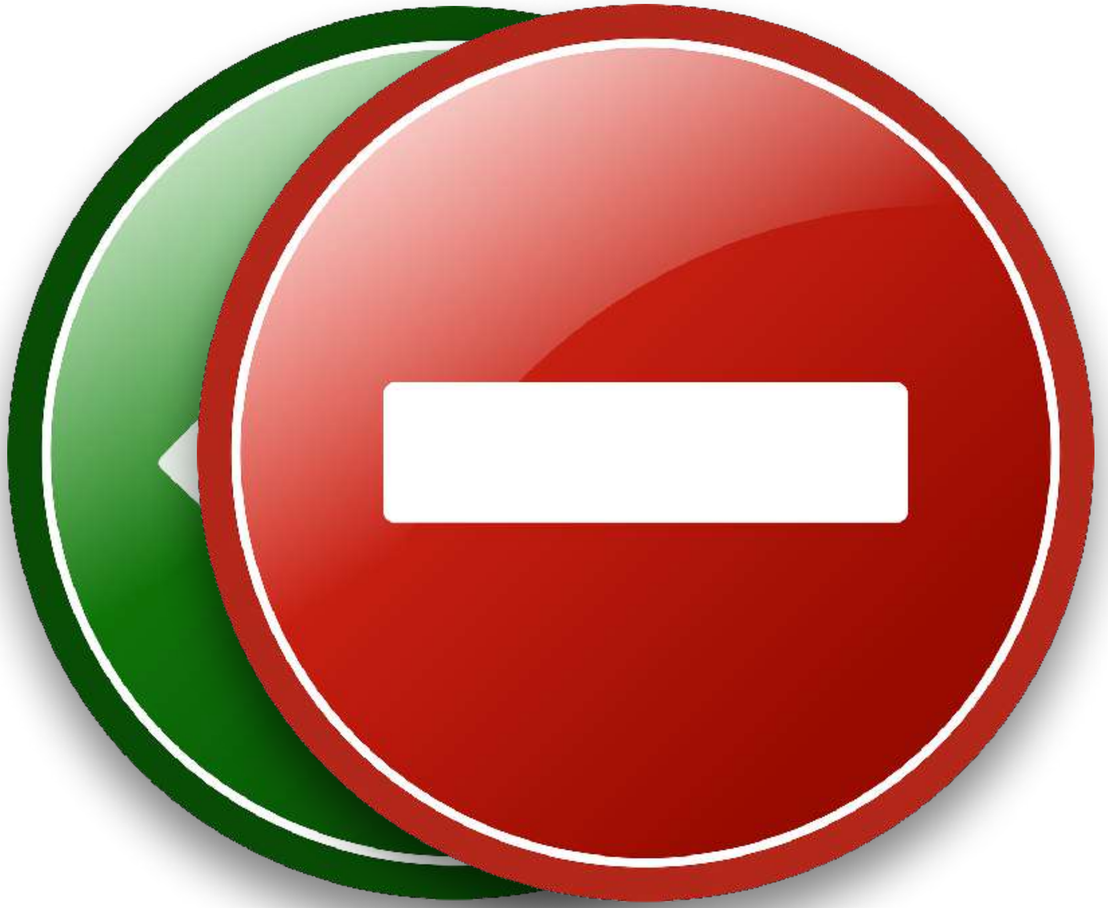
Infrastructure Security

Standard Access Control List (ACL) Configuration

Standard Access Control List (ACL) Configuration

Access Control Lists (ACLS):

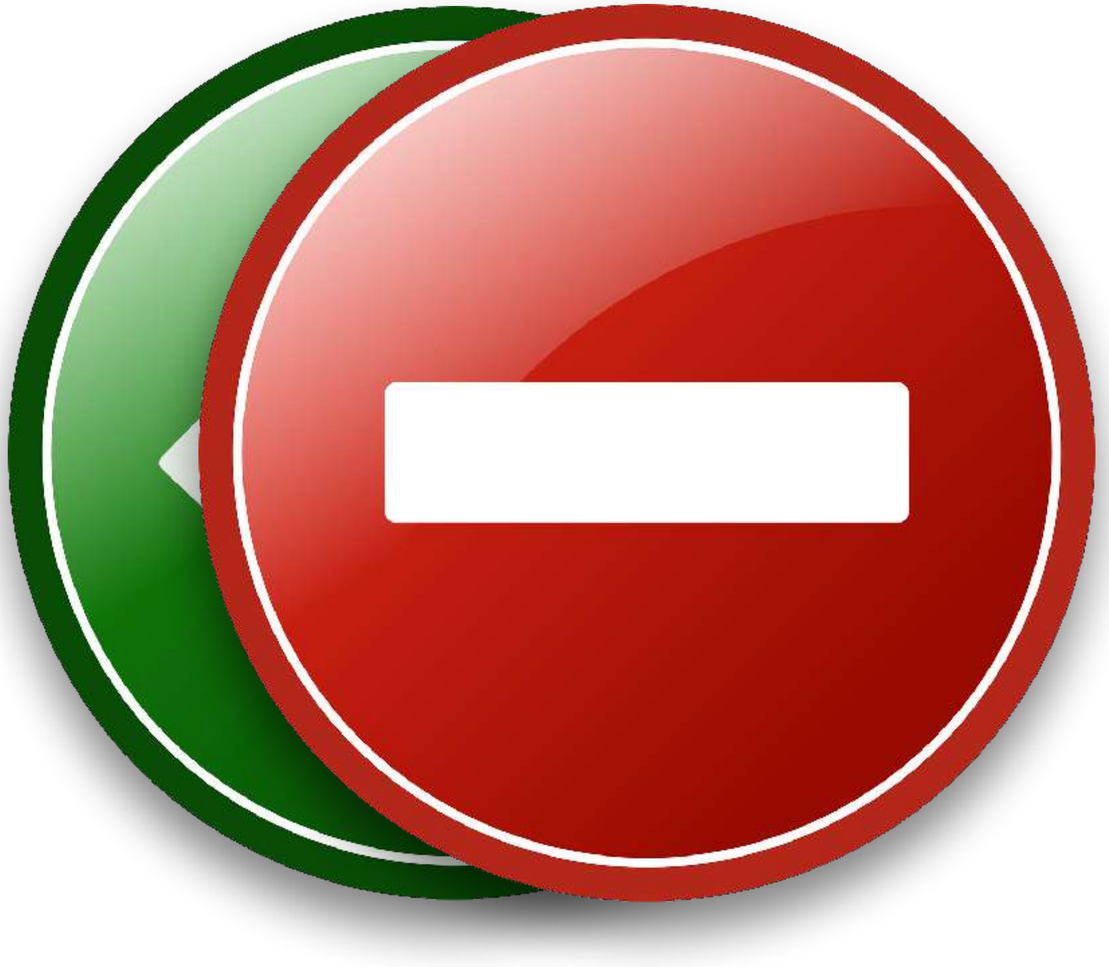
- Made up of access control entries (ACEs)
- Processed in a top-down manner
- Permit or deny traffic based on parameters
- Also used for traffic classification



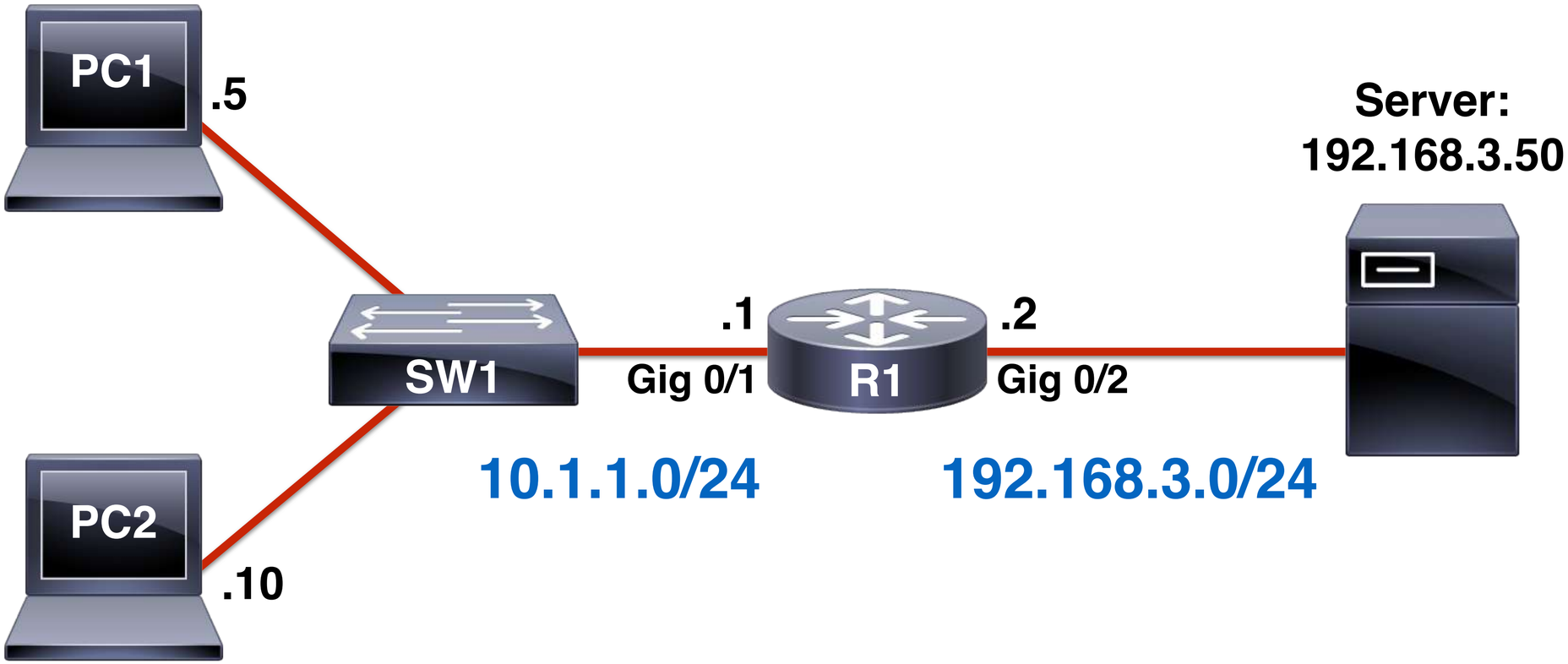
Standard Access Control List (ACL) Configuration

Standard Access Control Lists (ACLs):

- Only match source IP address
- Permit or deny entire protocol suite
- Numbers 1 - 99 (normal range)
- Numbers 1300 - 1999 (expanded range)
- Place as close to the destination as possible



Standard Access Control List (ACL) Configuration



Goals:

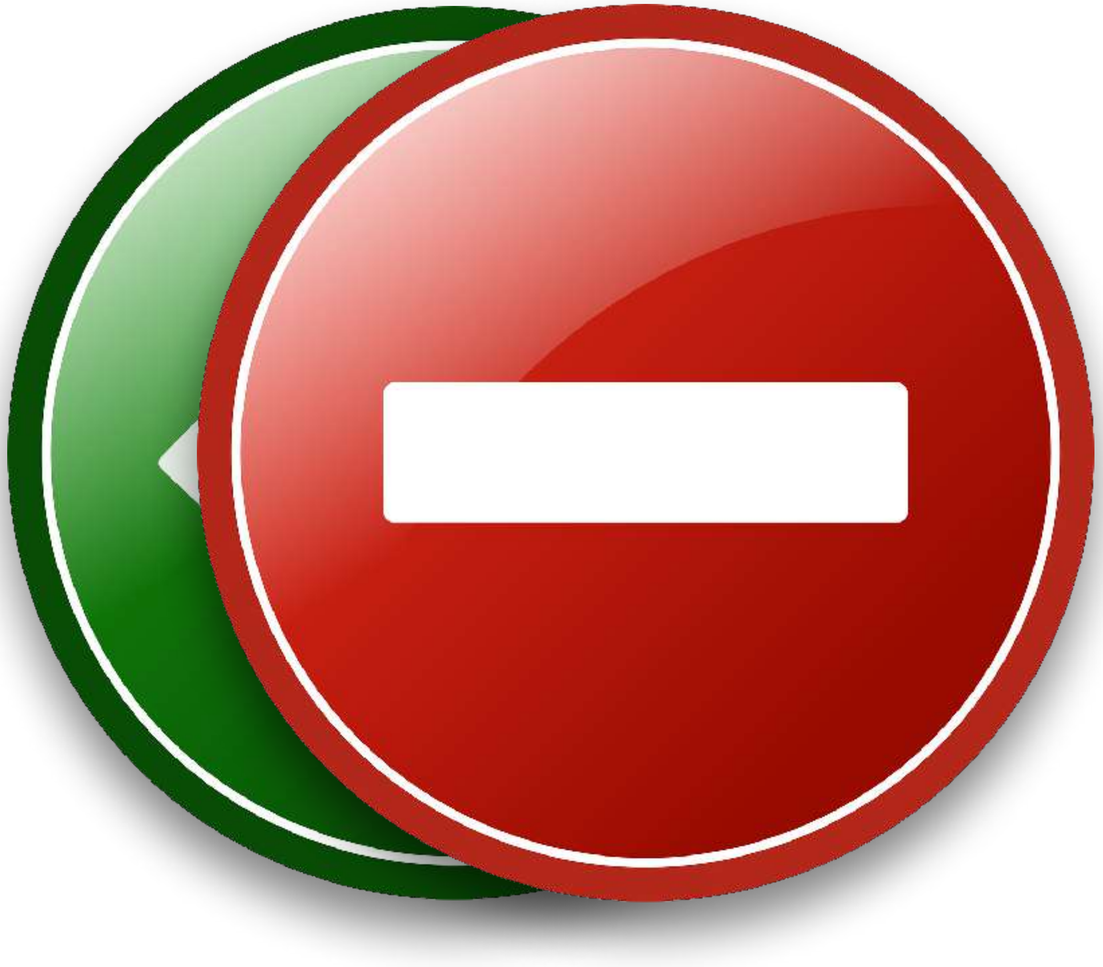
1. Permit all traffic from PC1 to Server
2. Deny all traffic from PC2 to Server

Extended Numbered ACL Configuration

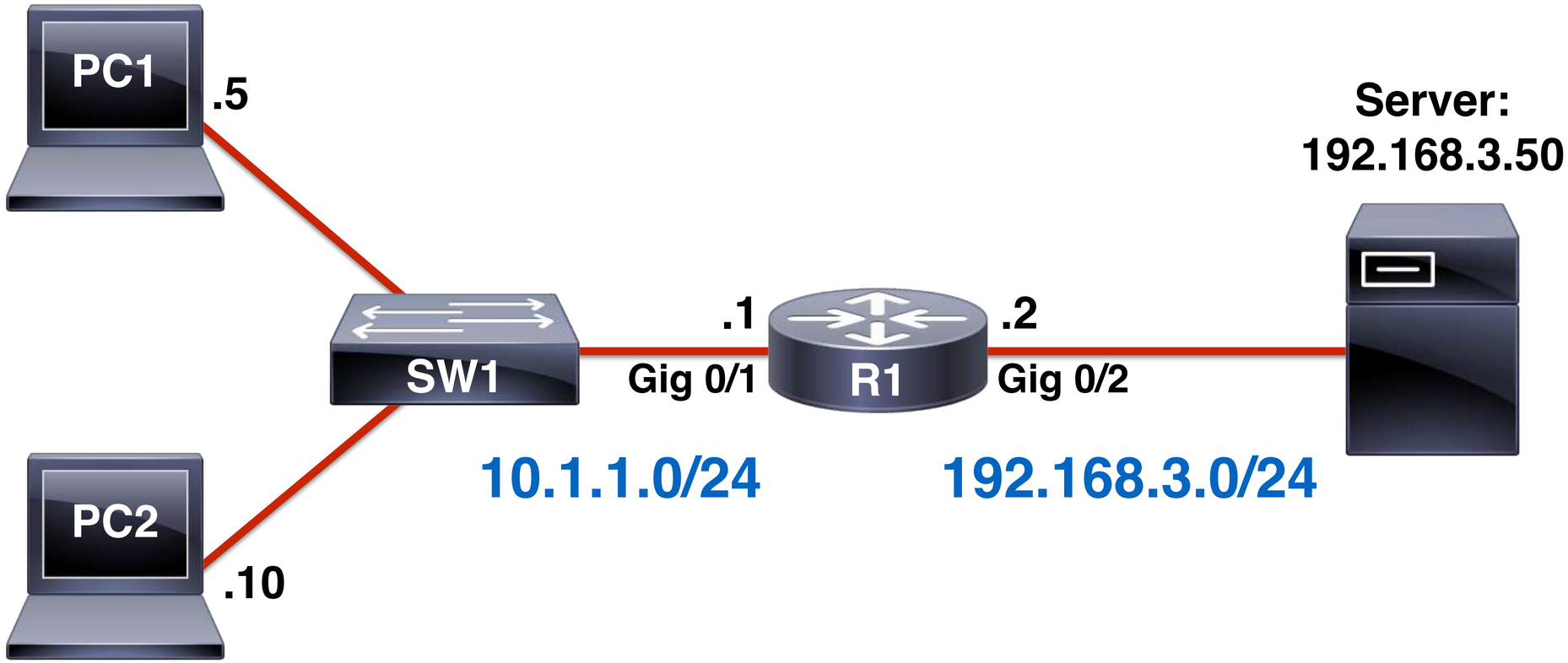
Extended Numbered ACL Configuration

Extended Access Control Lists (ACLs):

- Match source and destination IP addresses
- Specific filtering of protocols
- Numbers 100 - 199 (normal range)
- Numbers 2000 - 2699 (expanded range)
- Placed as close to the source as possible



Extended Numbered ACL Configuration



Goals:

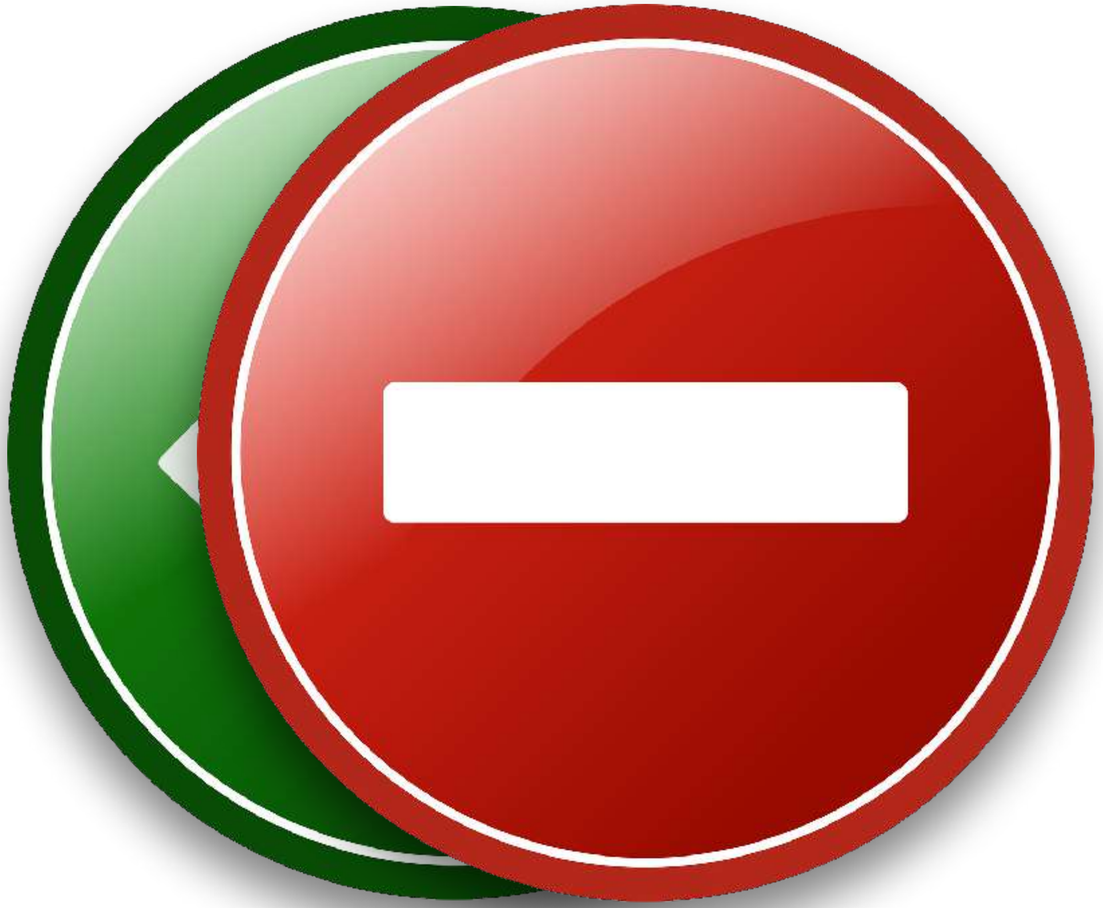
1. Deny telnet traffic from PC1 to Server
2. Permit all other traffic from both hosts

Extended Named ACL Configuration

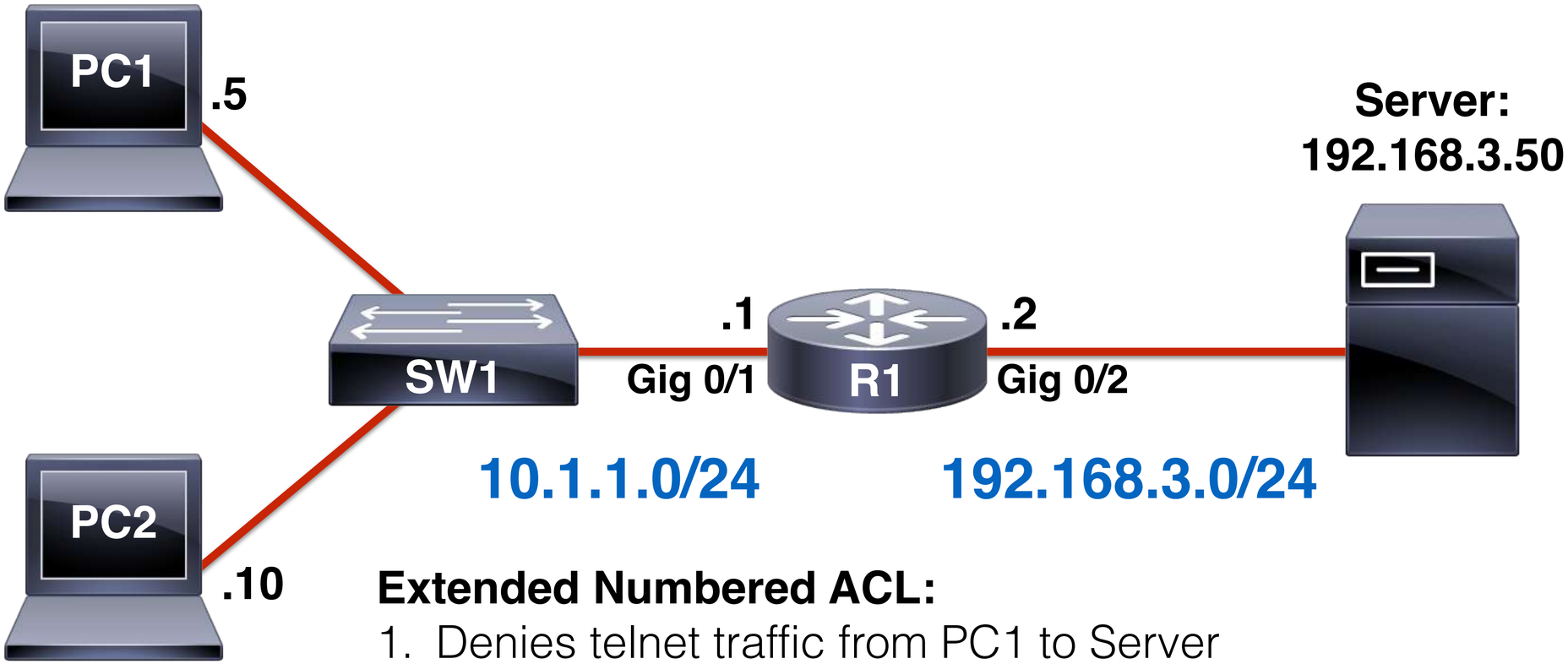
Extended Named ACL Configuration

Extended Named ACLs:

- More intuitive naming convention
- Easier to identify ACL purpose
- Allows an ACL to be edited



Extended Numbered ACL Configuration



Extended Numbered ACL:

1. Denies telnet traffic from PC1 to Server
2. Permits all other traffic from both hosts

Additional Requirements:

1. Deny HTTP traffic from PC1 to Server

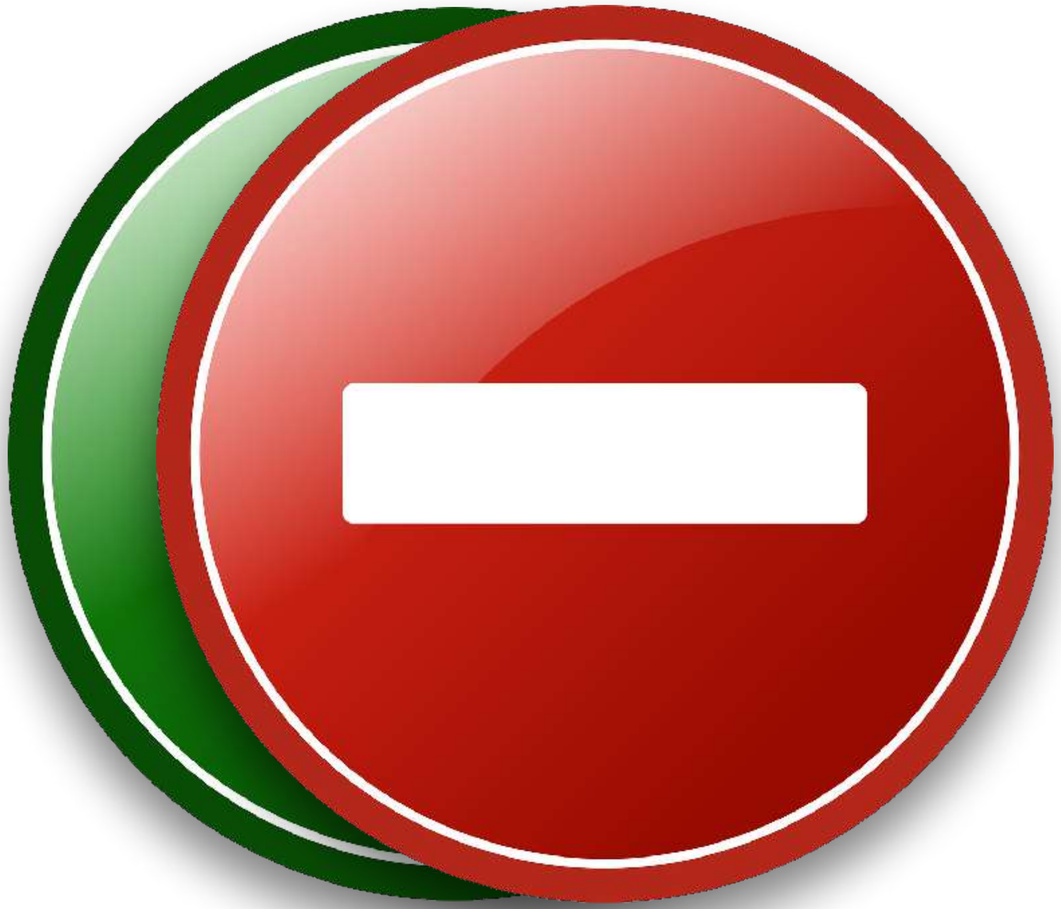
ACL Considerations

ACL Considerations

Access Control Lists (ACLs)

- List of rules that perform packet filtering
- Access control entries (ACEs)
- Sequentially processed from top-down
- Specific rules at top, general rules at bottom
- Implicit ***deny any*** at the end of each ACL

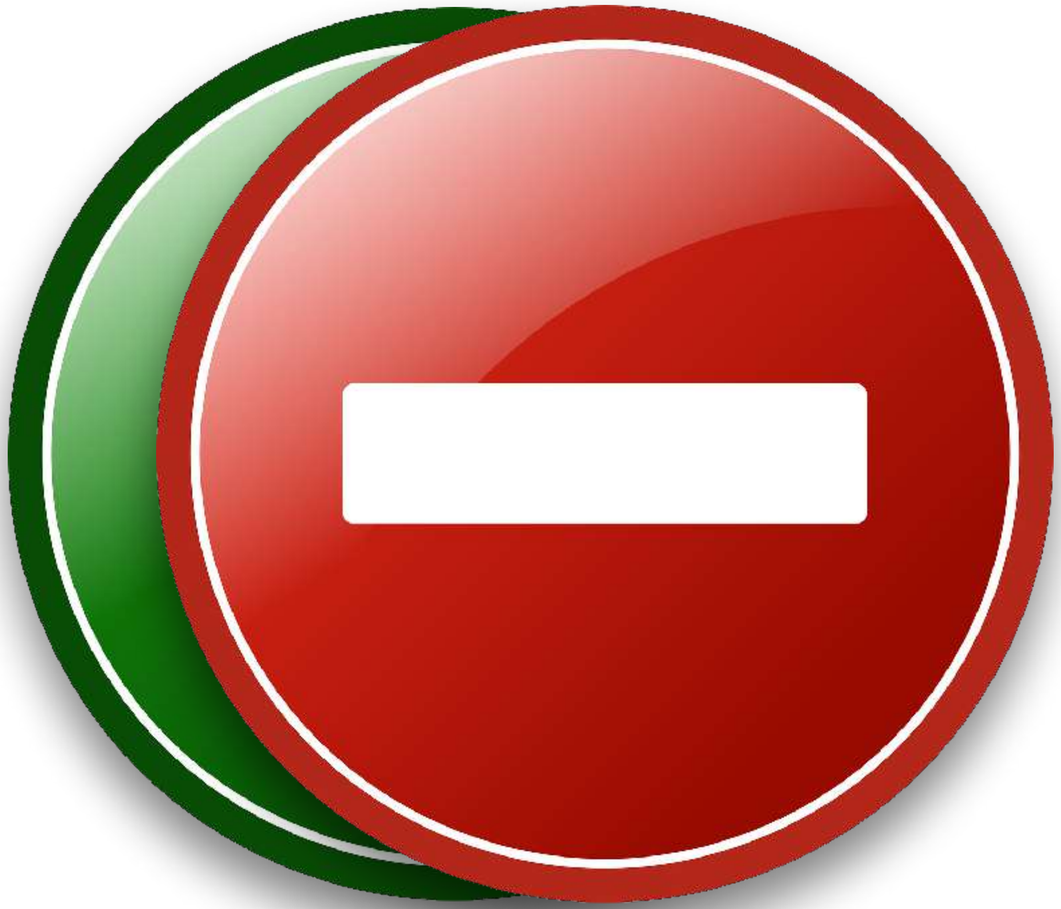
ACL Considerations



Standard ACLs:

- Not as extensive or flexible
- Match traffic to an entire protocol suite
- Match traffic based on source addressing
- Place as close to the destination as possible

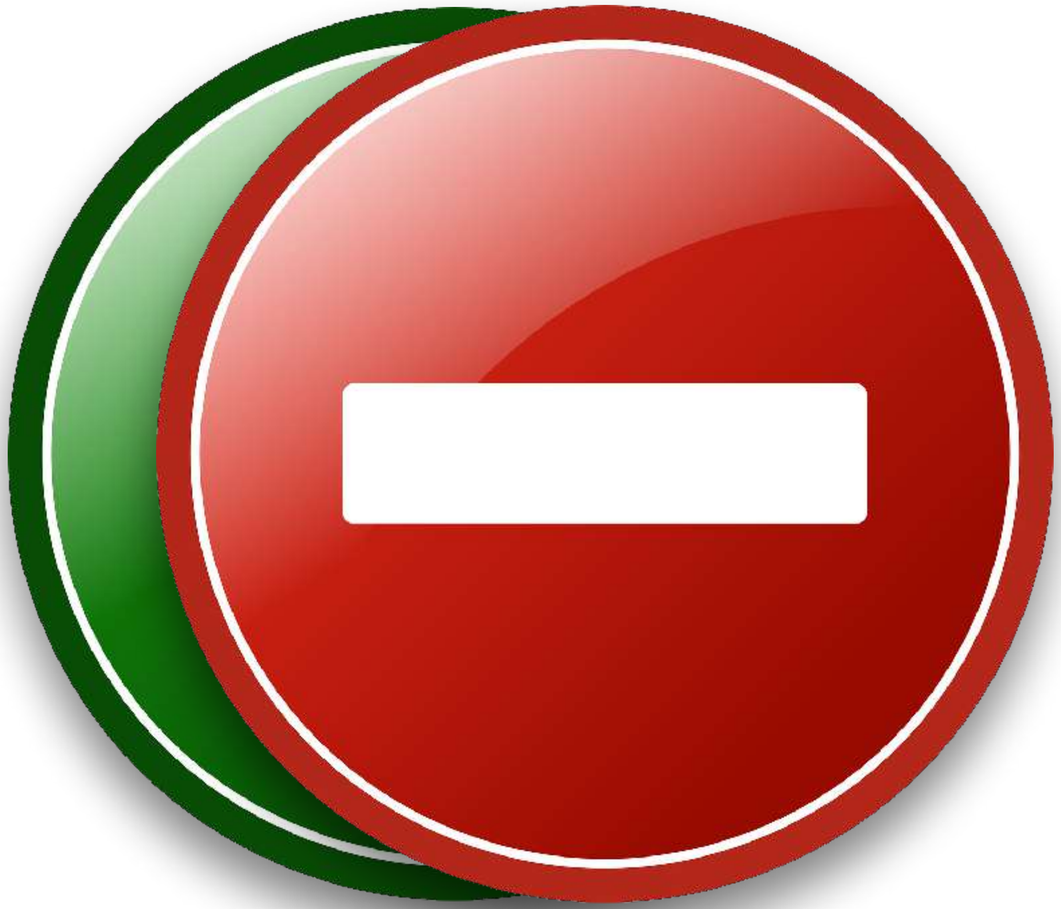
ACL Considerations



Extended ACLs:

- More powerful and flexible
- Can distinguish between protocol types
- Match traffic based on source and destination
- Place as close to the source as possible

ACL Considerations



Named ACLs:

- Intuitive naming convention
- ACL editing using sequence numbers

ACL Considerations

- Be mindful of inbound vs. outbound direction
- Create ACL before applying to interface
- Command ***permit any any*** overrides implicit deny at the end
- Keyword ***remark*** creates comments
- Keyword ***log*** creates logging entries

Control Plane Policing

Control Plane Policing (CoPP) Theory

Control Plane Policing (CoPP):

- Used to protect a device's route processor (RP)
- Protection from DoS conditions
- QoS policy used to rate-limit traffic

Control Plane Policing (CoPP) Theory

- User plane
- Traffic transiting the router

- Traffic initiated by the router
- Traffic destined to the router

- Management, configuration, and monitoring

Control Plane Policing (CoPP) Theory

Control Plane Policing (CoPP):

- Control plane considered as a separate entity, with its own ingress and egress ports
- Allows for traffic filtering and rate limiting through Modular QoS CLI (MQC)
- MQC concepts - **class maps**, **policy maps**, and **service policies**

Control Plane Policing (CoPP) Theory

Class Maps:

- Classify network traffic based on Layer 3, 4, and 7 information

Policy Maps:

- Define a series of actions to be taken against traffic matching a class map

Service Policies:

- Specify where a policy map should be implemented

Control Plane Policing (CoPP) Theory

Main objectives for CoPP:

- Identify and rate limit traffic that reaches the control plane
- Protect IOS process memory, buffers, and ingress packet queues
- Protection against DoS attacks

CoPP Configuration

Control Plane Policing (CoPP):

- Create an ACL to identify traffic
- Create a class map to classify the traffic
- Create a policy map to define the action taken against the traffic
- Create a service policy to enable policing on the control plane interface

Wireless Security

Extensible Authentication Protocol (EAP)

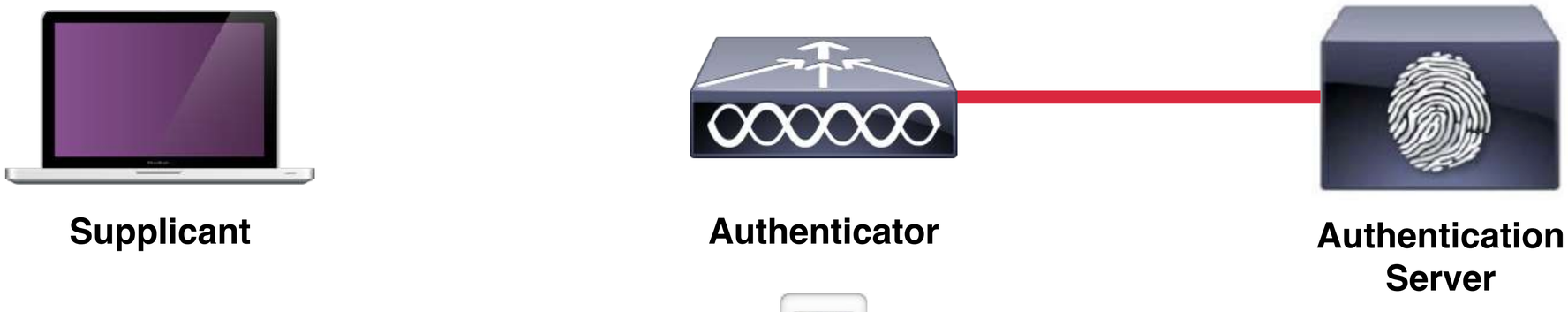
802.1x Authentication:

- IEEE standard which defines port-based network control
- Uses EAP over LAN (EAPoL) to control access to the local area network

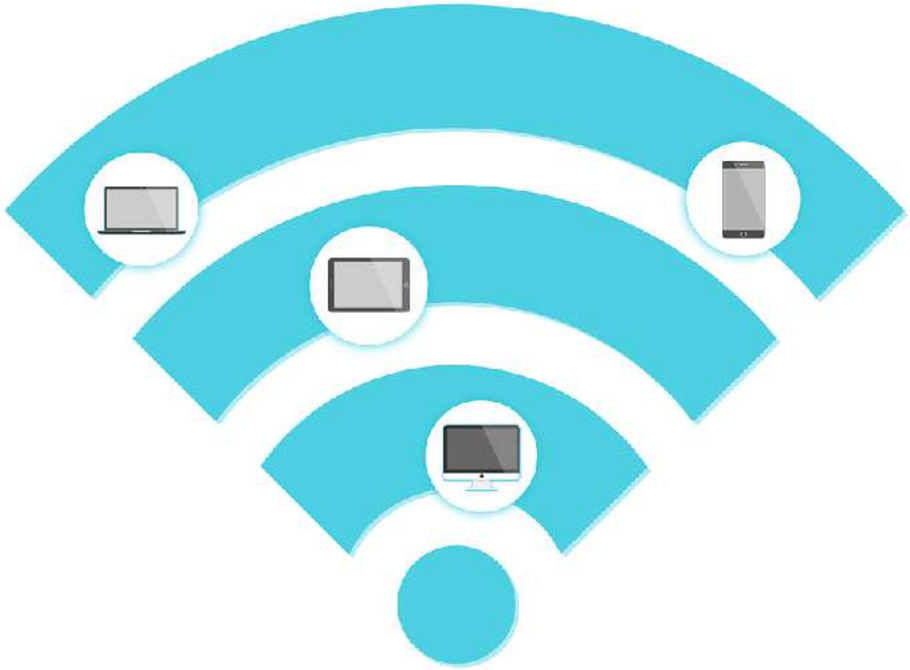
Extensible Authentication Protocol (EAP)

1. **Supplicant:** The endpoint requesting access
2. **Authenticator:** Network device controlling physical access to the network
3. **Authentication Server:** Performs the actual authentication of the endpoint

Extensible Authentication Protocol (EAP)



Extensible Authentication Protocol (EAP)

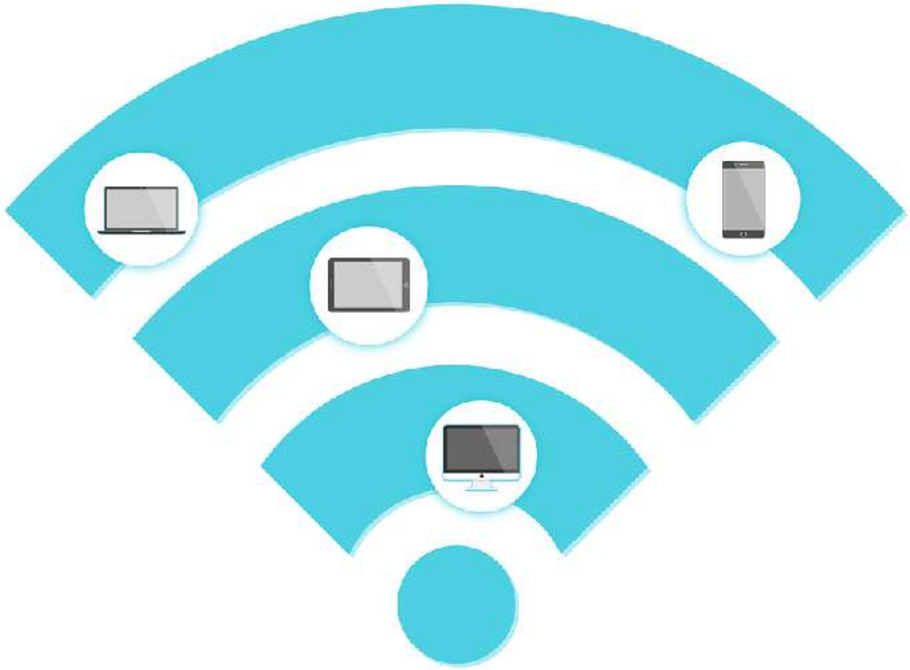


Native EAP Types

EAP-TLS:
- One of the most secure EAP types
- Uses X.509 certificates for mutual authentication
- Highly regarded in BYOD deployments

EAP-MD5
- Hides credentials in a hash
- Common on IP phones

Extensible Authentication Protocol (EAP)



Native EAP Types

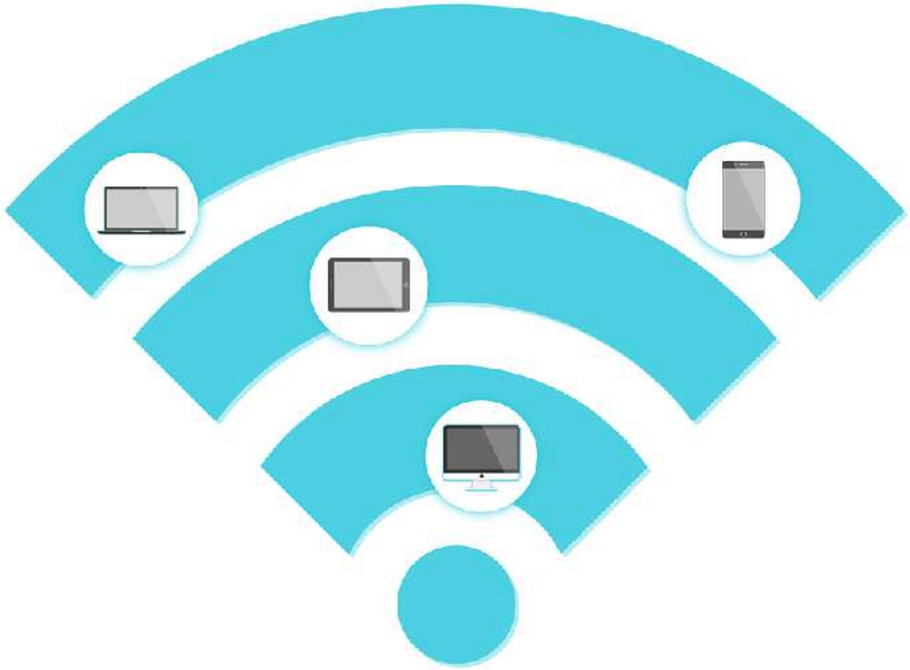
EAP-MSCHAPv2

- Credentials encrypted within an MSCHAPv2 session
- Simple transmission of credentials
- Ability to communicate with Active Directory

EAP-GTC

- Cisco alternative to MSCHAPv2
- Enables more generic authentication

Extensible Authentication Protocol (EAP)



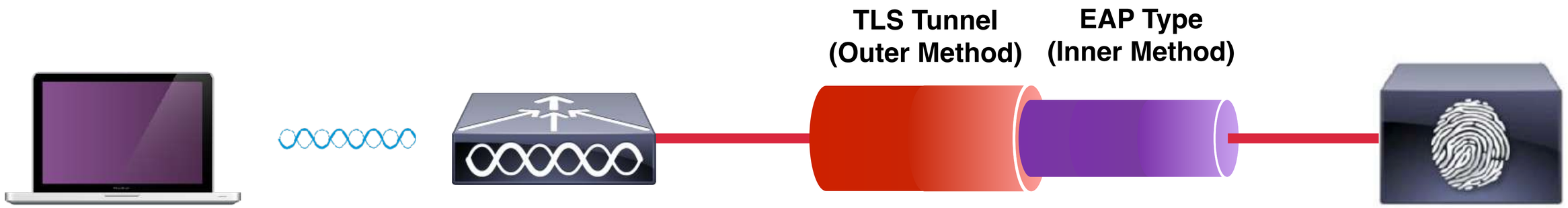
Tunneled EAP Types

PEAP (Protected EAP)
- Originally proposed by Microsoft
- Uses X.509 certificate
- Uses an additional native EAP type for inner method

EAP-FAST (Flexible Authentication via Secure Tunnel)
- Created by Cisco as a PEAP alternative
- Faster re-authentication
- Faster wireless roaming
- Uses protected access credentials (PACs)

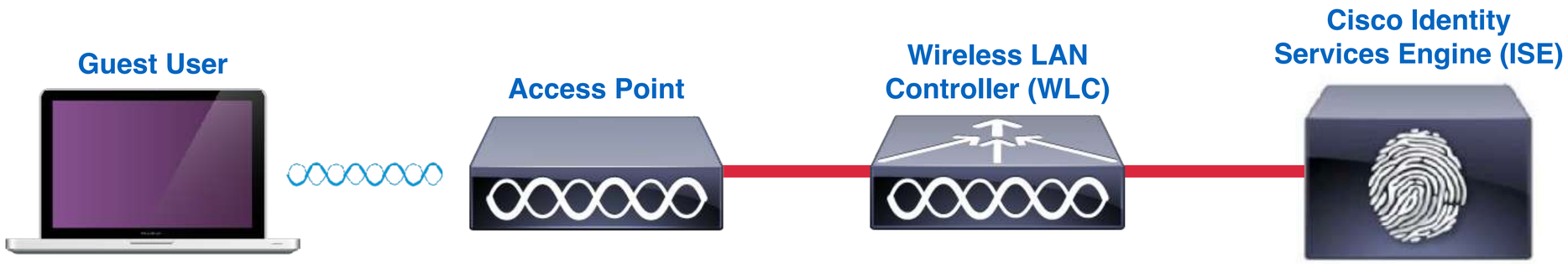
Extensible Authentication Protocol (EAP)

Tunneled EAP Types



WebAuth

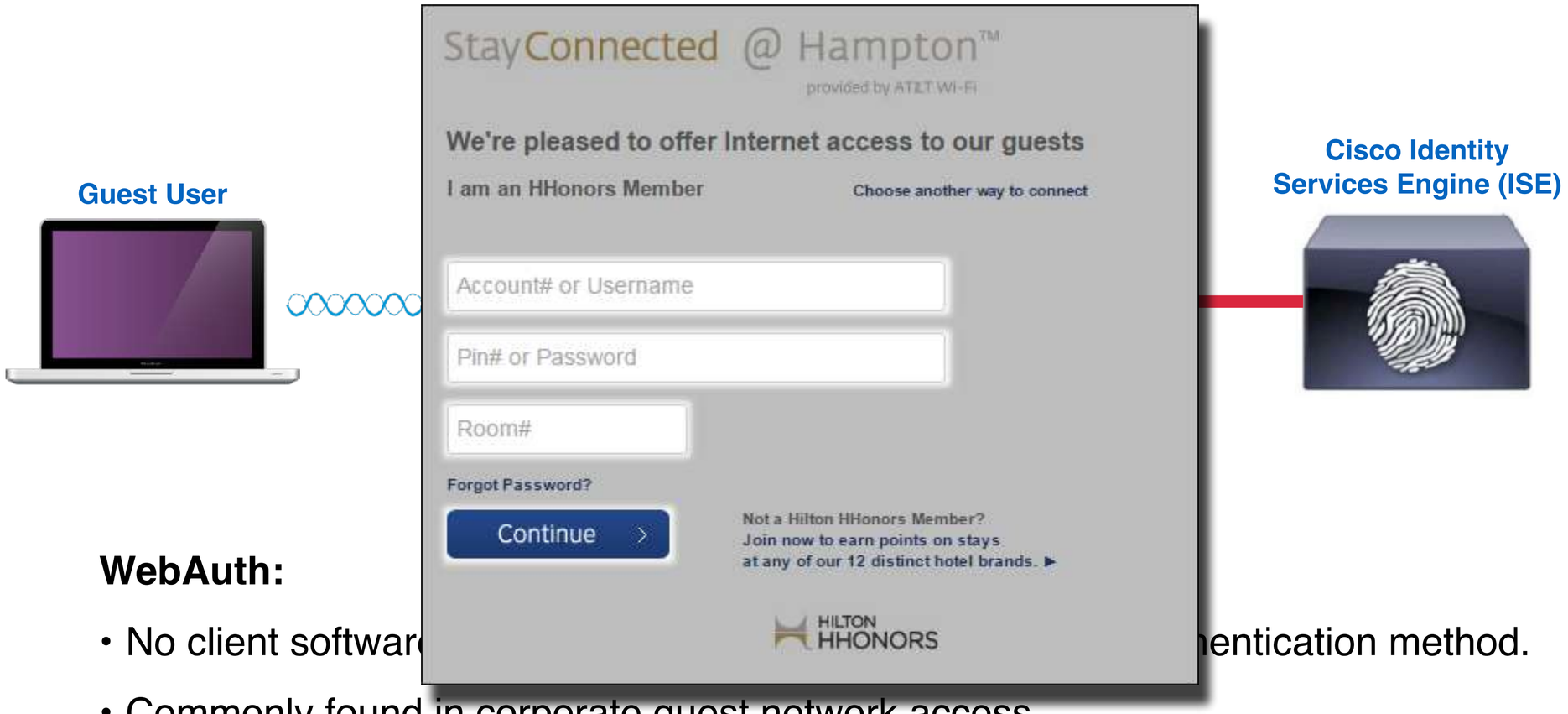
Web-Based Authentication (WebAuth)



WebAuth:

- No client software is required, making this a more flexible authentication method.
- Commonly found in corporate guest network access.

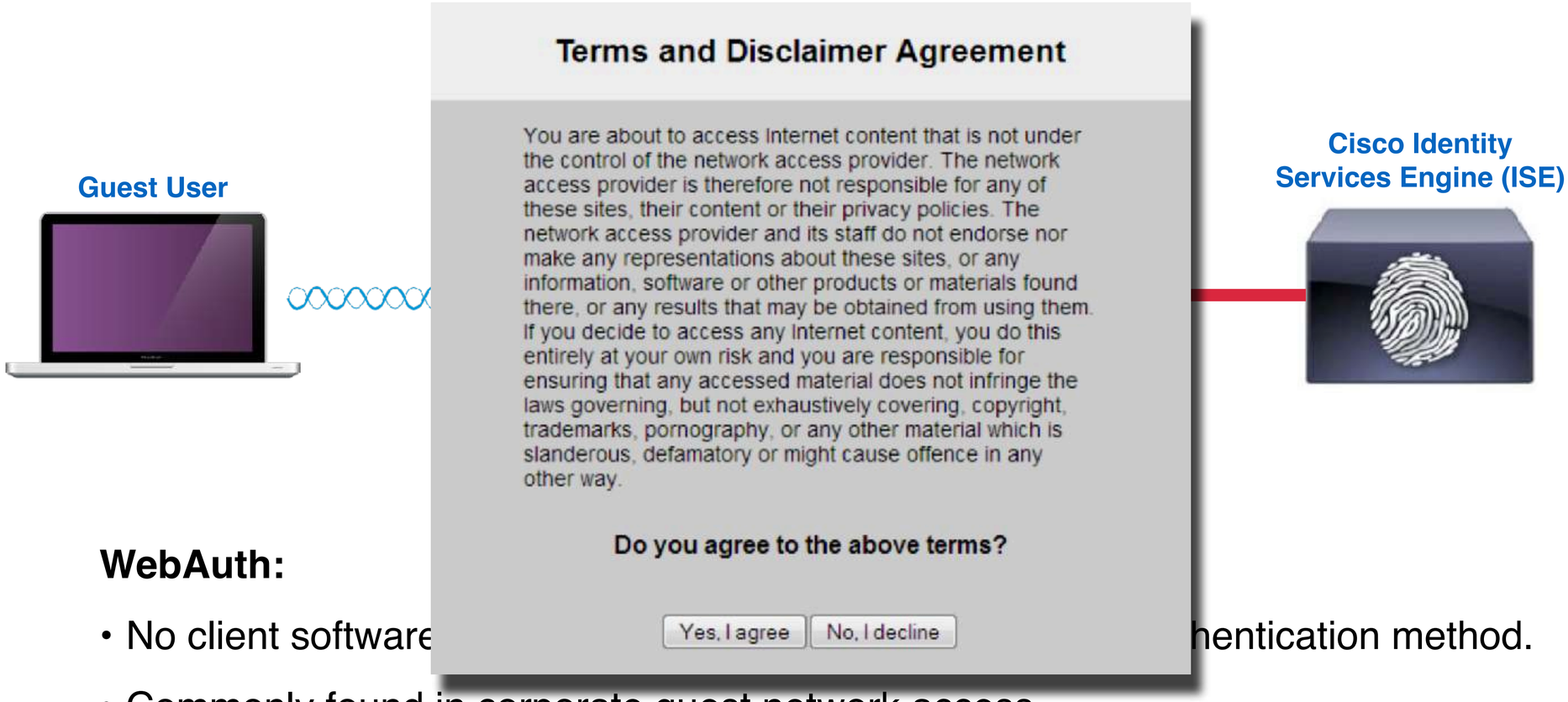
Web-Based Authentication (WebAuth)



WebAuth:

- No client softwar entication method.
- Commonly found in corporate guest network access.

Web-Based Authentication (WebAuth)

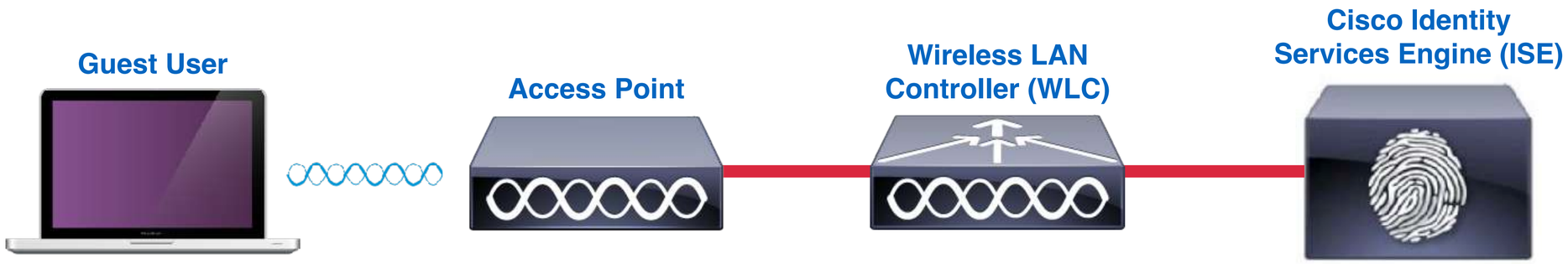


WebAuth:

- No client software
- Commonly found in corporate guest network access.

hentication method.

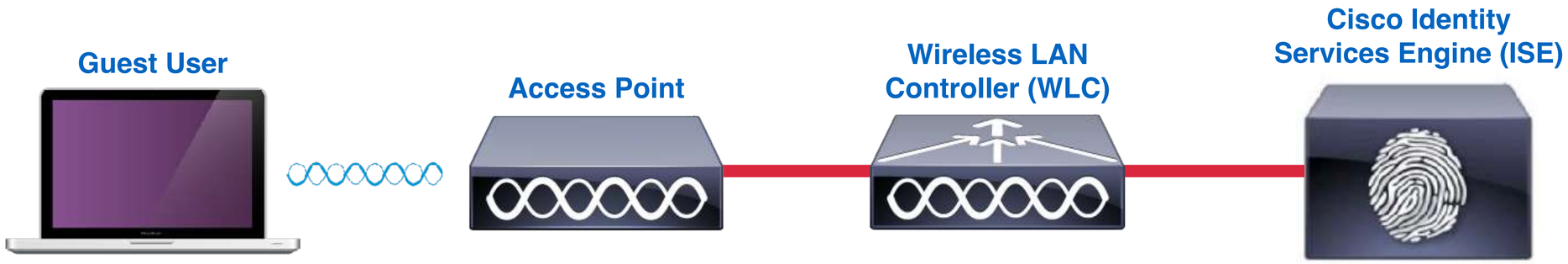
Web-Based Authentication (WebAuth)



WebAuth:

- No client software is required, making this a more flexible authentication method.
- Commonly found in corporate guest network access.
- No IP traffic allowed from the host before successful authentication.

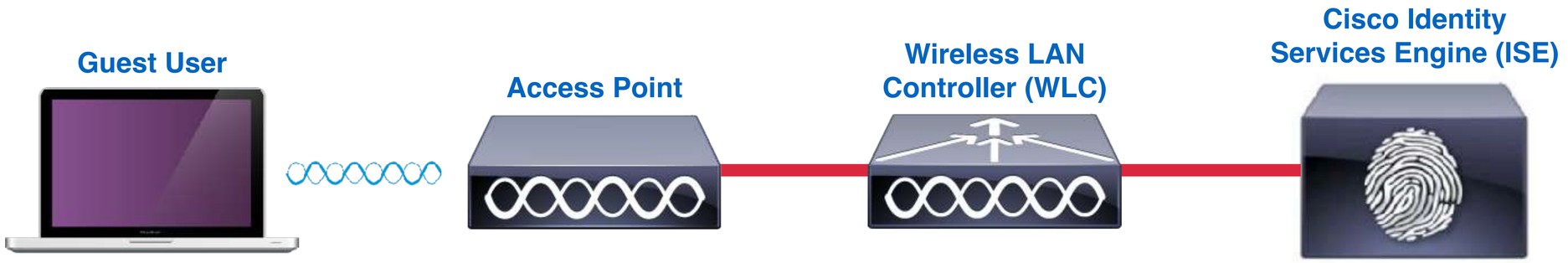
Web-Based Authentication (WebAuth)



Central Web Authentication (WebAuth): Used in larger WebAuth deployments where a centralized RADIUS database (such as Cisco ISE) is necessary.

Local Web Authentication (WebAuth): Used in smaller wireless deployments where WebAuth is handled locally by the wireless LAN controller.

Web-Based Authentication (WebAuth)



WebAuth Process:

1. Guest user connects to WebAuth configured SSID.
2. Guest user opens a web browser.
3. WLC redirects browser to guest portal.
4. Guest portal authenticates user and informs WLC via RADIUS.
5. Access control attributes are applied to the guest user.
6. WLC returns successful login page to user, and any acceptable user policies for review.

Web-Based Authentication (WebAuth)

WebAuth Benefits:

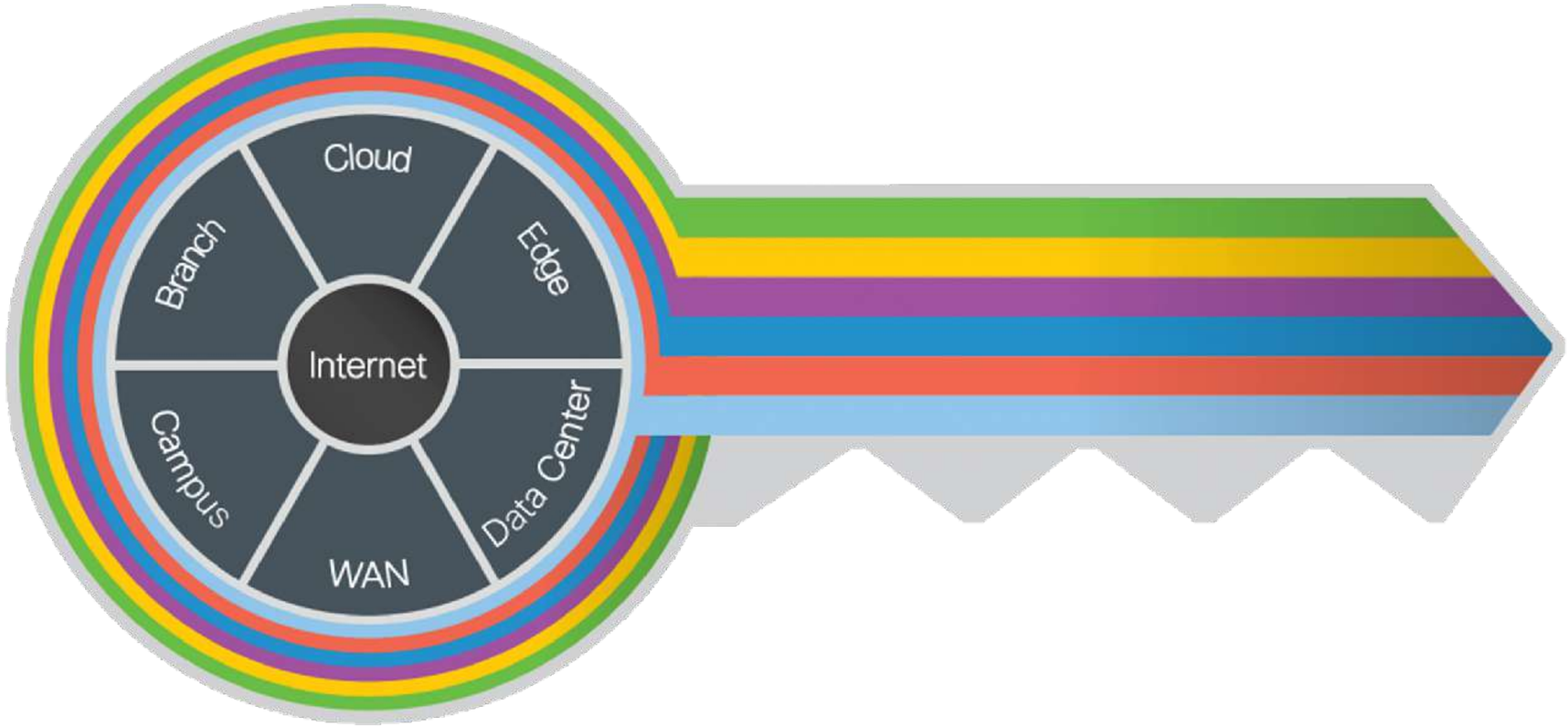
- No special client software required
- Familiarity for end users
- Customizable user interface

WebAuth Limitations:

- Not transparent to end users
- Not as secure as 802.1x
- Lack of single sign-on capabilities

Security Design Considerations

Cyber Threat Defense



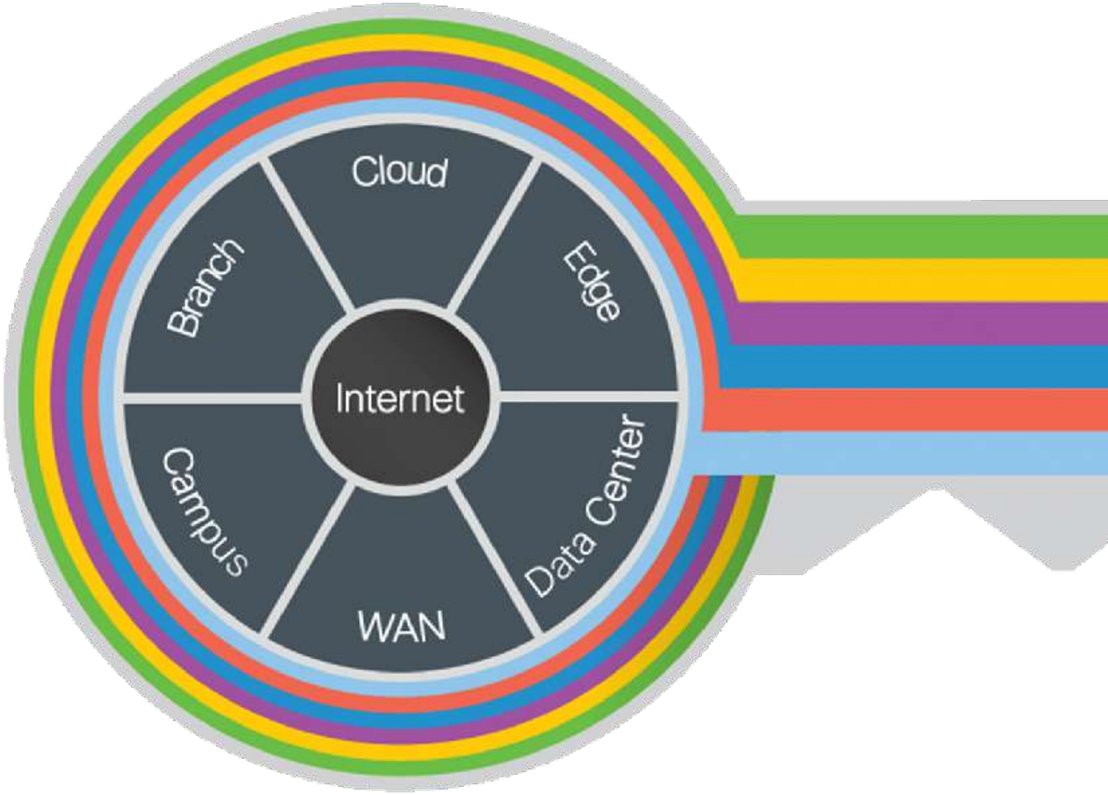
Cyber Threat Defense

Cisco SAFE:

- Security model for modern needs
- Logical Places in Network (PIN)

Common PINs

- Branch
- Campus
- WAN
- Data Center
- Edge
- Cloud



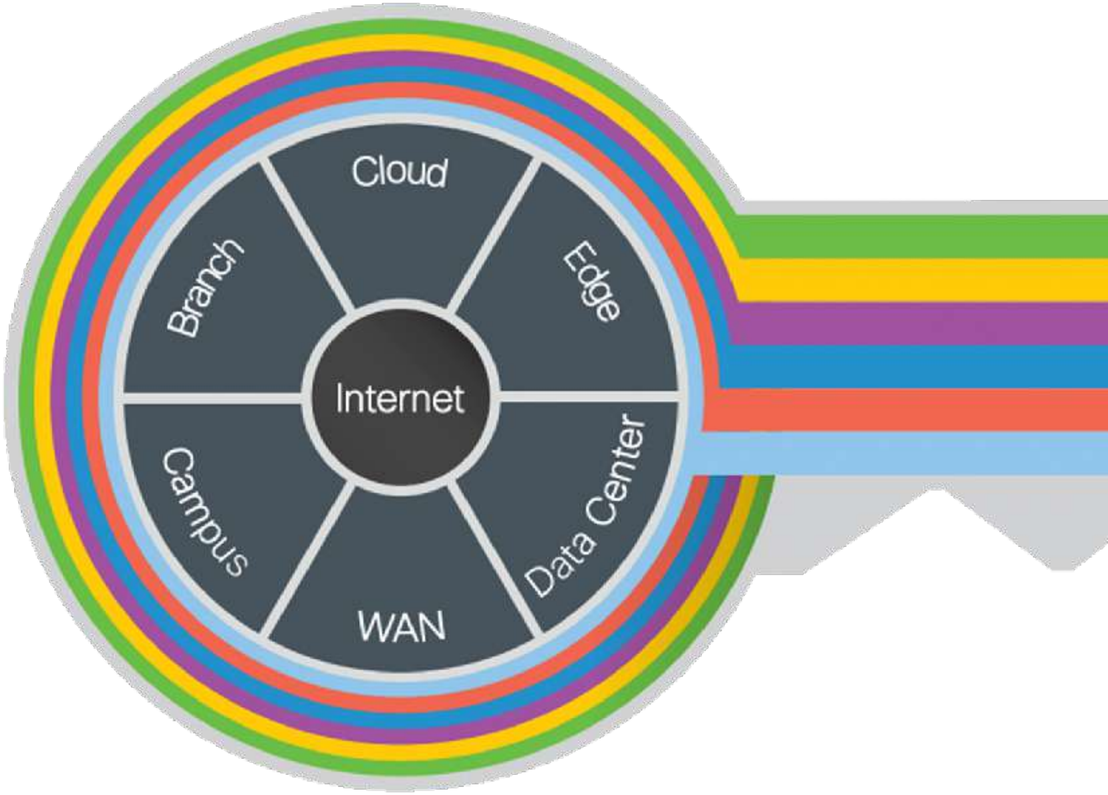
Cyber Threat Defense

Branch:

- Typically less secure due to cost
- Most susceptible to threats

Mitigation Focus:

- Endpoint malware and antivirus protection
- Wireless infrastructure protection
- Trust exploitation protection



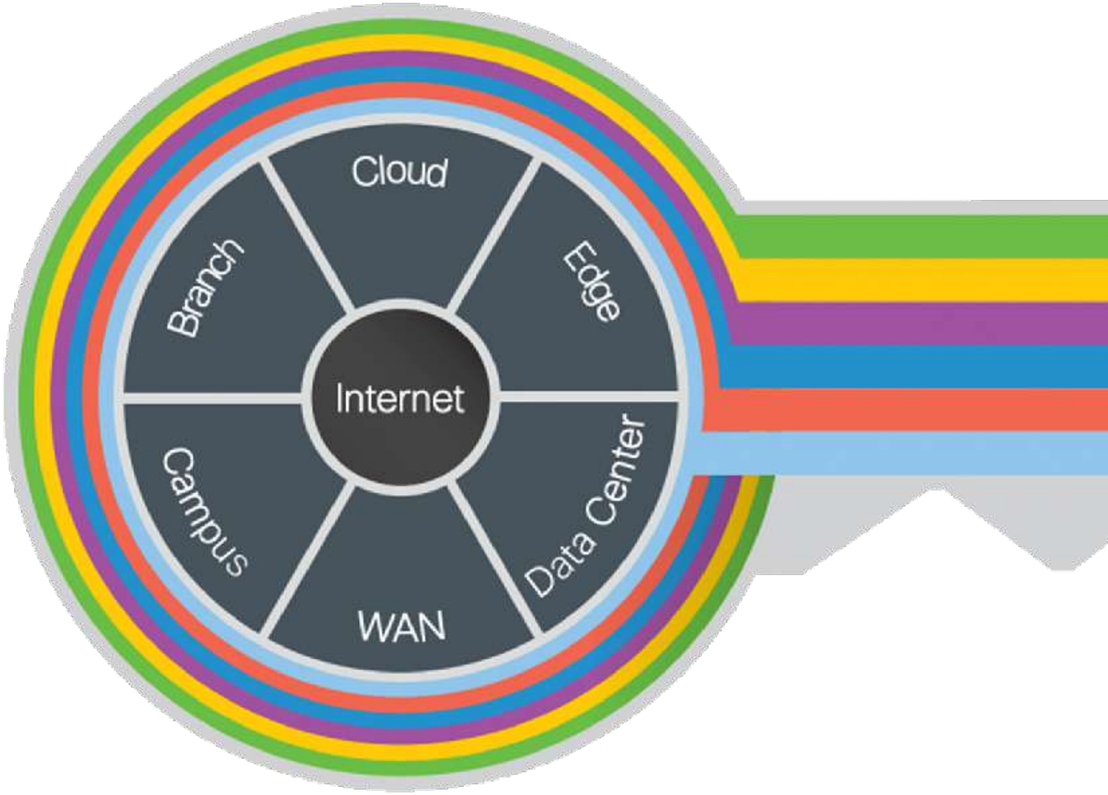
Cyber Threat Defense

Campus:

- Large user populations with varied devices
- Subnets and VLAN segmentation

Mitigation Focus:

- Phishing and web-based exploits
- Network malware and botnet infestation
- BYOD increases attack surface



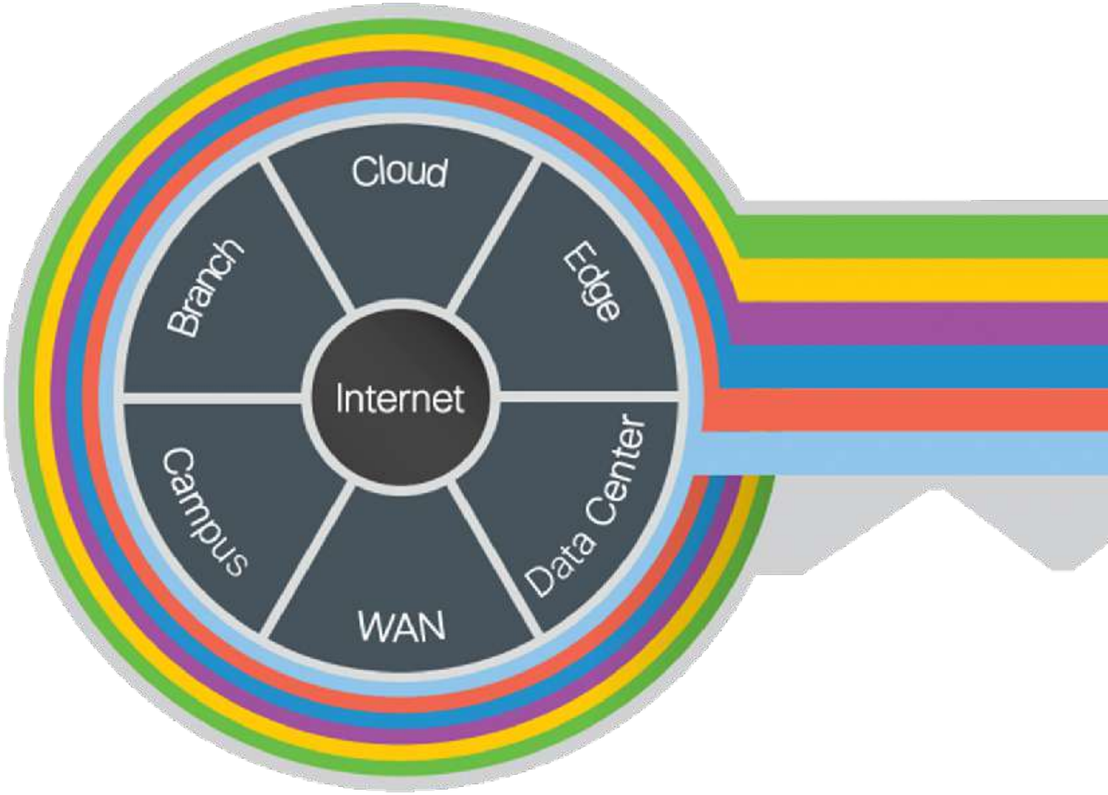
Cyber Threat Defense

Data Center:

- Informational assets
- Physical and/or virtual servers

Mitigation Focus:

- Malware propagation
- Unauthorized user access
- Reconnaissance attacks



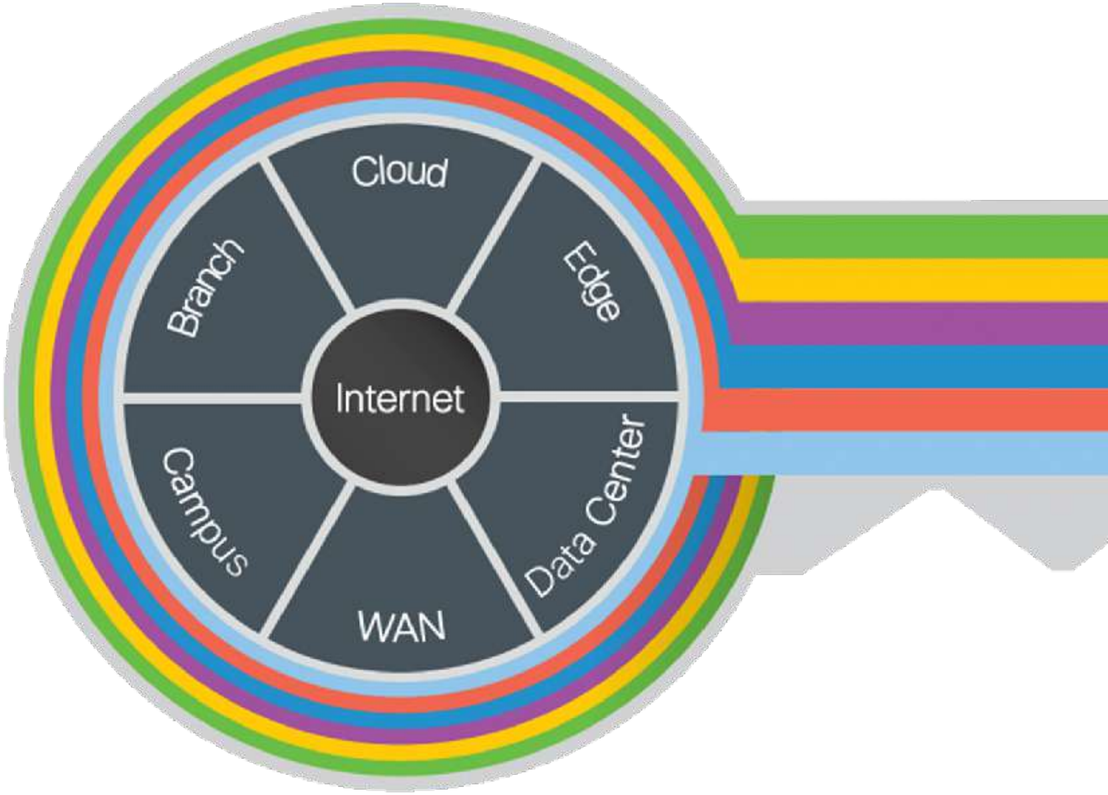
Cyber Threat Defense

Edge:

- Primary ingress/egress for network
- Most critical infrastructure resource

Mitigation Focus:

- Web server vulnerabilities
- Distributed Denial of Service (DDoS)
- Man-in-the-Middle (MITM)



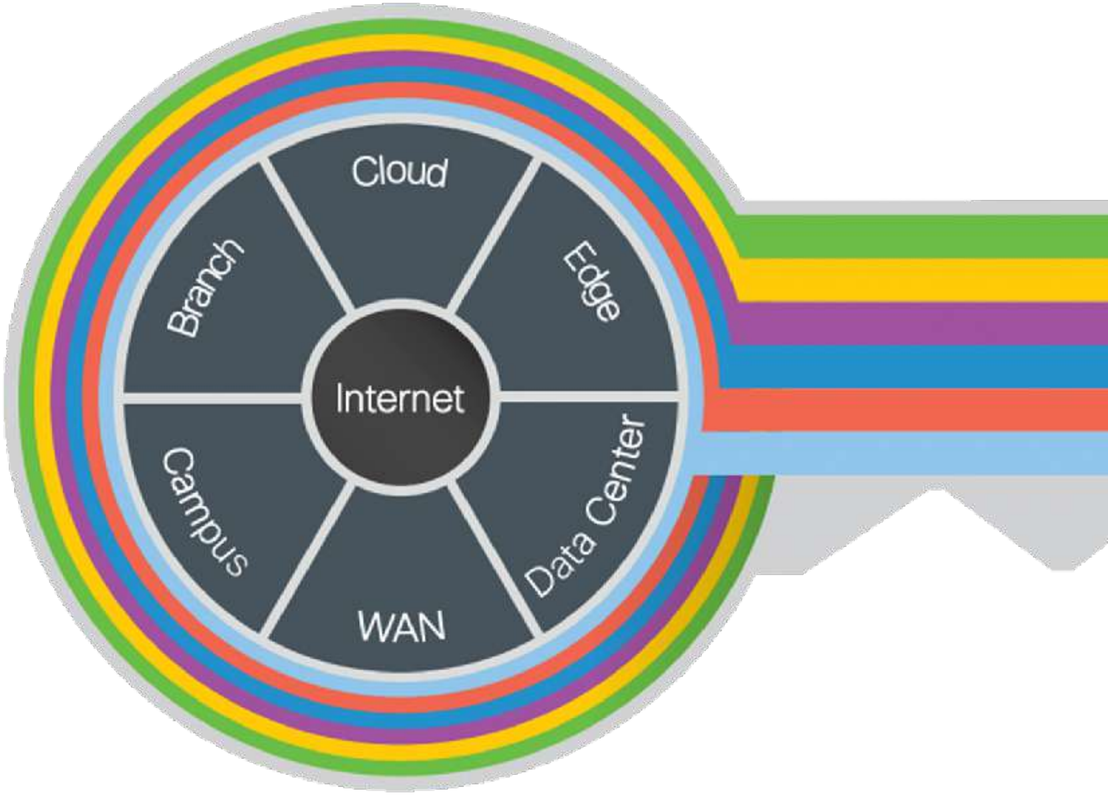
Cyber Threat Defense

Cloud:

- Popular for convenience and cost
- Rely largely on the provider for security

Mitigation Focus:

- SLA dictates security strength
- Information storage and access
- Uptime and recovery guidelines



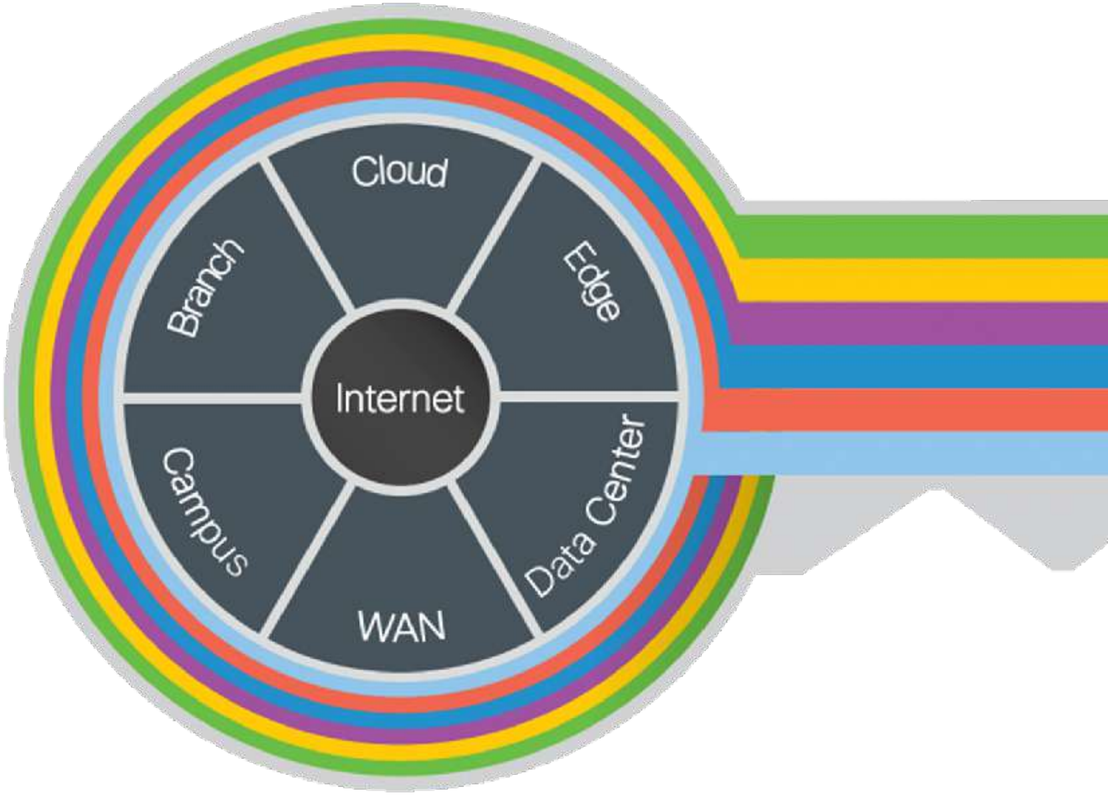
Cyber Threat Defense

WAN:

- Connects network resources together
- Provides critical network access

Mitigation Focus:

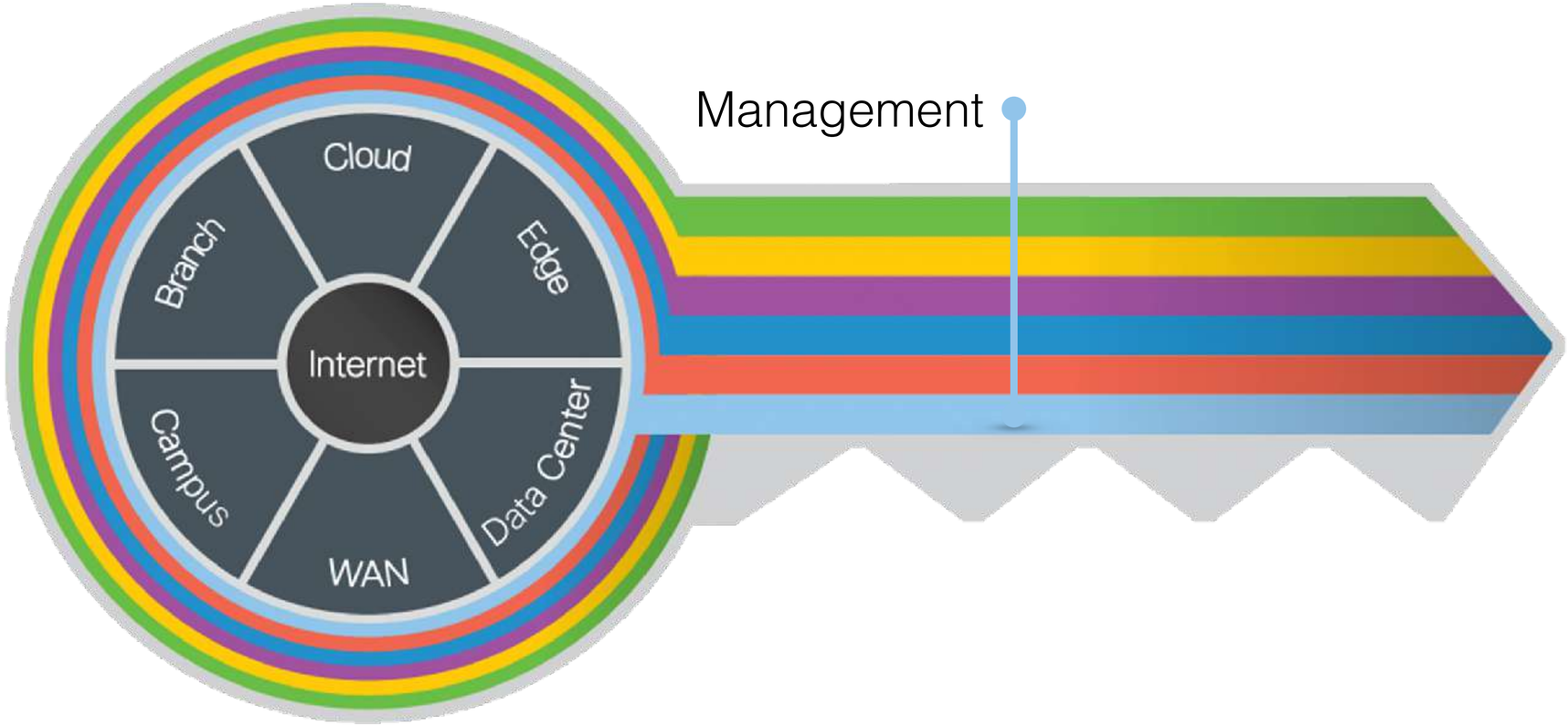
- Unauthorized application access
- Malware propagation
- Data exfiltration and/or loss



Cyber Threat Defense

Management:

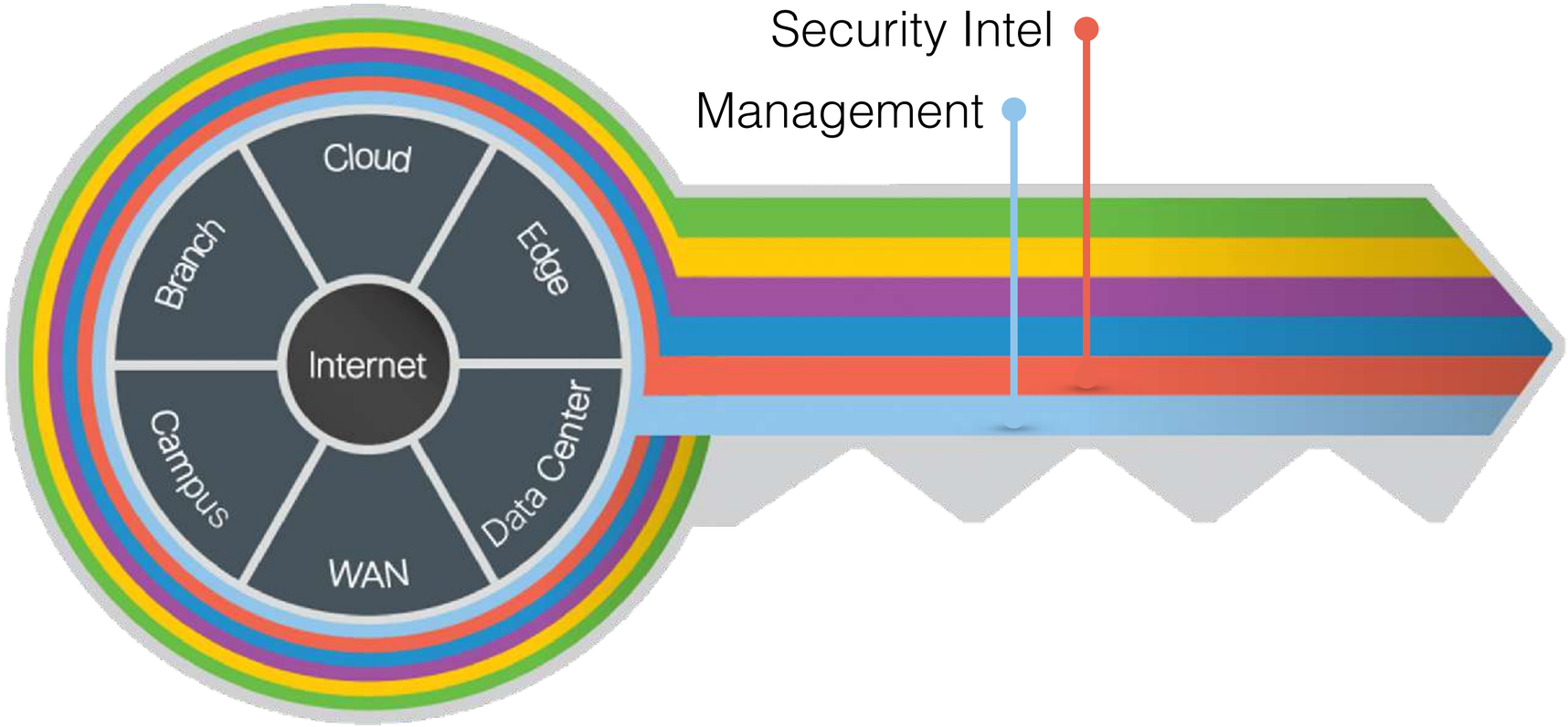
- Policy creation, change management, patching



Cyber Threat Defense

Security Intelligence:

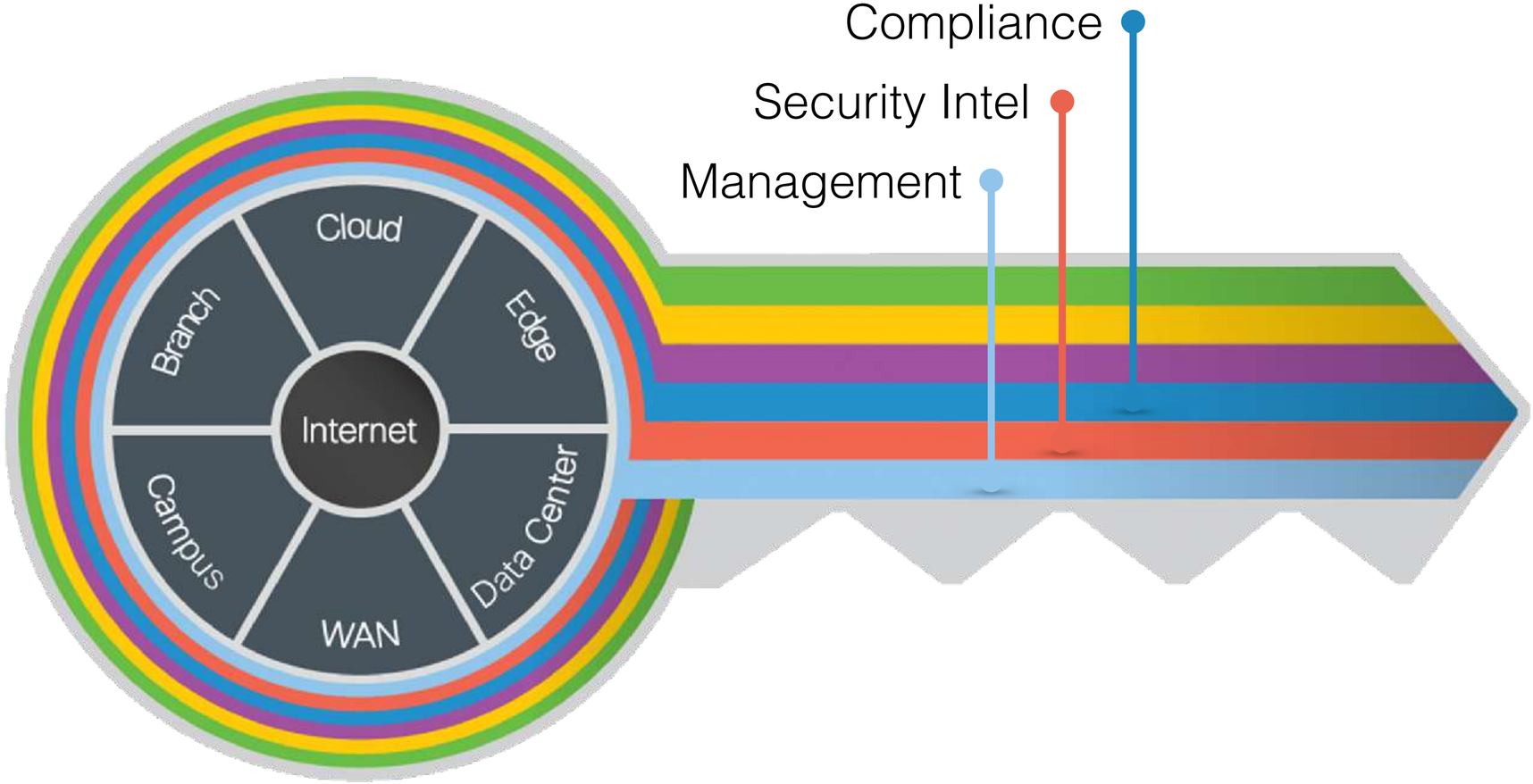
- Intelligence of emerging threats



Cyber Threat Defense

Compliance:

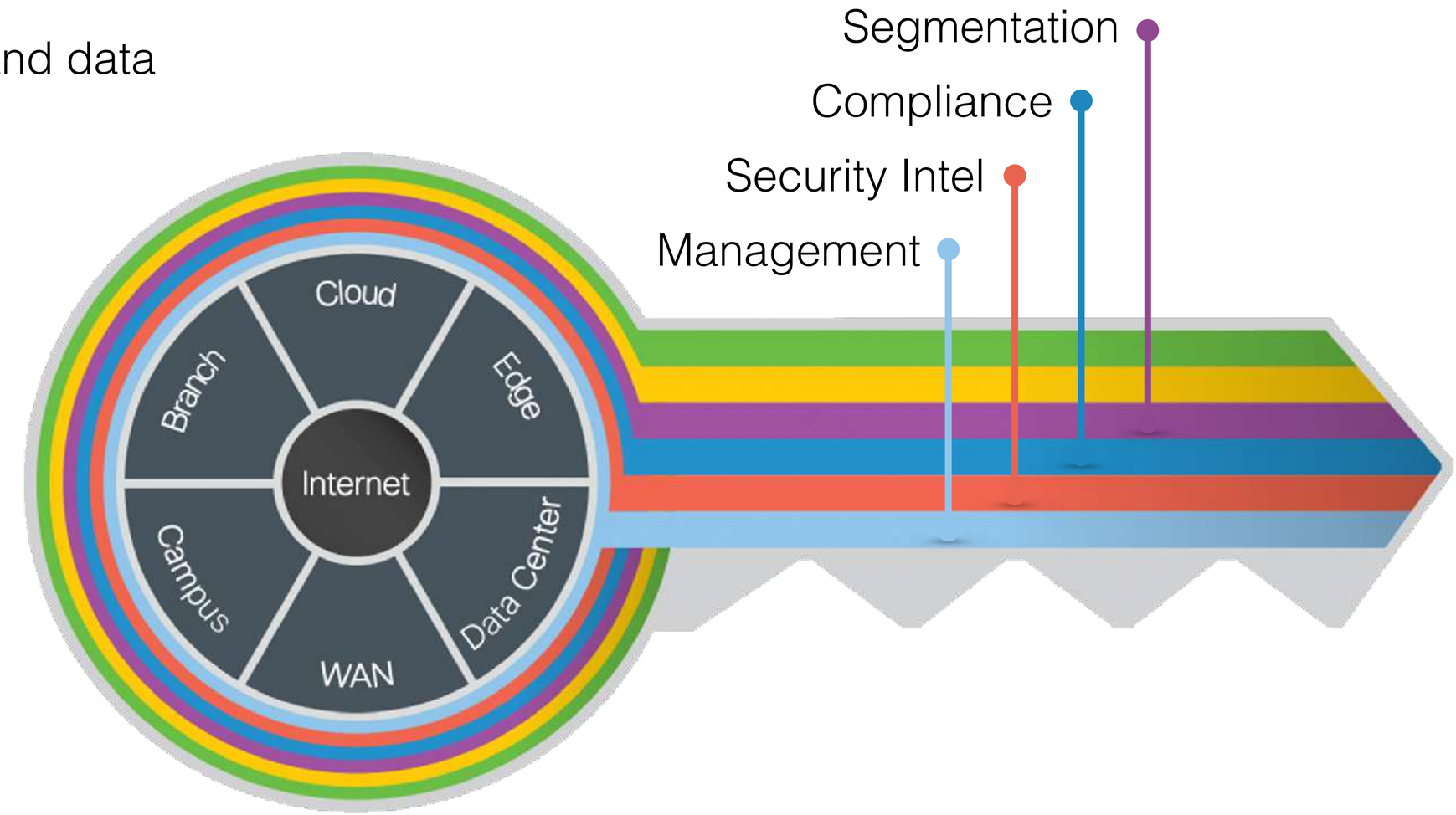
- Internal and external policies



Cyber Threat Defense

Segmentation:

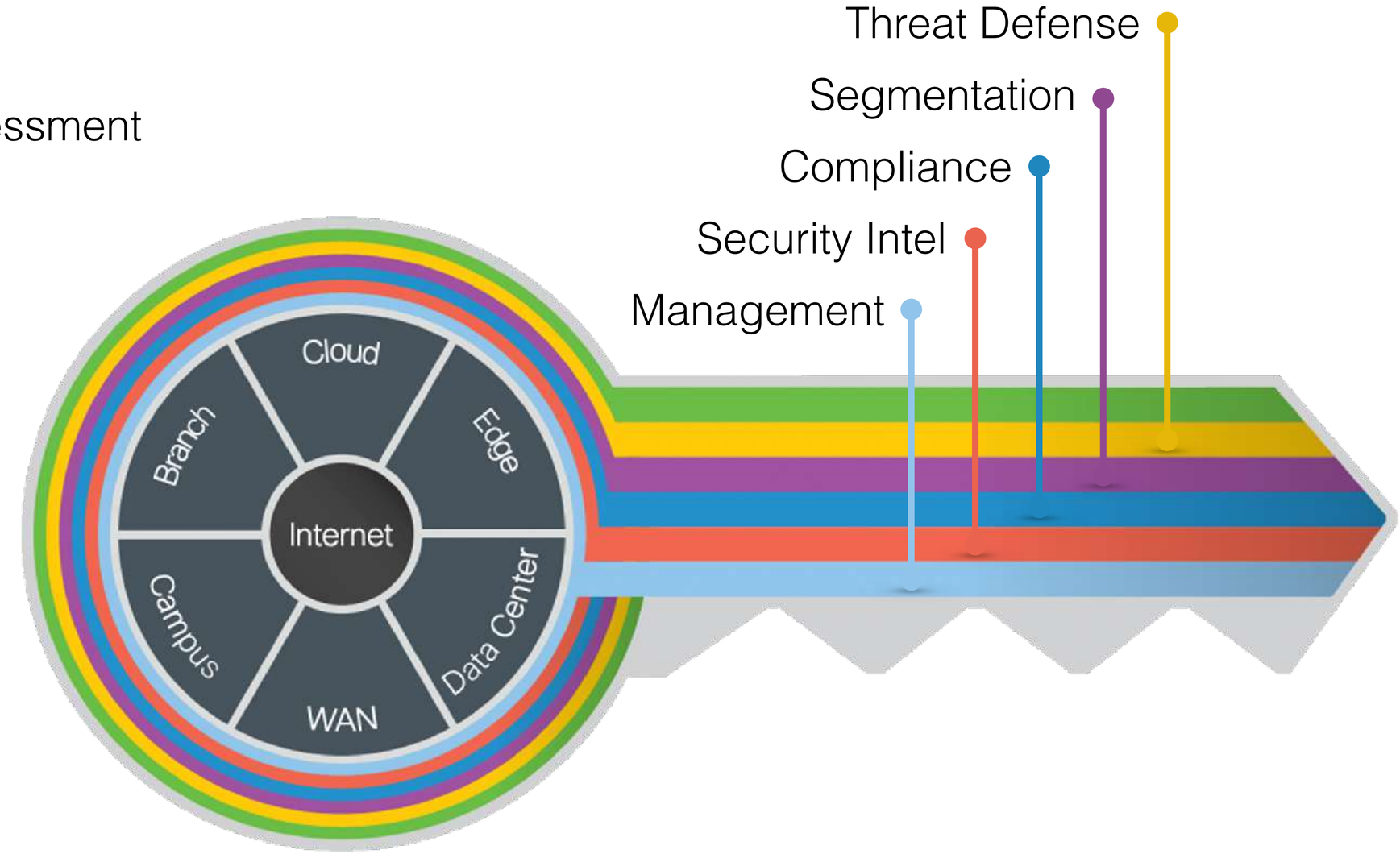
- Boundaries for users and data



Cyber Threat Defense

Threat Defense:

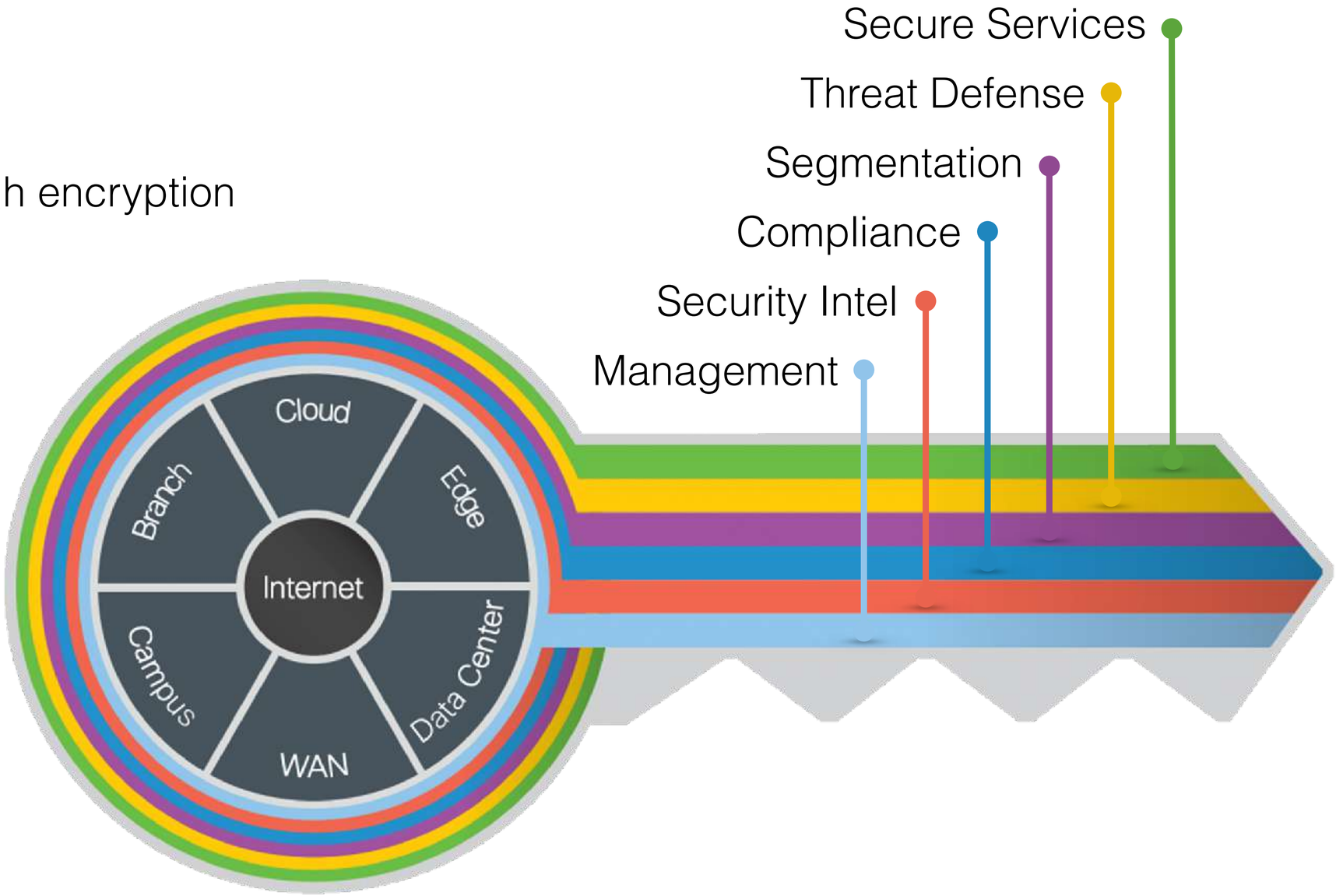
- Visibility for traffic assessment



Cyber Threat Defense

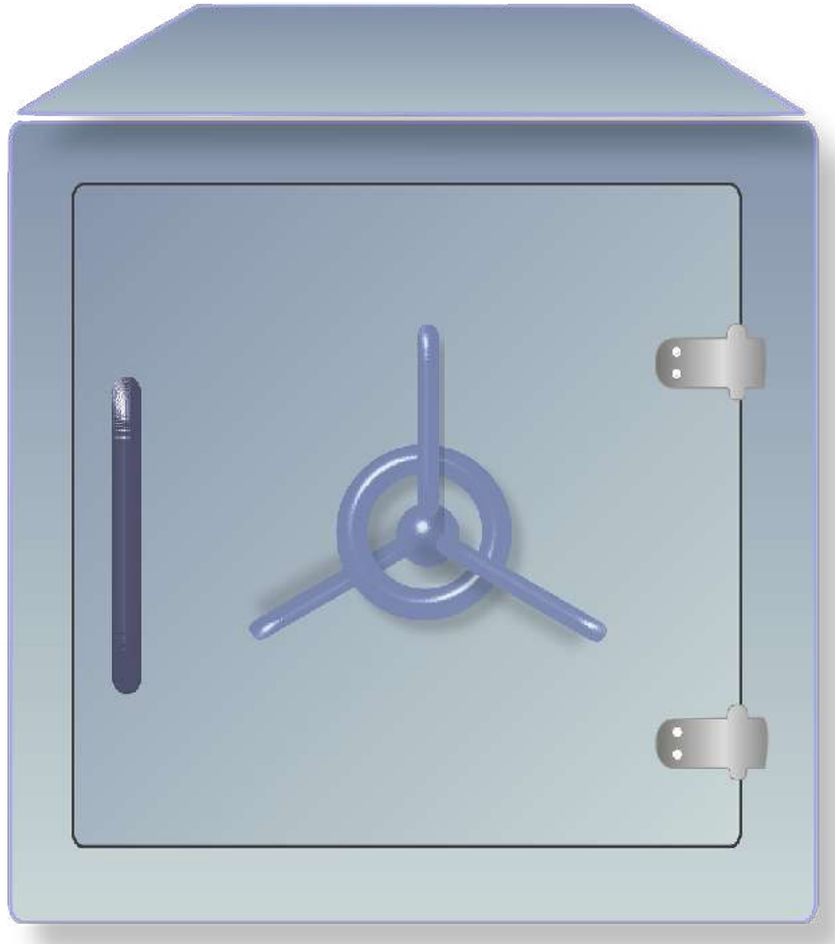
Secure Services:

- Traffic protection through encryption



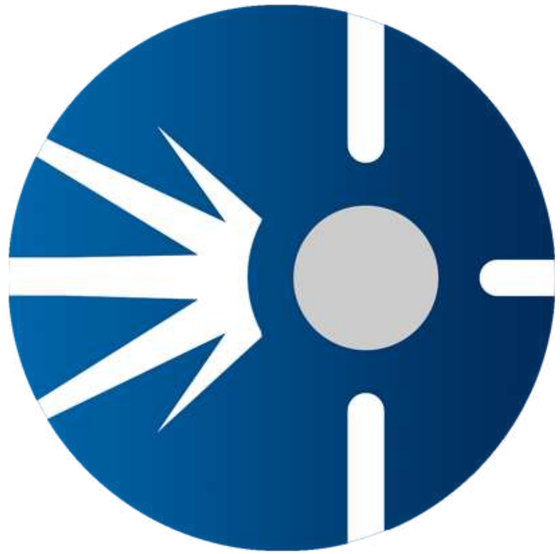
Endpoint Hardening

Endpoint Hardening



Endpoint Hardening

AMP for
Endpoints



- AMP = Advanced Malware Protection
- Prevention, detection, and response
- Intelligence from cloud-based analytics

Endpoint Hardening

Cisco TALOS:

- Global stats for threat tracking
- Feeds threat intel into Cisco AMP

Cisco ThreatGRID:

- Static and behavioral file analysis
- Used in conjunction with Cisco TALOS

Endpoint Hardening

AMP for
Endpoints

Detection Mechanisms:

- Continual endpoint monitoring
- Vulnerable software detection and reporting

Endpoint Hardening

AMP for
Endpoints

Response Mechanisms:

- Endpoint forensics
- File and device trajectories
- Powerful analysis and tracking features

Endpoint Hardening

Cisco Umbrella:

- Previously OpenDNS
- DNS filtering service for internet destinations
- Machine learning continually updates database

Endpoint Hardening

Deployment:

- Add network public IP address into configuration
- Point all network DNS to Umbrella
- Prevent end users from changing local DNS with firewall rules

Endpoint Hardening

Cisco AnyConnect VPN

Cisco AnyConnect VPN:

- Provides access to enterprise network over public networks
- Used in conjunction with Cisco Adaptive Security Appliance (ASA)

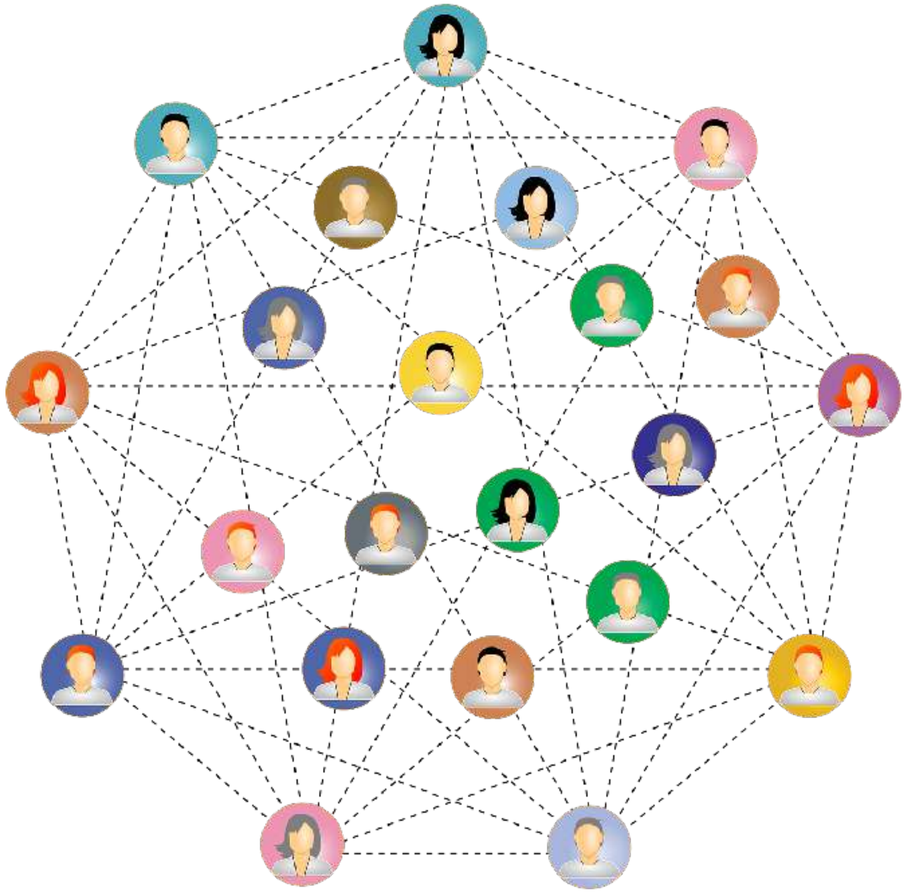
Endpoint Hardening

Cisco AnyConnect VPN:

- Provides access to enterprise network over public networks
- Used in conjunction with Cisco Adaptive Security Appliance (ASA)

Cisco TrustSec

Cisco TrustSec



Traditional Access Control:

- Based on topologies and segmentation
- Modern networks require flexibility
- Cisco TrustSec offers access control through contextual identification

Cisco TrustSec

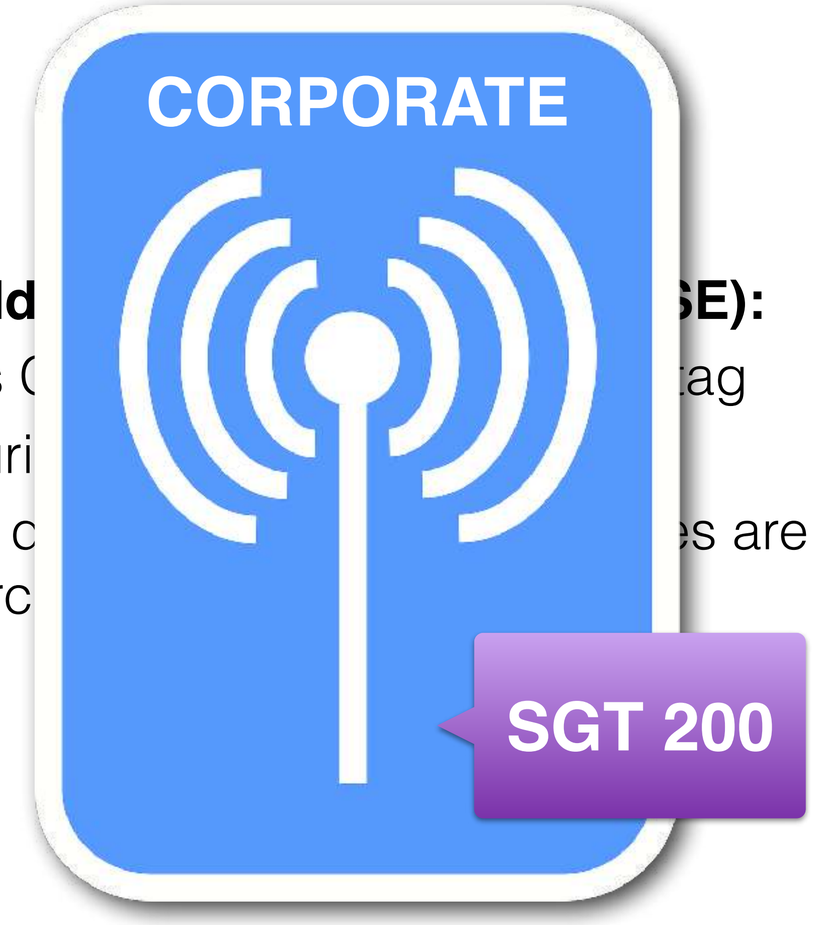
Cisco Identity Services Engine (ISE):

- Uses Cisco TrustSec to assign a tag
- Security Group Tag (SGT)
- Tags dictate which access policies are enforced throughout the network

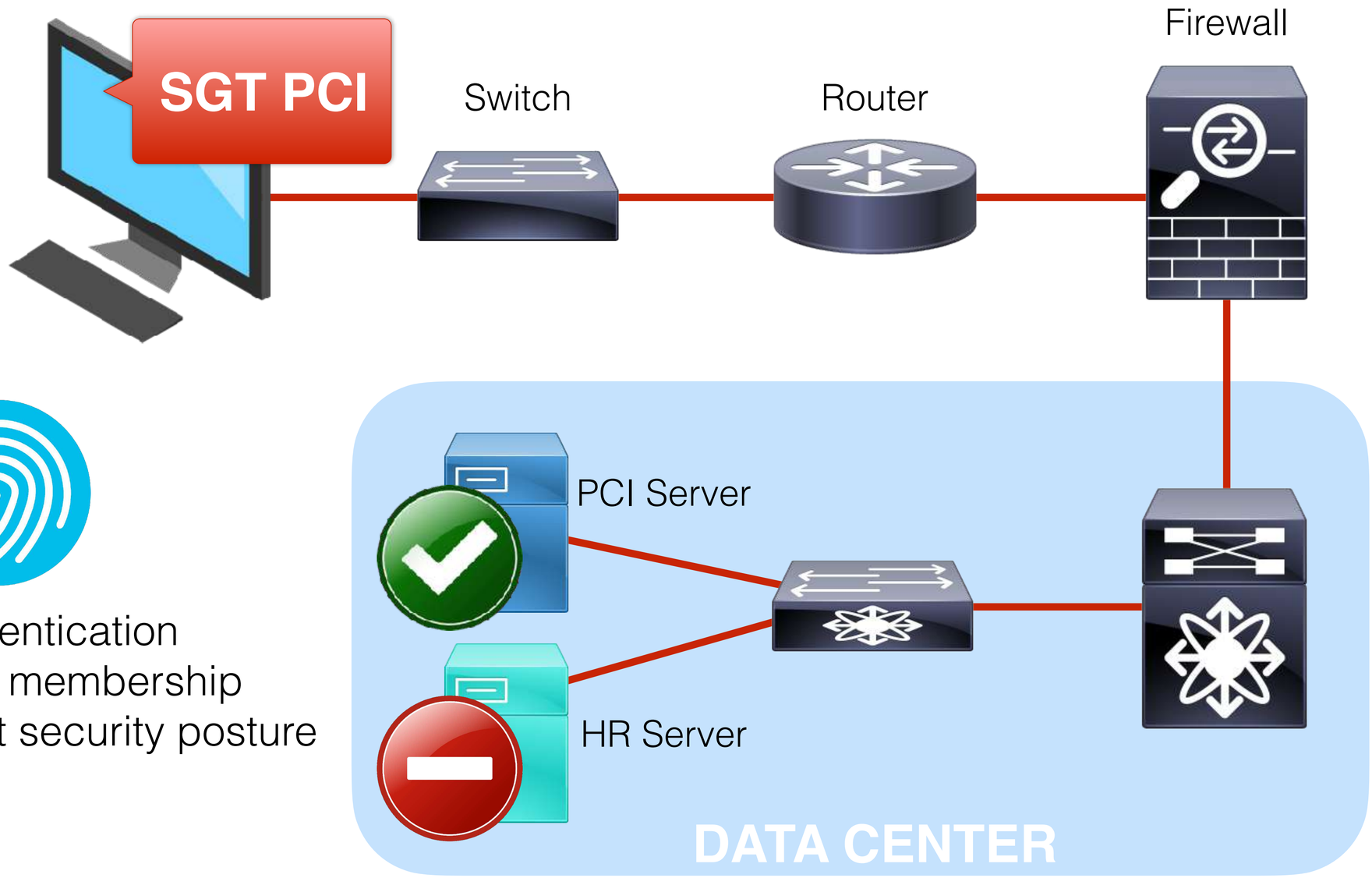
Cisco TrustSec

Cisco Id **SE):**

- Uses C tag
- Securi
- Tags c es are enforc

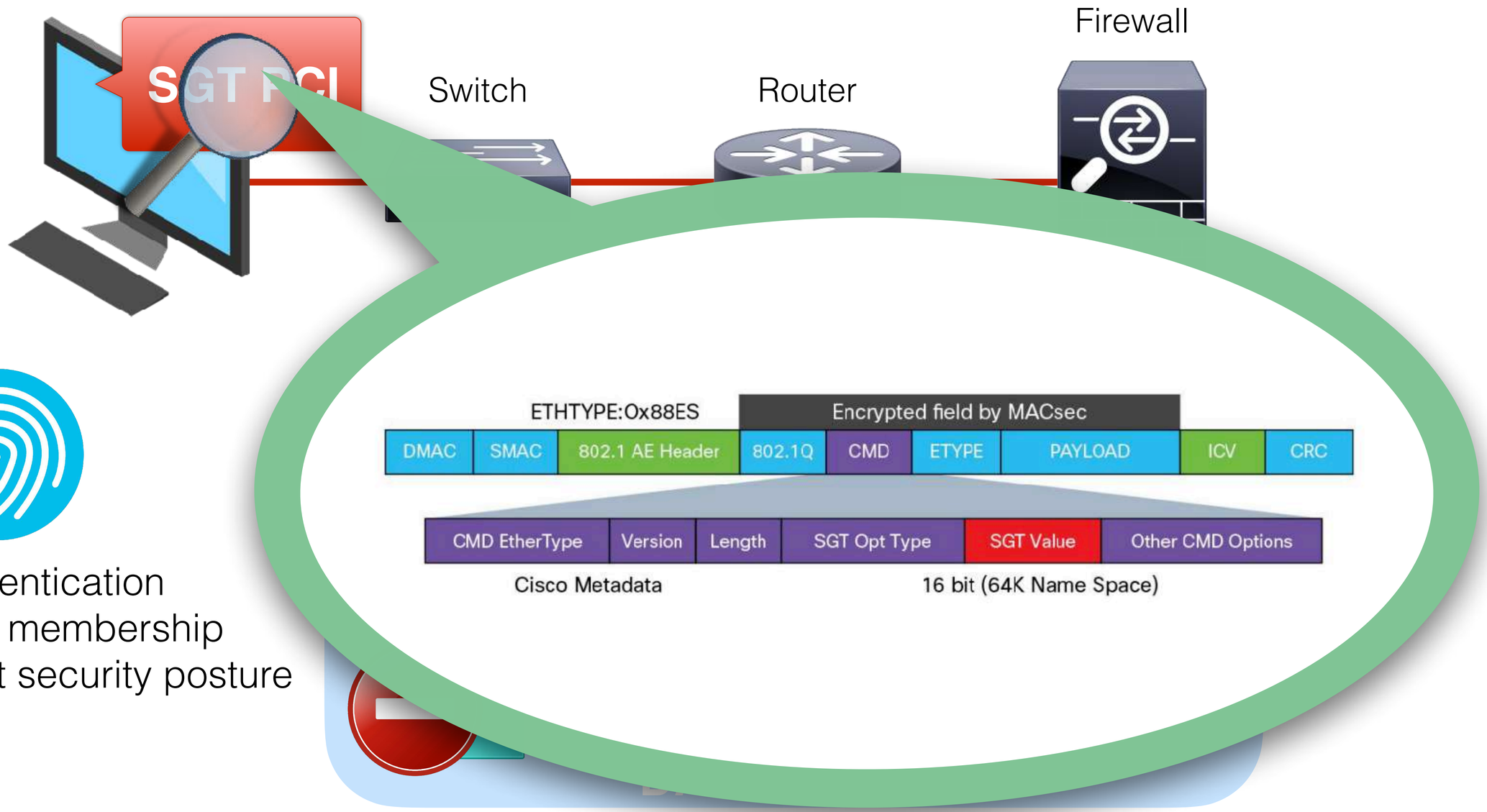


Cisco TrustSec



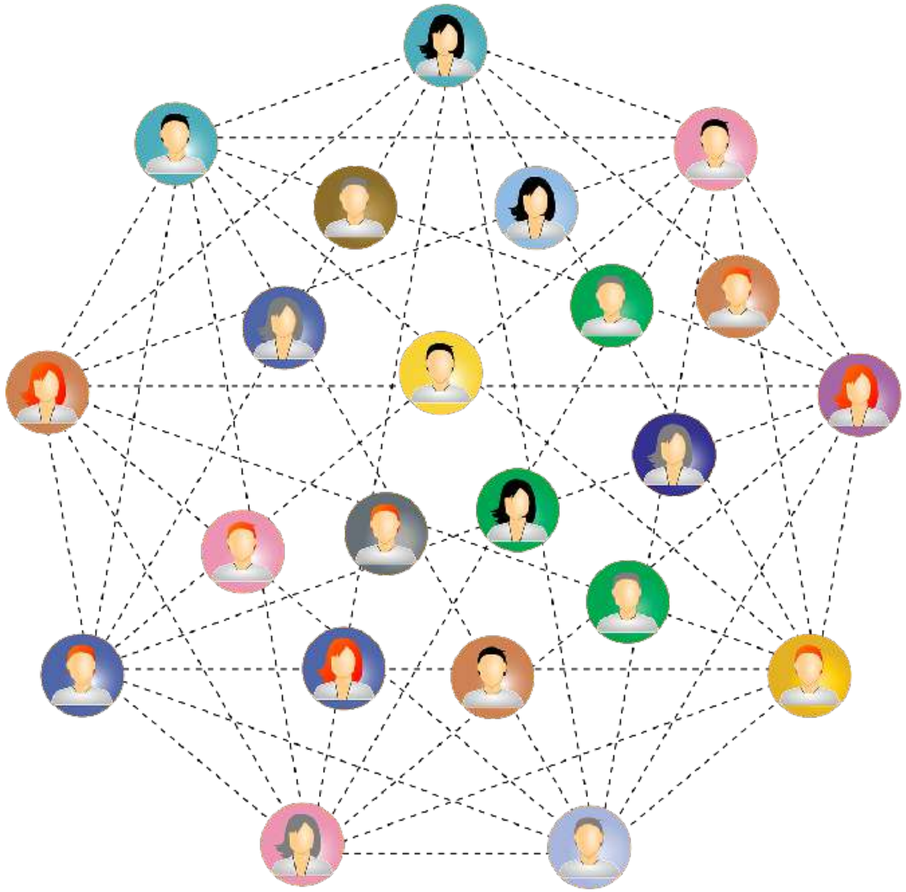
- User authentication
- AD group membership
- Compliant security posture

Cisco TrustSec



- User authentication
- AD group membership
- Compliant security posture

Cisco TrustSec



Advantages of Cisco TrustSec

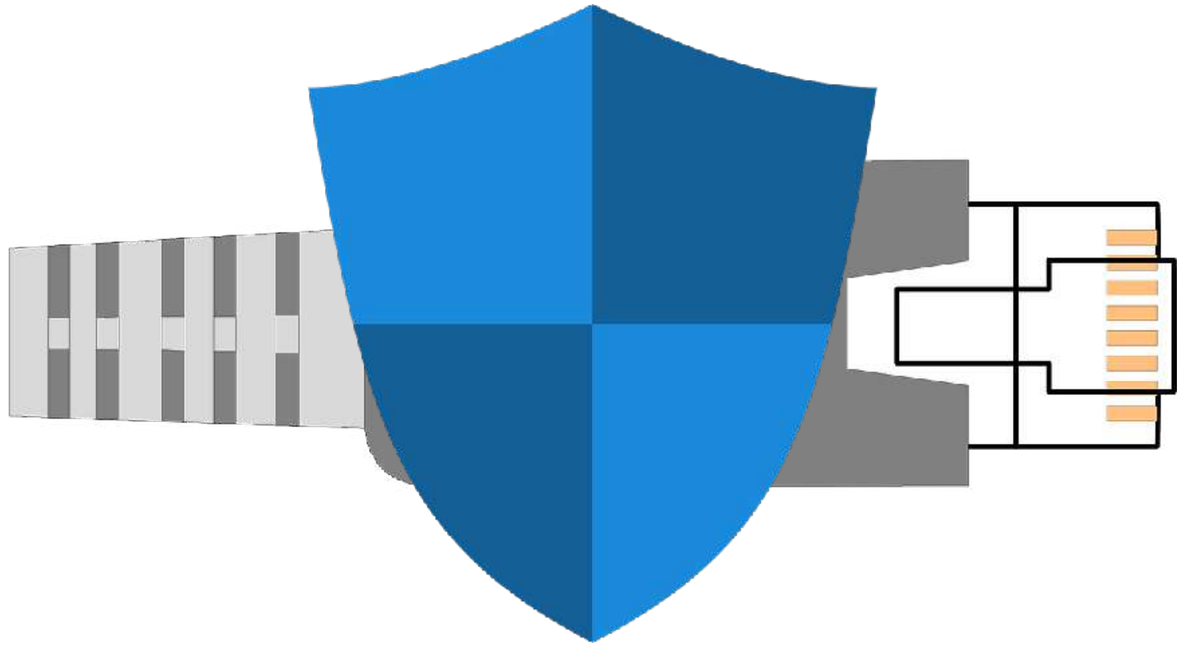
- Highly scalable and efficient
- No topology changes necessary when altering access control
- Not a replacement for traditional methods such as VLANs and subnets, but a supplement

Media Access Control Security (MacSec)

Media Access Control Security (MACsec)

MACsec:

- IEEE 802.1AE
- Layer 2 protocol
- Confidentiality and integrity over Ethernet



Media Access Control Security (MACsec)

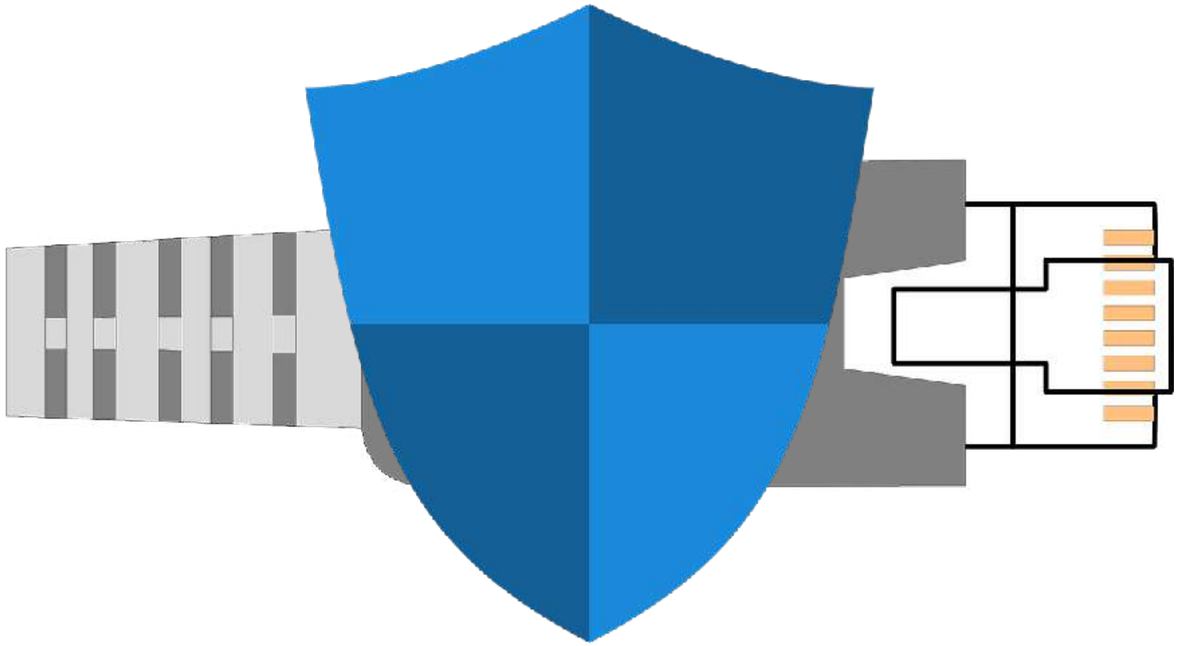
MACsec:

- IEEE 802.1AE
- Layer 2 protocol
- Confidentiality and integ

Media Access Control Security (MACsec)

MACsec:

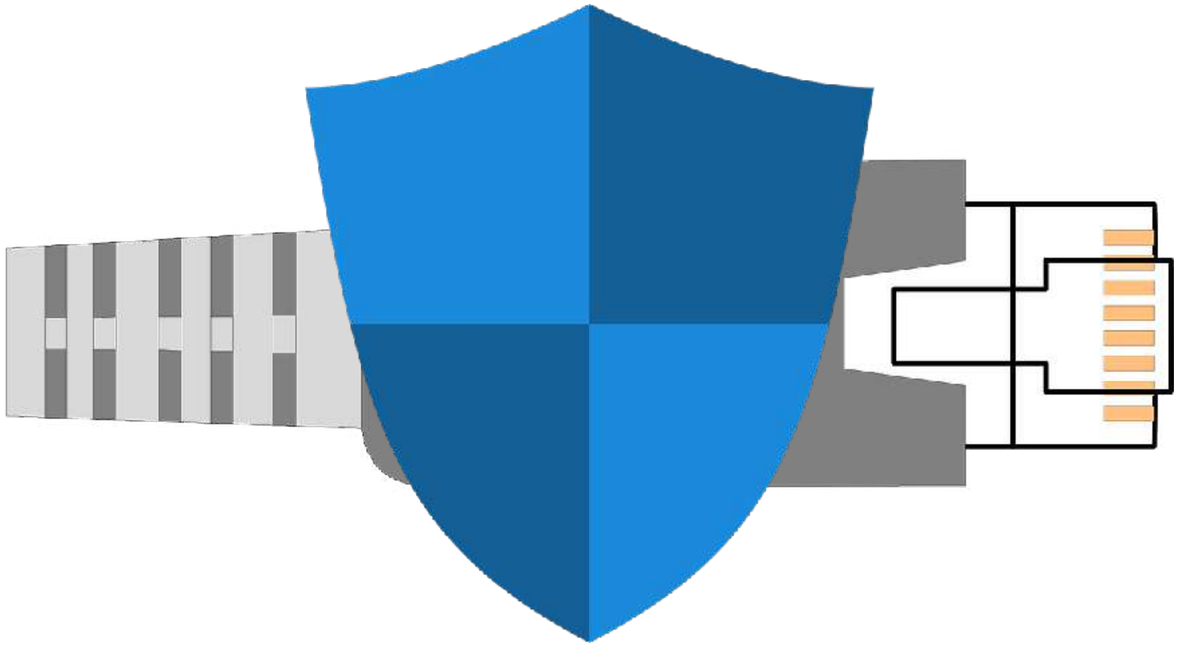
- Wired equivalent of WPA/WPA2 protection
- More viable option than IPsec everywhere
- 128-bit AES-GCM encryption



Media Access Control Security (MACsec)

MACsec:

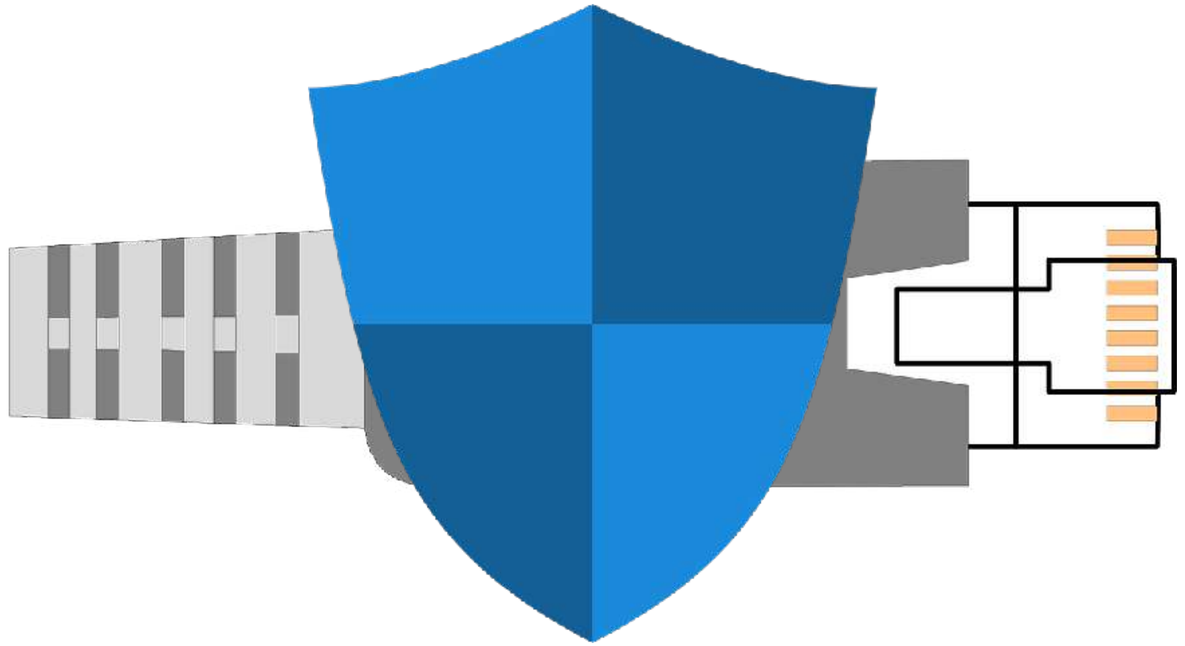
- Only encrypted between MACsec peers
- Internally on a switch, traffic is unencrypted
- Still allows for deep packet inspection



Media Access Control Security (MACsec)

MACsec:

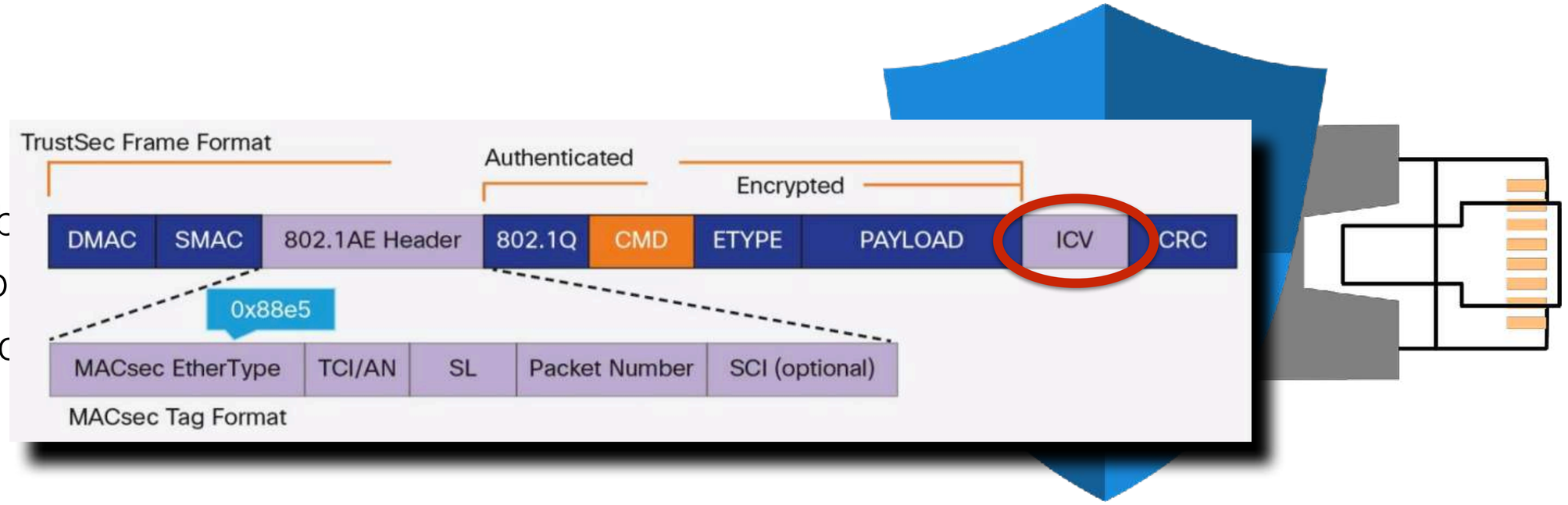
- Processed by switch ASICs
- ASICs perform encryption/decryption
- Less strenuous than IPsec encryption



Media Access Control Security (MACsec)

MACsec:

- Processed b
- ASICs perfo
- Less strenuc



Media Access Control Security (MACsec)

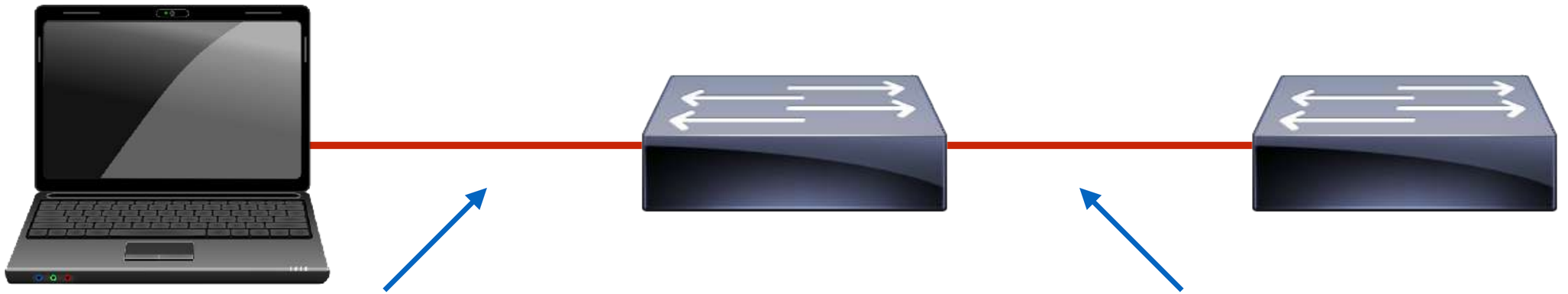
Security Association Protocol (SAP):

- Line-rate encryption/decryption
- 128-bit AES-GCM encryption
- Cisco-proprietary
- Used between Cisco switches

MACsec Key Agreement (MKA) Protocol:

- Line-rate encryption/decryption
- 128-bit AES-GCM encryption
- Open industry standard
- Used between endpoints and switches

Media Access Control Security (MACsec)



Downlink MACsec:

- Encrypted link between client and switch
- MACsec Key Agreement (MKA) protocol
- Requires supplicant software
- MACsec can be required or optional

Uplink MACsec:

- Encrypted link between switches
- Security Association Protocol (SAP)
- MKA option available
- Dynamic or manual negotiation

- Commonly layered with TrustSEC to add authentication