Network Defense and Monitoring

Dr Hisain Elshaafi

Outline

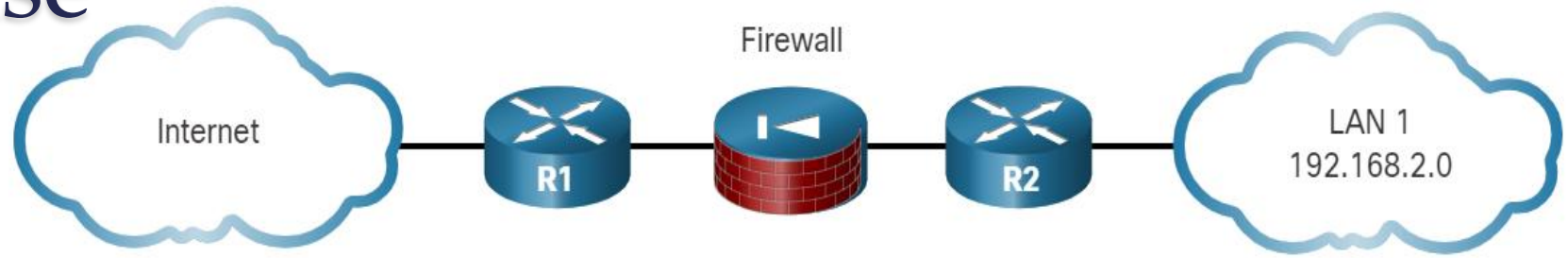
- Defense in Depth
- Network Security Infrastructure
- Access Control
- AAA
- Antimalware Protection
- Network Security Data
- Network Security Monitoring
- Security Onion
- Snort rules

Defense in Depth

Layered Defense

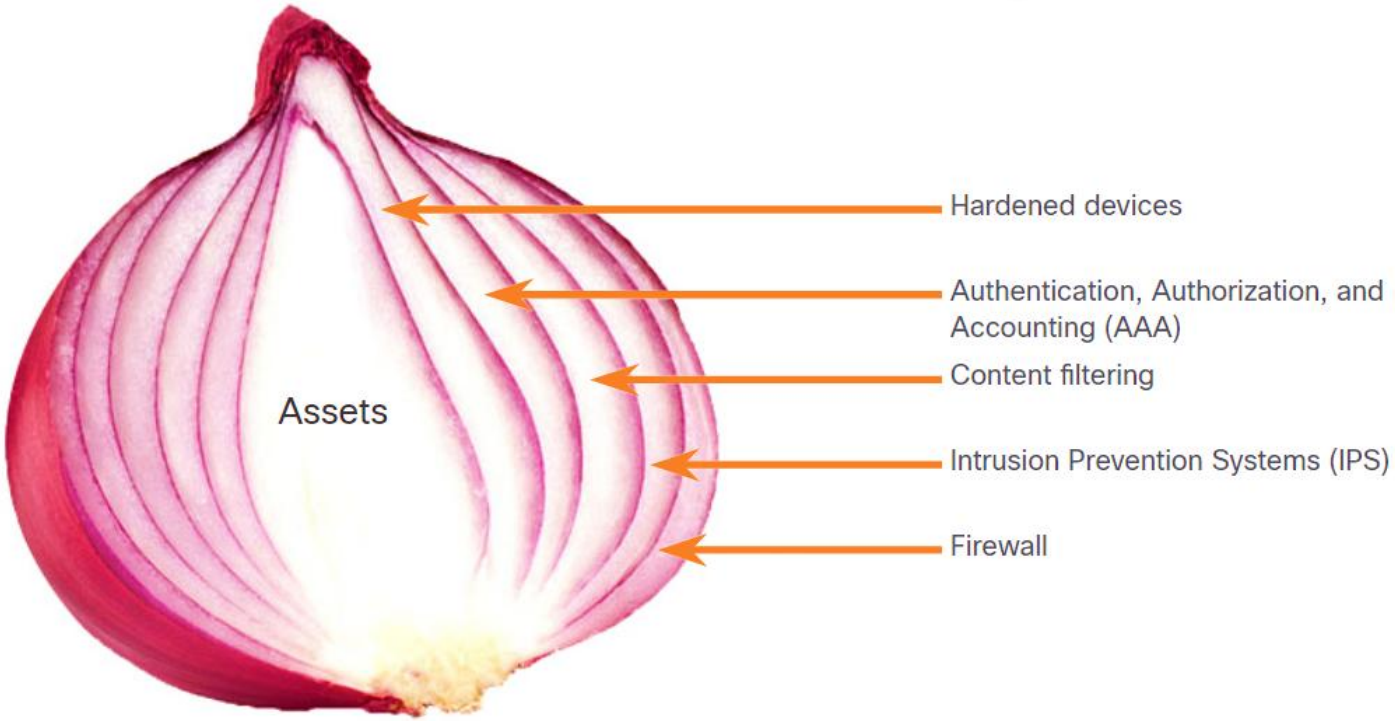
- **Defense-in-depth**
  - **Identify threats** and **secure vulnerable assets**
- **Multiple layers** of security
  - At network edge, within network, on endpoints
  - Router screens traffic, **forwards** to firewall e.g. Cisco ASA
  - IPS, advanced malware protection (AMP), web/email security systems, identity services, access controls, ...
- Different layers form **security architecture**
  - Failure of one safeguard **does not** affect other safeguards

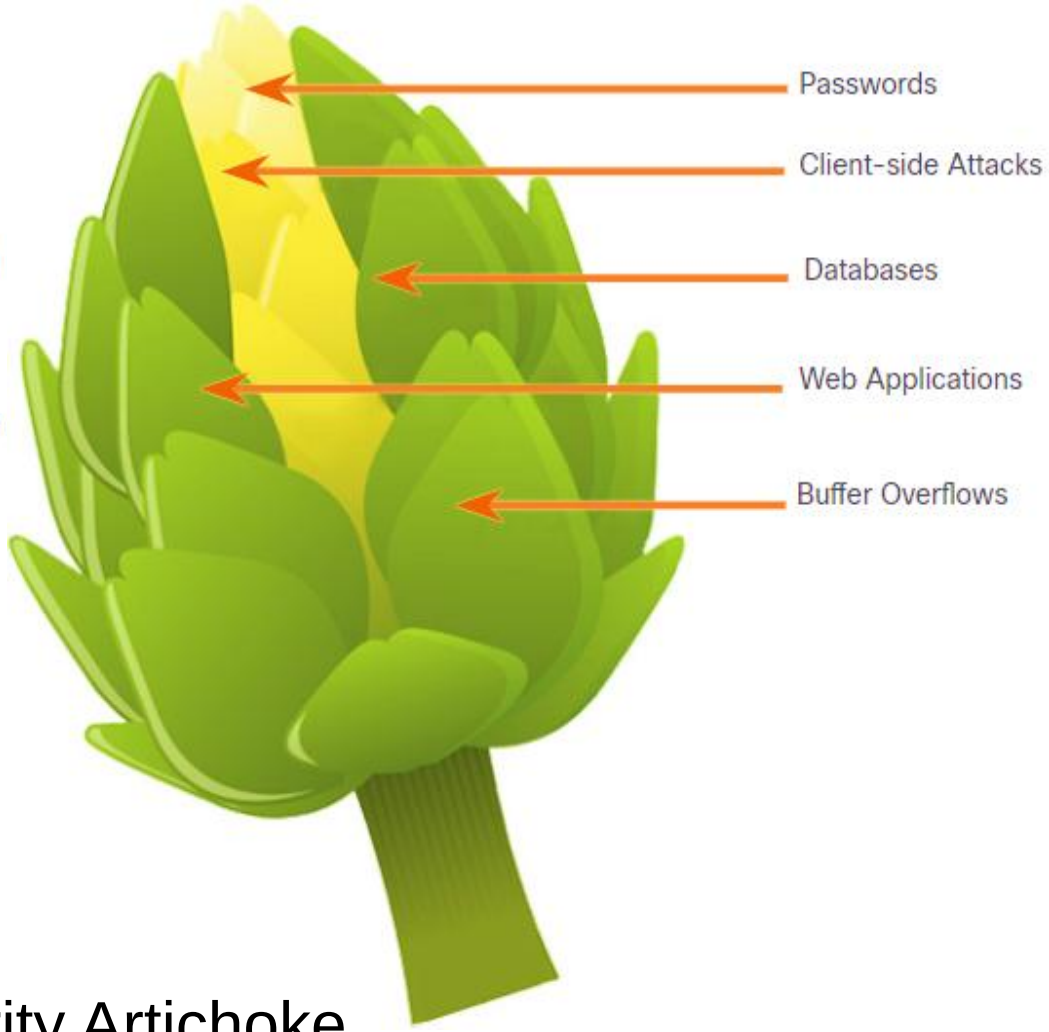
Layered Defense



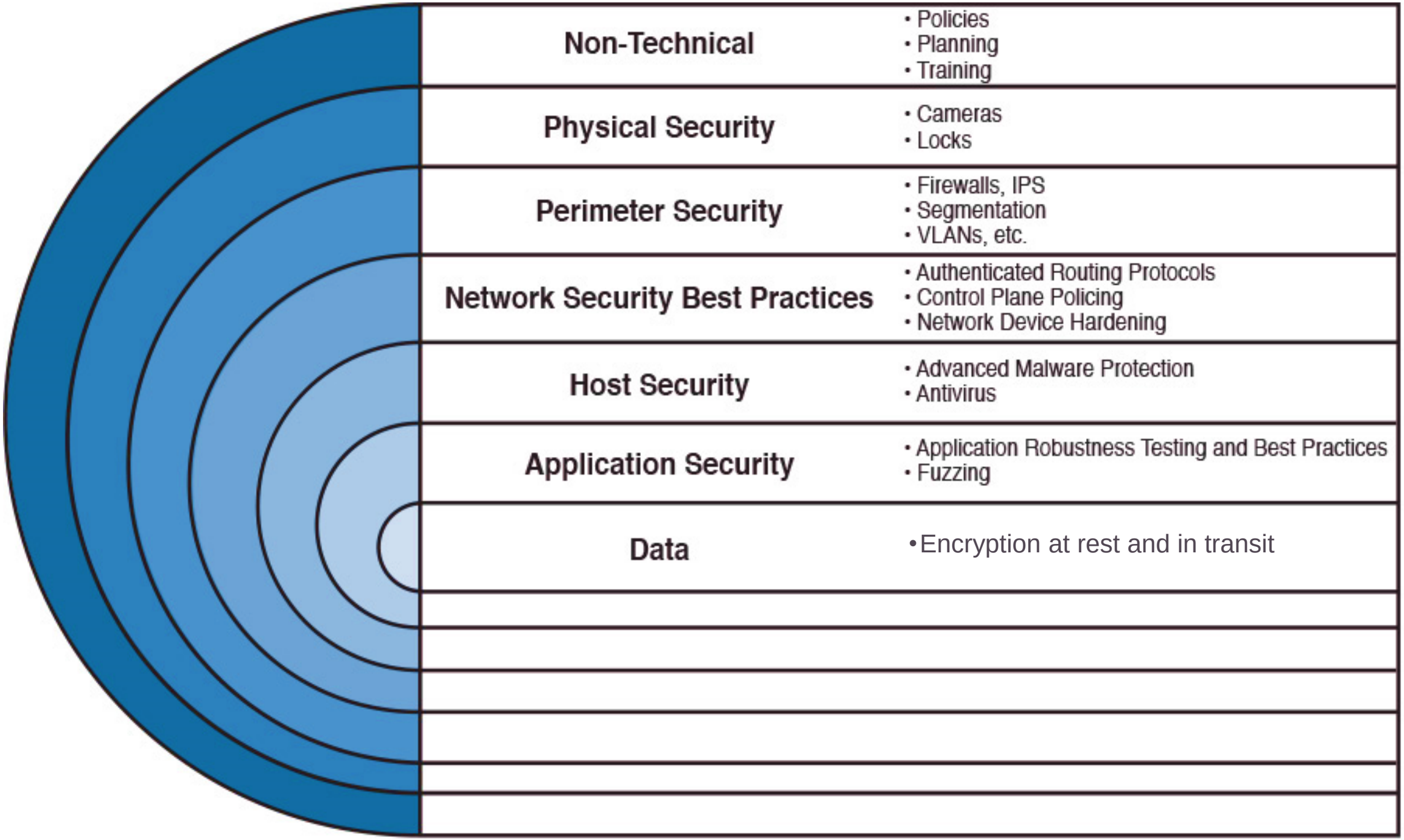
1. **Edge router**
   - First line of defense
   - Set of **rules** for what traffic it allows/denies
   - Passes connections intended for internal LAN to firewall
2. **Firewall**
   - Additional filtering and tracking **state of connections**
   - Deny **initiation** of connections from untrusted to trusted network
   - Allow **internal users** to establish connections to untrusted networks
3. **Internal router**
   - Apply **further filtering** on traffic before it is forwarded to destination

Visualizing Defense in Depth



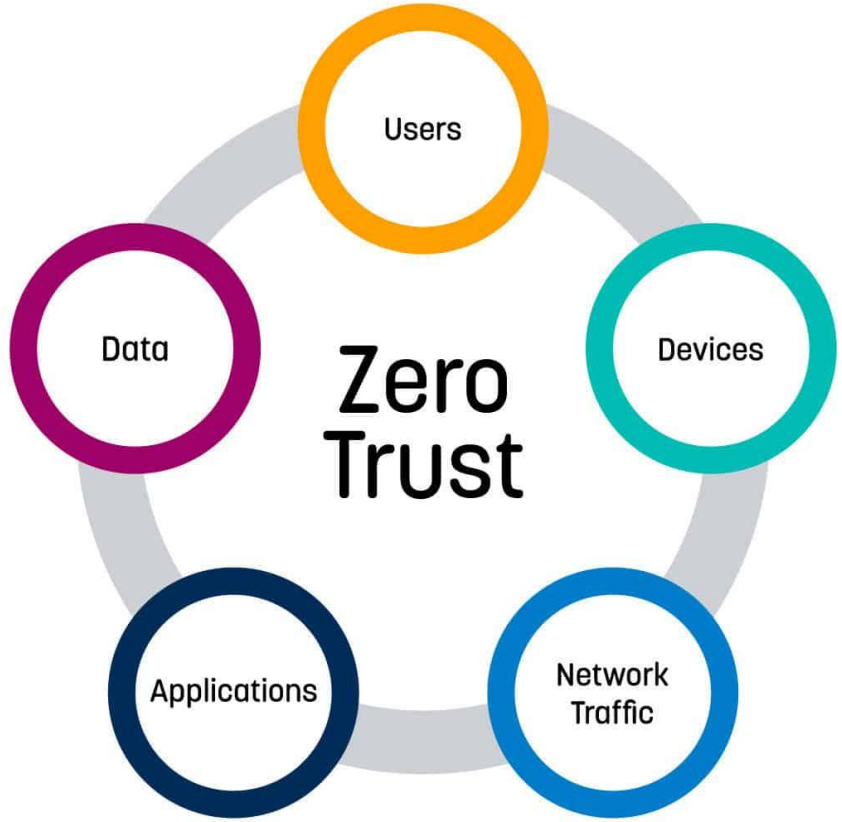


Security Artichoke


Non-Technical
• Policies
• Planning
• Training
Physical Security
• Cameras
• Locks
Perimeter Security
• Firewalls, IPS
• Segmentation
• VLANs, etc.
Network Security Best Practices
• Authenticated Routing Protocols
• Control Plane Policing
• Network Device Hardening
Host Security
• Advanced Malware Protection
• Antivirus
Application Security
• Application Robustness Testing and Best Practices
• Fuzzing
Data
• Encryption at rest and in transit

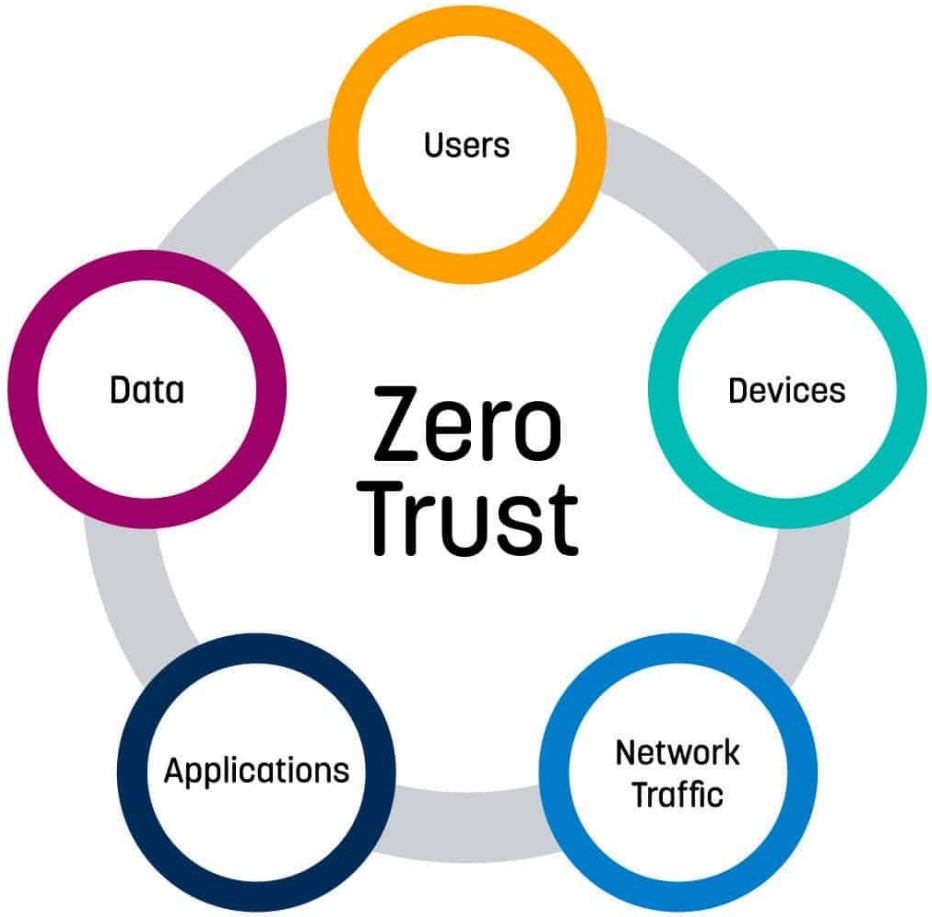
Zero Trust Security

- *Never trust always verify*
- **Comprehensive** approach to securing access
  - networks, applications, databases and environments
- Secure access from **users**, **devices**, **microservices**, **containers**, ...
- All users **in** or **outside network**, to be authenticated, authorized and continuously validated for security configuration



Zero Trust Security (cont)

- Remote users, hybrid cloud, ransomware, borderless networking, BYOD, mobile, …
- **Benefits**
  - **Prevent** unauthorized access
  - **Contain** breaches
  - Reduce risk of **lateral** attacks

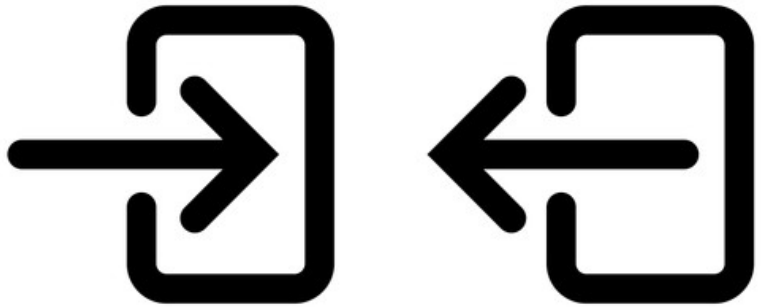


Zero Trust Security (cont)

NIST Zero Trust Architecture (NIST Special Publication 800-207, 8/2020)
Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows…Zero trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource.

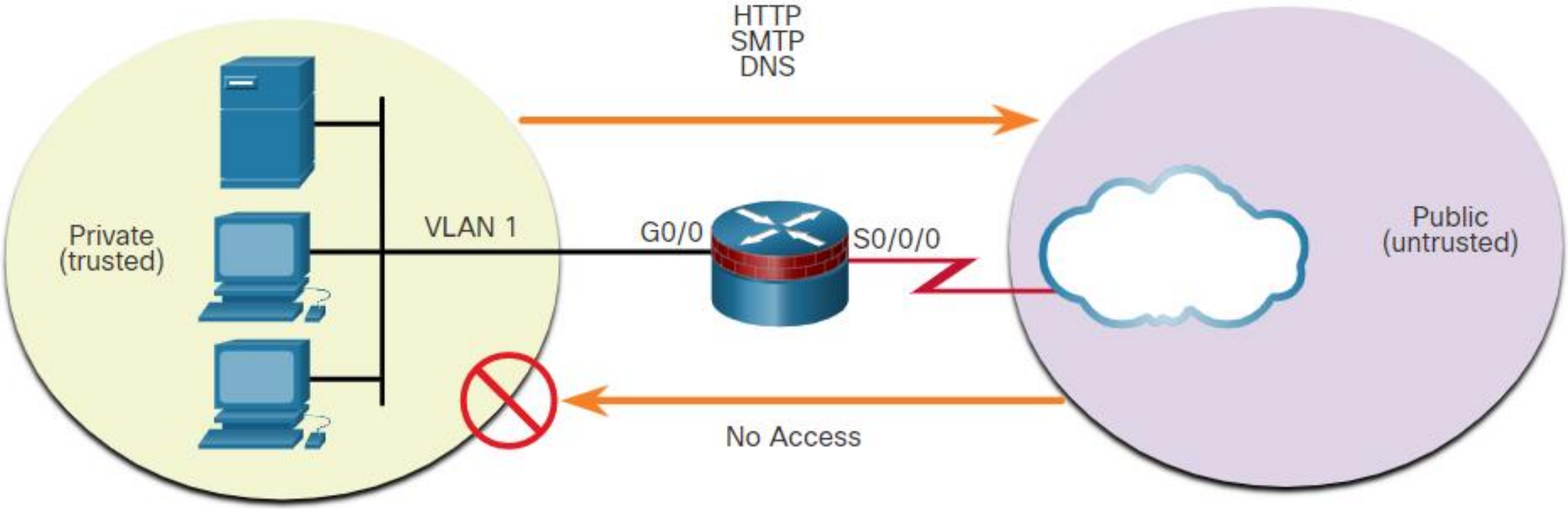
Attack Surface

- Sum of system **vulnerabilities** (attack **vectors**) accessible to attackers
  - Compromised credentials, weak and stolen passwords, malicious insiders, missing or poor encryption, misconfiguration, trust
- **Network** Attack Surface
  - network protocols, open ports
- **Software** Attack Surface
  - web, cloud, or host-based software
- **Human** Attack Surface
  - weaknesses in user behavior
- Discovering, reducing and monitoring



Network Security Infrastructure

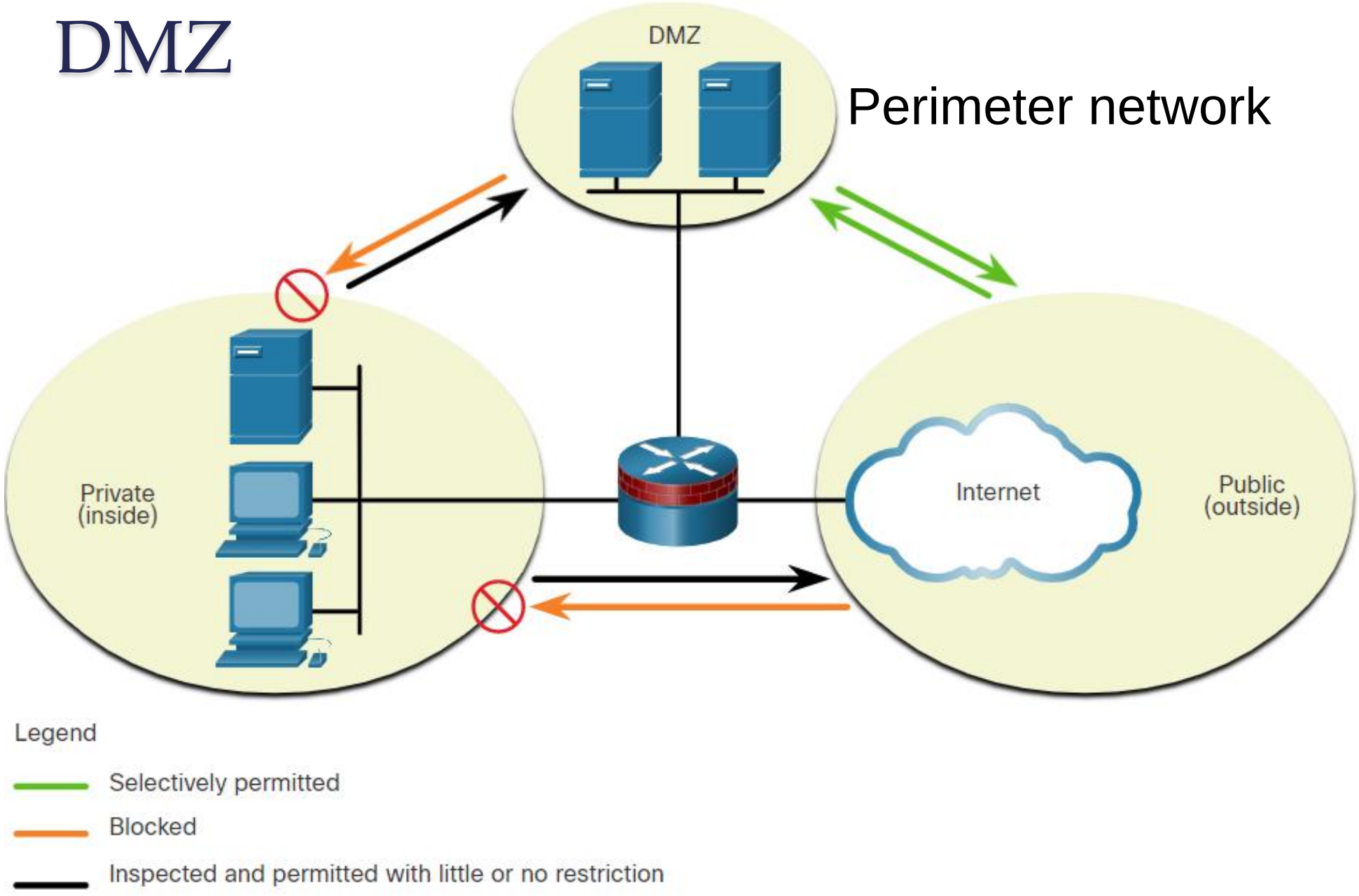
Public vs Private Networks



- Configure and manage network **security**
- Enforce **policies**
- Achieve network **segmentation**

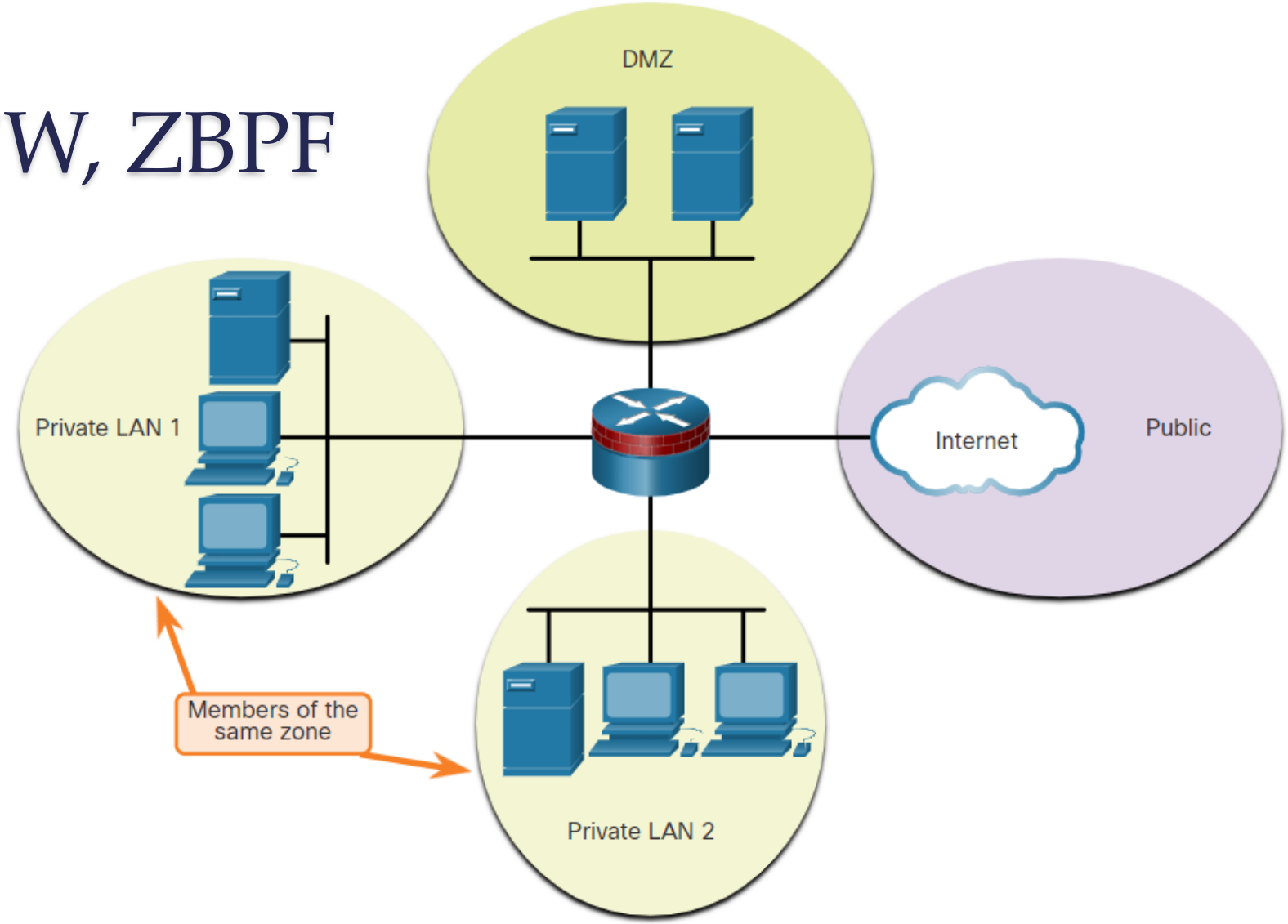
DMZ

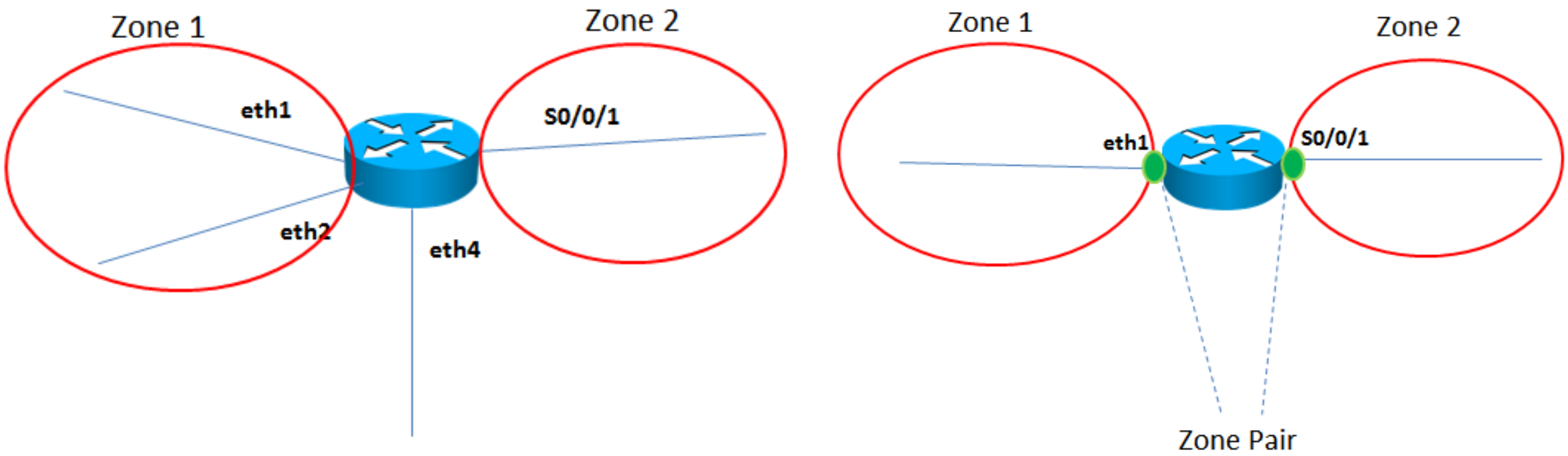
Perimeter network



Zone-based Policy Firewalls

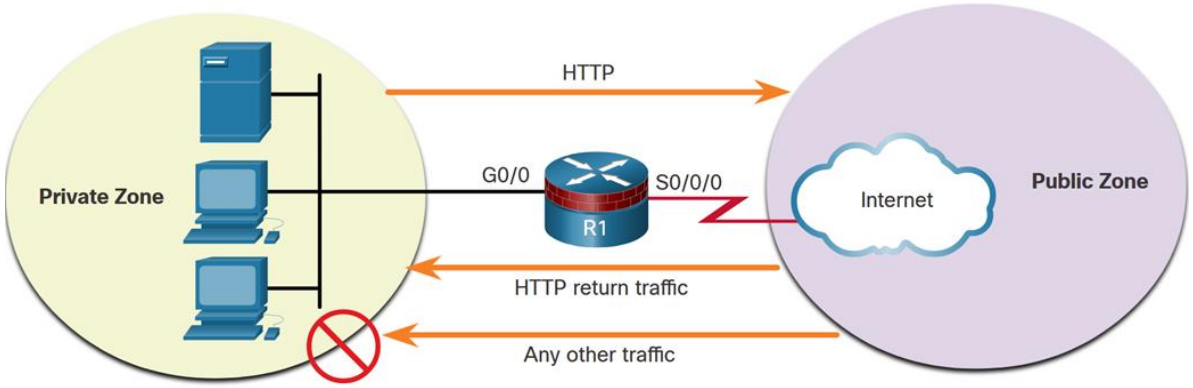
ZPF, ZFW, ZBPF





Firewall Policy Actions

inspect	An action that offers statebased traffic control. The router maintains session information for TCP and UDP and permits return traffic.
drop	Discards unwanted traffic
pass	A stateless action the allows the router to forward traffic from one zone to another




```
Router(config)# zone security zone-name
```

```
R1(config)# zone security PRIVATE
R1(config-sec-zone)# exit
R1(config)# zone security PUBLIC
R1(config-sec-zone)# exit
R1(config)#
```

Step 1: Create the zones.

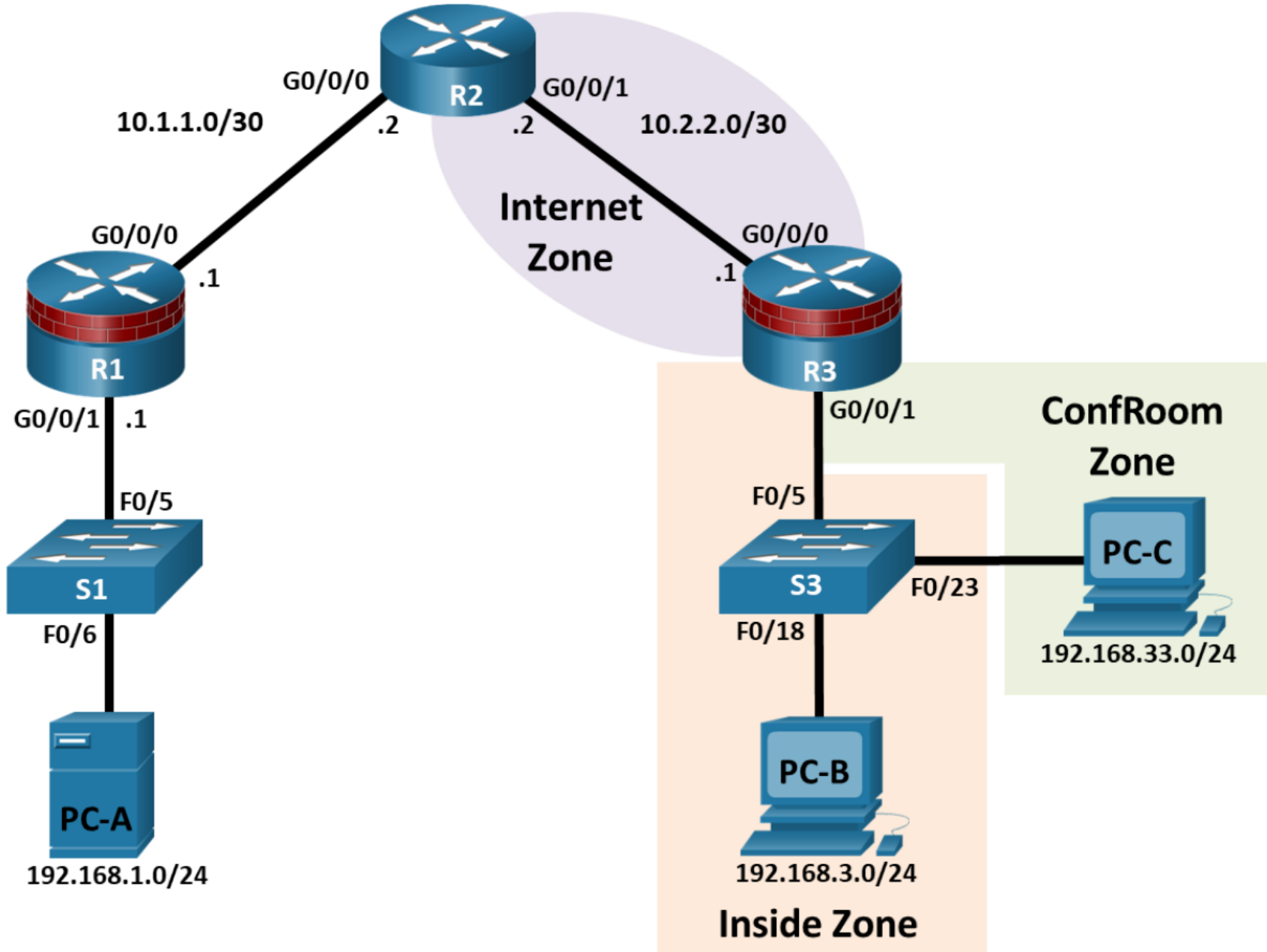
Step 2: Identify traffic with a class-map.

Step 3: Define an action with a policy-map.

Step 4: Identify a zone pair and match it to a policy-map.

Step 5: Assign zones to the appropriate interfaces.

```
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# zone-member security PRIVATE
R1(config-if)# interface Serial 0/0/0
R1(config-if)# zone-member security PUBLIC
```


R2
G0/0/0
G0/0/1
10.1.1.0/30
.2
.2
10.2.2.0/30
Internet
Zone
G0/0/0
.1
.1
R1
R3
G0/0/1
.1
G0/0/1
ConfRoom
Zone
F0/5
F0/5
S1
S3
F0/23
PC-C
F0/6
F0/18
192.168.33.0/24
PC-A
PC-B
192.168.1.0/24
192.168.3.0/24
Inside Zone

```
R3(config)# zone security INSIDE
R3(config)# zone security INTERNET
```
(1)

```
R3(config)# class-map type inspect match-any INSIDE_PROTOCOLS
R3(config-cmap)# match protocol tcp
R3(config-cmap)# match protocol udp
R3(config-cmap)# match protocol icmp
```
(2)

```
R3(config)# policy-map type inspect INSIDE_TO_INTERNET
R3(config-pmap)# class type inspect INSIDE_PROTOCOLS
R3(config-pmap-c)# inspect
```
(3)

```
R3(config)# zone-pair security INSIDE_TO_INTERNET source INSIDE destination
INTERNET
```
(4)

```
R3(config)# zone-pair security INSIDE_TO_INTERNET
R3(config-sec-zone-pair)# service-policy type inspect INSIDE_TO_INTERNET
```

```
R3(config)# interface g0/0/1.3
R3(config-if)# zone-member security INSIDE
```
(5)

```
R3(config)# interface g0/0/0
R3(config-if)# zone-member security INTERNET
```

Firewalls

Allow traffic from any external address to the web server.

Allow traffic to FTP server.

Allow traffic to SMTP server.

Allow traffic to internal IMAP server.

Deny all inbound traffic with network addresses matching internal-registered IP addresses.

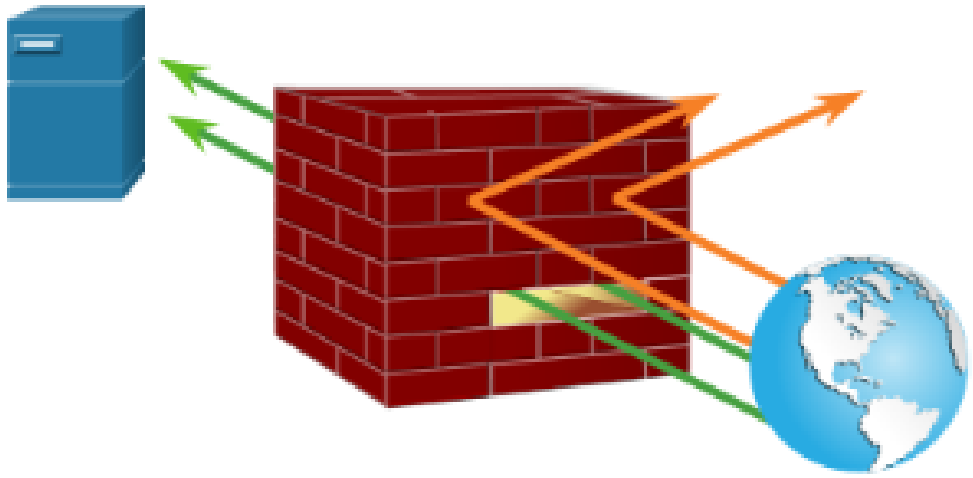
Deny all inbound traffic to server from external addresses.

Deny all inbound ICMP echo request traffic.

Deny all inbound MS Active Directory queries.

Deny all inbound traffic to MS SQL server queries.

Deny all MS Domain Local Broadcasts.



Firewall Benefits and Limitations

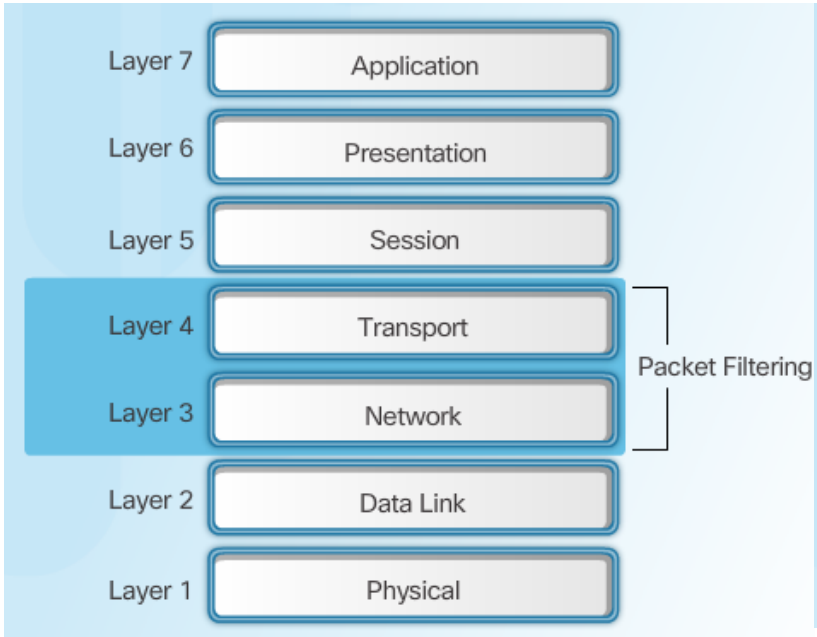
Firewall Benefits	Firewall Limitations
Prevent **exposure** of sensitive hosts and resources to untrusted users	**Misconfigured** firewall e.g. becoming a single point of failure
Sanitize protocol flow preventing exploitation of protocol flaws	Users proactively search for **ways around** firewall exposing network to threat
Block **malicious data** from servers and clients	Network **performance** can slow down
Reduce security **management** complexity	Unauthorized traffic **tunnelled** or hidden as legitimate traffic through firewall

Firewall Best Practices

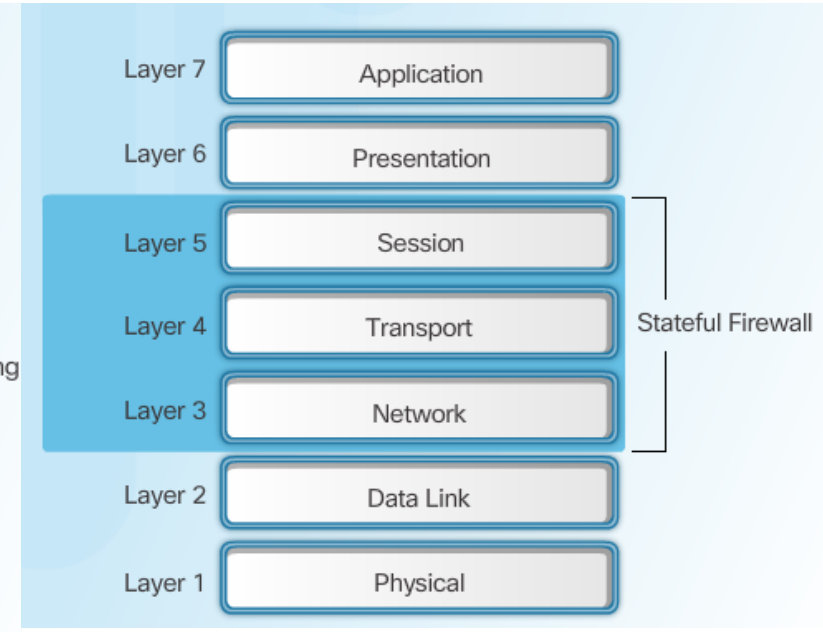
- Position firewalls at security **boundaries**
- It is **unwise** to rely exclusively on a firewall for security
- **Deny all** traffic by default. **Permit only** services needed
- Ensure **physical access** to the firewall is controlled
- Monitor firewall **logs**
- Firewalls primarily protect from attacks originating from **outside**
- Practice **change management** for firewall configuration changes
  - Requesting policy changes
  - Who can authorize change
  - Audit trail
  - Centralized management

Firewall Types

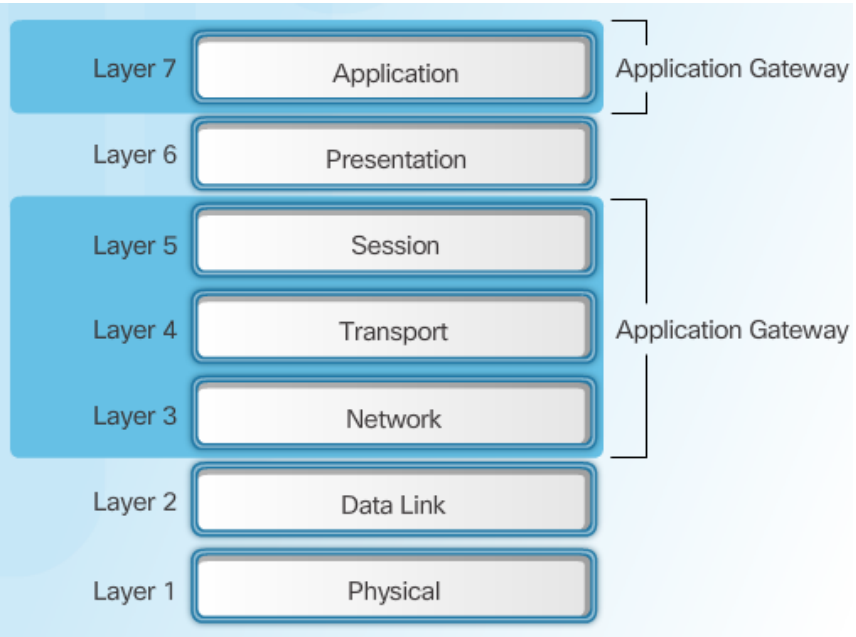
Packet Filtering Firewall



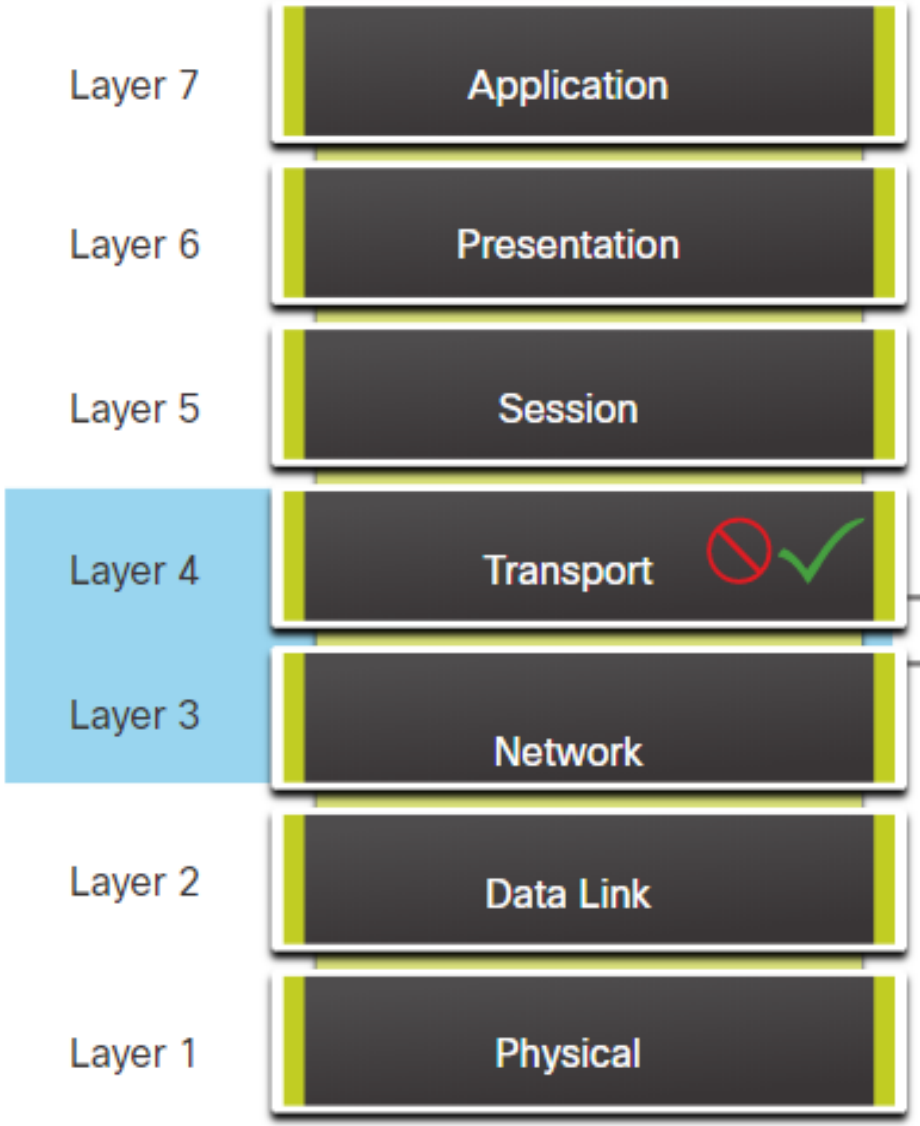
Stateful Firewall



Application Gateway Firewall



Packet Filtering (Stateless) Firewall



- Source IP address
- Destination IP address
- Protocol
- Source port number
- Destination port number
- **No** impact on network **performance**
- **ACLs** difficult to manage
- Can be **deceived** into permitting unauthorized access of **spoofed** packets
- Applications may create multiple connections on **arbitrarily negotiated ports**

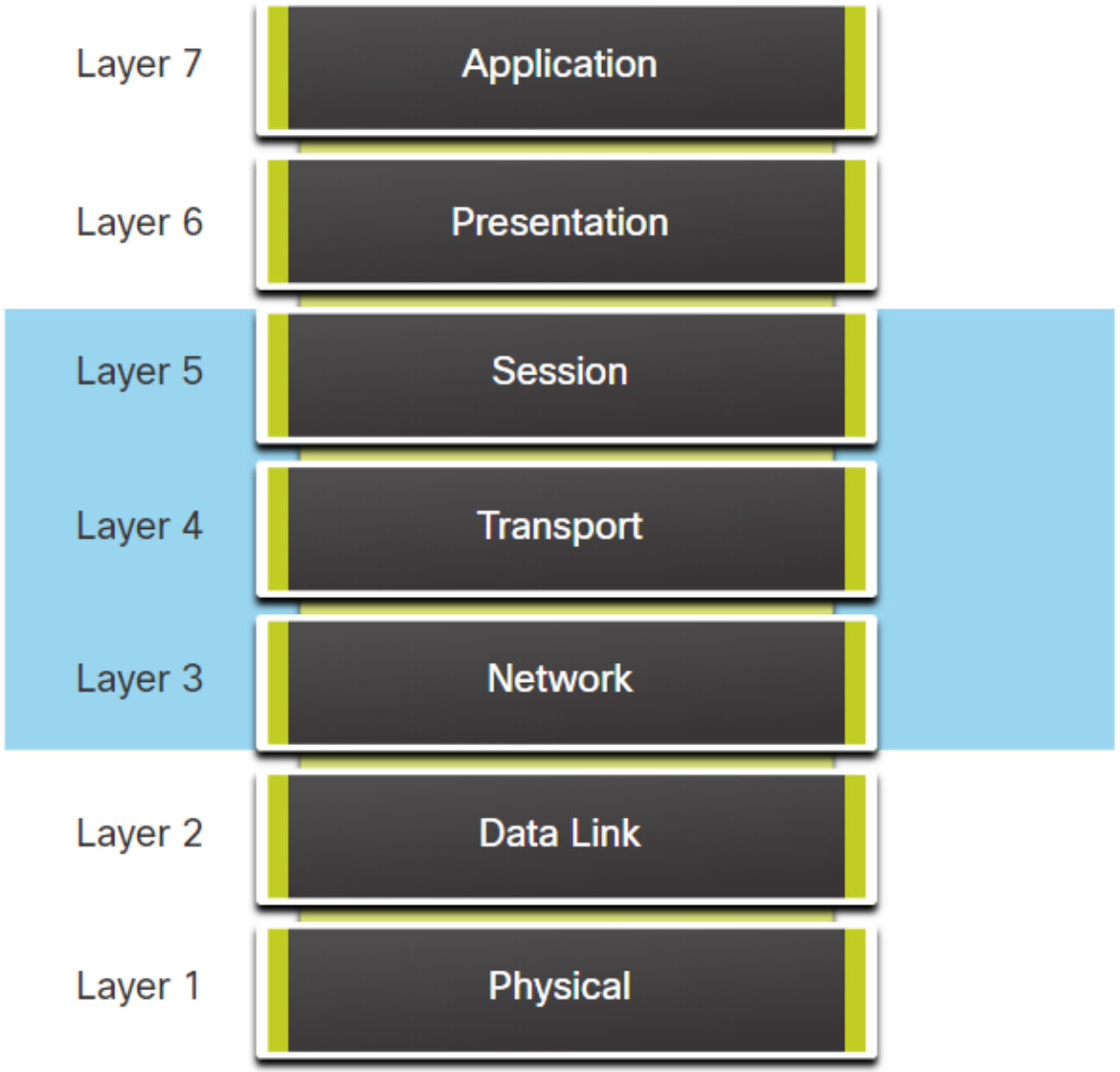
Stateful Firewalls

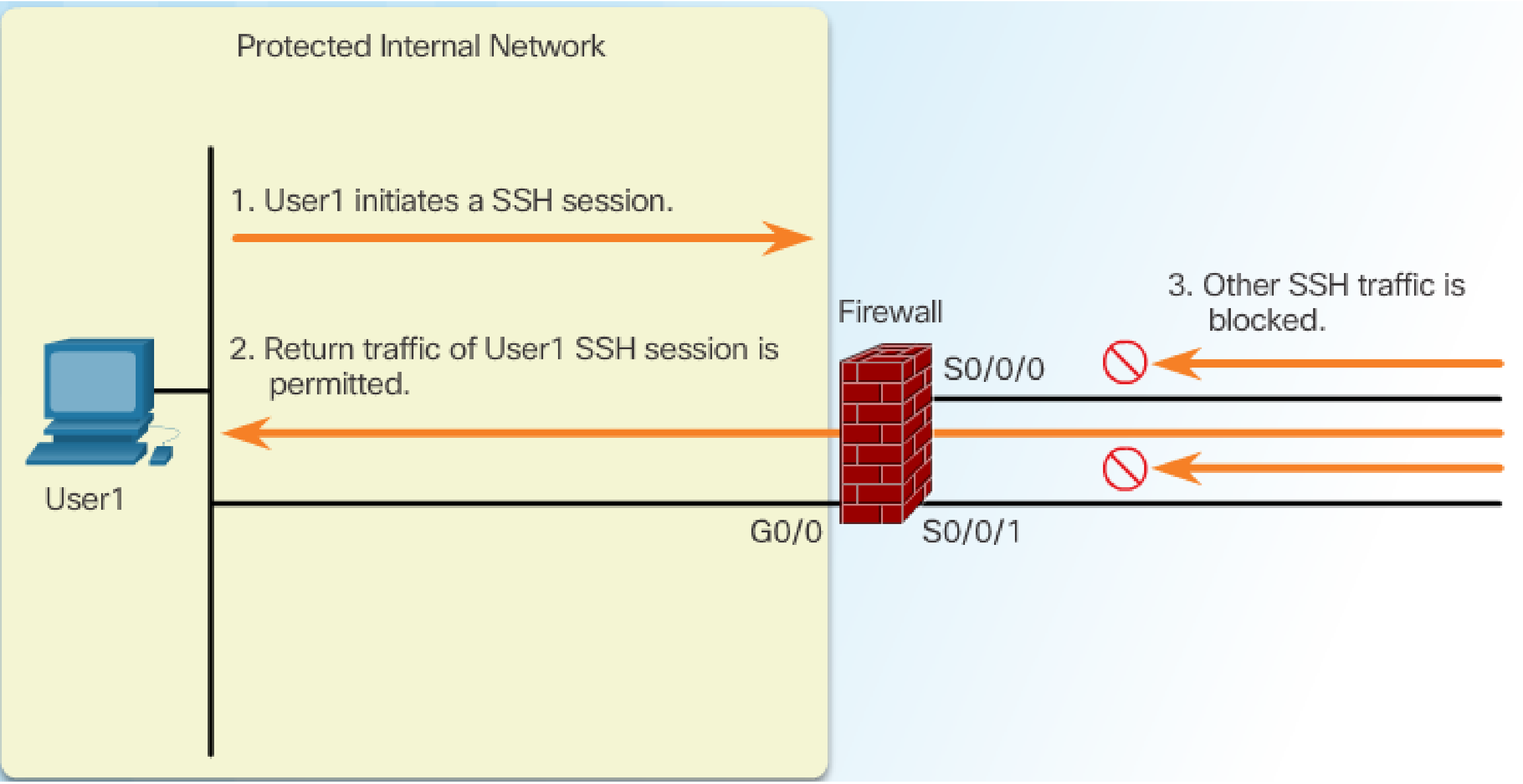
Stateful Packet Inspection (SPI)

- Slower but far more **secure**
- Maintain **state table** for connections

  e.g. established, closed, reset

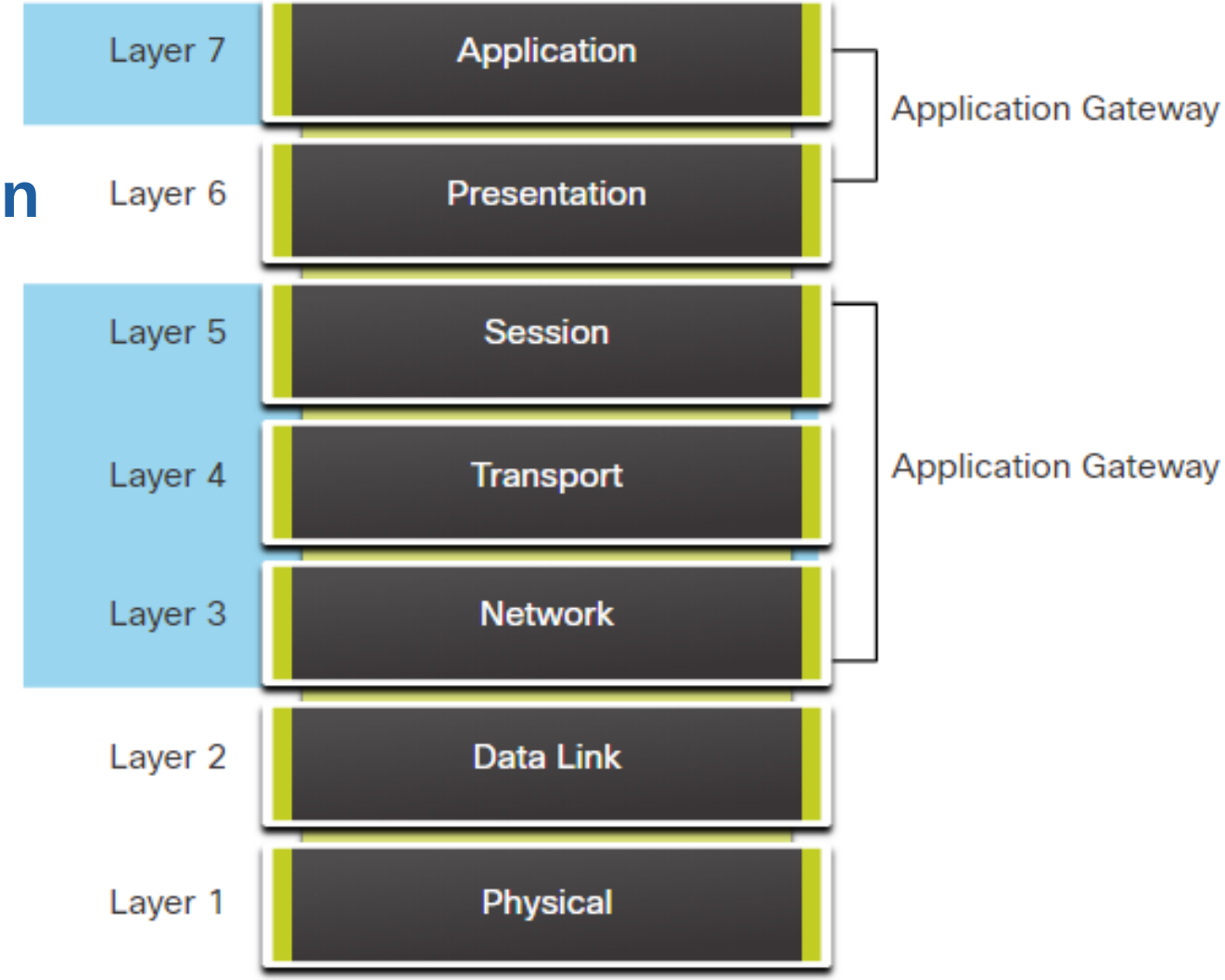
Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.22.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established




Protected Internal Network
1. User1 initiates a SSH session.
2. Return traffic of User1 SSH session is permitted.
3. Other SSH traffic is blocked.
Firewall
S0/0/0
User1
G0/0
S0/0/1

Application Gateway (Proxy) Firewalls

- Filter access based on **application info**
- Processing make them **slower**
- Can **cache** info to accelerate transactions



Next-Generation Firewalls (NGFW)

- **Deeper** inspection
- Integrate signature-based **IPS**
- **Application awareness**
- Techniques to address **evolving security threats**
- Little impact on network **performance**
- Traditional e.g. NAT, stateful inspection, VPN

+ other features e.g. identity management, encrypted traffic inspection

Other Firewall Types

- **Hybrid firewall**
- **Host-based firewall**
  - Server and personal

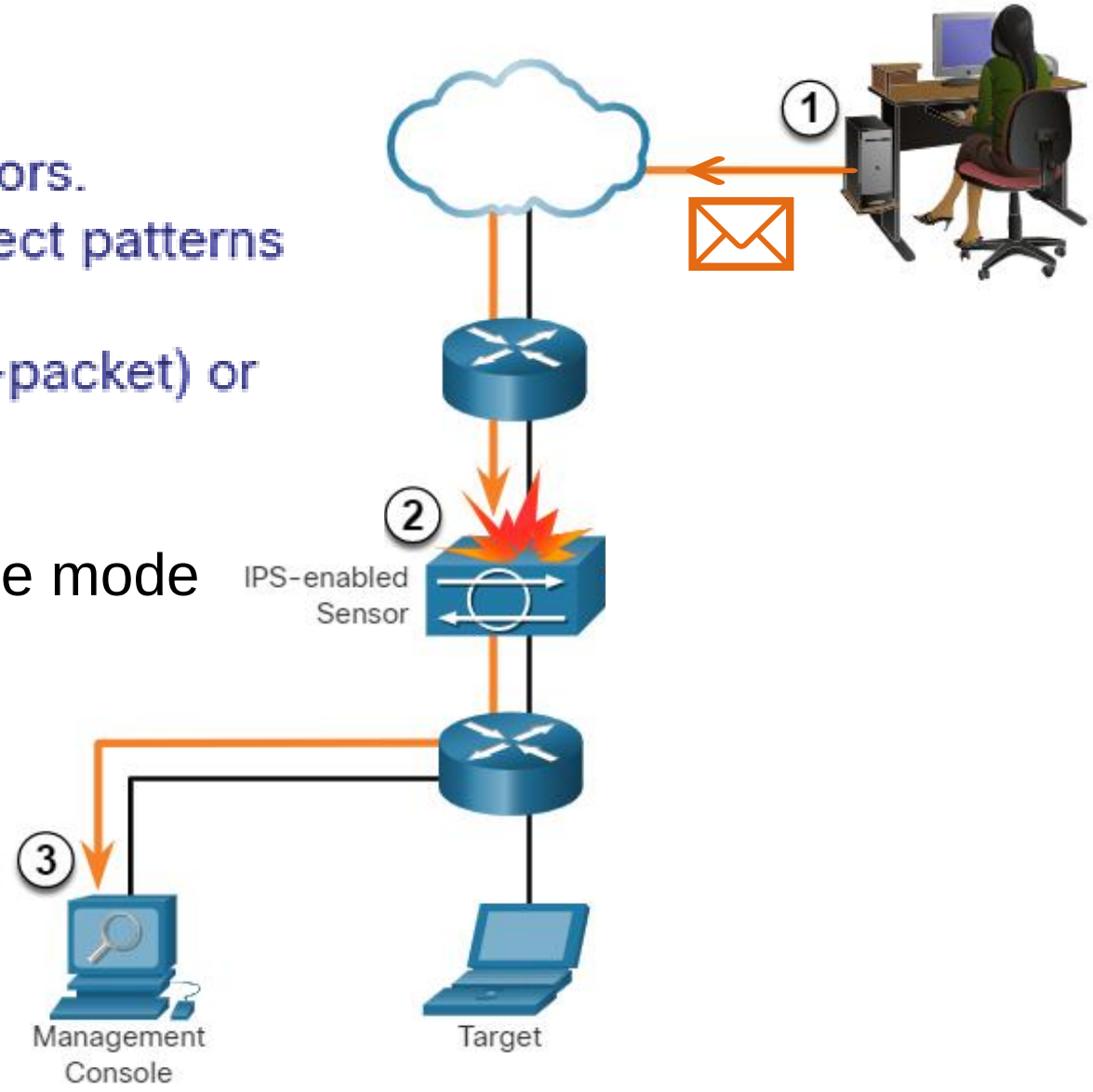
Intrusion Detection and Prevention Devices

Common Characteristics of IDS and IPS

- Both technologies are deployed as sensors.
- Both technologies use signatures to detect patterns of misuse in network traffic.
- Both can detect atomic patterns (single-packet) or composite patterns (multi-packet).

Monitoring (promiscuous) mode → Inline mode

True +ve
True –ve
False +ve
False -ve



Advantages and Disadvantages of IDS and IPS

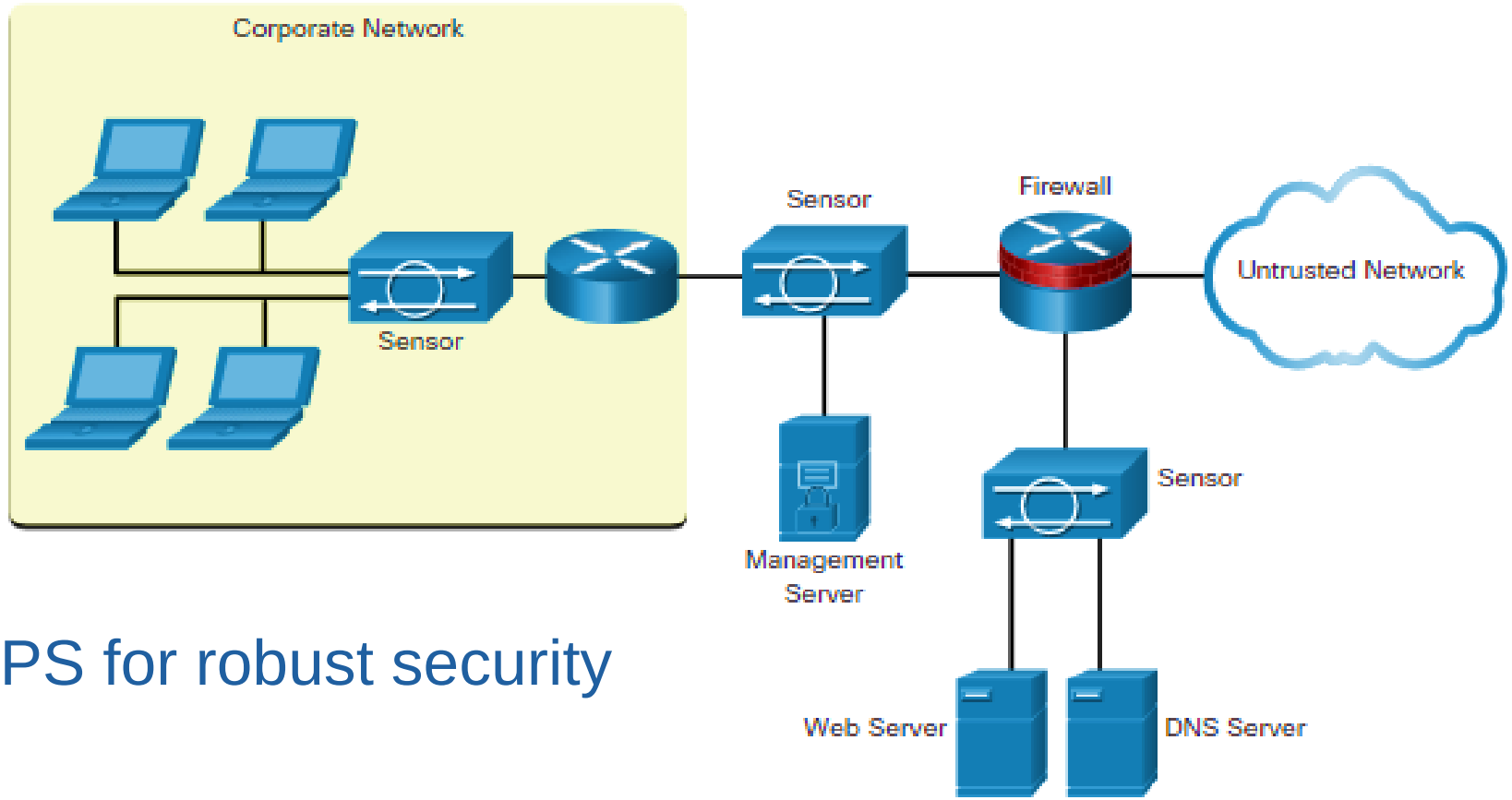
	Advantages	Disadvantages
IDS	• No impact on network (latency, jitter) • **No network impact** on sensor failure or overload • High availability good for **critical infrastructure**	• Response action **cannot stop** trigger packets
IPS	• Stops **trigger packets** • Use stream **normalization** techniques to protect from evasion • Protects from **immediate damage** e.g. sensitive data	• Sensor **failure/overload** affect network traffic • Some impact on network (**latency, jitter**)

Host-based vs Network-based IPS

	Advantages	Disadvantages
HIPS	• Protection specific to **host OS** • OS and **application level** protection • Protects host after message is **decrypted**	• **OS dependent** • Install on **every** hosts
NIPS	• **Cost** effective • OS independent	• Cannot examine encrypted traffic

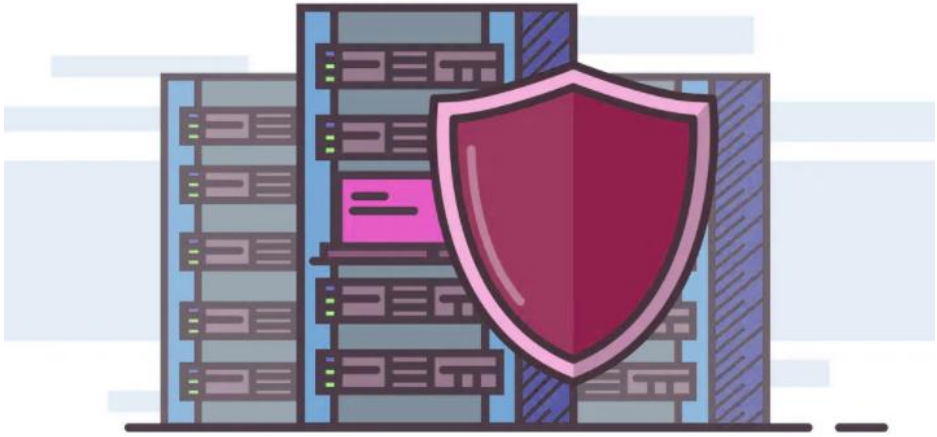
Network-based IPS (NIPS)

- **Dedicated** or non-dedicated IPS device
- **Real-time** prevention



- **Integrate** HIPS and NIPS for robust security

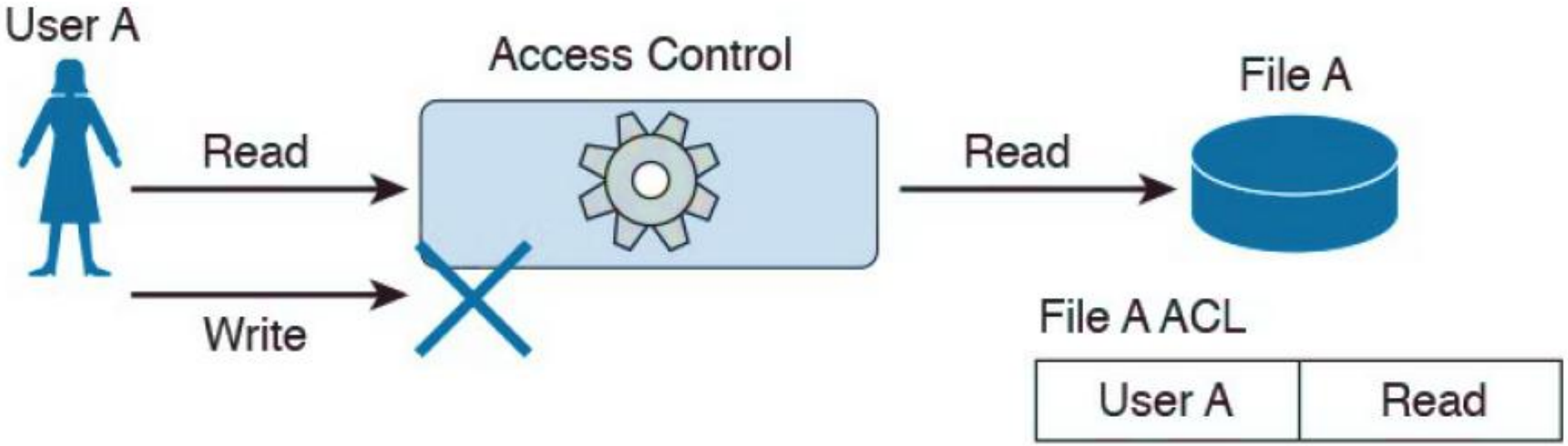
Access Control



Access Control Models

Discretionary access control
DAC

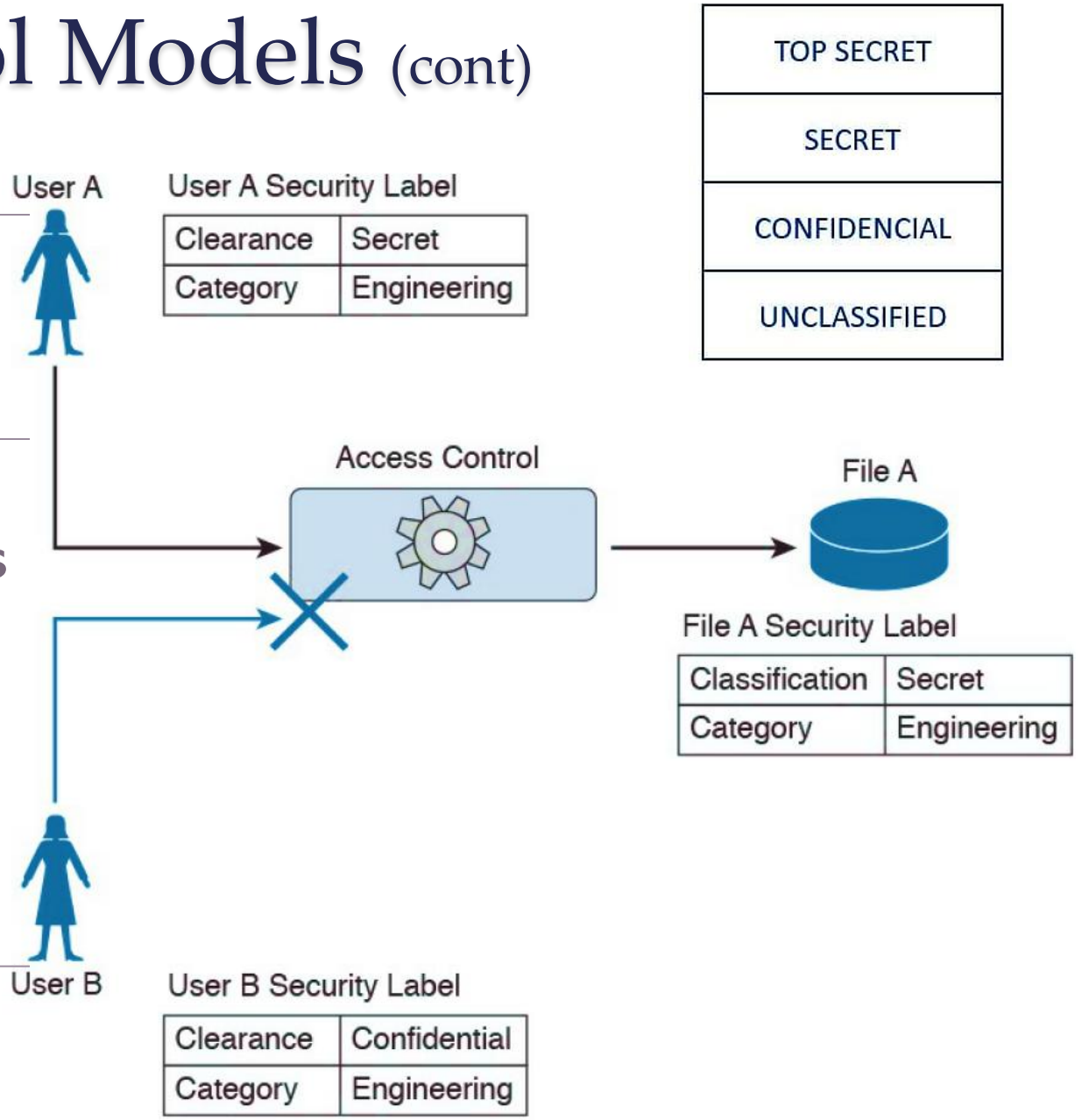
- Least restrictive model
- Users control access to their data as **owners**
- Use **ACLs** or other methods to specify which users or groups have access
- Scalability?



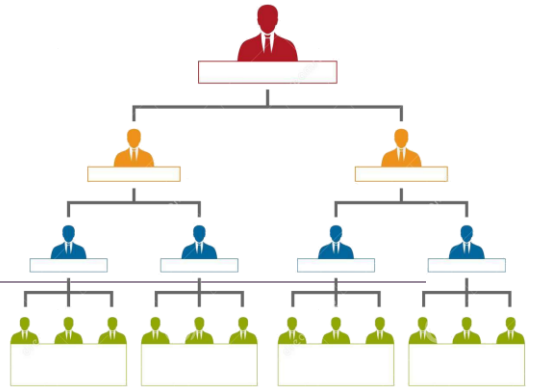
Access Control Models (cont)

Mandatory access control
MAC

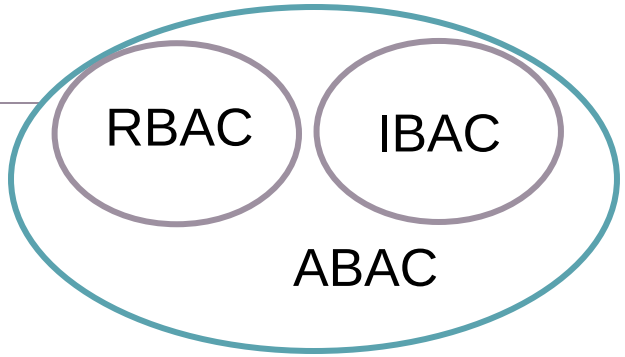
- Strictest
- Used in military and critical applications
- Assigns **security level labels** to resources
- Enables **users** with access based on their security level



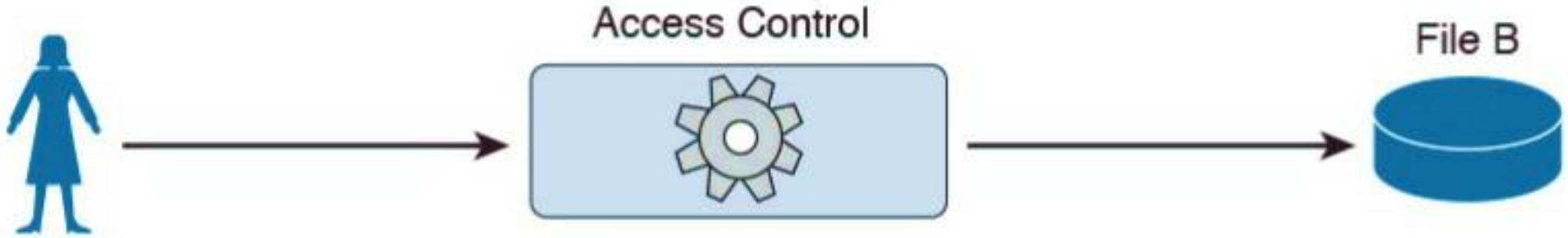
Access Control Models (cont)



Role-based access control (RBAC)	• Individuals assigned to **roles** • Different roles assigned **security privileges** • Separation of duty • **Non-discretionary** access control
Attribute-based access control (ABAC)	Based on attributes: • **object** to be accessed, • **subject** accessing resource • **environmental factors** on how object is accessed **XACML** (eXtensible Access Control Markup Language)
Rule-based access control	• **Sets of rules** associated with access to data or systems E.g. permitted/denied IP addresses, protocols, …



All Engineers who work in the Security Engineering Business Unit and are assigned to the NG Firewall Project are allowed to Read and Write all the Design Documents in the Project folder when connecting from Building A.

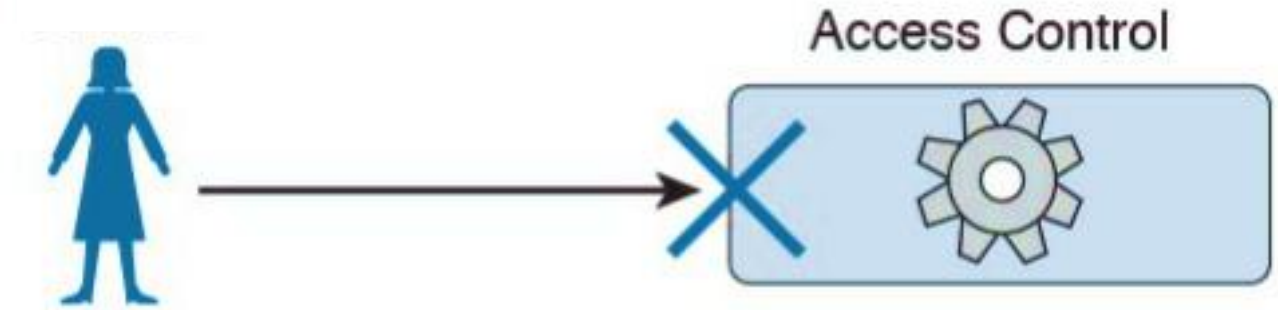


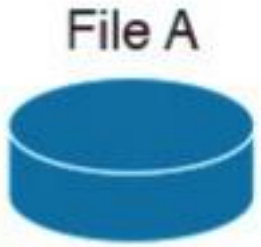
Role	Engineer
Business Unit	Security Engineering
Projects	NG Firewall NG IPS VPN Client
Location	Building A

Category	Engineer
Project	NG Firewall

User Attribute
Environmental Attributes
Resource Attribute

All Engineers who work in the Security Engineering Business Unit and are assigned to the NG Firewall Project are allowed to Read and Write all the Design Documents in the Project folder when connecting from Building A.

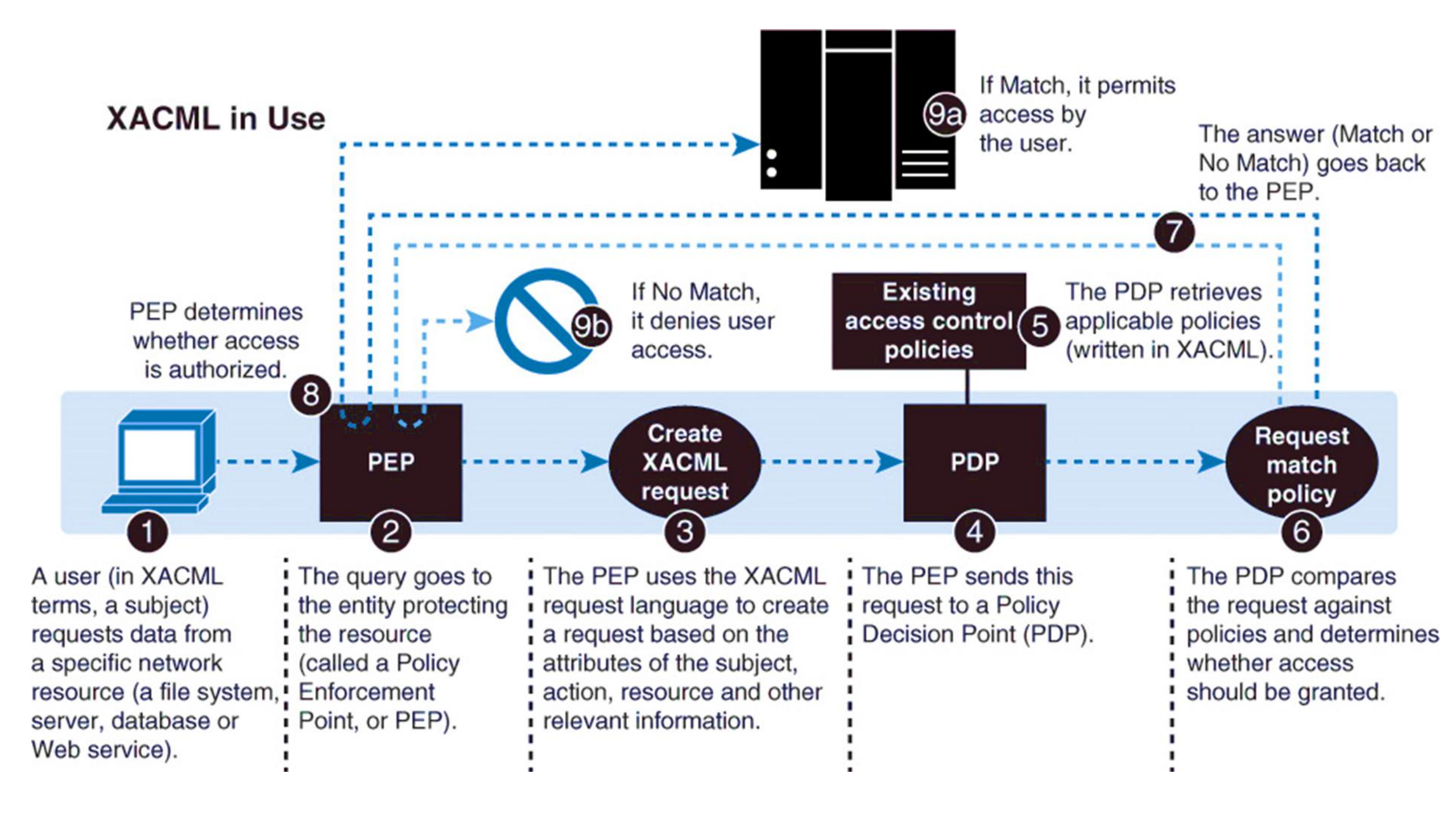




Role	Engineering
Business Unit	Security Engineering
Projects	NG Firewall NG IPS VPN Client
Location	**Connecting from Home**

Category	Engineer
Project	NG Firewall

User Attribute
Environmental Attributes
Resource Attribute


XACML in Use
If Match, it permits access by the user.
9a
The answer (Match or No Match) goes back to the PEP.
7
If No Match, it denies user access.
9b
PEP determines whether access is authorized.
8
Existing access control policies
5
The PDP retrieves applicable policies (written in XACML).
PEP
Create XACML request
PDP
Request match policy
1
2
3
4
6
A user (in XACML terms, a subject) requests data from a specific network resource (a file system, server, database or Web service).
The query goes to the entity protecting the resource (called a Policy Enforcement Point, or PEP).
The PEP uses the XACML request language to create a request based on the attributes of the subject, action, resource and other relevant information.
The PEP sends this request to a Policy Decision Point (PDP).
The PDP compares the request against policies and determines whether access should be granted.

Security Assertion Markup Language (SAML)

- **Federated identity** standard
- Enables **SSO** across SAML-enabled applications
- **IdP (SAML authority)**
  - authenticates users and passes **security information (SAML assertions)** about user (subject, principal) to
- **SP (relying party)**

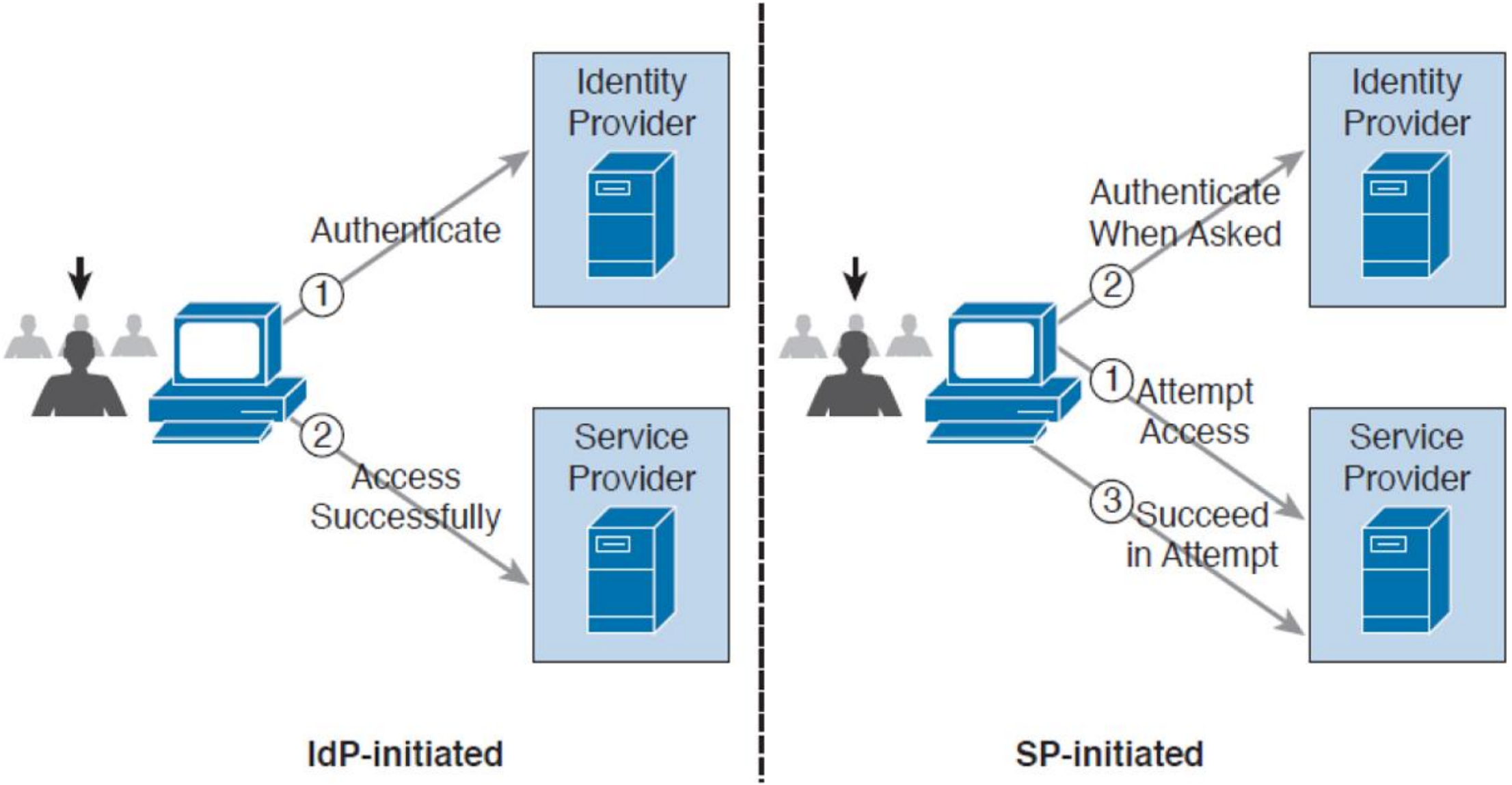
SAML (cont)

- **SAML Assertion** contain
  - Authentication statement
  - Attribute statement
  - Authorization statement

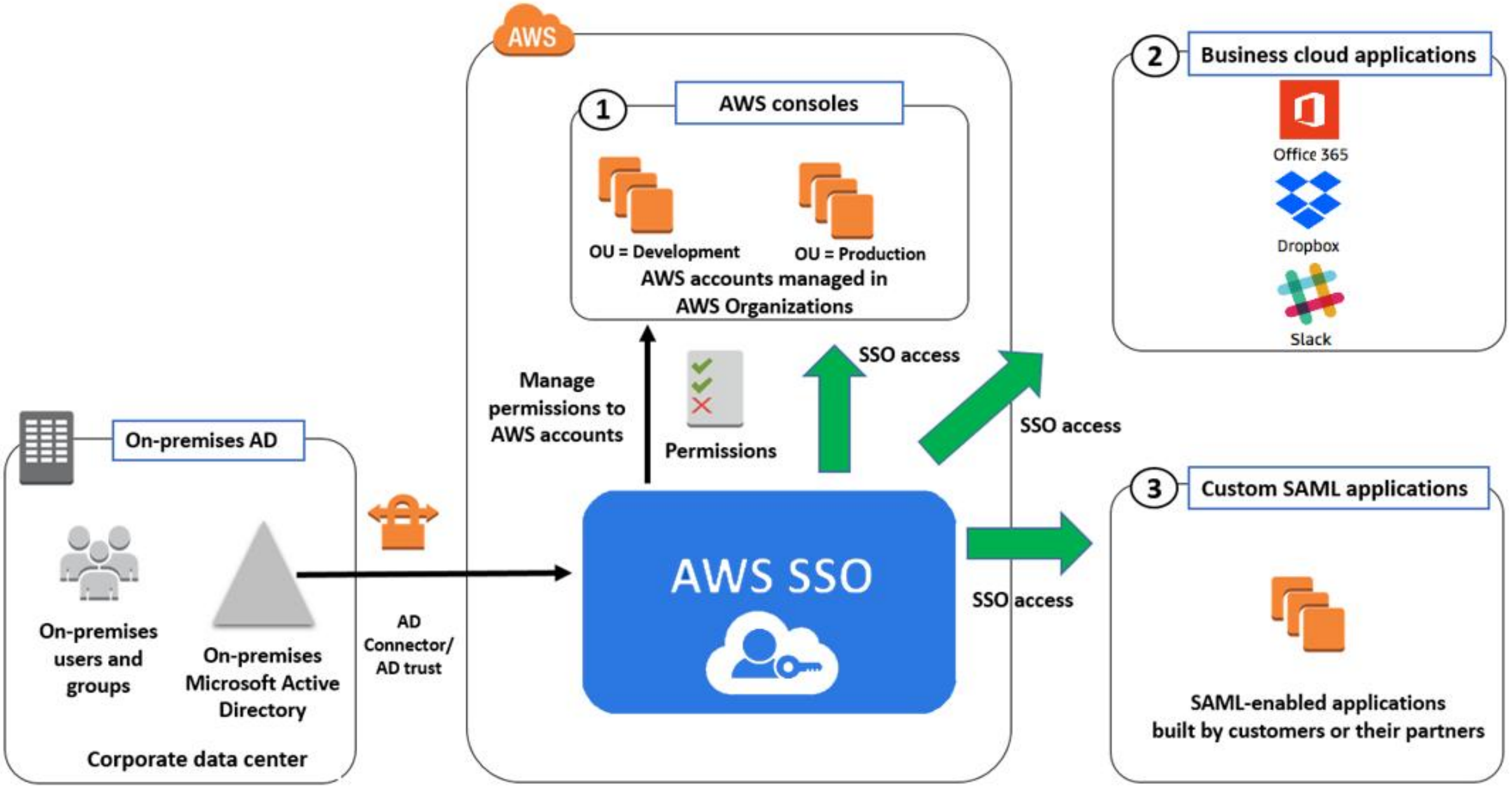
```
<saml:Assertion
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
   xmlns:xs="http://www.w3.org/2001/XMLSchema"
   ID="_d71a3a8e9fcc45c9e9d248ef7049393fc8f04e5f75"
   Version="2.0"
   IssueInstant="2004-12-05T09:22:05Z">

<saml:Issuer>https://idp.example.org/SAML2</saml:Is-
suer>
   <ds:Signature

xmlns:ds="http://www.w3.org/2000/09/xmld-
sig#">...</ds:Signature>
   <saml:Subject>
     <saml:NameID
       Format="urn:oasis:names:tc:SAML:2.0:nameid-for-
mat:transient">
       3f7b3dcf-1674-4ecd-92c8-1544f346baf8
     </saml:NameID>
     <saml:SubjectConfirmation
       Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
       <saml:SubjectConfirmationData
         InResponseTo="aaf23196-1773-2113-474a-
fe114412ab72"

Recipient="https://sp.example.com/SAML2/SSO/POST"
         NotOnOrAfter="2004-12-05T09:27:05Z"/>
     </saml:SubjectConfirmation>
   </saml:Subject>
   <saml:Conditions
     NotBefore="2004-12-05T09:17:05Z"
     NotOnOrAfter="2004-12-05T09:27:05Z">
     <saml:AudienceRestriction>

<saml:Audience>https://sp.example.com/SAML2</saml:Au-
dience>
     </saml:AudienceRestriction>
   </saml:Conditions>
   <saml:AuthnStatement
     AuthnInstant="2004-12-05T09:22:00Z"
     SessionIndex="b07b804c-7c29-ea16-7300-
4f3d6f7928ac">
     <saml:AuthnContext>
       <saml:AuthnContextClassRef>
         urn:oasis:names:tc:SAML:2.0:ac:classes:Pass-
wordProtectedTransport
       </saml:AuthnContextClassRef>
     </saml:AuthnContext>
   </saml:AuthnStatement>
   <saml:AttributeStatement>
     <saml:Attribute

xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:at-
tribute:X500"
       x500:Encoding="LDAP"

NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-for-
mat:uri"
       Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1"
       FriendlyName="eduPersonAffiliation">
       <saml:AttributeValue

xsi:type="xs:string">member</saml:AttributeValue>
       <saml:AttributeValue

xsi:type="xs:string">staff</saml:AttributeValue>
     </saml:Attribute>
   </saml:AttributeStatement>
 </saml:Assertion>
```

e.g. User A, who has the email address usera@domain.com authenticated via username and password, is a platinum member and is authorized for a 10% discount

SAML


Identity Provider
Authenticate
1
Service Provider
2
Access Successfully
IdP-initiated
Identity Provider
Authenticate When Asked
2
1
Attempt Access
Service Provider
3
Succeed in Attempt
SP-initiated

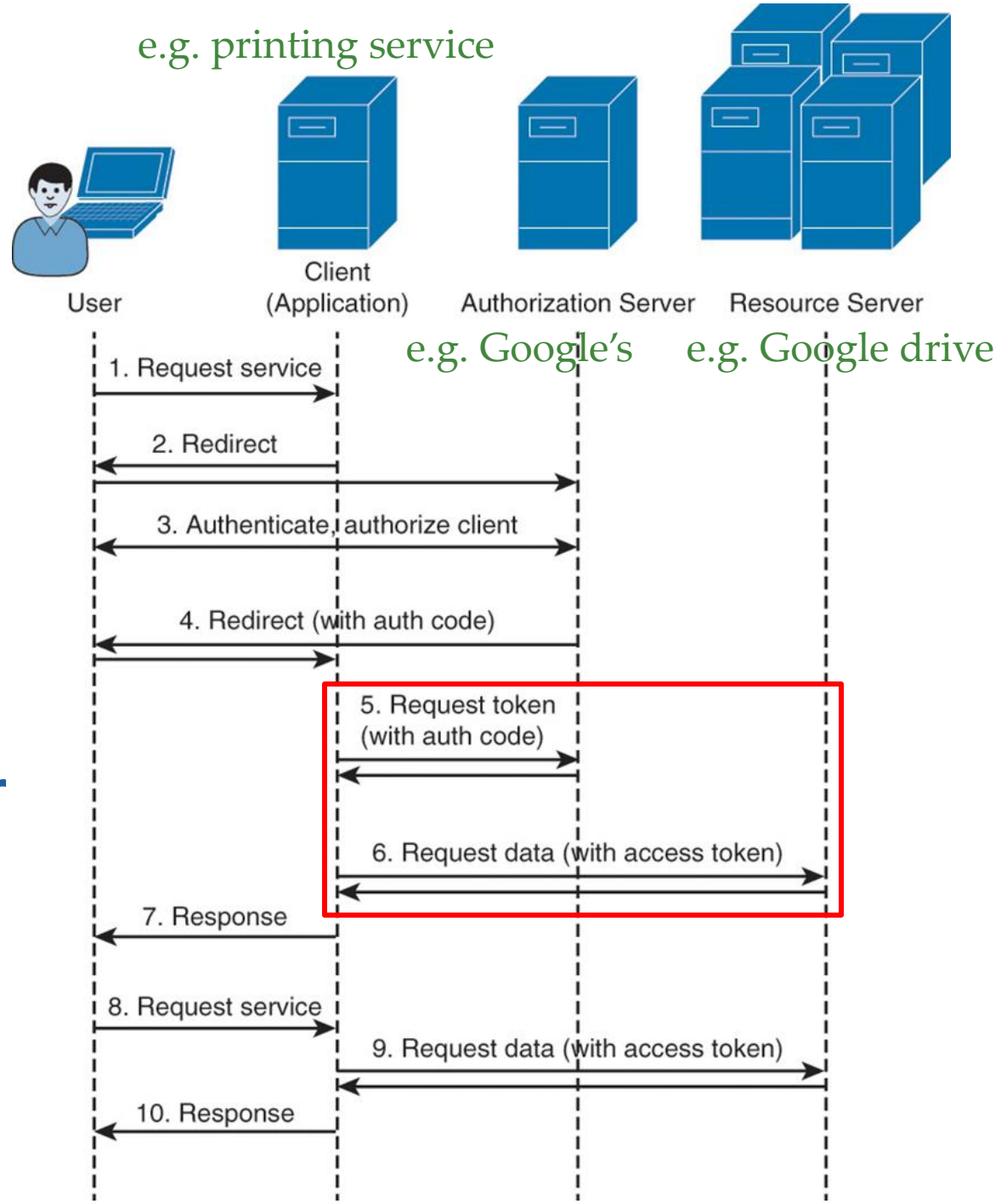
AWS SSO Use Cases



https://aws.amazon.com/blogs/security/introducing-aws-single-sign-on/

OAuth

- Open Authorization standard
- Allows users share private resources on one site to another site **without using credentials**
- Third party receives **access token**
- One web application uses **another web application's API** on behalf of the user



AAA

AAA Servers

Authentication	• Users must **prove** that they are who they say they are • Can be **established** using username/password, challenge/response questions, token cards, … • **Centralized** way to control access to network
Authorization	• Which **resources** and **operations** user can access E.g. User M can access host server X using SSH only
Accounting	• **Records** what user does i.e. what is accessed, amount of time, any changes made • Keeps **track** of how network resources are used E.g. User M accessed host server X using SSH for 15min

AAA Operation

- Network must **control** who is allowed to connect and what they are allowed to do
- **Security policy** specifies **how** users access network resources
  - Network administrators, corporate users, remote users, business partners, clients
- Policy may mandate **tracking** who, when and what they did while logged in
- **AAA** provides framework to enable **scalable access security**

Authentication

Who are you?

Authorization

How much can you spend?

Accounting

What did you spend it on?

Account Number	Statement Closing Date	Current Amount Due
1234-567-890	01-31-01	$278.50

JOE EMPLOYEE
456 SKYVIEW DRIVE
HOMETOWN, USA 99900-1234

MAIL PAYMENT TO :
THE BANK
132 VINE STREET
ANYTOWN, USA 67500-0010

872919345 00178255000000003

Detach here and return upper portion with check or money order. Do not staple or fold.

Statement of Personal Credit Card Account

Retain this portion for your files.

THE BANK

Cardmember Name	Account Number	Statement Closing Date
JOE EMPLOYEE	1234-456-890	01-31-01

Statement Date:	02-01-01	Payment Due Date:	03-01-01
Closing Date:	01-31-01		
Credit Limit	$1,500.00	Credit Available:	$1221.50
New Balance:	$278.50	Minimum Payment Due:	$20.00

Account Summary

Previous Balance:	+74.24	Transaction Fees:	+3.00
Purchases:	+250.50	Annual Fees:	+25.00
Cash Advances:	+0	Current Amount Due:	+250.50
Payments:	-74.25	Amount Past Due:	+0
Finance Charge:	+0	Amount Over Credit Line:	+0
Late Charge:	+0	NEW BALANCE:	$278.50

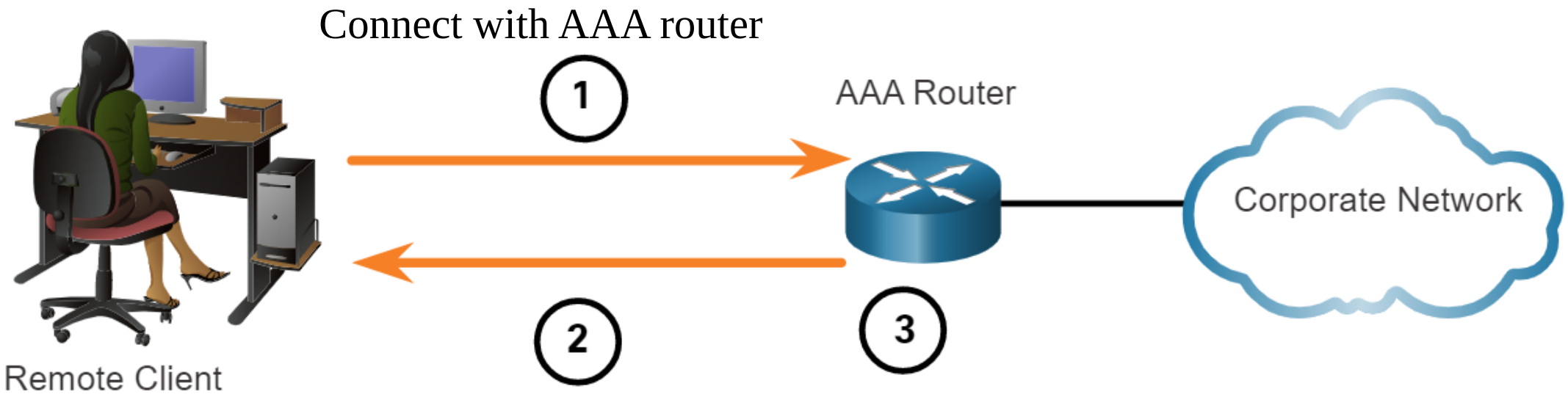
Reference Number	Sold	Posted	Activity Since Last Statement		Amount
43210987	01-03	01-13	Payment, Thank You		-$74.25
01234567	01-12	01-13	Wings 'N' Things	Anytown, USA	$25.25
78901234	01-14	01-17	Record Release	Anytown, USA	$40.00
45678901	01-14	01-17	Sports Stadium	Anytown, USA	$75.25
3210987	01-22	01-23	Tie Tack	Anytown, USA	$20.75
76543210	01-29	01-30	Electronic World	Anytown, USA	$89.25
23455678		01-30	Transaction Fees		$3.00
34567890		01-01	Annual Fee		$25.00

AAA Authentication

- Authenticate users for **administrative** or **remote** network access
- Two common methods for implementing AAA Services
  - Local
  - Server-based

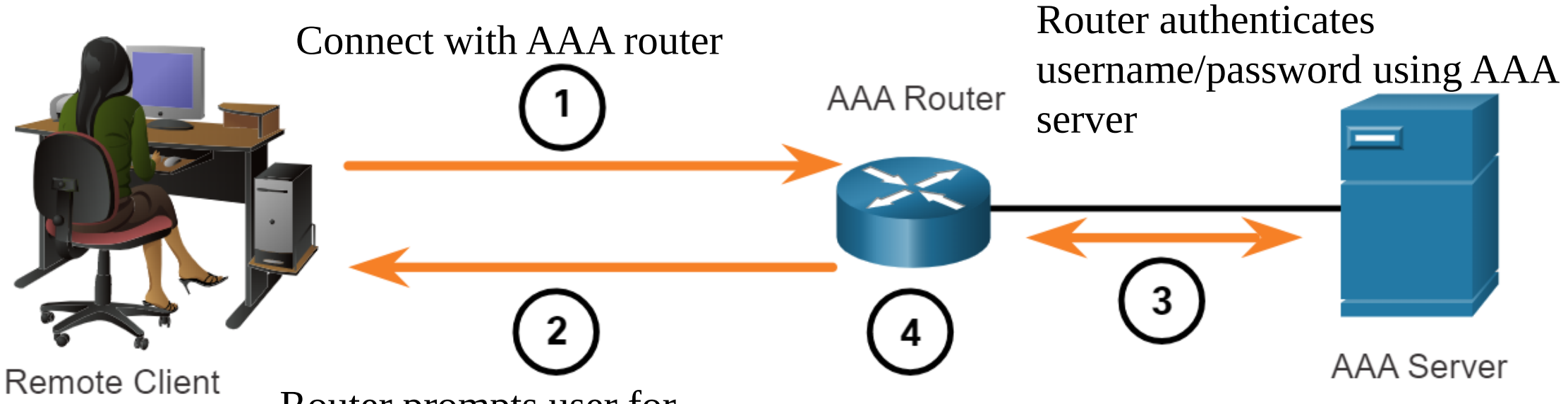
Local AAA Authentication

- **Self-contained** AAA
- Authenticates users against **locally stored** username/password
- Ideal for **small** networks



Server-based AAA Authentication

- Central AAA server contains usernames and passwords for all users
- Ideal for medium to large networks
- Uses RADIUS or TACACS+



Centralized AAA

- **Preferred** AAA implementation
  - More **scalable** and manageable than local AAA
- May **independently** maintain databases for A, A, and A
- Can leverage **Active Directory** or **LDAP** for authentication and group membership
  - While maintaining **own authorization and accounting** databases
- Devices communicate with AAA server using either
  - **RADIUS** (Remote Authentication Dial-In User Service)
  - **TACACS+** (Terminal Access Controller Access Control System)

Functions	TACACS+	RADIUS
Functionality	**Separates** authentication, authorization and accounting according to AAA architecture Modularity of security server implementation	**Combines** authentication and authorization but separates accounting Less flexibility in implementation
Standard	Cisco proprietary	Open/RFC standard
Transport	**TCP** port 49	**UDP** ports 1812/1813 or 1645/1646
Confidentiality	Encrypts **whole packet** but leaves TACACS+ header	Encrypts **password only** Remainder of packet is unencrypted, leaving username, authorized services and accounting **unprotected**

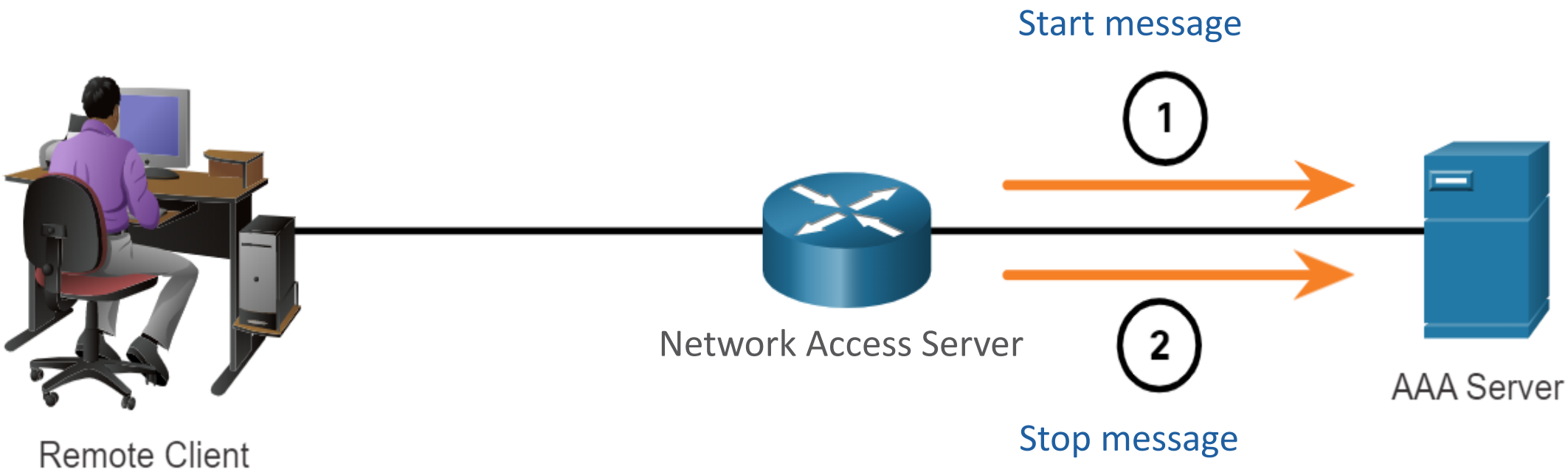
Functions	TACACS+	RADIUS
Customization	Provides **authorization of router commands** on per-user or per-group basis	Has **no option** to authorize router commands on per-user or per-group basis
Accounting	Limited	**Extensive**
Common Usage	Device administration	Network access

AAA Accounting Logs

- Accounting records from all devices sent to **centralized repositories** to simplify auditing
- Data includes start and stop connection **times**, executed **commands**, **no. packets** and **no. bytes**
- **Combining** with AA helps **manage access** to internetworking devices by administrative staff
  - Security **auditing**
  - Detailed log of what authenticated user does on device

  e.g. EXEC and configuration commands

AAA Accounting Logs (cont)



Types of Accounting Events

aaa accounting ***event-type*** {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} *method*

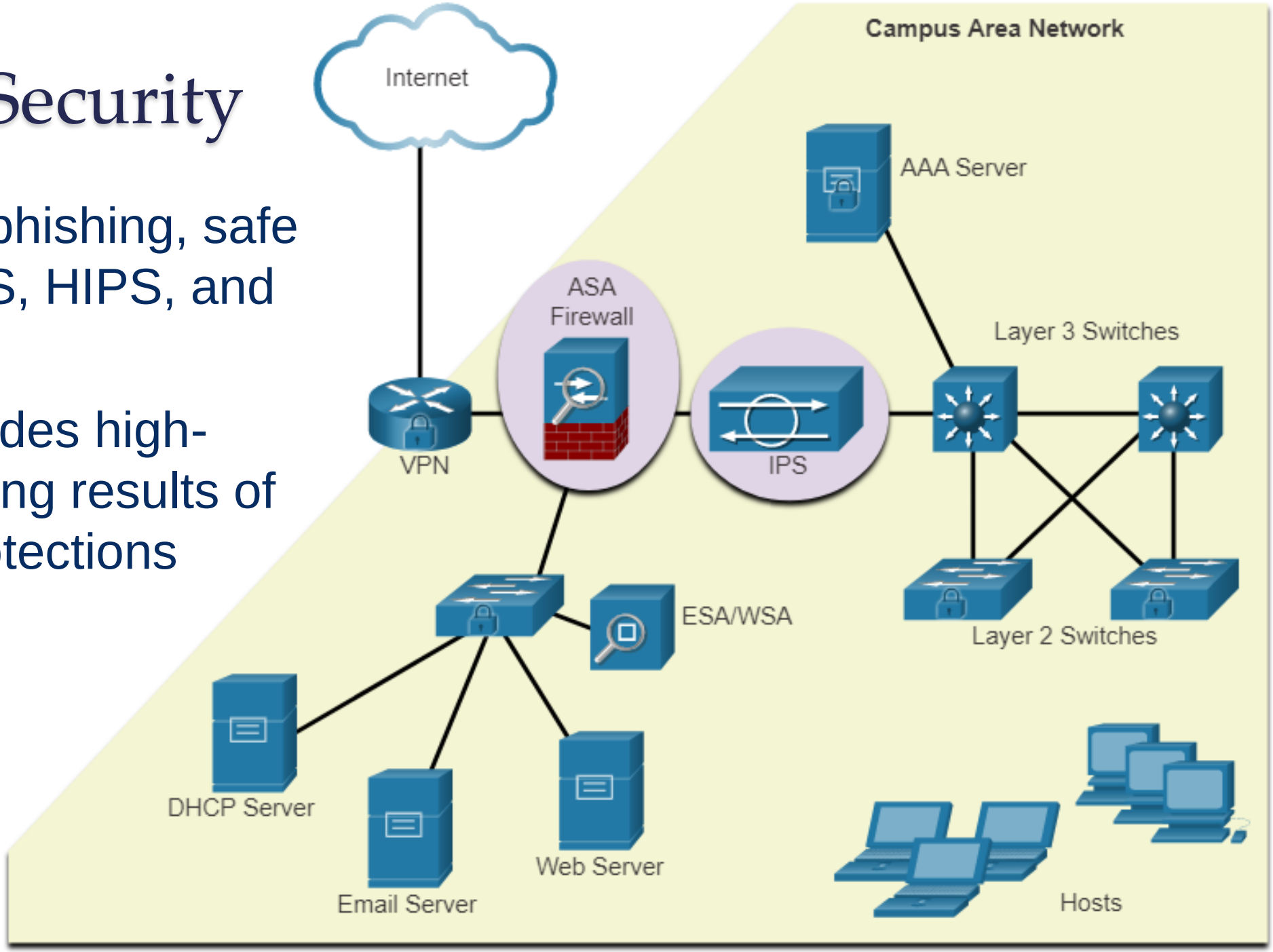
aaa accounting commands default start-stop radius

Network	Information for all Point-to-Point Protocol **(PPP) sessions** including packet and byte counts
Connection	Information on all **outbound connections** that are made from AAA client e.g. SSH to another device
EXEC	Information on **EXEC terminal sessions** on NAS e.g. username, date, start/stop time, user IP address
System	Information on all **system-level events** e.g. interface up/down, router reload
Commands	Information on **EXEC shell commands** for specified privilege level, date and time command executed and user involved
Resource	**'start'** and **'stop'** records for connections that passed user authentication

Anti-malware Protection

Endpoint Security

- Antivirus, anti-phishing, safe browsing, HIDS, HIPS, and firewall
- **AV-TEST** provides high-quality lab testing results of host-based protections



AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Deutsch | English | Français | Español

About the Institute | News | Tests | Statistics | Contact

AV-ATLAS.ORG | IOT-TESTS.ORG

Current security products for Windows 10 put to the test ›

All results can be found here

AV-atlas

The Threat Intelligence Platform from AV-TEST

Start AV-ATLAS.org ›

Subscribe to the AV-TEST Newsletter

Well-informed on security

More ›

CURRENT TEST: Windows 10

CURRENT TEST: MacOS

Test: 3 VPN Packages

Tests: EPPs and EDRs

Tests for home users

Tests for business users

Internet of Things (IoT)

Host-Based Anti-malware

- Installed on **hosts to** detect and mitigate viruses and malware
- Win Defender, Cisco AMP, Norton, McAfee, Trend Micro, …
  - **Signature-based**

    Recognizes static characteristics of known malware files
    e.g. strings, hash, code

  - **Heuristics-based**

    Recognizes features shared by various malware
    e.g. instructions, commands -> payload, replication, distribution

  - **Behavior-based**

    Employs static or dynamic analysis of suspicious behavior
    e.g. file access, OS calls

Host-Based Firewalls

- Software that control traffic **entering/leaving** host
- Issue **alerts** to users if suspicious behavior is detected
- Include **logging** functionality
- **Windows Defender**

  Profile-based approach to firewall functionality
- **iptables**

  Utility to allow **configuring** network access rules

  Part of Linux kernel **Netfilter** modules

Host-Based Firewalls (cont)

- **nftables**

Successor to iptables

Addresses scalability and performance issues

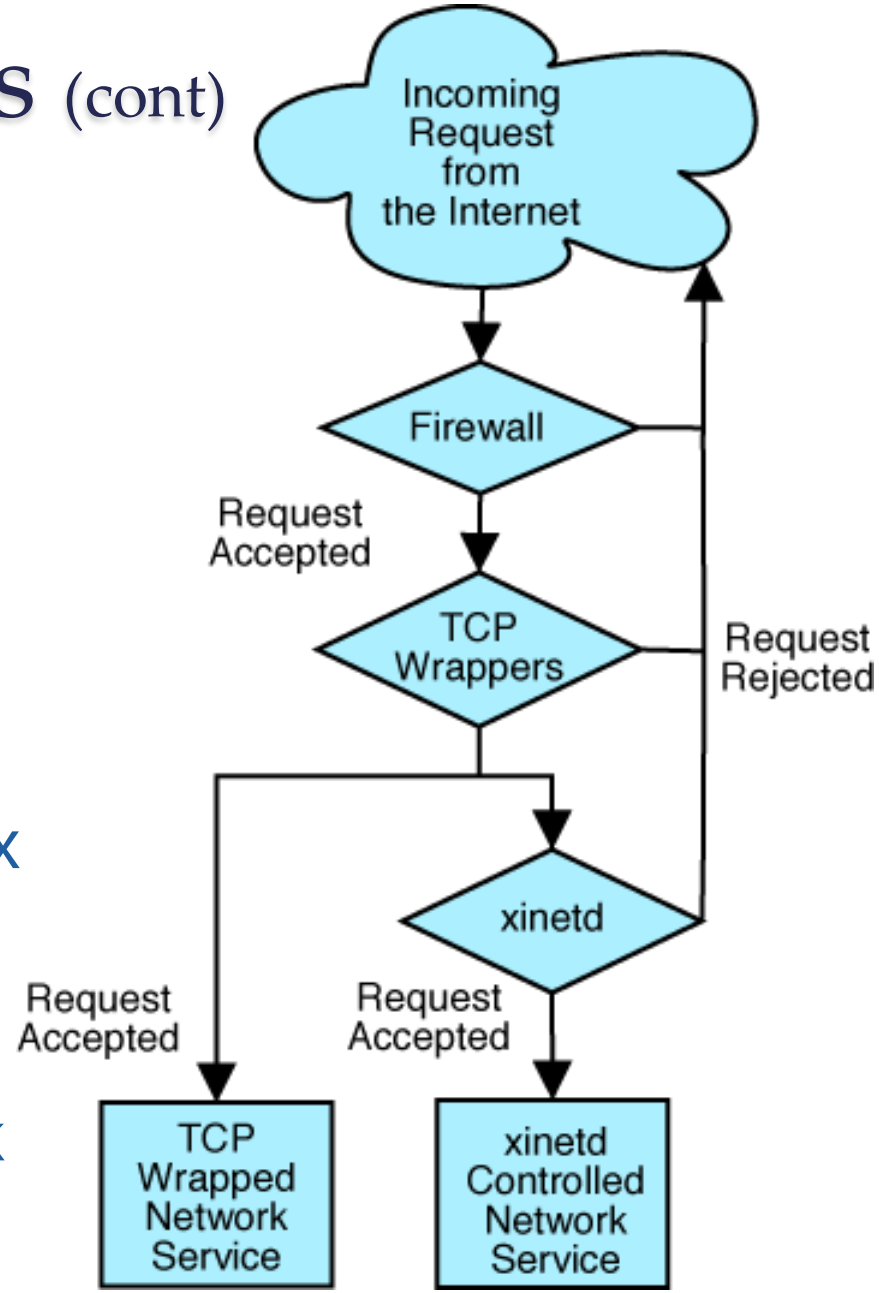
Uses virtual machine in Linux kernel

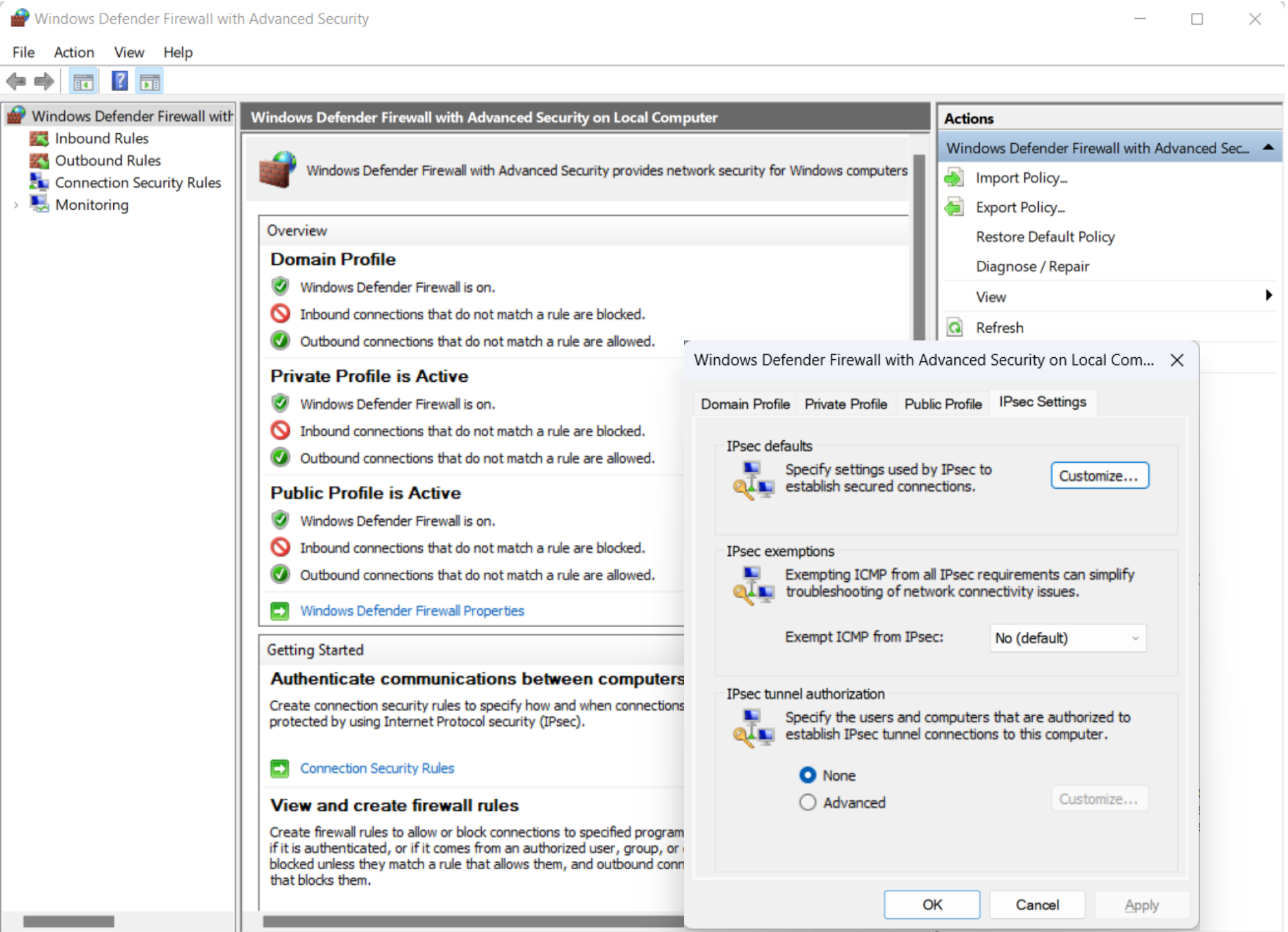
- **TCP Wrappers**

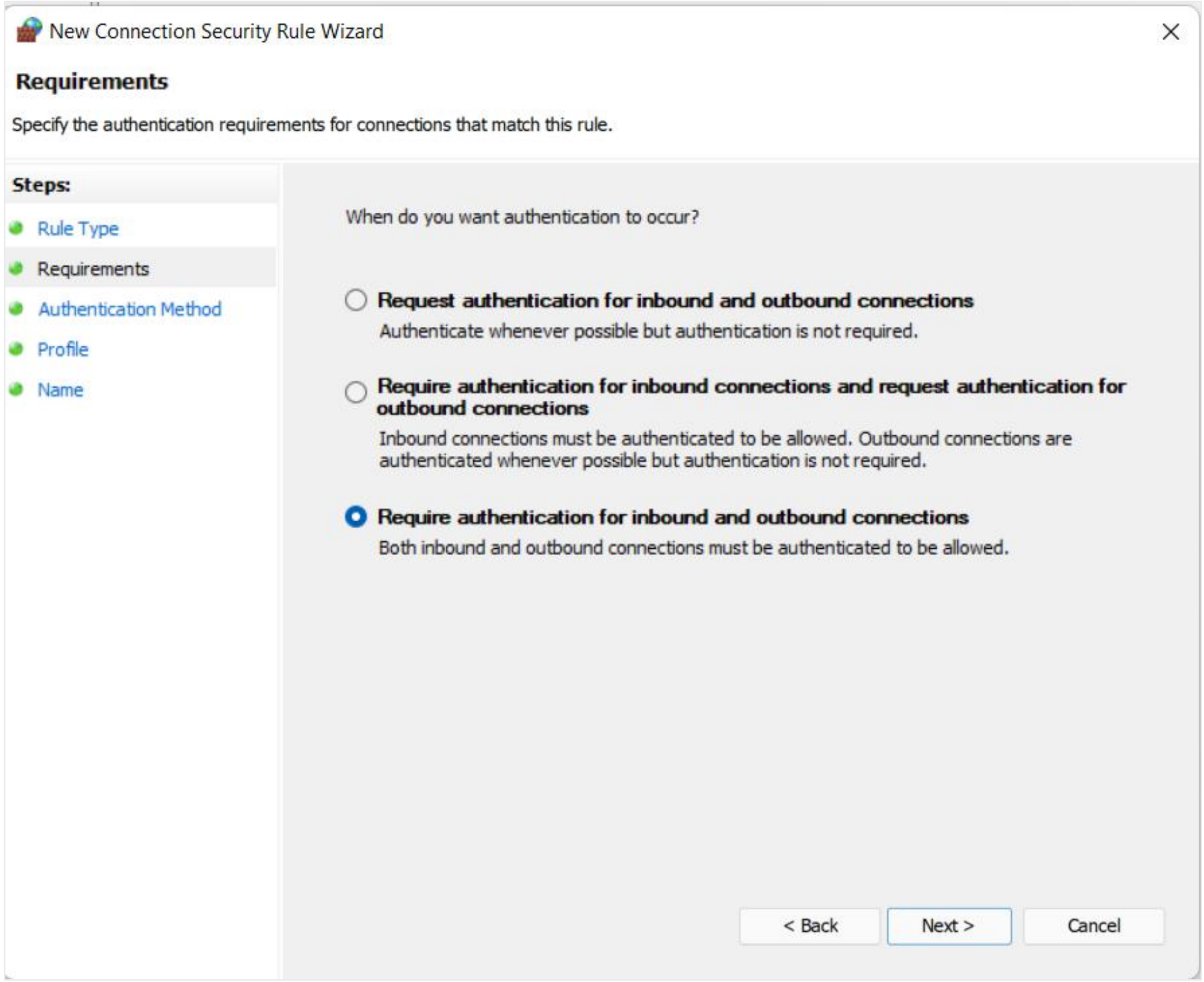
Rule-based access control and logging for Linux

Can provide **additional layer of protection** for some network services

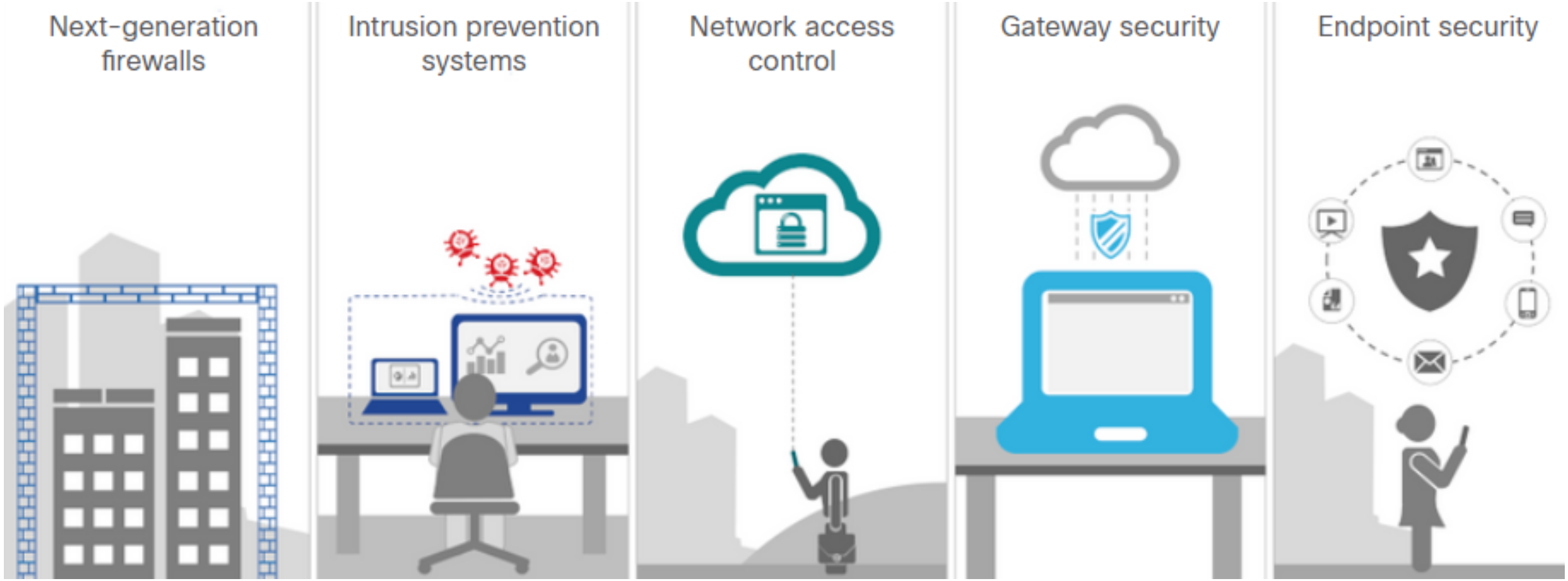
Which hosts are allowed to connect to network services e.g. xinetd




Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Defender Firewall with Advanced Security on Local Computer
Windows Defender Firewall with Advanced Security provides network security for Windows computers
Overview
Domain Profile
Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Private Profile is Active
Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Public Profile is Active
Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Windows Defender Firewall Properties
Getting Started
Authenticate communications between computers
Create connection security rules to specify how and when connections
protected by using Internet Protocol security (IPsec).
Connection Security Rules
View and create firewall rules
Create firewall rules to allow or block connections to specified program
if it is authenticated, or if it comes from an authorized user, group, or
blocked unless they match a rule that allows them, and outbound conn
that blocks them.
Actions
Windows Defender Firewall with Advanced Sec...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Windows Defender Firewall with Advanced Security on Local Com...
Domain Profile
Private Profile
Public Profile
IPsec Settings
IPsec defaults
Specify settings used by IPsec to establish secured connections.
Customize...
IPsec exemptions
Exempting ICMP from all IPsec requirements can simplify troubleshooting of network connectivity issues.
Exempt ICMP from IPsec:
No (default)
IPsec tunnel authorization
Specify the users and computers that are authorized to establish IPsec tunnel connections to this computer.
None
Advanced
Customize...
OK
Cancel
Apply


New Connection Security Rule Wizard
Requirements
Specify the authentication requirements for connections that match this rule.
Steps:
Rule Type
Requirements
Authentication Method
Profile
Name
When do you want authentication to occur?
Request authentication for inbound and outbound connections
Authenticate whenever possible but authentication is not required.
Require authentication for inbound connections and request authentication for outbound connections
Inbound connections must be authenticated to be allowed. Outbound connections are authenticated whenever possible but authentication is not required.
Require authentication for inbound and outbound connections
Both inbound and outbound connections must be authenticated to be allowed.
< Back
Next >
Cancel

Network-Based Malware Protection



Network-Based Malware Protection

Advanced Malware Protection (AMP)

- Endpoint protection from viruses and malware

Email Security Appliance (ESA)

- SPAM and potentially malicious email filtering before reaching endpoint

Web Security Appliance (WSA)

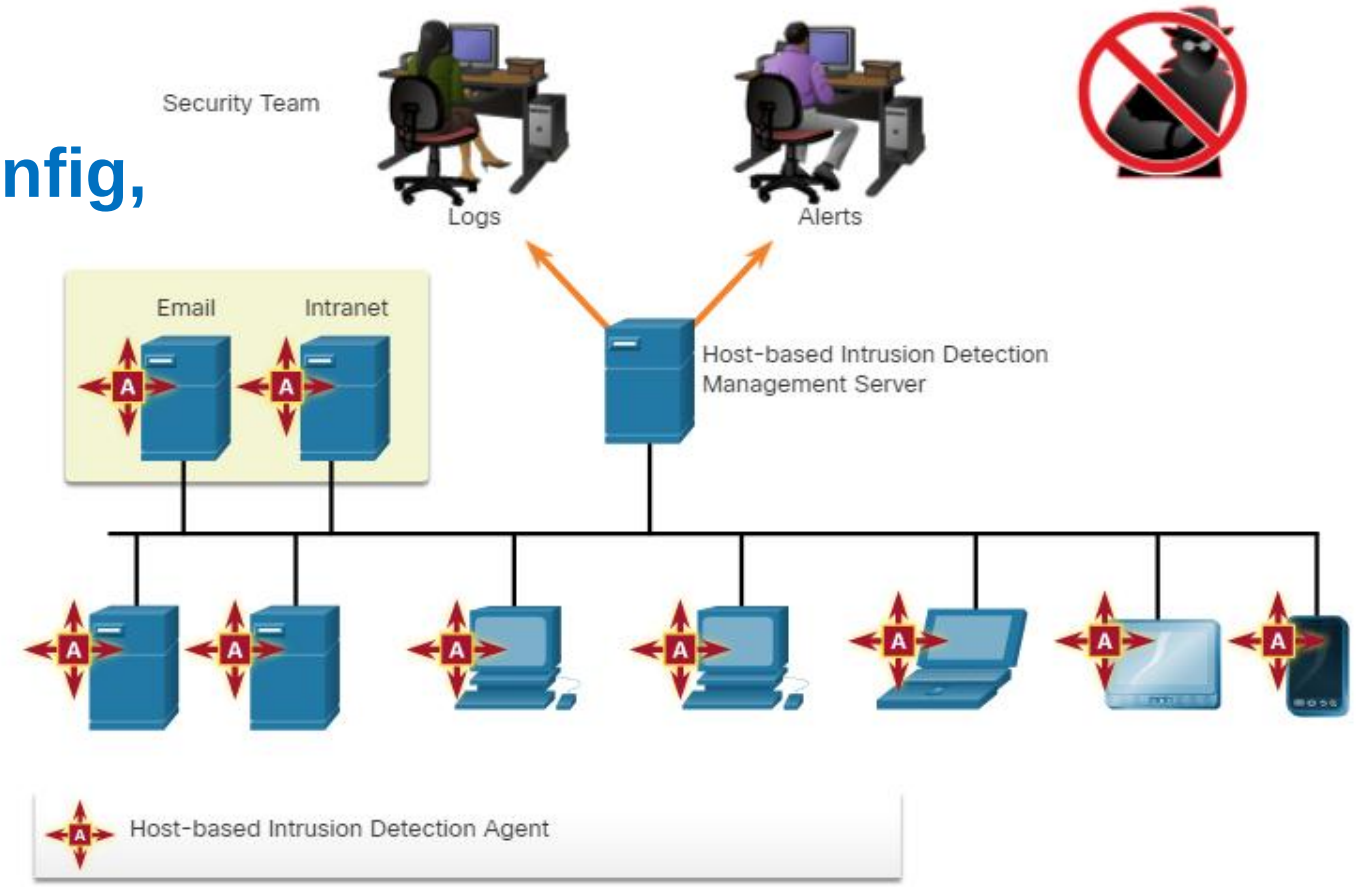
- Filtering of websites and blacklisting

Network Admission Control (NAC)

- Enforces user or machine authentication before granting network access
- Permits only authorized and compliant systems to connect to network

HIDS/HIPS

- Host-Based Intrusion Detection/Prevention
- Combines **antimalware** and **firewall** functionality
- Monitor and report on **system config, logs, file integrity (FIM), application activity**
- **Agent**-based with **central** security management
- Cisco AMP, AlienVault USM
- Open Source: Tripwire, OSSEC



HIDS/HIPS Operation

- Uses **signatures** to detect malware and prevent infection
- Additional strategies
  - **Anomaly based**

    System behavior compared to baseline model of **normal behavior**

    If intrusion detected, HIDS logs details, **send alerts** to **Managing server**
  - **Policy based**

    Normal system behavior described by **rules**

    Violating policies results in **action** by HIPS e.g. shutdown of processes
  - **Log based**

    Monitor and analyse log data

NGFWs

Intrusion Prevention (Subscription)

Firepower Analytics and Automation

Advanced Malware Protection and Sandboxing (Subscription)

URL Filtering (Subscription)

Application Visibility and Control

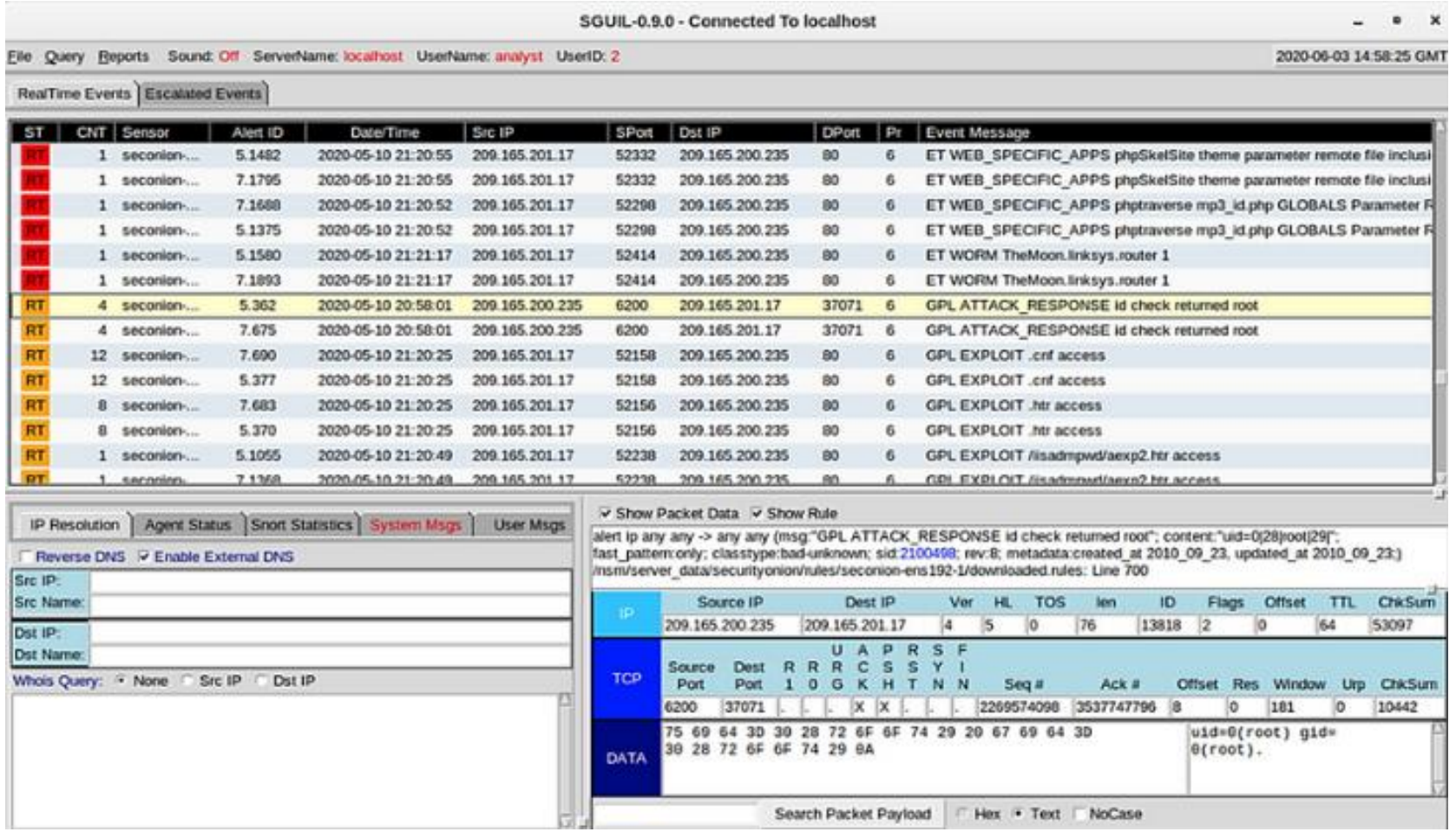
Built-in Network Profiling

Identity-Policy Control and VPN

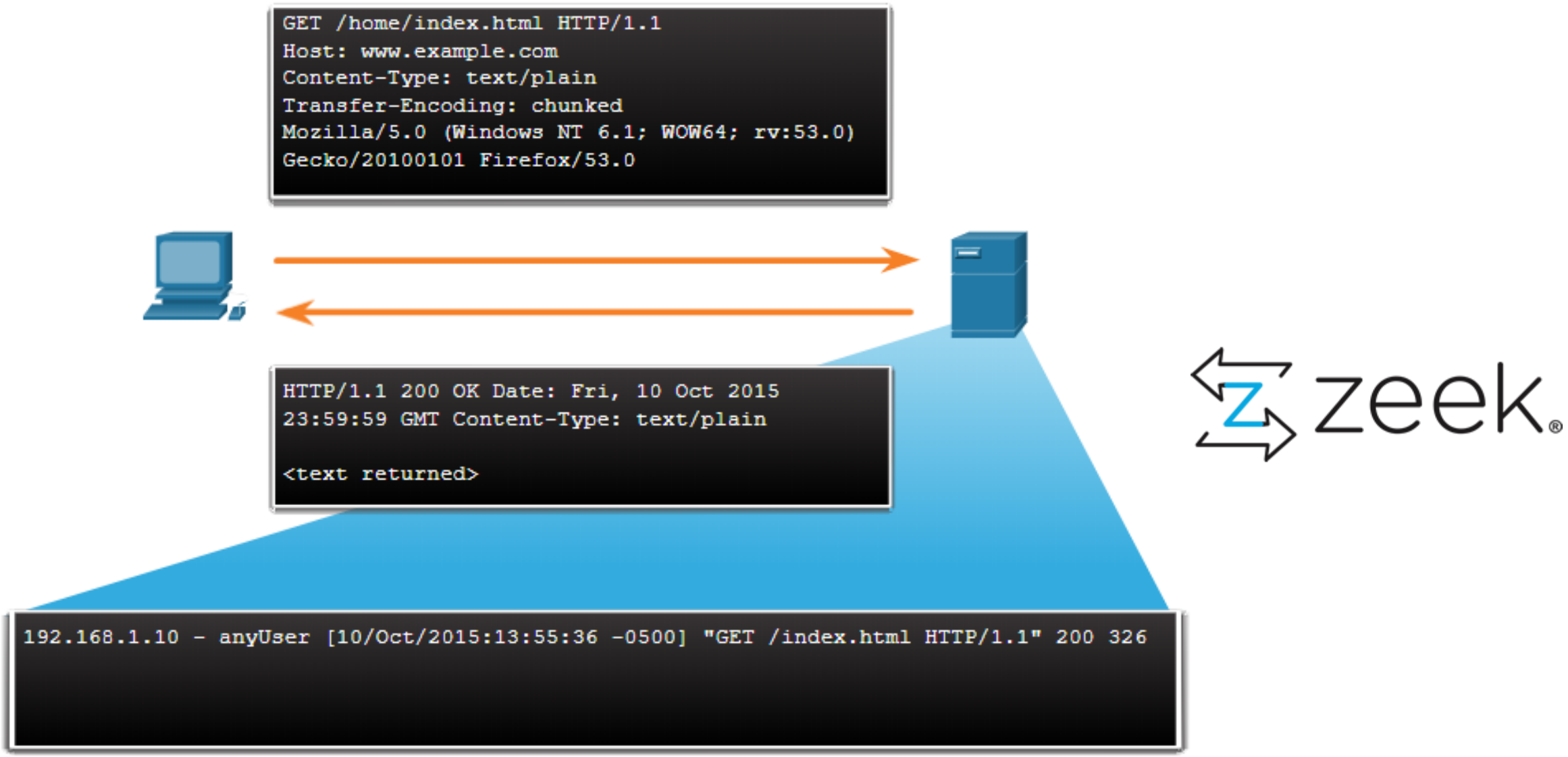
Network Security Data

Alert Data

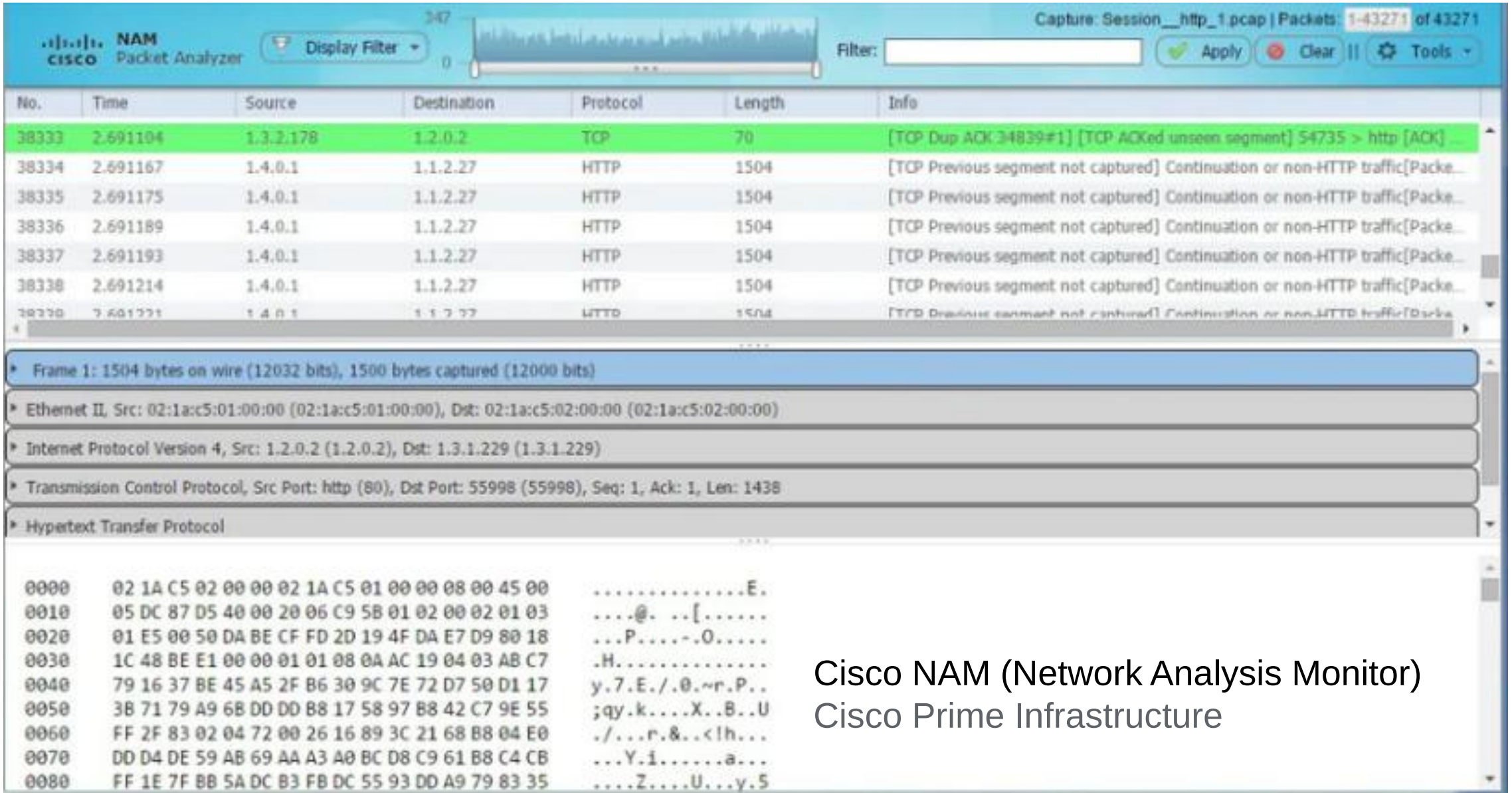
- Violation of IDS/IPS rule or matching the signature of a known exploit



Session and Transaction Data



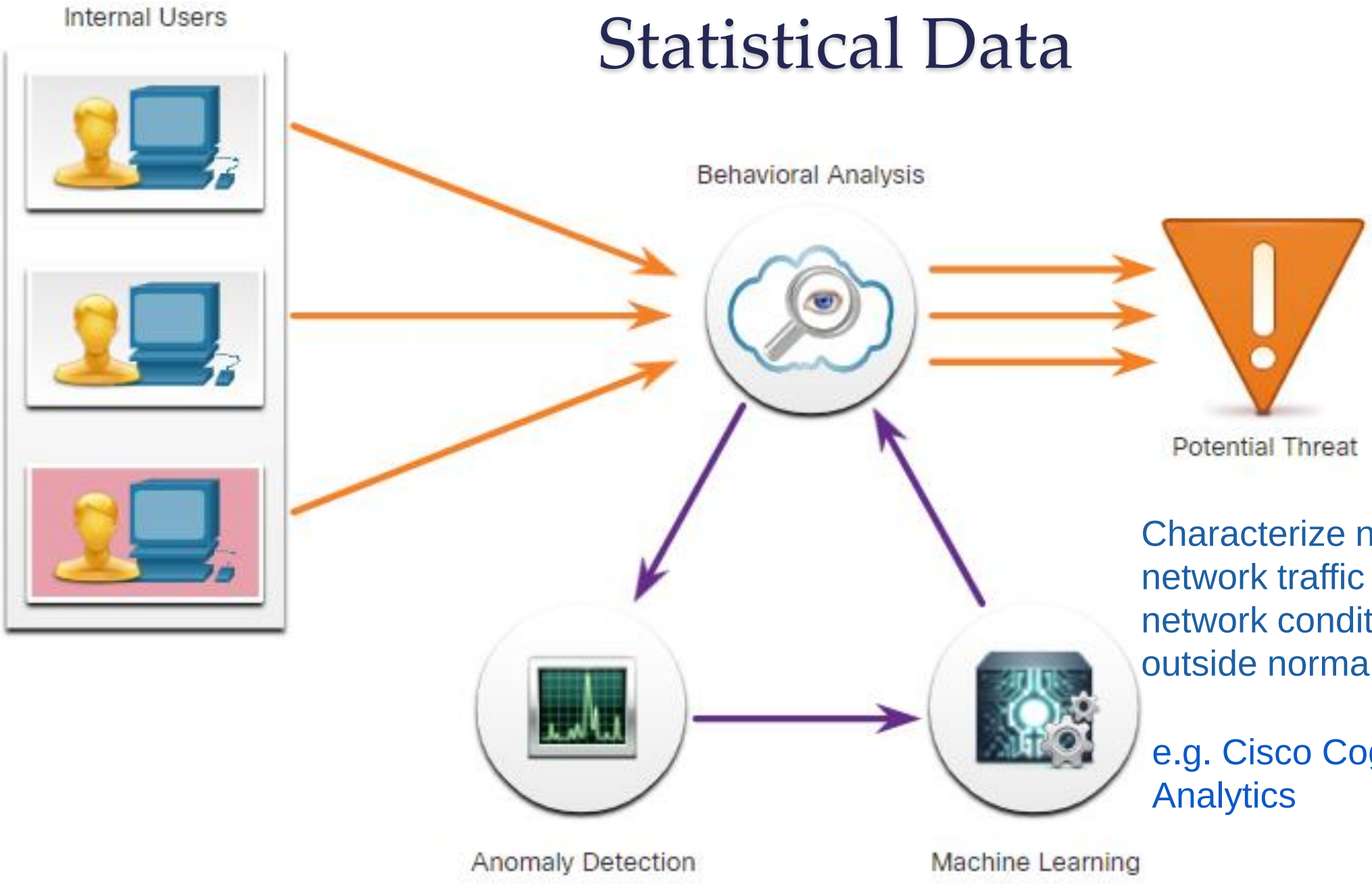
Full Packet Captures



Cisco NAM (Network Analysis Monitor)

Cisco Prime Infrastructure

Statistical Data



Characterize normal variation in network traffic patterns to identify network conditions that are outside normal ranges

e.g. Cisco Cognitive Threat Analytics

NSM

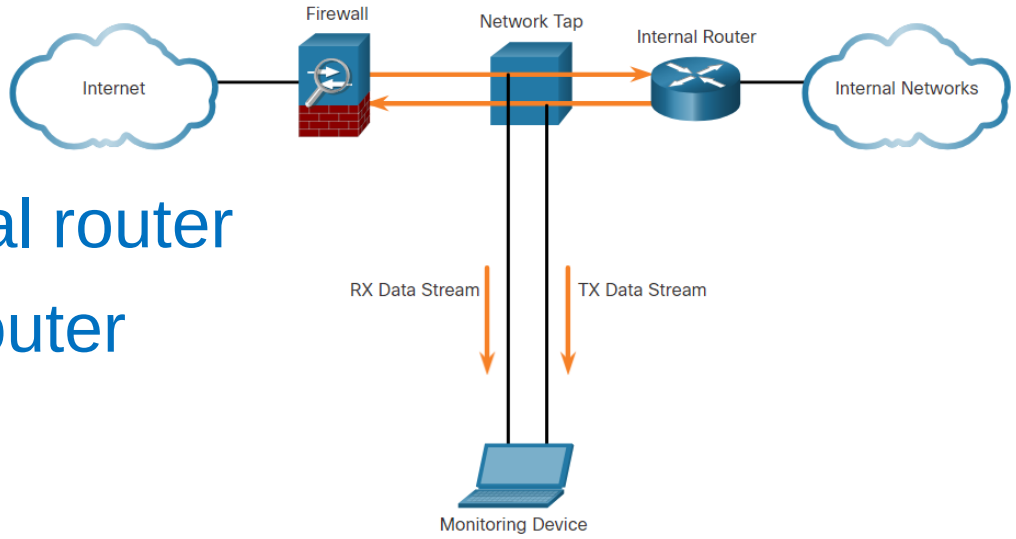
Network Monitoring Methods

- **Normal network behaviour** consists of traffic flow, bandwidth usage and resource access
- To determine network behaviour, **monitoring** must be implemented
- IDS, packet analyzers, SNMP, NetFlow, ….
- Two common methods to **capture traffic** for monitoring
  - **Network taps**
  - **Port mirroring**

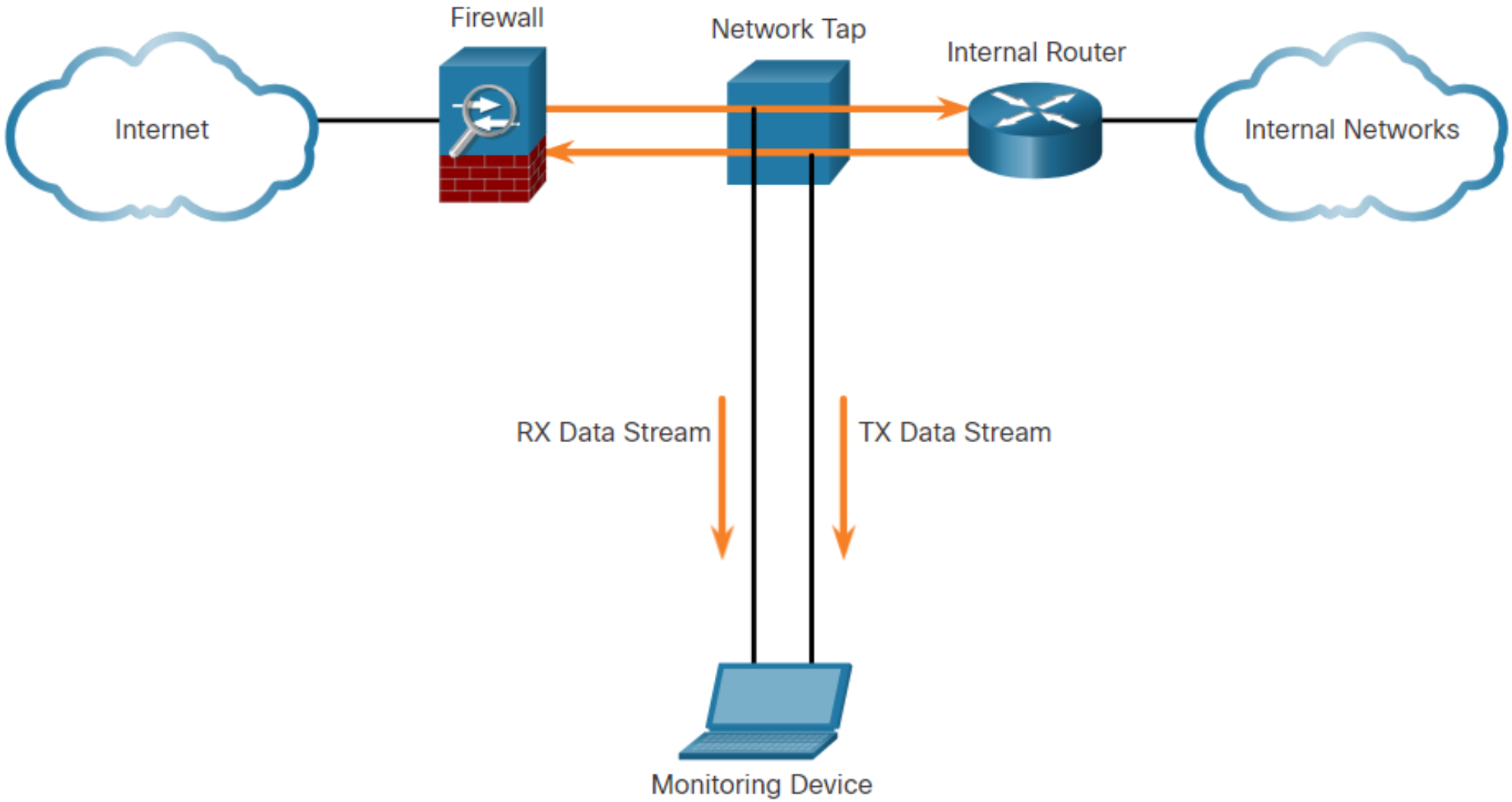
Network Taps

- **Passive** splitting device implemented **inline** between device of interest and network
- **Forwards** all traffic to analysis device while allowing traffic to its destination
- Simultaneously sends
  - **transmit (TX)** data stream from internal router
  - **receive (RX)** data stream to internal router

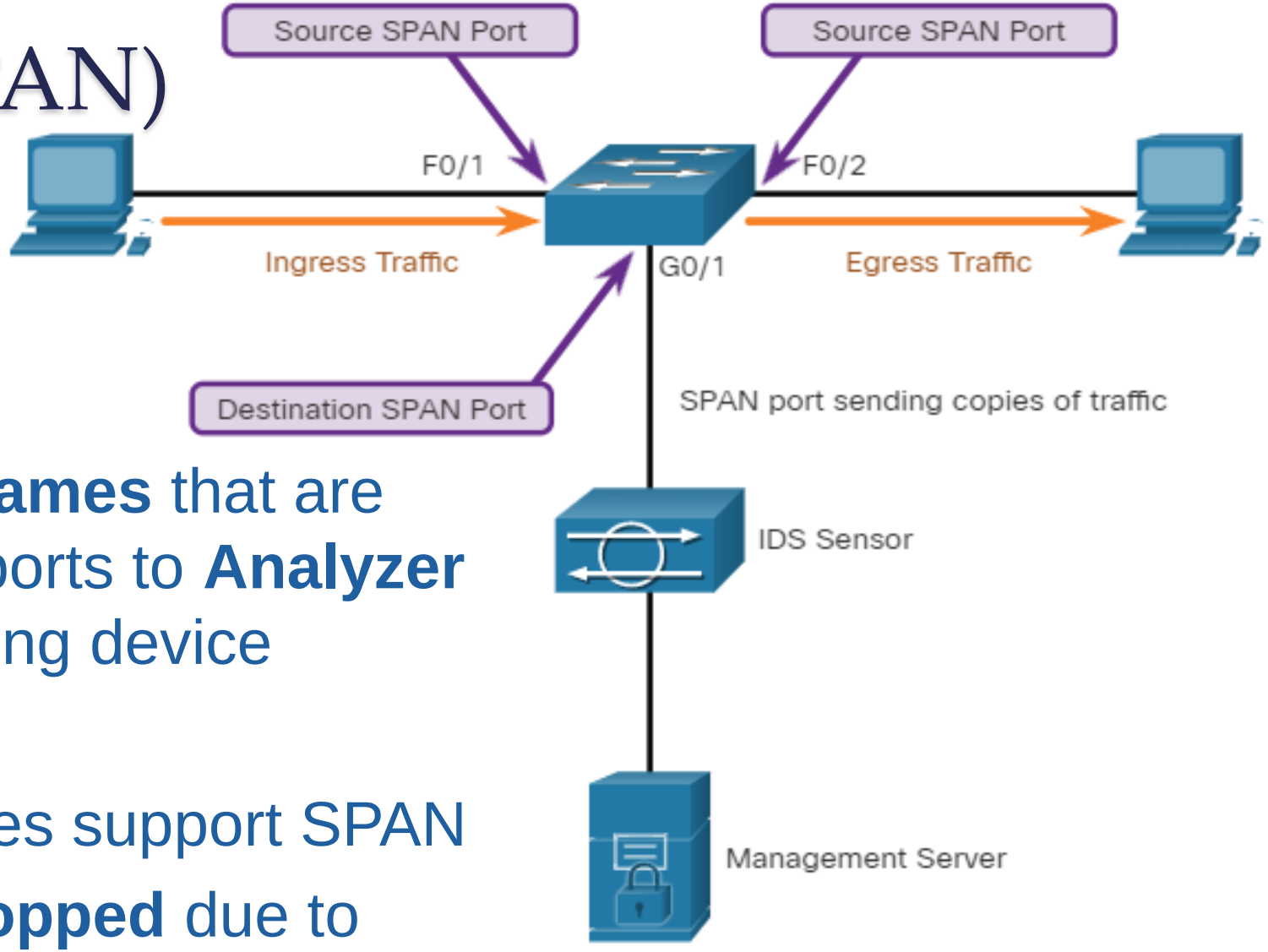
  on separate dedicated channels
- Fail-safe
- No impact on **performance**



Network Taps



Port Mirroring (SPAN)

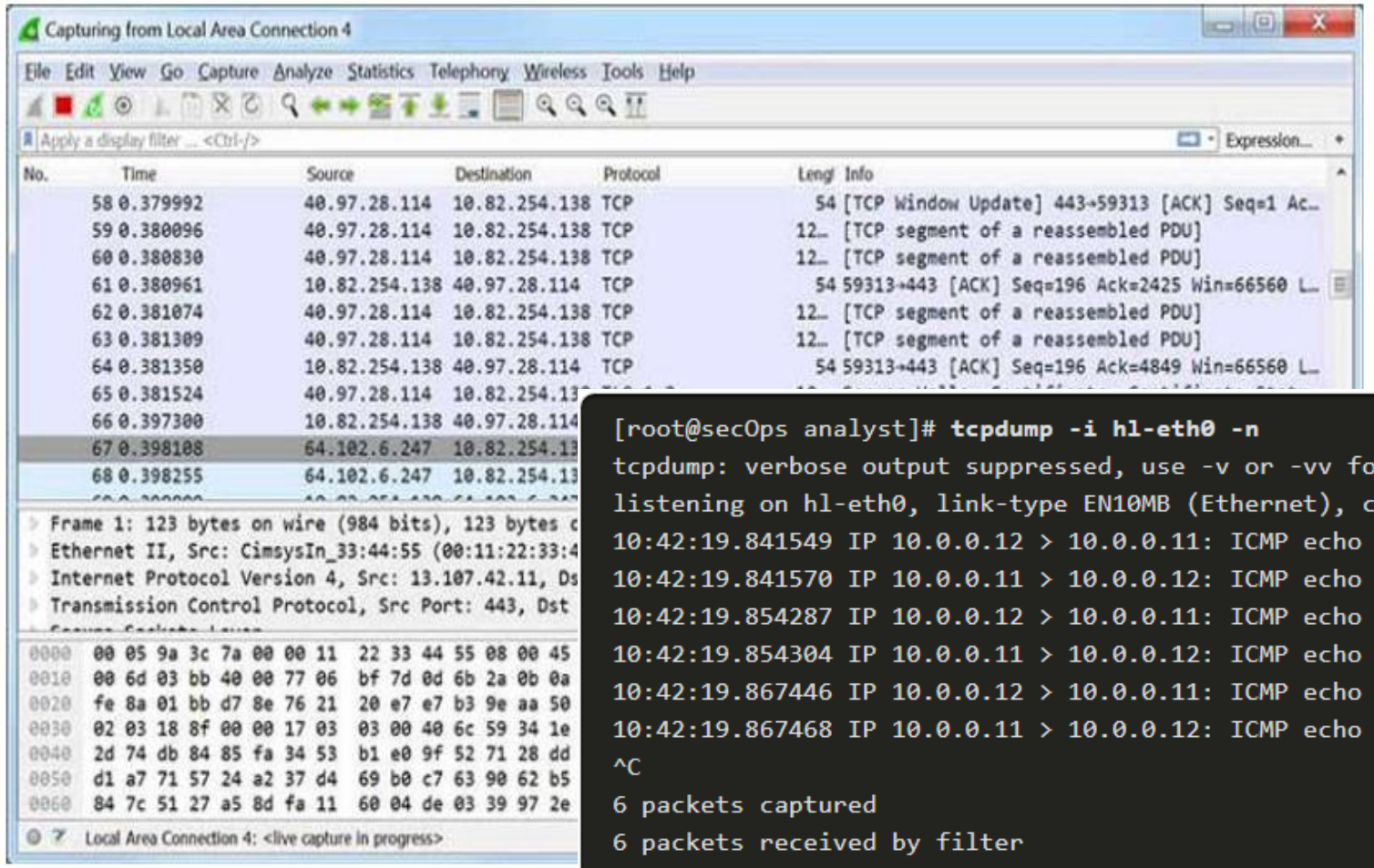


- Enables switch to **copy frames** that are received on one or more ports to **Analyzer** port connected to monitoring device
- Can affect **performance**
- **Not** all routers and switches support SPAN
- Some packets may be **dropped** due to overload

Network Security Monitoring Tools

- Network protocol **analyzers**
  - e.g. Wireshark and Tcpdump
- **NetFlow**
- **SNMP**
- **Log** files (Syslog)
- **SIEM** (Security Information and Event Management)

Network Protocol Analyzers (Packet Sniffers)



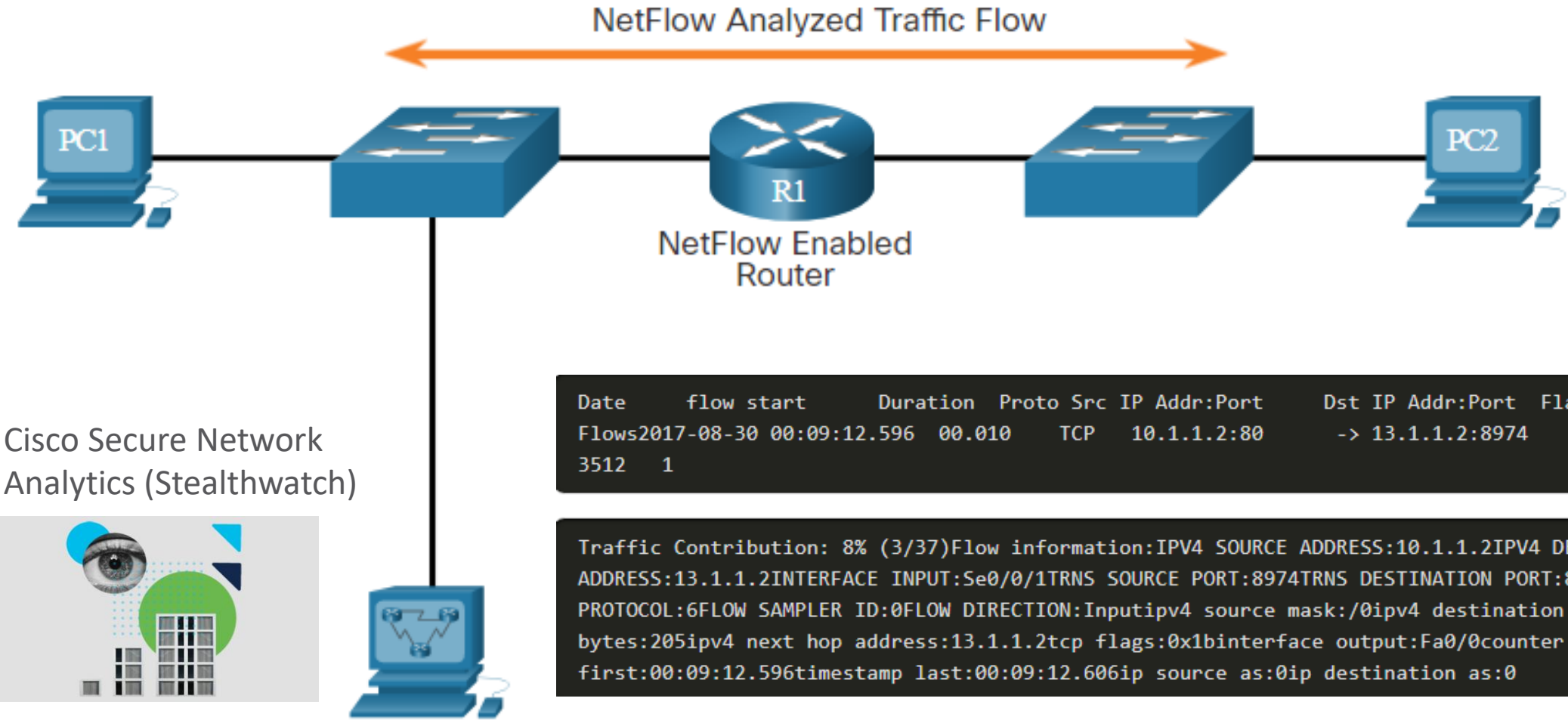

```
[root@secOps analyst]# tcpdump -i hl-eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on hl-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
10:42:19.841549 IP 10.0.0.12 > 10.0.0.11: ICMP echo request, id 2279, seq 5, length 64
10:42:19.841570 IP 10.0.0.11 > 10.0.0.12: ICMP echo reply, id 2279, seq 5, length 64
10:42:19.854287 IP 10.0.0.12 > 10.0.0.11: ICMP echo request, id 2279, seq 6, length 64
10:42:19.854304 IP 10.0.0.11 > 10.0.0.12: ICMP echo reply, id 2279, seq 6, length 64
10:42:19.867446 IP 10.0.0.12 > 10.0.0.11: ICMP echo request, id 2279, seq 7, length 64
10:42:19.867468 IP 10.0.0.11 > 10.0.0.12: ICMP echo reply, id 2279, seq 7, length 64
^C
6 packets captured
6 packets received by filter
0 packets dropped by kernel
[root@secOps analyst]#
```

- Security analysis
- Network troubleshooting
- Software and protocol development
- Education

NetFlow

- Cisco IOS provides 24/7 **statistics** on **packet flow** through **router** or multilayer switch
- Used for network and security **monitoring**, network **planning** and traffic **analysis**
- Complete **audit trail** of info about all IP flow forwarded on device
  - Monitors application connection by **tracking byte and packet** counts
  - Analysis of **security incidents** e.g. timeline of compromise
- NetFlow stores flow data in device **local cache**
  - Configure to forward data to **NetFlow collector**
  - **nfdump** CL utility for viewing NetFlow data

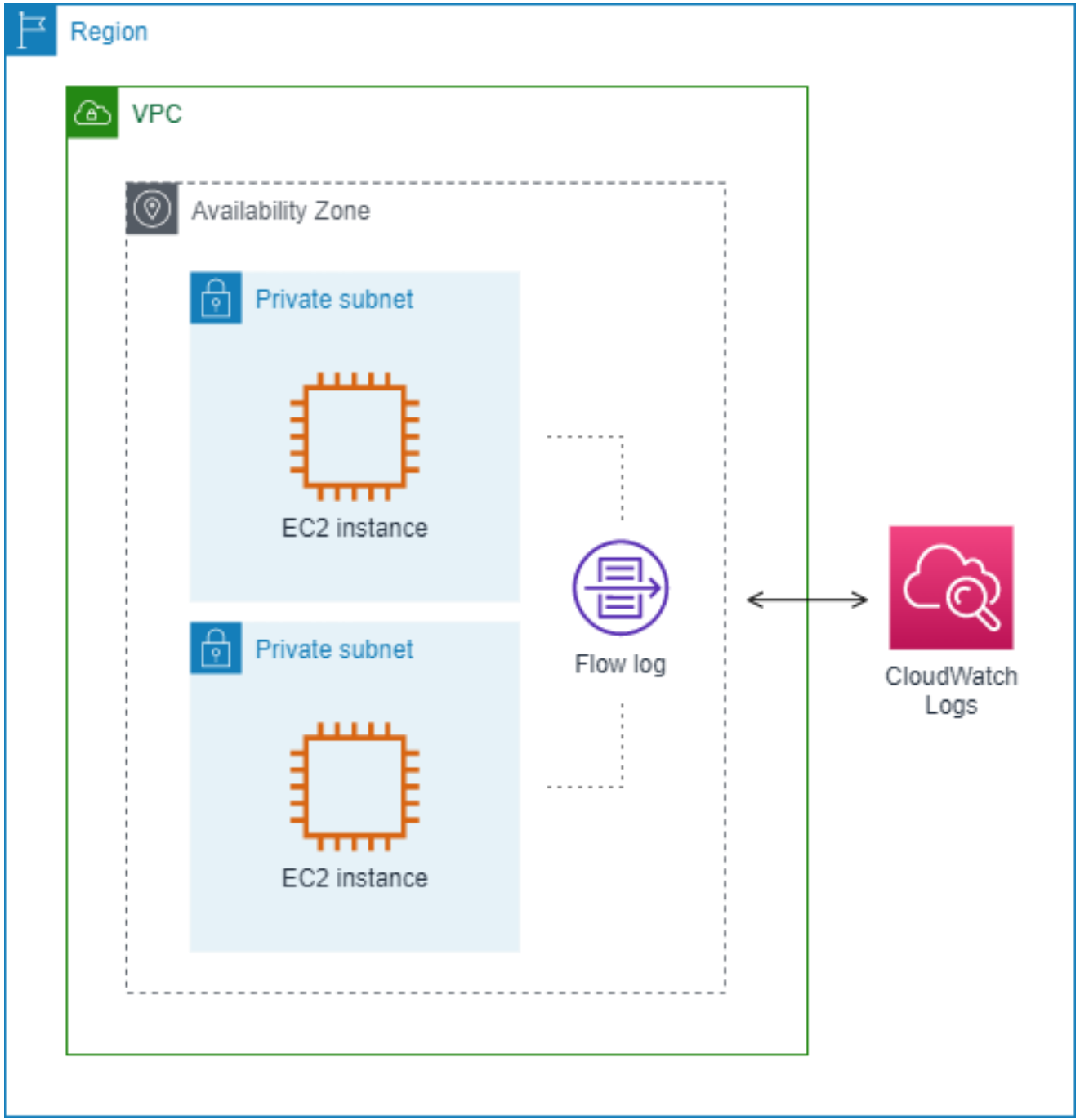
NetFlow (cont)




```
Date     flow start      Duration  Proto Src IP Addr:Port     Dst IP Addr:Port  Flags Tos Packets Bytes
Flows2017-08-30 00:09:12.596  00.010    TCP   10.1.1.2:80       -> 13.1.1.2:8974     .AP.SF  0   62
3512   1
```

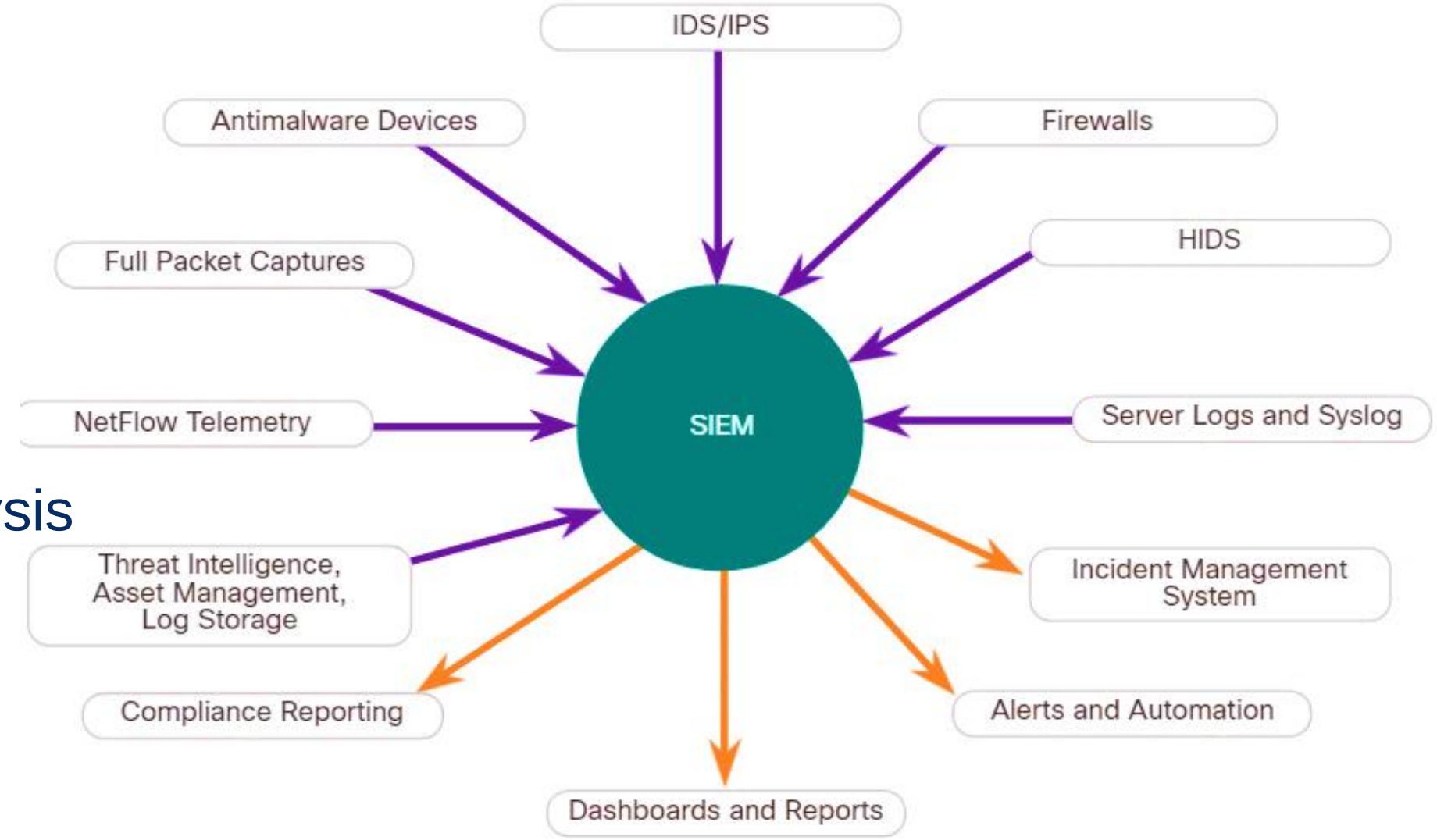
```
Traffic Contribution: 8% (3/37)Flow information:IPV4 SOURCE ADDRESS:10.1.1.2IPV4 DESTINATION
ADDRESS:13.1.1.2INTERFACE INPUT:Se0/0/1TRNS SOURCE PORT:8974TRNS DESTINATION PORT:80IP TOS:0x00IP
PROTOCOL:6FLOW SAMPLER ID:0FLOW DIRECTION:Inputipv4 source mask:/0ipv4 destination mask:/8counter
bytes:205ipv4 next hop address:13.1.1.2tcp flags:0x1binterface output:Fa0/0counter packets:5timestamp
first:00:09:12.596timestamp last:00:09:12.606ip source as:0ip destination as:0
```

Cisco Secure Network Analytics (Stealthwatch)

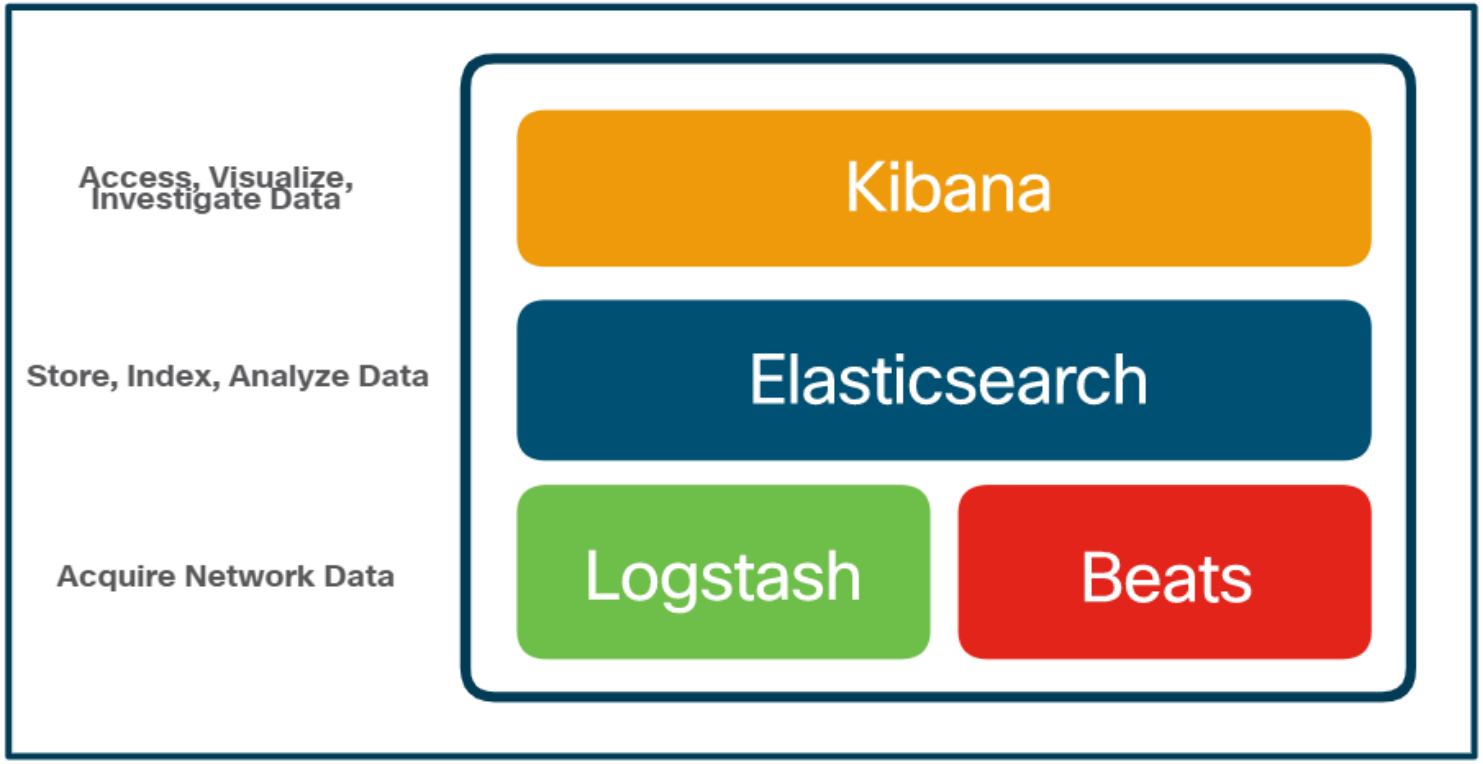

Region
VPC
Availability Zone
Private subnet
EC2 instance
Private subnet
EC2 instance
Flow log
CloudWatch
Logs

SIEM

- Log collection
- Normalization
- Correlation
- Aggregation
- Reporting
- Forensic analysis
- Compliance



SIEM Systems



Security Onion includes **Elastic Stack** (ELK) for SIEM features

Commercial SIEM

- SolarWinds Security Event Manager
- Splunk Enterprise Security
- IBM QRadar

SIEM Systems (cont)

- **Elasticsearch**

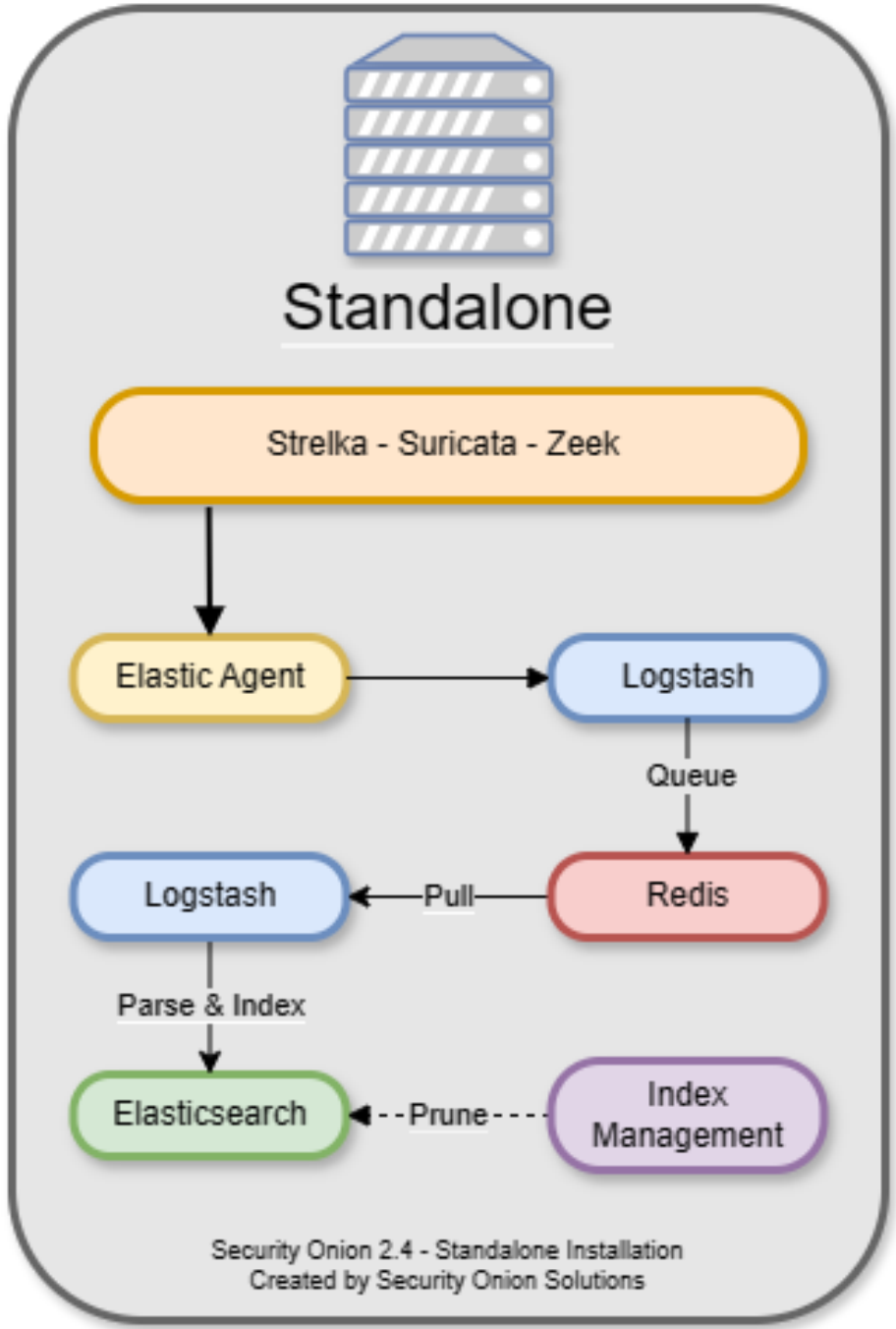
  Searching and analyzing organization's data in near **real-time**
- **Logstash**

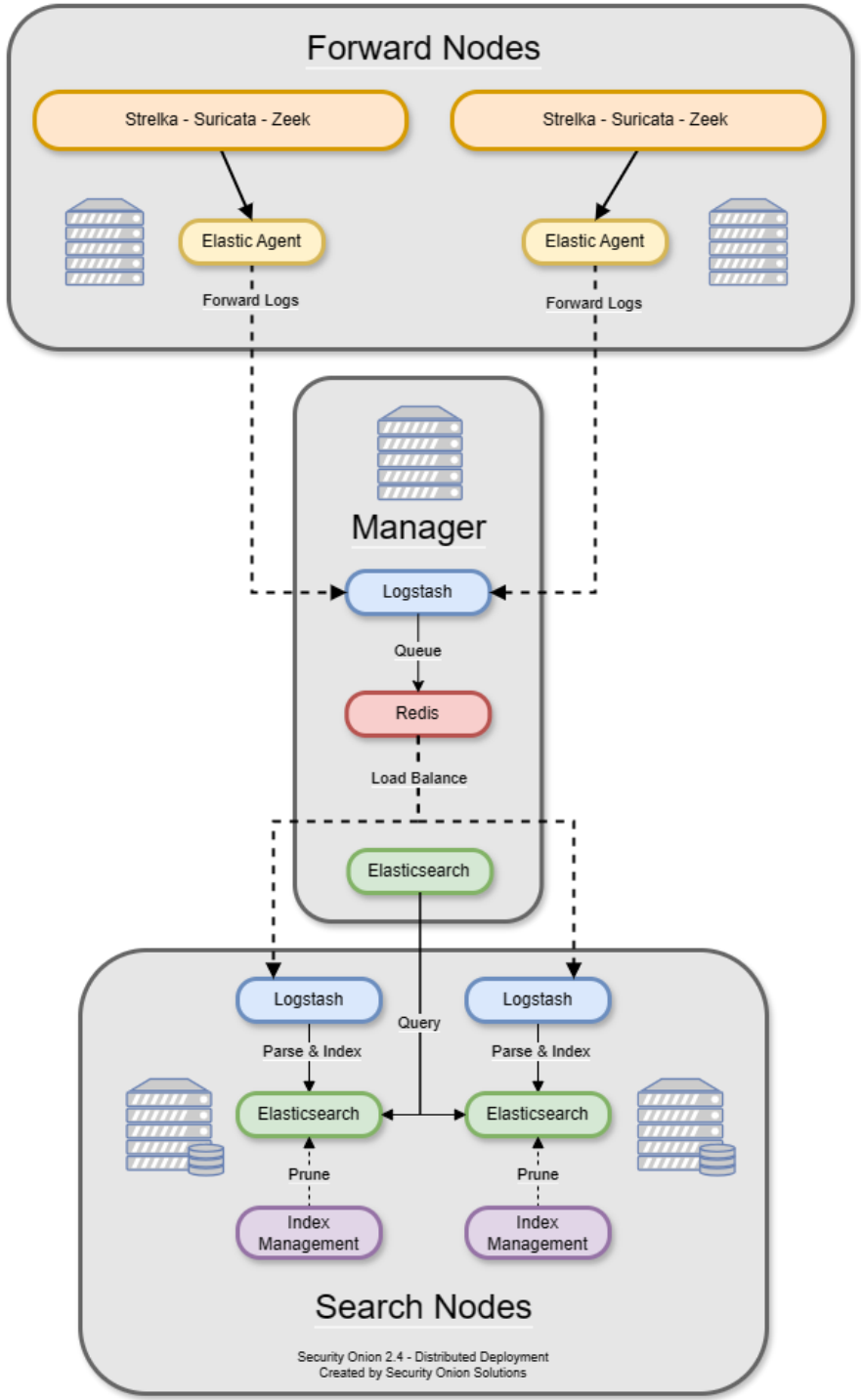
  Collection and **normalization** of network data into **format** to be efficiently searched by Elasticsearch
- **Kibana**

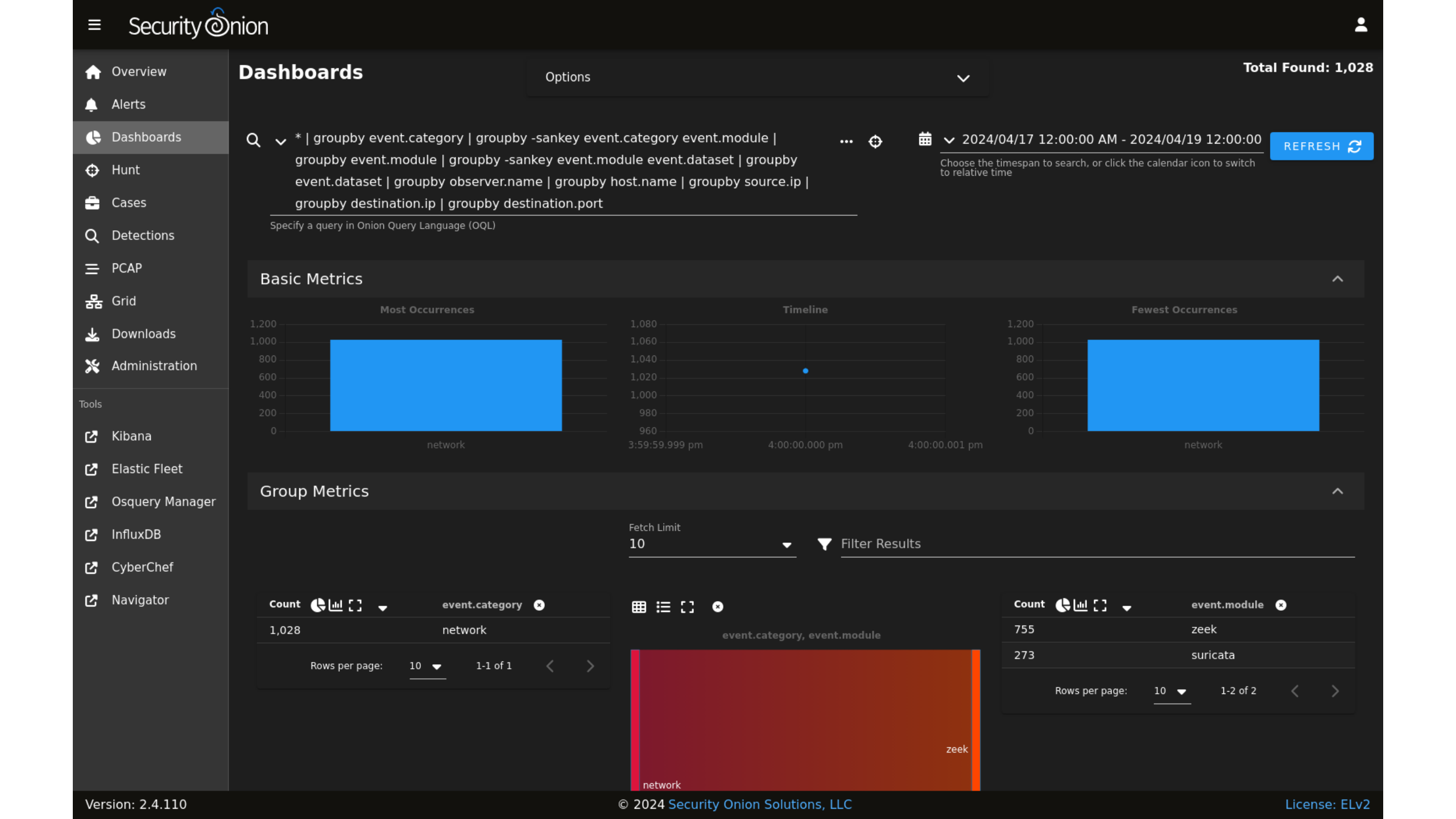
  GUI to data compiled by Elasticsearch
- **Beats**

  Agents on servers that send data to Elasticsearch datastores

Security Onion

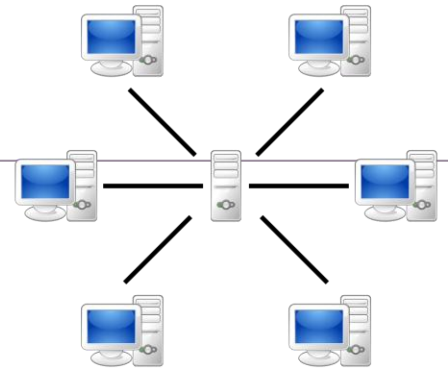

Standalone
Strelka - Suricata - Zeek
Elastic Agent
Logstash
Queue
Logstash
Pull
Redis
Parse & Index
Elasticsearch
Prune
Index Management
Security Onion 2.4 - Standalone Installation
Created by Security Onion Solutions


Forward Nodes
Strelka - Suricata - Zeek
Strelka - Suricata - Zeek
Elastic Agent
Elastic Agent
Forward Logs
Forward Logs
Manager
Logstash
Queue
Redis
Load Balance
Elasticsearch
Logstash
Logstash
Query
Parse & Index
Parse & Index
Elasticsearch
Elasticsearch
Prune
Prune
Index Management
Index Management
Search Nodes
Security Onion 2.4 - Distributed Deployment
Created by Security Onion Solutions


Security Onion
Overview
Alerts
Dashboards
Hunt
Cases
Detections
PCAP
Grid
Downloads
Administration
Tools
Kibana
Elastic Fleet
Osquery Manager
InfluxDB
CyberChef
Navigator
Dashboards
Options
Total Found: 1,028
* | groupby event.category | groupby -sankey event.category event.module | groupby event.module | groupby -sankey event.module event.dataset | groupby event.dataset | groupby observer.name | groupby host.name | groupby source.ip | groupby destination.ip | groupby destination.port
Specify a query in Onion Query Language (OQL)
2024/04/17 12:00:00 AM - 2024/04/19 12:00:00
Choose the timespan to search, or click the calendar icon to switch to relative time
REFRESH
Basic Metrics
Most Occurrences
1,200
1,000
800
600
400
200
0
network
Timeline
1,080
1,060
1,040
1,020
1,000
980
960
3:59:59.999 pm
4:00:00.000 pm
4:00:00.001 pm
Fewest Occurrences
1,200
1,000
800
600
400
200
0
network
Group Metrics
Fetch Limit
10
Filter Results
Count
event.category
1,028
network
Rows per page: 10
1-1 of 1
event.category, event.module
zeek
network
Count
event.module
755
zeek
273
suricata
Rows per page: 10
1-2 of 2
Version: 2.4.110
© 2024 Security Onion Solutions, LLC
License: ELv2

Security Onion (cont)

CapME	Web interface for viewing **pcap transcripts** rendered with tcpflow or Zeek
Stenographer	
Strelka	
Suricata	NIDS, NIPS Signature-based approach
Wireshark	Packet capture Can be opened from other tools to display **full packet captures**



Security Onion (cont)

Zeek	NIDS + Network **traffic analyzer** and security monitor Behavior-based approach **Inspects** all traffic on network segment with **in-depth** analysis Pivot from **Sguil to Zeek** for access to transaction logs, file content and customized output
Cyberchef	
Kibana	**Interactive dashboard** interface to Elasticsearch data Allows **querying** of NSM data with flexible **visualizations** Possible to **pivot** from Sguil into Kibana

Snort Rules

Snort Rule Structure

```
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root";
content:"uid=0|28|root|29|"; fast_pattern:only; classtype:bad-unknown; sid:2100498;
rev:8;)
/nsm/server_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692
```

Component	Example	Explanation
rule header	alert ip any any -> any any	Action to be taken, protocol, source and dest addresses, ports and direction of traffic
rule options	(msg:"GPL ATTACK_RESPONSE ID CHECK RETURNED ROOT";…)	Message to be displayed, packet content, event type, source ID and additional details e.g. reference for rule or vulnerability
rule location	/nsm/server_data/securityonion/rules/…	Added by Sguil to indicate rule location in Security Onion and in rule file

Rule Header

```
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root";
content:"uid=0|28|root|29|"; fast_pattern:only; classtype:bad-unknown; sid:2100498;
rev:8;)
/nsm/server_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692
```

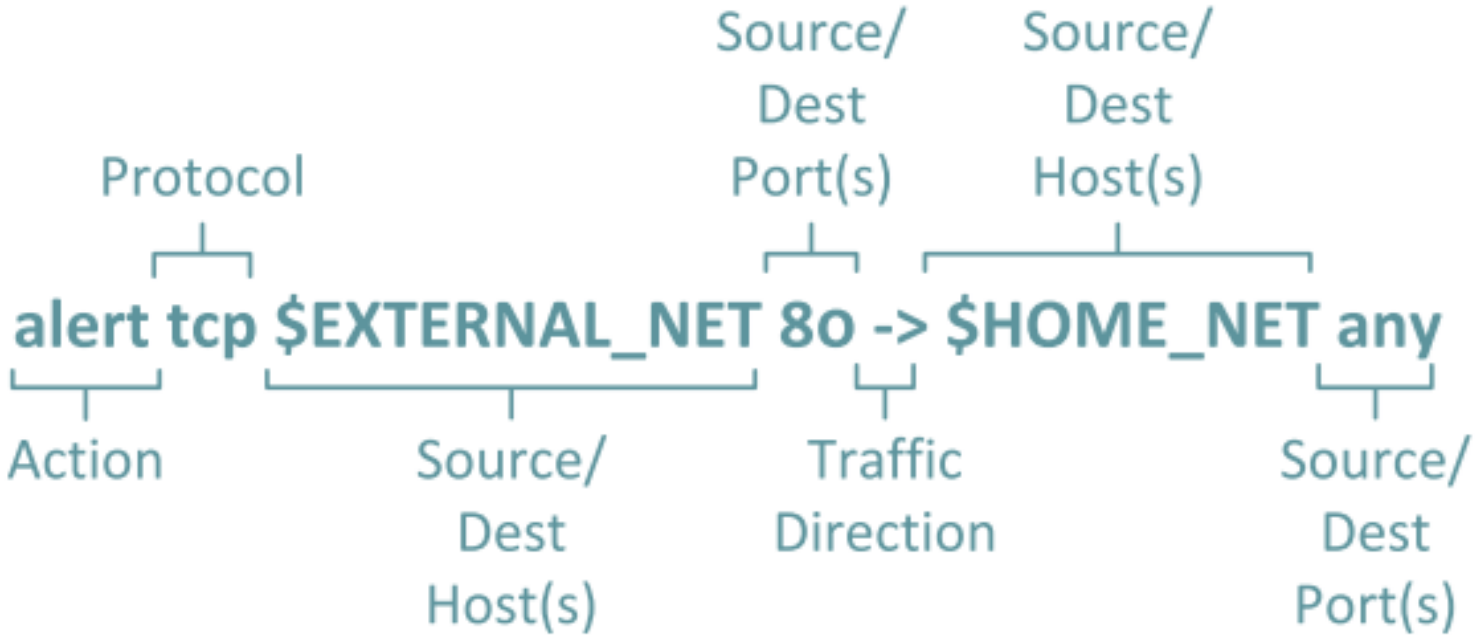
alert	Action is to issue an alert, other actions: **log**, **pass**
ip	Protocol; IP, TCP, UDP, ICMP
any any	Specified source is any IP address and any Layer 4 port
->	Direction of flow is from source to destination
any any	Specified destination is any IP address and any Layer 4 port

Rule Options

```
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root";
content:"uid=0|28|root|29|"; fast_pattern:only; classtype:bad-unknown; sid:2100498;
rev:8;)
/nsm/server_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692
```

msg:	Describes alert
content:	Refers to packet content Alert is sent if text “uid=0(root)” appears in packet data
reference:	Link to URL for more info on rule
classtype:	Category for attack e.g. bad-unknown = potentially bad traffic
sid:	Unique numeric rule identifier
rev:	Revision of rule represented by sid
fast_pattern:	only evaluate rule if content is found in payload

Rule Header



Rule Options

```
<option>: <option values>;
<option>;
```

```
reference: <reference name>,<reference>;
```

```
reference:url,vil.nai.com/vil/content/v_157489.htm;
```

Sources for Snort rules

- **GPL**
  - Older rules created by **Sourcefire** and distributed under GPLv2
  - Available from **Snort website** and used in Security Onion
- **ET**
  - **Emerging Threats (Proofpoint, Inc)**
  - Collection point for rules from multiple sources
  - A set of ET rules is included with Security Onion
- **VRT**
  - Created and maintained by Cisco Talos

Summary

- Defense in Depth
  - Layered security, security onion, artichoke, zero trust, attack surfaces
- Network Security Infrastructure
  - DMZ, ZPF, stateless, stateful, proxy, IPS, IDS, NGFW
- Access Control
  - MAC, DAC, RBAC, ABAC, XACML, SSO, SAML, OAuth, AAA
- Antimalware Protection
  - Host-based antimalware, host-based firewalls, HIDS
- Network Security Data
  - Alerts, packet captures, session data, transactional, statistical, logs, …
- Network Security Monitoring
  - Taps, SPAN, Netflow, SIEM, …
- Security Onion
  - Kibana, Zeek, Wazuh, Suricata, Wireshark, …
- Snort rules
  - Header, options