

NDE
Network Defense Essentials

Module 05

# Network Security Controls - Technical Controls

# Module Objectives



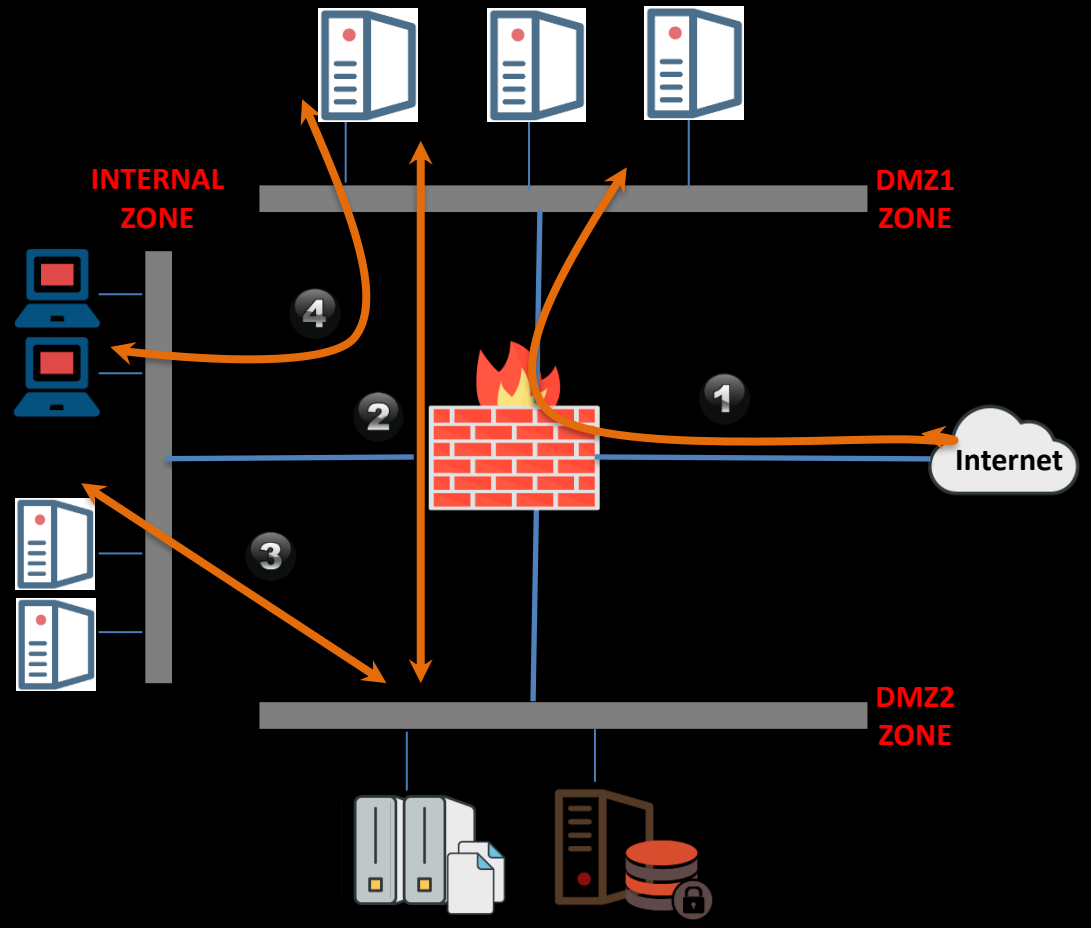
- Understanding Network Segmentation and its Types
- Understanding the Different Types of Firewalls and their Roles
- Understanding the Different Types of IDS/IPS and their Roles
- Overview of Different Types of Honeypots
- Understanding the Different Types of Proxy Servers and their Benefits
- Understanding the Fundamentals of Virtual Private Networks (VPNs) and their Importance in Network Security
- Overview of Security Incident and Event Management (SIEM) and User Behavior Analytics (UBA)
- Overview of Various Antivirus/Anti-malware Software

# Module Flow

1. Understand Different Types of Network Segmentation
2. Understand Different Types of Firewalls and their Role
3. Understand Different Types of IDS/IPS and their Role
4. Understand Different Types of Honeypots
5. Understand Different Types of Proxy Servers and their Benefits
6. Discuss Fundamentals of VPN and its importance in Network Security
7. Discuss Security Incident and Event Management (SIEM)
8. Discuss User Behavior Analytics (UBA)
9. Understand Various Antivirus/Anti-malware Software

# What is Network Segmentation?

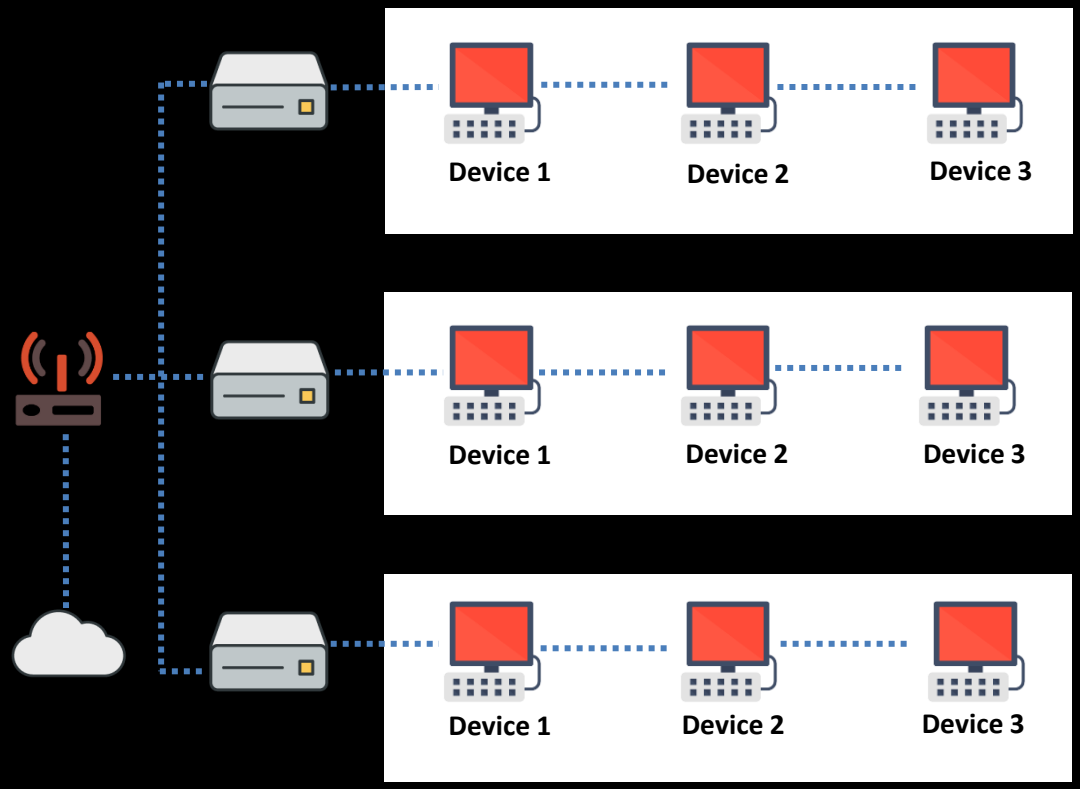
- Network segmentation is the practice of **splitting** a network into smaller network segments and separating groups of systems or applications from each other
- In a segmented network, groups of systems or applications that have no interaction with each other will be placed in different network segment
- Security benefits of Network Segmentation
  - ✓ Improved Security
  - ✓ Better Access Control
  - ✓ Improved Monitoring
  - ✓ Improved Performance
  - ✓ Better Containment



# Types of Network Segmentation

- smaller physical components
- intermediary devices
- expensive

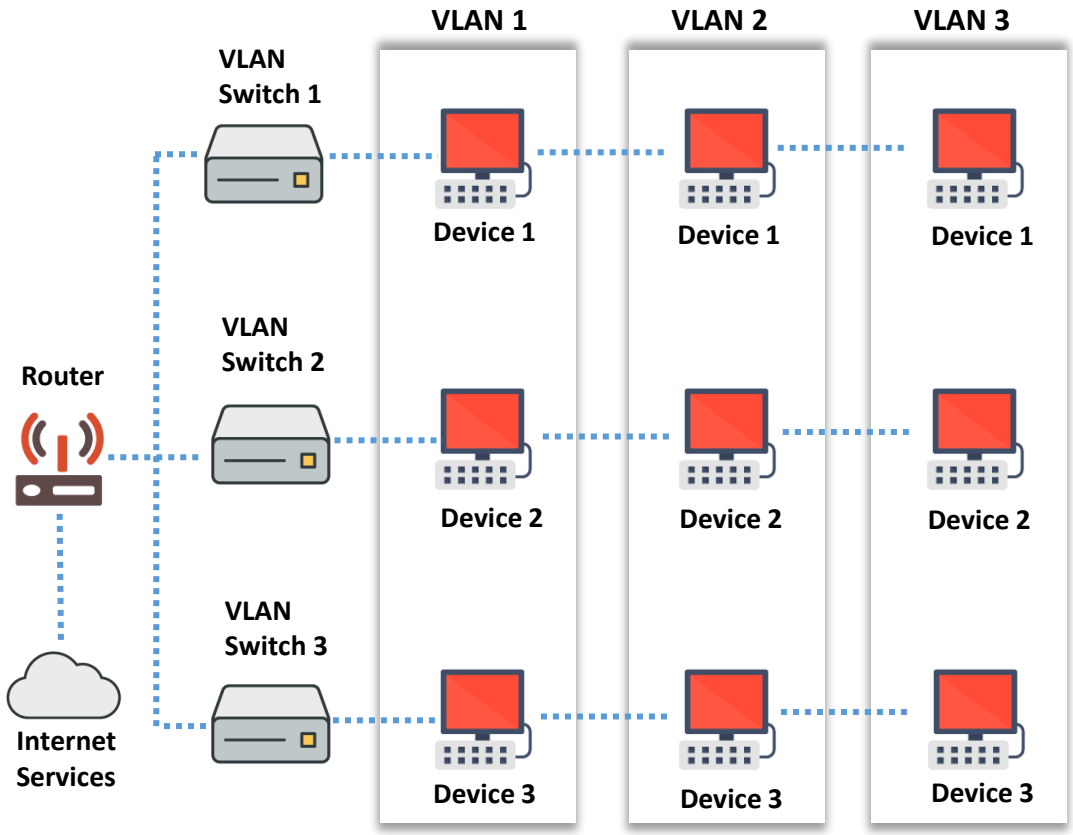
## Physical Segmentation



# Types of Network Segmentation (Cont'd)

- Logical segmentation utilizes **VLANs**, which are **isolated logically** without considering the physical locations of devices
- Each VLAN is considered an **independent logical unit**, and the devices within a VLAN communicate as though they are in their own isolated network
- In this approach, **firewalls** are shared, and **switches** handle the VLAN infrastructure
- It is easier to implement and flexible to operate

## Logical Segmentation

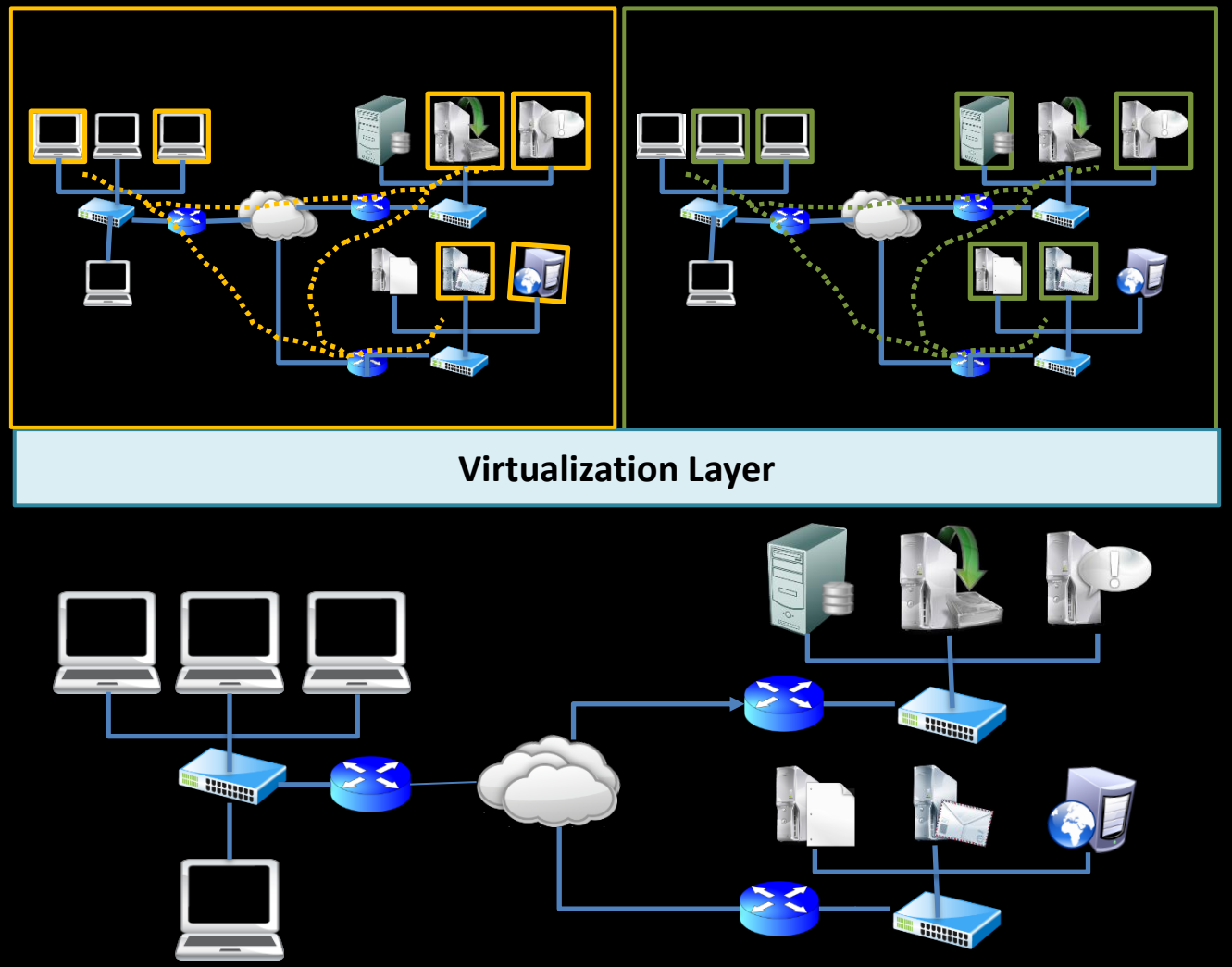


# Types of Network Segmentation (Cont'd)

## Network Virtualization

- Network virtualization is a process of combining all the available network resources and enabling security professionals to share these resources amongst the network users using a **single administrative unit**

- Network virtualization enables each user to access available network resources such as files, folders, computers, printers, hard drives, etc. from their system



# Introduction to Bastion Host

01 A bastion host is a computer system designed and configured to **protect network resources** from attacks

02 A bastion host is the only host computer on the Internet that can be **addressed directly** from the public network

03 It provides a **limited range of services** such as website hosting, and mail to ensure security



# Need for Bastion Host

01 **Minimize the chances of penetration** by intruders

02 **Create all the logs**, which can be used to identify attack or attempts to attack

03 In case of an attack, bastion host acts as **scapegoat**

04 **Provide an additional level of security**



# Positioning the Bastion Host



## Physical Location

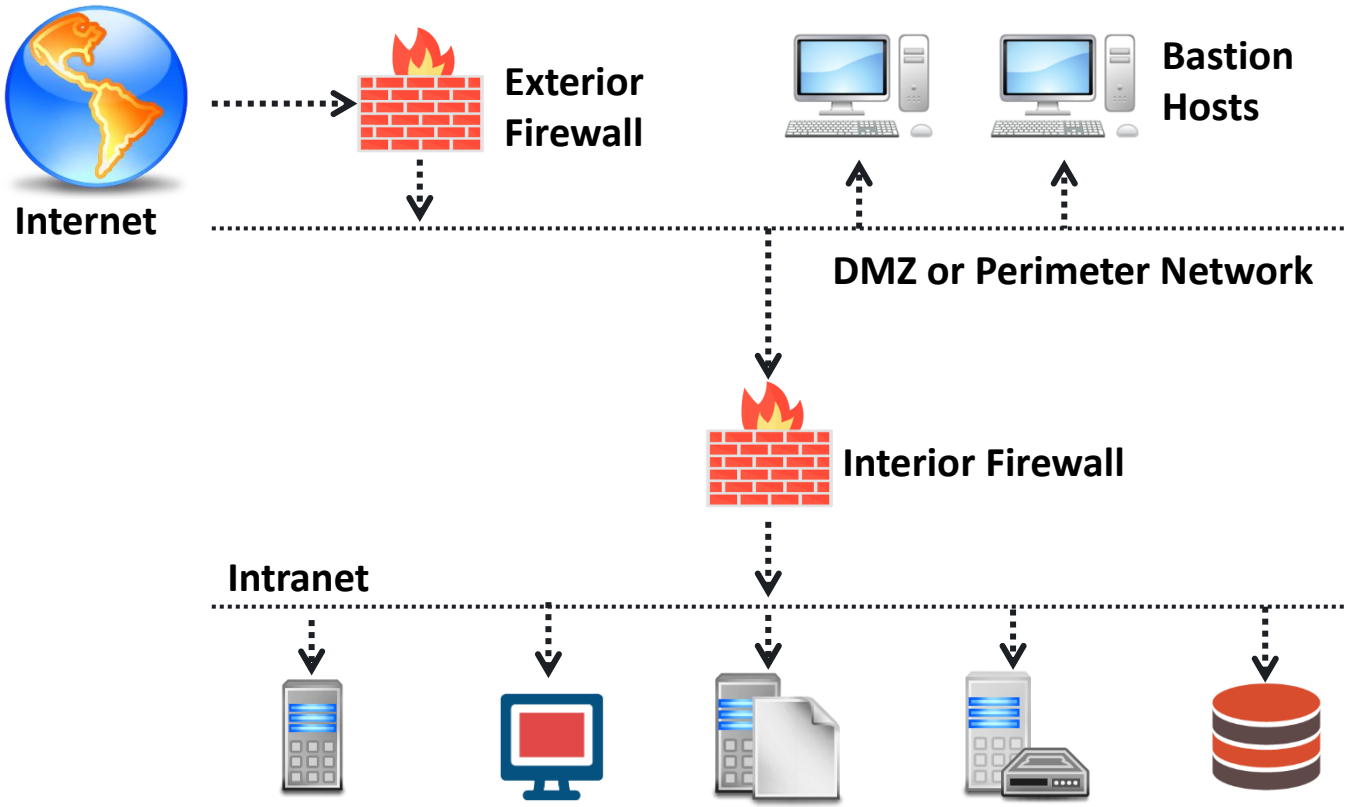
- Placed in a specially selected server room with suitable **environmental controls**
- Must be set up in a locked server cabinet with proper **ventilation**, cooling, and backup power



## Network Location

- Set on a special network also known as **Demilitarized zone** (**DMZ**) that does not carry sensitive data
- Avoid placing the **bastion host** on internal networks
- Should be located on an additional layer known as a **perimeter network**
- Attach packet filtering router

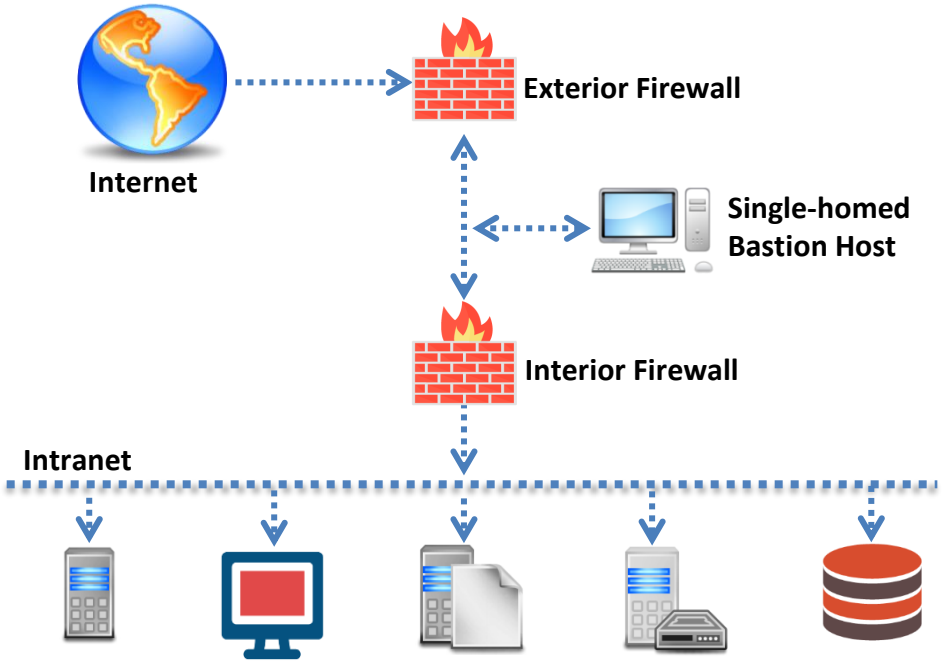
# Positioning the Bastion Host (Cont'd)

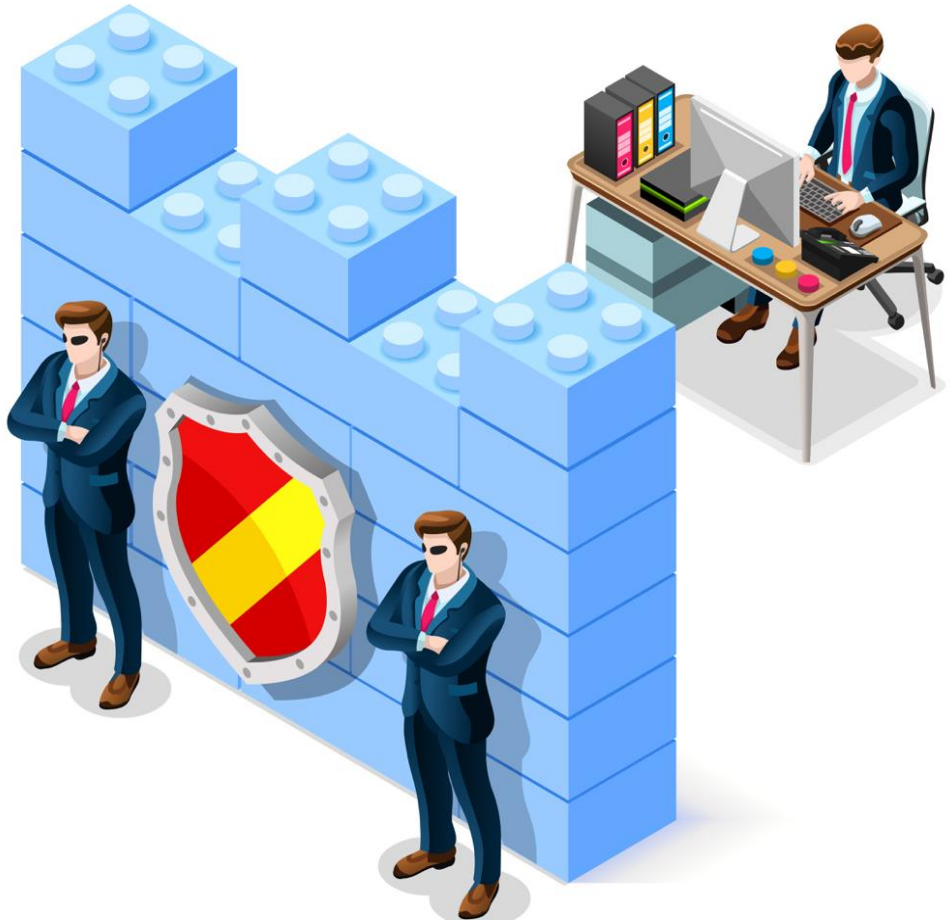





# Types of Bastion Hosts: Single-homed

- A firewall device with only **one network interface**
- All the traffic, both incoming and outgoing, is **routed through** the bastion host
- It tests data against security guidelines and acts accordingly

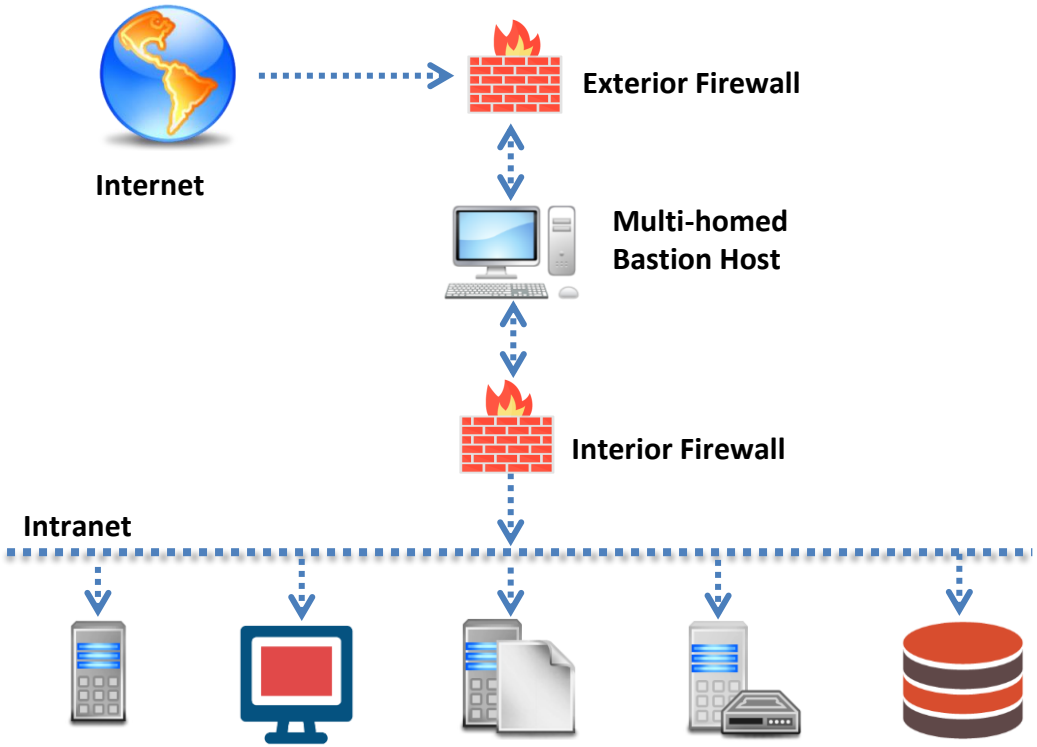


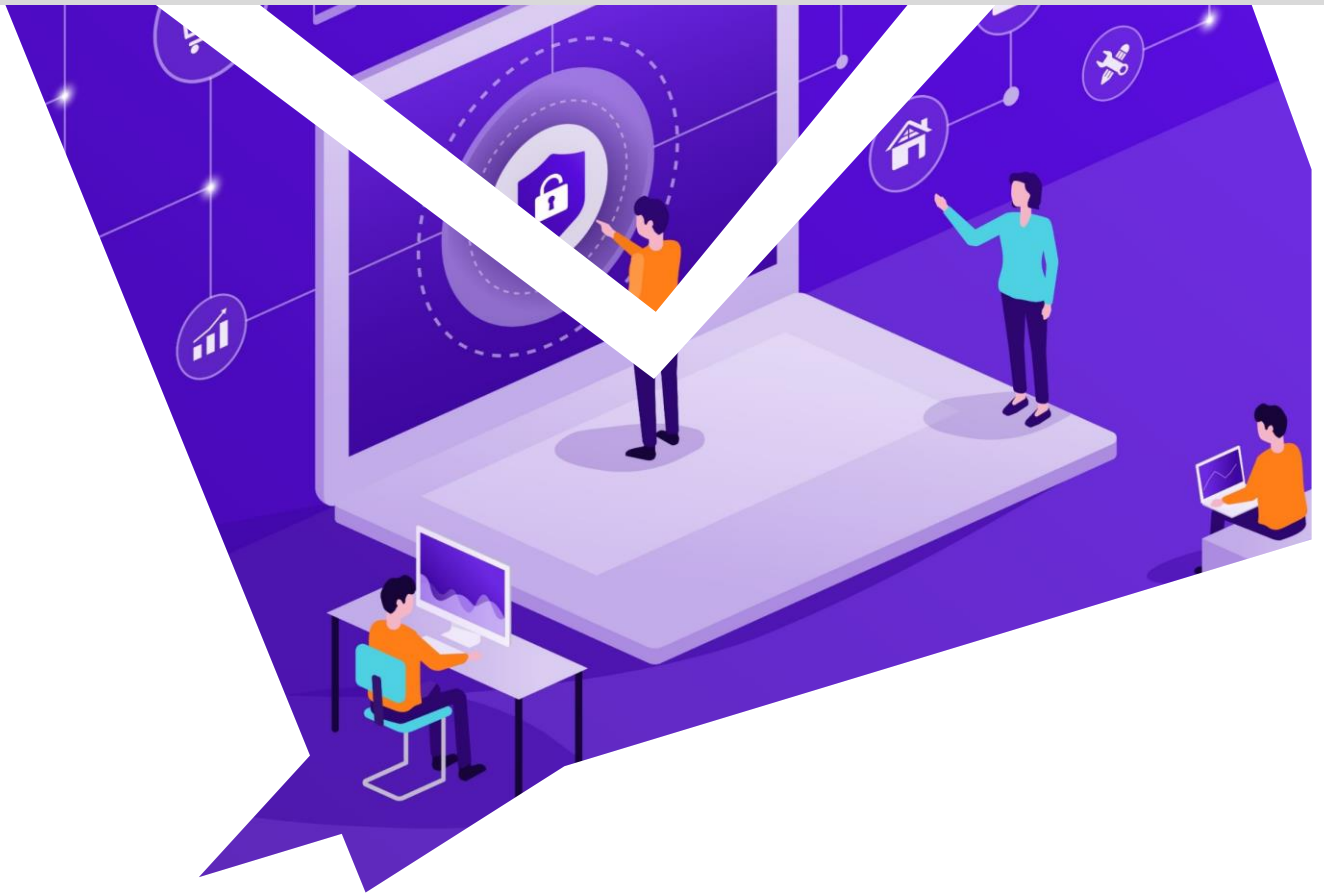



# Types of Bastion Hosts: Multi-homed



- A firewall device with at least **two network interfaces**
- This type of bastion host is capable of separating internal and external networks, thereby **improving security**



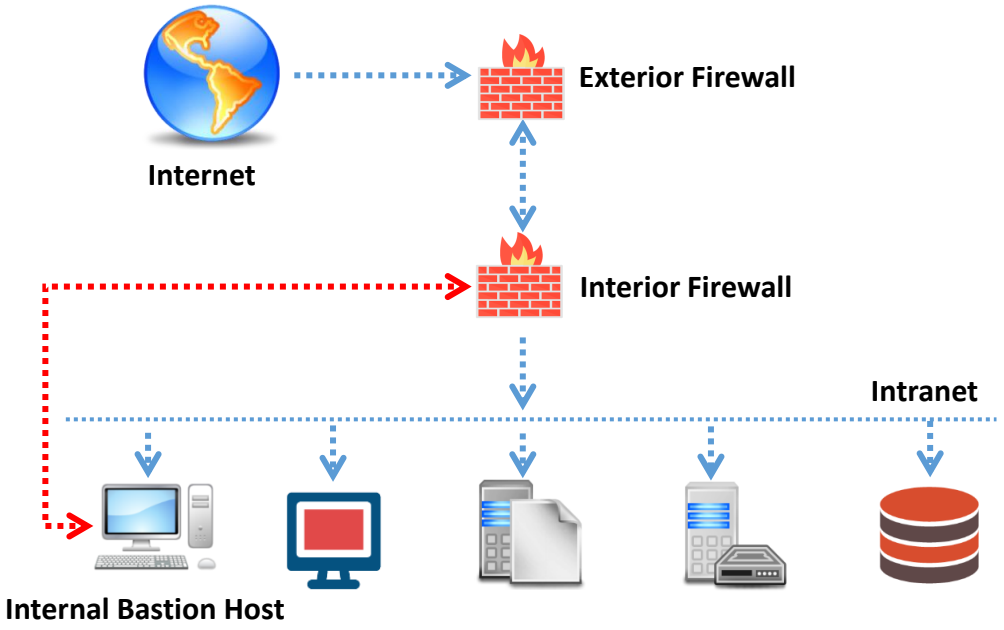


# Types of Bastion Hosts: Internal Bastion Host

01 They reside **inside** the internal network of an organization

02 It can be **single-homed** or **multi-homed**

03 The internal network devices **communicate** with the internal bastion host



# Types of Bastion Hosts (Cont'd)

## Non-routing Dual-homed Hosts

- ✓ They operate with **multiple network connections**, but the network connections **don't interact** with each other

## Victim Machines

- ✓ Victim machines allow any user to **login**
- ✓ They are useful in testing new applications whose security flaws are not yet known and to run services which are not secure

## External Services Hosts

- ✓ Bastion hosts are visible to everyone, which makes them vulnerable to attack
- ✓ They require only **minimum access privileges** to the internal network, providing only a few services

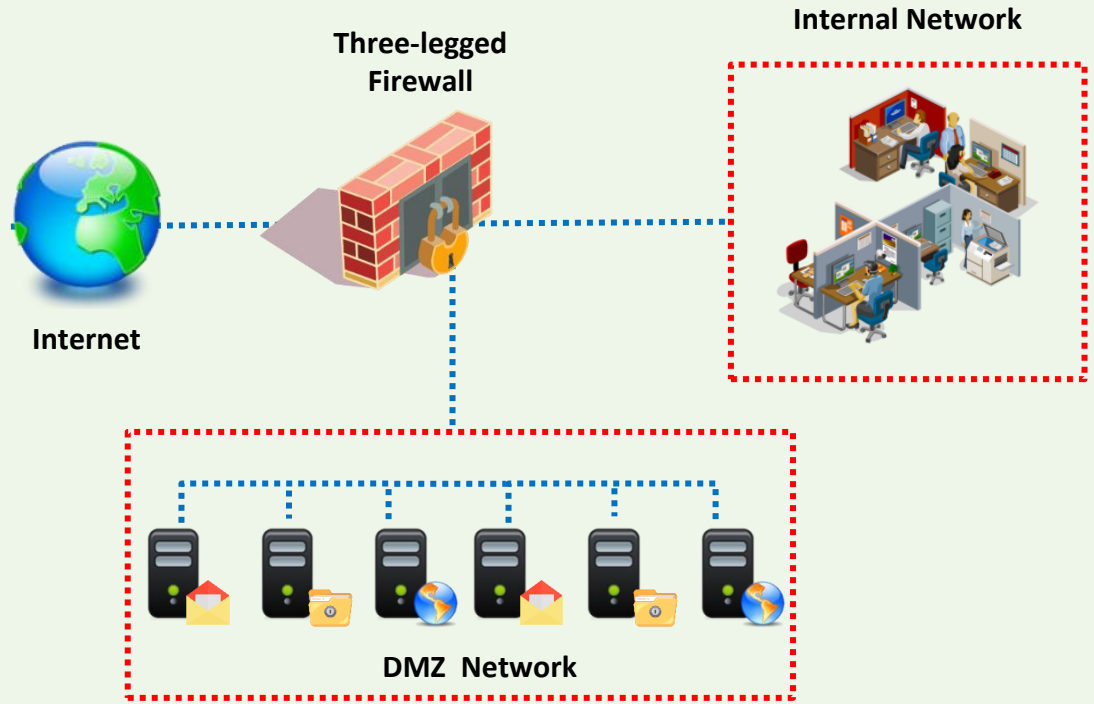
## One-box Firewalls

- ✓ If a machine is constructed as a firewall, it is prone to more **attacks**
- ✓ The entire site's security relies on this single machine, so it is necessary to guarantee that this machine is absolutely secure

# What is Demilitarized Zone (DMZ)?

- A computer subnetwork is placed between the organization's private network such as a **LAN**, and an outside public network such as the **Internet**, and acts as an additional security layer

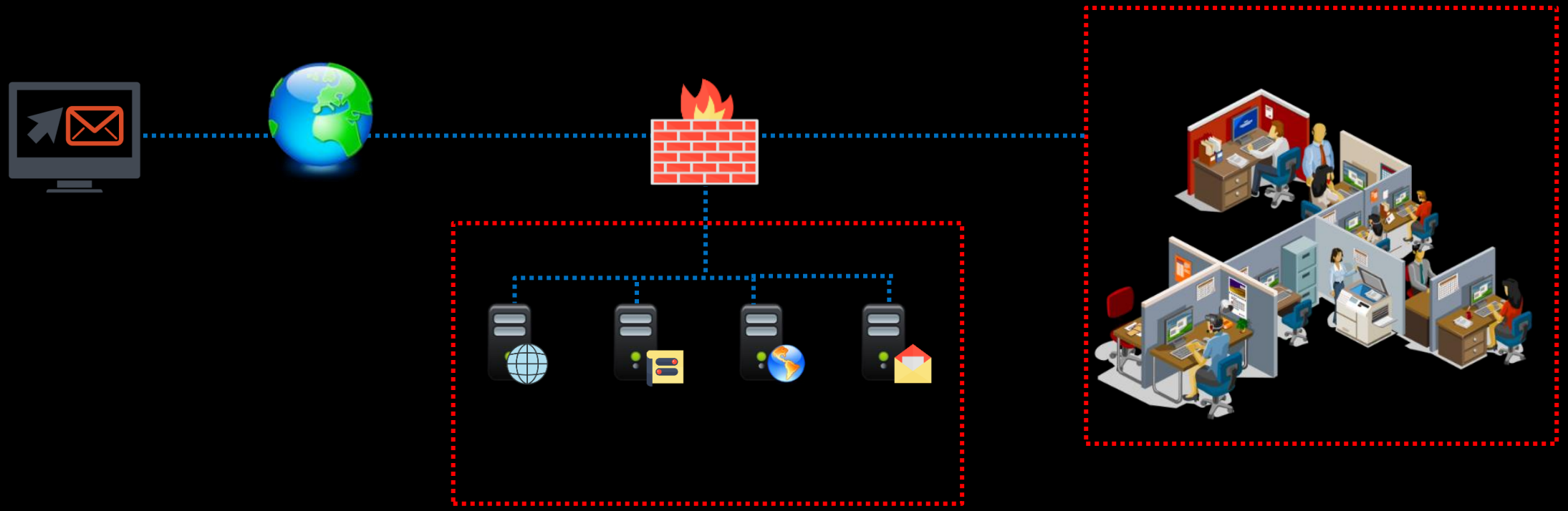
- Contains the servers that need to be accessed from an outside network
  - Web servers
  - Email servers
  - DNS servers
- DMZ configurations
  - Both **internal** and **external** networks can connect to the DMZ
  - **Hosts** in the DMZ can connect to external networks
  - But hosts in the DMZ can not connect to internal networks



# Different Ways to Create a DMZ

## Single Firewall DMZ

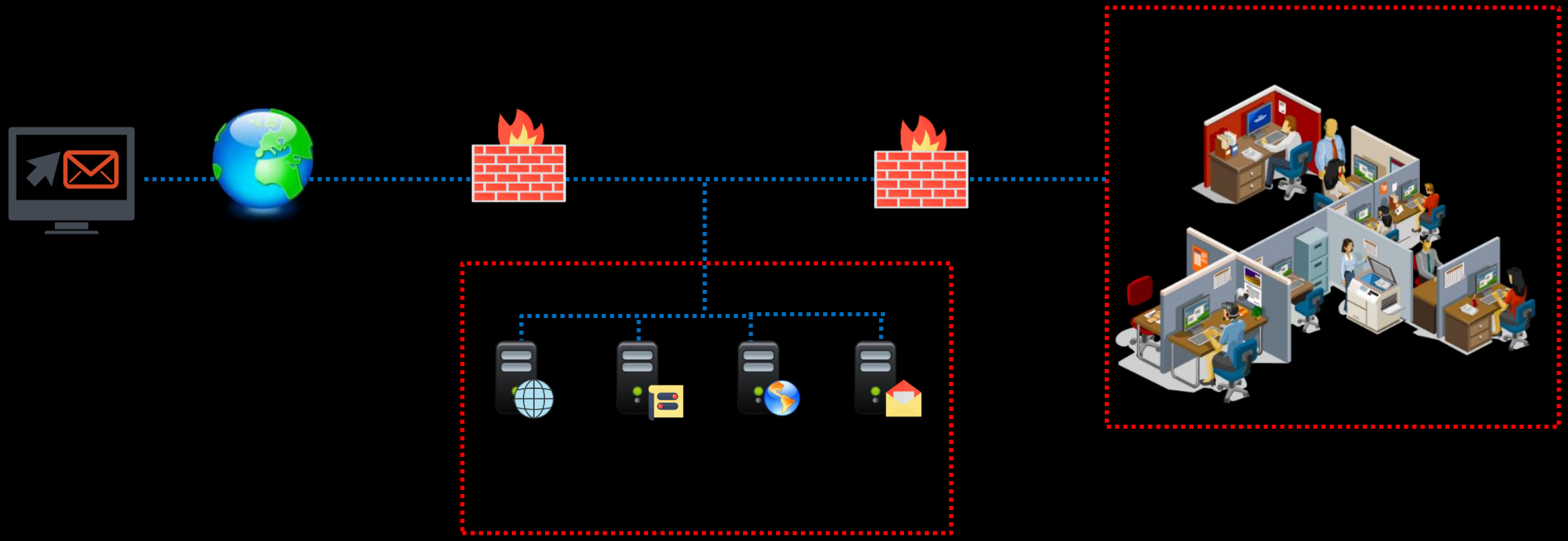
- In this model, the network architecture containing the DMZ consists of **three network interfaces**
- The first network interface connects the **ISP to the firewall**, forming the external network, whereas the second interface forms the **internal network**
- The third interface forms the **DMZ**



# Different Ways to Create a DMZ (Cont'd)

**Dual Firewall DMZ**

- This approach uses **two firewalls** to create a DMZ
- The first firewall allows only **sanitized traffic** to enter the DMZ, whereas the second firewall conducts a double check on it
- It is the most **secure approach** in implementing a DMZ



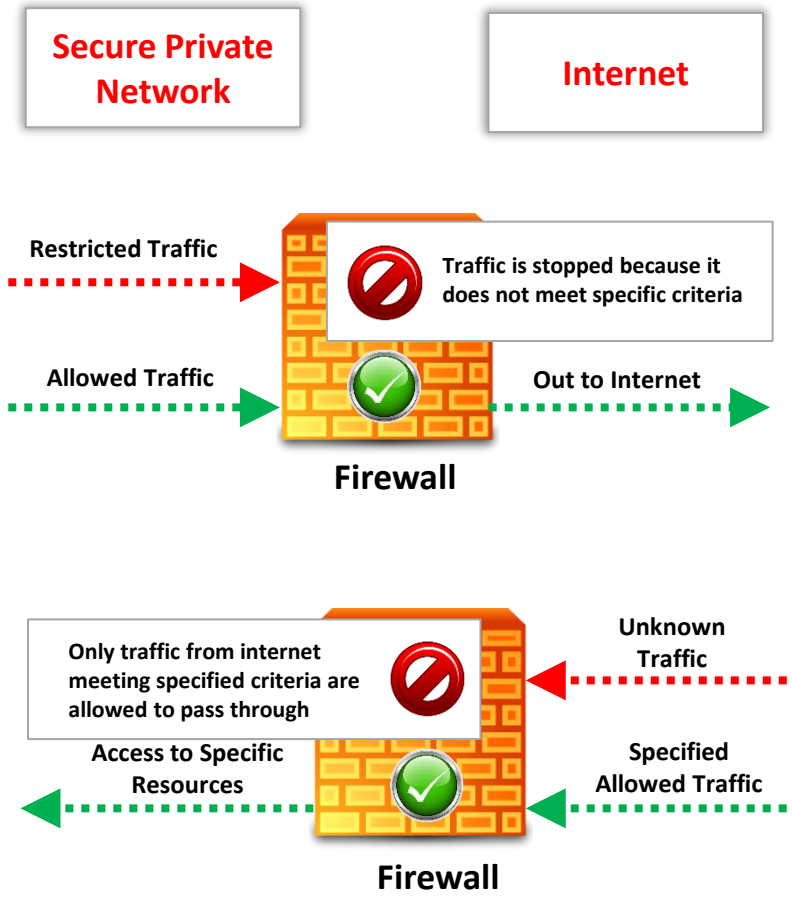
# Module Flow

1. Understand Different Types of Network Segmentation
2. **Understand Different Types of Firewalls and their Role**
3. Understand Different Types of IDS/IPS and their Role
4. Understand Different Types of Honeypots
5. Understand Different Types of Proxy Servers and their Benefits
6. Discuss Fundamentals of VPN and its importance in Network Security
7. Discuss Security Incident and Event Management (SIEM)
8. Discuss User Behavior Analytics (UBA)
9. Understand Various Antivirus/Anti-malware Software



# What is a Firewall?

- Firewall is a software or hardware, or a combination of both, **which is generally used to separate a protected network from an unprotected public network**
- It monitors and filters the incoming and outgoing **traffic** of the network and prevents unauthorized access to private networks

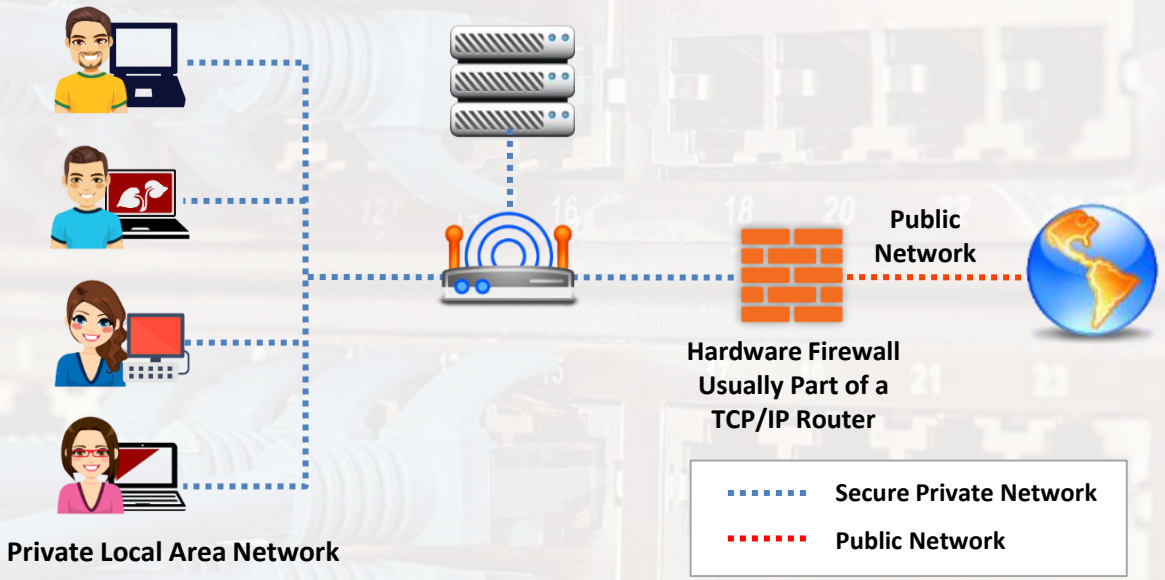


# Types of Firewalls: Hardware Firewalls

**01** A hardware firewall is either a dedicated **stand-alone hardware device** or it comes as part of a router

**02** The network traffic is filtered using the **packet filtering** technique

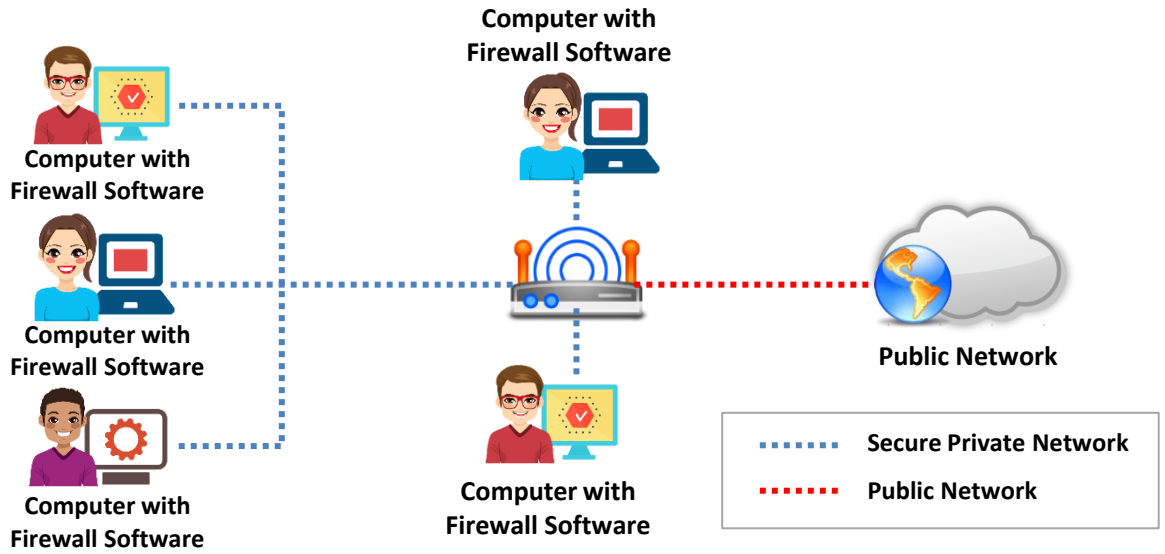
**03** It is used to **filter out** the network traffic for large business networks






# Types of Firewalls: Software Firewalls

- A software firewall is a **software program** installed on a computer, just like normal software
- It is generally used to **filter traffic** for individual home users
- It only filters traffic for the computer on which it is **installed**, not for the entire network




**Note**: It is recommended that you configure both a software and a hardware firewall for best protection

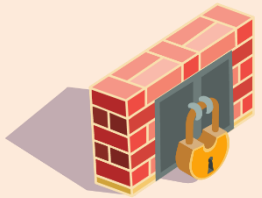
# Types of Firewalls: Host-based and Network-based Firewalls

## Host-based Firewalls

- The host-based firewall is used to filter inbound/outbound traffic of an **individual computer** on which it is installed
- It is a **software-based** firewall
- This firewall software comes as part of OS
- **Example**: Windows Firewall, Iptables, UFW etc.

## Network-based Firewalls

- The network-based firewall is used to filter inbound/outbound traffic from **Internal LAN**
- It is a **hardware-based** firewall
- **Example**: pfSense, Smoothwall, Cisco SonicWall, Netgear, ProSafe, D-Link, etc.

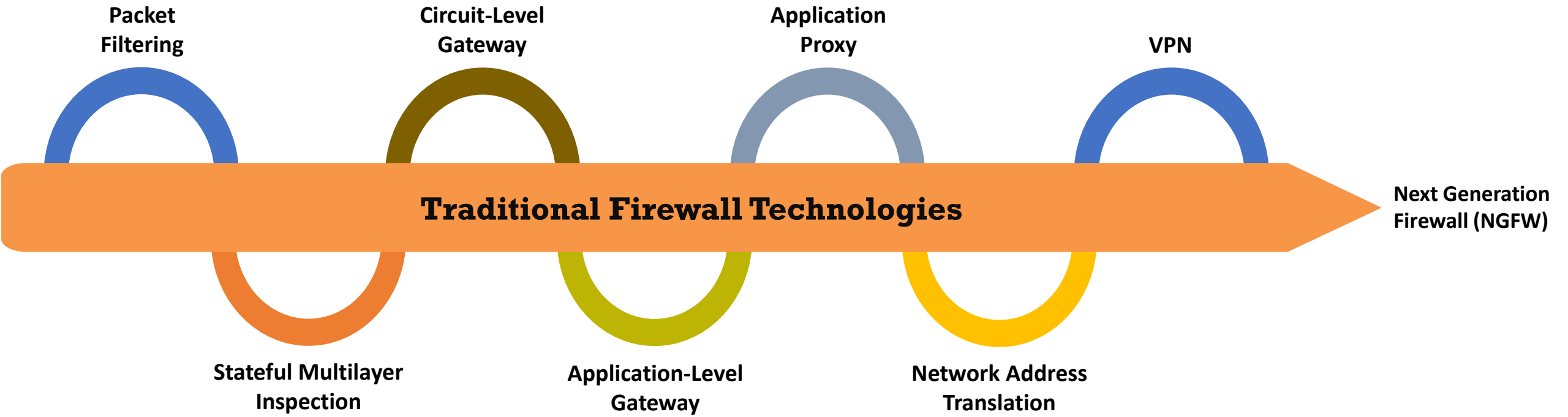


**Note**: It is recommended to configure both a host and network-based firewall for best protection

# Firewall Technologies

- Firewalls are designed and developed with the help of different **firewall services**
- Each firewall service provides security depending on their **efficiency** and **sophistication**





# Firewall Technologies (Cont'd)

## Firewall technologies operating at each OSI layer

| OSI Layer | Firewall Technology |
|---|---|
| Application | ✓ Virtual Private Network (VPN)<br>✓ Application Proxies |
| Presentation | ✓ Virtual Private Network (VPN) |
| Session | ✓ Virtual Private Network (VPN)<br>✓ Circuit-Level Gateways |
| Transport | ✓ Virtual Private Network (VPN)<br>✓ Packet Filtering |
| Network | ✓ Virtual Private Network (VPN)<br>✓ Network Address Translation (NAT)<br>✓ Packet Filtering<br>✓ Stateful Multilayer Inspection |
| Data Link | ✓ Virtual Private Network (VPN)<br>✓ Packet Filtering |
| Physical | ✓ Not Applicable |

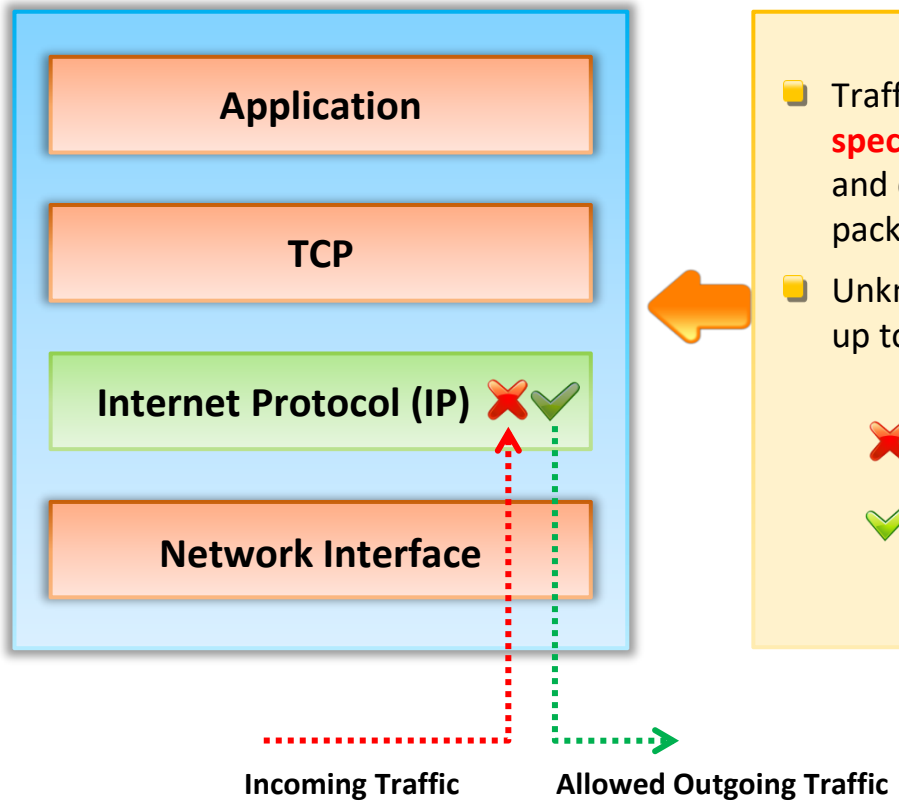


# Packet Filtering Firewall

Packet filtering firewalls work at the network level of the **OSI model** (or the IP layer of TCP/IP)

They are usually part of a **router**. Most routers support **packet filtering**

In a packet filtering firewall, each packet is compared to a **set of criteria** before it is forwarded




- Traffic is filtered based on **specified rules**, including source and destination IP address, packet type, and port number
- Unknown traffic is only allowed up to **level 2 of the network stack**

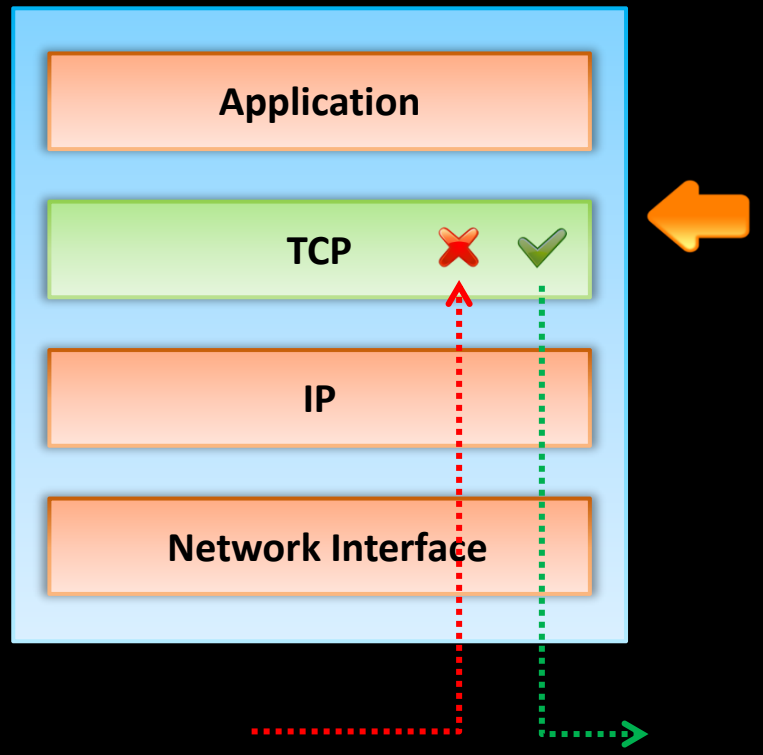
**Disallowed**

**Allowed**



# Circuit-Level Gateway

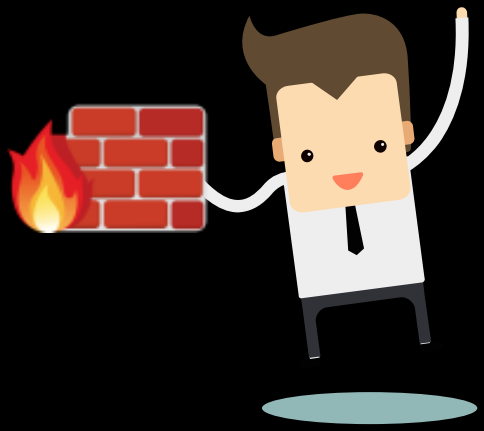
- Circuit level gateways work at the **session layer** of the OSI model, or the TCP layer of TCP/IP
- They monitor the TCP handshake between packets to determine whether a requested session is **legitimate or not**
- Information passed to a remote computer through a circuit-level gateway appears to have originated from the **gateway**




- Traffic is filtered based on **specified session rules**, such as when a session is initiated by a recognized computer
- Unknown traffic is only allowed up to **level 3 of the network stack**

**Disallowed**

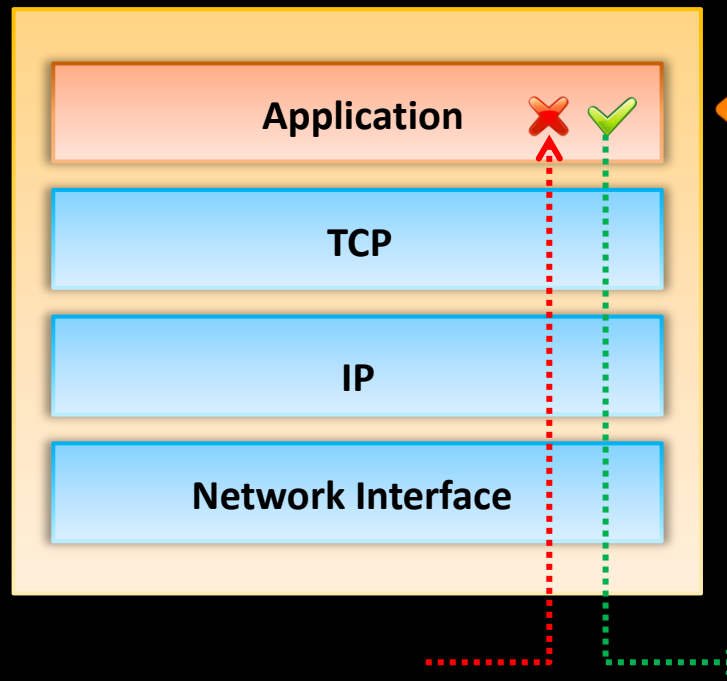
**Allowed**



# Application Level Gateways

- Application level gateways can filter packets at the applicati
- Because they examine packets at the application layer, they commands such as **http:post** and **get**
- In plain terms, an application level gateways can be configu will not allow any **FTP**, **gopher**, **Telnet**, or other traffic throu

**OSI model**




- Traffic is filtered based on specified application rules, applications (e.g. browser) and/or a protocol (e.g. FTP) or a combination of all of these
- Unknown traffic is only allowed up to the top of the network stack

**Disallowed**

**Allowed**

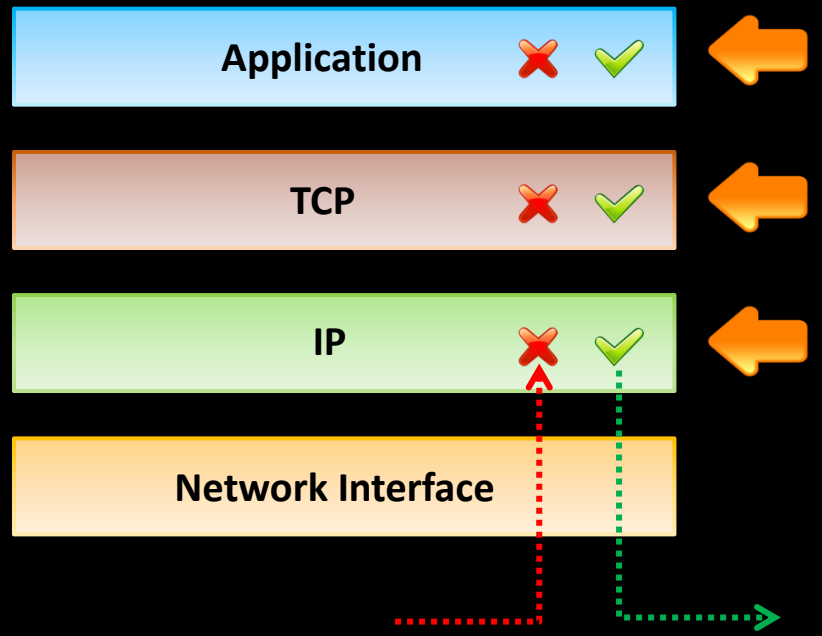


# Stateful Multilayer Inspection Firewall

A stateful multilayer inspection firewall **combines the aspects** of the other three types

They filter packets at the network layer, determine whether **session packets** are **legitimate** and evaluate the contents of packets at the **application layer**

They are **expensive** and require competent personnel to administer the device




Traffic is filtered at **three levels**, based on a wide range of specified application, session, and packet filtering rules

Unknown traffic is allowed up to **level 2 of the network stack**

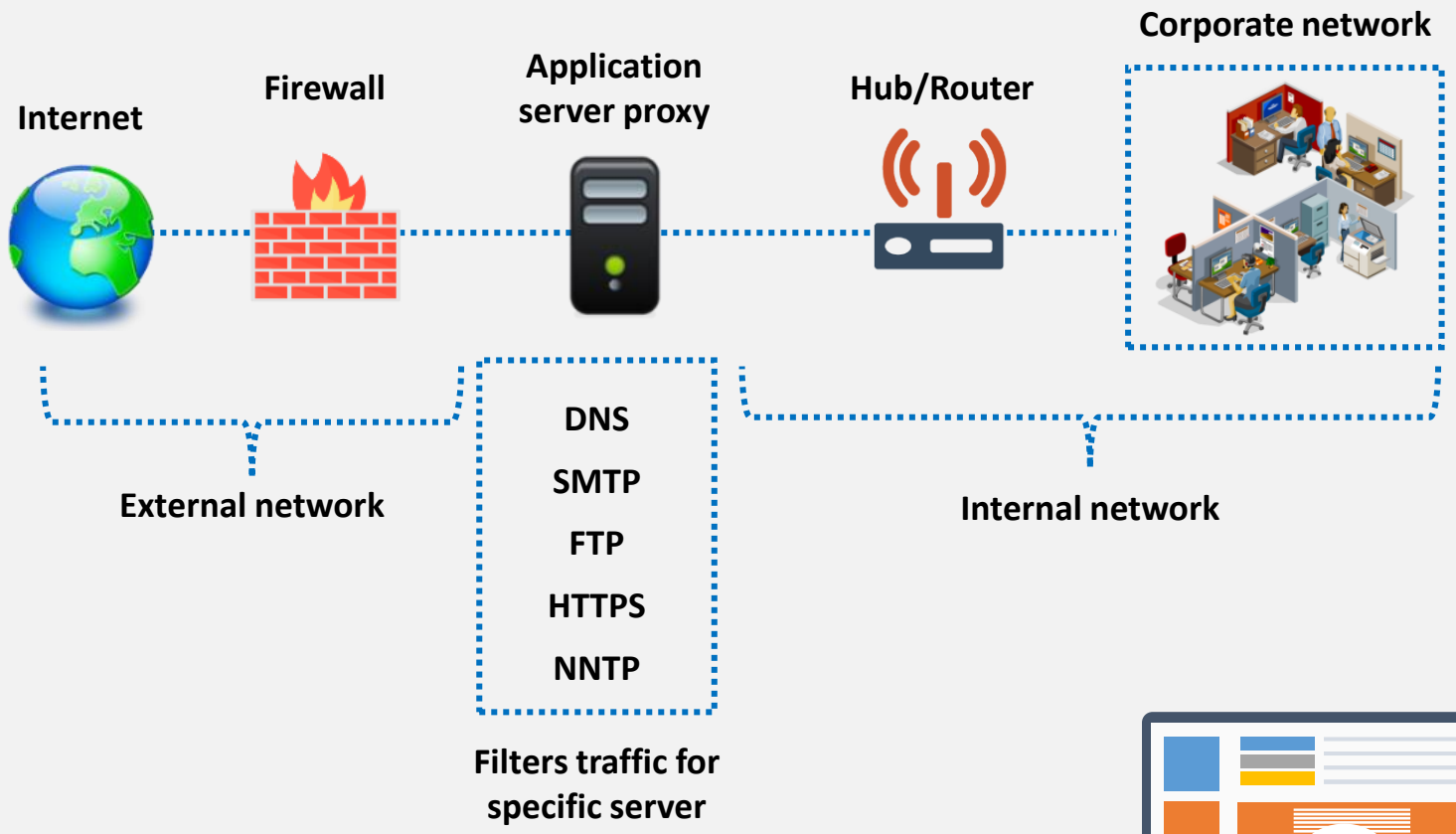
Disallowed

Allowed



# Application Proxy

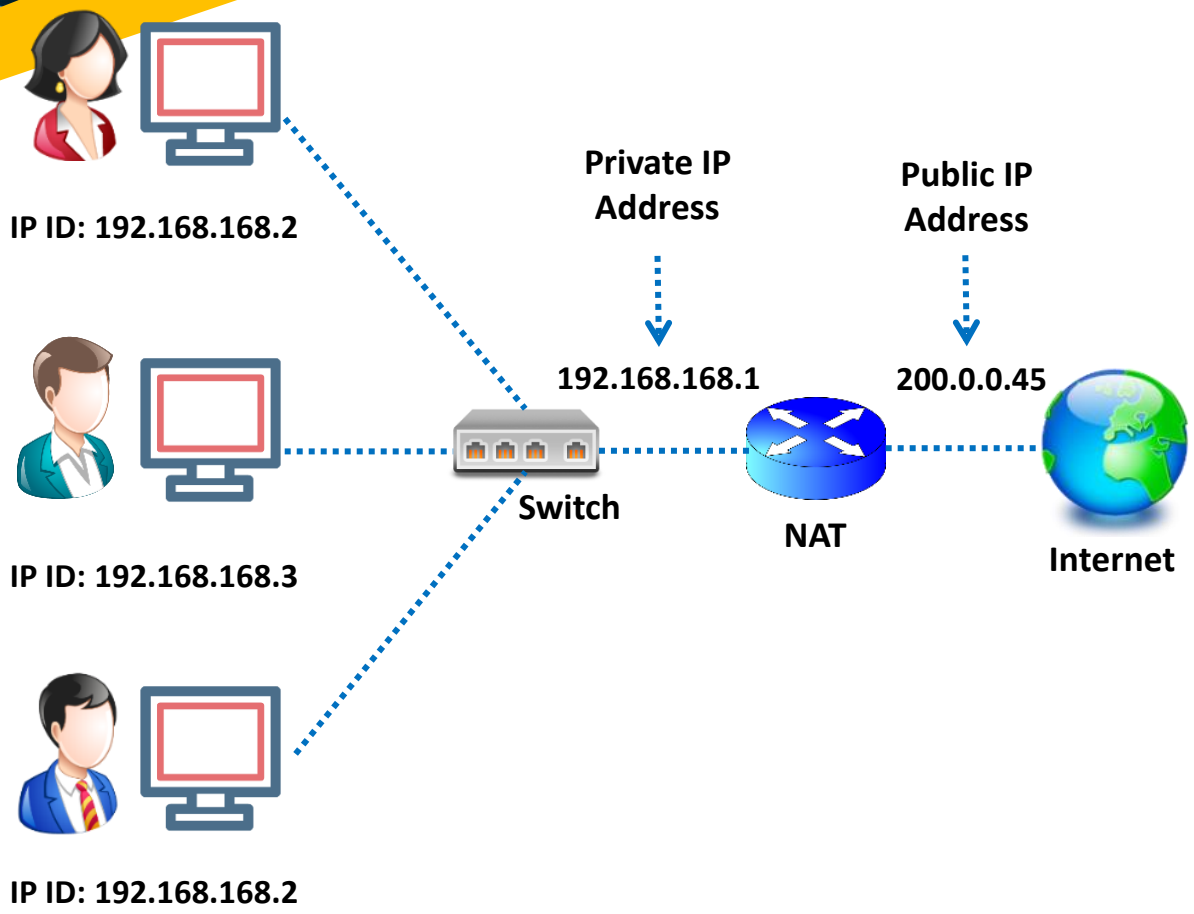
- An application-level proxy works as a proxy server and **filters connections** for specific services
- It filters connections based on the **services** and **protocols**
- **For example**, an FTP proxy will only allow FTP traffic to pass through, while all other services and protocols will be blocked





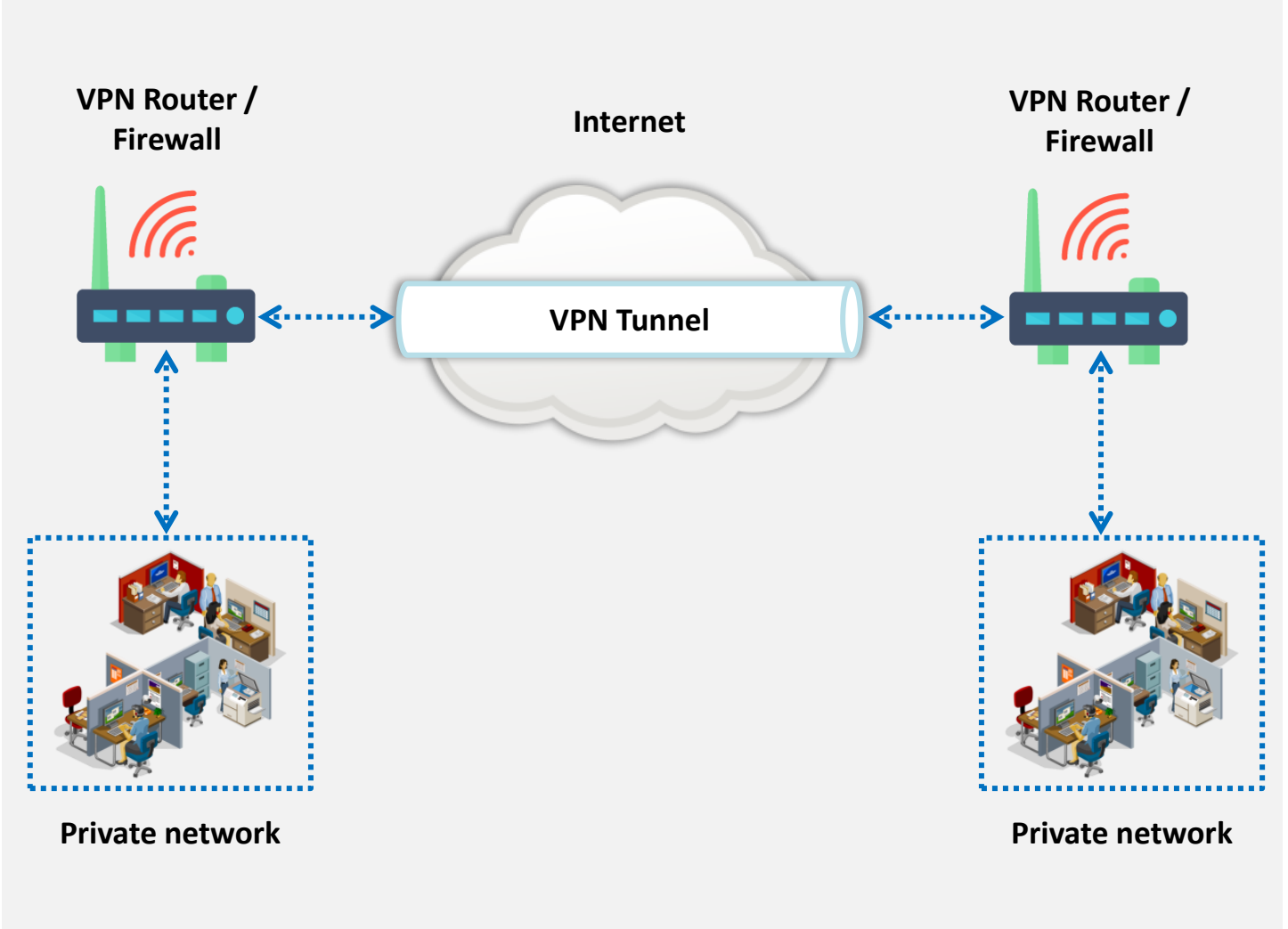

# Network Address Translation (NAT)

- Network address translation separates IP addresses into two sets and enables the LAN to use these addresses for **internal** and **external traffic** respectively
- It also works with a router, the same as packet filtering does; NAT will also **modify** the packets the router sends at the same time
- It has the ability to **change** the **address** of the packet and make it appear to have arrived from a valid address
- It limits the number of **public IP addresses** an organization can use



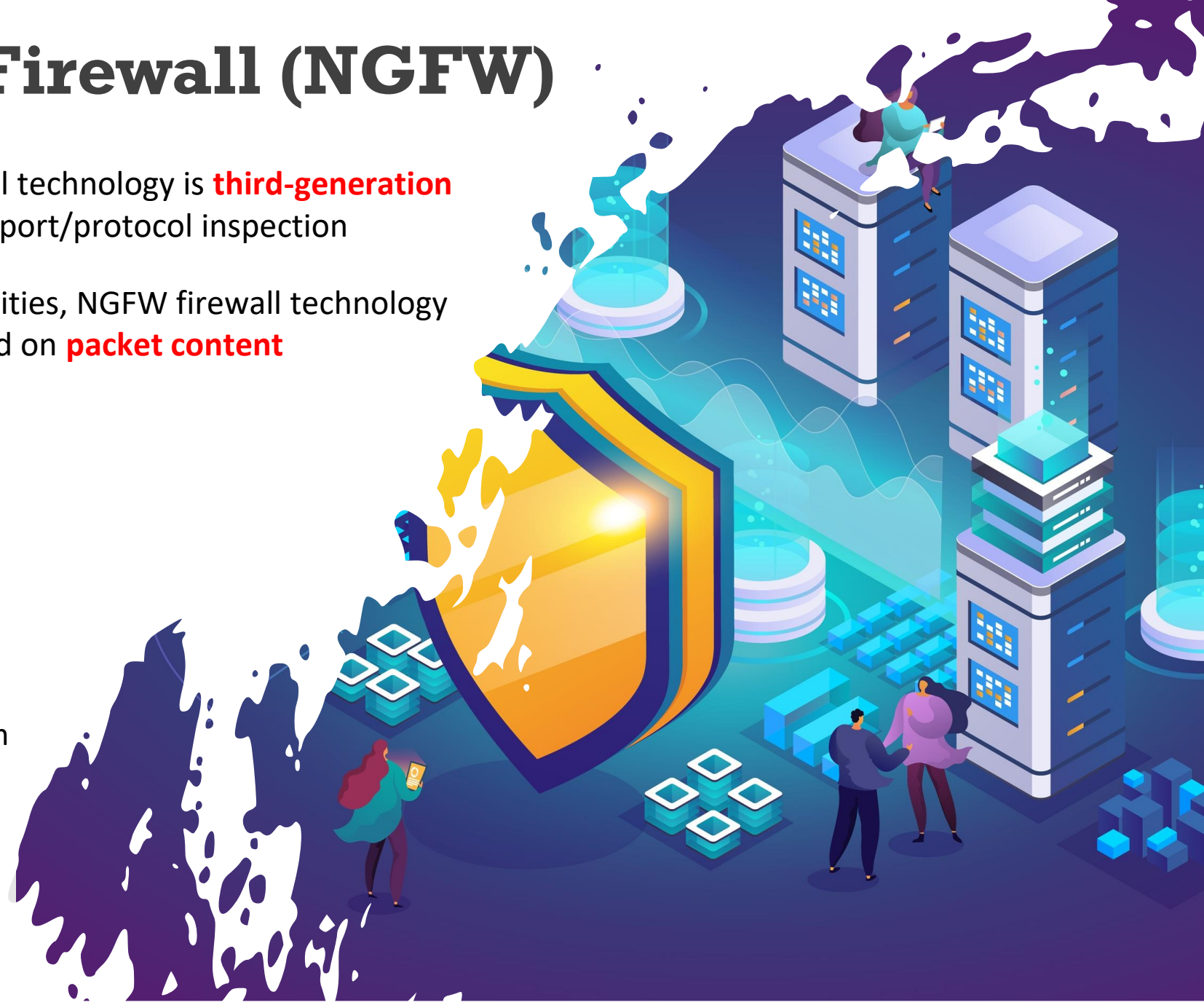
# Virtual Private Network

- A VPN is a **private network** constructed using public networks, such as the Internet
- It is used for the **secure transmission** of sensitive information over an untrusted network, using **encapsulation** and encryption
- It establishes a virtual point-to-point connection through the use of **dedicated connections**
- The **computing device** running the VPN software can only access the VPN



# Next Generation Firewall (NGFW)

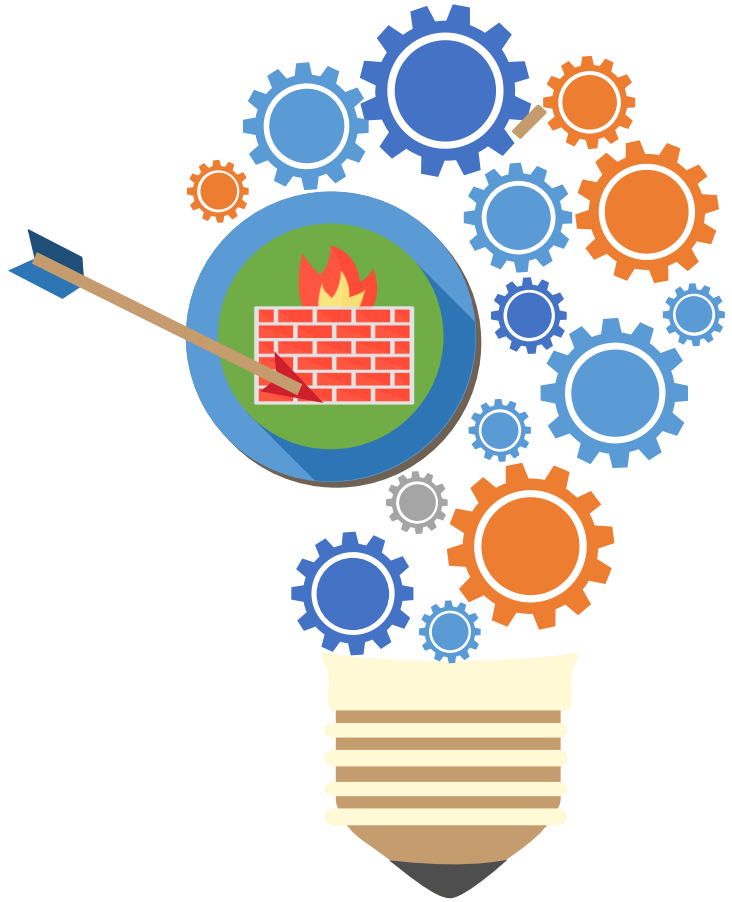
- Next generation firewall (NGFW) firewall technology is **third-generation firewall technology** that moves beyond port/protocol inspection
- In addition to traditional firewall capabilities, NGFW firewall technology has the capability to inspect traffic based on **packet content**
- Typical NGFW capabilities:
  - ✓ Deep packet inspection (DPI)
  - ✓ Encrypted traffic inspection
  - ✓ QoS/bandwidth management
  - ✓ Threat intelligence integration
  - ✓ Integrated intrusion prevention system
  - ✓ Advanced threat protection
  - ✓ Application control
  - ✓ Antivirus inspection



# Firewall Capabilities



- Prevent network scanning
- Controls traffic
- Performs user authentication
- Filters packets, services, and protocols
- Performs traffic logging
- Performs network address Translation (NAT)
- Prevents malware attacks



# Firewall Limitations

1

A firewall does not prevent the network from **backdoor attacks**

2

A firewall does not protect the network from **insider attacks**

3

A firewall cannot do anything if the network design and **configuration** is **faulty**

4

A firewall is not an alternative to **antivirus** or **antimalware**

5

A firewall does not prevent **new viruses**

6

A firewall cannot prevent **social engineering threats**

7

A firewall does not prevent **passwords misuse**

8

A firewall does not block attacks from a higher level of the **protocol stack**

# Firewall Implementation and Deployment Process

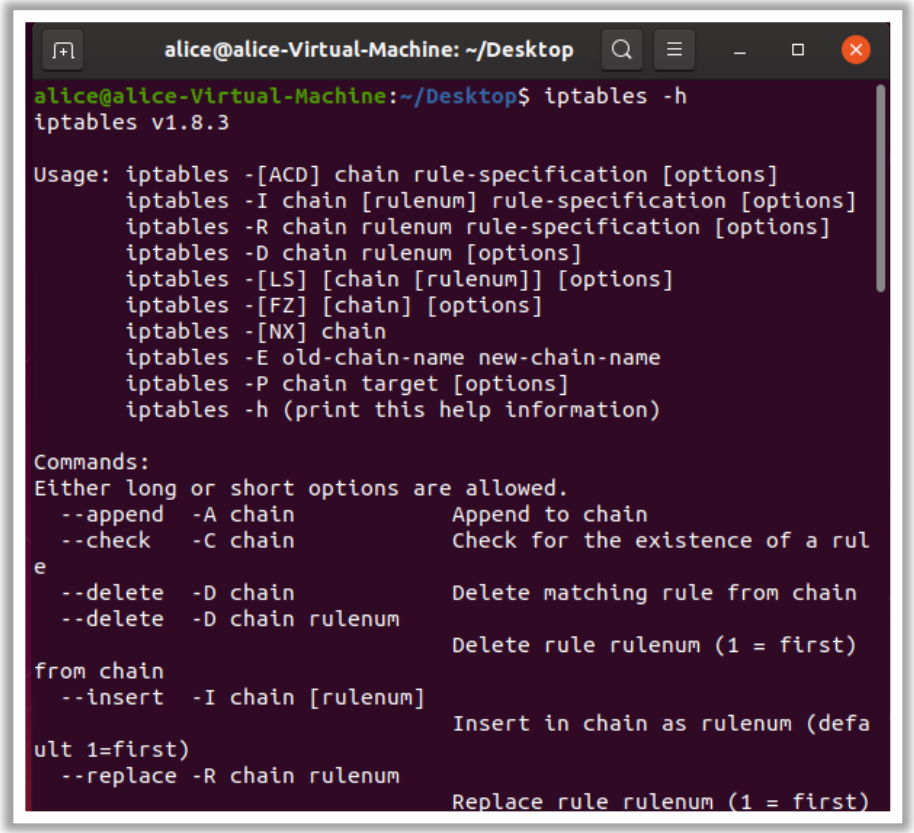
- Use a step-by-step process to ensure a **successful** firewall implementation and deployment
- The process helps to minimize any unforeseen **issues** and identify any potential **pitfalls** early on

## Firewall Implementation and Deployment Process

| | |
|---|---|
| **Planning** | When implementing a firewall for the network, organizations must **plan their positioning** in advance |
| **Configuring** | Involves configuring various components and features such as hardware, software, **policy configuration**, implementing **logging**, and **alerting** mechanisms |
| **Testing** | Mainly focuses on whether the **firewall rules** are set according to the actions performed by the firewall |
| **Deploying** | A phased approach to deploy multiple firewalls on a network helps detect and **resolve issues** regarding conflicting policies |
| **Managing and Maintaining** | Includes maintaining the **firewall architecture**, **policies**, software, and other components deployed on the network |

# Host-based Firewall Protection with Iptables

- Iptables is a **built-in firewall utility** for Linux OSes
- Iptables comes pre-installed on any Linux distribution. However, you can update/install it with `sudo apt-get install iptables` command




| Task | Iptable Commands |
|---|---|
| Filtering non TCP packets | iptables -A INPUT -p tcp ! --syn -m state --state NEW -j DROP |
| Blocking XMAS scan Attack | iptables -A INPUT -p tcp --tcp-flags ALL -j DROP |
| Drop any NULL packets | iptables -A INPUT -f -j DROP |
| Drop any fragmented packets | iptables -A INPUT -f -j DROP |

# Host-based Firewall Protection with Iptables (Cont'd)

Existing rules can be checked using **`sudo iptables -L -n -v`** command



```
root@alice-Virtual-Machine: /home/alice
root@alice-Virtual-Machine:/home/alice# iptables -L -n -v
Chain INPUT (policy ACCEPT 97 packets, 7270 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       all  --  *      eth0    0.0.0.0/0            0.0.0.0/0
    owner UID match 1001
root@alice-Virtual-Machine:/home/alice#
```

Specific IP address can be block using **`Iptables Firewall`**

**`iptables -A INUPT -s 10.10.10.55 -j DROP`**

```
root@alice-Virtual-Machine: /home/alice
root@alice-Virtual-Machine:/home/alice# iptables -A INPUT -s 10.10.10.55 -j DROP
root@alice-Virtual-Machine:/home/alice#
```

# Secure Firewall Implementation: Best Practices

- Filter unused and common **vulnerable** ports
- If possible, create a **unique user ID** to run the firewall services. Rather than running the services using the administrator or root IDs
- Set the firewall ruleset to deny all traffic and enable only the services required
- Change all the **default passwords** and create a strong password that is not found in any dictionary. A strong password to ensure brute-force attacks also fail.
- To enhance the **performance** of the firewall, limit the applications that are running
- Configure a **remote syslog server** and apply strict measures to protect it from malicious users
- Monitor **firewall logs** at regular intervals. Include them in your data retention policy
- Immediately investigate all **suspicious log** entries found

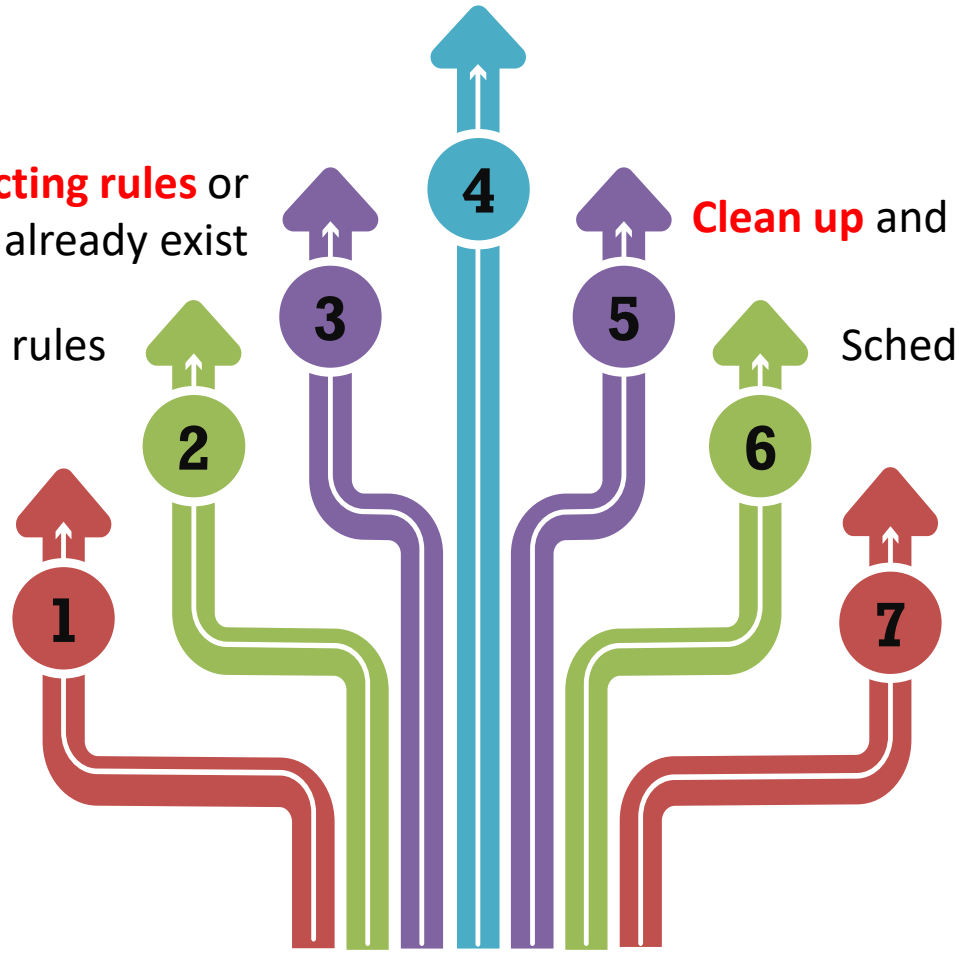
# Secure Firewall Implementation: Recommendations

Use a standard **method** and **workflow** for requesting and implementing firewall changes

Do not set **conflicting rules** or eliminate them, if they already exist

**Remove** unused or outdated rules

Notify the **security policy administrator** on firewall changes and document them




**Clean up** and **optimize** the firewall rule base

Schedule regular **firewall security audits**

Keep a **log** of the firewall rules and configuration changes

# Secure Firewall Implementation: Do’s and Don’ts

01 Implement a strong firewall

02 Limit the applications that run on a firewall

03 Control physical access to the firewall

04 Evaluate firewall capabilities

05 Consider workflow integration

06 Don't overlook scalability

07 Don't rely on packet filtering alone

08 Don’t be unsympathetic to hardware needs

09 Don’t cut back on additional security

10 Don't implement without SSL encryption

# Module Flow

1. Understand Different Types of Network Segmentation
2. Understand Different Types of Firewalls and their Role
3. **Understand Different Types of IDS/IPS and their Role**
4. Understand Different Types of Honeypots
5. Understand Different Types of Proxy Servers and their Benefits
6. Discuss Fundamentals of VPN and its importance in Network Security
7. Discuss Security Incident and Event Management (SIEM)
8. Discuss User Behavior Analytics (UBA)
9. Understand Various Antivirus/Anti-malware Software

# Intrusion Detection and Prevention System (IDS/IPS)

## 01

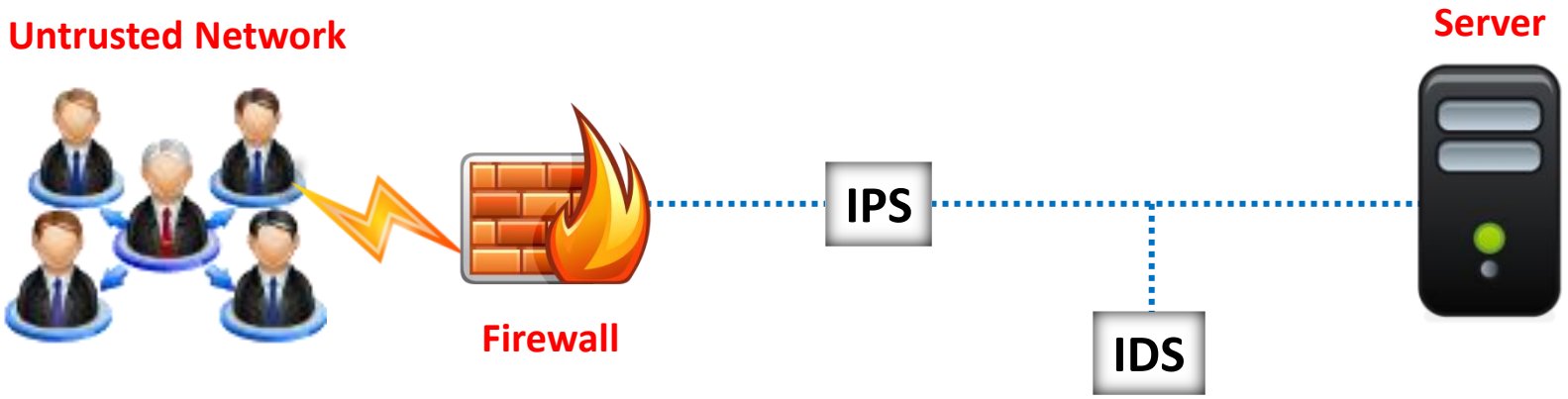
An intrusion detection and prevention system (IDS/IPS) is a network security appliance that **inspects all inbound and outbound network traffic** for suspicious patterns that might indicate a network or system security breach

## 02

If found, the IDS will alert the administrator about the **suspicious activities**

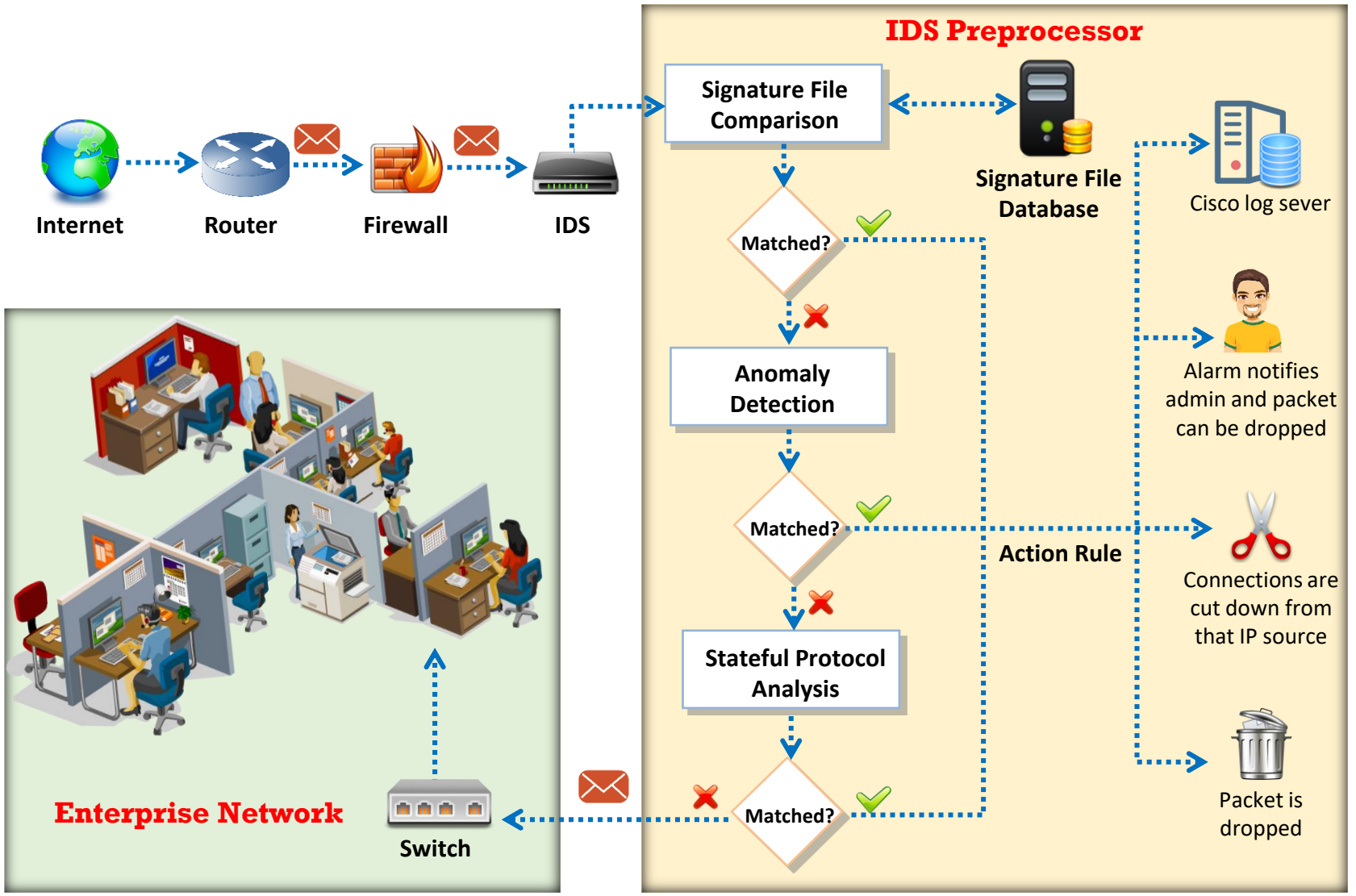
## 03

IDS checks the network traffic for **signatures** that match known intrusion patterns and triggers an alarm when a match is found






# How does an IDS Work?



# Role of an IDS in Network Defense






- An IDS works from inside the network, unlike a firewall which only looks **outside** the network for intrusions
- An IDS is placed behind the firewall, inspecting all the traffic, looking for **heuristics** and a **pattern** match for intrusions

# How an IDS Detects an Intrusion?

## Signature Recognition

Signature recognition, also known as misuse detection, tries to **identify events** that indicate an abuse of a system or network resource



## Anomaly Detection

It detects the **intrusion based** on the fixed behavioral characteristics of the users and components in a computer system

## Protocol Anomaly Detection

In this type of detection, models are built to explore **anomalies** in the way in which vendors deploy the **TCP/IP specification**

# IDS Capabilities



- IDS provides an additional layer of security to the network under the **defense-in-depth** principle
- IDS does several things that basic **firewalls** cannot do
- IDS helps minimize the chance of **missing security threats** that could come from firewall evasions

## IDS/IPS Functions

- **Monitoring and analyzing both user and system activities**
- **Analyzing system configurations and vulnerabilities**
- **Assessing system and file integrity**
- **Recognizing typical attack patterns**
- **Analyzing abnormal activity patterns**
- **Tracking user policy violations**



# IDS/IPS Limitations: What an IDS/IPS is NOT?

**IDS/IPS cannot act as or replacement of**

- Network Logging Systems
- Vulnerability Assessment Tools
- Antivirus Products
- Cryptographic Systems

# IDS/IPS Security Concerns



- ❑ Improper IDS/IPS configuration and management will make an IDS/IPS **ineffective**
- ❑ IDS/IPS deployment should be done with careful planning, preparation, prototyping, testing, and specialized training

## Common Mistakes in IDS/IPS Configuration

- ✓ Deploying an IDS in a location where it **does not see** all the network traffic
- ✓ Frequently **ignoring** the **alerts** generated by the IDS
- ✓ Not having the proper **response policy** and the best possible solutions to deal with an event
- ✓ Not fine-tuning the IDS for **false negatives** and **false positives**
- ✓ Not updating the IDS with the **latest new signatures** from the vendor
- ✓ Only monitoring **inbound connections**



# General Indications of Intrusions

## File System Intrusions

- The presence of new or **unfamiliar files**, or programs
- Changes in **file permissions**
- Unexplained changes in a file's **size**
- **Rogue files** on the system that do not correspond to the master list of signed files
- Missing files



## Network Intrusions

- **Repeated probes** of the available services on your machines
- Connections from **unusual locations**
- Repeated login attempts from **remote hosts**
- A sudden **influx of log data**



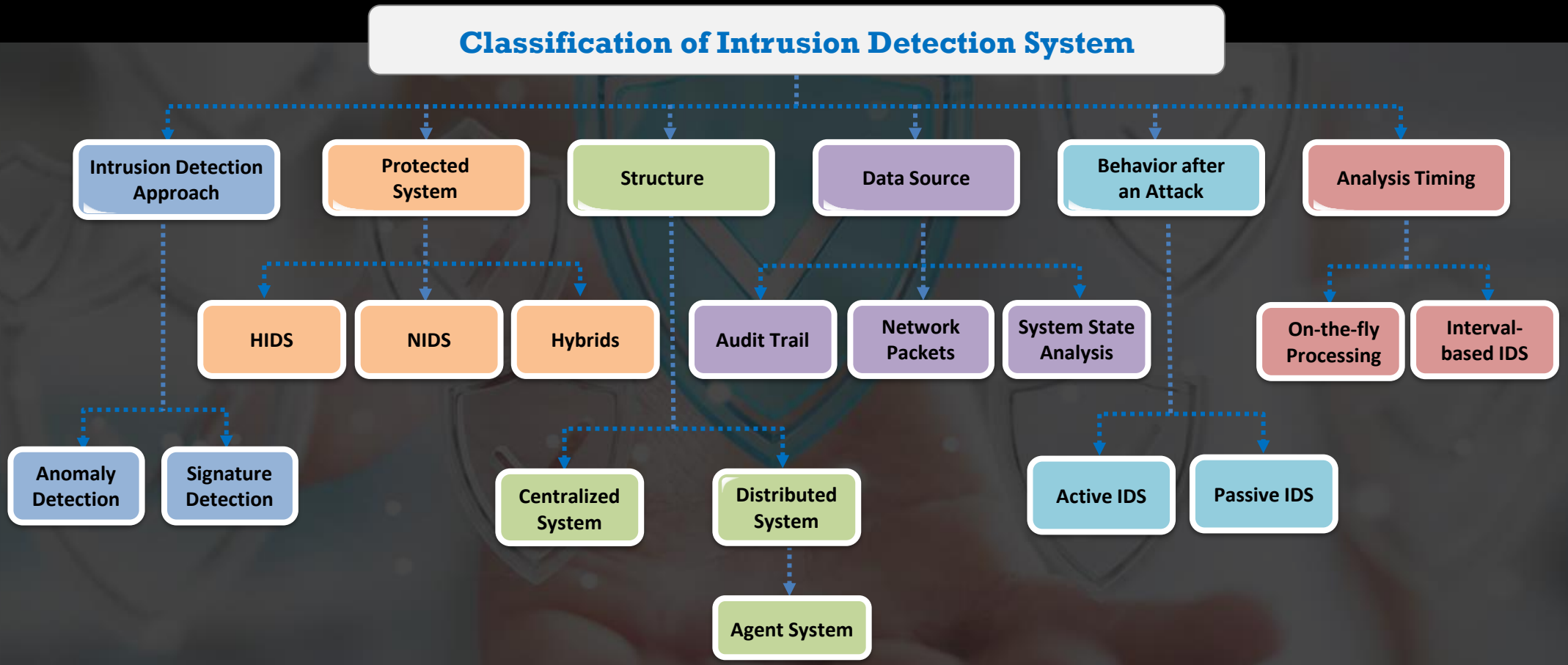
## System Intrusions

- **Short** or incomplete logs
- Unusually **slow** system performance
- **Missing** logs or logs with incorrect permissions or ownership
- **Modifications** to system software and configuration files
- Unusual **graphic displays** or text messages
- **Gaps** in system accounting
- System crashes or **reboots**
- **Unfamiliar** processes

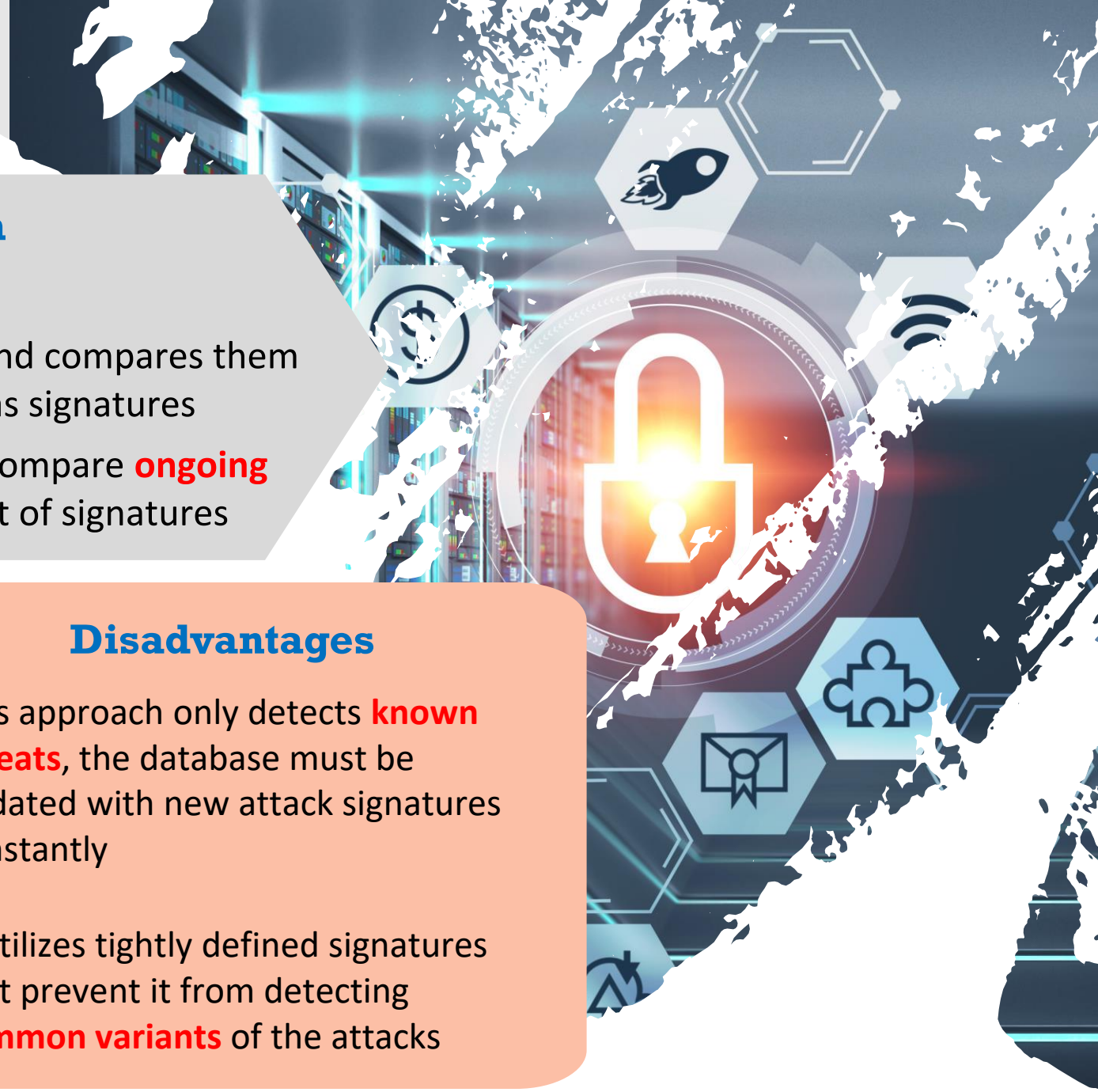
# IDS Classification

classified

Please write your great title is here



# Approach-based IDS



## Signature-Based Detection

- Known as **misuse detection**
- **Monitors** patterns of data packets in the network and compares them to pre-configured network attack patterns, known as signatures
- This method uses string comparison operations to compare **ongoing activity**, such as a packet or a log entry, against a list of signatures

## Advantages

- It detects attacks with minimal false alarms
- It can **quickly** identify the use of a specific tool or technique
- It assists administrators to quickly track any potential **security issues** and initiate incident handling procedures

## Disadvantages

- This approach only detects **known threats**, the database must be updated with new attack signatures constantly
- It utilizes tightly defined signatures that prevent it from detecting **common variants** of the attacks

# Approach-based IDS (Cont'd)

## Anomaly-based Detection

- In this approach, alarms for **anomalous** activities are generated by evaluating network patterns such as what sort of bandwidth is used, what protocols are used, and what ports and which devices are connected to each other
- An IDS monitors the typical activity for a particular time interval and then builds the **statistics** for the network traffic
- For example: anomaly-based IDS monitors activities for normal Internet bandwidth usage, failed logon attempts, processor utilization levels, etc.



### Advantages

- ✓ An anomaly-based IDS identifies **abnormal** behavior in the network and detects the symptoms for attacks without any clear details
- ✓ Information acquired by anomaly detectors is further used to define the signatures for **misuse detectors**



### Disadvantages

- ✓ The rate of generating **false alarms** is high due to unpredictable behavior of users and networks
- ✓ The need to create an **extensive set of system events** in order to characterize normal behavior patterns

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Approach-based IDS (Cont'd)

## Stateful Protocol Analysis



This method **compares** observed events with predetermined profiles based on accepted definitions of benign activity for each protocol to identify any deviations of the protocol state

It also detects variations in command length, minimum/maximum values for **attributes** and other **potential anomalies**

It can identify unpredictable sequences of commands. For example, it can identify activities such as issuing the same commands repeatedly or arbitrary commands being used

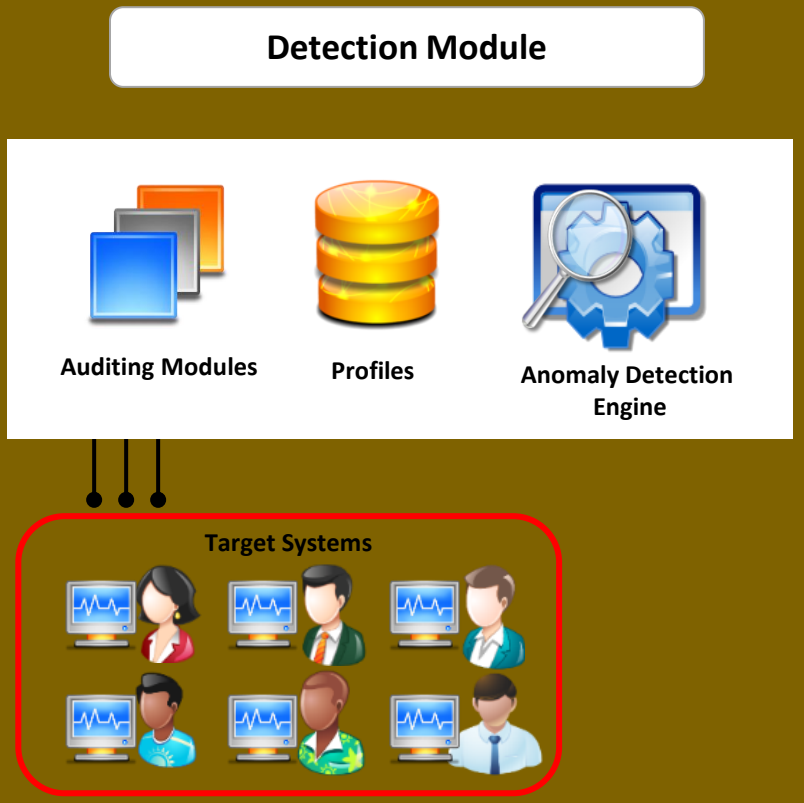
For any protocol performing **authentication**, the IDS/IPS will keep track of the authenticator being used for each session and will record the authenticator involved in the suspicious activity

# Anomaly and Misuse Detection Systems

## Misuse Detection System




## Anomaly Detection System



# Behavior-based IDS

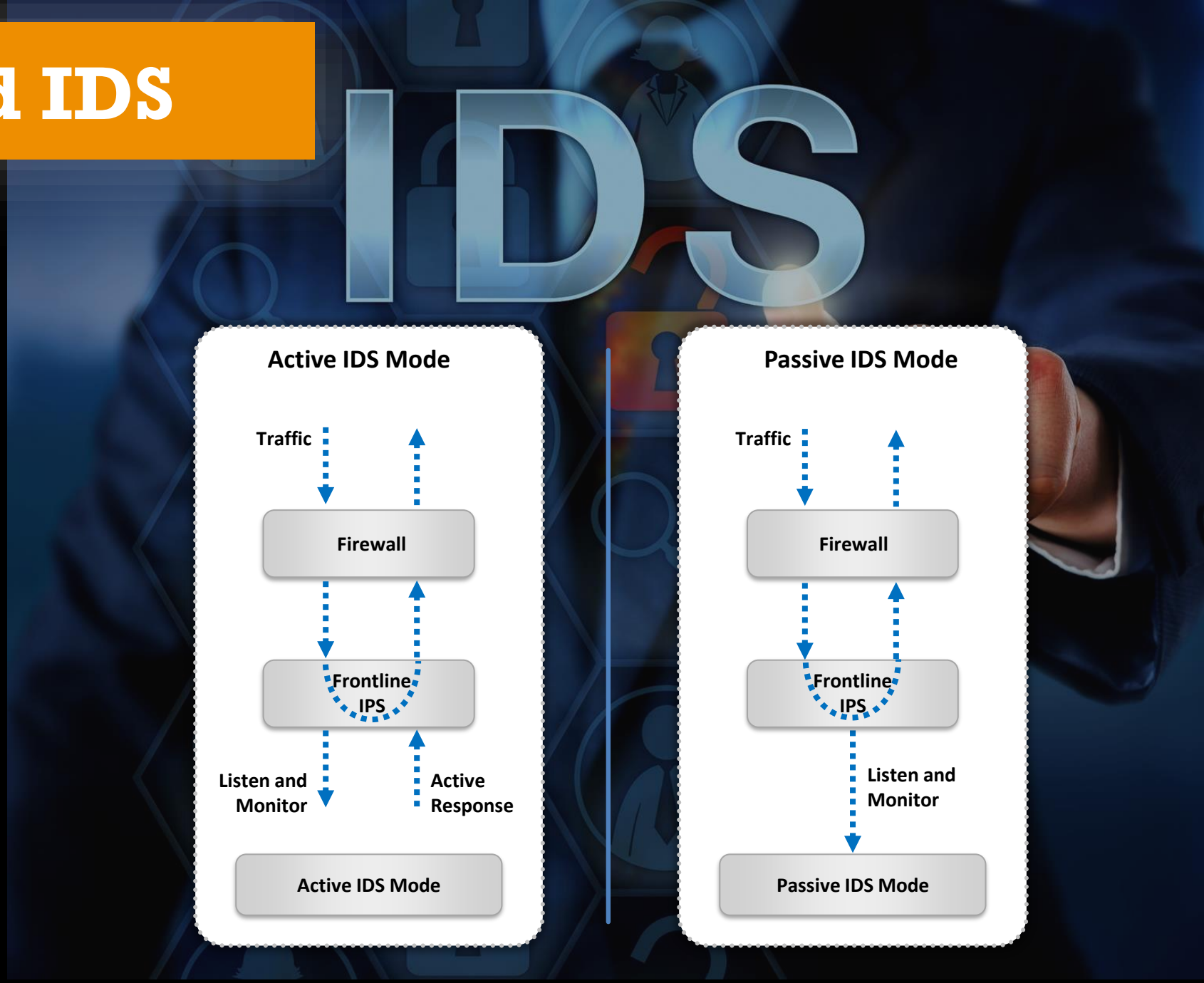
potential

intrusion

Detects

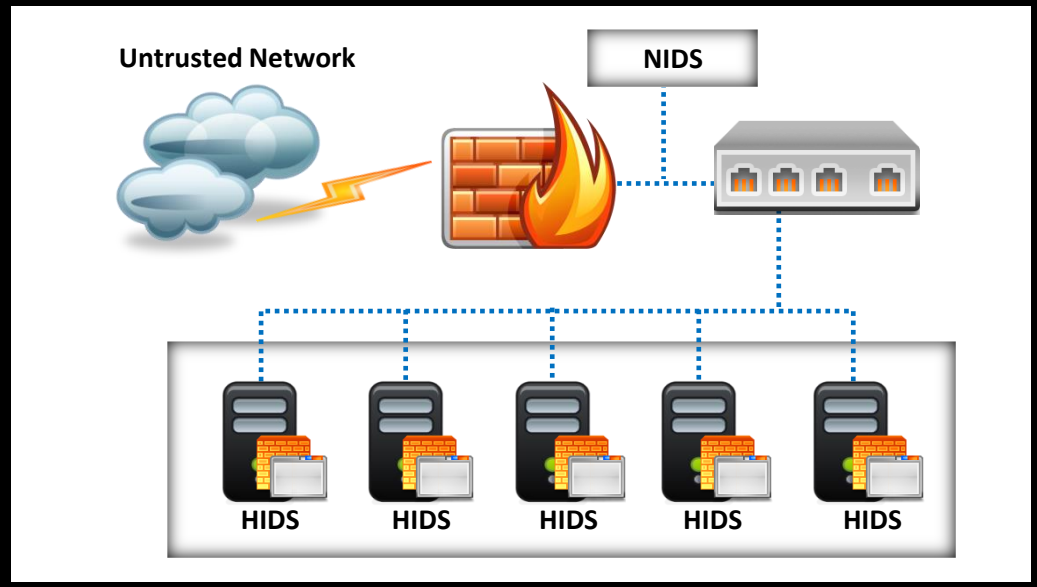
responds

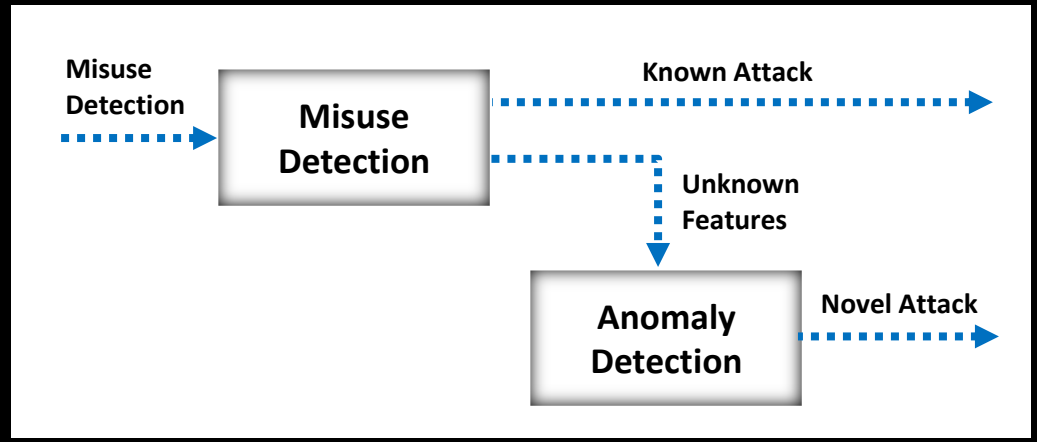
Only detects



# Protection-based IDS

- protection
  - NIDS
  - HIDS
  - Hybrid IDS
- low false-positive rate



# Structure-based IDS



centralized IDS

distributed IDS

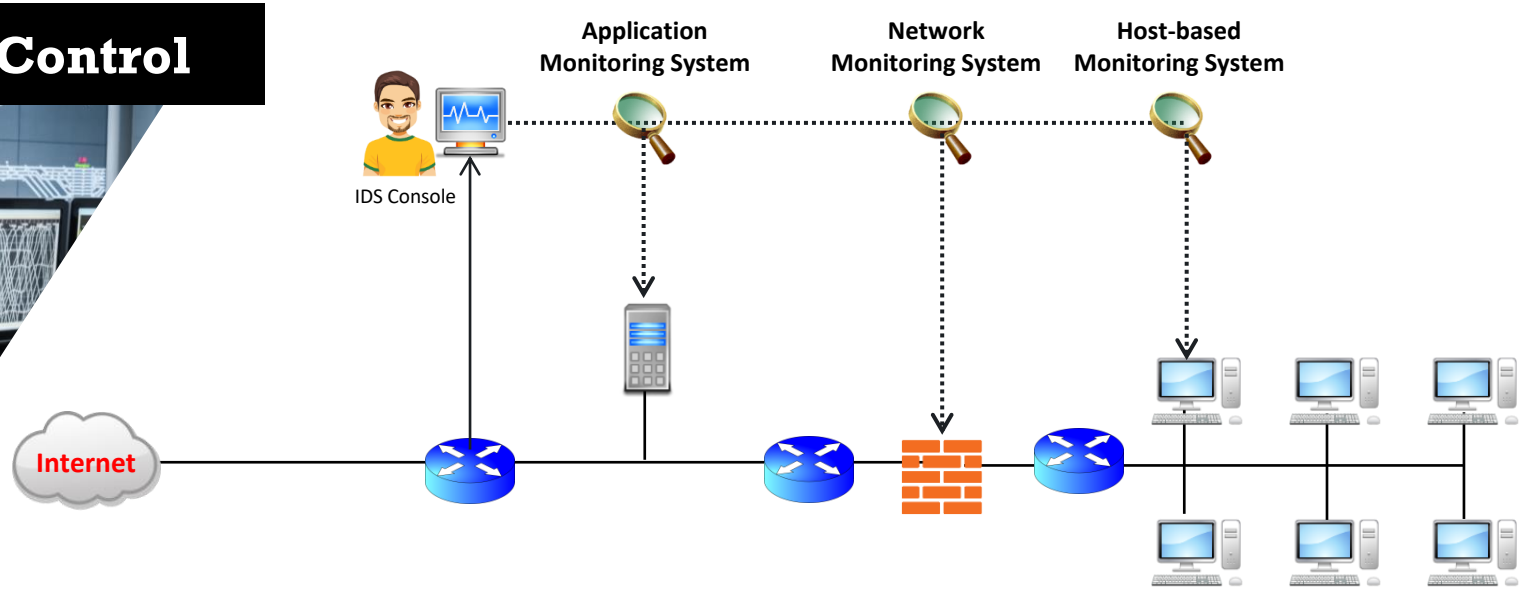
central location

several IDS

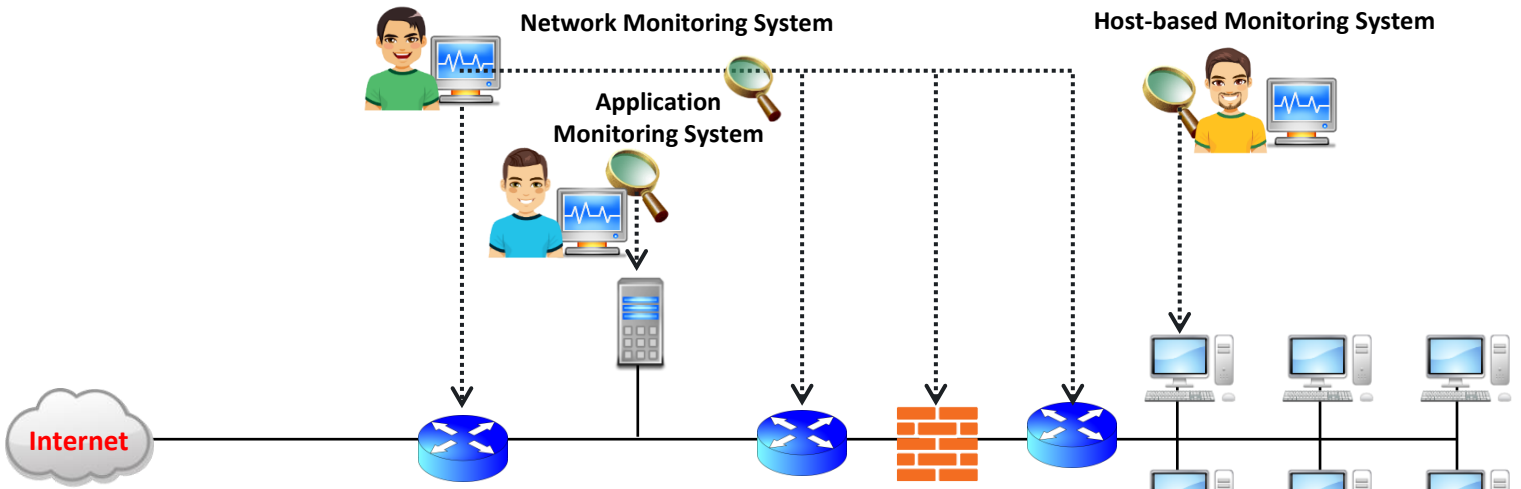
# Structure-based IDS (Cont'd)

## Centralized Control






## Fully Distributed (Agent-based) Control






# Analysis Timing–based IDS



Analysis time is a **span of time elapsed** between the events occurring and the analysis of those events

**An IDS is Categorized based on Analysis Time as:**

## Interval-based IDS

stored and forwarded

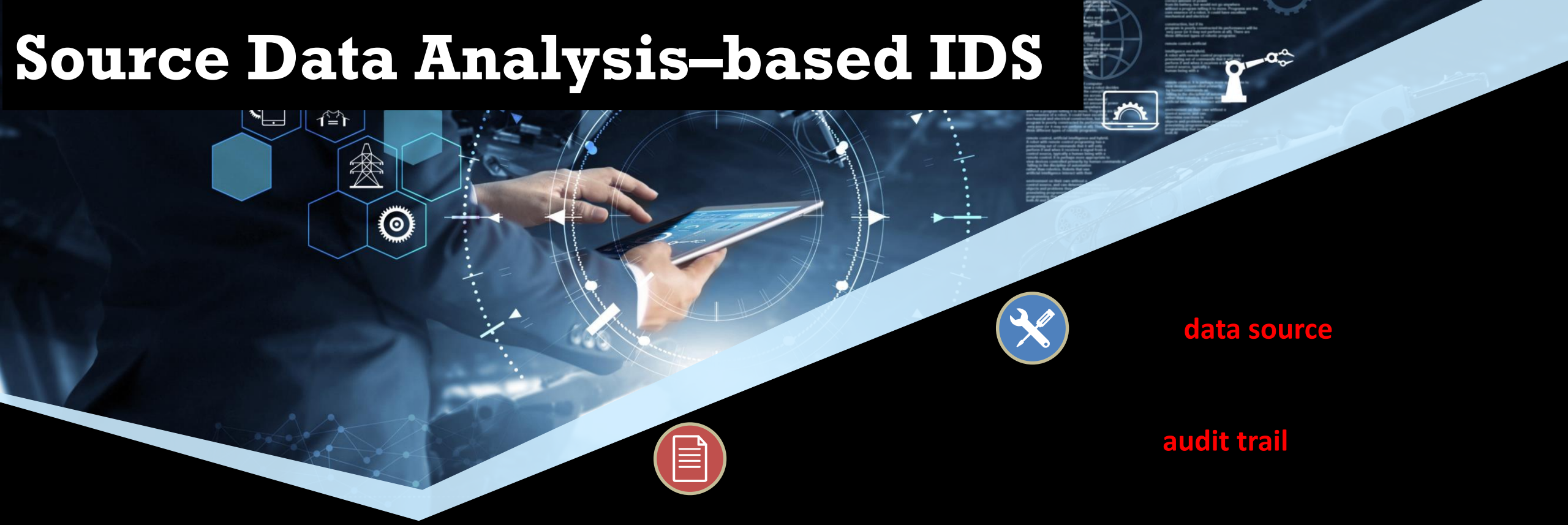
offline

## Real-Time–based IDS

flows continuously

on the fly

# Source Data Analysis–based IDS



data source

audit trail

## Intrusion Detection Using Audit Trails

- **Audit trails** help the IDS detect performance problems, security violations, and flaws in applications

## Intrusion Detection Using Network Packets

- Capturing and analyzing **network packets** help an IDS detect well-known attacks

# IDS Components

An IDS system is built on various components. Knowledge of their **functions** and **placement** is required for effective IDS implementation

## IDS Components



- **Network Sensors**
- **Alert Systems**
- **Command Console**
- **Response System**
- **Attack Signature Database**

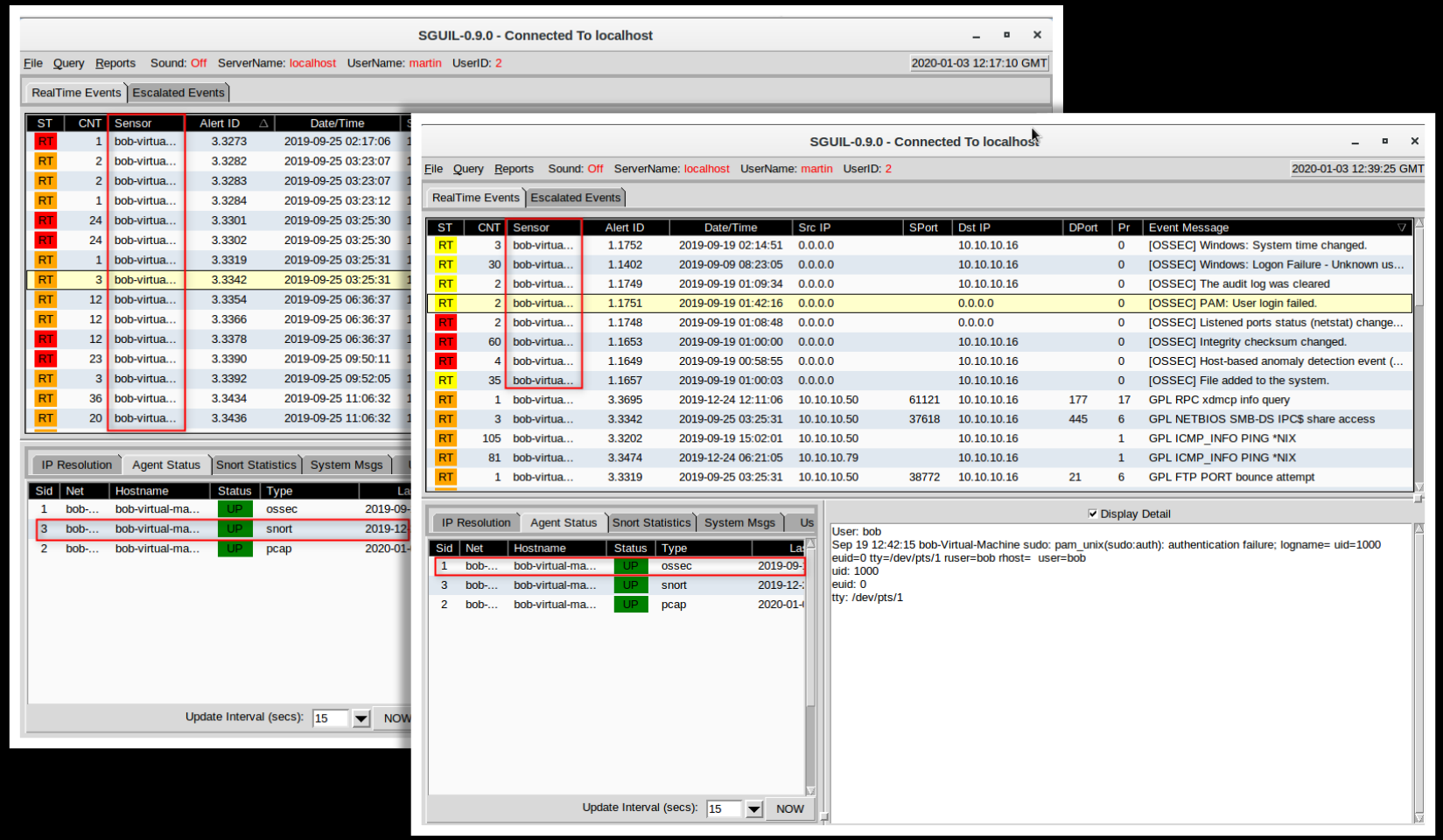


# Network Sensors

Network sensors are hardware and software components that **monitor** network traffic and trigger **alarms** if any abnormal activity is detected

**Network sensors should be placed and located at common entry points in a network such as:**

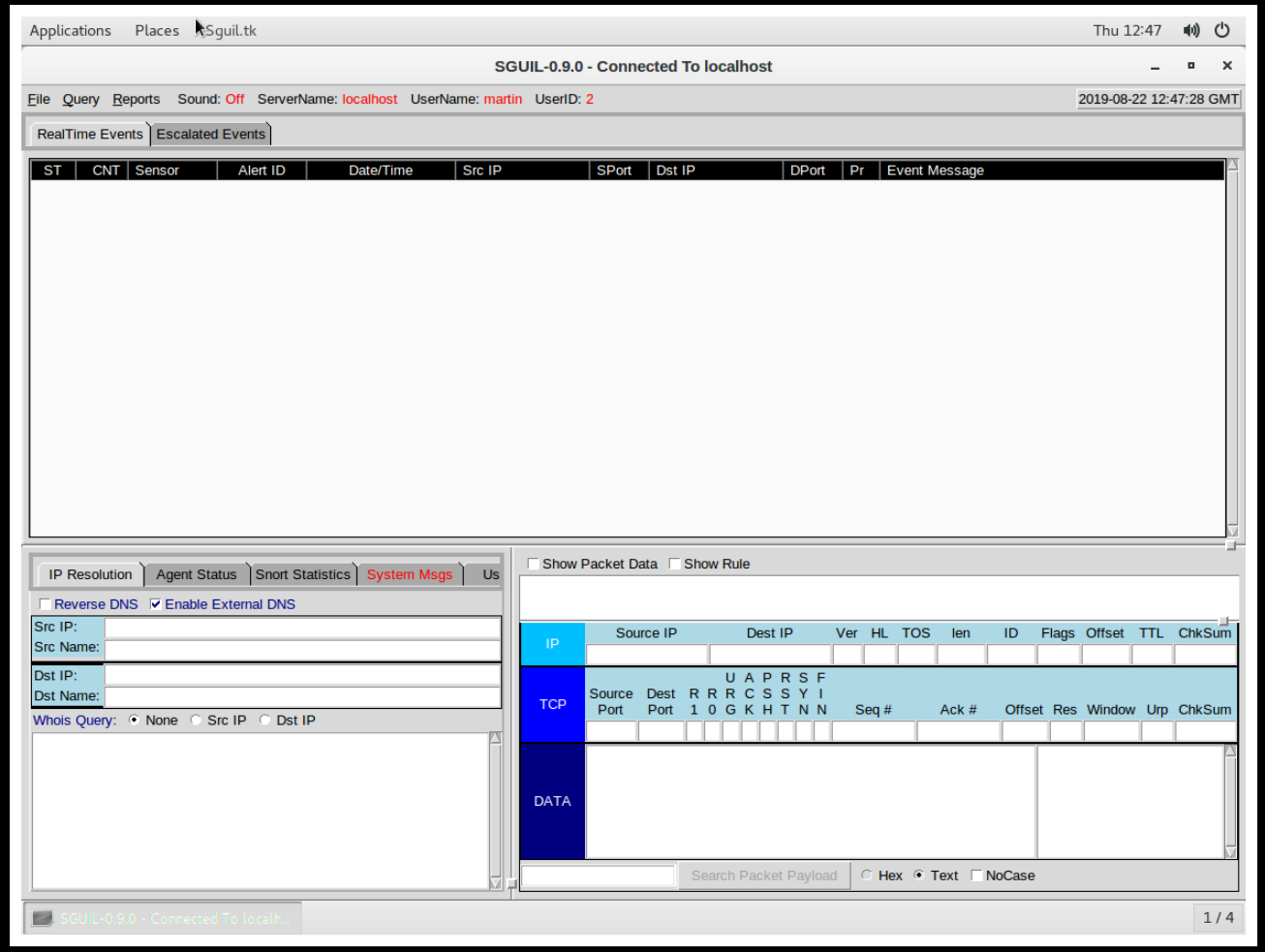
- ❑ Internet gateways
- ❑ In between LAN connections
- ❑ Remote access servers used to receive dial-up connections
- ❑ VPN devices
- ❑ Either side of firewall



# Command Console

- Command console software is installed and runs on a **separate system** that is dedicated to the IDS
- It provides a **user interface** to an administrator for the purpose of receiving and analyzing security events, alert message, and log files
- It evaluates **security event** information from different security devices
- **Caution**: If the command console is installed on a non-dedicated computer system (e.g., firewall, backup server), it will drastically slow down the response to security events as those systems may be busy handling other tasks

## Sguil Command Console

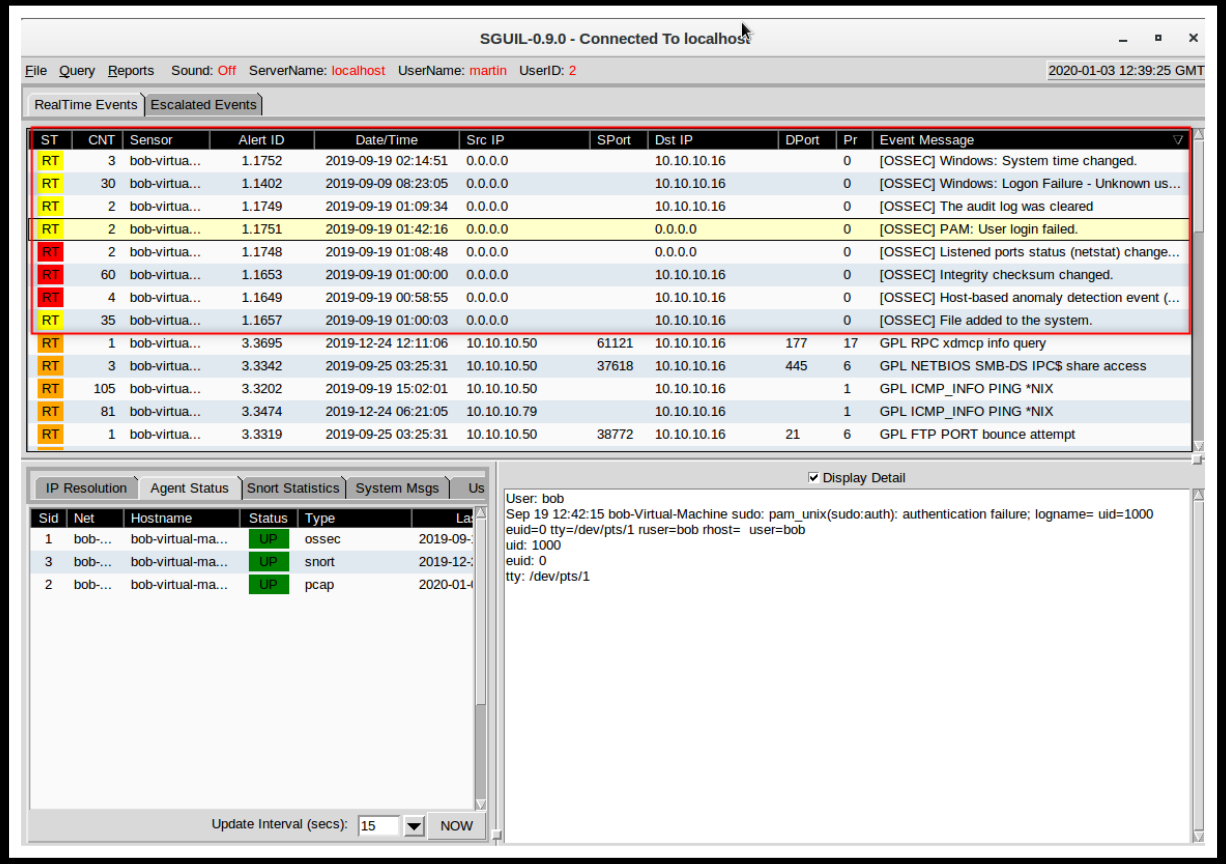


# Alert Systems

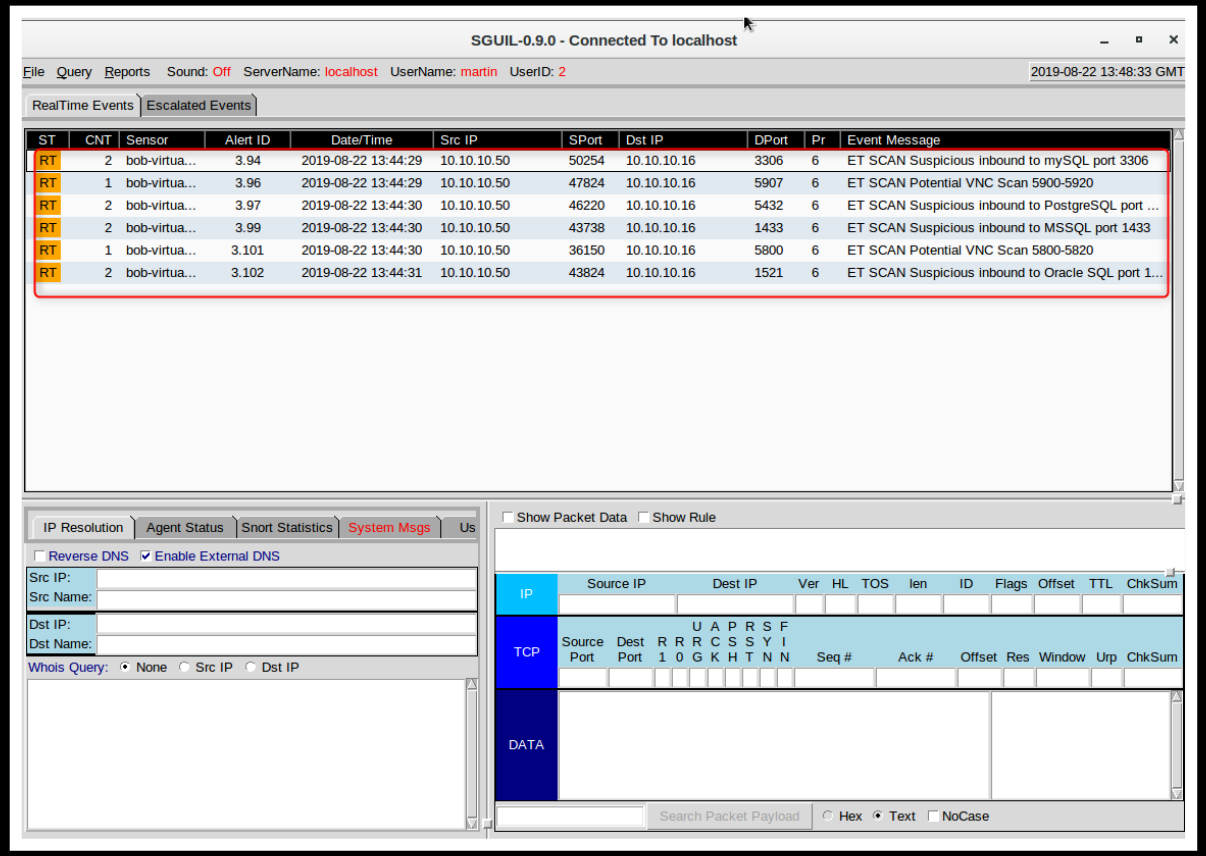
An alert system sends an **alert message** when any anomaly or misuse is detected



## OSSEC HIDS Alerts in Sguil




## Snort NIDS Alerts in Sguil



# Response System

countermeasures

decisions

Recommendation



# Attack Signature Database



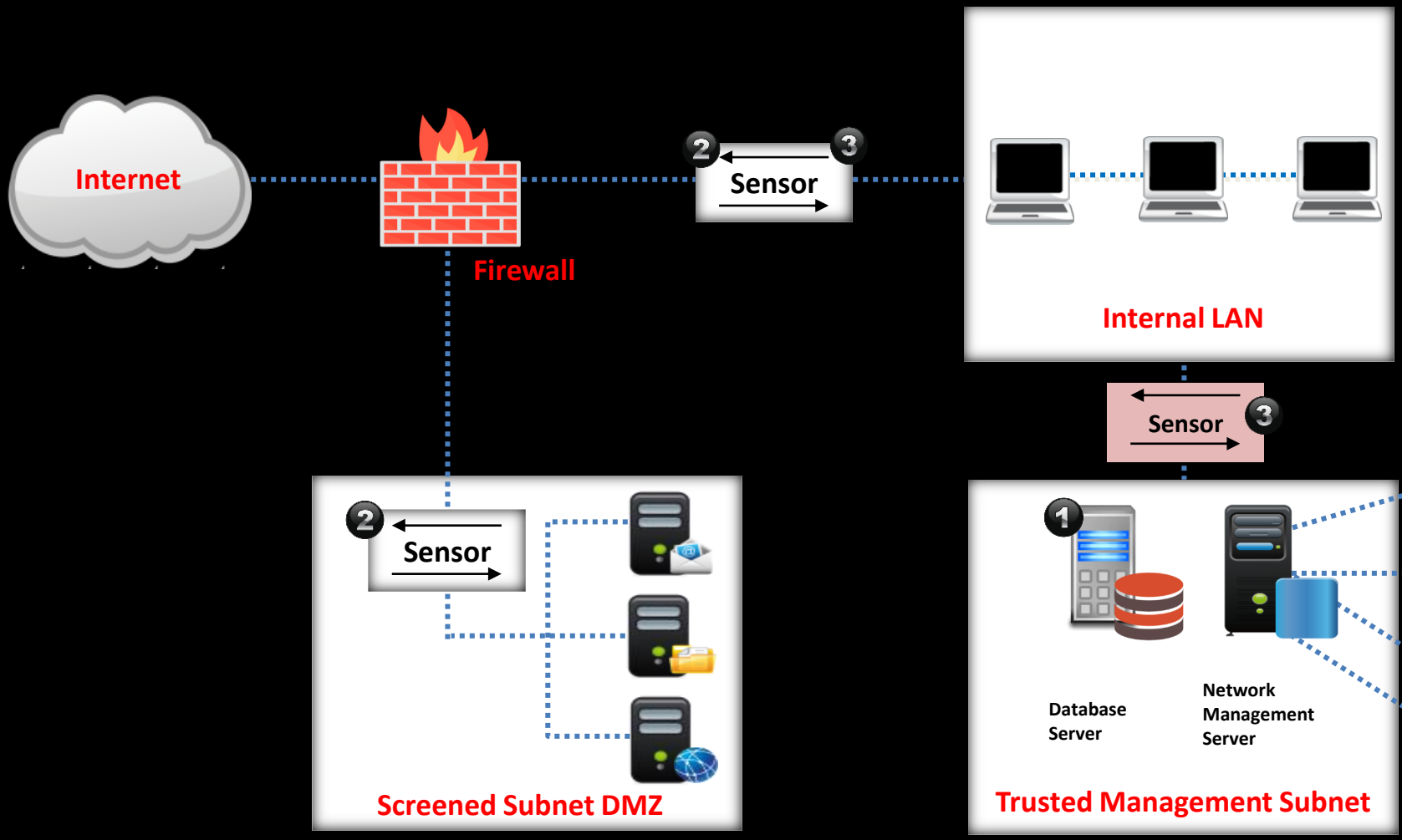
An IDS does not have the capability to make a decision, instead it maintains a **database** of attack signatures and patterns

Network traffic is compared against these known **attack signatures** and then a decision can be made

If any matches are found, the IDS will raise an alert and **block** the suspicious traffic

**Recommendation**: You need to periodically update the IDS attack signature database

# Collaboration of IDS Components in Intrusion Detection

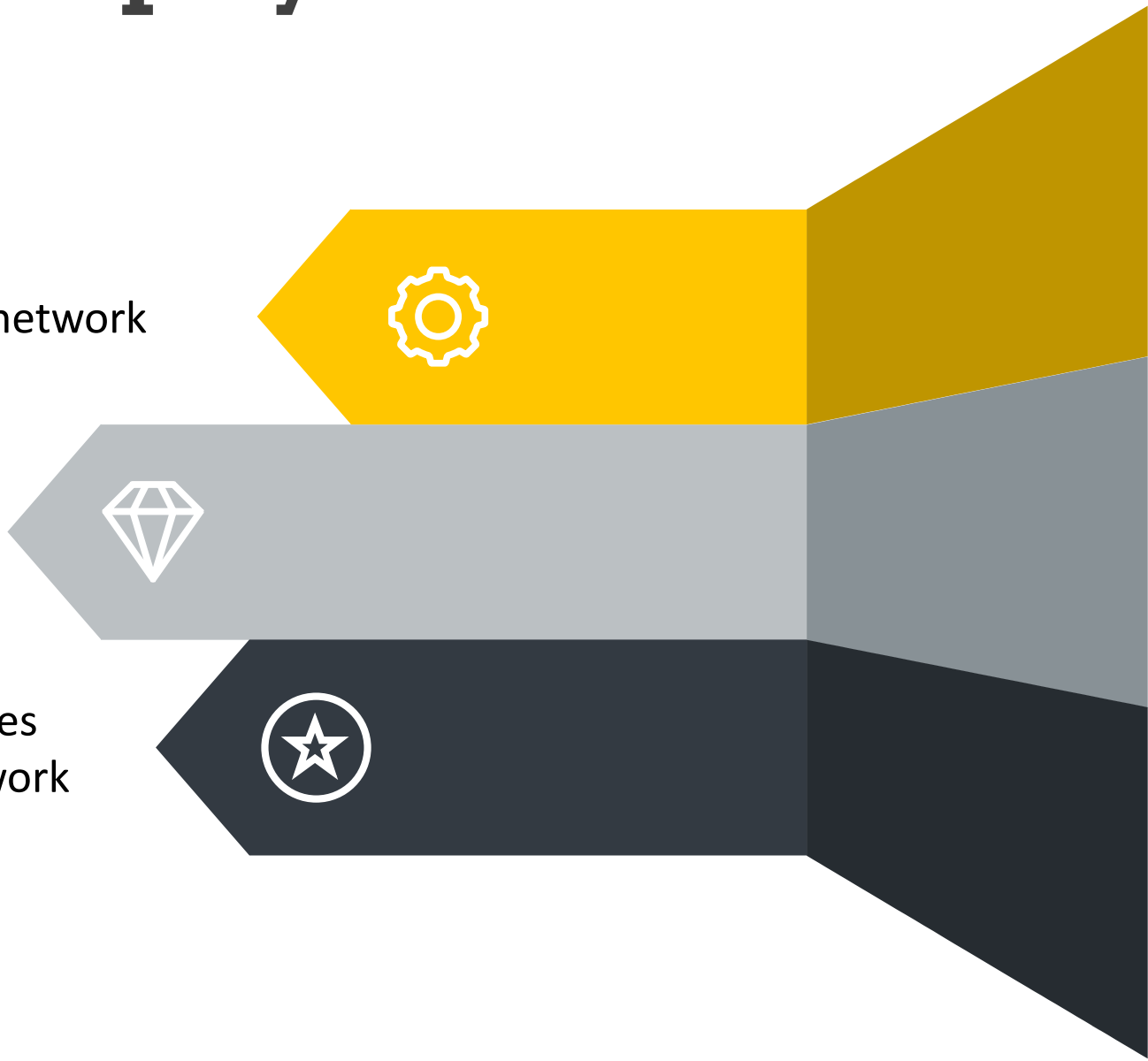



1. Install Database Signatures
2. Gather Data
3. Alert Message Sent
4. IDS Responds
5. Administrator Assesses Damage
6. Escalation Procedures Followed if Necessary
7. Events are Logged and Reviewed

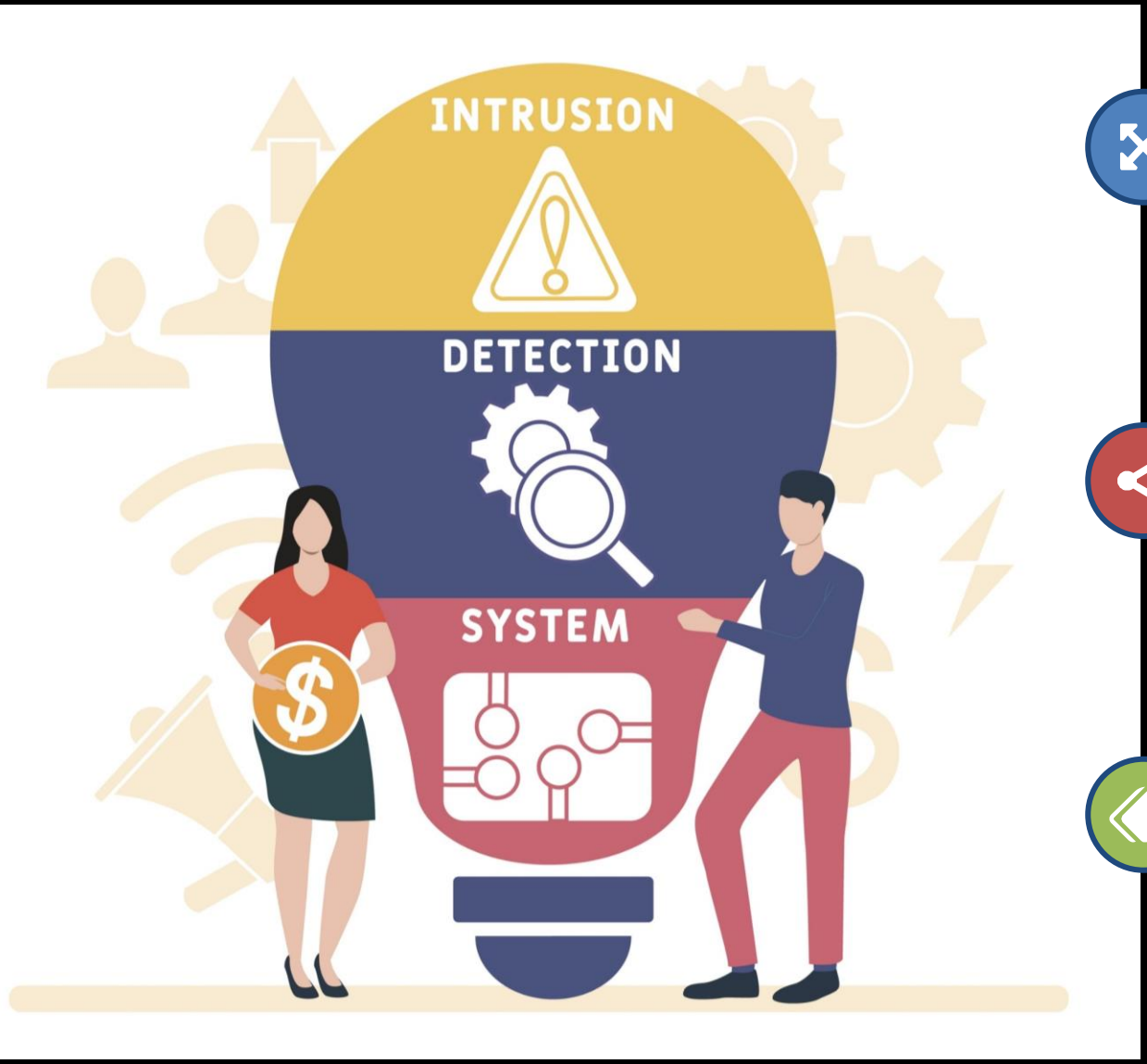
# Deployment of Network and Host-based IDS

# Staged IDS Deployment

- You should **plan** for a staged IDS deployment in their network
- A staged deployment will help you gain **experience** and **discover** how much monitoring and maintenance of network resources is actually required
- The **monitoring** and **maintenance** of network resources varies depending on the size of an organization's network



# Deploying Network-based IDS



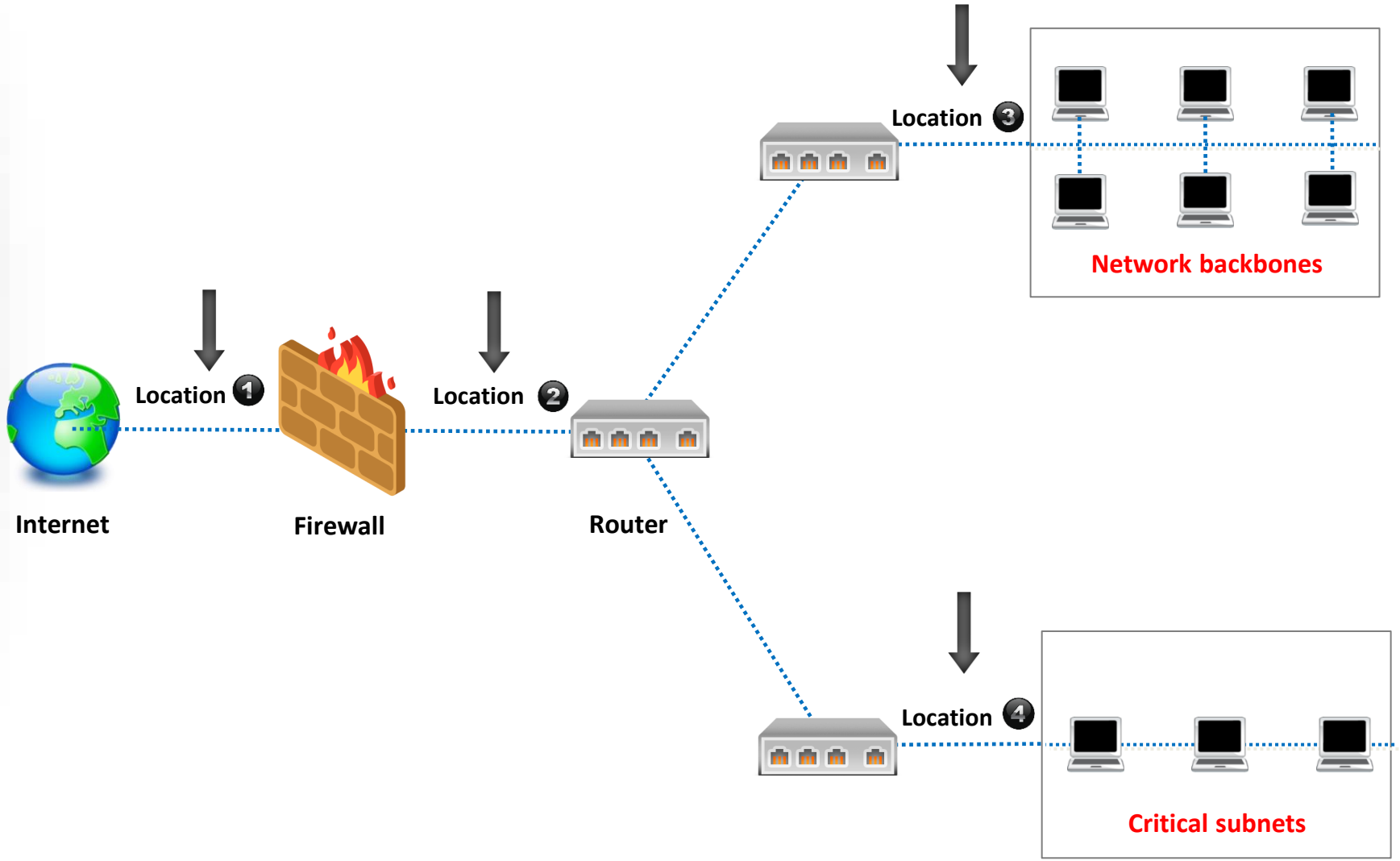

network topology

options

advantages/disadvantages

# Deploying Network-based IDS (Cont'd)





# Deploying Network-based IDS (Cont'd)

## Location 1

- Place an IDS sensor behind each **external firewall** and in the **network DMZ**

### Advantages

- ✓ Monitors attacks originating from the outside world
- ✓ Highlights the inability of the firewall and its policies to defend against attacks
- ✓ It can see attacks which target the web or FTP servers located in the DMZ
- ✓ Monitors outgoing traffic results from a compromised server

## Location 2

- Place an IDS sensor outside an **external firewall**

### Advantages

- ✓ Ability to identify the number and types of attack originating from the Internet to the network



# Deploying Network-based IDS (Cont'd)



## Location 3

- ❑ Place an IDS sensor on major **network backbones**

### Advantages

- ✓ Monitors and inspects large amounts of traffic, increasing the chance for attack detection
- ✓ Detects unauthorized attempts from outside the organization

## Location 4

- ❑ Place an IDS sensor on **critical subnets**

### Advantages

- ✓ Detects attacks on critical systems and resources
- ✓ Focuses on specific critical systems and resources

# Deploying a Host-based IDS

Deploying a host-based IDS provides an **additional layer of security**

This type of IDS must be installed and configured on **each critical system** in the network

You should consider installing a host-based IDS on **every host** in the organization

When deploying a host-based IDS, it is recommended that it has **centralized management** and **reporting** functions, which reduces the complexity for managing alerts from a large number of hosts



# What is an IDS Alert?

- Alert is a **graduated event**, which notifies that a particular event (or series of events) has reached a specified threshold and needs proper action by a responsible party



- It sends the notification, indicating that something is wrong and **requires immediate attention** and monitoring

# Types of IDS Alerts



| | |
|---|---|
| **True Positive (Attack - Alert)** | ❑ An IDS raises an alarm when a **legitimate attack** occurs |
| **False Positive (No Attack - Alert)** | ❑ An IDS raises an alarm when **no attack** has taken place |
| **False Negative (Attack - No Alert)** | ❑ An IDS does not raise an alarm when a **legitimate attack** has taken place |
| **True Negative (No Attack - No Alert)** | ❑ An IDS does not raise an alarm when an **attack** has not taken place |

# Characteristics of Good IDS Solutions

01 less human intervention

02 fault tolerant

03 subversion

04 Minimal overhead

05 deviations

06 deceived

07 system needs

08 dynamic system behavior



# Selection of an Appropriate IDS/IPS Solutions

- IDS products must meet certain **criteria** to be deployed in an organization
- Compare the different technology types, then select the most appropriate **technology** to meet the requirements

**The products should be evaluated based on organizational requirements such as:**

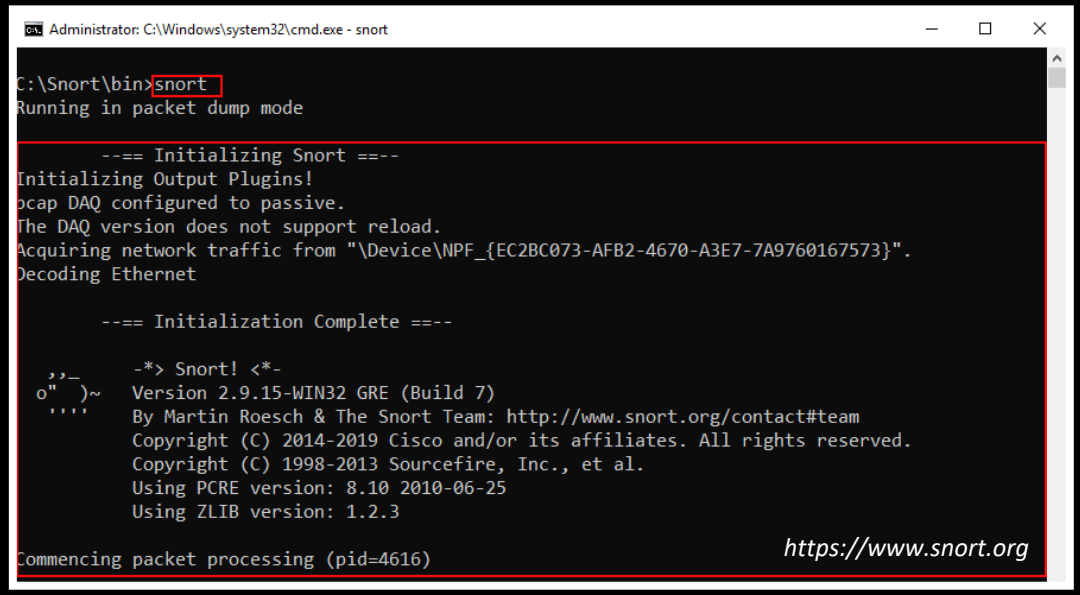
| | |
|---|---|
| **General requirements** | ❑ Evaluate the general requirements the IDS products will have to meet post deployment<br>❑ Size of an organization also modifies the number of IDS products needed |
| **Security Capability Requirements** | ❑ The selection of an IDS depends on an organization's environment and policies as well as the current security and network infrastructure |
| **Performance requirements** | ❑ Evaluate an IDS product's general performance characteristics by assessing its capacity to handle the network traffic or packet monitoring capabilities for NIDS and event monitoring capabilities for HIDS |
| **Management requirements** | ❑ The products need to comply with the organization's management policy in order to be used effectively |
| **Life Cycle Costs** | ❑ Estimated lifecycle costs of the products should be within the available budget |

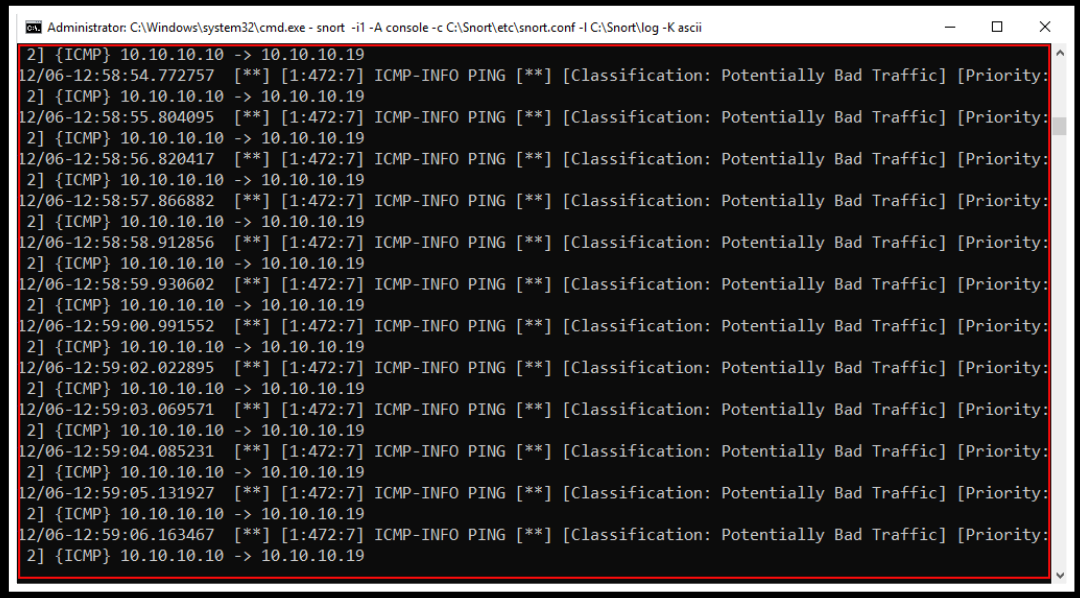
# Intrusion Detection with Snort

01 traffic analysis and packet logging on IP networks

02 protocol analysis content searching/matching attacks and probes

03 rules language detection engine

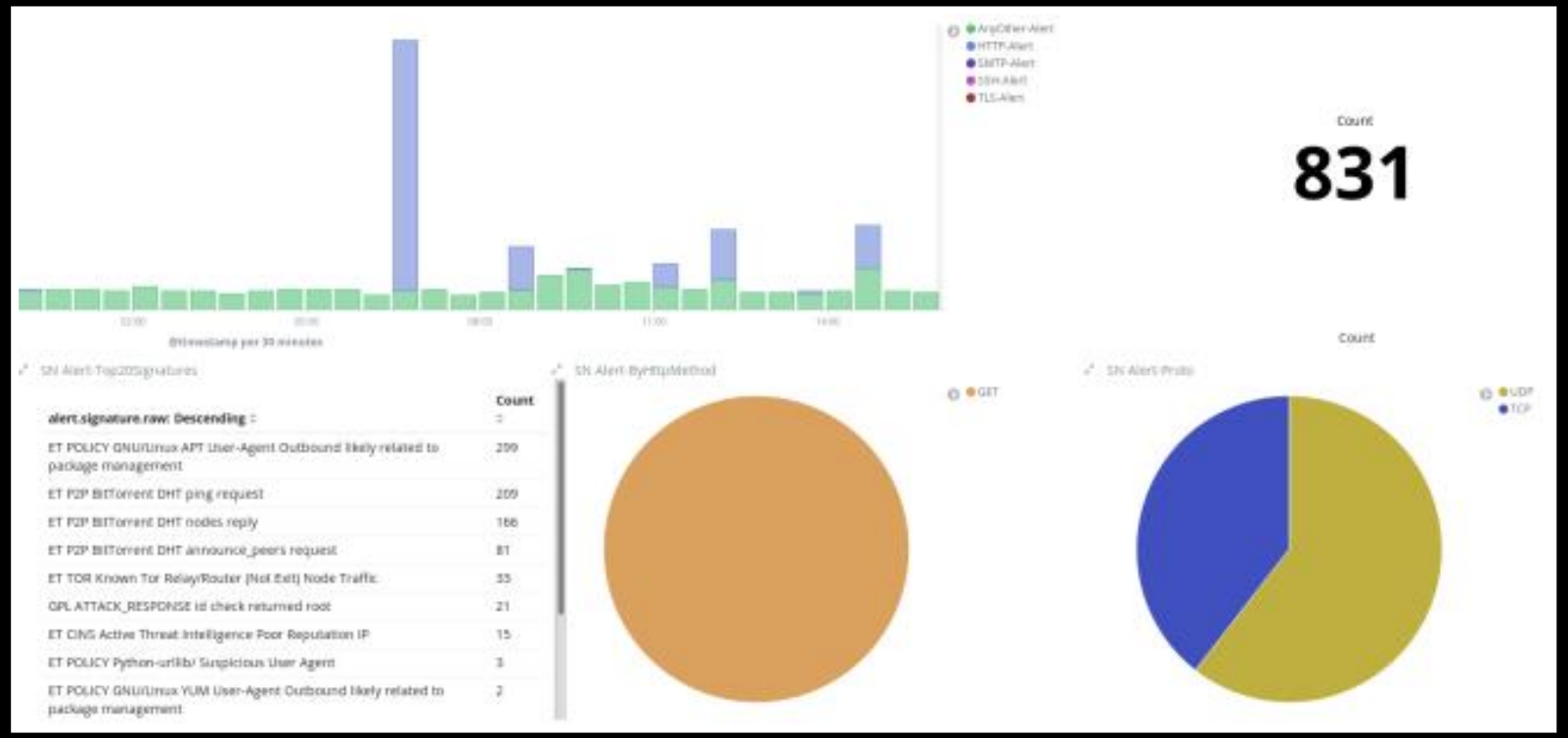


# Intrusion Detection Tools

**Suricata**

Suricata is a robust network threat detection engine capable of **real-time intrusion detection (IDS)**, **inline intrusion prevention (IPS)**, **network security monitoring (NSM)**, and **offline pcap processing**



# Module Flow

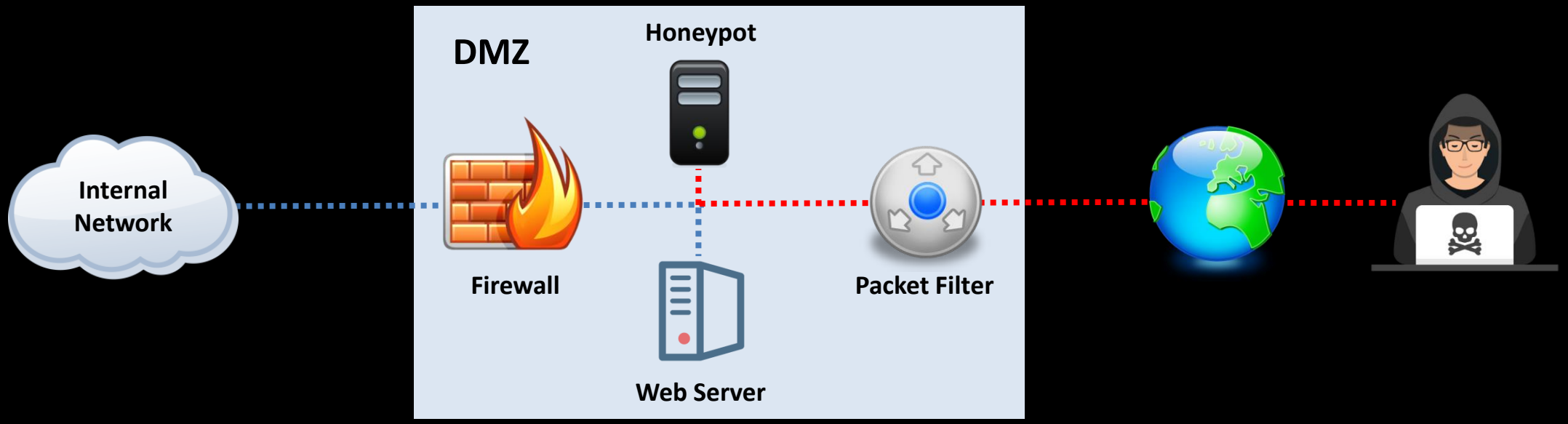
1. Understand Different Types of Network Segmentation
2. Understand Different Types of Firewalls and their Role
3. Understand Different Types of IDS/IPS and their Role
4. **Understand Different Types of Honeypots**
5. Understand Different Types of Proxy Servers and their Benefits
6. Discuss Fundamentals of VPN and its importance in Network Security
7. Discuss Security Incident and Event Management (SIEM)
8. Discuss User Behavior Analytics (UBA)
9. Understand Various Antivirus/Anti-malware Software

# Honeypot

A honeypot is an information system resource that is expressly **set up to attract and trap people** who attempt to penetrate an **organization's network**

It has no authorized activity, does not have any **production value**, and any traffic to it is likely to be a **probe**, **attack**, or **compromise**

A honeypot can **log port access** attempts or monitor an **attacker's keystrokes**. These could be **early warnings** of a more concerted attack



# Types of Honeypots

## Classification of Honeypots based on their design criteria

### Low-interaction Honeypots

limited number of services

### High-interaction Honeypots

simulate all services



### Medium-interaction Honeypots

real operating system

### Pure Honeypots

real production network

# Types of Honeypots (Cont'd)

## Classification of honeypots based on their deployment strategy



**Production Honeypots**



**Research Honeypots**

# Types of Honeypots (Cont'd)



## Classification of honeypots based on their deception technology

### Malware Honeypots

- Are used to trap malware campaigns or malware attempts over the network infrastructure

### Database Honeypots

- Employ fake databases that are vulnerable to perform database-related attacks such as SQL injection and database enumeration

### Spam Honeypots

- Specifically target spammers who abuse vulnerable resources such as open mail relays and open proxies

### Email Honeypots

- Fake email addresses that are specifically used to attract fake and malicious emails from adversaries

### Spider Honeypots

- Specifically designed to trap web crawlers and spiders

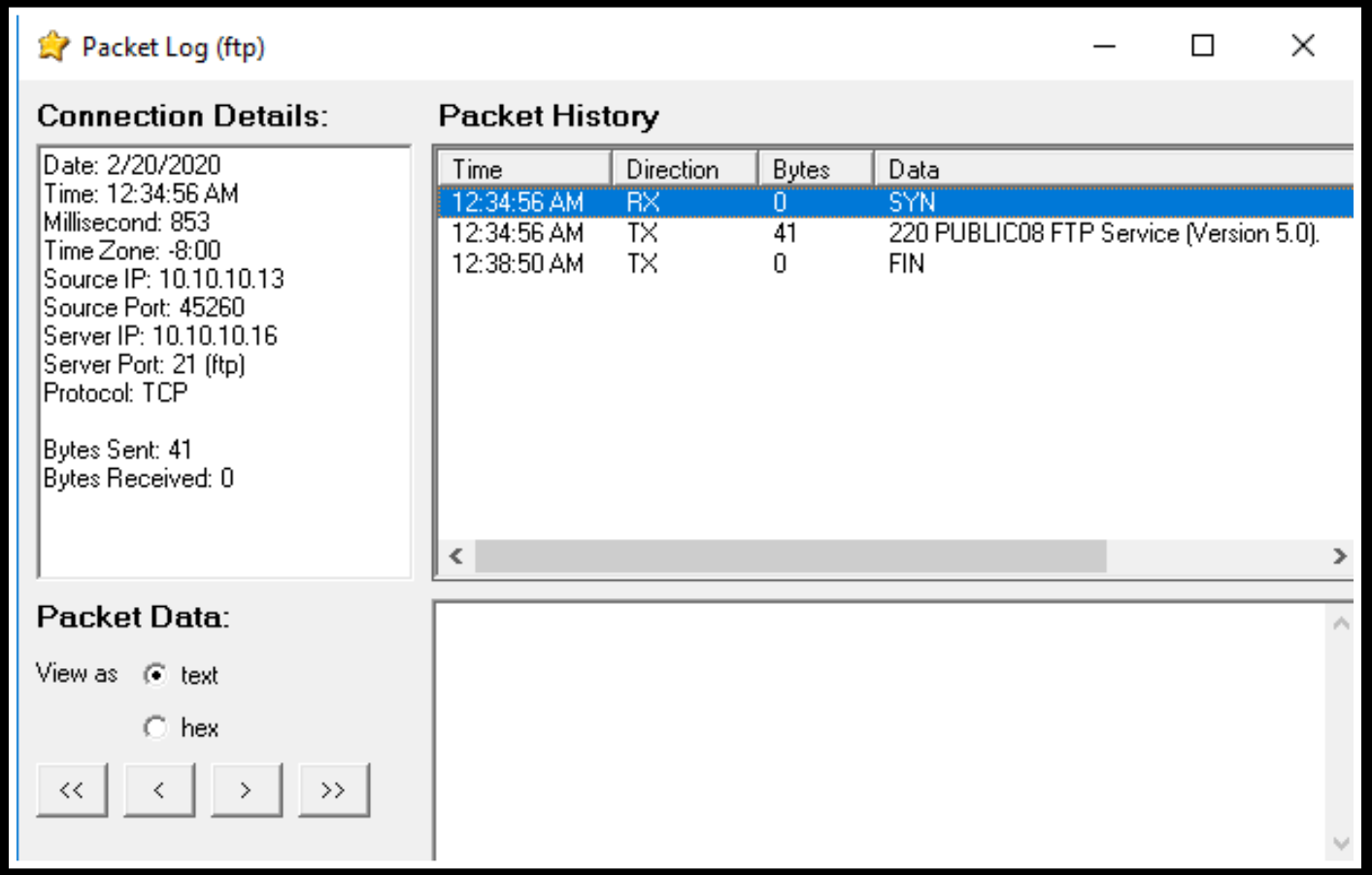
### Honeynets

- Networks of honeypots which are very effective in determining the entire capabilities of the adversaries

# Honeypot Tools

**HoneyBOT**

HoneyBOT is a medium interaction honeypot for windows. It is an easy-to-use solution that is ideal for network security research



# Module Flow

1. Understand Different Types of Network Segmentation
2. Understand Different Types of Firewalls and their Role
3. Understand Different Types of IDS/IPS and their Role
4. Understand Different Types of Honeypots
5. **Understand Different Types of Proxy Servers and their Benefits**
6. Discuss Fundamentals of VPN and its importance in Network Security
7. Discuss Security Incident and Event Management (SIEM)
8. Discuss User Behavior Analytics (UBA)
9. Understand Various Antivirus/Anti-malware Software

# What are Proxy Servers?

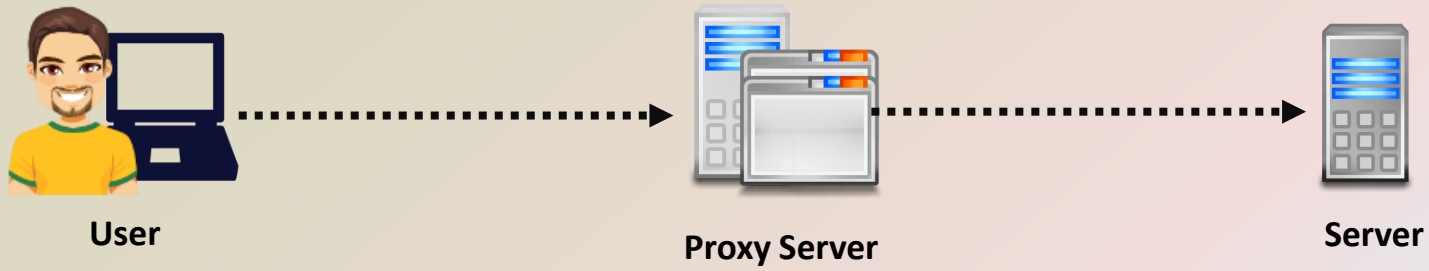
01 dedicated computer

02 sentinel

03 clients requests

04 layer of defense

05 intercept



# Benefits of Proxy Server

1

Acts as a **security protector** between the user devices and a server

2

Enhances the security and **privacy of client devices**

3

Improves the **browsing speed**

4

Provides **advanced logging capabilities** for user activities

5

**Controls access** to specific types of restricted services

6

**Hides internal IP addresses** and filters requests from external sites

7

Reduces the chances of modifying cookies in the **browser configuration**

8

**Enables authentication** for the proxy servers before handling user requests

# Functioning of a Proxy Server



01 web site

02 packet header

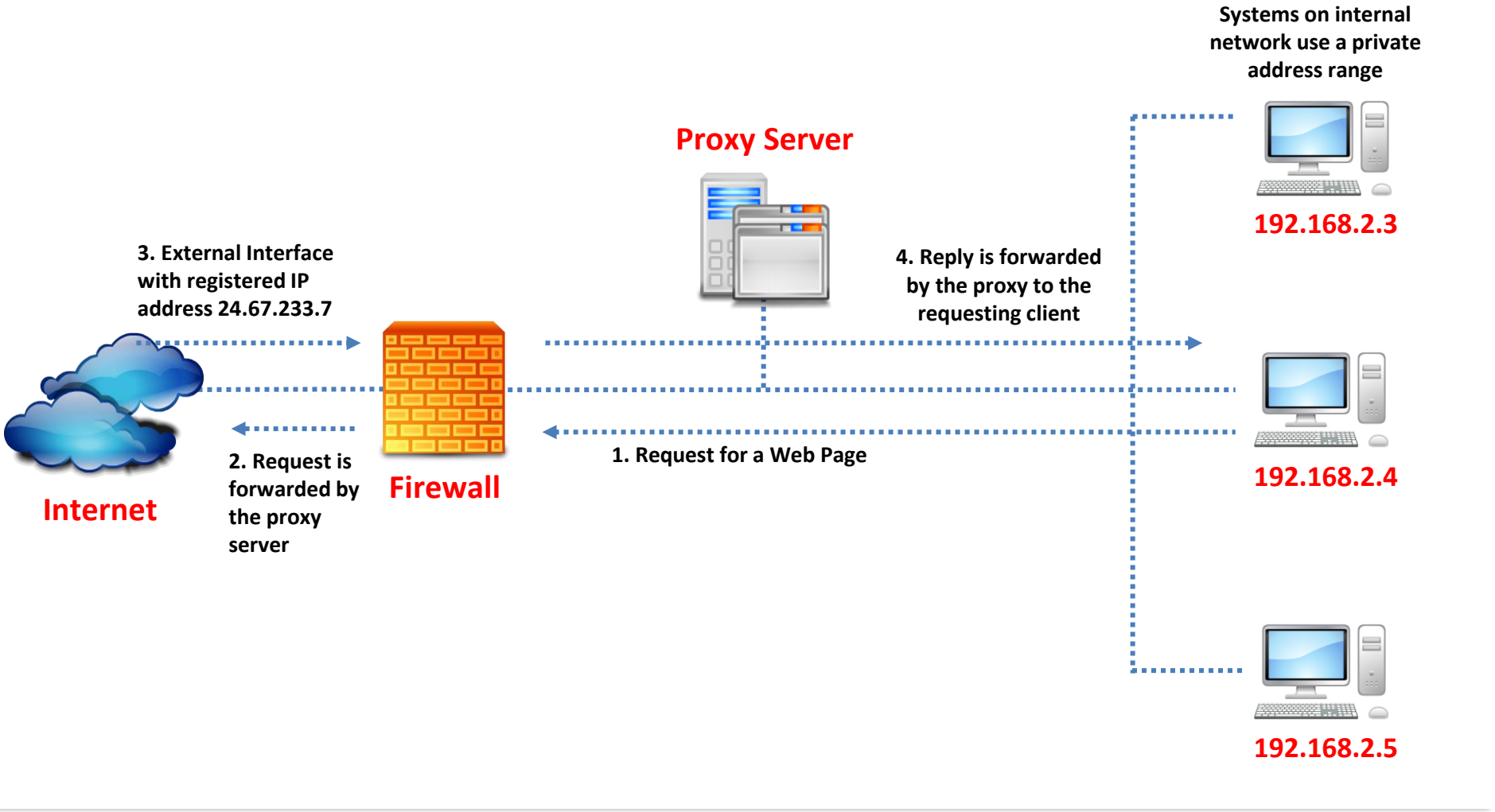
03 reconstructs different source IP address

04 target address

05 proxy server

06 reconstructed

# Functioning of a Proxy Server (Cont'd)



# Proxy Servers vs Packet Filters

| Proxy Servers | Packet Filters |
| --- | --- |
| ❑ Proxy server examines the **data payload** of the packet | ❑ Packet filters examine the **routing information** of the packet |
| ❑ Creates detailed **log file** listings, since they scan the entire data of IP packets | ❑ Logs only the **header information** of the IP packets |
| ❑ **Restructures** the packet with new source IP data | ❑ **Allows** or **blocks** the data depending on the packet filter rules |
| ❑ In the case of failure of a proxy server, all **network communications** would cease | ❑ In the case of failure of a packet filter, all packets may be allowed to **pass through** the internal network |



# Types of Proxy Servers



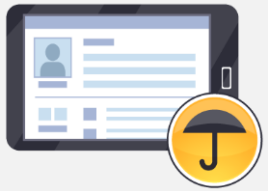
Transparent Proxy



Non Transparent Proxy



SOCKS Proxy



Anonymous Proxy



Reverse Proxy



# Transparent Proxy



01 A transparent proxy is a proxy through which a **client system connects** to a server without its knowledge

02 It is configured to be entirely **invisible** to an end user

03 With a transparent proxy, all the web clients must be **configured manually**

# Non-transparent Proxy



- Require **client software to be configured** to use the proxy server
- The **client** is made aware of the **proxy's existence**
- They are difficult to configure, as each client program must be set up to route all requests to a single port

| 01 | 02 | 03 | 04 |
|---|---|---|---|
| Group Annotation Services | Media Type Transformation | Protocol Reduction | Anonymity Filtering |

# SOCKS Proxy



- The SOCKS is an **Internet Engineering Task Force (IETF)** standard
- It is a proxy server that does not have the special caching abilities of a caching HTTP proxy server
- The SOCKS proxy server does not allow **external network components** to collect information on the client that generated the request

**The SOCKS package includes or contains the following components**



A SOCK server for the specified operating system (OS)



A client program such as FTP, Telnet, or an Internet browser



A client library for SOCKS

# Anonymous Proxy

- An anonymous proxy does not transfer information about the IP address of its user, thereby **hiding information** about the user and their **surfing interests**



## Pros

- A user can surf the Internet **privately** by using an anonymous proxy
- With the help of an anonymous proxy server, a user can access even **censored websites**



## Cons

- Using this type of proxy server may **decrease the speed** of loading a web page on to the browser
- Using anonymous proxy servers to **bypass Internet censorship is illegal** in some countries





# Reverse Proxy

01 A reverse proxy is usually **situated closer to the server(s)** and will only return a configured set of resources

02 It can **optimize content** by compressing it to speed up loading

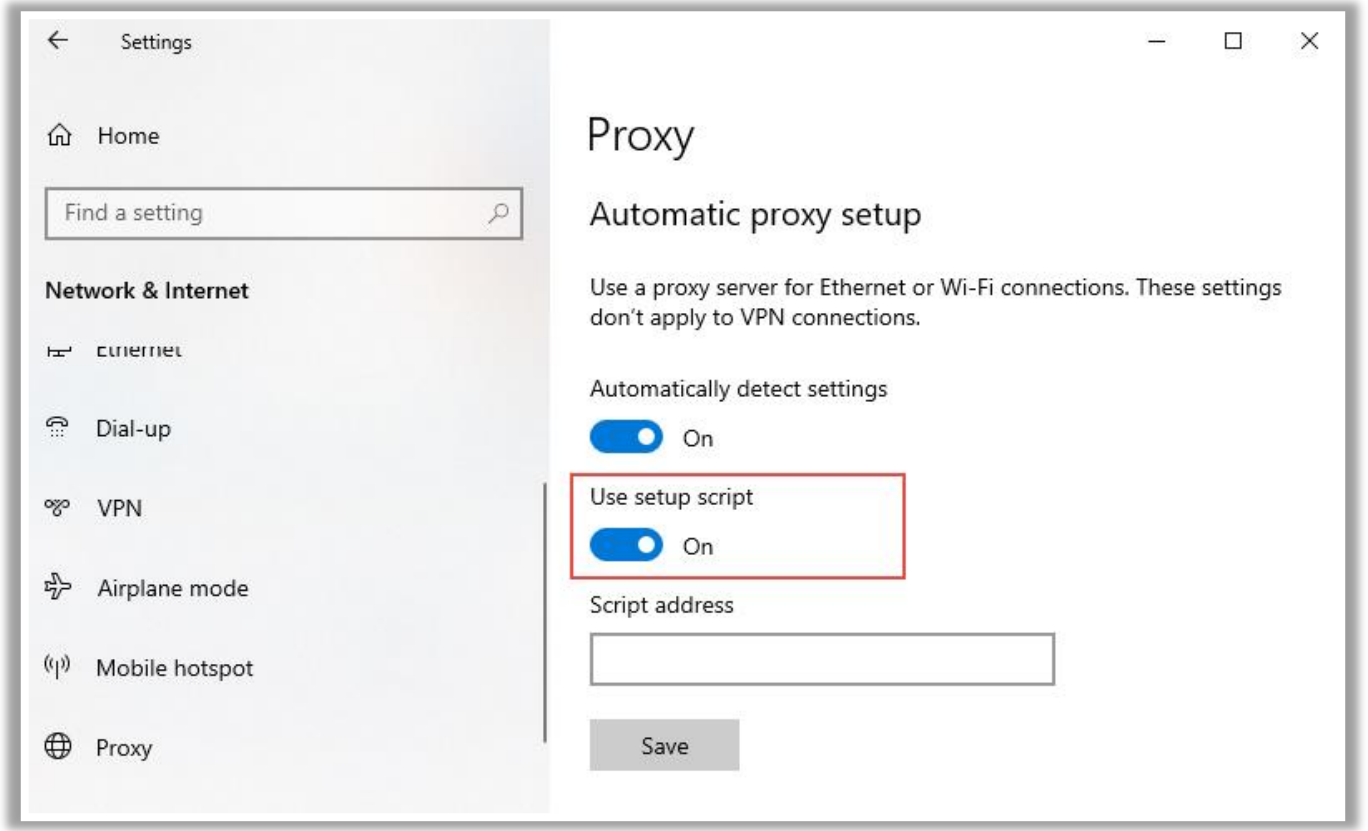
03 The client is **unaware of the presence** of a reverse proxy

04 A reverse proxy server is an **intermediate server** that is located between a client and the actual web server

# How to Configure Proxy Server

## Configuring Automatic Proxy Setup in Windows 10

| | |
|---|---|
| **Step 1** | Open Windows Settings by pressing the **Windows key** and **I** together |
| **Step 2** | Click **Network & Internet → Proxy** |
| **Step 3** | Check if the "**Automatically detect settings**" toggle button is **On** |
| **Step 4** | Windows runs an automatic check by default |
| **Step 5** | If Windows detects PAC file, set the "**Use Setup Script**" toggle button to **On** |
| **Step 6** | Type **proxy.certifiedhacker.com** in the "**Script Address**" field |
| **Step 7** | Click **Save** to implement the changes and use the Internet through the proxy |






# How to Configure Proxy Server (Cont'd)

Windows key + I

Network & Internet → Proxy

Manual proxy setup

Use a Proxy Server On

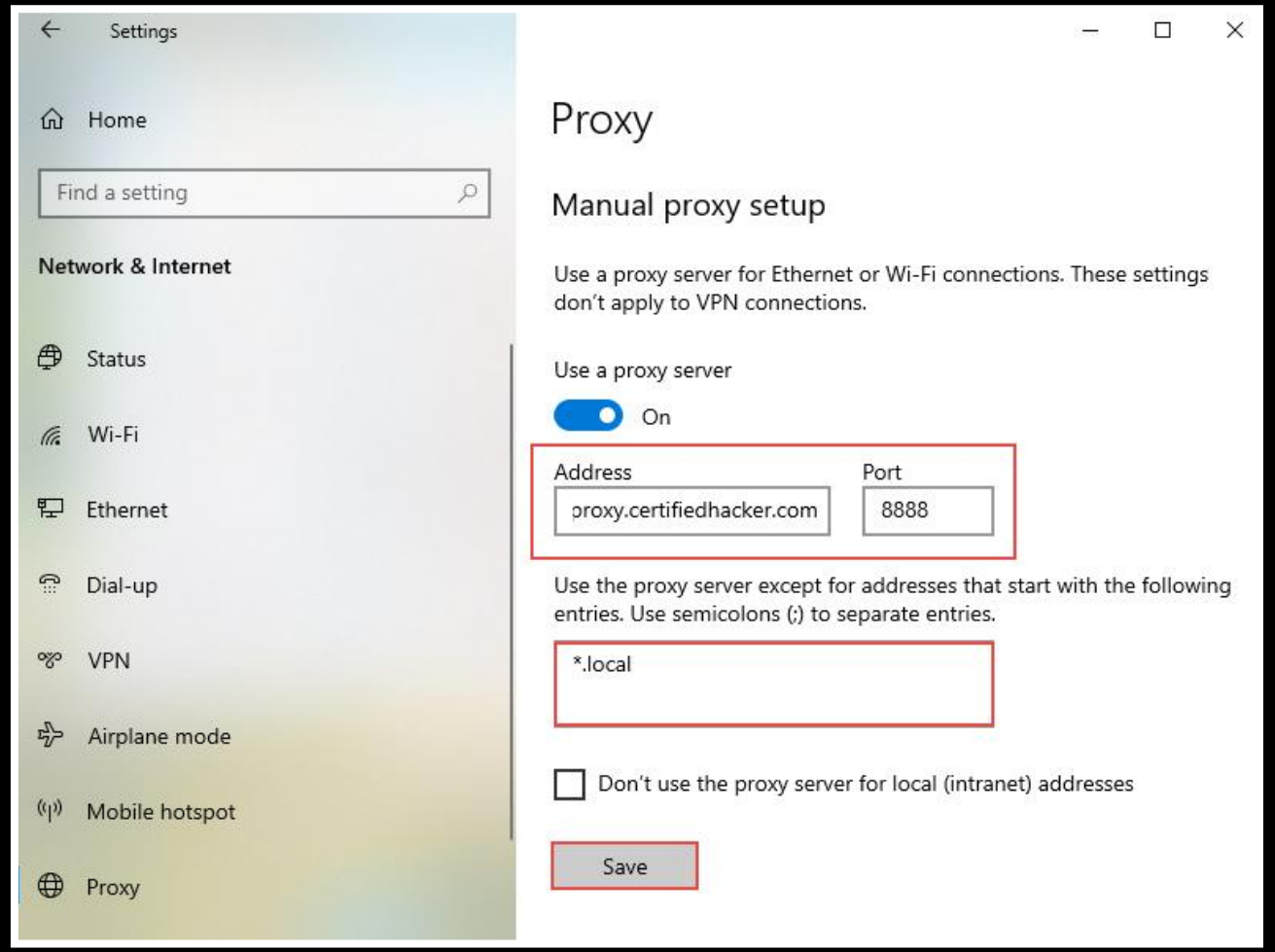
proxy.certifiedhacker.com

8888

*.local

Save

## Configuring Manual Proxy Setup in Windows 10



# How to Configure Proxy Server (Cont'd)

## Configuring Proxy Setup in Google Chrome

### Step 1

Open the Google Chrome browser and select "**Settings**" in the toolbar

### Step 2

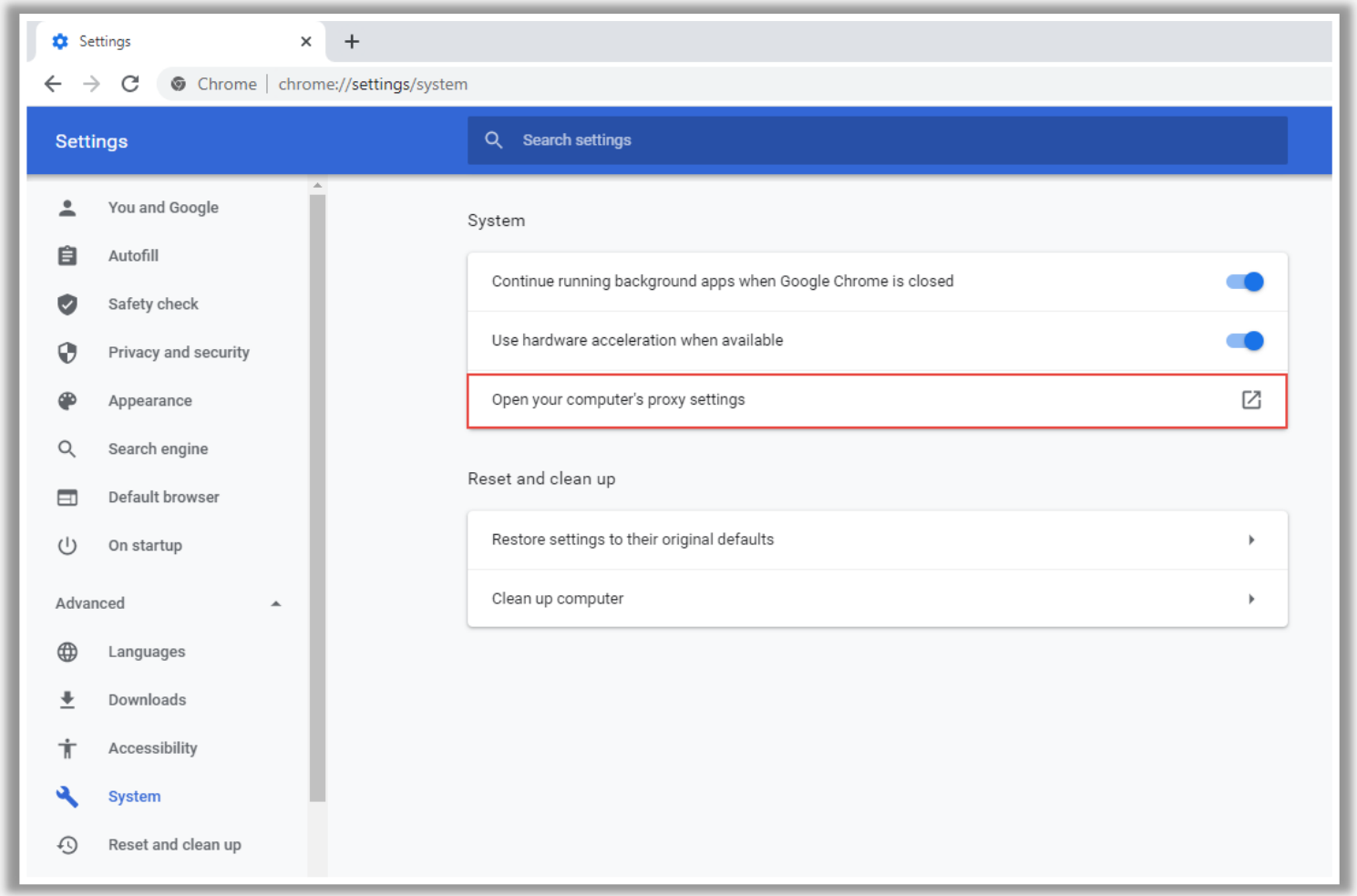
Scroll down on the page and Click **Advanced → System**

### Step 3

The **System** window opens. Click "**Open your computer's proxy settings**"

### Step 4

The proxy server settings window opens. Follow the instructions to configure the proxy



# How to Configure Proxy Server (Cont'd)

## Configuring Proxy Setup in Microsoft Edge

### Step 1

Open the Microsoft Edge browser and click "**Settings**" from the menu displayed on the top-right corner

### Step 2

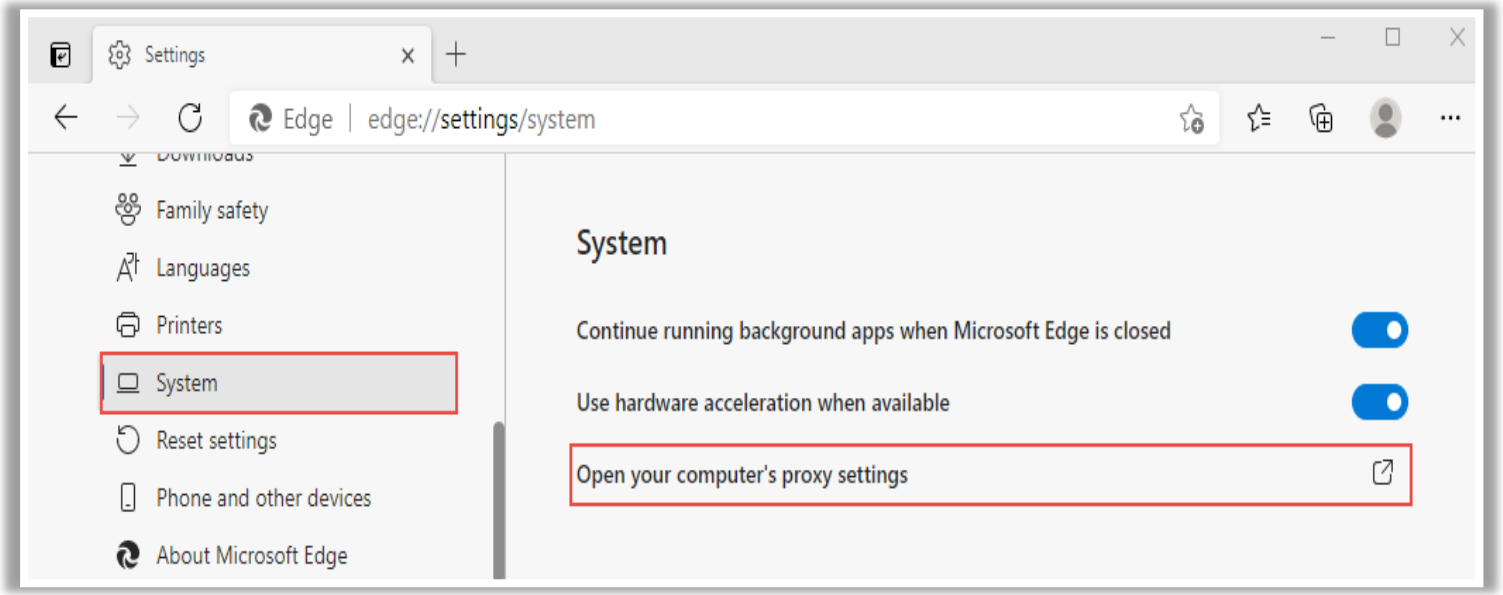
Scroll down on the page and click "**System**"

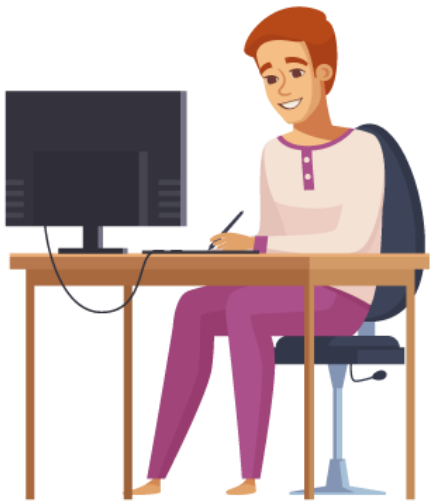
### Step 3

The **System** window opens. Click "**Open your computer's proxy settings**"

### Step 4

The proxy server setup window opens. Follow the instructions to configure the proxy server

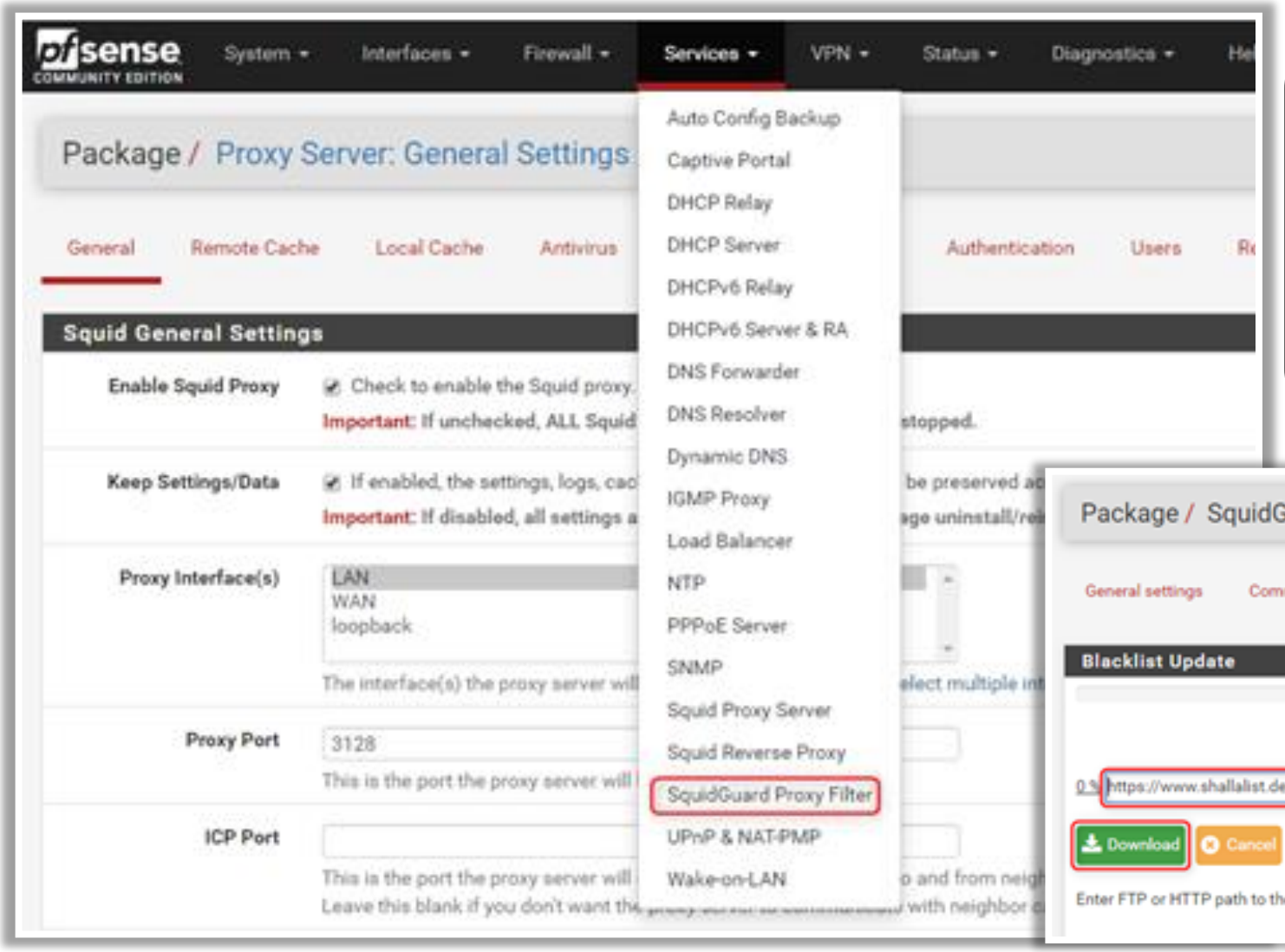


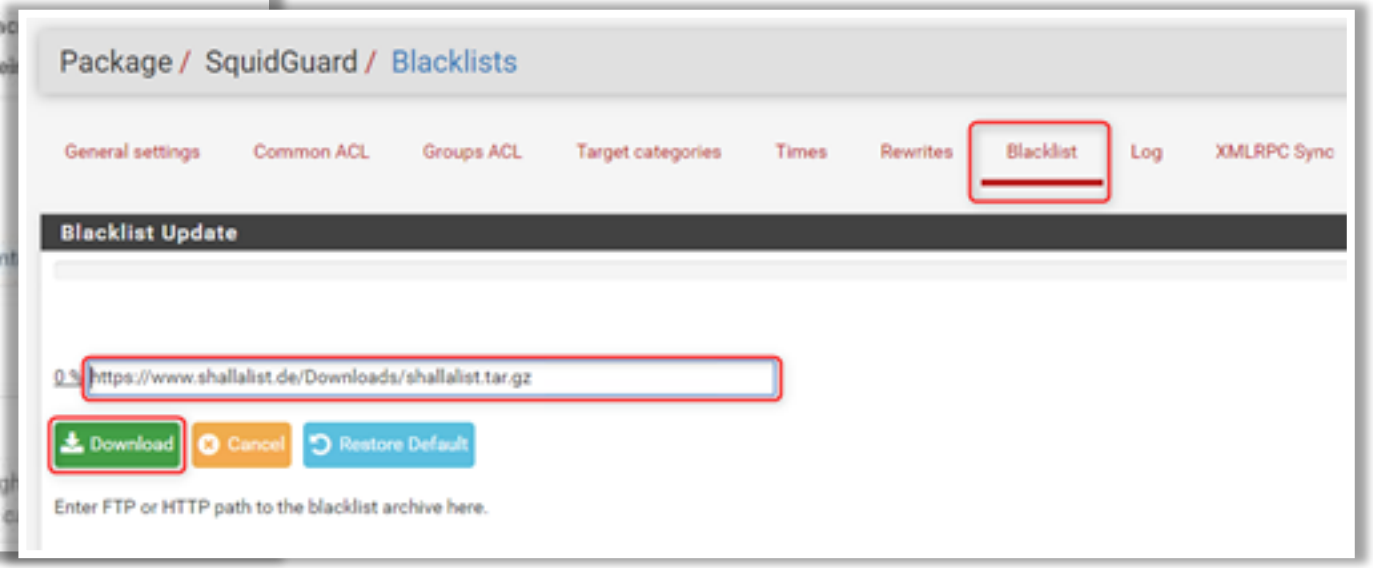
# Limitations of Proxy Server

1. If proxy is **not properly secured,** then it may become point of failure in an event of attack
2. **Increase in workload** since proxy must be configured for each and every service it provides
3. If we attempt to change the **default settings**, the proxy server might not function properly
4. Proxy servers have to **reroute information**, thus web pages can sometimes load slowly
5. If the proxy server is attempting to **bypass suspicious software**, some elements of a page may not load

# Example of a Proxy Server: Squid Proxy




- Squid is a **caching proxy for the web** and supports HTTP, HTTPS, FTP, and more
- It **reduces the bandwidth** and **improves the response time** by caching and reusing frequently-requested web pages



# List of Proxy Tools



**Whonix**
*https://www.whonix.org*



**Psiphon**
*https://psiphon.ca*



**FoxyProxy**
*https://getfoxyproxy.org*



**GeoSurf**
*https://www.geosurf.com*



**JonDo**
*https://anonymous-proxy-servers.net*



**Proxify**
*https://proxify.com*



**Guardster**
*http://www.guardster.com*



**Global Proxy Network**
*https://infatica.io*



**Anonym8**
*https://github.com*



**ProxySite**
*https://www.proxysite.com*



**ProxyCap**
*https://www.proxycap.com*



**CCProxy**
*https://www.youngzsoft.net*



**Fiddler**
*https://www.telerik.com*



**BlackArch Proxy**
*https://blackarch.org*



**Artica Proxy**
*https://artica-proxy.com*

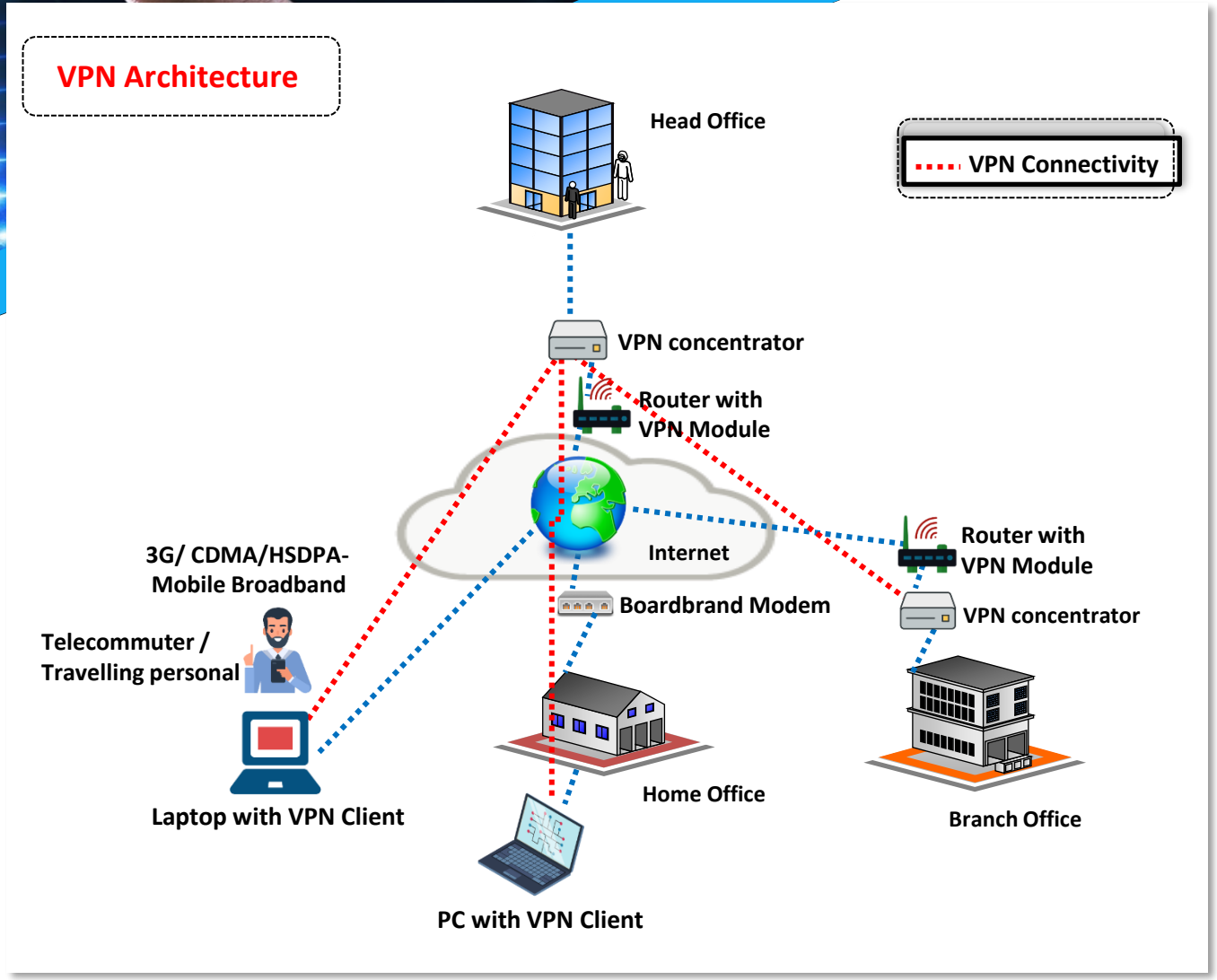
# Module Flow

1. Understand Different Types of Network Segmentation
2. Understand Different Types of Firewalls and their Role
3. Understand Different Types of IDS/IPS and their Role
4. Understand Different Types of Honeypots
5. Understand Different Types of Proxy Servers and their Benefits
6. **Discuss Fundamentals of VPN and its importance in Network Security**
7. Discuss Security Incident and Event Management (SIEM)
8. Discuss User Behavior Analytics (UBA)
9. Understand Various Antivirus/Anti-malware Software

# What is a VPN?

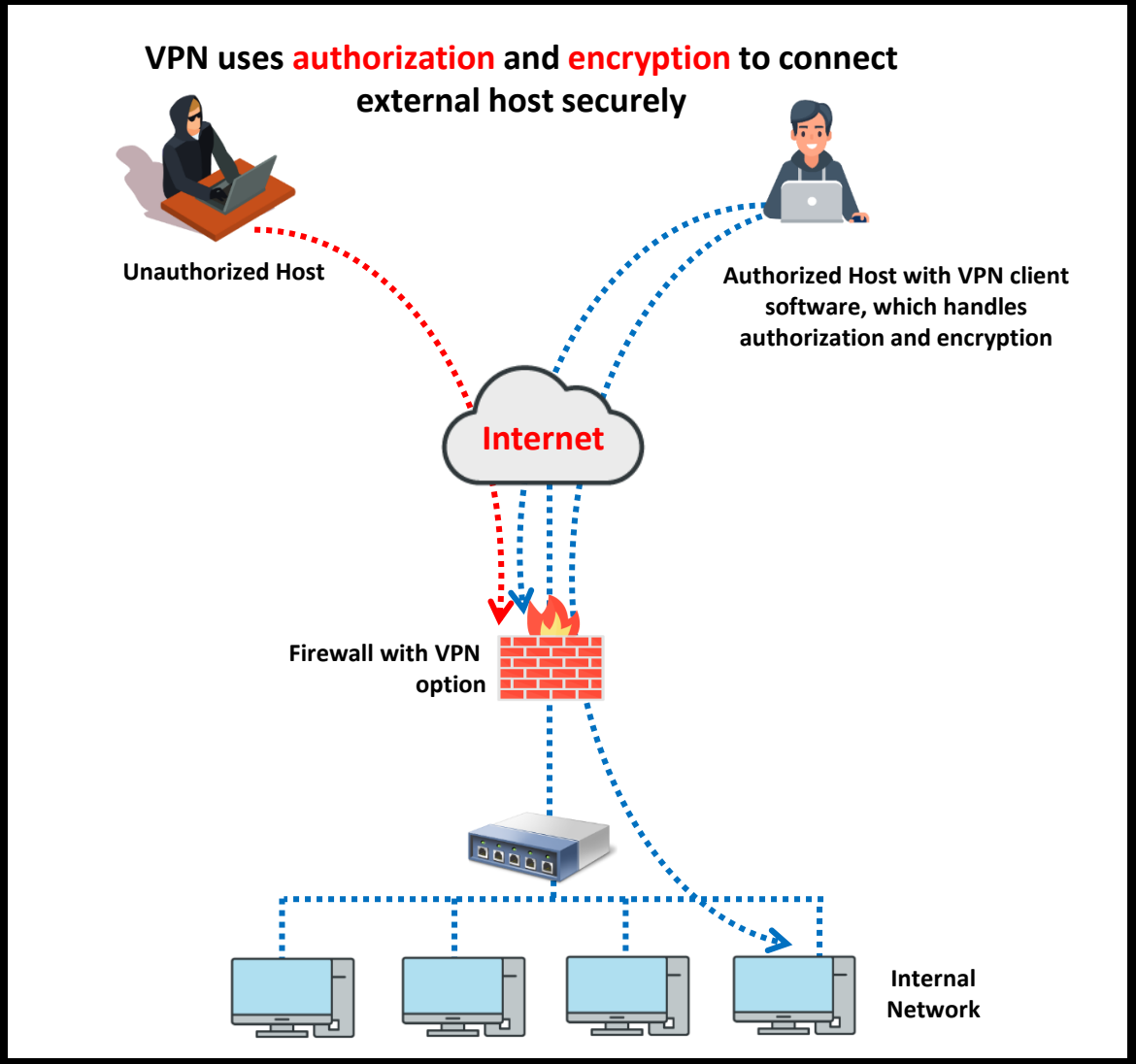



- VPNs are used to **securely communicate** with different computers over insecure channels
- A VPN use the Internet and ensures secure communication to distant offices or users within the **enterprise's network**



# How VPN Works

- A client willing to connect to a company's network initially connects to the Internet
- Then, the client initiates a **VPN connection** with the company's server
- Before establishing a connection, end points must be **authenticated** through passwords, biometrics, personal data, or any combination of these
- Once the connection is established, the client can **securely access** the company's network






# Why Establish VPN?

**A well-designed VPN provides the following benefits:**

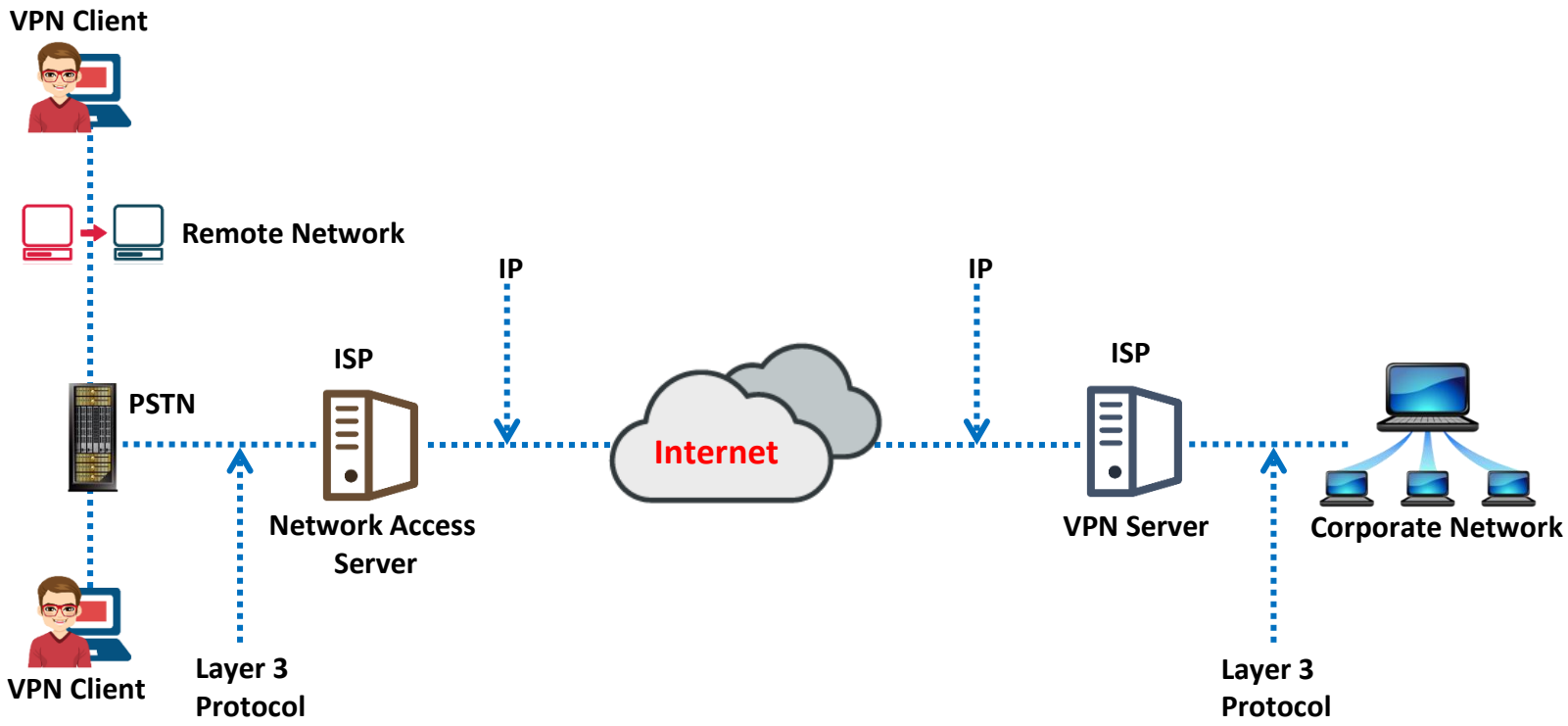
- ✓ Extend **geographic connectivity**
- ✓ Reduce **operational costs** versus traditional WANs
- ✓ Reduce **transit times** and traveling costs for remote users
- ✓ Improve **productivity**
- ✓ Simplify **network topology**
- ✓ Provide **global networking** opportunities

# VPN Components

## VPN Components

- ✓ VPN client
- ✓ Network access server (NAS)
- ✓ Tunnel Terminating Device (or VPN server)
- ✓ VPN protocol

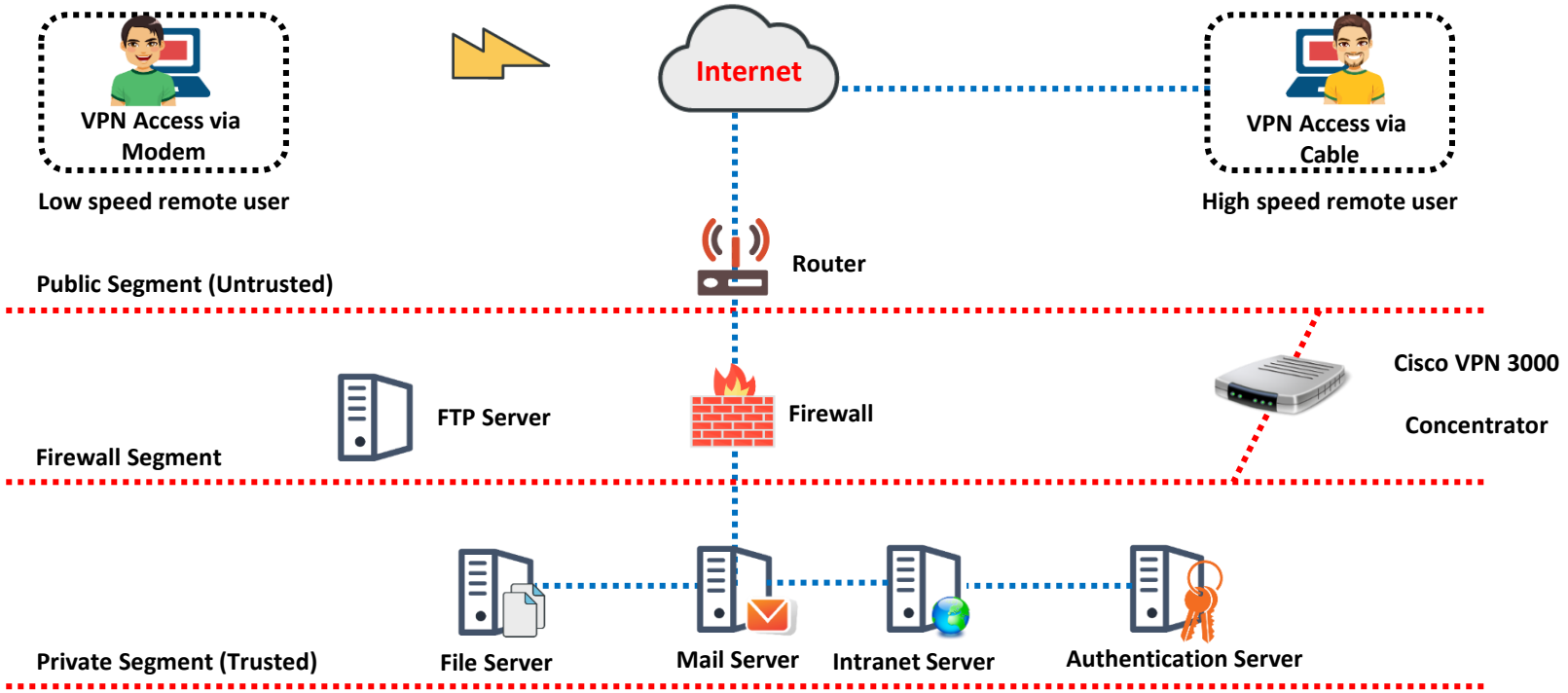


# VPN Concentrators

- A VPN Concentrator is a network device used to create **secure VPN connections**
- It acts as a VPN router which is generally used to create a remote access or **site-to-site** VPN
- It uses tunnelling protocols to **negotiate security** parameters, create and manage tunnels, encapsulate, transmit, or receive packets through the tunnel, and de-encapsulate them








# Functions of a VPN Concentrator

- A VPN Concentrator functions as a **bi-directional** tunnel endpoint

## The VPN Concentrator functions are:

01 Encrypts and decrypts data

02 Authenticates users

03 Manages data transfer across the tunnel

04 Negotiates tunnel parameters



05 Manages security keys

06 Establishes Tunnels

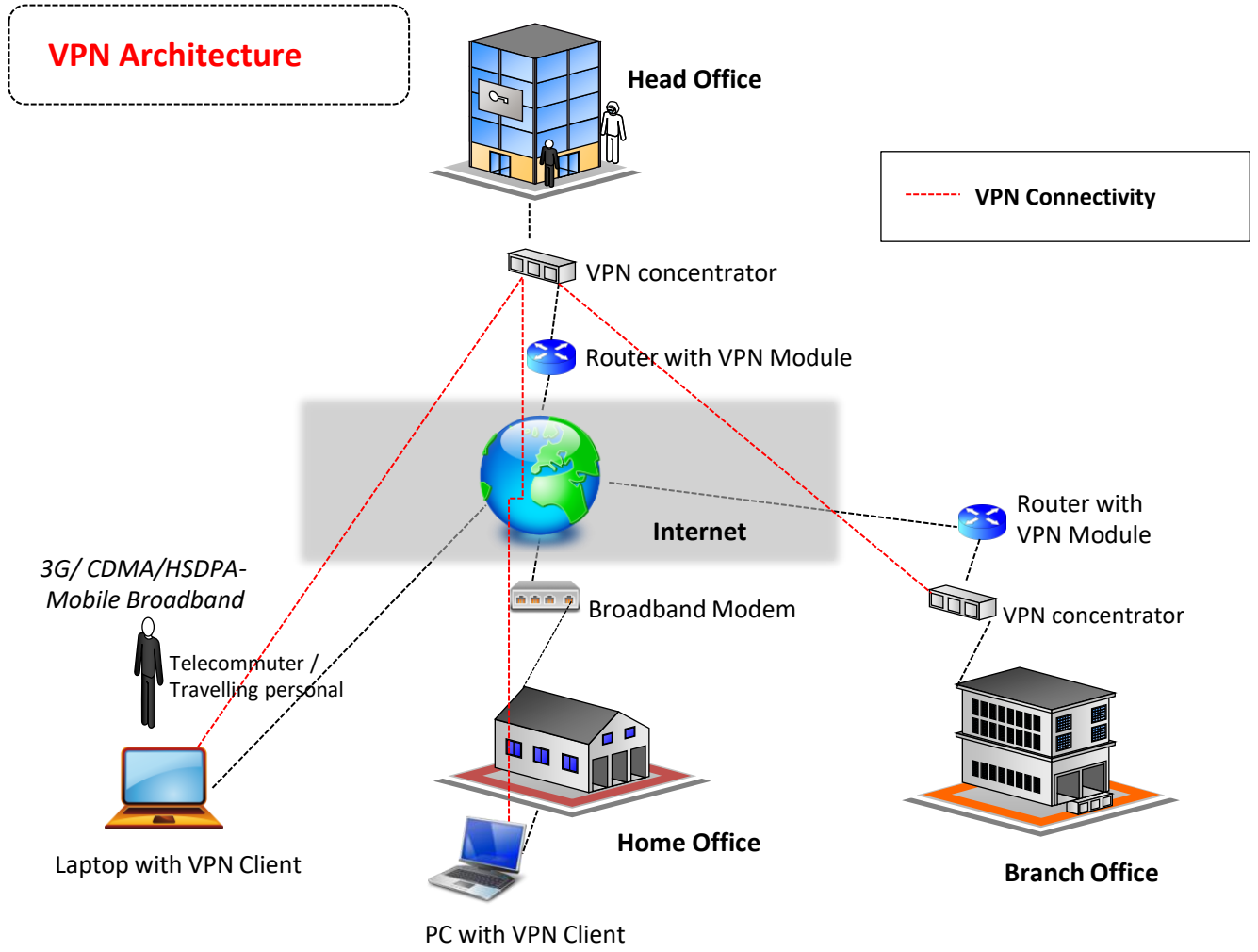
07 Assigns user addresses

08 Manages inbound and outbound data transfers as a tunnel endpoint or router

# VPN Types and Categories

# Client-to-Site (Remote-access) VPNs

- Remote-Access VPNs allow **individual hosts** or clients, such as telecommuters and mobile users to establish secure connections to a company's network over the Internet
- Each host contains VPN client software or uses a **web-based** client
- The VPN **encrypts** the data packets that are forwarded over the Internet to the VPN gateway at the edge of the target network, with the software installed on the client's machine
- A **VPN Gateway** receives the packets and then closes the connection to the VPN after transfer is complete

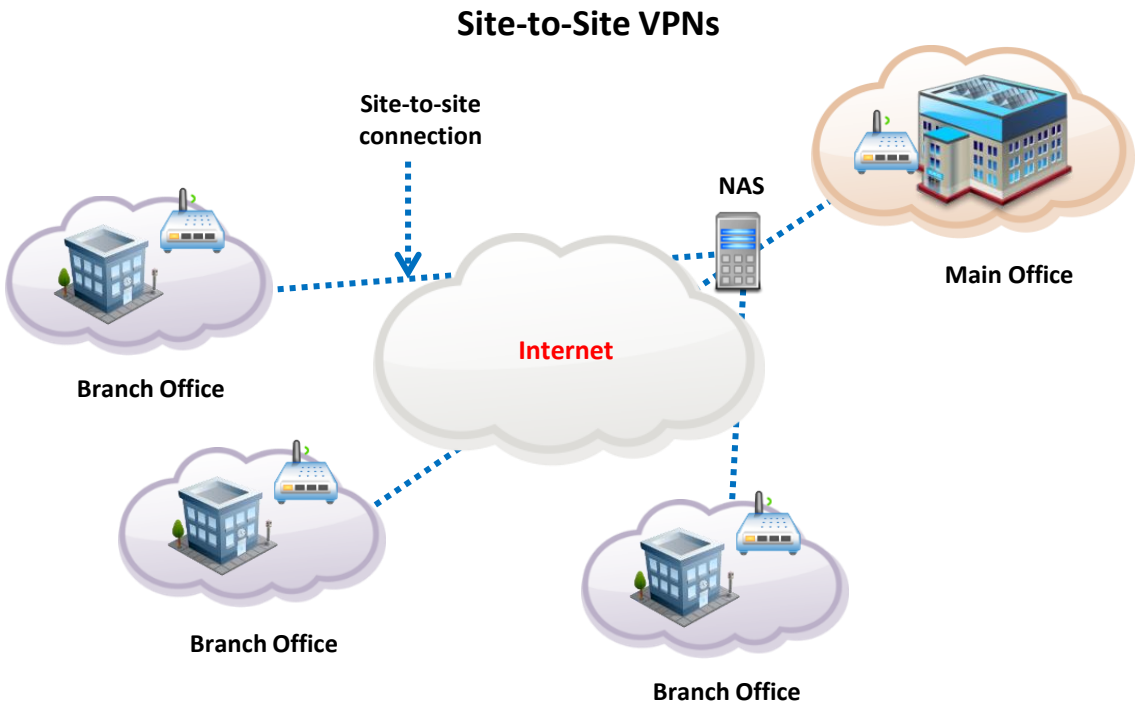


# Site-to-Site VPNs

Site-to-site VPN is classified in two types:

- **Intranet-based**: VPN connectivity is between sites of a **single organization**
- **Extranet-based**: VPN connectivity is between **different organizations** such as business partners, business, and its clients

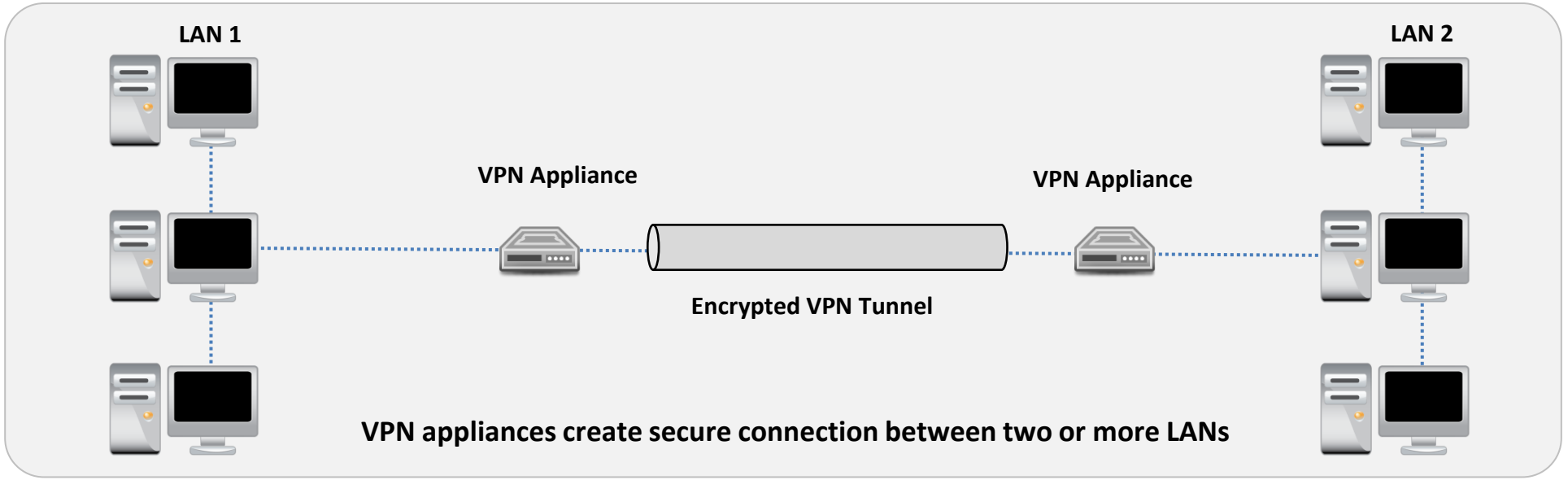
- Site-to-site VPN extends the **company's network**, allows access of an organization's network resources from different locations
- It connects a **branch** or remote office network to the **company's headquarters** network
- Also known as **LAN-to-LAN** or L2L VPNs



# Hardware VPNs

- A dedicated hardware VPN appliance is used to connect **routers** and **gateways** to ensure communication over an insecure channel
- It is designed to serve as a VPN endpoint and can connect to multiple LANs



# Hardware VPN Products

| Manufacturer | Product Name | Web Site |
|---|---|---|
| Cisco Systems | VPN 3000 series concentrators, VPN 3002 Hardware Clients, 7600 series routers, and Web VPN Services Module | *https://www.cisco.com* |
| SonicWALL | SonicWALL PRO 5060,4060,3060,2040,1260 | *https://www.sonicwall.com* |
| Juniper Networks | NetScreen 5000, 500,200, and ISG series | *https://www.juniper.net* |
| WatchGuard | WatchGuard Firebox X series | *https://www.watchguard.com* |



# Software VPNs

- VPN software is **installed** and **configured** on routers, servers and firewalls or as a gateway that functions as a VPN

## Advantages

- **No extra devices** need to be installed
- It is an **easy and low-cost way** to deploy a VPN and does not change the target network



## Disadvantages



- **Extra processing** burden to devices on which it is installed
- It is **less secure** and prone to attacks

# Software VPN Products

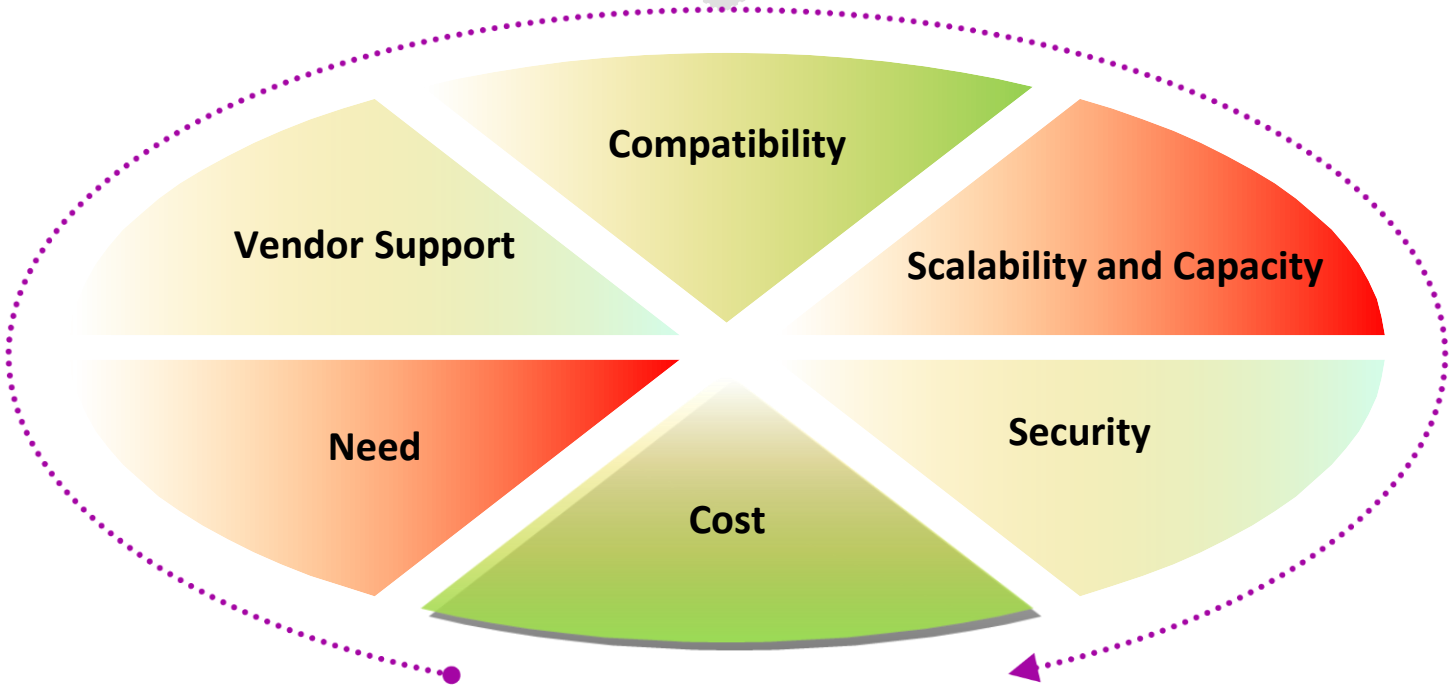
| Manufacturer | Product Name | Web Site |
|---|---|---|
| CheckPoint | VPN-1 VSX,VPN-1 Pro, VPN-1 Edge, Firewall-1 | *https://www.checkpoint.com* |
| NETGEAR | ProSafe VPN | *https://www.netgear.com* |
| Cisco Systems | Cisco AnyConnect Secure Mobility Client | *https://www.cisco.com* |



# Selecting an Appropriate VPN

- Choose the **best possible VPN solution** for your enterprise

**Choose the type of VPN solution based on**



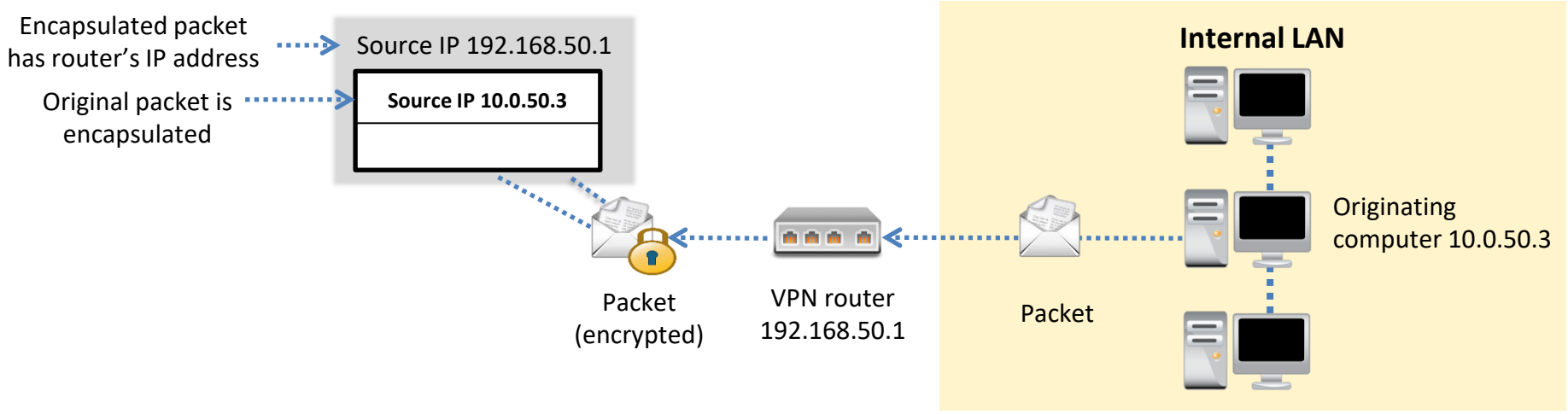



# VPN Core Functionality: Encapsulation

- Packets over a VPN are **enclosed** within another packet (encapsulation) which has a different IP source and destination
- Concealing the source and destination of the packets protects the **integrity** of the data sent
- The most common VPN encapsulation protocols:
  - Point-to-Point Tunneling Protocol (PPTP)
  - Layer 2 Tunneling Protocol (L2TP)
  - Secure Shell (SSH)
  - Socket Secure (SOCKS)



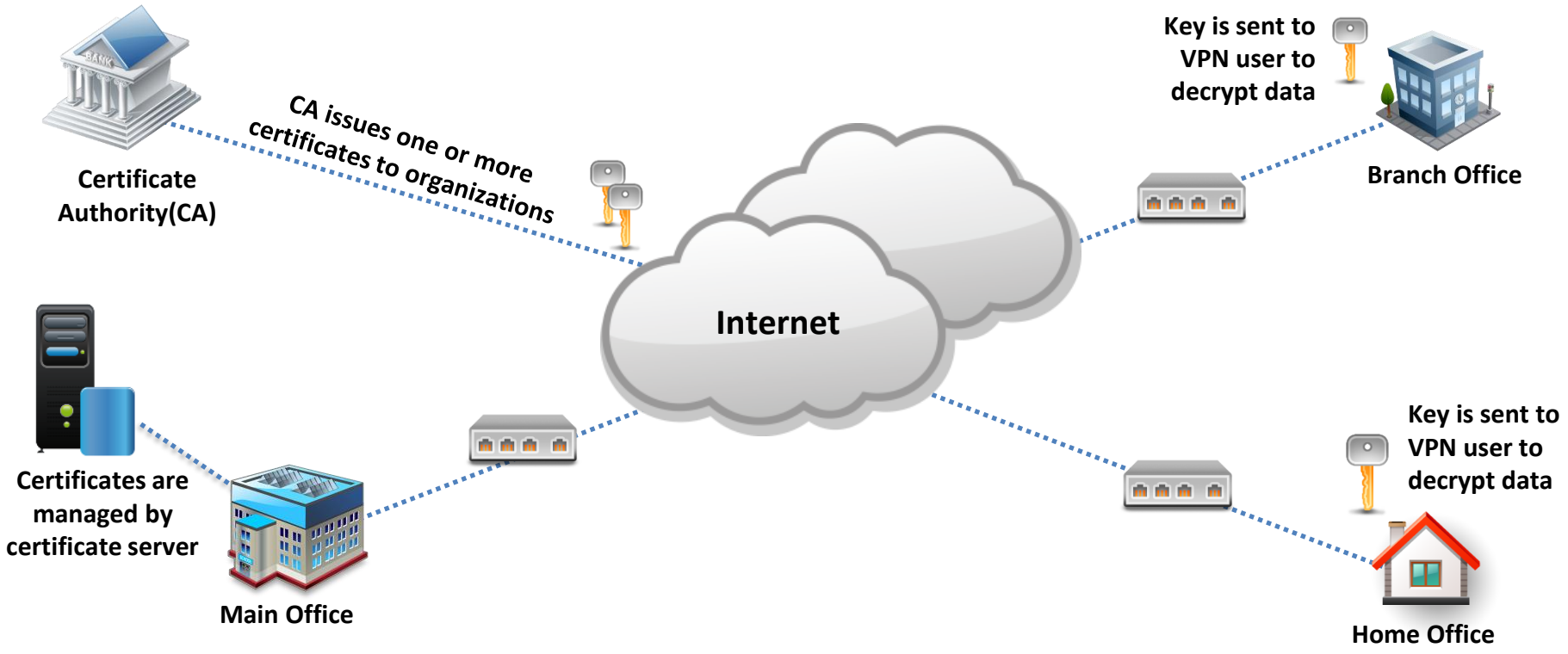
**Encapsulating data to conceal source and destination information**



# VPN Core Functionality: Encryption

- Packets sent over a VPN are **encrypted** to maintain the confidentially of the information
- Packets are read by decrypting with the **encryption key** from the sender

- **Common VPN Encryption Technologies**
  - Triple Data Encryption Standard (3DES)
  - Secure Sockets Layer (SSL)
  - Open VPN

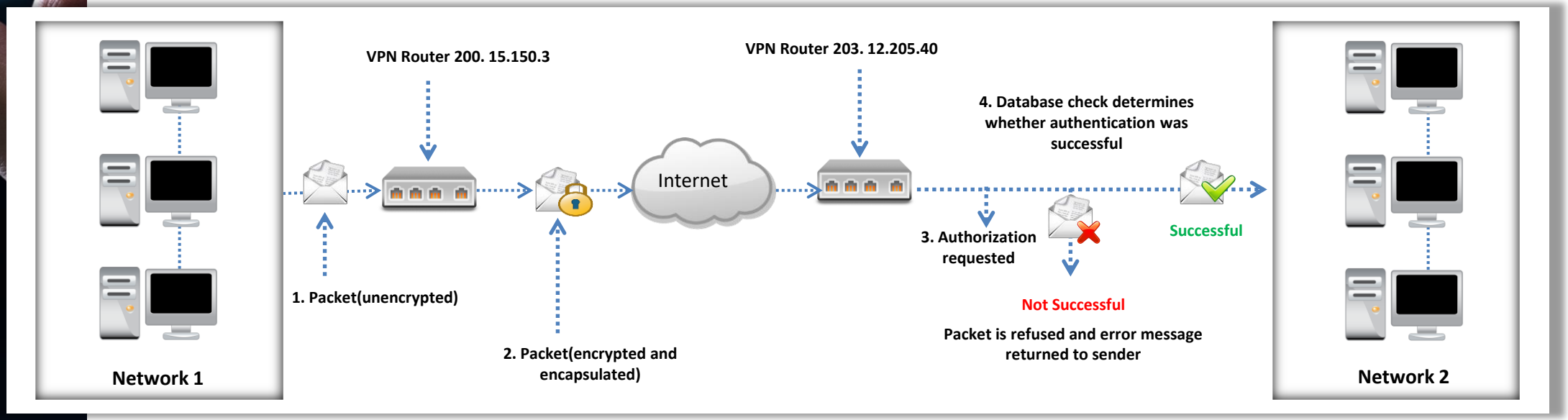




# VPN Core Functionality: Authentication

- Users are **authenticated** to access the VPN and its resources
- It uses **digital certificates** to authenticate users
- Common user authentication techniques for a VPN
  - IPSec
  - MS-CHAP
  - Kerberos





# VPN Technologies

## 01 Trusted VPNs

- Were used before the **Internet** became **universal**
- Companies leased circuits from a communications provider and used them the same way as **physical cables** in a private LAN
- Organization`s know and control the pathway for their transmission
- A customer trusted communication provider maintains the integrity and security but not the encryption, these are called Trusted VPNs
- Technologies such as **ATM** circuits, **frame-relay** circuits, Multiprotocol Label Switching (MPLS) are used to implement trusted VPNs

## Secure VPNs 02

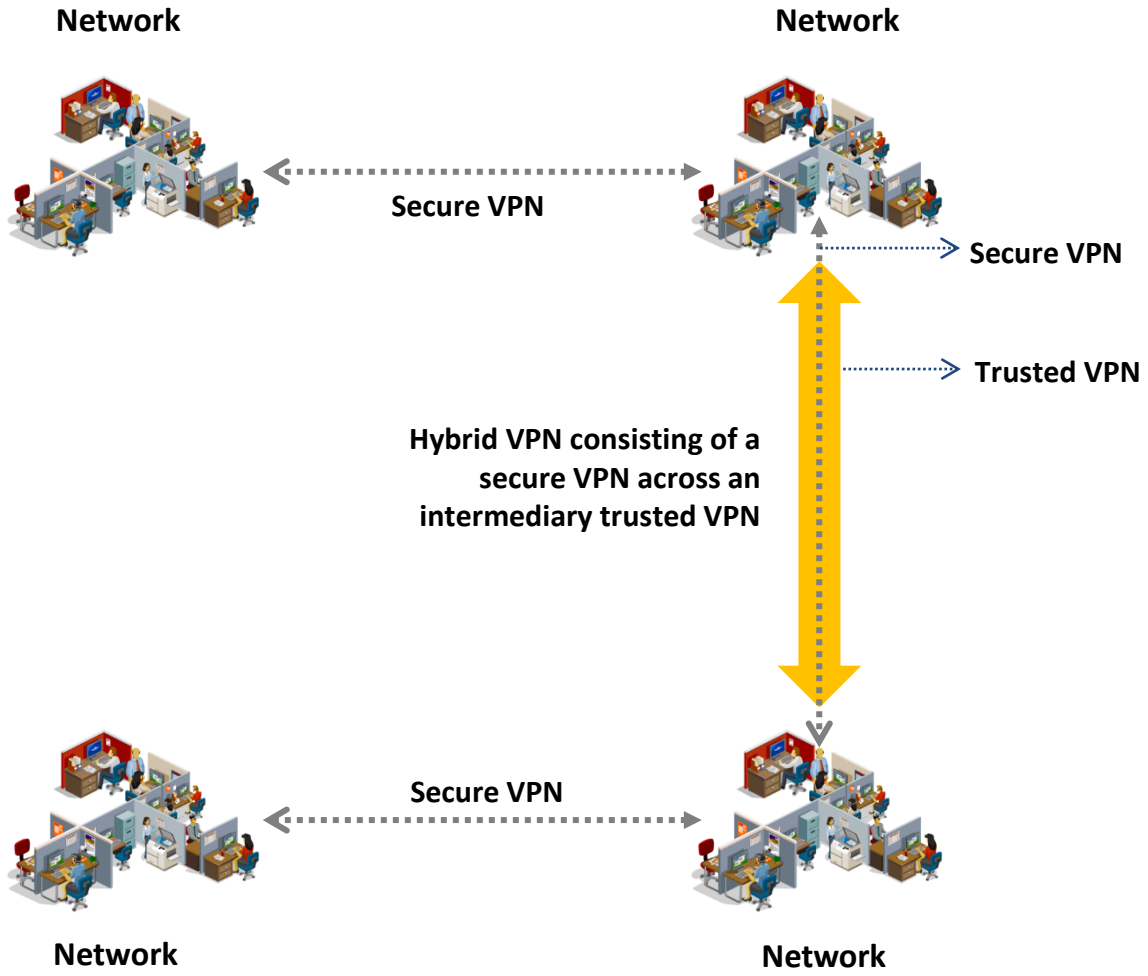
- Used when the **Internet** became a corporate **communications medium**
- Vendors created a protocol which encrypts the traffic at the originating computer and decrypts at the receiving computer
- The **encrypted** traffic acts as a tunnel between two networks, even if an attacker sees the traffic will not be able to read it
- Secure VPNs are networks constructed using encryption
- They protect the **confidentiality** and **integrity** of the data, but do not ensure the transmission path

# VPN Technologies (Cont'd)

03

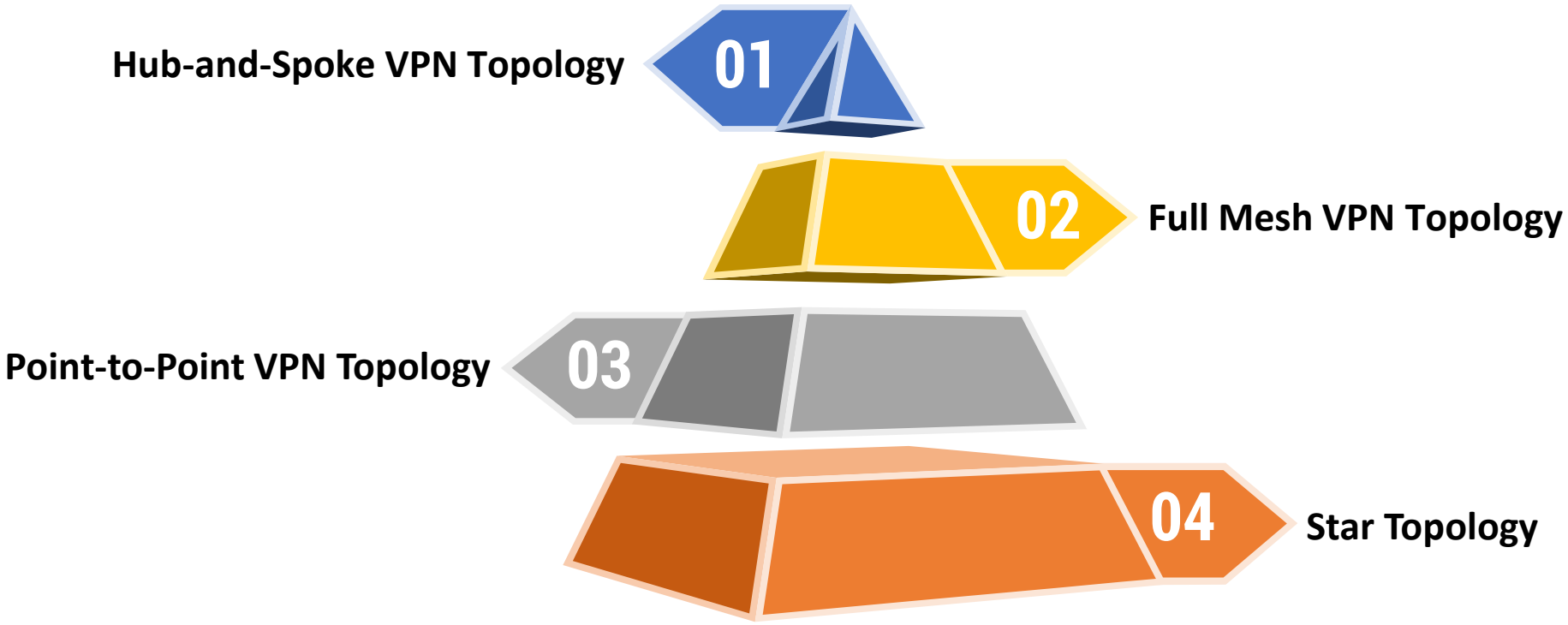
## Hybrid VPNs

- A secure VPN is part of a trusted VPN, creating a hybrid VPN
- The secure part of a hybrid VPN is administered by the **customer** or the **provider**, who has provided the trusted part of the hybrid VPN



# VPN Topologies

- A VPN topology specifies how the **peers** and **networks** within a VPN are connected
- Some VPN topologies include

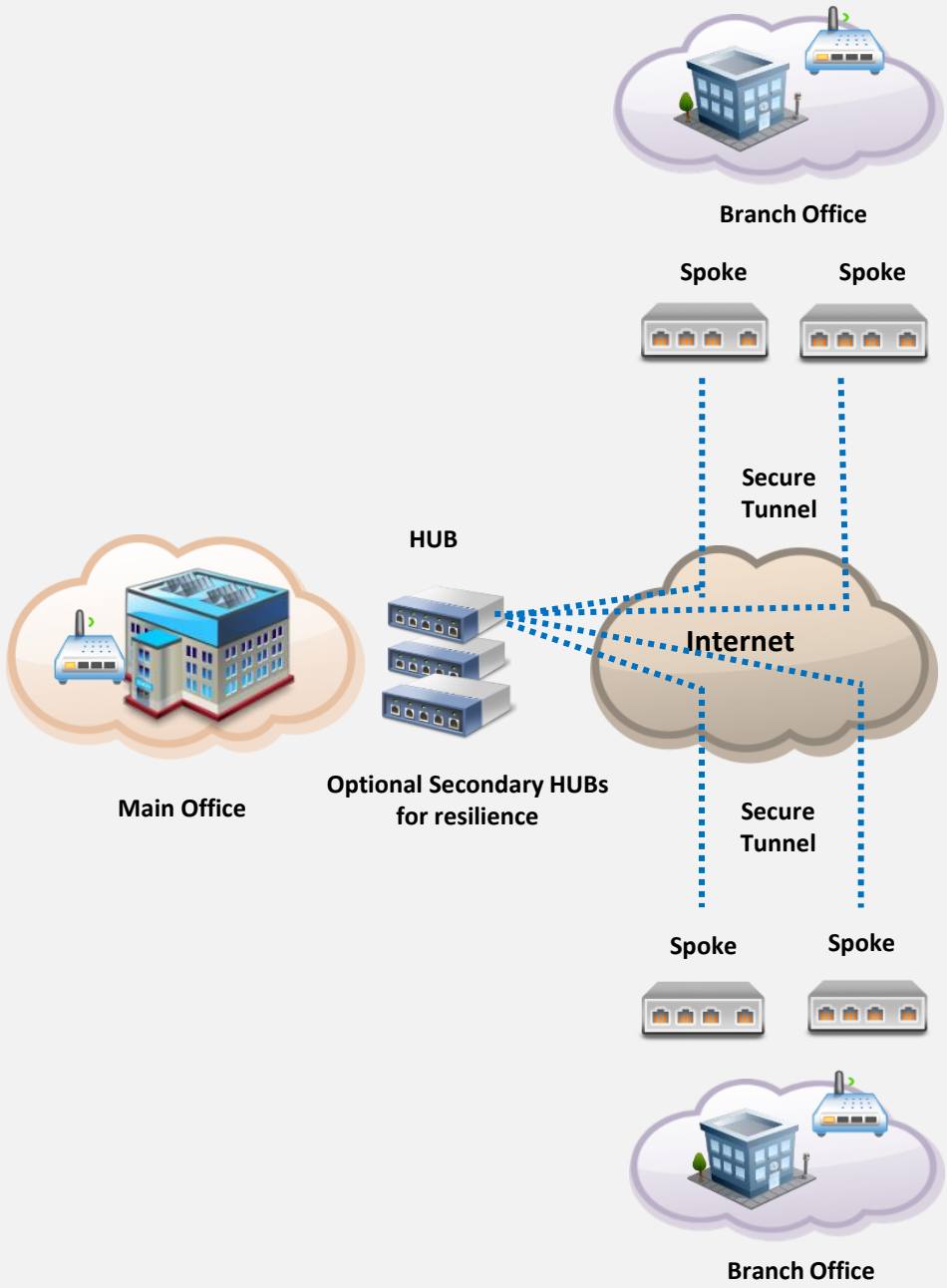


# Hub-and-Spoke VPN Topology

Each individual spoke connected to the remote office is communicated securely with the **central device** (hub)

A separate and secure tunnel is **established** between the hub and each individual spoke

A **persistent connection** is established between an organization's main office and their branch offices using a third-party network or the Internet



# Point-to-Point VPN Topology

**1**

Unlike the Hub-and-Spoke topology, offices at different locations can directly communicate with each other without any **IPsec failover**

**2**

This topology treats two end points as two **peer devices** participating in communication

**3**

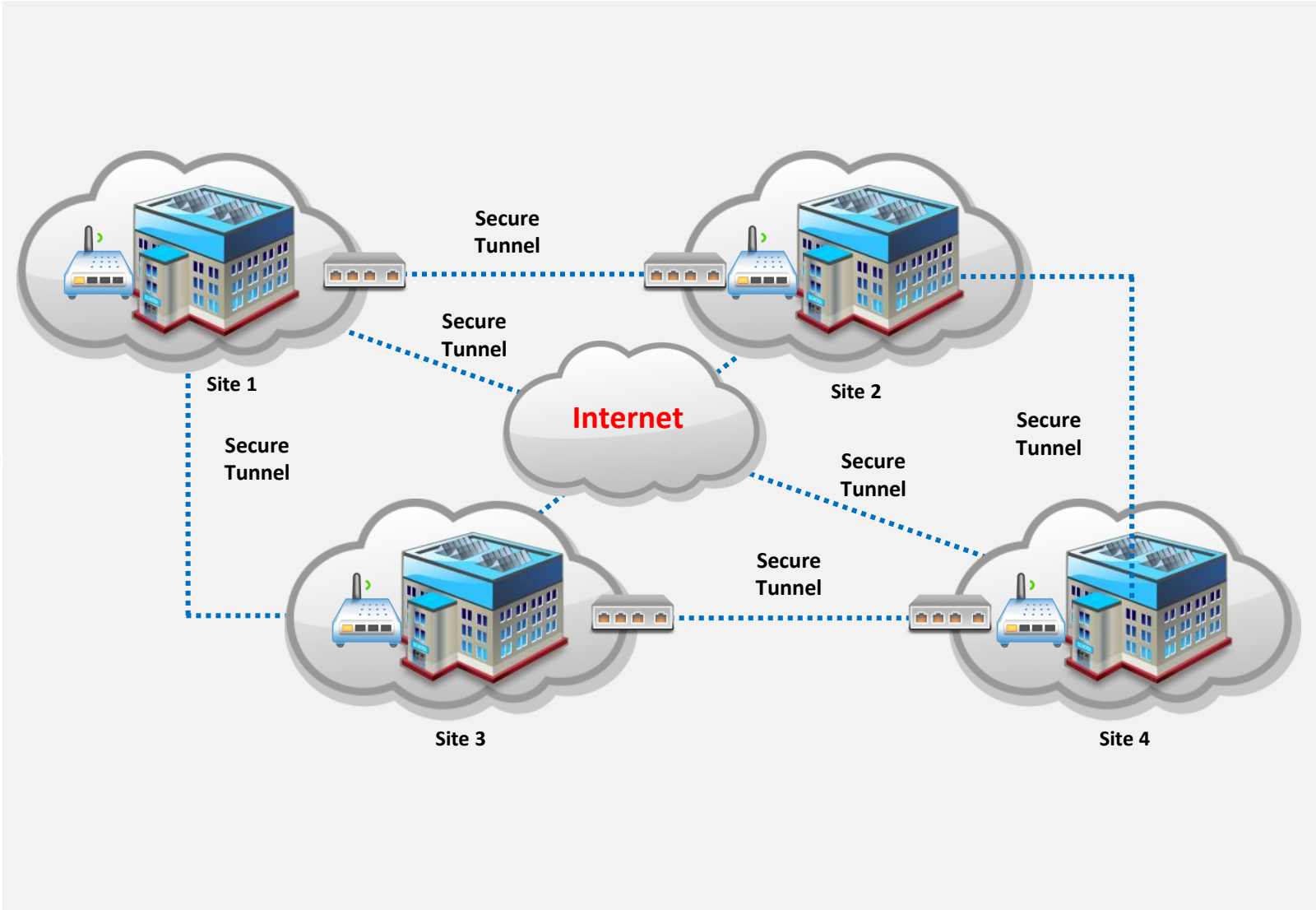
Only Regular IPsec or IPsec/GRE is assigned for the tunnel, as any of the **peer devices** can initiate the communication

**Point-to-point VPN Topology**



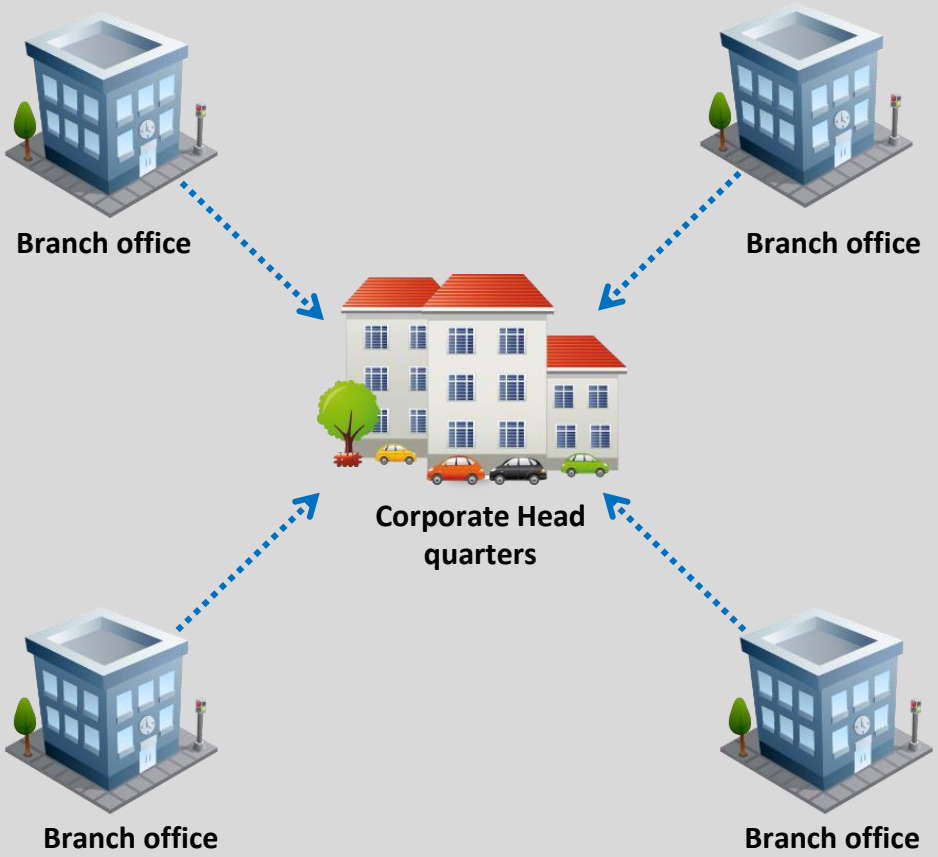
# Full Mesh VPN Topology

- This topology is suitable for complicated networks where all **peers communicate** with one another
- Device to device communication in a network takes place with a unique IPsec tunnel
- A peer-to-peer connection is established between each device, preventing a **bottleneck** at the VPN gateway and saving encryption/decryption overhead
- This topology is reliable and offers **redundancy**



# Star Topology

- This topology allows remote branches to **securely communicate** with corporate headquarters
- **Interconnection** between branches is not allowed
- Deployed in a bank network, preventing one branch from compromising another branch
- Attackers must first **compromise** the central network before being able to compromise a second branch
- New sites can be **added** easily and only the central sites needs to be updated
- The central site plays a major role in this **topology**. If it fails, all connections go down

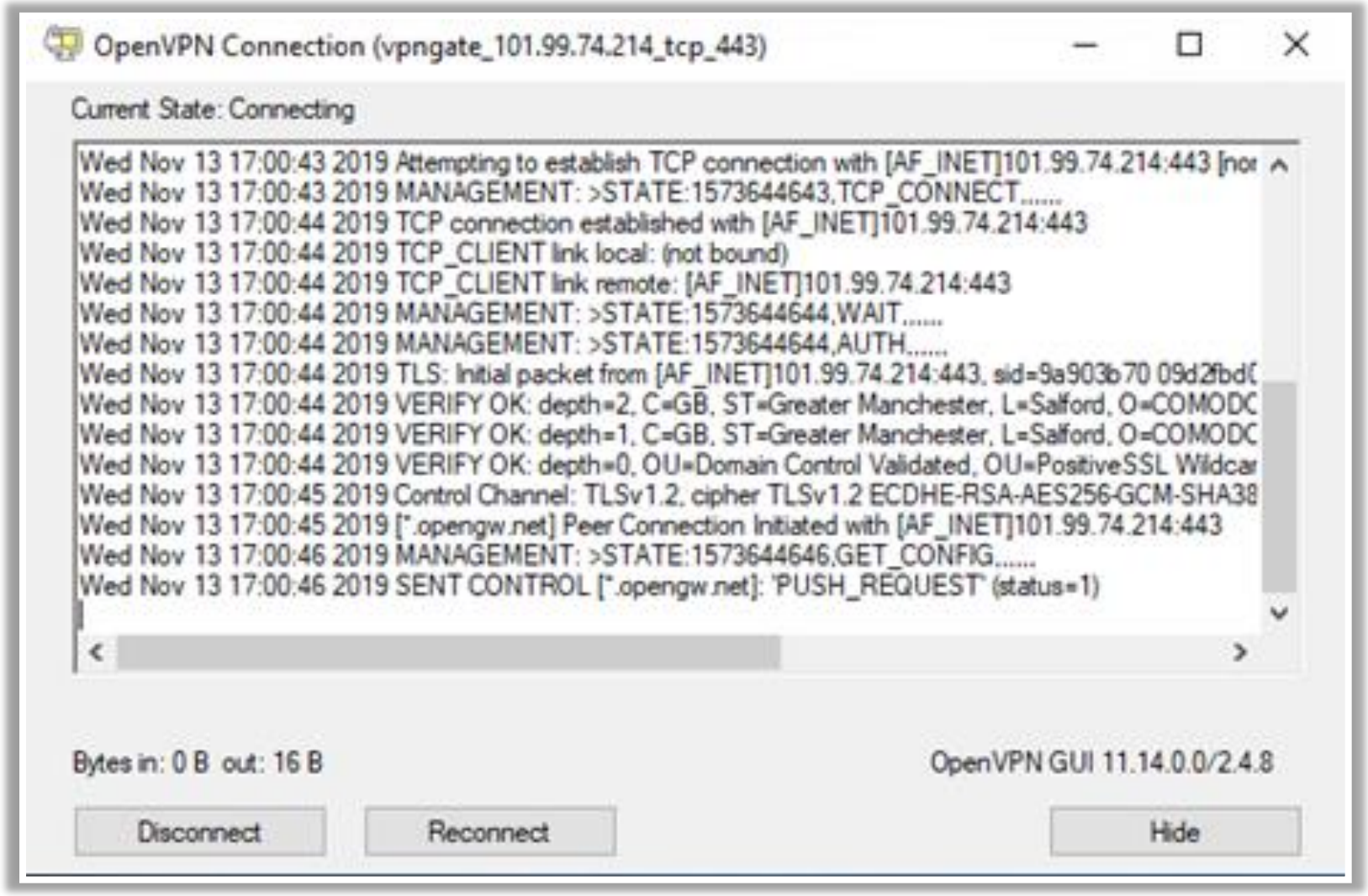





# Example of a VPN: OpenVPN

- OpenVPN provides flexible VPN solutions **to secure data communications** for Internet privacy, remote access for employees, securing IoT, or for networking Cloud data centers

- It is a VPN server software solution that can be deployed **on-premises** using standard servers or **virtual appliances**, or **on the cloud**




*https://openvpn.net*

# VPN Security Risks

01 VPN Fingerprinting

02 Insecure Storage of Authentication Credentials

03 Username Enumeration Vulnerabilities

04 Offline Password Cracking



05 Man-in-the-Middle Attacks

06 Lack of Account Lockout

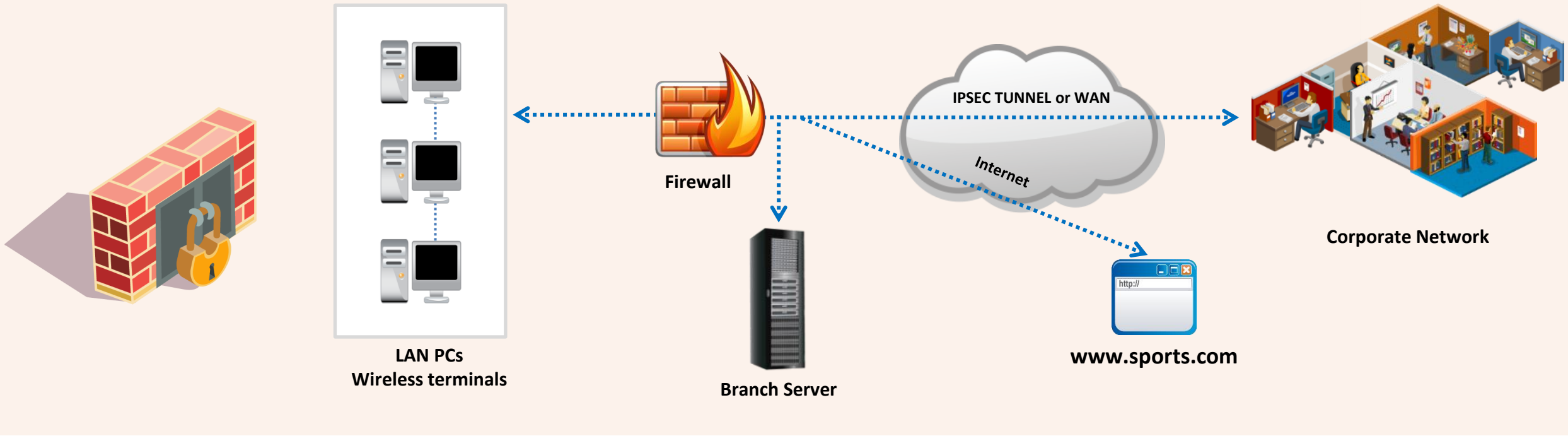
07 Poor Default Configurations

08 Poor Guidance and Documentation

# VPN Security

# Firewalls

- Firewalls establish a protection barrier between the VPN and the Internet
- Before implementing a VPN, ensure that a **good firewall** is in place
- Firewalls should be configured to restrict open **ports**, the types of **packets** and **protocols** that traffic is allowed to pass through to the VPN



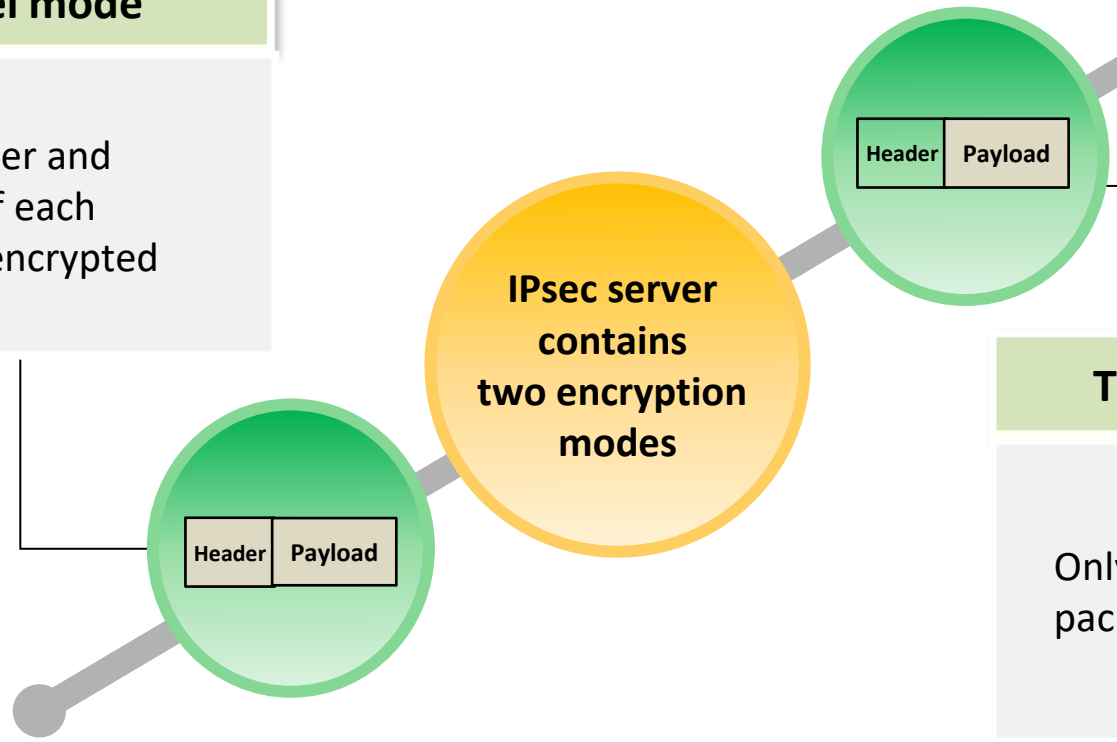
# IPsec Server

- The IPsec server enhances VPN security through the use of strong **encryption algorithms** and authentication



**Tunnel mode**

Both header and payload of each packet is encrypted




**Transport mode**

Only payload of each packet is encrypted

# AAA Server

</> ❑ The AAA server is used to establish secure access in a **remote-access** VPN environment

## AAA server performs the following types of checks



### Authentication

- Who are you ?



### Authorization

- What are you allowed to do?



### Accounting

- What do you actually do?

# Remote Access Dial-In User Service

1. Remote Access Dial-In User Service (**RADIUS**) is the simplest way to use centralized authentication in VPNs

2. RADIUS is a **software application** that runs on a server and has access to all users in the domain

3. In a VPN environment, RADIUS manages both the user authentication and authorization. This reduces the total cost of ownership by managing the credentials from a **central location**

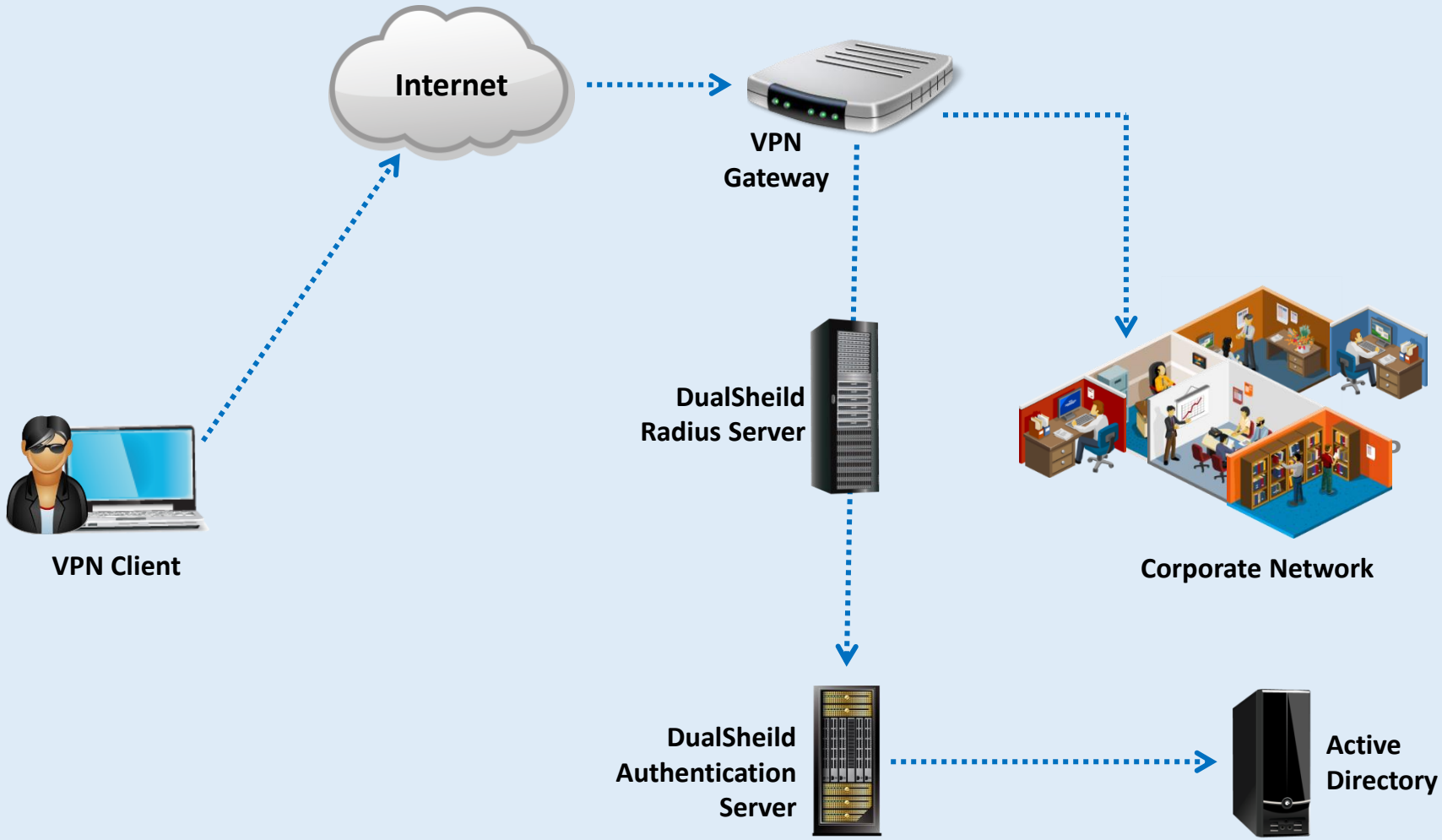
4. When a user attempts to connect the VPN server contacts the RADIUS server who then authenticates the user through a **Windows domain** using both a username and a password (typically a Windows domain controller)

5. If the username and password are correct and they have “**dial-in**” access granted they will be allowed to access the VPN

6. The VPN equipment must securely communicate with the RADIUS server and verify the user meets certain set conditions, before granting **permission** to access the network



# Remote Access Dial-In User Service (Cont'd)





# Connection to VPN: SSH and PPP

- PPP and SSH are **integrated in kernels** that use VPN
- VPNs using PPP and SSH work well with **dynamic IP addresses**



## Configuring Network Connection

While configuring **multiple tunnels** to the computer, ensure that **IP address** of every tunnel is unique

Client and server contain **PPP processes** to communicate

PPP processes communicate using **SSH connection**

# Connection to VPN: SSL and PPP

- **Point-to-point protocol** over a secure socket layer connection
- **Secure Socket Layer**
  - Built-in support for host authentication through digital certificates
- Establishing a **network connection**
  - Initial handshake for secure communication
  - "**Hello**" messages establish:
    - **SSL Version**, support for Cipher suites, and some random data
  - Key is determined separately from handshake
  - Data transferred over the link



# Connection to VPN: Concentrator

## Concentrator

- Expert mechanism that allows connections from **VPN peers**
- Validates its clients
- Insists on **security policies** of VPN
- Reduces operating cost of **VPN administration** and encryption from gateways, local hosts

## Configuring Network Connection

- **Configure** the concentrator
- Set up **client software**
- To use VPN, client should use client software



# Module Flow

1. Understand Different Types of Network Segmentation
2. Understand Different Types of Firewalls and their Role
3. Understand Different Types of IDS/IPS and their Role
4. Understand Different Types of Honeypots
5. Understand Different Types of Proxy Servers and their Benefits
6. Discuss Fundamentals of VPN and its importance in Network Security
7. Discuss Security Incident and Event Management (SIEM)
8. Discuss User Behavior Analytics (UBA)
9. Understand Various Antivirus/Anti-malware Software

# Security Incident and Event Management (SIEM)

1

- SIEM performs **real-time SOC** (Security Operations Center) functions like identifying, monitoring, recording, auditing, and analyzing security incidents

2

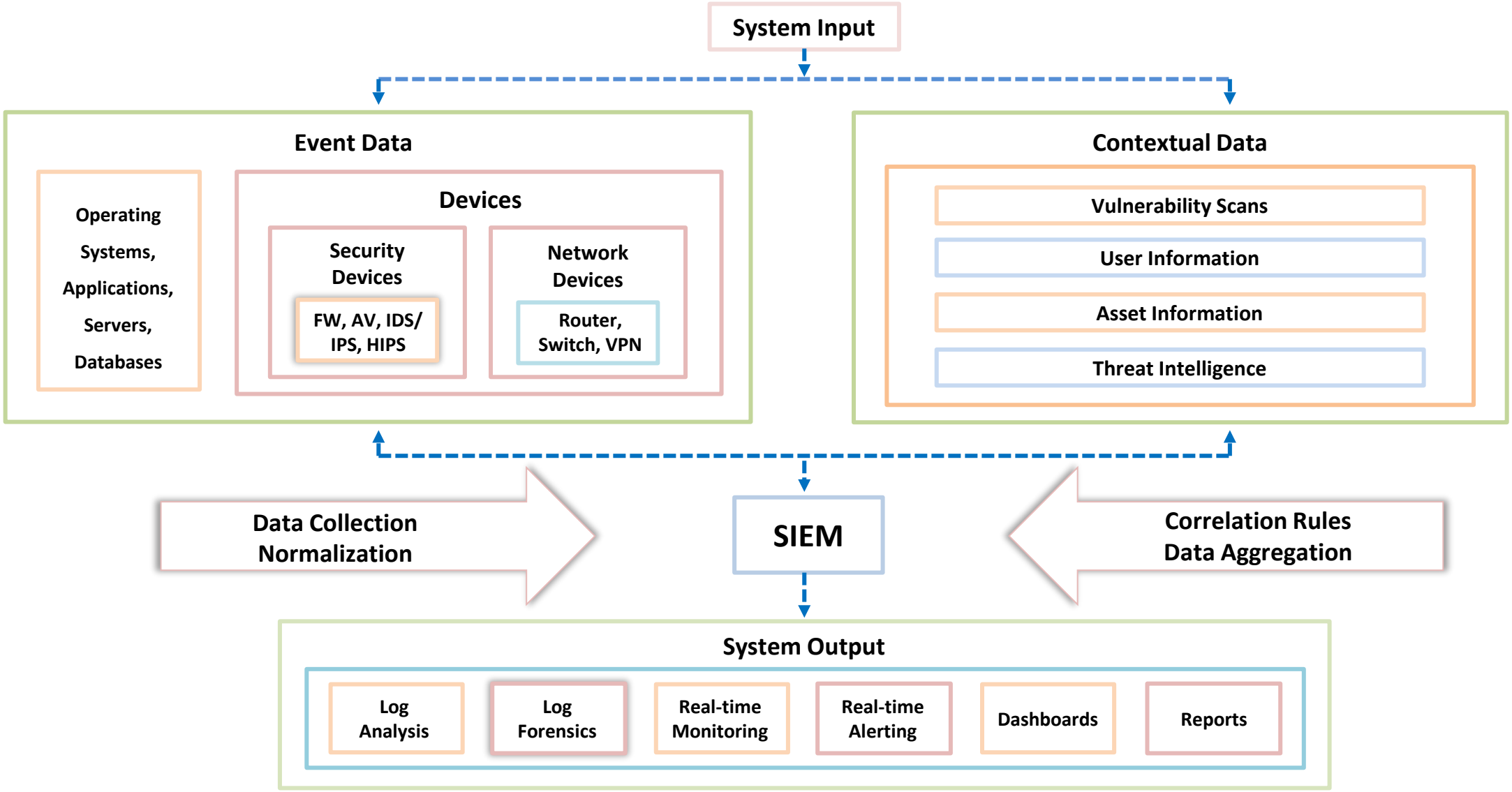
- It provides security by **tracking suspicious end-user behavior** activities within a real-time IT environment

3

- It provides security management services combining **Security Information Management** (SIM), and **Security Event Management** (SEM)
  - ✓ SIM supports permanent storage, analysis and reporting of log data
  - ✓ SEM deals with real-time monitoring, correlation of events, notifications, and console views



# SIEM Architecture



# SIEM Functions

1. Log Collection and Log Analysis
2. Event Correlation
3. Log Forensics
4. IT Compliance and Reporting
5. Application Log Monitoring
6. Object Access Auditing

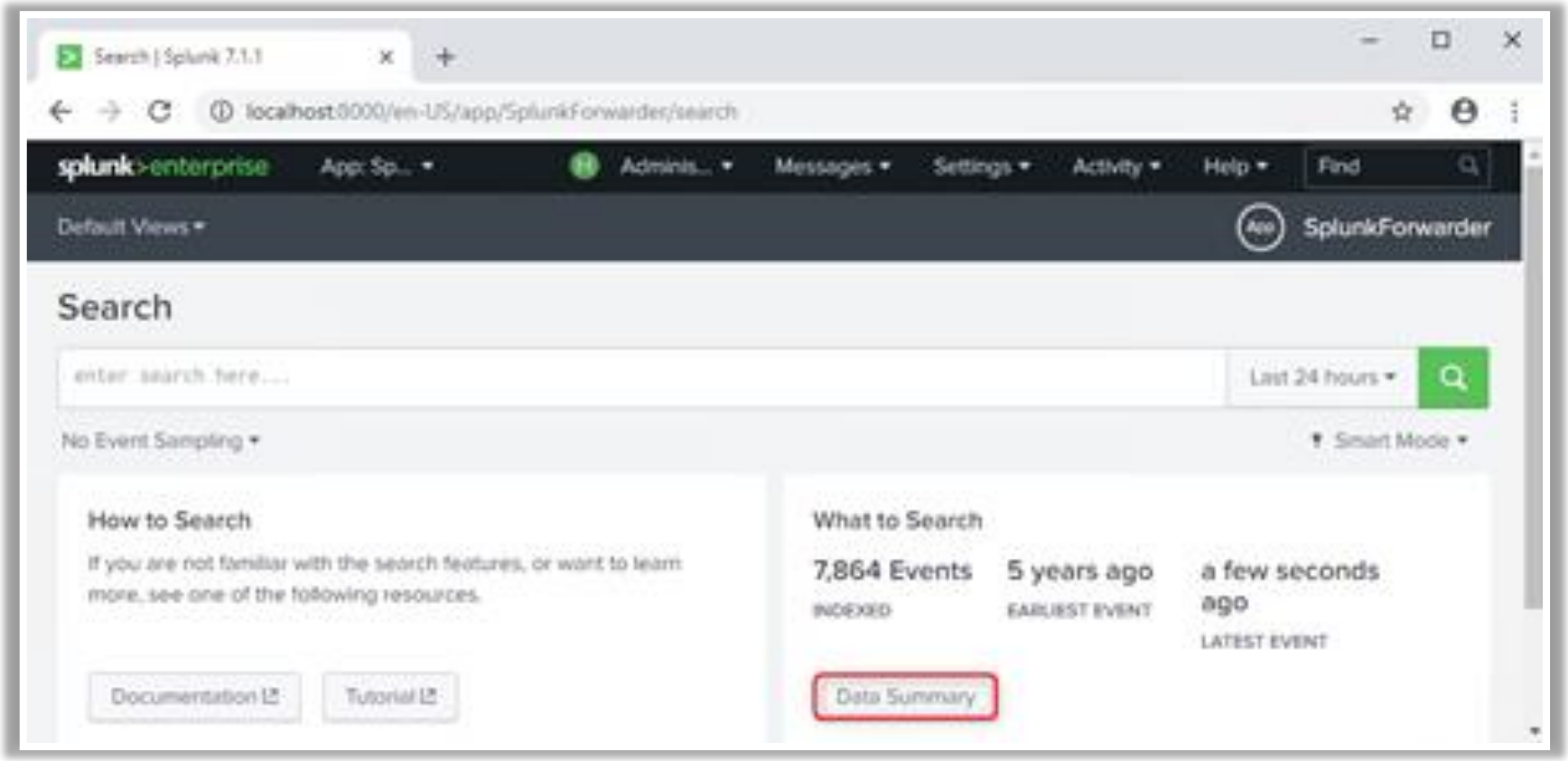


7. Data Aggregation
8. Real-time Alerting
9. User Activity Monitoring and Dashboards
10. File Integrity Monitoring
11. System and Device Log Monitoring
12. Log Retention

# SIEM Solutions

**Splunk ES**

An analytics driven SEIM solution that provides you with what you need to detect and **respond to internal** and **external attacks** quickly




*https://www.splunk.com*

**ArcSight ESM**
***https://www.microfocus.com***

**IBM Qradar SIEM**
***https://www.ibm.com***

**AlienVault OSSIM**
***https://cybersecurity.att.com***

**FortiSIEM**
***https://www.fortinet.com***

**SolarWinds Security Event Manager (SEM)**
***https://www.solarwinds.com***

# Module Flow

1. Understand Different Types of Network Segmentation
2. Understand Different Types of Firewalls and their Role
3. Understand Different Types of IDS/IPS and their Role
4. Understand Different Types of Honeypots
5. Understand Different Types of Proxy Servers and their Benefits
6. Discuss Fundamentals of VPN and its importance in Network Security
7. Discuss Security Incident and Event Management (SIEM)
8. **Discuss User Behavior Analytics (UBA)**
9. Understand Various Antivirus/Anti-malware Software

# User Behavior Analytics (UBA)

01 UBA is the process of **tracking user behavior** to detect malicious attacks, potential threats, and financial fraud

02 It provides **advanced threat detection** in an organization to monitor specific behavioral characteristics of employees

03 UBA technologies are designed to **identify variations** in **traffic patterns** caused by user behaviors which can be either disgruntled employees or malicious attackers



# Why User Behavior Analytics is Effective?

1

Detects malicious insiders and outsiders at an early stage

2

Identifies possible risk events in the IT infrastructure

3

Analyzes different patterns of human behavior and large volumes of user's data

4

Monitors geo-location for each login attempt

5

Detects malicious behavior and reduces risk

6

Monitors privileged accounts and provides real time alerts for suspicious behavior

7

Provides insights to security teams

8

Produces results soon after deployment

# UBA/UEBA Tools

- User Behavior Analytics (UBA)/User and Entity Behavior (UEBA) Tools collect user activity details from multiple sources and **use artificial intelligence and machine learning (AI/ML)** algorithms to perform user behavior analysis to prevent and detect various threats before the fraud is perpetrated



**Exabeam Advanced Analytics**
*https://www.exabeam.com*

**LogRhythm UEBA**
*https://logrhythm.com*

**Dtex Systems**
*https://dtexsystems.com*

**Gurucul Risk Analytics (GRA)**
*https://gurucul.com*

**Securonix UEBA**
*https://www.securonix.com*

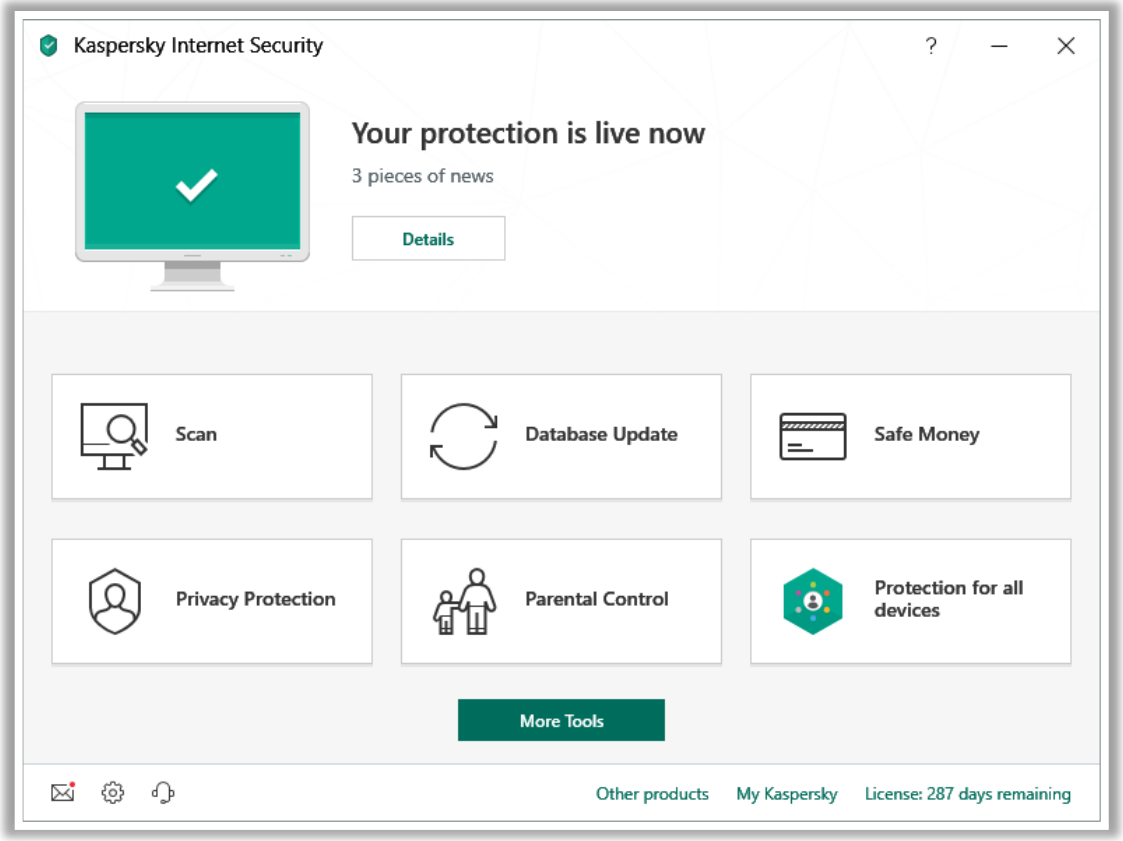
# Module Flow

1. Understand Different Types of Network Segmentation
2. Understand Different Types of Firewalls and their Role
3. Understand Different Types of IDS/IPS and their Role
4. Understand Different Types of Honeypots
5. Understand Different Types of Proxy Servers and their Benefits
6. Discuss Fundamentals of VPN and its importance in Network Security
7. Discuss Security Incident and Event Management (SIEM)
8. Discuss User Behavior Analytics (UBA)
9. Understand Various Antivirus/Anti-malware Software

# Anti-Trojan Software

**Kaspersky Internet Security**

**Kaspersky Internet Security** provides protection against Trojans, viruses, spyware, ransomware, phishing, and dangerous websites




*https://www.kaspersky.com*

**McAfee® LiveSafe™**
***https://www.mcafee.com***

**Bitdefender Total Security**
***https://bitdefender.com***

**HitmanPro**
***https://www.hitmanpro.com***

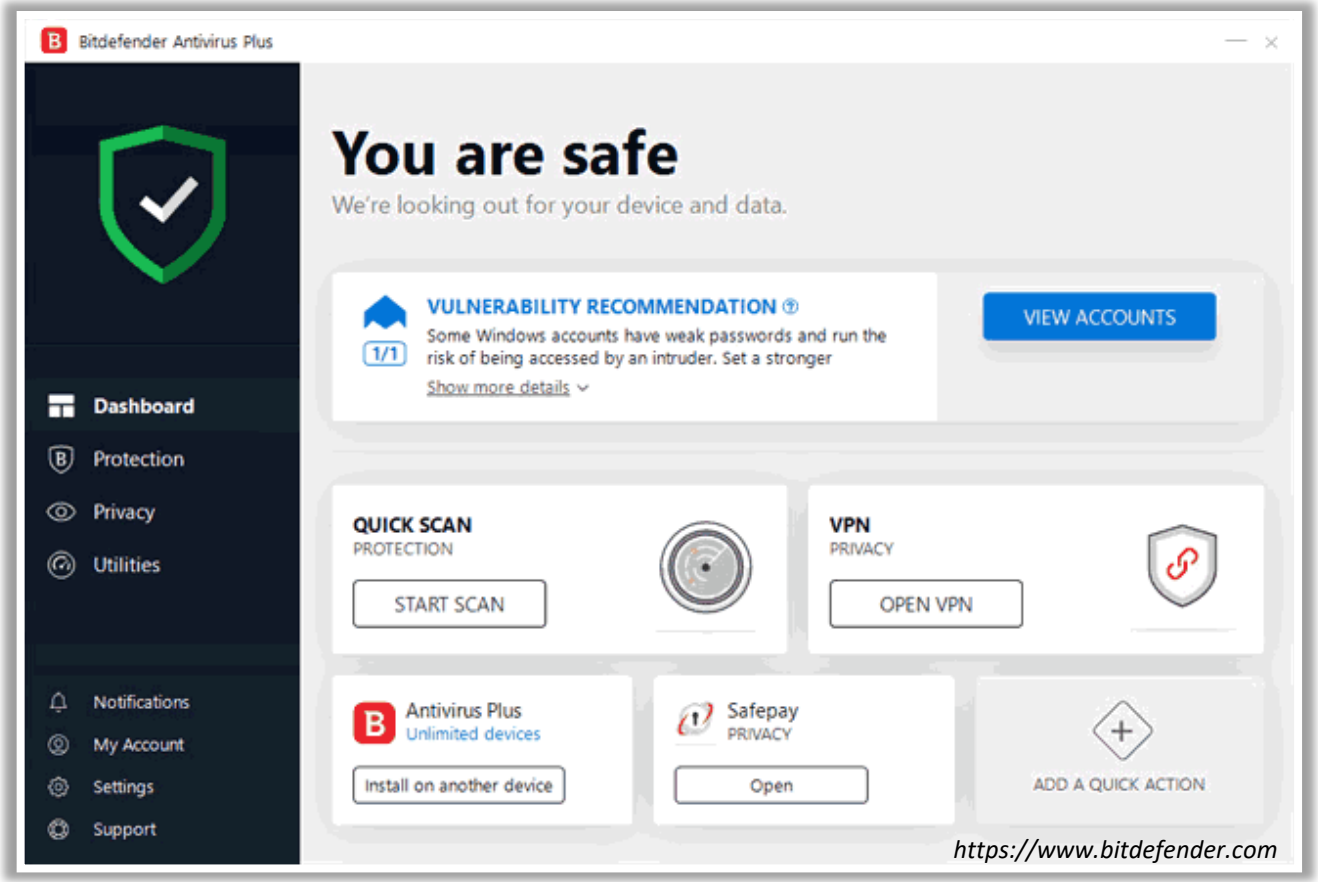
**Malwarebytes**
***https://www.malwarebytes.org***

**Zemana Antimalware**
***https://www.zemana.com***

# Antivirus Software

**Bitdefender Antivirus Plus**

**Bitdefender Antivirus Plus** works against all threats – from viruses, worms and Trojans, to ransomware, zero-day exploits, rootkits and spyware



*https://www.bitdefender.com*

**ClamWin**
***http://www.clamwin.com***

**Kaspersky Anti-Virus**
***https://www.kaspersky.com***

**McAfee Total Protection**
***https://www.mcafee.com***

**Avast Premier Antivirus**
***https://www.avast.com***

**ESET Internet Security**
***https://www.eset.com***

# Module Summary

- This module has discussed network segmentation and its types
- This module introduced you to the different types of firewalls and their roles
- It has also discussed the different types of IDS/IPS and their roles
- This module also explained in detail on the different types of honeypots
- It has also explained the different types of proxy servers and their benefits
- This module briefly explained the fundamentals of VPN and its importance in the network security
- It has also discussed the SIEM and SIEM solutions
- Finally, this module ended with an overview on various antivirus/anti-malware software
- In the next module, we will discuss on virtualization and cloud computing concepts in detail

