Network Security Tools

Outline

- Firewalls
- Intrusion Detection and Prevention Systems
- Malware Defense

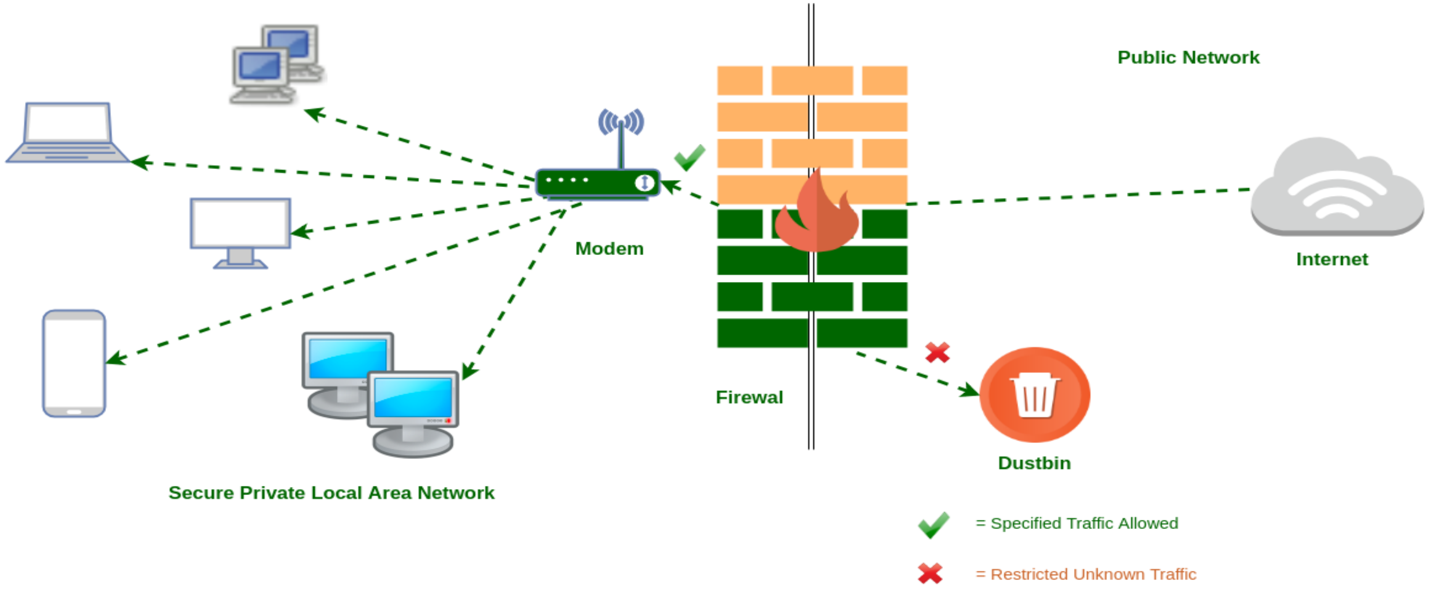
Firewalls

Firewalls: Overview (1/3)

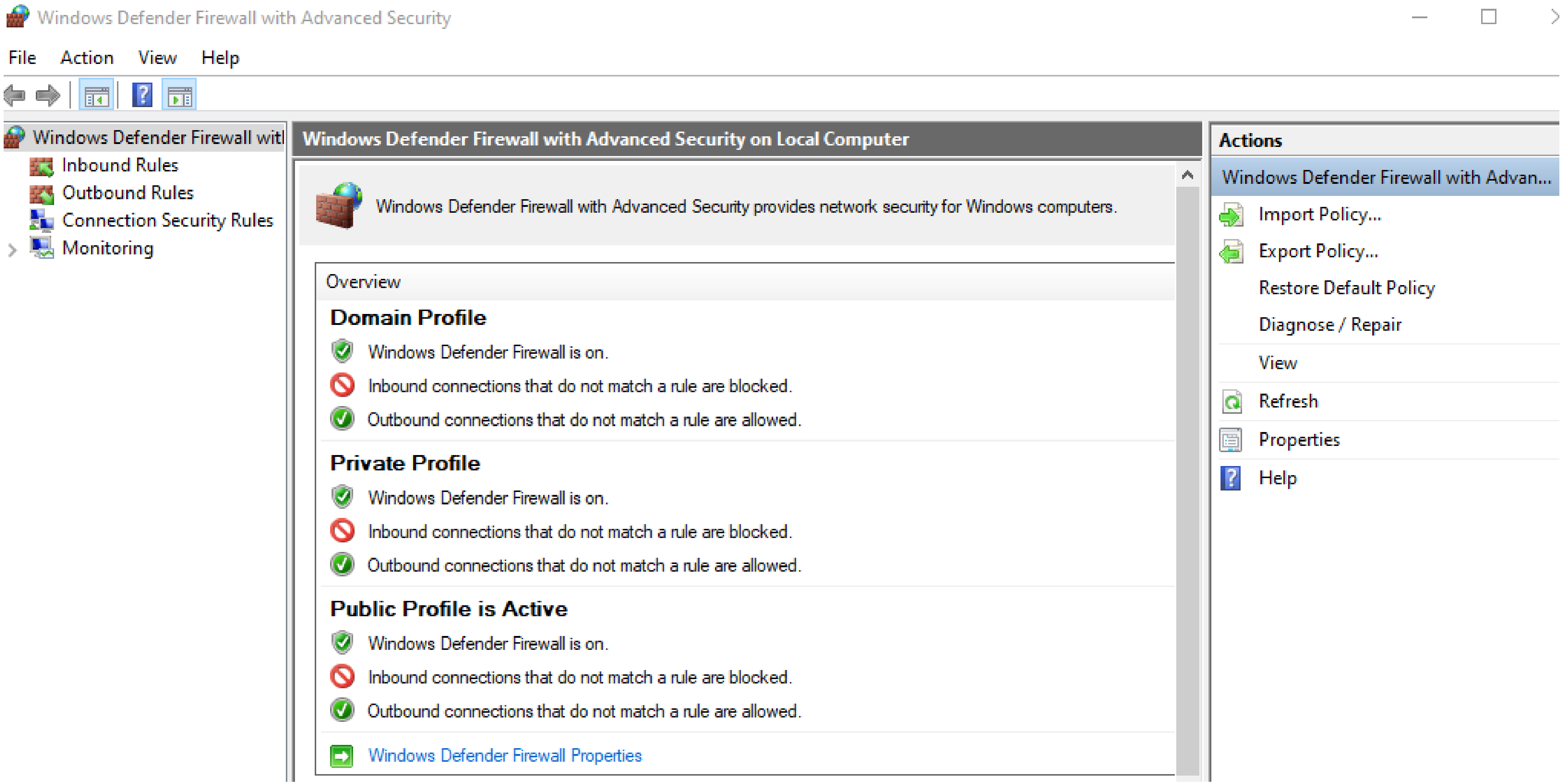
- Firewalls are tools that implement various security mechanisms designed to protect networks by controlling traffic based on predefined rules. These mechanisms typically belong to Access Control Policies and Network Security Monitoring Policies, depending on their specific function.

Firewalls: Overview (2/3)

- Packet Filtering is the core function of a firewall, where the firewall inspects incoming and outgoing packets based on predefined security rules. It checks information such as IP addresses, ports, and protocols to determine if the packet should be allowed or blocked.


Public Network
Modem
Internet
Firewal
Dustbin
Secure Private Local Area Network
✓ = Specified Traffic Allowed
✗ = Restricted Unknown Traffic

Firewalls: Overview (3/3)



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

- ✓ 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

Firewalls: Two Types

Feature	1. Network Firewall	2. Host-Bsed Firewall
Scope	Protects a network or subnet	Protects a single device (host)
Placement	At the network perimeter or gateway	On the host operating system
Traffic Type	Filters traffic between networks	Filters traffic to/from the host
Administration	Centrally managed	Managed per device

Firewalls: Filtering Criteria (1/4)

- IP addresses: Source and destination.

Example: Only devices with IPs in 192.168.1.0/24 are permitted access to internal resources.

- Port numbers: Applications or services.

Example: Allow web traffic (HTTP/HTTPS) using port number 443 only while blocking others (80).

- Protocol types: TCP, UDP, ICMP.

Example: Deny UDP traffic to limit streaming services on a corporate network.

Firewalls: Filtering Criteria (2/4)

Actions include:

- Allow: Let the packet through.
- Deny/Block: Reject or discard the packet.
- Limit: Restrict the number of packets under the same type.

Firewalls: Filtering Criteria (3/4)

Firewall Rule for (allow or deny): These are syntaxs in high-level representations

[ACTION] [PROTOCOL] [SOURCE IP/SUBNET] [SOURCE PORT] -> [DESTINATION IP/SUBNET] [DESTINATION PORT]

"Inbound" means traffic is entering the host. Destination IP matches the local IP.

INBOUND ALLOW TCP ANY ANY -> 192.168.1.10 3389

"Outbound" means traffic is leaving the host. Source IP matches the local IP.

OUTBOUND BLOCK UDP 192.168.1.10 ANY -> ANY 53

Tips: private IP addresses is a strong indicator of which device or network is local

Firewalls: Filtering Criteria (4/4)

Firewall Rule for (limit):

LIMIT <Protocol> <Source IP> -> <Destination IP> <Port> <Flags> rate <Rate>

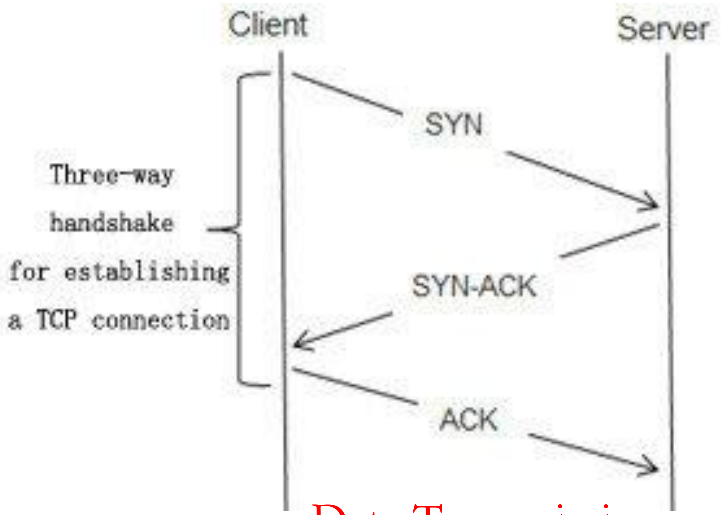
Flags: Specify flag inside the source of protocol

Rate: how many packets per second (or minute) are allowed.

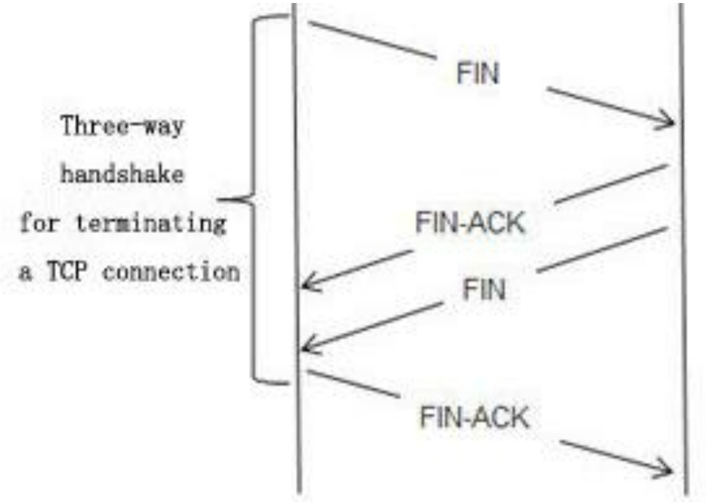
LIMIT TCP ANY -> 192.168.1.1 80 SYN rate 200/s

Allow up to 200 packets per second from any source to a web server (port 80)

Firewalls: Applications (1/9)



Data Transmission



A SYN Flood attack is a type of Denial of Service (DoS) attack that targets the TCP handshake process. Here's a brief explanation:

In a normal TCP connection, the client sends a SYN (synchronize) request to the server to initiate a connection. The server responds with a SYN-ACK (synchronize-acknowledge), and the client replies with an ACK (acknowledge), completing the three-way handshake.

In a SYN Flood attack, the attacker sends many SYN requests to the server but never completes the handshake by sending the final ACK. The server allocates resources and waits for the ACK that never comes, resulting in a large number of half-open connections. As the server's resources are consumed, it becomes overwhelmed and unable to handle legitimate connections, leading to service disruption.

Firewalls: Applications (2/9)

Firewall Rule against TCP SYN Flood attack:

- Rejecting SYN Packets After a Threshold

  LIMIT TCP ANY -> <Host IP> 80 SYN rate 50/s

- Denying SYN Packets from Known Bad Sources

  DENY TCP <Malicious IP Range> -> <Host IP> 80 SYN

Firewalls: Applications (3/9)

UDP Flooding (Amplification Attack) is a type of Distributed Denial of Service (DDoS) attack that exploits the stateless nature of the User Datagram Protocol (UDP) and often amplifies the attack using a feature like UDP-based services that respond with larger data than the request sent.

1. Attacker Sends Small UDP Packets: The attacker sends a large volume of small UDP packets to various servers. These packets typically request data from services like DNS, NTP, or other UDP-based services that reply with larger responses.

2. Spoofing the Source IP: The attacker forges (spoofs) the source IP address of the UDP packets to make it appear as though they are coming from the victim's IP address.

3. Amplified Response: The server responds to the spoofed IP with a much larger data payload than the original request. Since UDP is connectionless, the server has no way to verify the legitimacy of the source IP address.

4. Flooding the Victim: The victim (no the server)'s network gets overloaded with massive amounts of response data, effectively clogging the network and degrading or taking down services.

Firewalls: Applications (4/9)

Firewall Rule against UDP Flooding (Amplification Attack) :

- Limit incoming UDP traffic to port 53 (DNS):

  LIMIT UDP ANY -> 192.168.1.100 53 rate 10/s

- Drop unnecessary UDP services (e.g., port 123 for NTP):

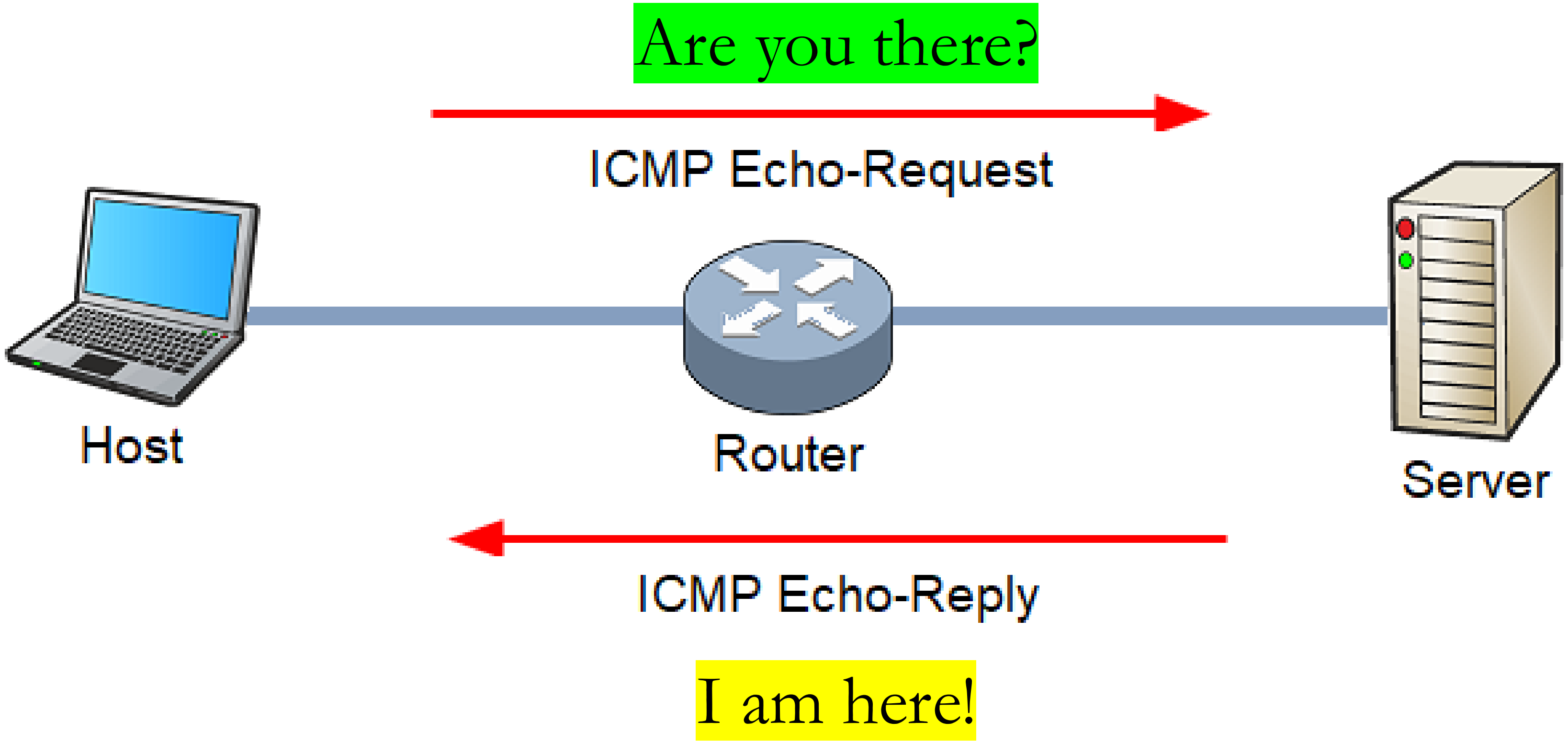
  DROP UDP ANY -> 192.168.1.100 123

- Block large UDP responses to prevent amplification:

  DENY UDP 192.168.1.100 -> ANY 53 size > 512

  (extra functionality support)

Firewalls: Applications (5/9)



The ping protocol requires the server to unconditionally answer messages --> attack!

Firewalls: Applications (6/9)

ICMP Flooding (Denial-of-Service Attack):

- Description: Attackers send a high volume of ICMP Echo Request (ping) packets to overwhelm a target system's resources, leading to degraded performance or complete unresponsiveness.
- Impact: This can cause significant network disruption, making services unavailable and impacting overall network stability.

Ping of Death:

- Description: Exploits vulnerabilities in a system's handling of oversized ICMP packets, which can cause (old systems) crashes (Lack of Size Checking).
- Impact: This can lead to system crashes or reboots, affecting the availability and reliability of network services.

Firewalls: Applications (7/9)

Firewall Rule against ICMP Flooding:

- Limit the number of ICMP echo requests (ping requests) to 1 per second for traffic directed to the IP address

  LIMIT ICMP ANY -> 192.168.1.100 echo-request rate 1/s

- Deny all ICMP echo requests (ping requests) directed to the IP address

  Deny ICMP ANY -> 192.168.1.100 echo-request

- Limit the size to mitigate Ping of Death

  LIMIT ICMP ANY -> ANY echo-request length 1000-65535

Firewalls: Applications (8/9)

Firewalls primarily operate at the following two layers

1. Internet Layer

Protocols: IP (Internet Protocol), ICMP (Internet Control Message Protocol)

Function: Filters traffic based on IP addresses and network protocols.

2. Transport Layer

Protocols: TCP (Transmission Control Protocol), UDP (User Datagram Protocol)

Function: Filters traffic based on port numbers and transport layer protocols.

Firewalls: Applications (9/9)

- A stateless firewall, also known as a packet-filtering firewall, operates by inspecting each packet individually without considering the context of the traffic flow. It filters packets based on predefined rules that consider only the packet's source and destination IP addresses, ports, and protocol types.

- Stateless firewalls do not track the state of connections, making them unable to distinguish between legitimate and illegitimate packets that are part of the same session. In a TCP connection, a stateless firewall cannot track the three-way handshake (SYN, SYN-ACK, ACK) process. It treats each packet independently, which can lead to issues in properly managing the connection state and filtering traffic accurately.

Firewalls: Softwares (not important)

- Windows Defender Firewall:

Platform: Windows

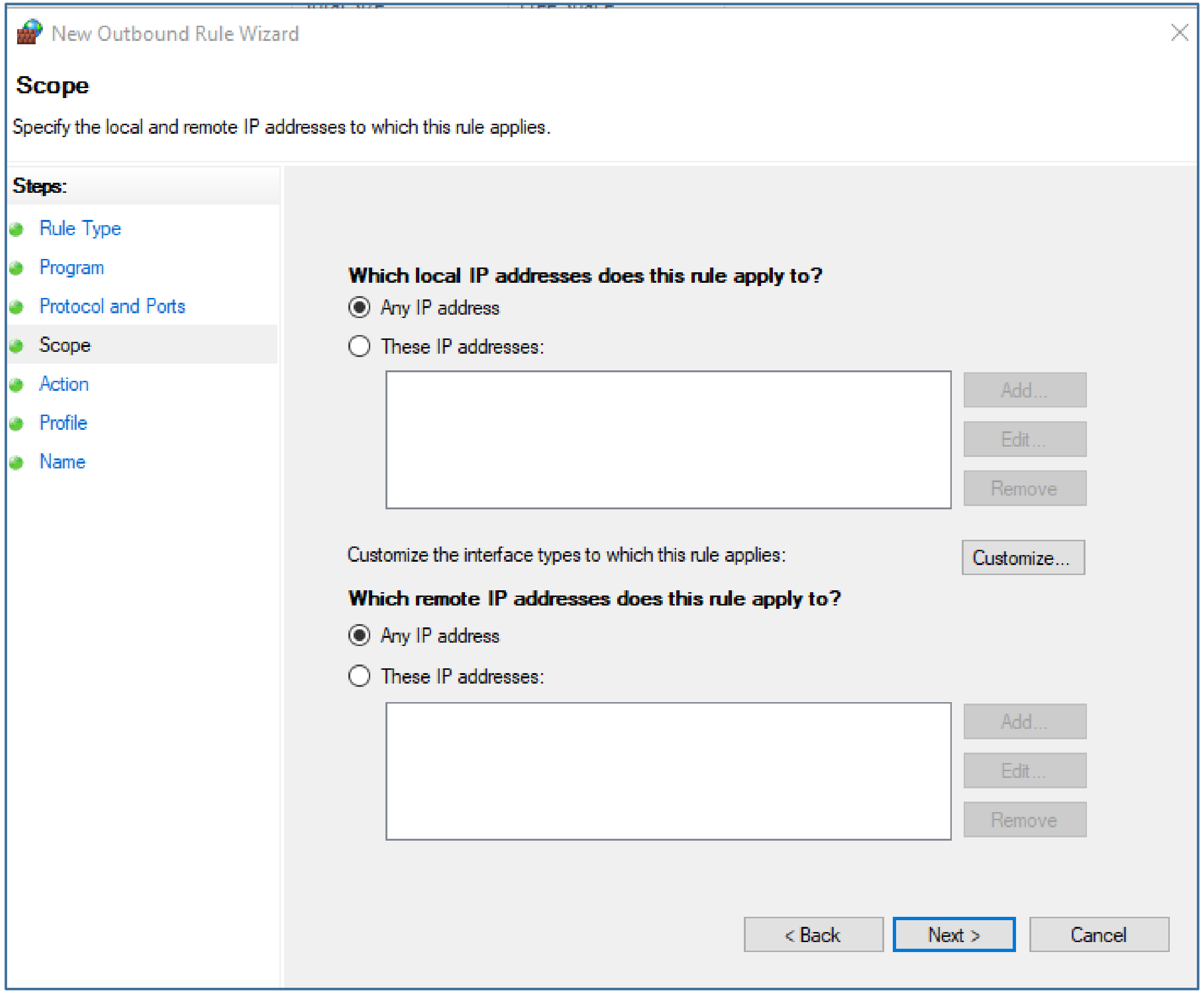
Features: Integrated with Windows OS, easy to use, supports inbound and outbound rules, profiles for different network types (Domain, Private, Public).

- iptables/nftables:

Platform: Linux

Features: Highly flexible and powerful, supports detailed packet filtering, NAT, and rate limiting. nftables is the modern replacement for iptables.

7.4 Firewalls: Windows Defender Firewall


New Outbound Rule Wizard

Scope

Specify the local and remote IP addresses to which this rule applies.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

Which local IP addresses does this rule apply to?

● Any IP address

○ These IP addresses:

Customize the interface types to which this rule applies:

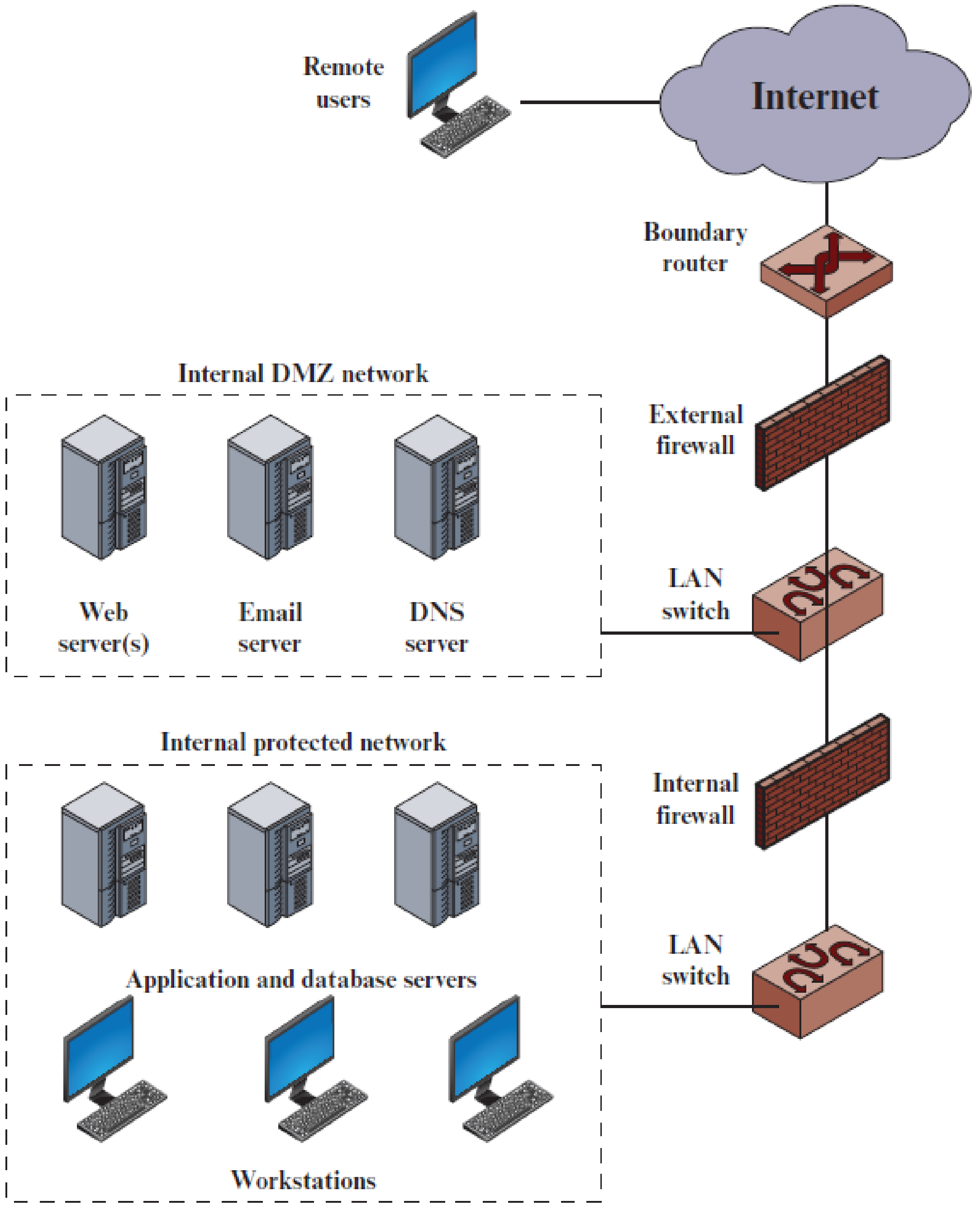
Which remote IP addresses does this rule apply to?

● Any IP address

○ These IP addresses:

DMZ Networks

- An external firewall is placed at the edge of a local or enterprise network
- One or more internal firewalls protect the bulk of the enterprise network.
- Between these two types of firewalls are one or more networked devices in a region referred to as a demilitarized zone (DMZ) network.
- Systems that are externally accessible but need some protections are usually located on DMZ networks.



DMZ Networks

The external firewall provides a measure of access control and protection for the DMZ systems consistent with their need for external connectivity. It also provides a basic level of protection for the remainder of the enterprise network.

The internal firewalls serve three purposes:

1. Adds more stringent filtering capability
2. Provides two-way protection with respect to the DMZ
3. Multiple internal firewalls can be used to protect portions of the internal network from each other.

Intrusion Detection and Prevention Systems

Intrusion Detection

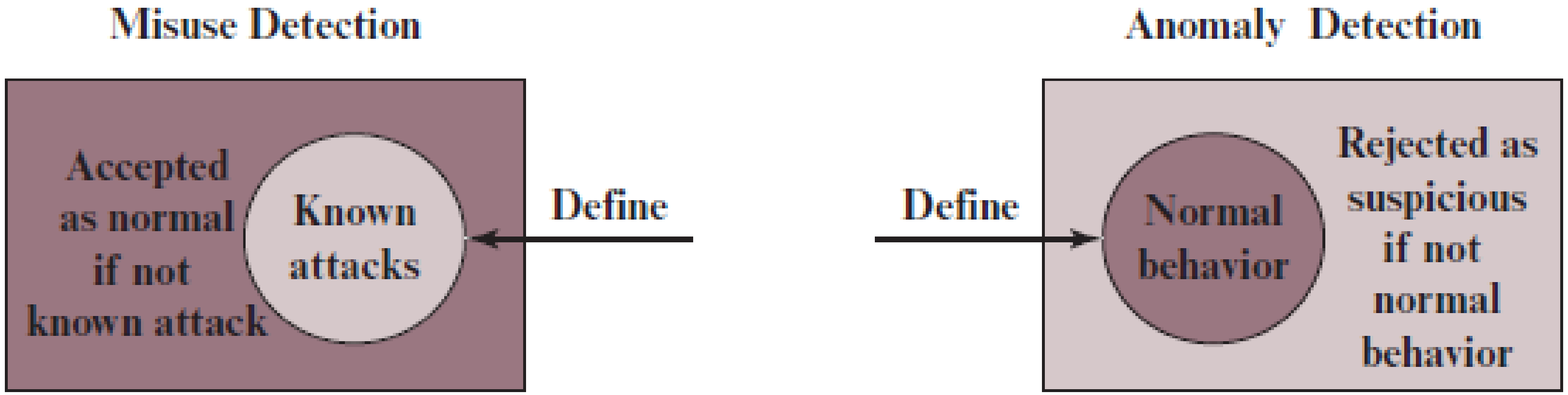
An IDS is designed to monitor network traffic or system activity for suspicious behavior, policy violations, or unauthorized access. It functions as a passive monitoring tool, alerting administrators when potential threats are detected but not actively taking measures to stop them. IDS can be categorized into two main types:

- Network-based IDS (NIDS): Monitors network traffic for malicious activities.
- Host-based IDS (HIDS): Monitors activities on individual devices for anomalies.

Approaches to Intrusion Detection

Intrusion detection assumes that the behavior of the intruder differs from that of a legitimate user in ways that can be quantified.

There are two general approaches to intrusion detection: **misuse detection** and **anomaly detection**.


Misuse Detection
Accepted as normal if not known attack
Known attacks
Define
Anomaly Detection
Define
Normal behavior
Rejected as suspicious if not normal behavior

Misuse Detection

Misuse detection is based on rules that specify system events, sequences of events, or observable properties of a system that are believed to be symptomatic of security incidents.

Misuse detectors use various pattern-matching algorithms, operating on large databases of attack patterns, or *signatures*.

An advantage of misuse detection is that it is accurate and generates few false alarms.

A disadvantage is that it cannot detect novel or unknown attacks.

Anomaly Detection

Anomaly detection searches for activity that is different from the normal behavior of system entities and system resources.

An advantage of anomaly detection is that it is able to detect previously unknown attacks based on an audit of activity.

A disadvantage is that there is a significant trade-off between false positives and false negatives.

Intrusion Prevention

- An IPS extends IDS functionality by not only detecting potential threats but also actively blocking malicious activities. It operates in-line with network traffic, enabling it to prevent harmful actions by dropping packets, resetting connections, or blocking access based on pre-defined rules.

- IPS also has the firewall functions. However, an IPS does not rely on firewall rules. It uses its own methods (pattern) to identify and block threats, even if those threats bypass the firewall. Together, they provide layered security, but they have distinct roles.

IDP: Against SQL Injection Attack

Description: An SQL injection attack occurs when an attacker exploits a vulnerability in a web application by inserting malicious SQL queries into input fields (e.g., login forms). This allows the attacker to manipulate the backend database, potentially gaining unauthorized access to sensitive data.

How IDP Stops It:

- Detection: The IDP system can detect malicious SQL queries embedded in network traffic, looking for known patterns or suspicious strings (e.g., OR 1=1) Namely, based on payload.
- Prevention: When an attack is detected, the IDP can block the query or immediately stop the connection (more than drop packets) from being processed, preventing the attacker from executing the harmful SQL command.

Example: An attacker tries to inject malicious SQL code into a website’s login form to bypass authentication. The IDP system detects the abnormal query structure in the traffic and blocks it before it reaches the backend database.

Malware Defense

Malicious Software

Malicious software, commonly called **malware**, is perhaps the most significant security threat to organizations.

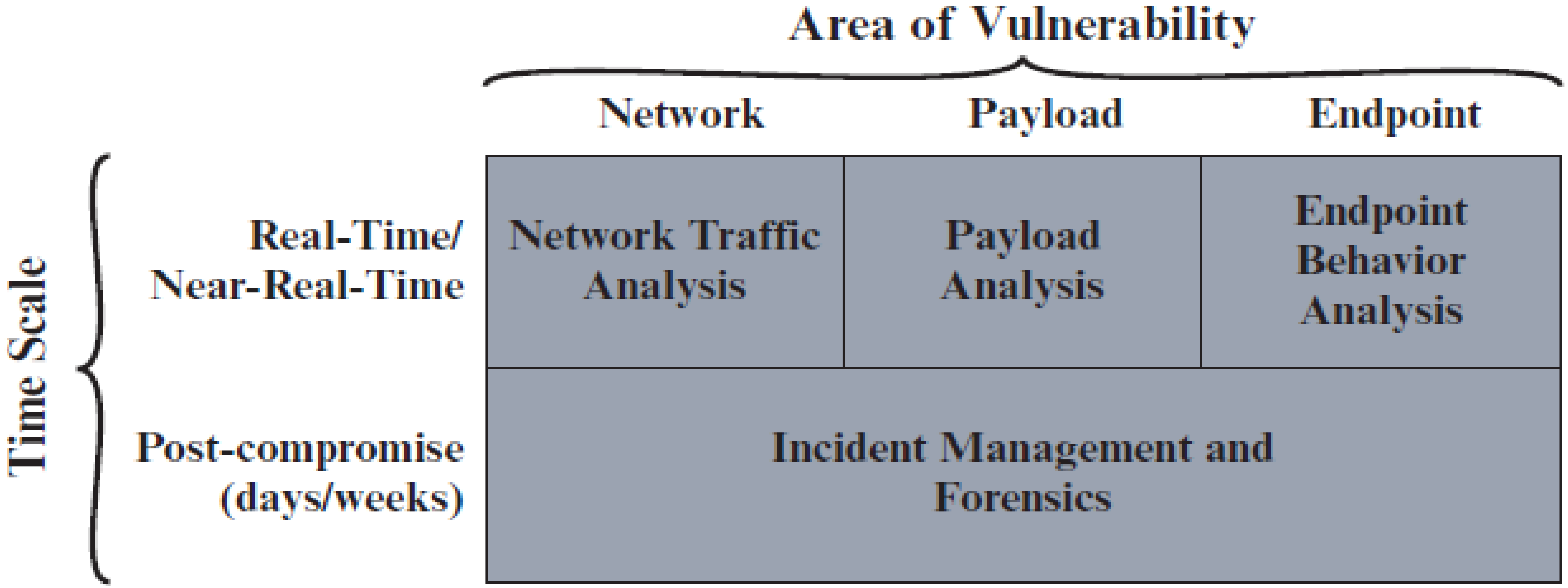
NIST SP 800-83 defines malware as a as “a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim’s data, applications, or operating system.”

Malware can pose a threat to application programs, to utility programs, such as editors and compilers, and to kernel-level programs. Malware can also be used on compromised or malicious Web sites and servers, or in especially crafted spam emails or other messages, which aim to trick users into revealing sensitive personal information.

Common Types of Malware

- Virus
- Worm
- Trojan Horse
- Spyware
- Rootkit
- Backdoor
- Bot
- Ransomware

Malware Defense



Time Scale	Area of Vulnerability		
	Network	Payload	Endpoint
Real-Time/ Near-Real-Time	Network Traffic Analysis	Payload Analysis	Endpoint Behavior Analysis
Post-compromise (days/weeks)	Incident Management and Forensics		

Network Traffic Analysis

Network traffic analysis involves monitoring traffic flows to detect potentially malicious activity.

As with intrusion detection, traffic analysis can involve misuse detection (signature detection) or anomaly detection.

As an example of misuse detection, a dramatic surge in traffic at any point likely indicates that a DDoS attack is underway.

For anomaly detection, network security software needs to collect and maintain profiles of typical network traffic patterns, and then monitor current traffic for significant deviation from normal behavior. For example, anomalous DNS (Domain Name System) traffic is a good indicator of botnet activity.

Payload Analysis

Payload analysis involves looking for known malicious payloads (signature detection) or looking for payload patterns that are anomalous.

One useful technique for payload analysis is the use of a sandbox environment, which quarantines the payload until the analysis is done. This enables a payload analysis system to observe the behavior of payloads in motion, such as when they cross the network perimeter, and to either flag suspicious payloads or block them outright.

Endpoint Behavior Analysis

This category involves a wide variety of tools and approaches implemented at the endpoint.

Antivirus software uses signature and anomaly detection techniques to identify malware and prevent it from executing on the host system.

Application whitelisting, which restricts application execution to only known good applications is also employed.

At the system software level, application containers can isolate applications and files in virtual containers to prevent damage.

Incident Management

Information security incident management consists of processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.

Key elements: data collection, data aggregation, data normalization, correlation, alerting, reporting/compliance.

Also covered in CSIT123, CSIT302, CSIT488/CSIT988.

Forensics

NIST SP 800-96 defines computer forensics, or digital forensics, as the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.

Computer forensics seeks to answer questions such as:

- What happened?
- When did the events occur?
- In what order did the events occur?
- What was the cause of these events?
- Who caused these events to occur?
- What enabled these events to take place?
- What was affected? How much was it affected?