




# NEW YORK INSTITUTE OF TECHNOLOGY

INCS 775  
Data Center Security

*Cloud Security – Part 1*



Dr. Zakaria Alomari  
zalomari@nyit.edu

# What is Cloud Security?

---

**Cloud security** refers to the technologies, policies, controls, and services that protect cloud data, applications, and infrastructure from threats.

# DDoS Attack Detection and Mitigation

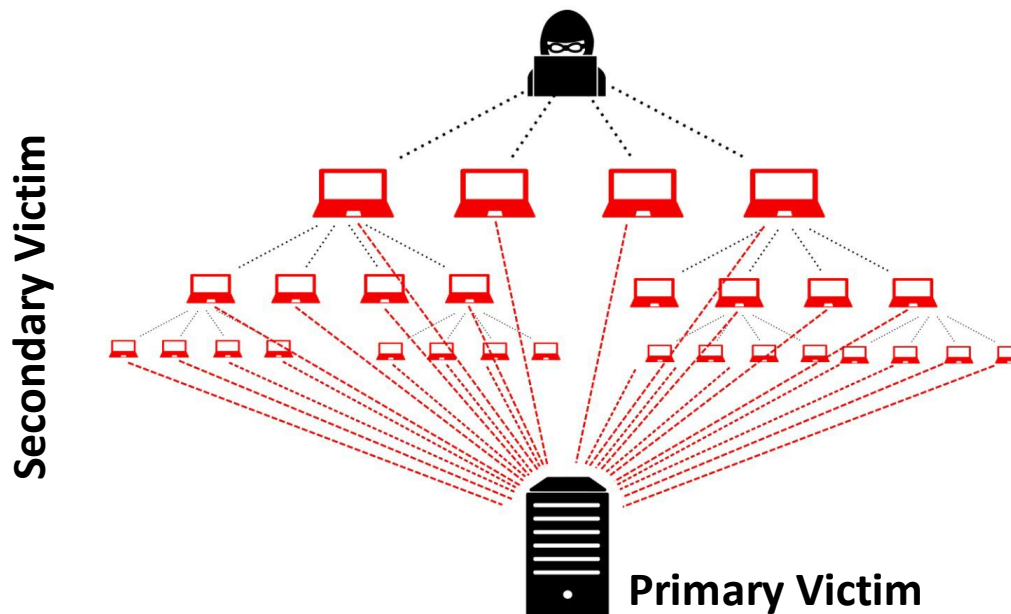
---

## What is Distributed Denial of Service (DDoS) attack?

- **Distributed Denial of Service attack** is carried out by using **multiple compromised systems** to attack a **target** to deny the service to the **legitimate users**.
- The **service under attack** is the “**primary victim**” while the **compromised systems used to launch the attack** are often called the “**secondary victims**”.
- The **sheer volume of sources involved in DDoS attacks** make it nearly impossible to stop.

# DDoS Attack Detection & Mitigation

---



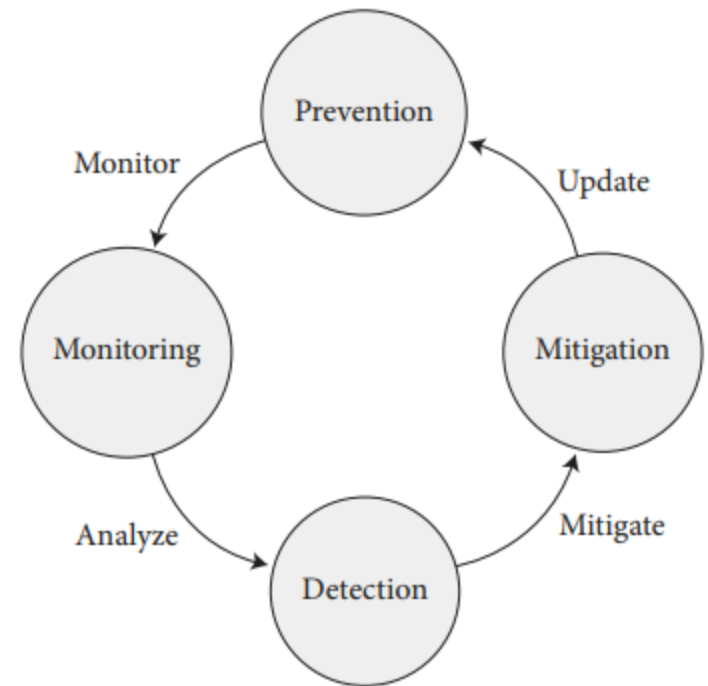
# DDoS Classes

Class 1: Brute-force	Class 2: Semantic
<p><b>Brute-force attacks</b> are performed by initiating a <b>vast amount of seemingly legitimate transactions</b>.</p> <p>Since an <b>intermediate network</b> can usually <b>deliver higher traffic volume than the victim network can handle</b>, a high number of attack packets exhausts the victim's resources.</p>	<p><b>Semantic attacks</b> exploit a <b>specific feature or implementation bug</b> of some <b>protocol or application</b> installed at the <b>victim</b> in order to <b>consume excessive amounts of its resources</b>. For example, in the TCP SYN attack.</p>
<ul style="list-style-type: none"><li>• Targets the bandwidth/resources</li><li>• Over million bots<ul style="list-style-type: none"><li>- Mirai attack</li></ul></li></ul>	Targets a protocol or an application

# DDoS defense life-cycle

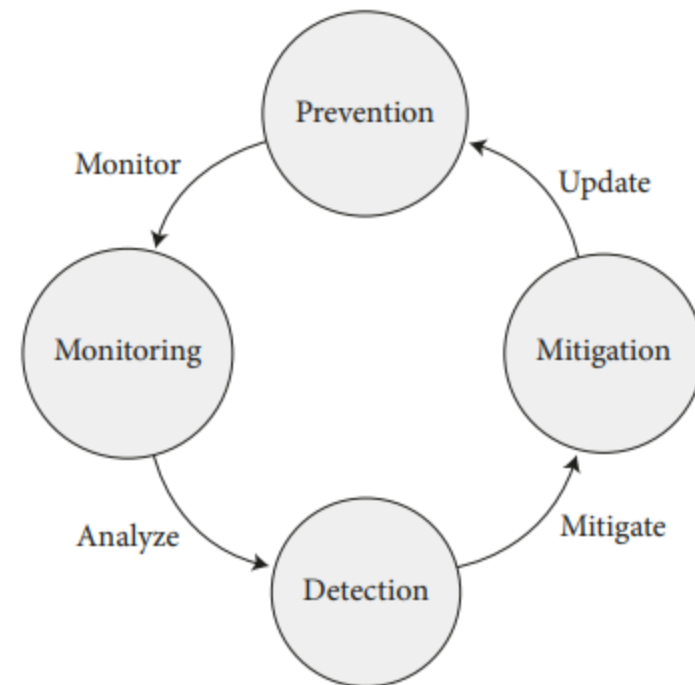
There are several phases that are involved in defending DDoS attack, as follows:

- **Prevention:** The prevention phase focuses on protecting a system against an attack by applying appropriate security appliances at varied places.
- **Monitoring:** As for the monitoring phases, necessary information about a host or network is obtained by using tools, such as network monitoring software. Monitoring is conducted in real time as it becomes compulsory for detection of DDoS attack.



# DDoS defense life-cycle

- **Detection:** The detection phase requires analysis of the running system to discover malicious traffic that leads to DDoS attack. Detection involves a sophisticated approach to identify large illegal GET request traffic against a web server.
- **Mitigation:** The mitigation phase is applied when an attack occurs, and a suitable security countermeasure is executed to handle the attack or to slow down the attack. A mitigation technique operates by stopping the attack.



# DDoS Detection

---

## ❑ Signature-based Detection

- Also referred to as *pattern matching*.
- Operates by comparing data or network traffic against a predefined database of known threat signatures or patterns.
- Primarily used to detect known threats, such as *viruses, malware, or specific attack techniques*.
- Highly effective for identifying previously documented attacks but may fail to detect new or unknown threats.
- **Example:**
  - Detecting the WannaCry ransomware using its unique file hash or known malicious code pattern stored in an antivirus signature database.



# DDoS Detection

---

## ❑ Behavior-based Detection

- Also known as *heuristic detection or anomaly detection*.
- Focuses on **monitoring and analyzing system or user behaviors to identify abnormal or suspicious activities**.
- Does not rely on known threat signatures; instead, it **detects deviations from established normal behavior patterns**.
- **Capable of identifying unknown or emerging threats**, including zero-day attacks, based on unusual system or user activities.
- **Example:**
  - Detecting an **insider threat** when a **user suddenly starts accessing sensitive files at unusual hours or transferring large amounts of data**, which deviates from their normal behavior profile.

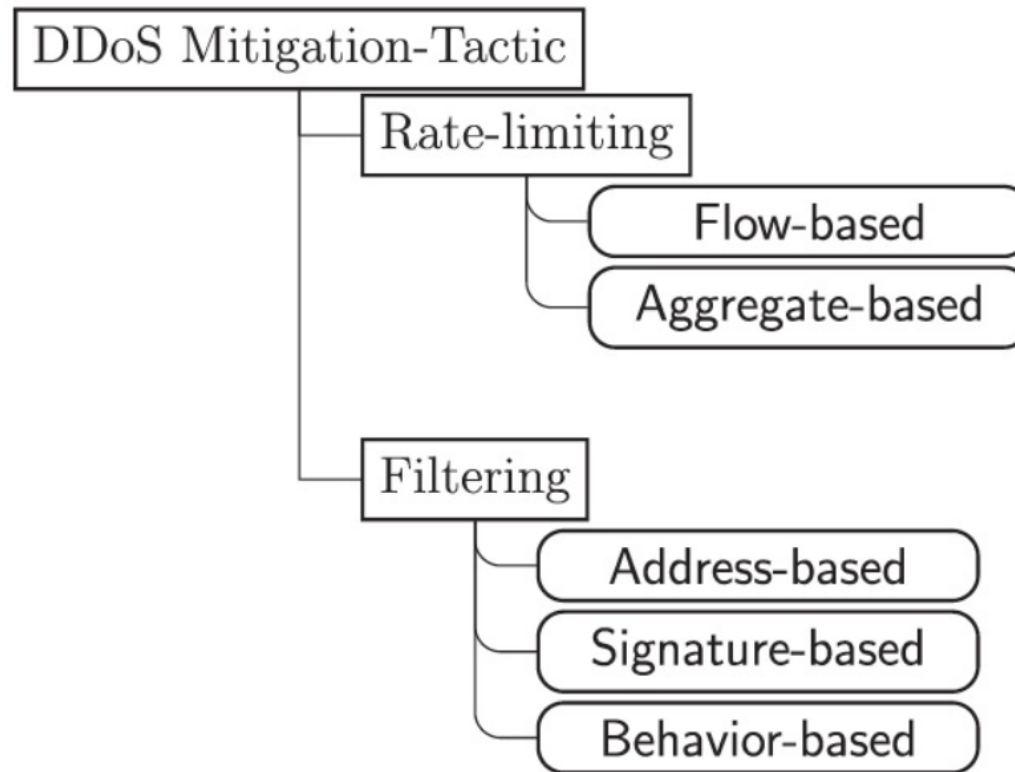
# DDoS Mitigation

---

- DDoS Mitigation Tactic
  - Rate limiting
  - Filtering
- DDoS Mitigation Strategy
  - Collaborative
  - Non-collaborative

# DDoS Mitigation Tactic

---



# DDoS Mitigation Tactic

---

## ❑ DDoS Mitigation Tactic – Rate limiting

- It involves **setting limits on the rate of incoming traffic**, typically **based on the number of requests per second or minute from a particular source IP address or subnet**.
- Here's how rate limiting works in DDoS mitigation:
  - 1. Setting Traffic Thresholds:**
    - Once the **normal traffic patterns** are **identified**, **thresholds are set to determine the rate at which traffic will be limited**.
    - These **thresholds can be based on various factors**, such as the **capacity of the network infrastructure**, the **expected rate of legitimate traffic**, or the **historical data of previous attacks**.

# DDoS Mitigation Tactic

---

## 2. IP Address or Subnet-Based Rate Limits:

- Rate limiting can be implemented on a per-IP address or per-subnet basis.
- This allows organizations to differentiate between legitimate users and potential attackers. By imposing stricter rate limits on suspicious or known malicious sources, organizations can effectively reduce the impact of DDoS attacks.

## 3. Whitelisting and Exemptions

- Allows trusted IP addresses, users, or services to bypass rate limits. This ensures legitimate traffic (like internal systems or partners) isn't affected during an attack.
- **Example:** An *e-commerce website whitelists the IP address of its payment gateway service*, so even during a DDoS attack, payment transactions are not blocked by rate limiting.

# DDoS Mitigation Tactic

---

## 4. Dynamic Rate Limiting

- Adjusts rate limits automatically based on real-time traffic patterns. If suspicious activity is detected, the system tightens limits temporarily.
- **Example:** A news website normally allows 100 requests per minute per user. But during a sudden traffic spike from a single IP, the system dynamically reduces the limit to 10 requests per minute for that IP to prevent abuse.

## 5. Dropping or Delaying Excessive Traffic

- Extra traffic beyond the allowed threshold is either dropped (discarded) or delayed (slowed down), preventing server overload.
- **Example:** A gaming server allows 200 requests per second. If an attacker tries sending 1000 requests per second, the server drops the extra 800 requests or adds a delay, making the attack ineffective.

# DDoS Mitigation Tactic

---

## 6. Monitoring and Tracking Traffic

- Continuously **observes incoming traffic to detect anomalies, spot attack patterns, and fine-tune rate-limiting rules accordingly.**
- **Example: A cloud service provider continuously monitors traffic and notices a large number of requests from a specific country where the service has no users — triggering alerts and defensive action.**

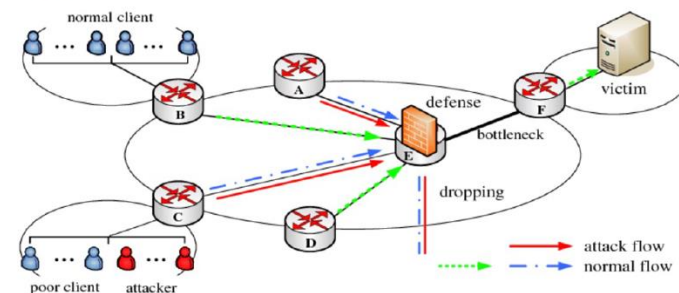
## 7. Identifying Normal Traffic Patterns

- **Analyzes typical user behavior to differentiate between legitimate and malicious traffic,** helping set effective rate limits without affecting genuine users.
- **Example: An online banking site observes that users usually log in 2-3 times a day. If a single user account suddenly makes 200 login attempts in 1 minute, it's flagged as abnormal — possibly a brute-force attack — and rate limits are enforced.**

# DDoS Mitigation Tactic

- **Flow-based** might involve dropping specific attack flows (e.g., from the **attacker**) while sparing normal flows.
- **Aggregation-based** might trigger a bottleneck or dropping when total traffic exceeds a threshold, affecting both attackers and some legitimate users.
- **Normal clients** (A, B, C, D) interact through these systems. The **defense mechanisms** (bottleneck, and dropping) aim to protect the **Victim** by filtering out **attack flows** while allowing **normal flows**. An **attacker** targets the Victim, potentially impacting the **poor client** (e.g., collateral damage). Key techniques like traffic bottleneck and packet dropping mitigate attacks, highlighting the trade-offs between security and performance.

- Flow-based
- Aggregation-based





# DDoS Mitigation Tactic

---

## ❑ DDoS Mitigation Tactic – Filtering

- It involves the use of filters to **block or allow network traffic based on specified criteria**.
- Here's an overview of how filtering works in DDoS mitigation:
  - 1. Traffic Profiling:**
    - The **process of analyzing network traffic** to **identify patterns, behaviors, and characteristics** of legitimate and malicious traffic.
    - Before implementing filters, **it's essential to establish a baseline of normal network traffic behavior**.
    - This helps in **identifying anomalous traffic patterns during an attack**.
    - **Traffic profiling can involve monitoring network traffic** using various **tools and analyzing historical data to understand typical traffic patterns**.

# DDoS Mitigation Tactic

---

## 2. Blacklisting and Whitelisting:

- In DDoS mitigation, **blacklisting** involves **blocking traffic** from **known malicious sources or suspicious IP addresses**
- **Whitelisting**, on the other hand, **allows traffic only from trusted sources or known legitimate IP addresses.**
- **These lists are updated periodically based on emerging threats and identified patterns of malicious activity.**

## 3. Traffic Classification.

- **Identifying and categorizing incoming traffic** based on *behavior, source, type, or patterns* (e.g., normal users vs. bots). Helps in deciding which traffic to allow or block.
- **Example:** Classifying traffic by IP reputation — blocking all requests coming from known botnet IP addresses.

# DDoS Mitigation Tactic

---

## 4. Protocol Filtering.

- Blocking or limiting traffic based on specific network protocols (like TCP, UDP, ICMP) commonly abused in DDoS attacks.
- **Example: Blocking all ICMP (ping) traffic during an ICMP Flood attack** to prevent network overload.

## 5. Application-Layer Filtering.

- Analyzing and filtering traffic targeting specific applications (like HTTP, DNS). Detects abnormal requests like *fake logins* or *page floods* at Application Layer.
- **Example:** Detecting and blocking HTTP requests with fake user-agents or abnormal URL patterns targeting a website login page.

# DDoS Mitigation Tactic

---

## 6. Dynamic Filtering.

- Adaptive filtering that changes rules in real-time based on current attack patterns. Automatically updates filters to block evolving threats.
- **Example:** Auto-blocking an IP that sends 1000 requests in 1 second, then removing the block if the traffic normalizes.

# DDoS Mitigation Tactic

- ❑ The figure illustrates a layered security approach where **internet traffic** passes through three **protection methods** before reaching the **customer network**:
  - **Address-based filtering** (blocks/allows traffic by IP addresses).
  - **Signature-based filtering** (detects known threats via predefined patterns).
  - **Behavior-based filtering** (identifies anomalies in activity).
- ❑ These methods are applied through **filtering** mechanisms, collectively safeguarding the customer network from diverse cyber threats.

- Address-based filtering
- Signature-based filtering
- Behavior-based filtering

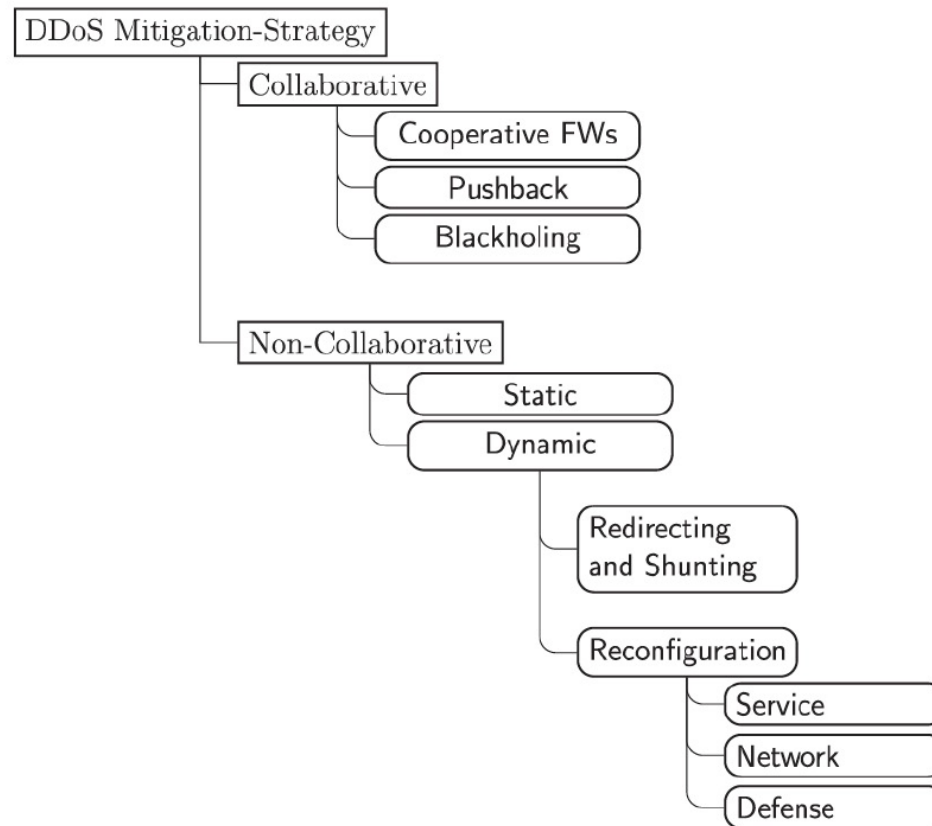


# Advantages and disadvantages of DDoS mitigation tactics

Mitigation Tactic	Advantages	Disadvantages
Rate-Limiting	<ul style="list-style-type: none"><li>○ <b>Easy to deploy:</b> Simple to implement on network devices (e.g., routers, firewalls).</li><li>○ <b>Dynamic thresholds:</b> Adjust limits based on traffic patterns (e.g., stricter during attacks).</li><li>○ <b>Reduces false positives:</b> Slows traffic instead of blocking it outright, useful if detection systems are error-prone.</li></ul>	<ul style="list-style-type: none"><li>○ <b>Affects legitimate users:</b> If a threshold is reached (e.g., 100 requests/second), even normal users get restricted.</li><li>○ <b>Partial defense:</b> Attackers can bypass it by staying under the limit or spreading attacks across multiple sources.</li></ul>
Filtering	<ul style="list-style-type: none"><li>○ <b>Easy to deploy:</b> Rules can be added/removed quickly on network devices.</li><li>○ <b>Flexible:</b> Update blocklists dynamically (e.g., add new malicious IPs).</li></ul>	<ul style="list-style-type: none"><li>○ <b>Overblocking:</b> Cannot distinguish between malicious and legitimate traffic from the same source. <i>(Example: Blocking a shared office IP might block innocent users.)</i></li><li>○ <b>Incomplete coverage:</b> Attackers can evade filters by rotating IPs or using proxies.</li></ul>

# DDoS Mitigation Strategy

---



# DDoS Mitigation Strategy

---

## ❑ Mitigation Strategy – Collaborative

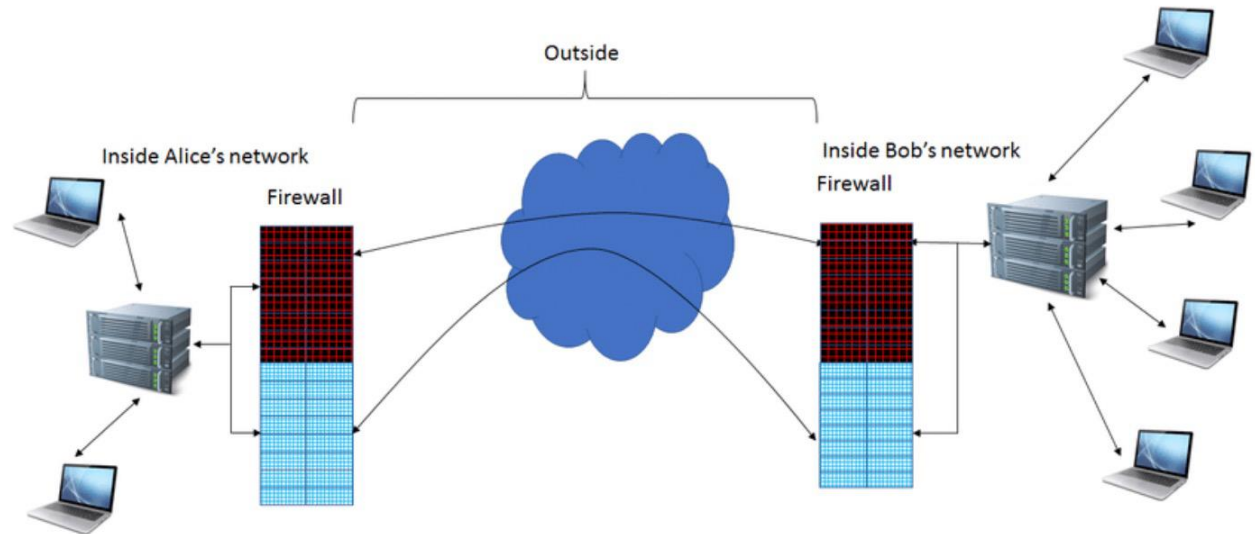
### 1- Firewalls cooperative defense:

- It involves the **coordinated efforts of multiple firewalls to collectively defend against DDoS attacks.**
- Here's a more detailed explanation of how **firewalls can collaborate to enhance DDoS mitigation:**
  - **Attack Detection and Information Sharing:** Each firewall actively monitors network traffic for signs of a DDoS attack. When an attack is detected, the firewall shares this information with the central coordination entity. The information includes details about the attack, such as *attack vectors, source IP addresses, attack intensity, and targeted services.*



# DDoS Mitigation Strategy

- The figure depicts two separate networks (**Alice's and Bob's**), each protected by a firewall.
- The **firewalls** act as security barriers dividing the "Inside" (secured internal network) from the "Outside" (external/untrusted environment).
- This setup ensures controlled access and protection for both networks.
- Upon detection of an attack, the firewall communicates the relevant information to the other firewall.



# DDoS Mitigation Strategy

---

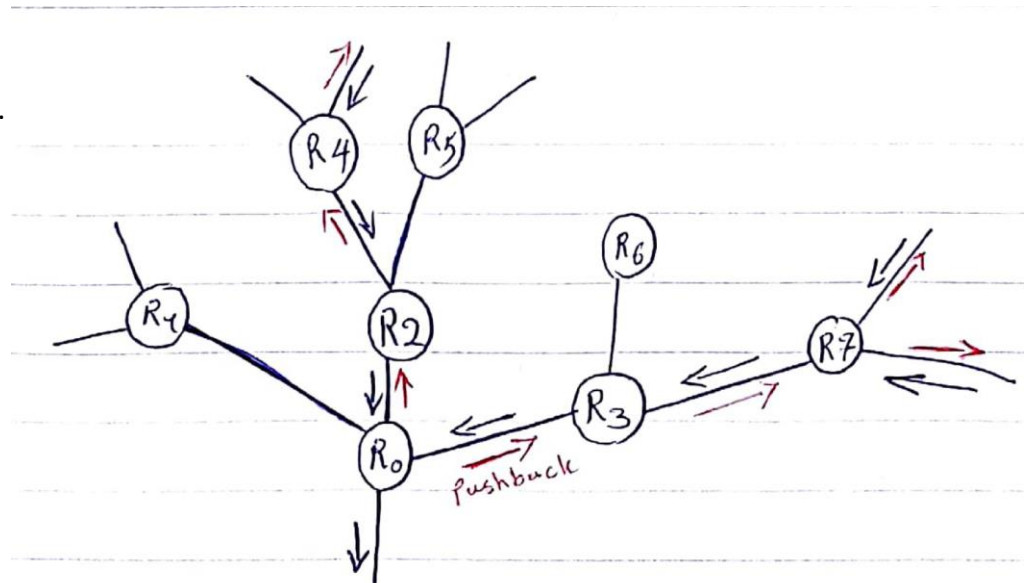
## 2- Pushback cooperative defense:

- It involves the **coordinated efforts among network entities to collectively respond and push back against DDoS attacks.**
- Here's a an explanation of how pushback cooperative defense can be implemented:
  - **Identification of Attack Traffic:** The **participating network entities**, such as *routers* or *switches*, **monitor incoming network traffic to identify potential DDoS attack patterns.** This can **involve analyzing packet headers, traffic behavior, or using anomaly detection techniques to detect deviations from normal traffic patterns**

# DDoS Mitigation Strategy

## □ Key Elements in the Diagram

- **Nodes (R0 to R7)** represent **routers** in a network.
- **Arrows** indicate the **direction of traffic flow**:
  - **Black arrows** – normal traffic flow.
  - **Red arrows** – **pushback signals** or **reverse-flow mechanisms** indicating **defensive actions**.
- **"Pushback" label** near R0 → R3 – the core concept being illustrated.



# DDoS Mitigation Strategy

## ❑ How This Diagram Works

### 1. Attack Traffic Flow:

- Malicious traffic appears to enter through multiple routers (e.g., R4, R5, R6, R7).
- These converge toward the central router R0, causing potential congestion or a threat.

### 2. Detection and Response:

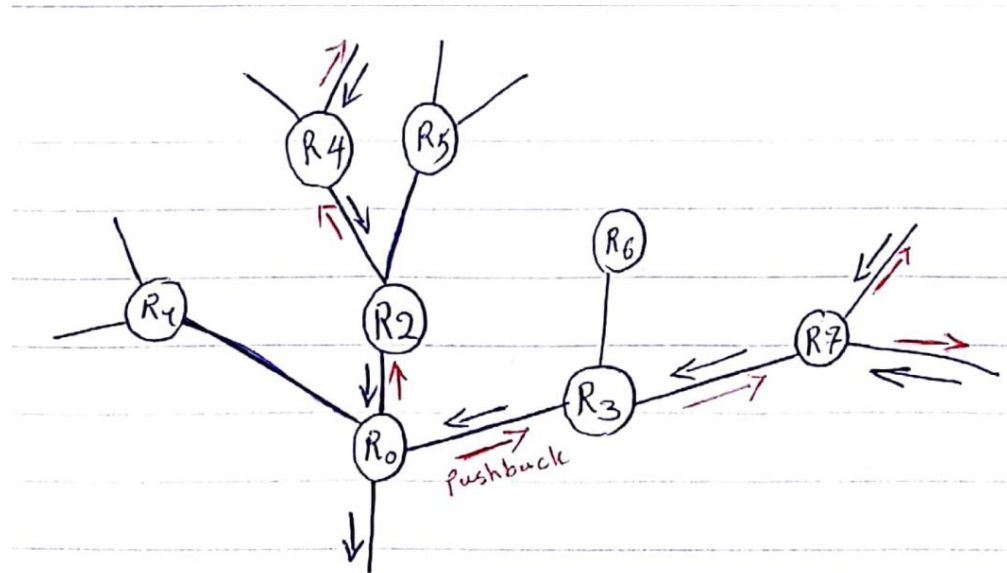
- R0 detects the issue (e.g., excessive traffic or attack behavior) and initiates a pushback to upstream nodes, like R2 and R3.
- This is indicated by the red arrows going "against" the normal traffic flow.

### 3. Cooperation:

- Routers R2, R3 then relay the pushback signal further upstream to R4, R5, R6, R7, asking them to rate-limit or drop suspicious packets.
- This cooperative behavior helps distribute the defense and reduce the burden on any single router.

### 4. Effect:

1. Traffic is filtered closer to the source.
2. The overall network is protected, and resources are used more efficiently.



# DDoS Mitigation Strategy

---

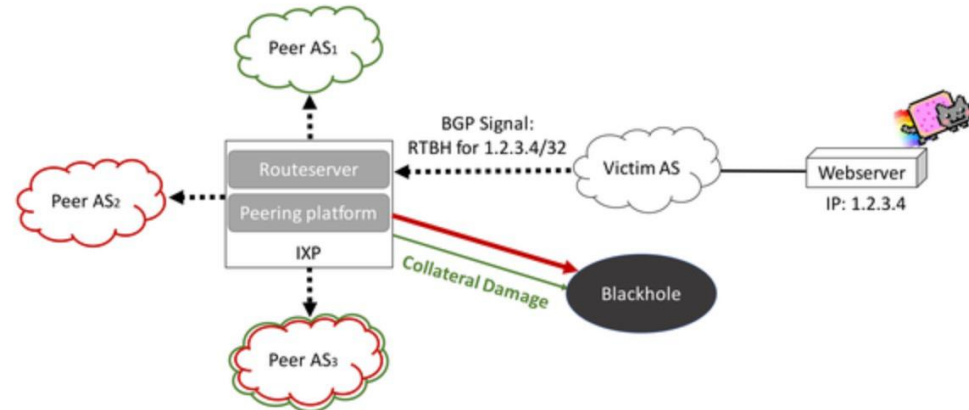
## 3- Blackholing cooperative defense:

- It involves the **coordinated efforts of multiple network entities to mitigate the impact of DDoS attacks.**
- It focuses on **diverting malicious traffic** to a "**blackhole**" or **sinkhole**, effectively **discarding the traffic before it reaches the target network.**
- Here's how blackholing cooperative defense can be implemented:
  - **Routing Configuration:** The participating entities update **their routing configurations to redirect the traffic towards the blackhole destination.** This can involve *modifying routing tables, applying access control lists (ACLs), or using Border Gateway Protocol (BGP) to route the attack traffic to the blackhole.*

# DDoS Mitigation Strategy

## □ Key Components:

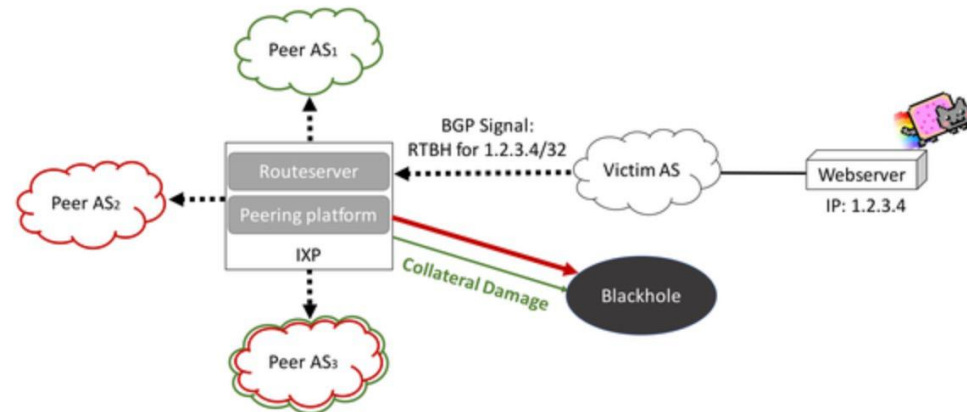
- **Victim AS:** The Autonomous System (AS) under attack, hosting a **webserver** at IP 1.2.3.4.
- **Peer AS1/AS2/AS3:** Neighboring ASes collaborating to filter attack traffic.
- **Routeserver/IXP/Peering Platform:** Infrastructure facilitating BGP route exchange between ASes.
- **Blackhole:** A null route where unwanted traffic is discarded.
- **BGP Signal:** The victim announces an RTBH (Remotely Triggered Black Hole) route for 1.2.3.4/32.



# DDoS Mitigation Strategy

## ❑ Process:

1. **Attack Detection:** The Victim AS detects a DDoS attack targeting its webserver (1.2.3.4).
2. **RTBH Trigger:** The victim sends a BGP update to the **Routeserver/IXP**, advertising a route for 1.2.3.4/32 with a "no-export" community or specific blackhole tag.
3. **Propagation:** The Routeserver distributes this route to **Peer AS1, AS2, and AS3** (cooperating networks).
4. **Traffic Filtering:**
  1. Peer ASes install **the blackhole route**, redirecting all traffic destined for 1.2.3.4 to a null interface (discarding it).
  2. This stops attack traffic at the edge of participating networks, reducing the load on the victim's infrastructure.



# DDoS Mitigation Strategy

---

## ❑ Mitigation Strategy – Non-Collaborative

- In **non-collaborative DDoS mitigation strategies**, there are two main approaches: **Static Mitigation** and **Dynamic Mitigation**.

### 1. Static Mitigation:

- It involves **implementing predetermined measures that are designed to withstand and mitigate common DDoS attack vectors**.
- These measures are typically **configured in advance and remain relatively unchanged during an attack**.
- Example of static mitigation strategies include: **Server Load Balancing**.



# DDoS Mitigation Strategy

---

- **Example: Server Load Balancing:**

- ✓ Distributing incoming traffic across multiple servers using load balancing techniques to prevent a single server from becoming overwhelmed by a DDoS attack.
- ✓ Load balancing helps distribute the load and ensures that resources are efficiently utilized.

# DDoS Mitigation Strategy

---

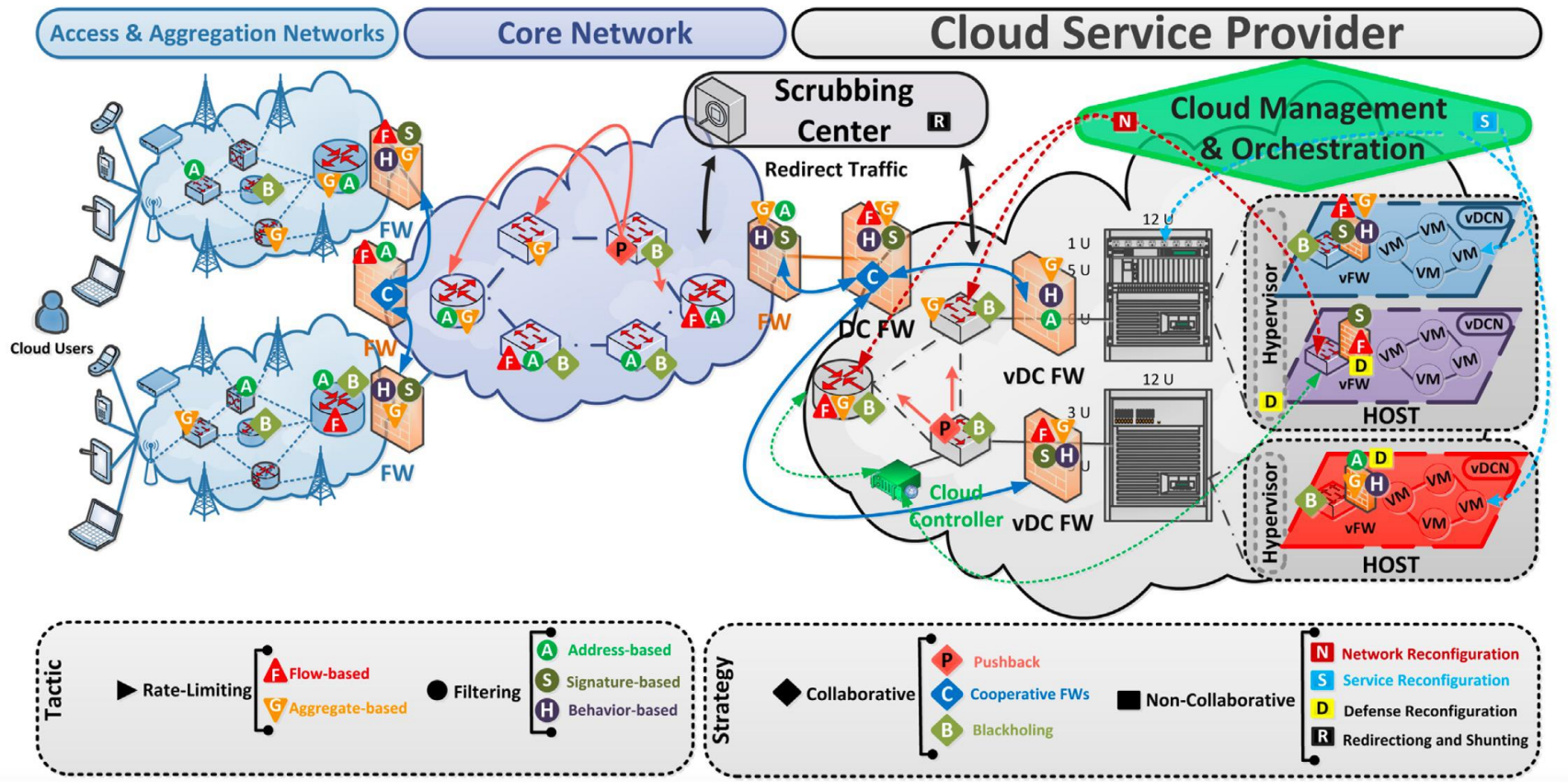
## 2. Dynamic Mitigation:

- It involves the use of real-time monitoring and adaptive techniques to respond to evolving DDoS attack patterns.
- These measures adapt and respond to the changing attack landscape during an attack.
- Examples of dynamic mitigation strategies include: Automatic Traffic Rate Adjustments.
- **Example: Automatic Traffic Rate Adjustments:**
  - ✓ Implementing automated traffic rate adjustments based on the network's capacity and available resources.
  - ✓ This can involve dynamically adjusting traffic shaping or rate limiting policies to prevent network congestion and ensure the availability of critical services.

# Advantages and disadvantages of DDoS mitigation strategies

Mitigation Strategy	Strategy Model	Advantages	Disadvantages
Collaborative	Cooperative Firewalls, Pushback, Blackholing	<ul style="list-style-type: none"><li>• Containing the attack close the attack sources</li><li>• Considering distributed mitigation architecture (robust against attack)</li></ul>	<ul style="list-style-type: none"><li>• Difficult to put in place the collaboration</li><li>• Difficult to put in place trust and secure interactions between different domains</li><li>• Dependent on network topology</li></ul>
Non-Collaborative	Static	<ul style="list-style-type: none"><li>• Easy to deploy and put in place</li></ul>	<ul style="list-style-type: none"><li>• Inability to automatically adjust the defense architecture based on severity of DDoS attack</li></ul>
	Reconfiguration (Service, Network, Defense)	<ul style="list-style-type: none"><li>• Efficient defense as it is elastic</li><li>• Distributed solution therefore more reliable as it could create instances in different DCs</li><li>• Scalable solution as it could divide the attack into smaller chunks</li></ul>	<ul style="list-style-type: none"><li>• Deploy at victim side</li><li>• Need for some orchestration and precise information about resources and network topology in order to put in place the defense mechanisms</li></ul>
	Redirecting and Shunting	<ul style="list-style-type: none"><li>• Shield completely the target</li></ul>	<ul style="list-style-type: none"><li>• More difficult to put in place</li></ul>

# mitigation strategies against DDoS attacks



# Recap: DDoS mitigation techniques

Mitigation strategy	Strategy model	Mitigation tactic	Network		Protection point		
			Traditional	SDN-based	Source-end	Core	Victim-end
Collaborative	Cooperative Firewalls	Rate-limiting	✓		✓		
Non-Collaborative	Static	Filtering	✓		✓		
Collaborative	Cooperative Firewalls	Rate-limiting	✓		✓		
Non-Collaborative	Static	Rate-limiting		✓		✓	
Non-Collaborative	Static	Filtering		✓		✓	
Non-Collaborative	Static	Rate-limiting		✓		✓	
Collaborative	Pushback	Rate-limiting		✓	✓		
Non-Collaborative	Network Reconfiguration	Filtering	✓				✓
Non-Collaborative	Static	Filtering		✓	✓		
Non-Collaborative	Static	Filtering	✓				✓
Non-Collaborative	Redirecting & Shunting	Filtering	✓				✓
Non-Collaborative	Service and Defense (hybrid) Reconfiguration	Filtering	✓				✓
Non-Collaborative	Defense Reconfiguration	Filtering		✓		✓	
Collaborative	Cooperative Firewalls	Rate-limiting		✓	✓	✓	
Collaborative	Pushback	Rate-limiting		✓	✓		