Security Fundamentals

Security Terminology

- **Mitigation Techniques**

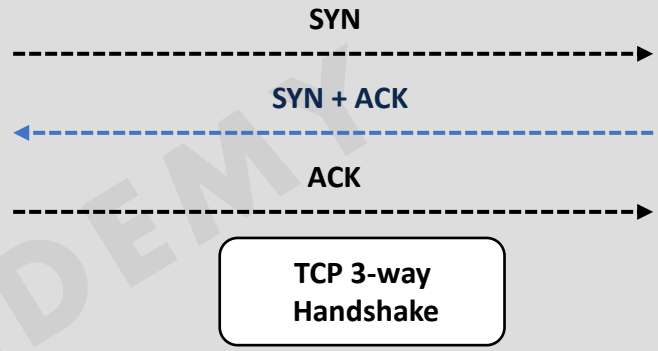
Common Security Threats

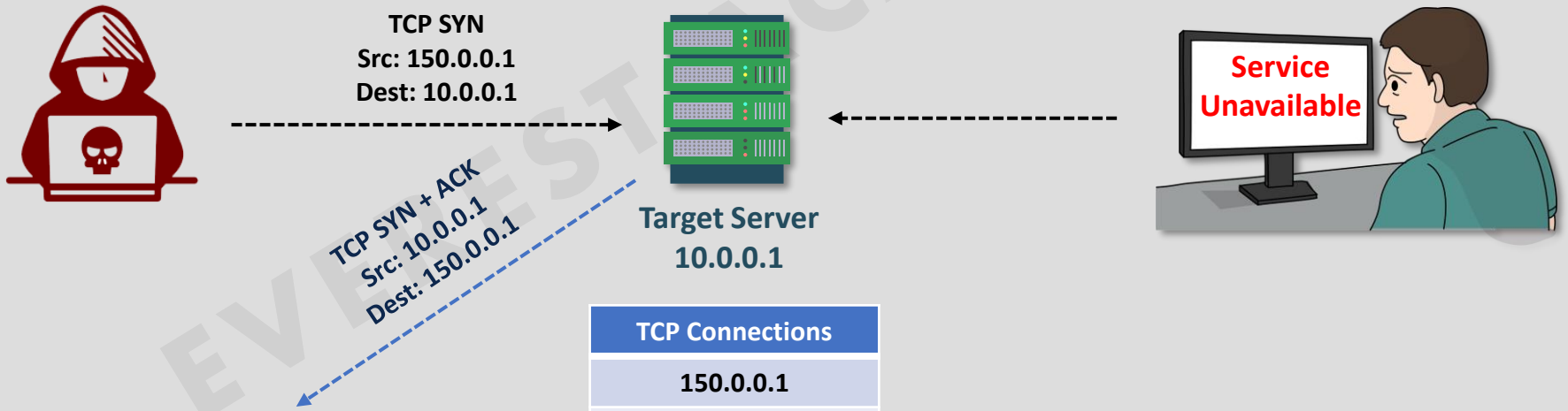
- **Attacks That Spoof Addresses :**
  - Denial-of-Service (DoS) Attacks.
  - Reflection and Amplification Attacks.
  - Man-in-the-Middle Attacks.

Common Security Threats

❑ Attacks That Spoof Addresses :

- ➢ Denial-of-Service (DoS) Attacks.
- ➢ Reflection and Amplification Attacks.
- ➢ Man-in-the-Middle Attacks.

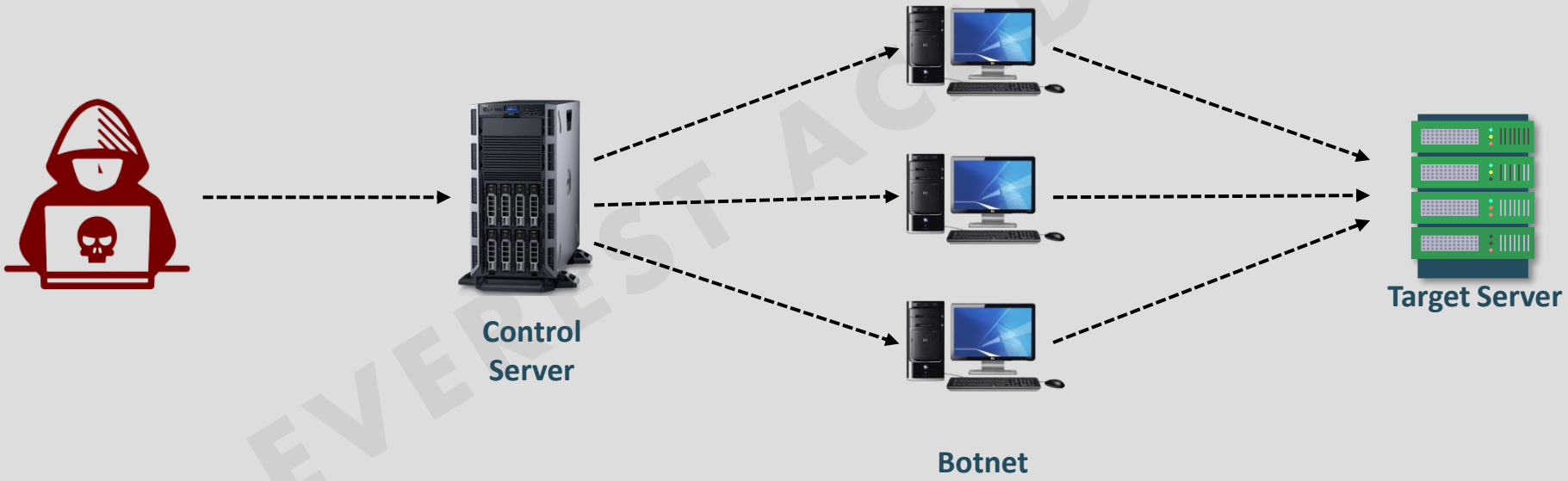




TCP Connections
150.0.0.1
150.0.0.1
150.0.0.1
150.0.0.1
Full

Common Security Threats

- **Attacks That Spoof Addresses :**
  - Denial-of-Service (DoS) Attacks.
  - Reflection and Amplification Attacks.
  - Man-in-the-Middle Attacks.

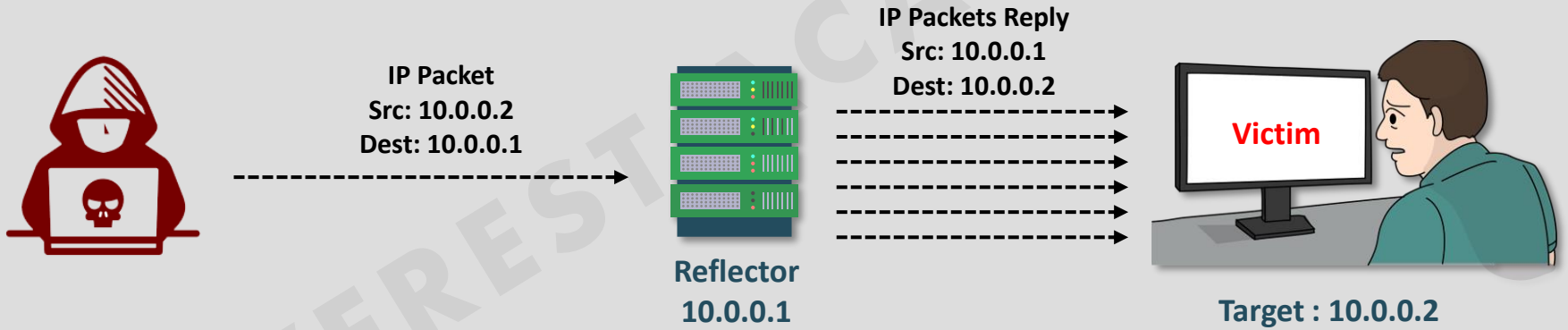


Distributed Denial-of-Service (DDOS) Attack

Common Security Threats

❑ Attacks That Spoof Addresses :

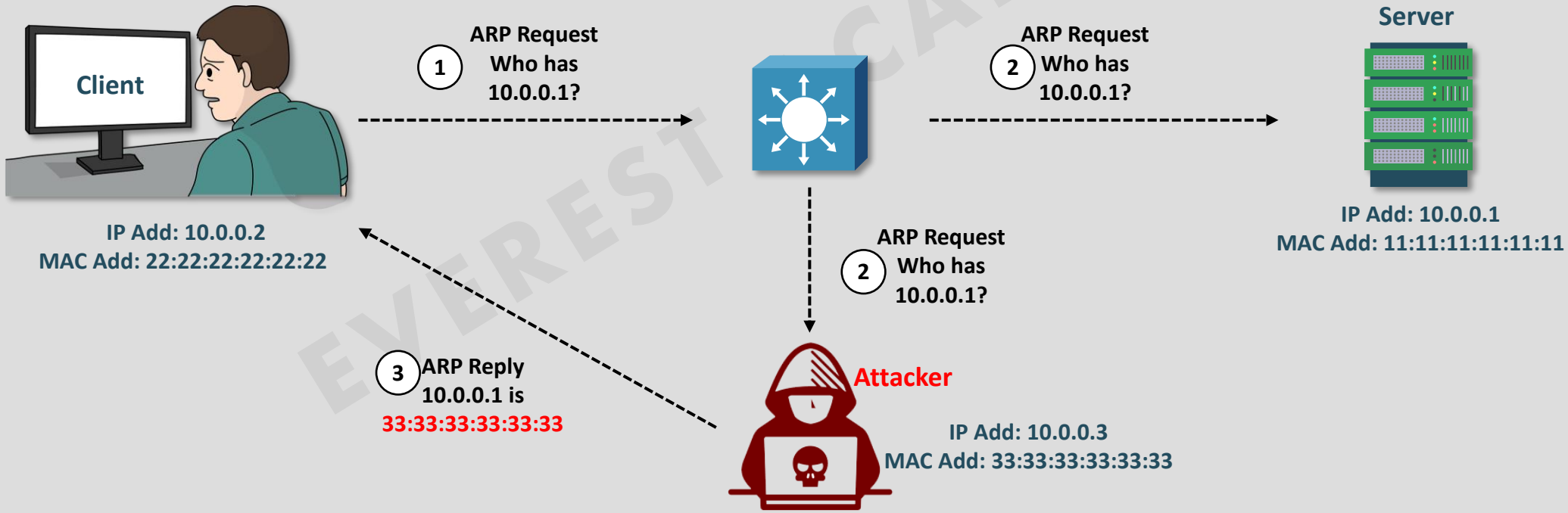
- ➢ Denial-of-Service (DoS) Attacks.
- ➢ Reflection and Amplification Attacks.
- ➢ Man-in-the-Middle Attacks.



Common Security Threats

❑ Attacks That Spoof Addresses :

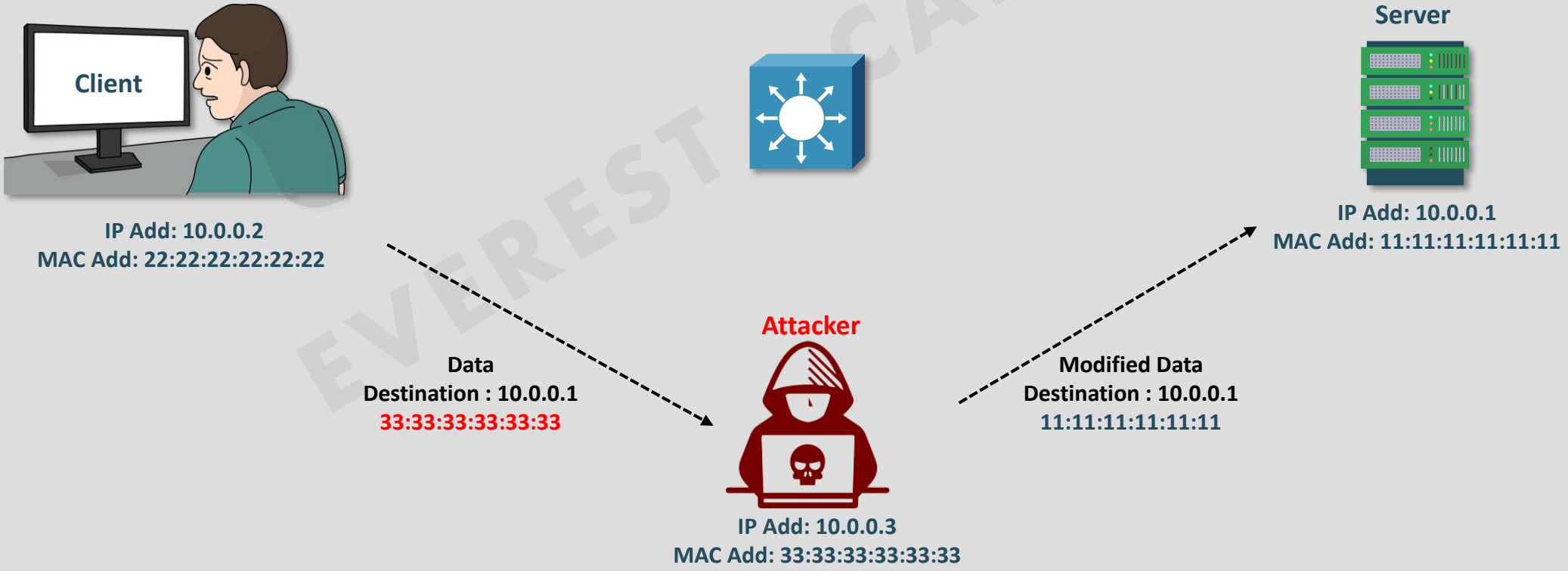
- ➢ Denial-of-Service (DoS) Attacks.
- ➢ Reflection and Amplification Attacks.
- ➢ Man-in-the-Middle Attacks.



Common Security Threats

❑ Attacks That Spoof Addresses :

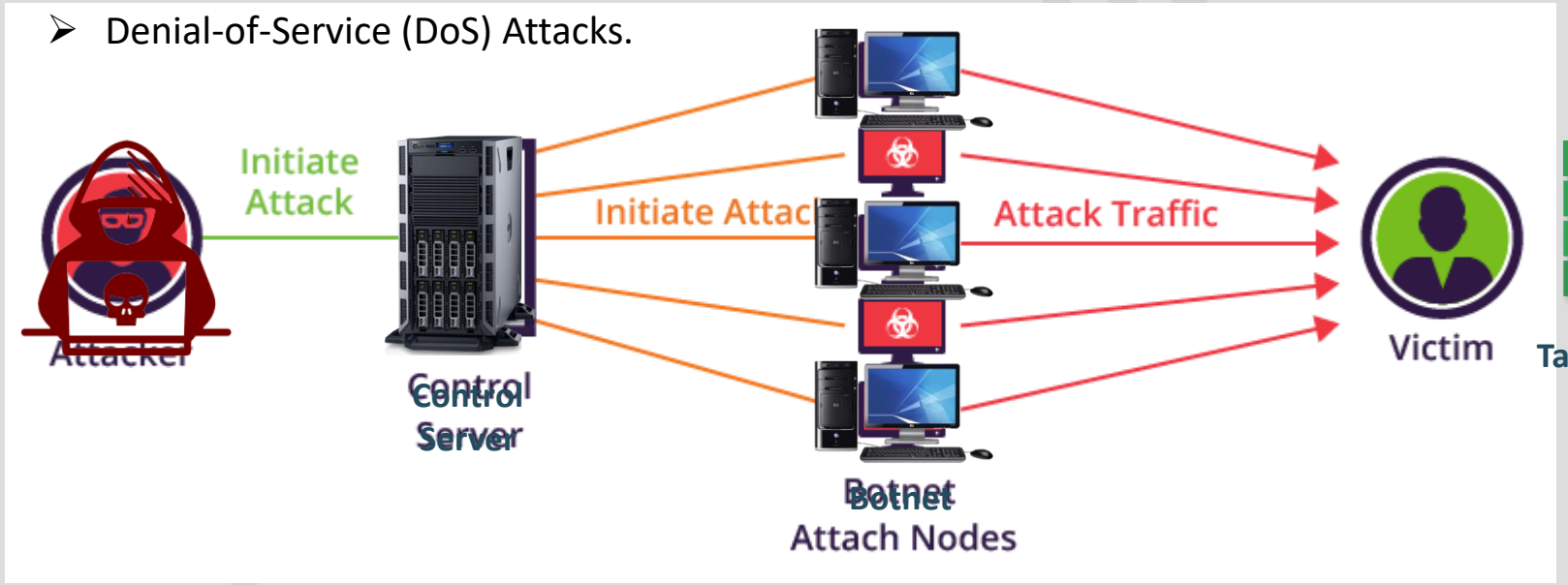
- ➢ Denial-of-Service (DoS) Attacks.
- ➢ Reflection and Amplification Attacks.
- ➢ Man-in-the-Middle Attacks.



Security Fundamentals

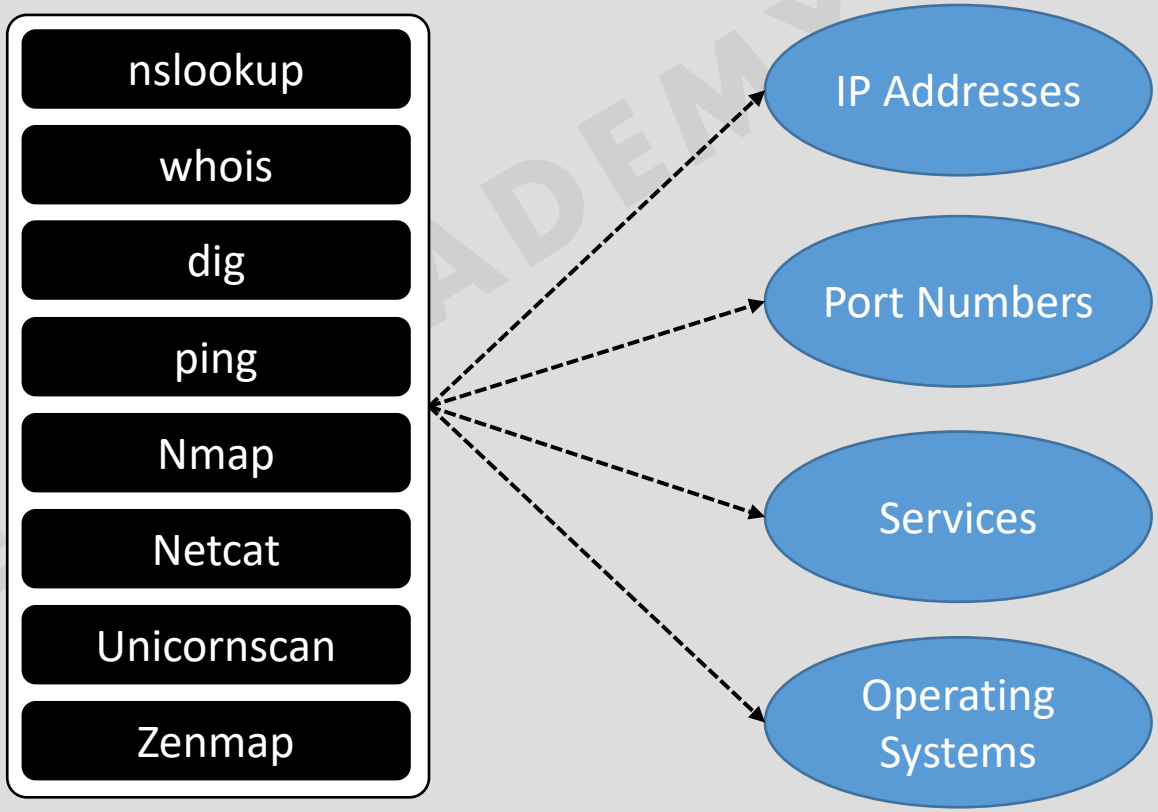
Common Security Threats

❑ **Attacks That Spoof Addresses :**



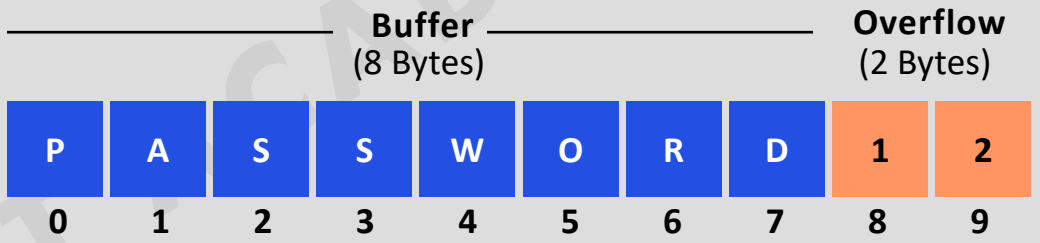
Common Security Threats

- **Attacks That Spoof Addresses :**
  - Denial-of-Service (DoS) Attacks.
  - Reflection and Amplification Attacks.
  - Man-in-the-Middle Attacks.
- **Reconnaissance Attacks.**
- **Buffer Overflow Attacks.**
- **Malware.**
- **Human Vulnerabilities.**
- **Password Vulnerabilities.**



Common Security Threats

- **Attacks That Spoof Addresses :**
  - Denial-of-Service (DoS) Attacks.
  - Reflection and Amplification Attacks.
  - Man-in-the-Middle Attacks.
- **Reconnaissance Attacks.**
- **Buffer Overflow Attacks.**
- **Malware.**
- **Human Vulnerabilities.**
- **Password Vulnerabilities.**



Common Security Threats

- **Attacks That Spoof Addresses :**
  - Denial-of-Service (DoS) Attacks.
  - Reflection and Amplification Attacks.
  - Man-in-the-Middle Attacks.
- **Reconnaissance Attacks.**
- **Buffer Overflow Attacks.**
- **Malware.**
- **Human Vulnerabilities.**
- **Password Vulnerabilities.**

Common Security Threats

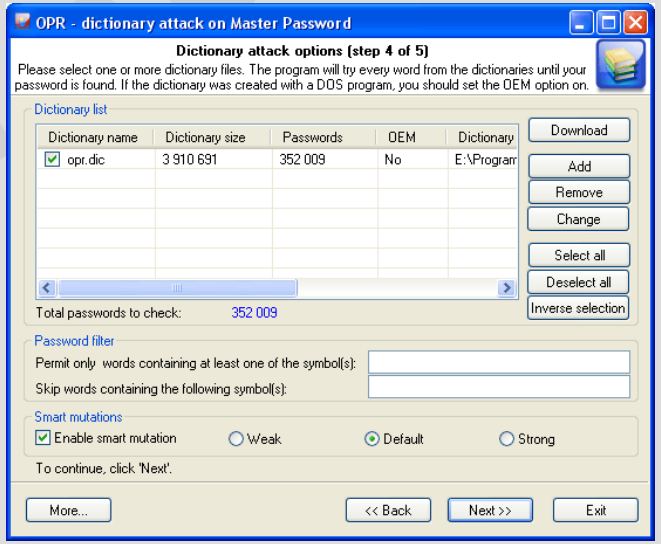
- **Attacks That Spoof Addresses :**
  - Denial-of-Service (DoS) Attacks.
  - Reflection and Amplification Attacks.
  - Man-in-the-Middle Attacks.
- **Reconnaissance Attacks.**
- **Buffer Overflow Attacks.**
- **Malware.**
- **Human Vulnerabilities.**
- **Password Vulnerabilities.**

1	**Social Engineering**	Exploits human trust and social behavior
2	**Phishing**	Disguises a malicious invitation as something legitimate
3	**Spear Phishing**	Targets group of similar users
4	**Whaling**	Targets high-profile individuals
5	**Vishing**	Uses voice calls
6	**Smishing**	Uses SMS text messages
7	**Pharming**	Uses legitimate services to send users to a compromised site
8	**Watering Hole**	Targets specific victims who visit a compromised site

Common Security Threats

- **Attacks That Spoof Addresses :**
  - Denial-of-Service (DoS) Attacks.
  - Reflection and Amplification Attacks.
  - Man-in-the-Middle Attacks.
- **Reconnaissance Attacks.**
- **Buffer Overflow Attacks.**
- **Malware.**
- **Human Vulnerabilities.**
- **Password Vulnerabilities.**
  - Dictionary attack
  - Brute-force Attack

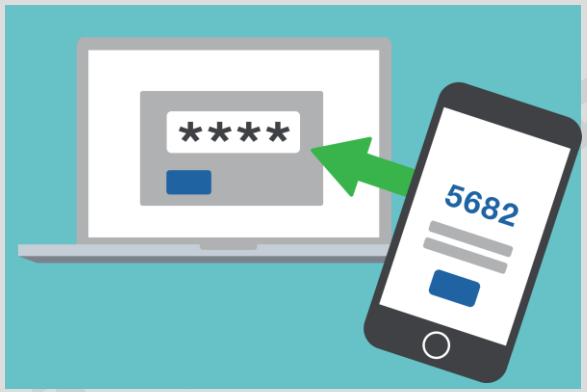
User Name	Password
admin	admin
admin	123
admin	password
admin	123456



Common Security Threats

- **Attacks That Spoof Addresses :**
  - Denial-of-Service (DoS) Attacks.
  - Reflection and Amplification Attacks.
  - Man-in-the-Middle Attacks.
- **Reconnaissance Attacks.**
- **Buffer Overflow Attacks.**
- **Malware.**
- **Human Vulnerabilities.**
- **Password Vulnerabilities.**
  - Dictionary attack
  - Brute-force Attack
- **Password Alternatives.**

Two-factor

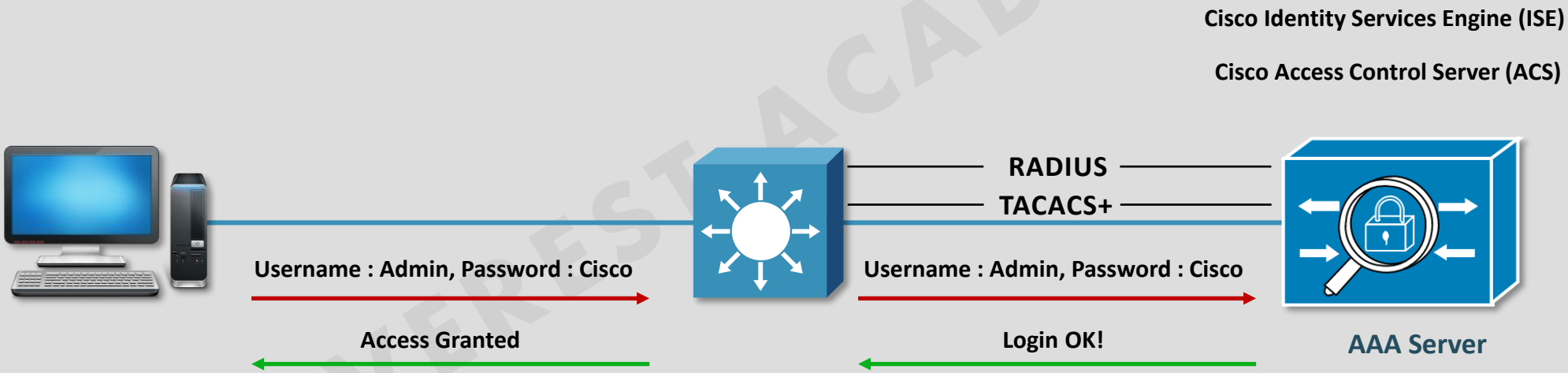


Digital Certificate

Biometric

Controlling and Monitoring User Access

- **Authentication, authorization, and accounting (AAA).**
  - **Authentication**: Who is the user?
  - **Authorization**: What is the user allowed to do?
  - **Accounting**: What did the user do?



Securing IOS Passwords

1

```
R1# conf t
R1(config)# enable password MyEnablePassword
R1(config)# line vty 0 4
R1(config-line)# transport input telnet
R1(config-line)# password MyTelnetPassword
R1(config-line)# login
R1(config-line)# end
```

1

```
R1# show run
no service password-encryption
enable password MyEnablePassword
line vty 0 4
 password MyTelnetPassword
 login
 transport input telnet
```

2

```
R1# conf t
R1(config)# service password-encryption
R1(config)# enable password MyEnablePassword
R1(config)# line vty 0 4
R1(config-line)# transport input telnet
R1(config-line)# password MyTelnetPassword
R1(config-line)# login
R1(config-line)# end
```

2

```
R1# show run
service password-encryption
enable password 7 080C557D0C1A1712063B0D17393C2B3A37
line vty 0 4
 password 7 11240031121E0509101A2A373B243A3017
 login
 transport input telnet
```

3

```
R1# conf t
R1(config)# service password-encryption
R1(config)# enable secret MySecretPassword
R1(config)# line vty 0 4
R1(config-line)# transport input telnet
R1(config-line)# password MyTelnetPassword
R1(config-line)# login
R1(config-line)# end
```

3

```
R1# show run
service password-encryption
enable secret 5 $1$lKdP$00L7JOY8vqQ3d84TVuhbV.
line vty 0 4
 password 7 11240031121E0509101A2A373B243A3017
 login
 transport input telnet
```

Securing IOS Passwords

3

```
R1# conf t
R1(config)# service password-encryption
R1(config)# enable secret MySecretPassword
R1(config)# line vty 0 4
R1(config-line)# transport input telnet
R1(config-line)# password MyTelnetPassword
R1(config-line)# login
R1(config-line)# end
```

3

```
R1# show run
service password-encryption
enable secret 5 $1$lKdP$00L7JOY8vqQ3d84TVuhbV.
line vty 0 4
  password 7 11240031121E0509101A2A373B243A3017
  login
  transport input telnet
```

4

```
R1# conf t
R1(config)# username admin password AdminPassword
R1(config)# enable secret MySecretPassword
R1(config)# line vty 0 4
R1(config-line)# transport input telnet
R1(config-line)# login local
R1(config-line)# end
```

4

```
R1# show run
enable secret 5 $1$Pmn8$8vShVq3TrDaRO/ugQBc39/
username admin password 0 AdminPassword
line vty 0 4
 login local
 transport input telnet
```

5

```
R1# conf t
R1(config)# username admin secret AdminPassword
R1(config)# enable secret MySecretPassword
R1(config)# line vty 0 4
R1(config-line)# transport input telnet
R1(config-line)# login local
R1(config-line)# end
```

5

```
R1# show run
enable secret 5 $1$Pmn8$8vShVq3TrDaRO/ugQBc39/
username admin secret 5 $1$nBMc$X80wz4vpBtbauWFRo2zqP.
line vty 0 4
 login local
 transport input telnet
```

Securing IOS Passwords

Type 5	R1(config)# enable algorithm-type **md5** secret *MySecretPassword*
Type 8	R1(config)# enable algorithm-type **sha256** secret *MySecretPassword*
Type 9	R1(config)# enable algorithm-type **scrypt** secret *MySecretPassword*

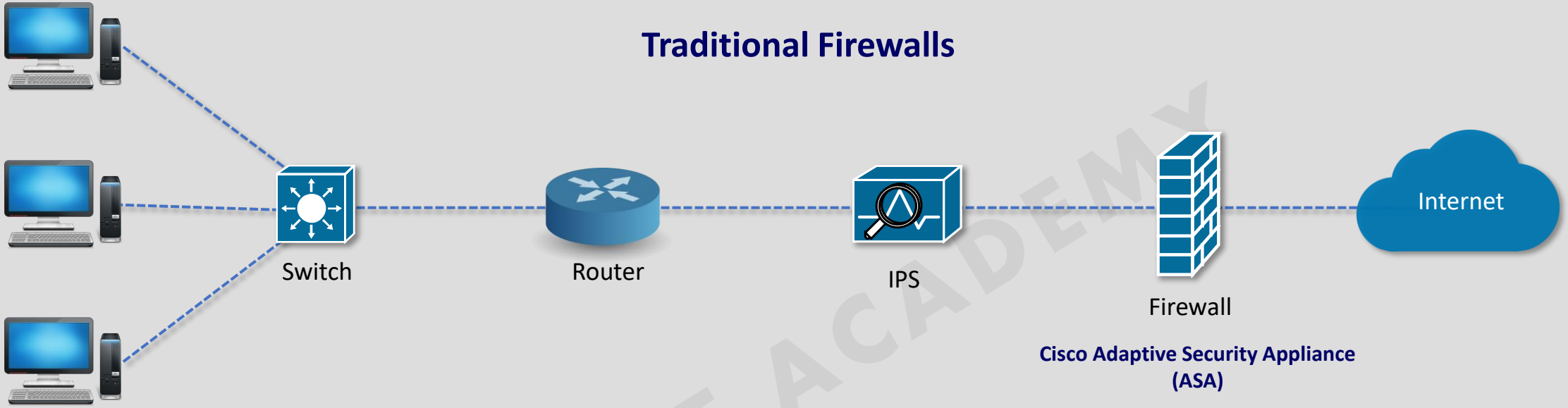
md5	Selects the message digest algorithm 5 (**MD5**) as the hashing algorithm.
sha256	Selects Password-Based Key Derivation Function 2 (**PBKDF2**) with Secure Hash Algorithm, 26-bits (**SHA-256**) as the hashing algorithm.
scrypt	Selects **scrypt** as the hashing algorithm.

Securing VTY Access Using ACL

```
R2(config)# line vty 0 4
R2(config-line)# access-class standard_ACL_#  in | out
```

Firewalls and Intrusion Prevention Systems (IPSs)

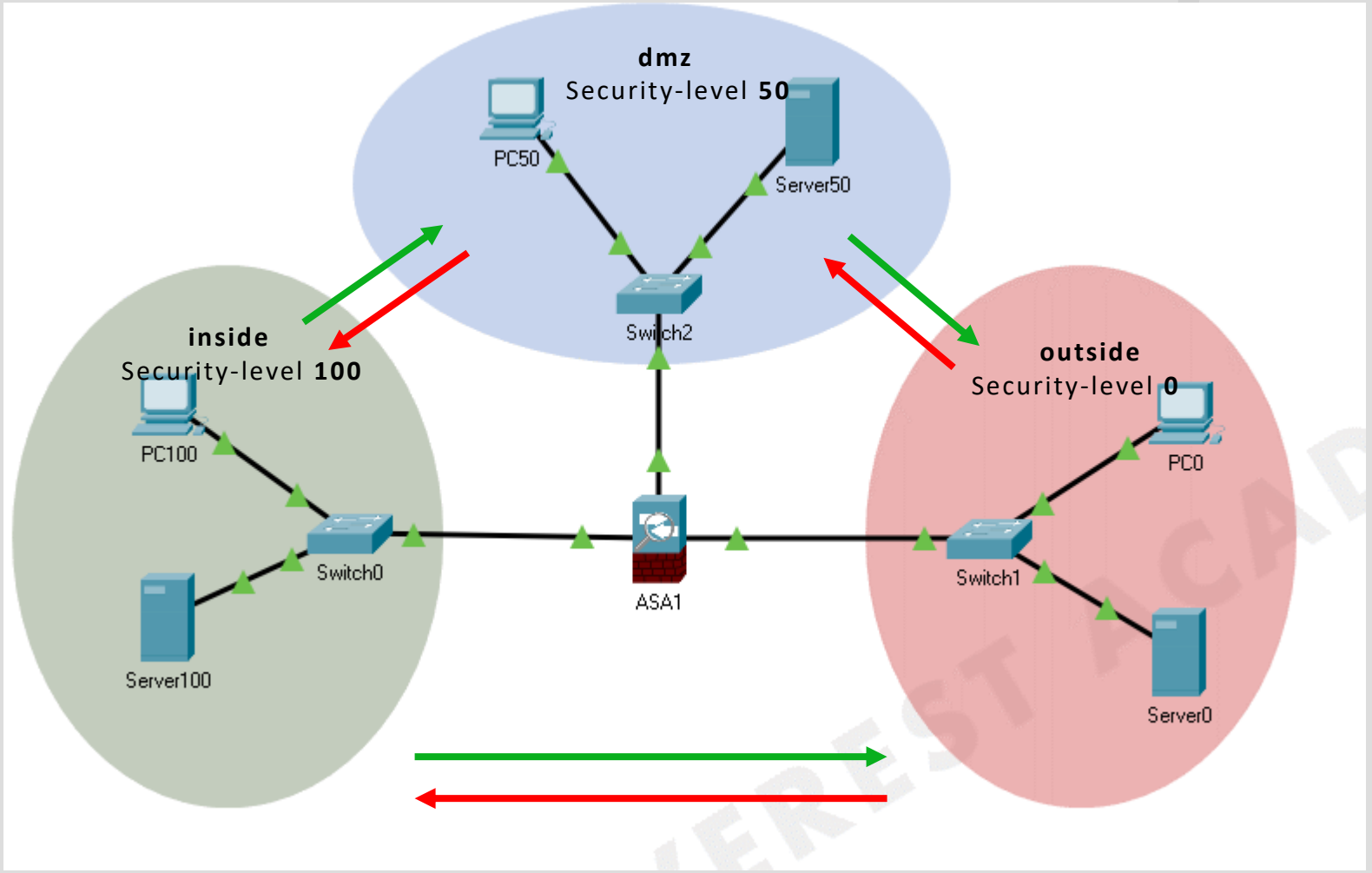
Traditional Firewalls

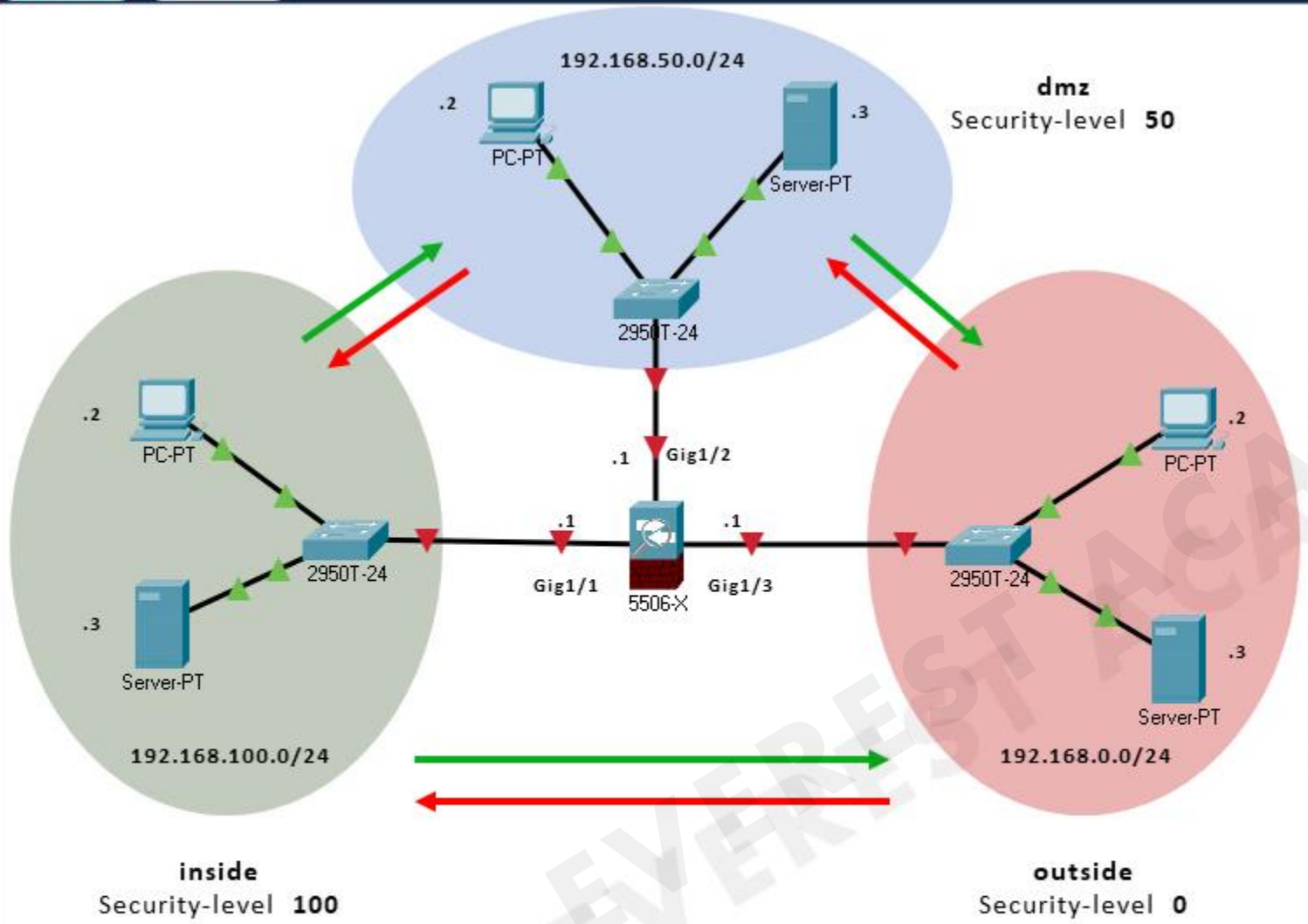


- Match the source and destination IP addresses.
- Identify applications by matching their static well-known TCP and UDP ports.
- Watch application-layer flows to know what additional TCP and UDP ports are used by a particular flow, and filter based on those ports.
- Match the text in the URI of an HTTP request.
- Keep state information by storing information about each packet, and make decisions about filtering future packets based on the historical state information (called ***stateful inspection***).

Firewalls and Intrusion Prevention Systems (IPSs)

Security Zones






```
conf t
class-map inspection_default
 match default-inspection-traffic
exit
policy-map global_policy
class inspection_default
  inspect dns
  inspect ftp
  inspect http
  inspect icmp
  inspect tftp
service-policy global_policy global

access-list outside-to-dmz permit tcp any host 192.168.50.3 eq www
access-group outside-to-dmz in interface outside
```

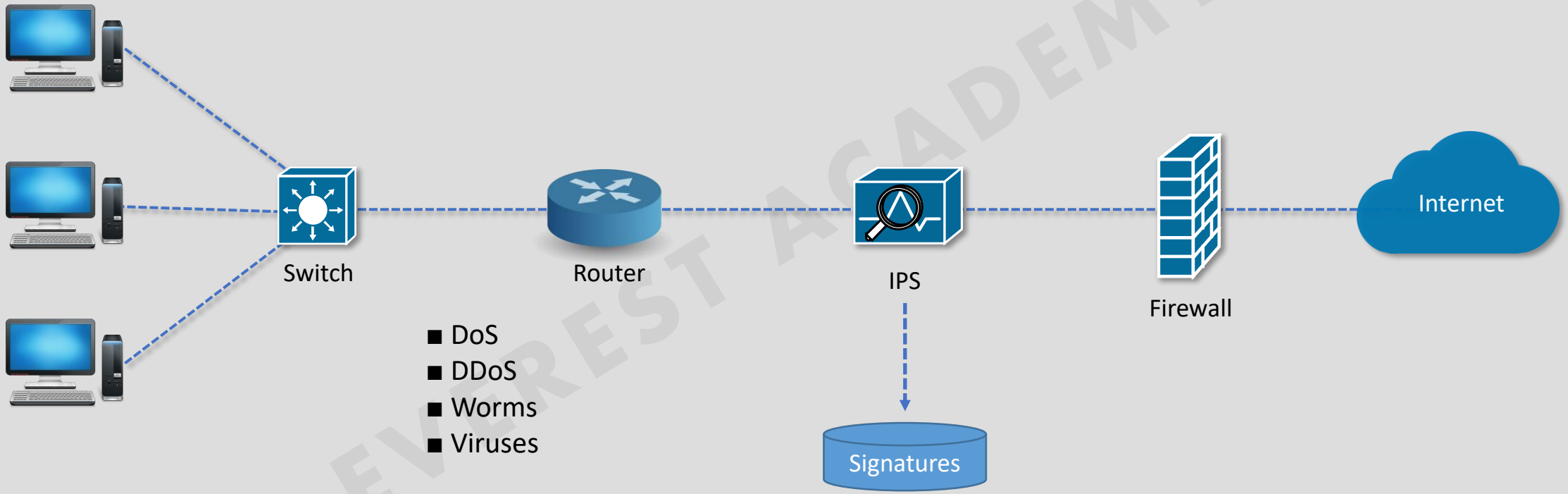
```
interface GigabitEthernet1/1
 ip address 192.168.100.1 255.255.255.0
 nameif inside
 security-level 100
 no shutdown
```

```
interface GigabitEthernet1/2
 ip address 192.168.50.1 255.255.255.0
 nameif dmz
 security-level 50
 no shutdown
```

```
interface GigabitEthernet1/3
 ip address 192.168.0.1 255.255.255.0
 nameif outside
 security-level 0
 no shutdown
```

Firewalls and Intrusion Prevention Systems (IPS)

Traditional Intrusion Prevention Systems (IPS)



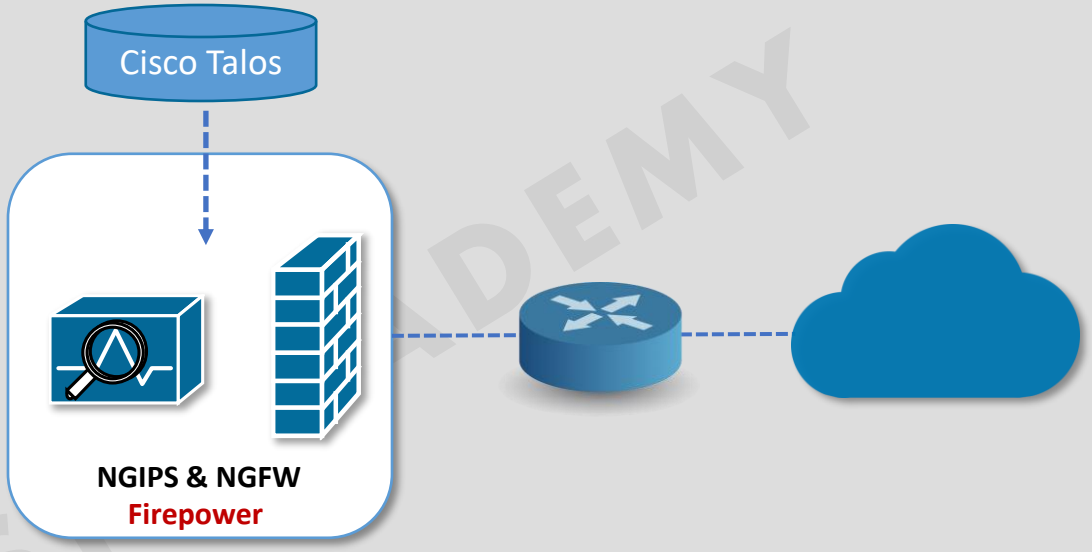
Firewalls and Intrusion Prevention Systems (IPS)

Next-Generation Firewalls and Next-Generation IPS

- Traditional Firewalls
- Traditional IPS

2013

Sourcefire



- Next-Generation Firewall with Next-Generation IPS Module

NGFW features	NGIPS features
▪ Traditional firewall.	▪ Traditional IPS.
▪ Application Visibility and Control (AVC).	▪ Application Visibility and Control (AVC).
▪ Advanced Malware Protection (AMP).	▪ Contextual Awareness.
▪ URL Filtering.	▪ Reputation-Based Filtering.
▪ Running NGIPS feature along with the firewall.	▪ Event Impact Level.

Firewalls and Intrusion Prevention Systems (IPS)

Next-Generation Firewalls and Next-Generation IPS

NGFW features	
▪ Traditional firewall.	An NGFW performs traditional firewall features, like stateful firewall filtering, NAT/PAT, and VPN termination.
▪ Application Visibility and Control (AVC).	This feature looks deep into the application layer data to identify the application. For instance, it can identify the application based on the data, rather than port number, to defend against attacks that use random port numbers.
▪ Advanced Malware Protection (AMP).	NGFW platforms run multiple security services, not just as a platform to run a separate service, but for better integration of functions. A network-based antimalware function can run on the firewall itself, blocking file transfers that would install malware, and saving copies of files for later analysis.
▪ URL Filtering.	This feature examines the URLs in each web request, categorizes the URLs, and either filters or rate limits the traffic based on rules. **The Cisco Talos security group** monitors and creates reputation scores for each domain known in the Internet, with URL filtering being able to use those scores in its decision to categorize, filter, or rate limit.
▪ NGIPS	The Cisco NGFW products can also run their NGIPS feature along with the firewall.

Firewalls and Intrusion Prevention Systems (IPS)

Next-Generation Firewalls and Next-Generation IPS

NGIPS features	
▪ Traditional IPS.	An NGIPS performs traditional IPS features, like using exploit signatures to compare packet flows, creating a log of events, and possibly discarding and/or redirecting packets.
▪ Application Visibility and Control (AVC).	As with NGFWs, an NGIPS has the ability to look deep into the application layer data to identify the application.
▪ Contextual Awareness	NGFW platforms gather data from hosts—OS, software version/ level, patches applied, applications running, open ports, applications currently sending data, and so on. Those facts inform the NGIPS as to the often more limited vulnerabilities in a portion of the network so that the NGIPS can focus on actual vulnerabilities while greatly reducing the number of logged events.
▪ Reputation-Based Filtering.	**The Cisco Talos security intelligence group** researches security threats daily, building the data used by the Cisco security portfolio. Part of that data identifies known bad actors, based on IP address, domain, name, or even specific URL, with a reputation score for each. A Cisco NGIPS can perform reputation-based filtering, taking the scores into account.
▪ Event Impact Level.	Security personnel need to assess the logged events, so an NGIPS provides an assessment based on impact levels, with characterizations as to the impact if an event is indeed some kind of attack.