

CHƯƠNG 3

WEB APPLICATION FIREWALL

9/21/2021

ThS. Nguyễn Duy
duyn@uit.edu.vn

Content

- What is WAF?
- Why we need to use WAF?
- Web Application architecture
- How does WAF prevent attacks?
- How to deploy WAF?

Content

- **What is WAF?**
- Why we need to use WAF?
- Web Application architecture
- How does WAF prevent attacks?
- How to deploy WAF?

What is WAF?

- A web application firewall (or WAF) filters, monitors, and blocks HTTP/HTTPS traffic to and from a web application.
- A WAF is differentiated from a regular firewall in that a WAF is able to filter the content of specific web applications while regular firewalls serve as a safety gate between servers.
- By inspecting HTTP traffic, it can prevent attacks stemming from web application security flaws, such as SQL injection, cross-site scripting (XSS), file inclusion, and security misconfigurations

TOP 10 OWASP – 2019

<https://owasp.org/www-project-top-ten/>

5

9/21/2021

Injection

Broken Authentication

Sensitive Data Exposure

XML External Entities (XXE)

Broken Access Control

Security Misconfiguration

Cross-Site Scripting XSS

Insecure Deserialization

Using Components with Known Vulnerabilities

Insufficient Logging & Monitoring

Web Attack Damage

- Loss of sensitive data
- Defaced Web site
- Lost Business
 - Web site blocked by search engines and AV software
 - Loss of customer trust



Reported Attack Site!

This web site at [http://www.example.com](#) has been reported as an attack site and has been blocked based on your security preferences.

Attack sites try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack sites intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

[Get me out of here!](#)

[Why was this site blocked?](#)

[Ignore this warning](#)

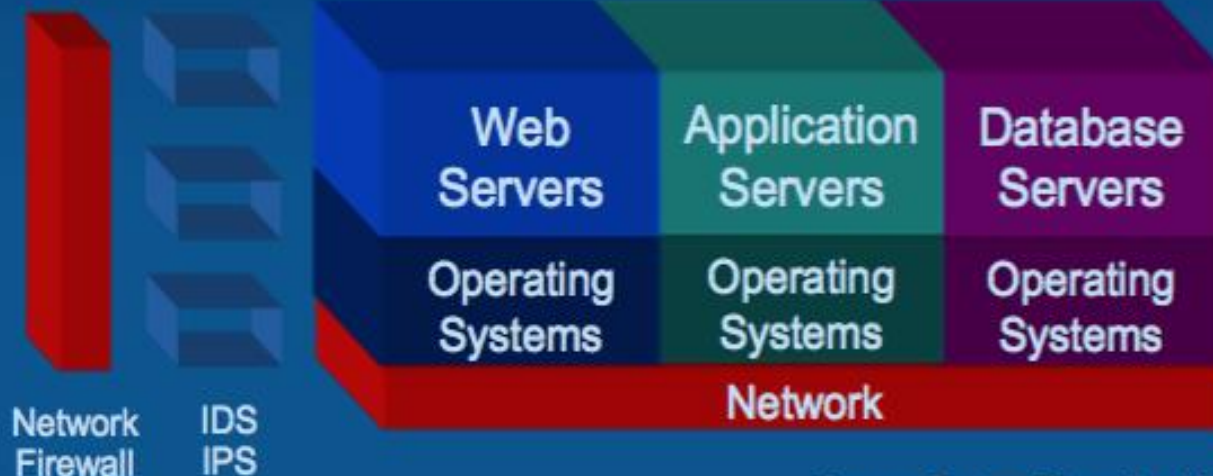
How Widespread Are Application Attacks?

75% of Attacks Focused on the Web applications

SQL Injection
Parameter Tampering
Cross-Site Scripting
Other Attacks

Customized Application Code

- Rushed to Production
- Written Before Security was a Priority



Confidential Data

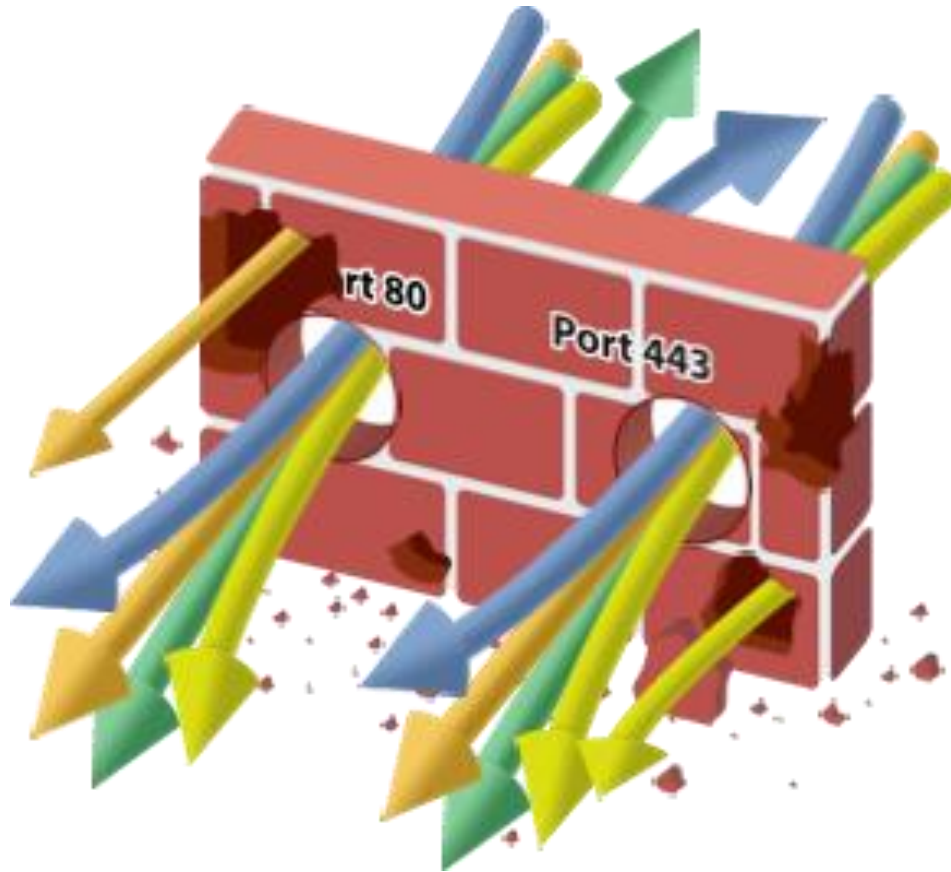
Content

- What is WAF?
- **Why we need to use WAF?**
- Web Application architecture
- How does WAF prevent attacks?
- How to deploy WAF?

Why we need to use WAF?

9

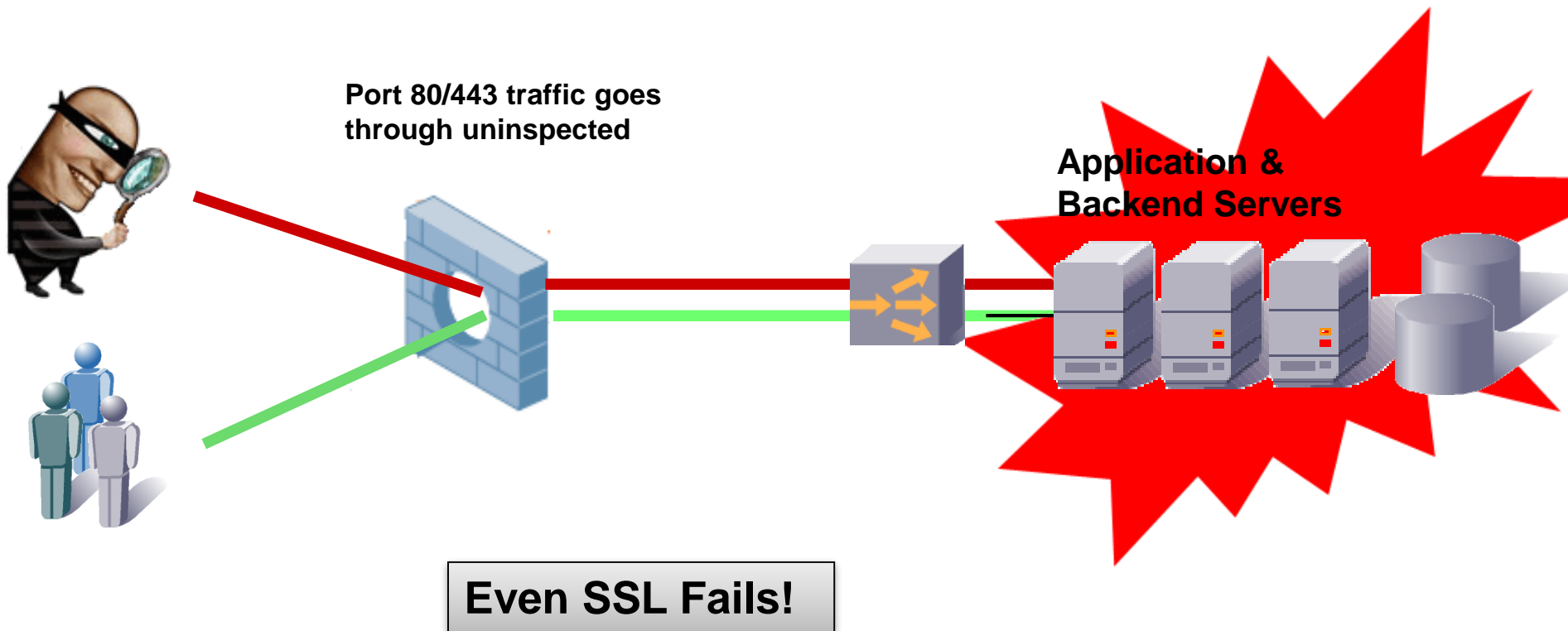
duyn@uit.edu.vn



Why Network Firewalls Fail

10

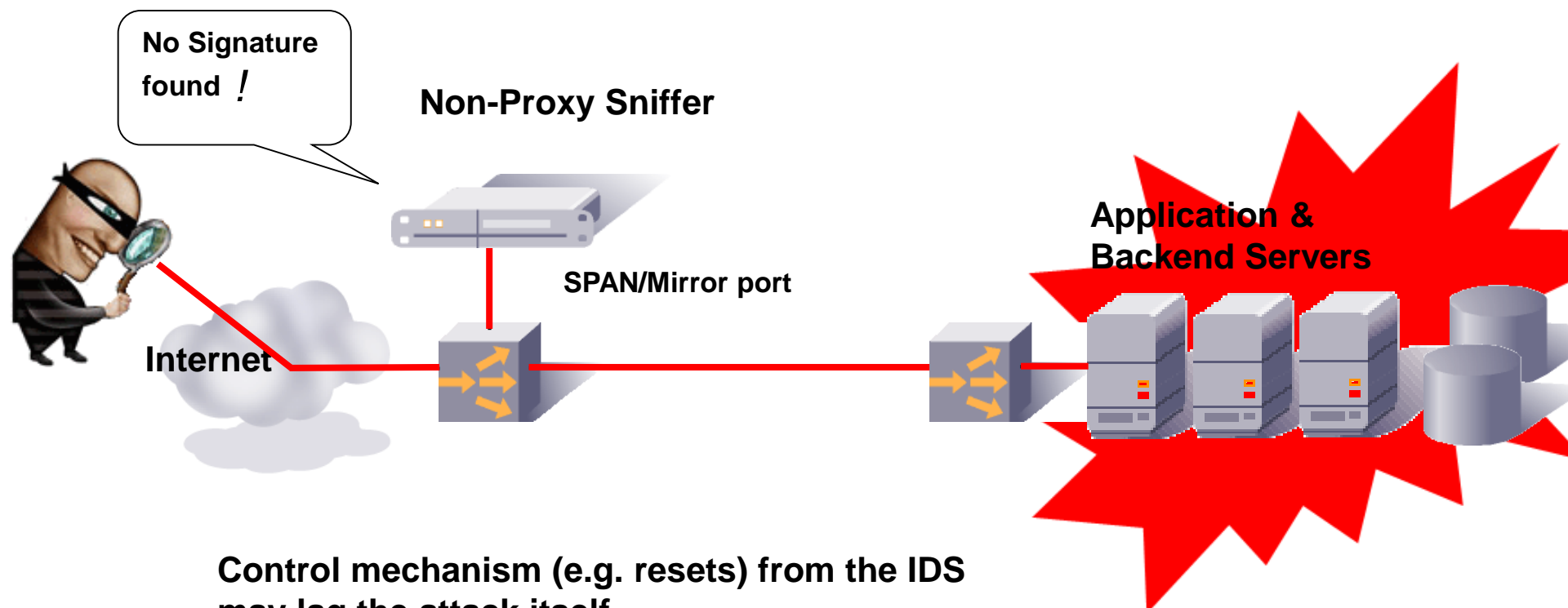
9/21/2021



Why Offline IDS/IPS Fail

11

9/21/2021



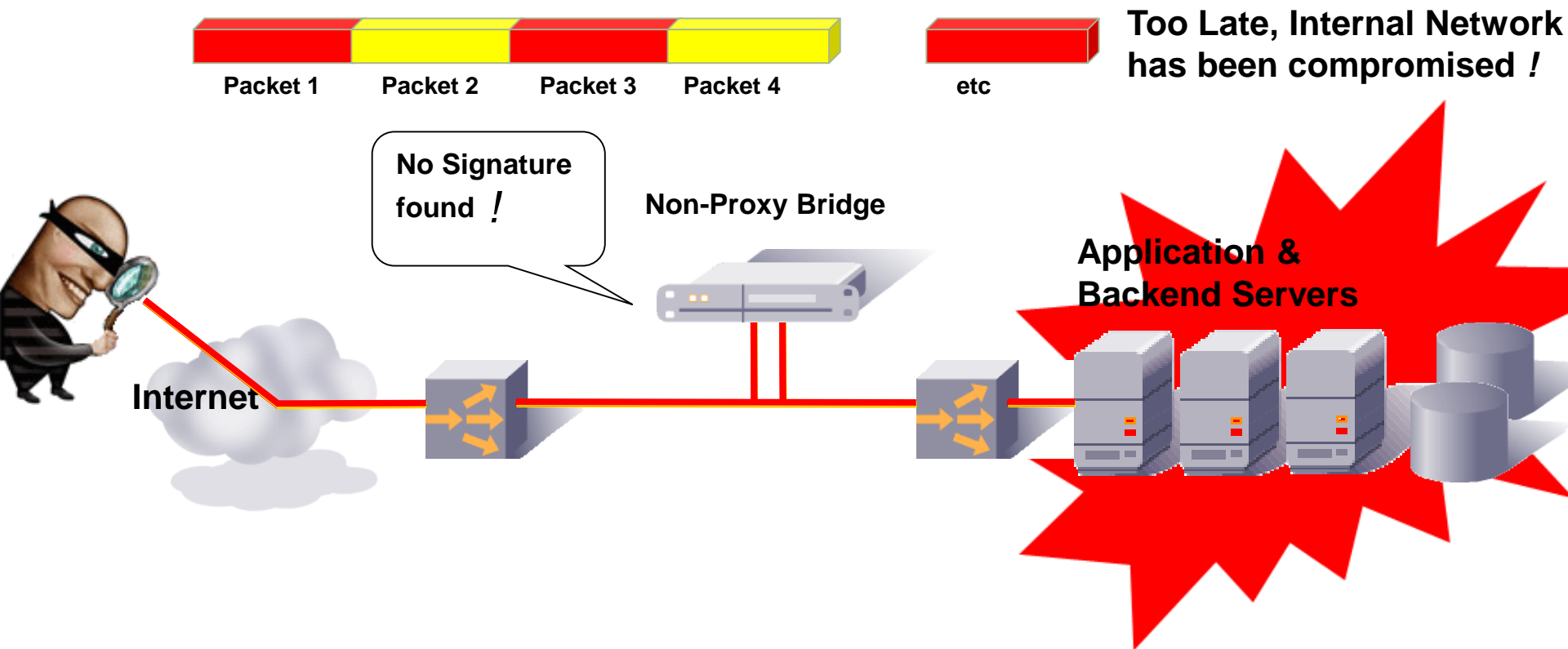
Control mechanism (e.g. resets) from the IDS may lag the attack itself

Signature based security does not protect from *zero day attacks*

Why Non-Proxy Inline Bridge Fails

12

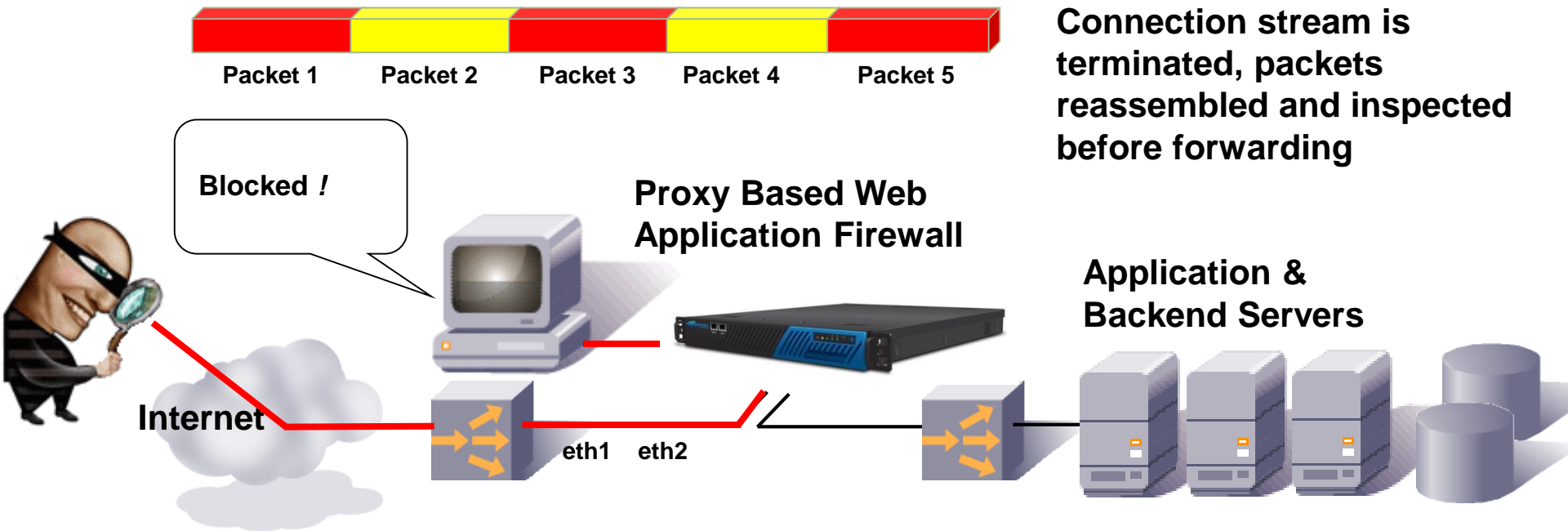
9/21/2021



Why Application Firewall Proxies Work

13

9/21/2021

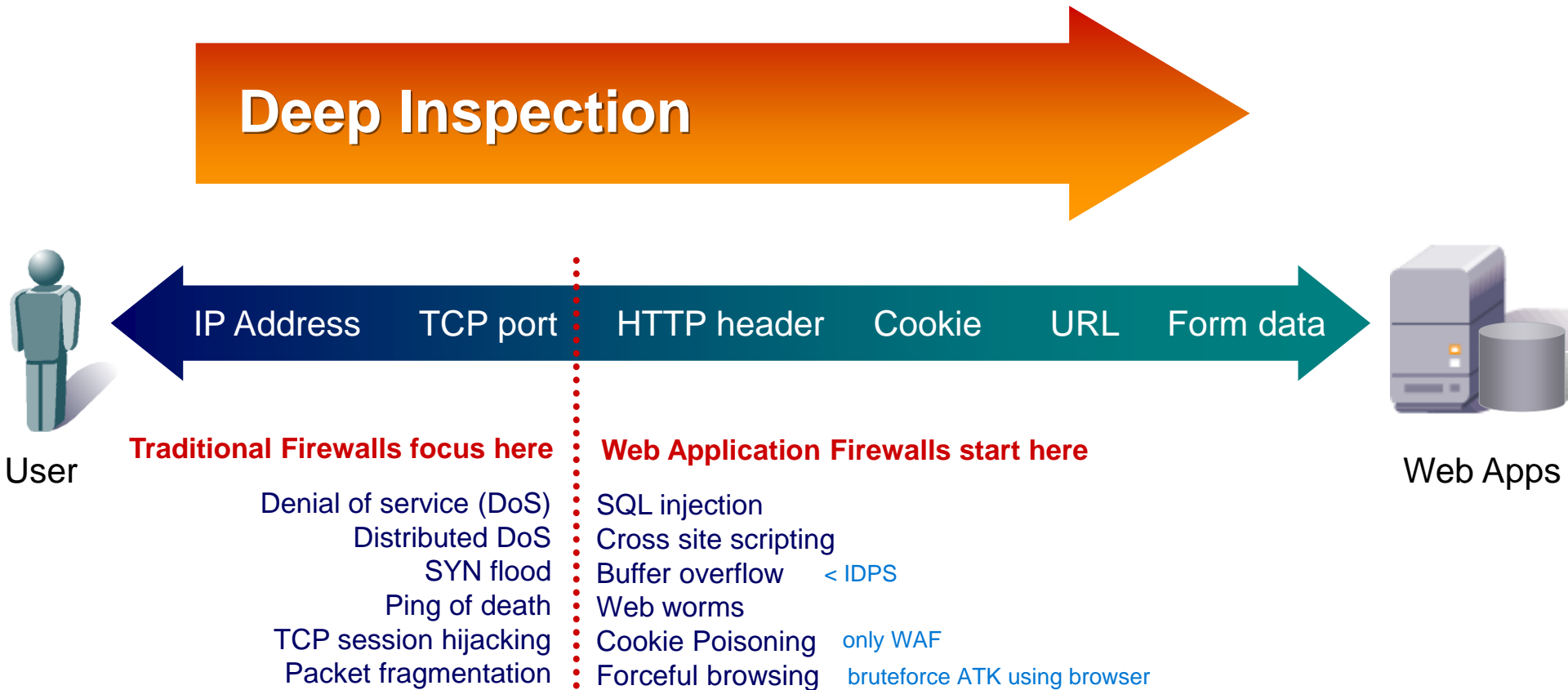


WAFs Inspect Application Data

14

9/21/2021

Deep Inspection



Why Network Firewall/IDS not enough?

15

9/21/2021

Network firewalls and IPS solutions are packet based, not session based - No session state is maintained

Full context of user sessions must be understood to effectively inspect for attacks

IDS monitors network traffic looking for the characteristics of known attacks.

| Application Threat | IPS / Network Firewalls | Barracuda Web App Firewall |
|--|----------------------------|----------------------------|
| Cookie poisoning | Well known signatures only | ✓ |
| Hidden field manipulation | Well known signatures only | ✓ |
| Cross Site scripting | Well known signatures only | ✓ |
| SQL and Command Injection | None | ✓ |
| Stealth Commanding <small>cmd creating stateful connections</small> | None | ✓ |
| Parameter Tampering | None | ✓ |
| Buffer overflow | None | ✓ |
| Forceful Browsing | None | ✓ |
| Identity Theft | None | ✓ |
| Application DoS | None | ✓ |
| Data Theft | None | ✓ |

Content

16

duyn@uit.edu.vn

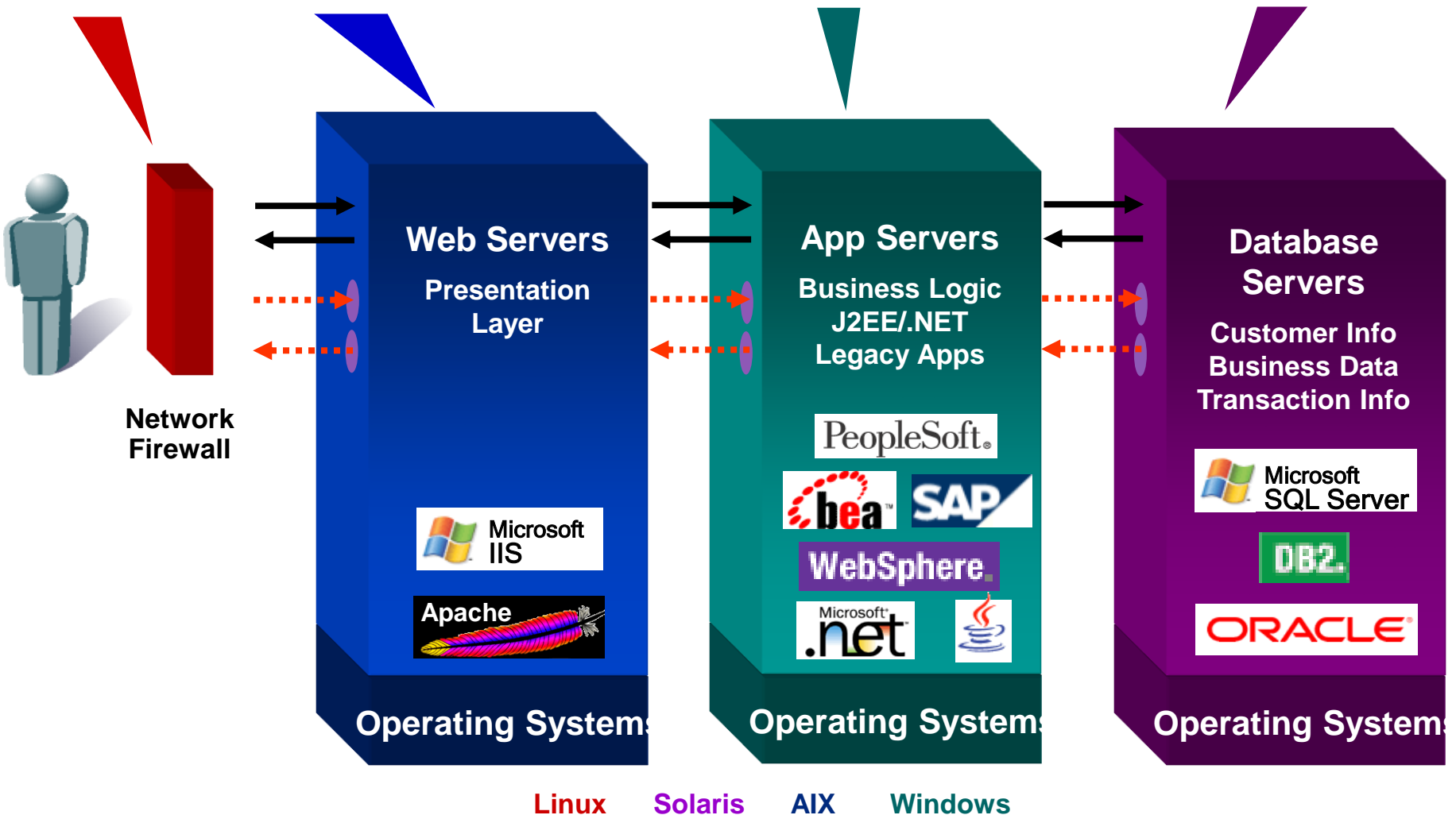
- What is WAF?
- Why we need to use WAF?
- **Web Application architecture**
- How does WAF prevent attacks?
- How to deploy WAF?

Web Application architecture

17

9/21/2021

<http://www.none.to/script?submenu=update&uid=1'+or+like'%25admin%25';--%00>



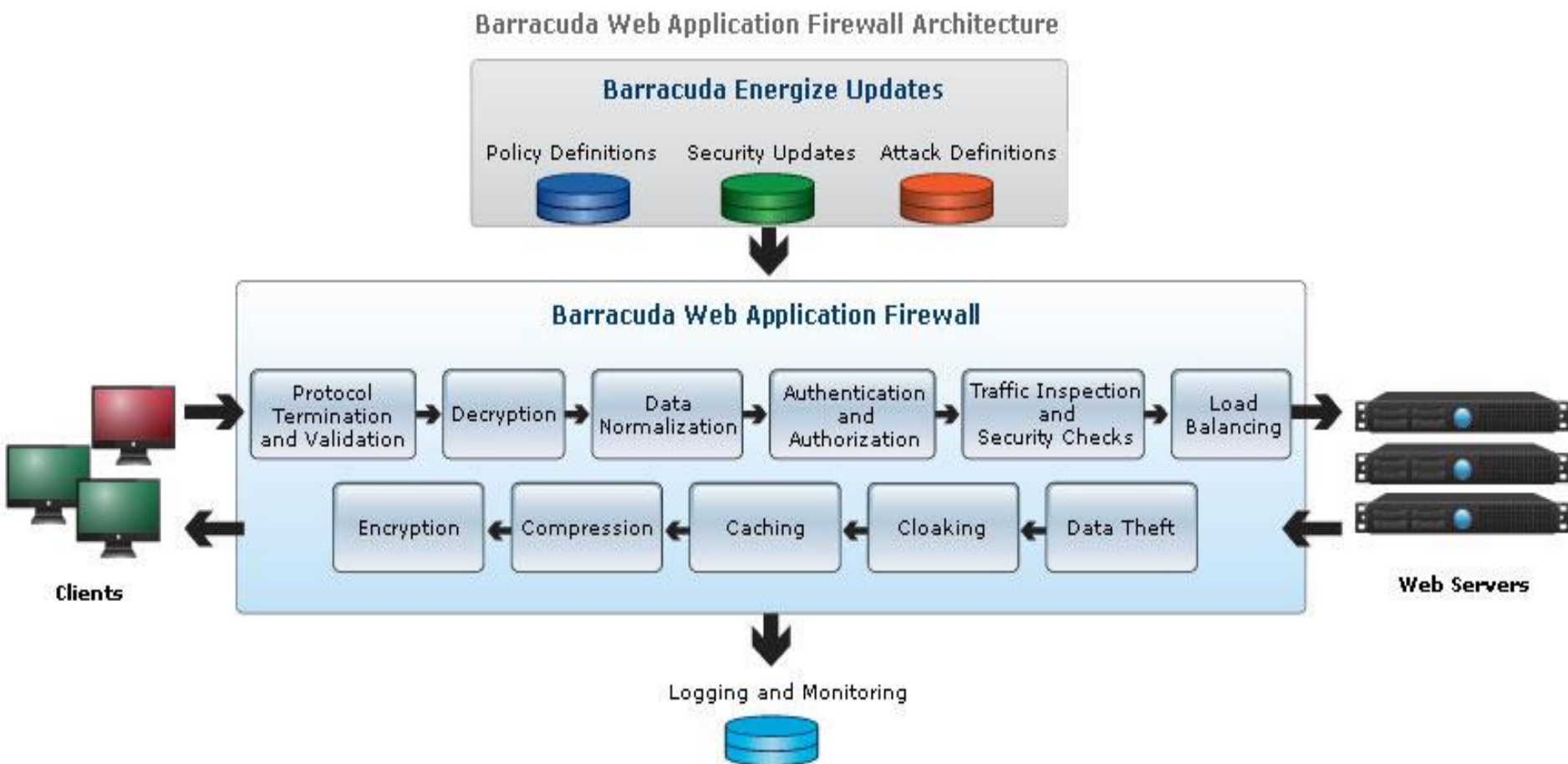
Content

- What is WAF?
- Why we need to use WAF?
- Web Application architecture
- **How does WAF prevent attacks?**
- How to deploy WAF?

How does WAF prevent attacks?

19

9/21/2021





Security

Application
Delivery

Manageability

+ LB

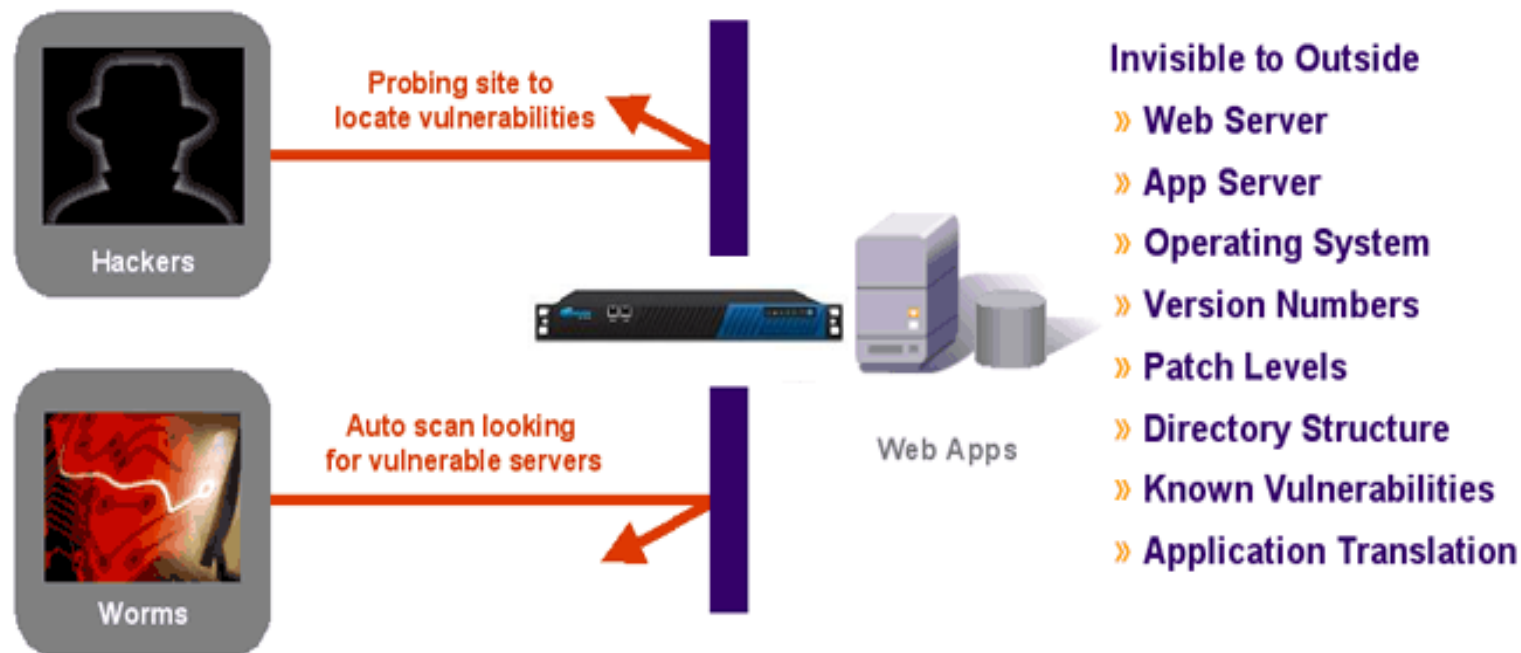
-> HA for application



Cloaking

22

9/21/2021



Attackers first task – Reconnaissance of network for weakness

- What Web, Database, App server etc?
- What versions, patches, known vulnerabilities etc?

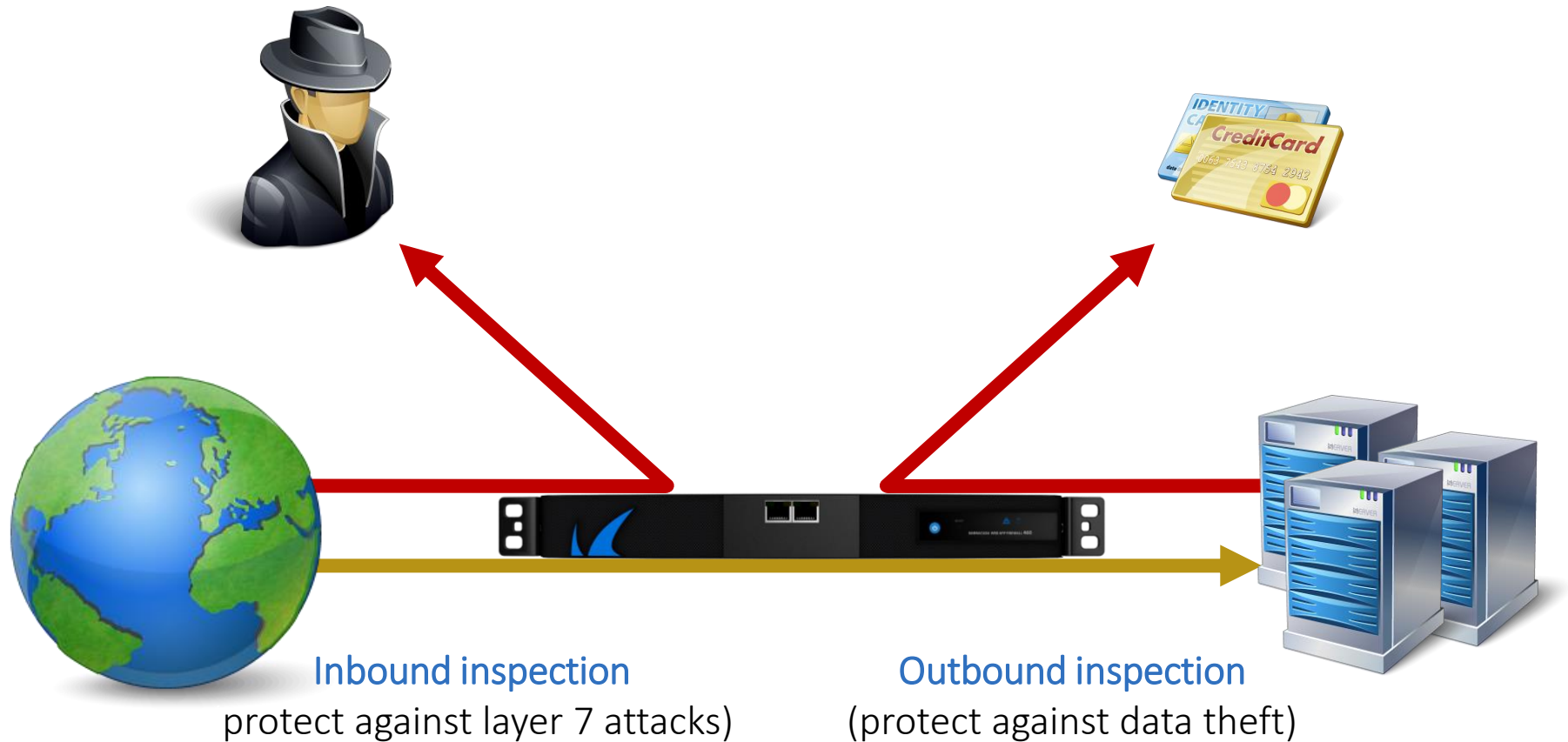
Cloaking makes enterprise Web resources invisible to hackers and worms

- Hides all error codes, HTTP headers, IP addresses etc

Layer 7 Web Application Firewall

23

9/21/2021

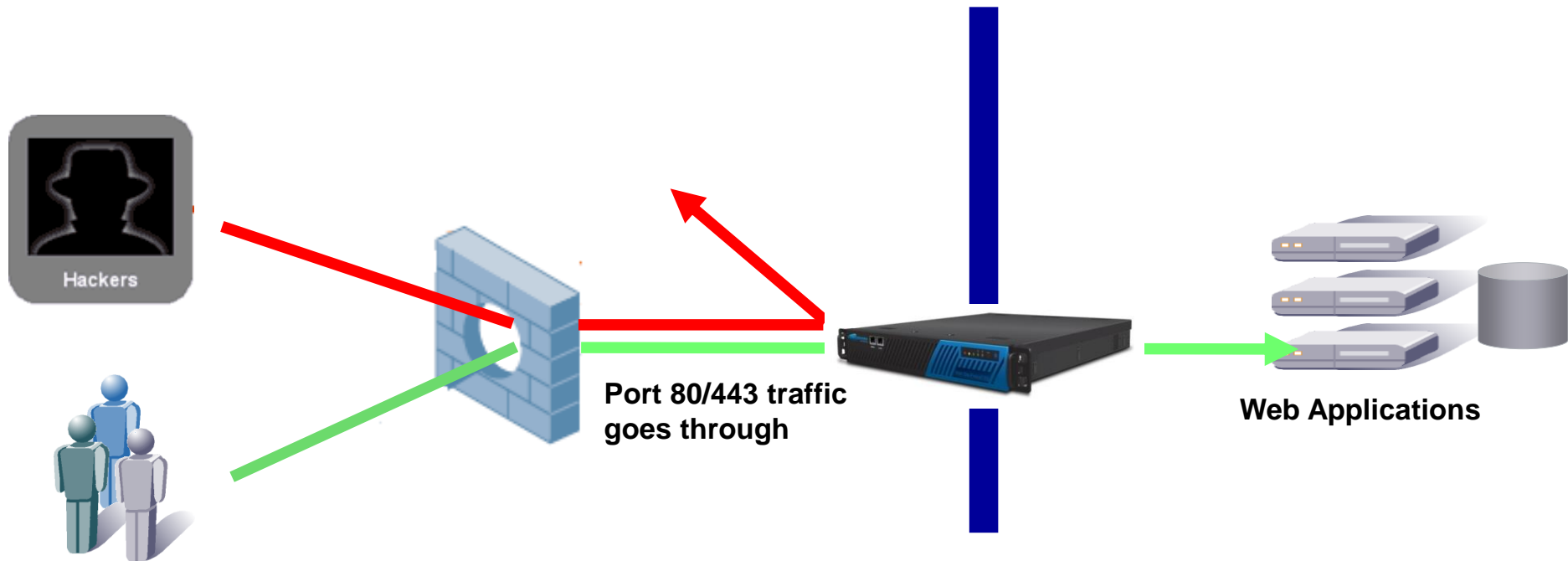


Inbound Protection

24

9/21/2021

- Injection – SQL, OS commands etc
- Scripting – XSS, CSRF
- Cookie/Session Poisoning
- Parameter/Form Tampering
- Protocol Sanitization
- Zero day attacks protection
- Anti Virus Attacks prevention
- XML Attacks



Prevention in TOP 10 OWASP

25

9/21/2021

OWASP Top 10

Prevention

| | |
|---|--|
| 1. Cross Site Scripting (XSS) | Validate inputs for Script injections |
| 2. Injection Flaws | Validate inputs for interpreter injection attacks, particularly SQL injection |
| 3. Malicious File Execution | Prevent remote code execution, root kit installs, and use of file system resources |
| 4. Insecure Direct Object Reference | Learn and enforce only valid direct access to objects, files, directories, database records, URLs and form parameters |
| 5. Cross Site Request Forgery (CSRF) | Insert random character sequence in URLs to prevent against CSRF attacks |
| 6. Info Leakage / Improper Error Handling | Prevents sensitive data from being exposed |
| 7. Broken Authentication and Session Management | Enforce proper authentication, protection of session tokens. |
| 8. Insecure Cryptographic Storage | Securely store the private /confidential data |
| 9. Insecure Communications | Enable encryption for the communication channels |
| 10. Failure to restrict URL Access | Enforce URL access by Learning and allowing access to valid URLs. This can be further tuned by configuring authorization rules via the AAA functionality |

Outbound Protection

26

9/21/2021

Deep Inspection of outgoing content blocks:

- Credit Cards
- Social Security Numbers
- Custom Patterns
- Error details in 200 OK responses



Advanced Application Security

27

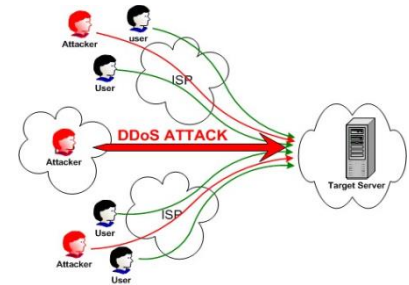
9/21/2021



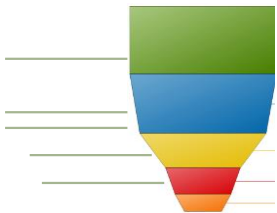
Anti Virus Protection



XML Firewall



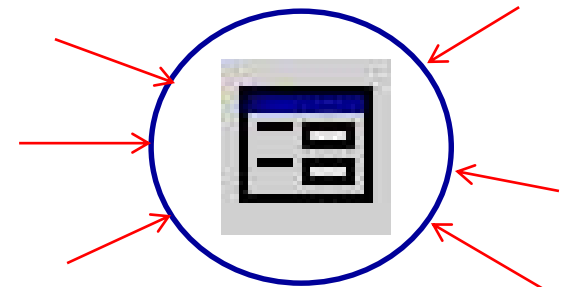
Session Tracking



Rate Control



Adaptive Profiling



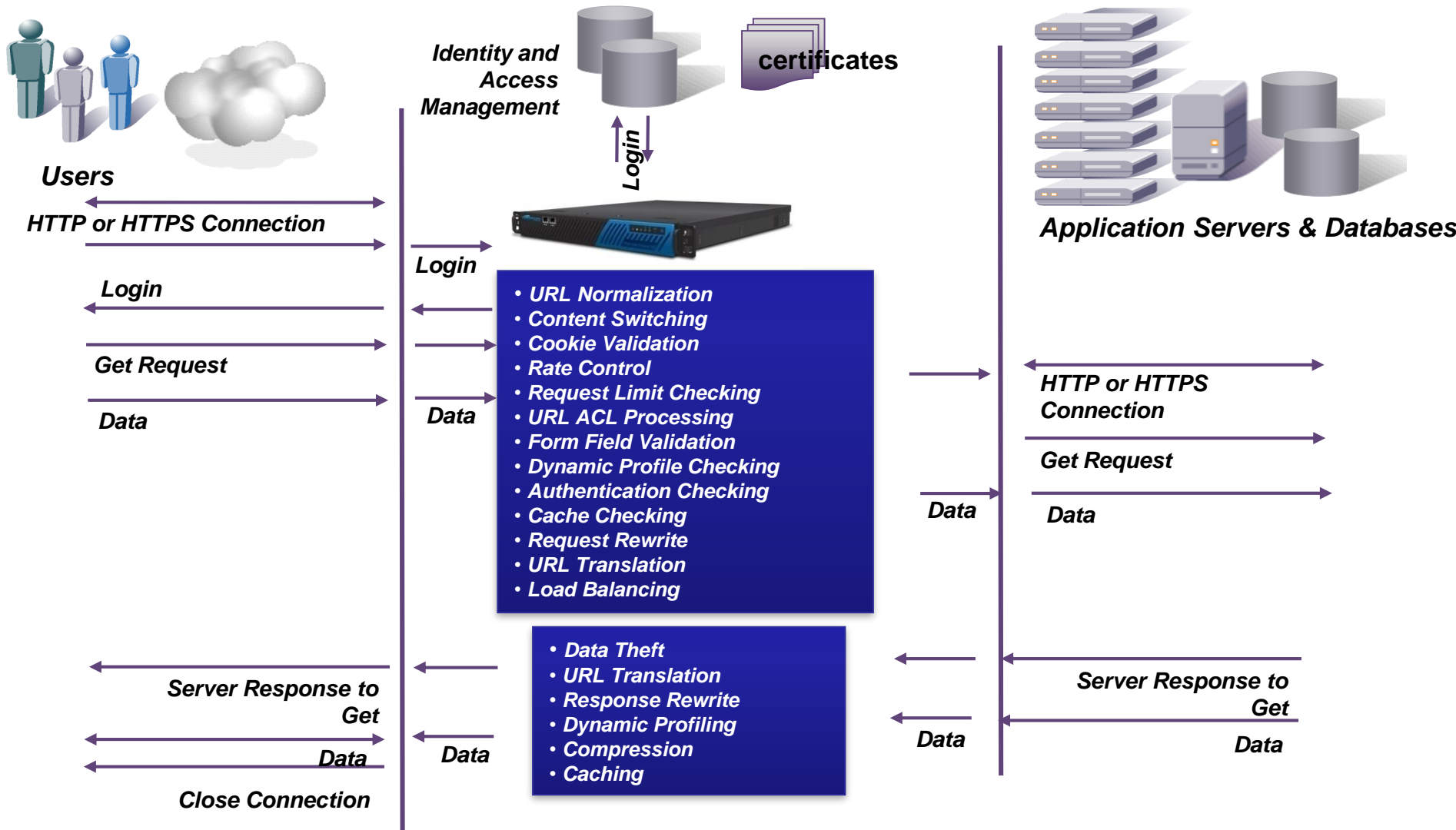
Bruteforce prevention

Profile A, B, C suitable for each case

Bi-Directional Detection and Mitigation

28

9/21/2021



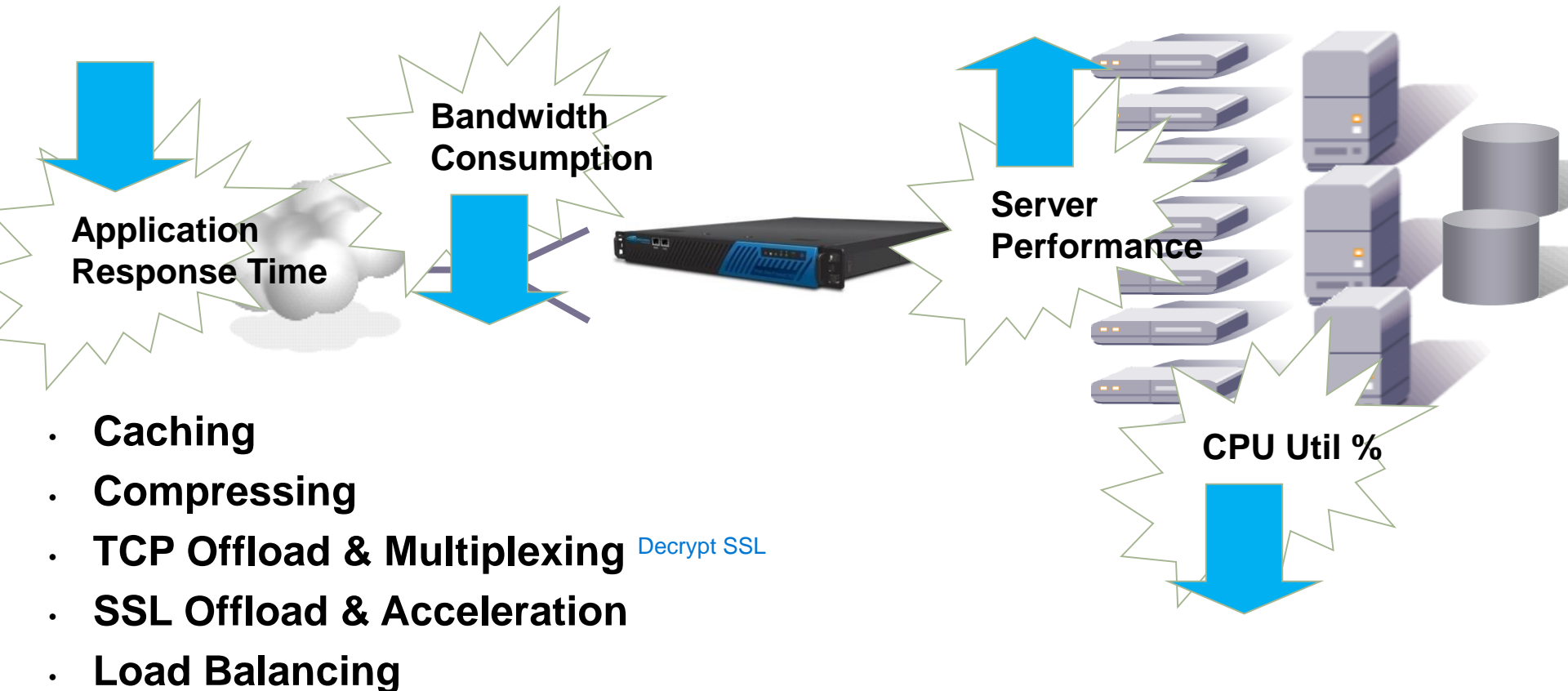


Application Delivery

Also Improves Operational Efficiency

30

9/21/2021



30 – 400% Response Time Improvement Plus Complete Application Security

Plug & Play Deployment & Management

31

9/21/2021



Level of Customization

High

Custom & Positive Security

Medium

Template-Based Security

Low

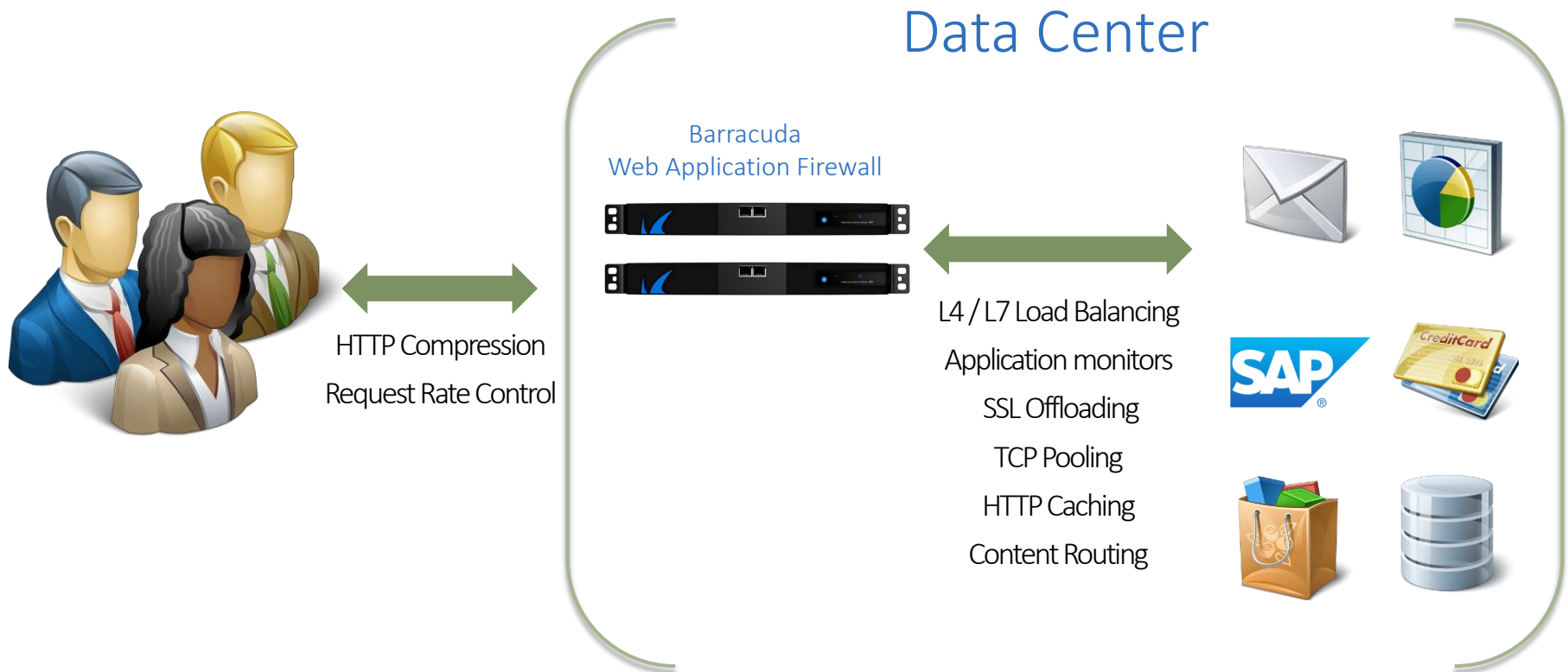
Default Security



Acceleration & Load Balancing

32

9/21/2021

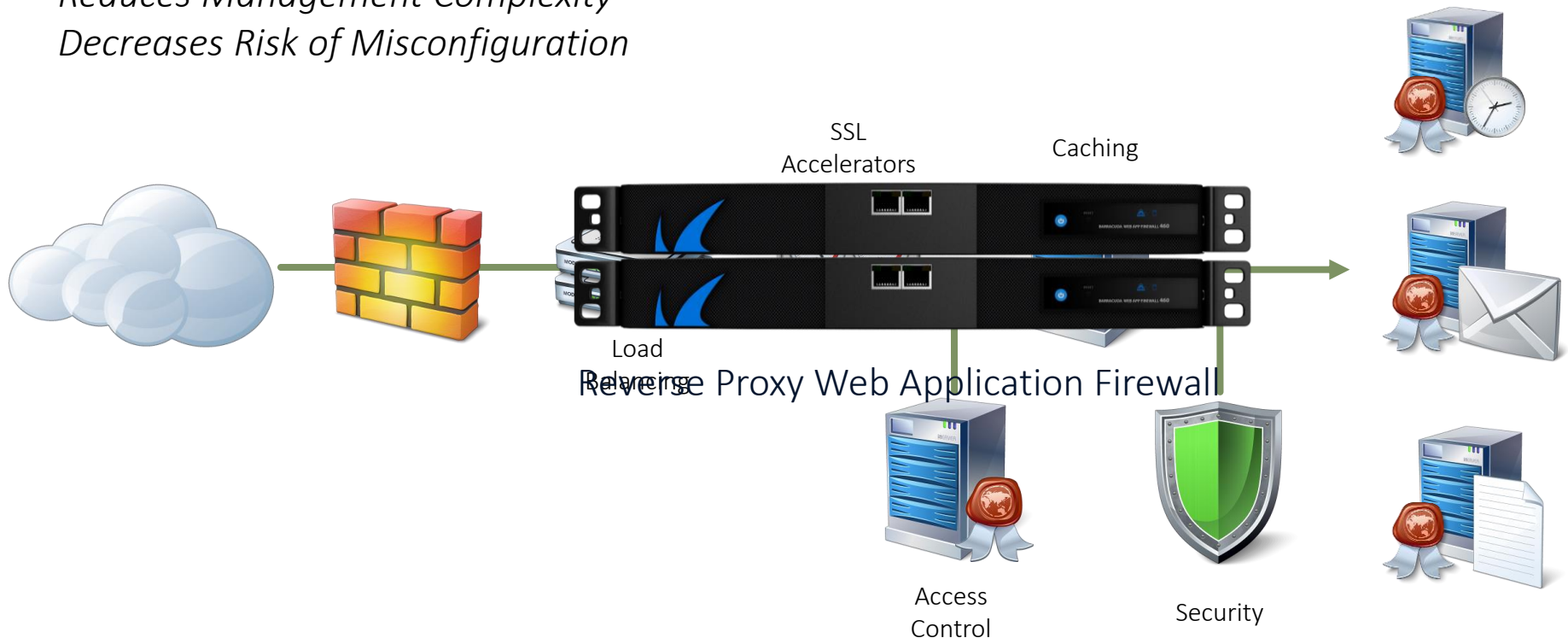


Consolidate Disparate Appliances in DMZ

33

9/21/2021

Reduces Management Complexity
Decreases Risk of Misconfiguration



Content

34

duyn@uit.edu.vn

- What is WAF?
- Why we need to use WAF?
- Web Application architecture
- How does WAF prevent attacks?
- **How to deploy WAF?**

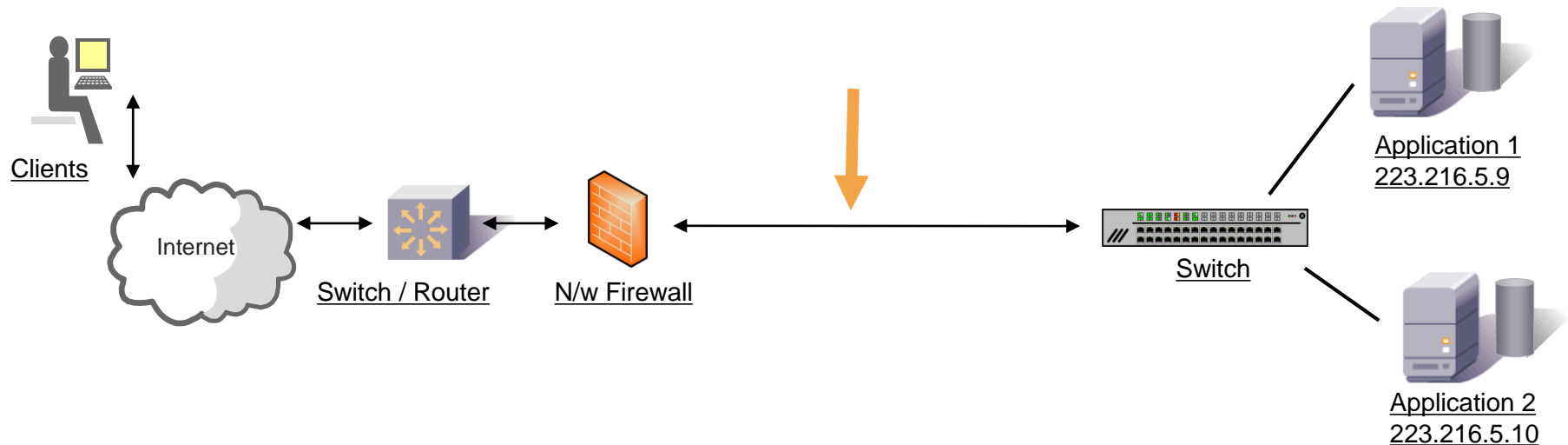
Bridge Mode

35

9/21/2021

Existing Network/Application Data Flow

The Barracuda Web Application Firewall is inserted between the Network firewall and the switch to the backend.

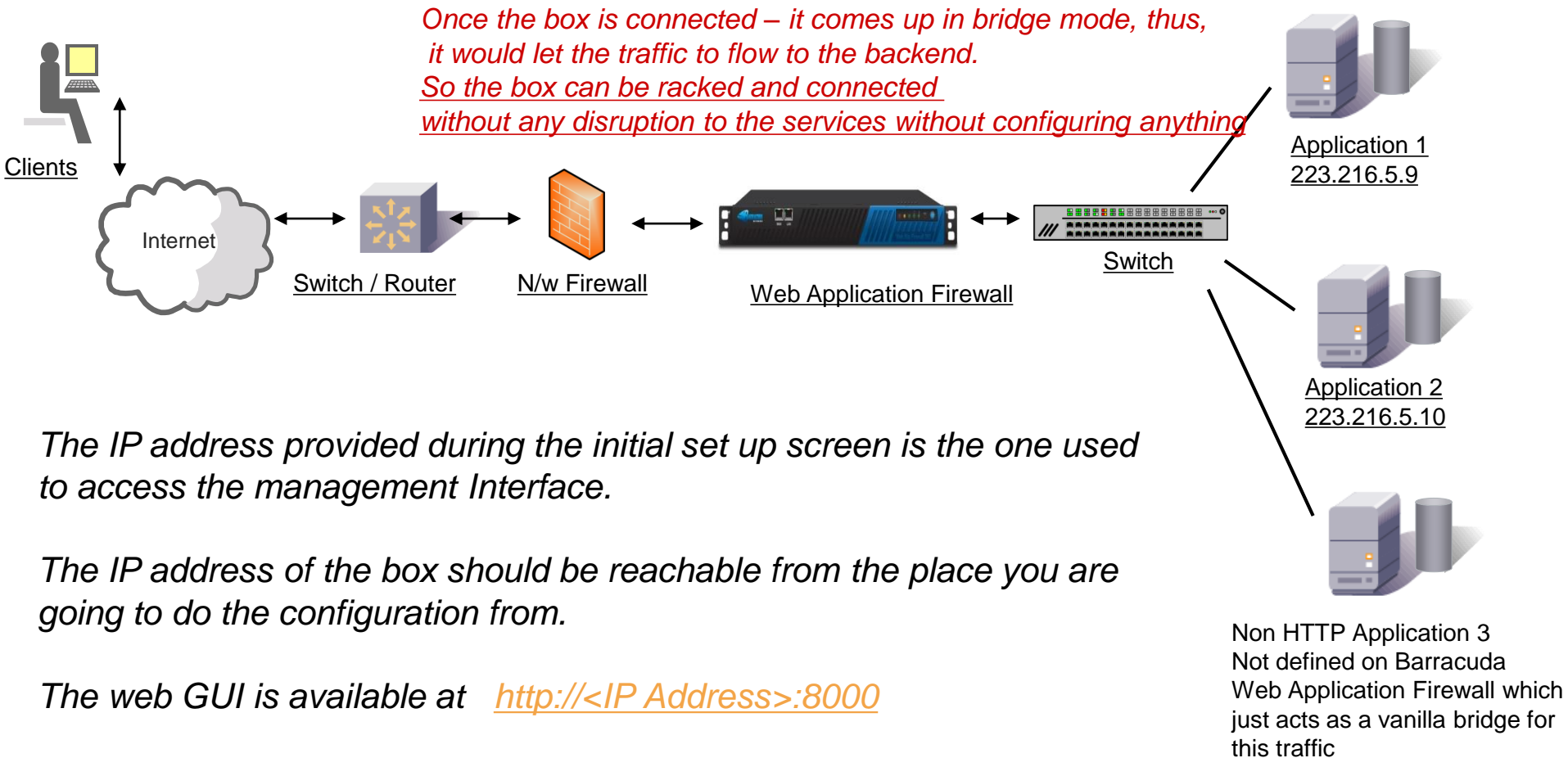


Connecting in Bridge Mode HTTP

36

9/21/2021

The Barracuda Web Application Firewall is inserted between the Network firewall and the switch to the backend.



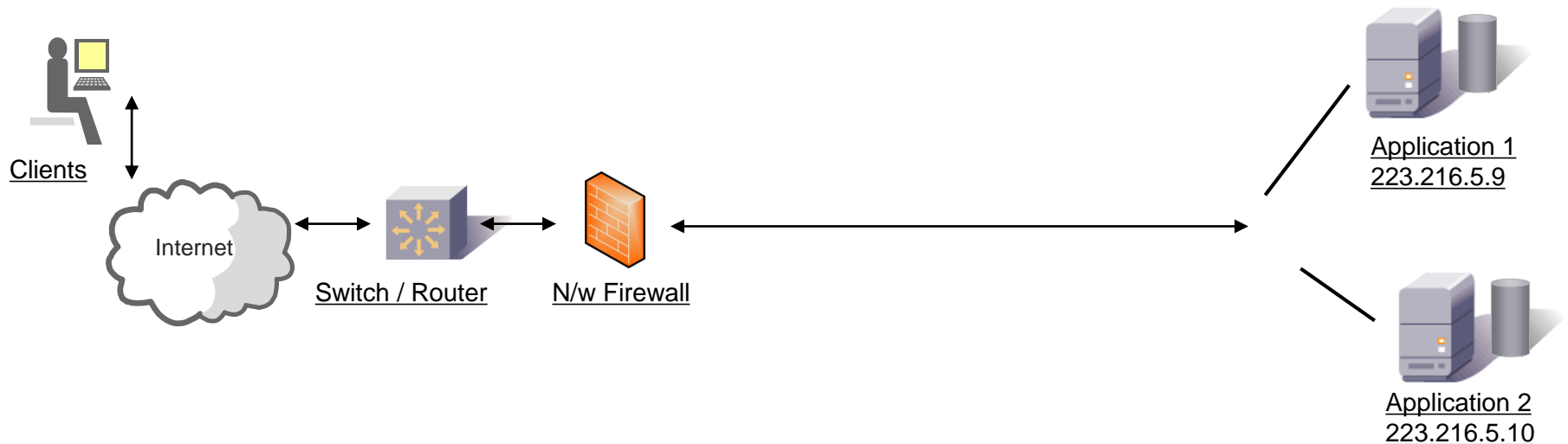
Proxy mode

37

9/21/2021

Existing Network/Application Data Flow

The Barracuda Web Application Firewall is inserted between the Network firewall and the switch to the backend.



Connecting in Proxy Mode

In - line

38

9/21/2021

The Barracuda Web Application Firewall is inserted between the Network firewall and the switch to the backend.

before and after WAF: not same subnet

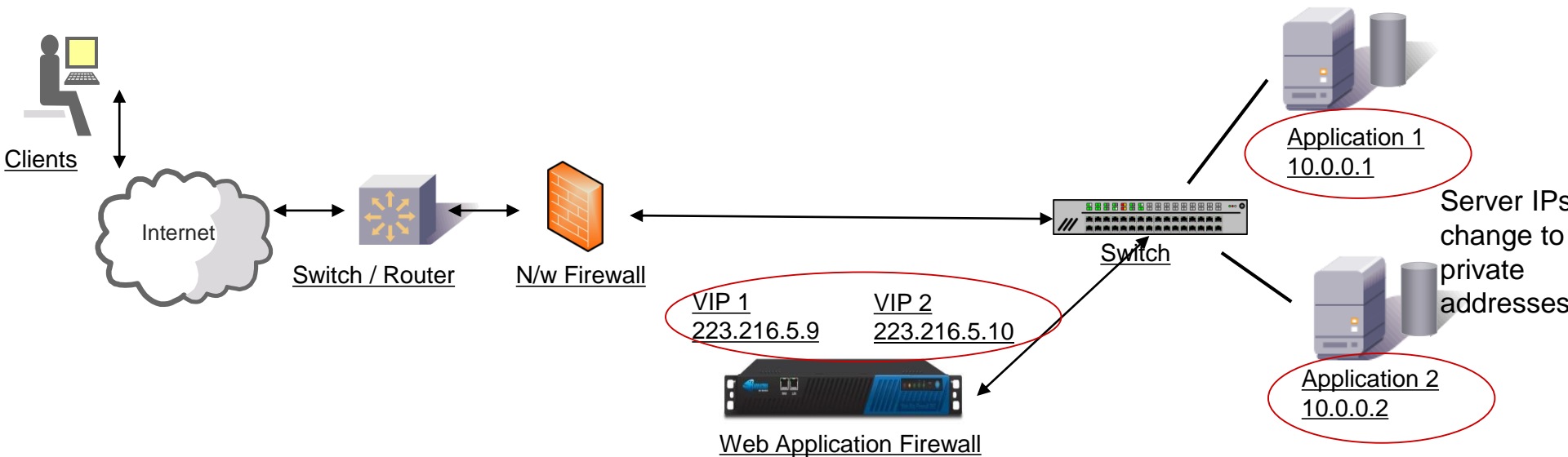


One-Arm Proxy mode

39

9/21/2021

The Barracuda Web Application Firewall is inserted between the Network firewall and the switch to the backend.



bypass hardware FW to reduce failover

Question ???