

# CHƯƠNG 2

## NEXT GENERATION FIREWALL

3/25/23

ThS. Nguyễn Duy  
duyn@uit.edu.vn

# Nội dung

2

duyn@uit.edu.vn

- Tường lửa là gì?
- Phân loại tường lửa?
- Tính năng của tường lửa thế hệ mới?
- Mô hình triển khai tường lửa

# Nội dung

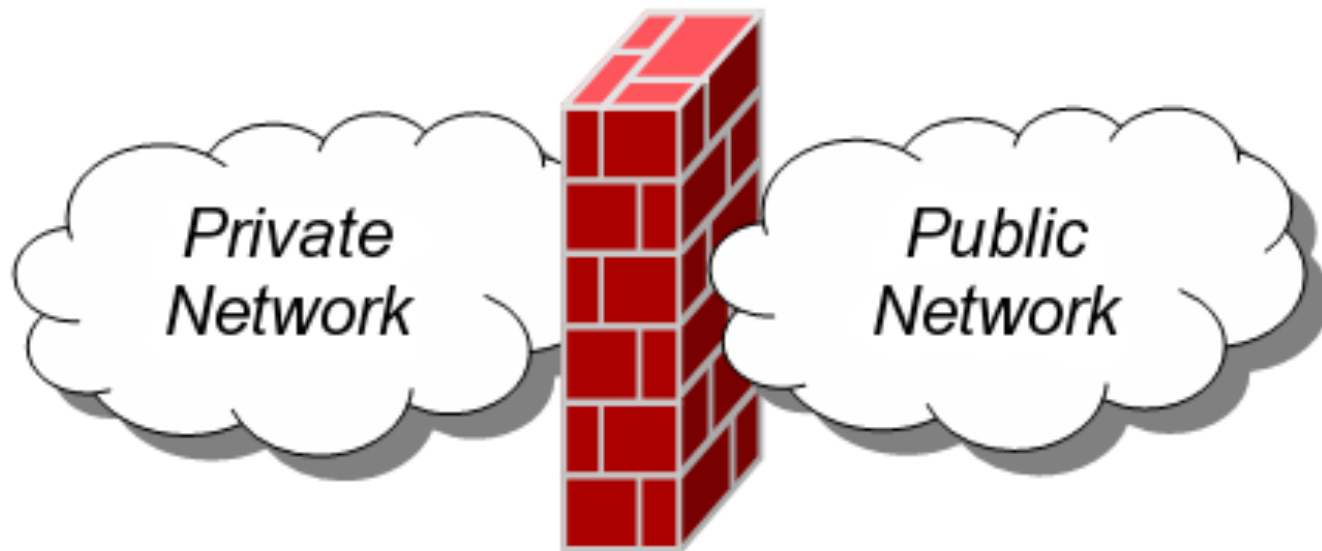
3

duyn@uit.edu.vn

- **Tường lửa là gì?**
- Phân loại tường lửa?
- Tính năng của tường lửa thế hệ mới?
- Mô hình triển khai tường lửa

# Tường lửa là gì

- Firewall hay còn được gọi là Tường Lửa. Là thiết bị, phần cứng hay phần mềm bảo mật được sử dụng để quản lý luồng gói tin qua nó : cho phép (permit) hay cấm (deny).



# Nội dung

5

duyn@uit.edu.vn

- Tường lửa là gì?
- **Phân loại tường lửa?**
- Tính năng của tường lửa thế hệ mới?
- Mô hình triển khai tường lửa

# Phân loại tường lửa

6

duyn@uit.edu.vn

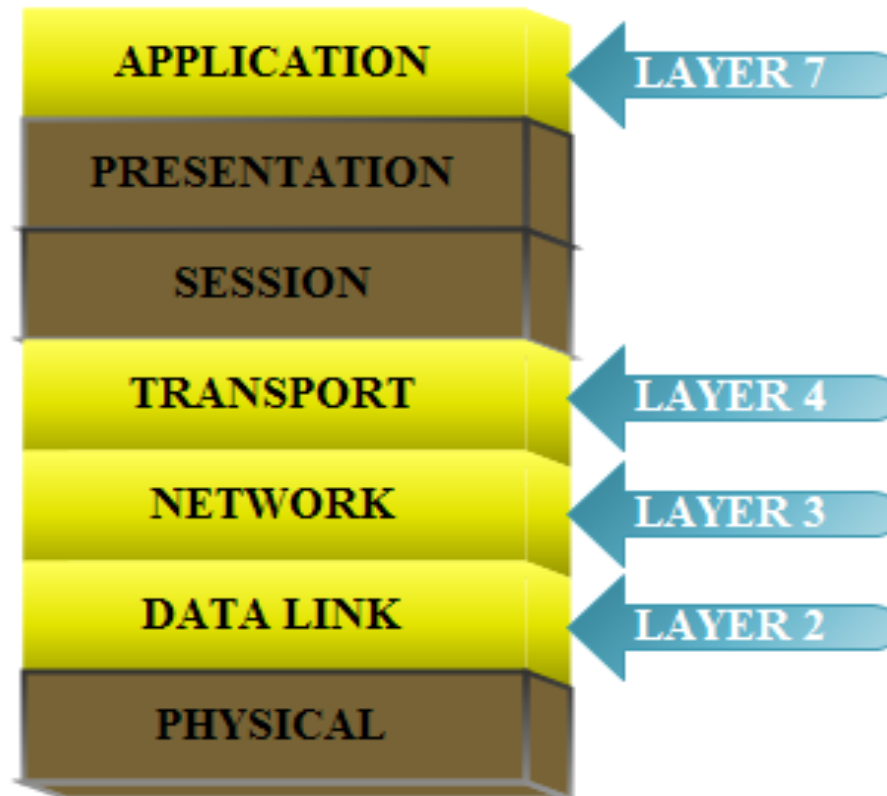
- Appliances: Thiết bị mạng
  - Checkpoint, Cisco ASA, Astaro, Cyberoam,...
- Software: Ứng dụng bảo mật được cài trên máy tính
  - ISA Server, IPCop, Smoothwall, Pfsense,...
- Virtual Appliances
  - SOPHOS, Palo Alto,.....

# Phân loại tường lửa

7

duyn@uit.edu.vn

- Firewall hoạt động ở những lớp nào trong mô hình OSI ???



# Phân loại tường lửa

- **Cả Personal Firewall và Network Firewall được chia làm 3 loại chính :**
  - **Simple Packet Filter Firewalls**
  - **Stateful Packet Filter Firewalls**
  - **Application Level Firewalls**



# Phân loại tường lửa

## ➤ Simple Packet Filter Firewalls

- Kiểm tra gói tin qua firewall bằng cách so sánh nó với những nguyên tắc (Rule) đã được đặt ra, để quyết định gói tin đó được cho phép hay bị từ chối.
- Những thông tin sẽ được kiểm tra :
  - IP Nguồn
  - IP Đích
  - Giao thức
  - Port Nguồn
  - Port Đích
- Hoạt động ở Layer 2 và Layer 3

# Phân loại tường lửa

10

duyn@uit.edu.vn

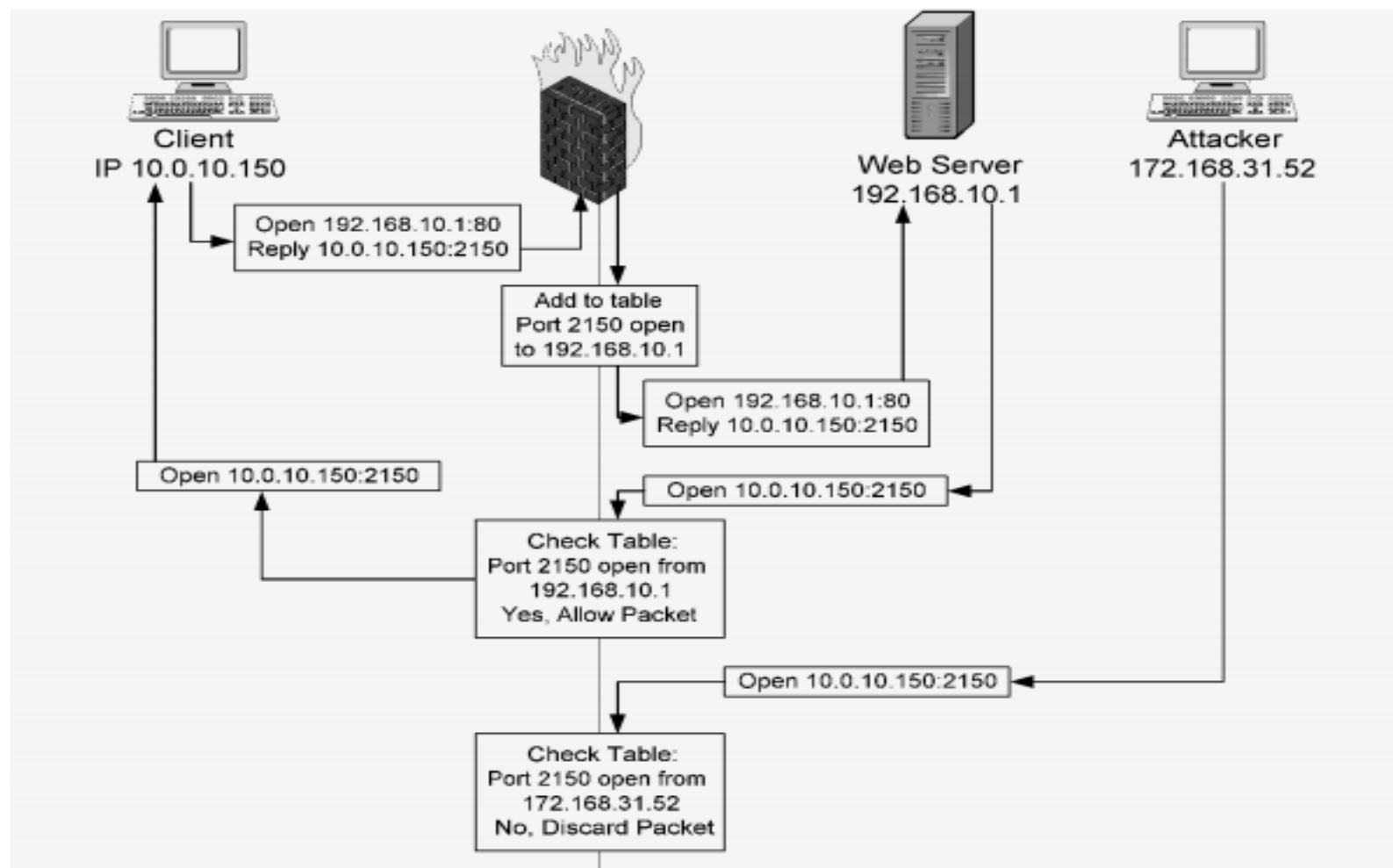
- Điểm yếu
  - Application Specific Vulnerabilities
  - Limited Logging
  - No Authentication
  - Vulnerable to Spoofing
  - Large Attack Surface
  - Easy to Misconfigure

# Phân loại tường lửa

11

duyn@uit.edu.vn

## ➤ Stateful Packet Filter Firewalls



# Phân loại tường lửa

12

duyn@uit.edu.vn

## ➤ **Stateful Packet Filter Firewalls**

- Hoạt động ở Layer 2, Layer 3 và Layer 4
- Những khắc phục so với Simple Packet Filter Firewalls :
  - Lower Attack Footprint
  - Less Susceptible to Spoofing
  - Easy Black hole configuration
  - Less Resource Intensive

# Phân loại tường lửa

## ➤ **Application Level Firewalls**

- Còn được gọi Application-Proxy Gateways.
- Là loại Firewall có độ phức tạp cao nhất do có khả năng điều khiển truy cập từ Layer 2 đến Layer 7
- Deep Packet Inspection : kiểm tra chi tiết gói tin nên có khả năng ngăn chặn các ứng dụng Instant Message, Peer to Peer,...
- Hoạt động ở Layer 7

# Phân loại tường lửa

## ➤ **Application Level Firewalls**

### ➤ Có khả năng xác thực :

- UserID và Password
- Hardware hoặc Software Token
- Source Address
- Biometric

### ➤ Những ưu điểm :

- Extensive Logging Capabilities
- Enforcement of Authentication
- Less Susceptible to TCP/IP Vulnerabilities
- Có khả năng tạo rule ngăn cản gói tin đã mã hóa

# Nội dung

15

duyn@uit.edu.vn

- Tường lửa là gì?
- Phân loại tường lửa?
- **Tính năng của tường lửa thế hệ mới?**
- Mô hình triển khai tường lửa

# Next-Generation Firewall

16

duyn@uit.edu.vn

## New Requirements for the Firewall

1. Identify applications regardless of port, protocol, evasive tactic or SSL
2. Identify users regardless of IP address
3. Granular visibility and policy control over application access / functionality
4. Protect in real-time against threats embedded across applications
5. Multi-gigabit, in-line deployment with no performance degradation



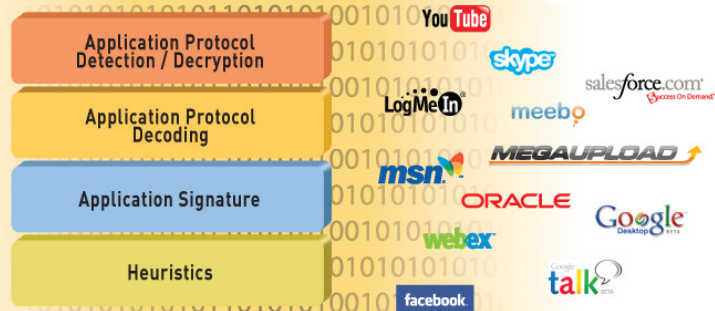


# NG Firewall' Technology

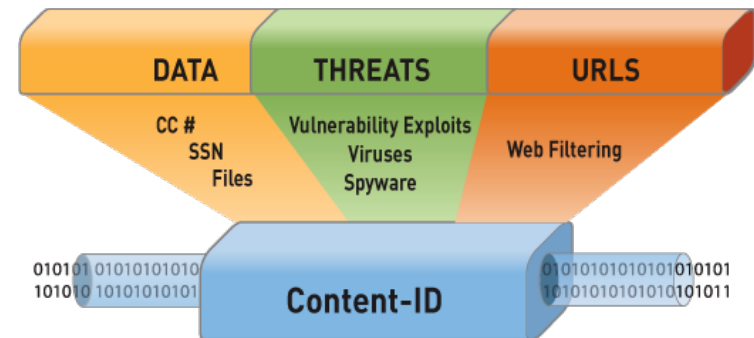
17

3/25/23

#1

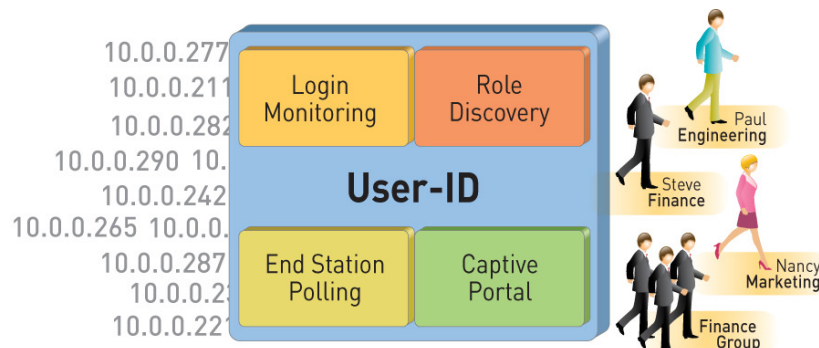


#3



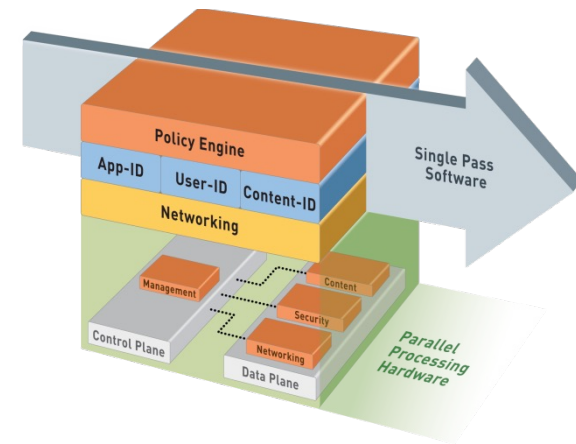
#2

## User-ID



#4

## SP3 Architecture



# Next Generation Firewall

18

duyn@uit.edu.vn

**SECURITY**

**APPLICATION AWARENESS**

**PERFORMANCE**

# Next Generation Firewall

19

duyn@uit.edu.vn

## **SECURITY**

- **DEEP PACKET INSPECTION**
- **INTRUSION PREVENTION**
- **SSL DECRYPTION**

# Stateful Packet Inspection

Stateful is limited  
inspection that can  
only block on ports

No Data Inspection!

INSPECT

Source 212.56.32.49	Destination 65.26.42.17
Source Port 823747	Dest Port 80
Sequence 28474	Sequence 2821
Syn state SYN	IP Option none

Stateful  
Packet  
Inspection

Firewall Traffic Path

# Deep Packet Inspection

## Signature Database

ATTACK-RESPONSES 14BACKDOOR  
58BAD-TRAFFIC 15DDOS 33DNS  
19DOS 18EXPLOIT >35FINGER  
13FTP 50ICMP 115Instant  
Messenger 25IMAP 16INFO  
7Miscellaneous44MS-SQL 24MS-  
SQL/SMB 19MULTIMEDIA 6MYSQL  
2NETBIOS 25NNTP 2ORACLE  
25P2P 51POLICY 21POP2 4POP3  
18RPC 124RSERVICES 13SCAN  
25SMTP 23SNMP 17TELNET  
14TFTP 9VIRUS 3WEB-ATTACKS  
47WEB-CGI 312WEB-CLIENT

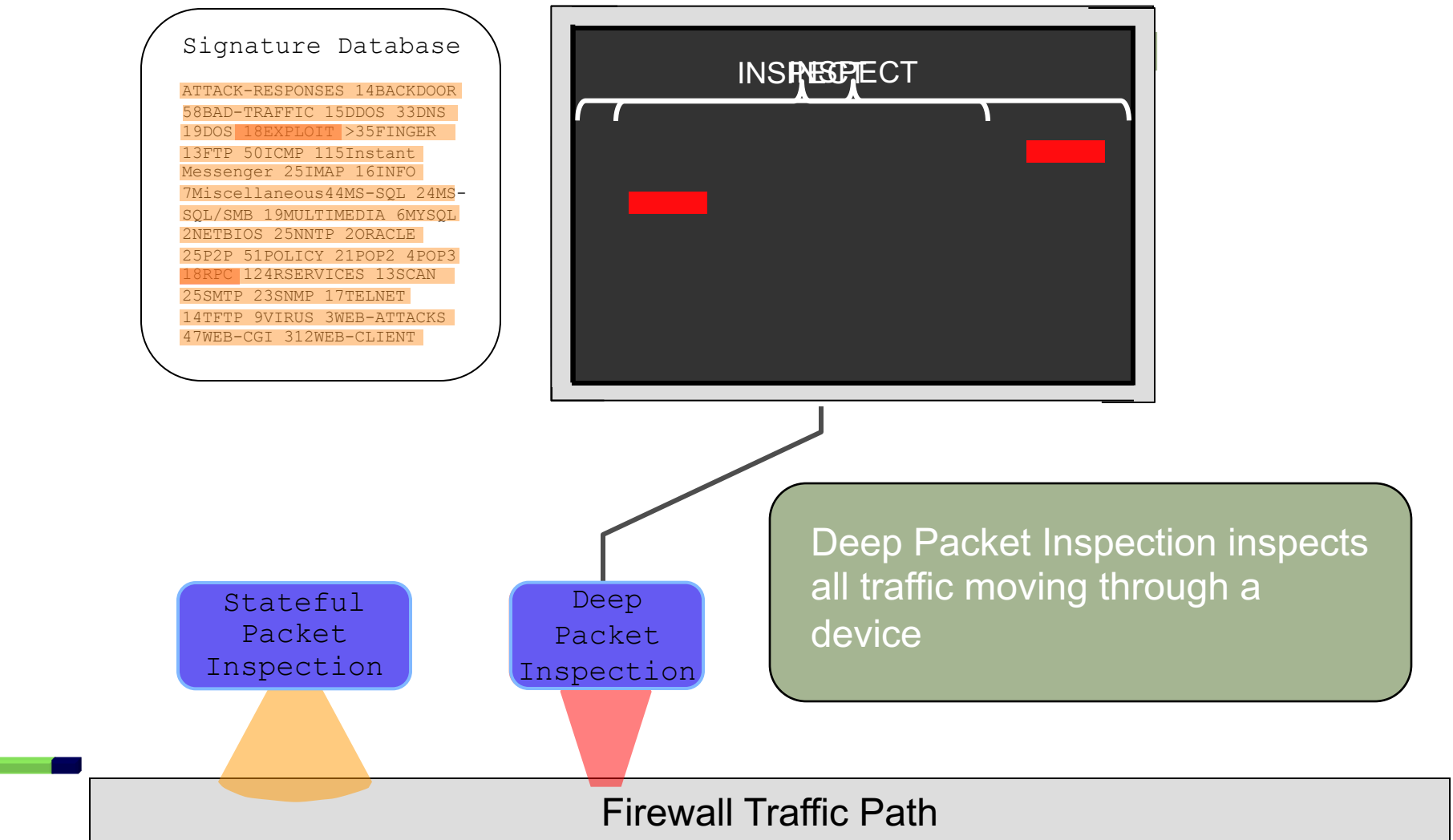
INSPECT

Stateful  
Packet  
Inspection

Deep  
Packet  
Inspection

Deep Packet Inspection inspects  
all traffic moving through a  
device

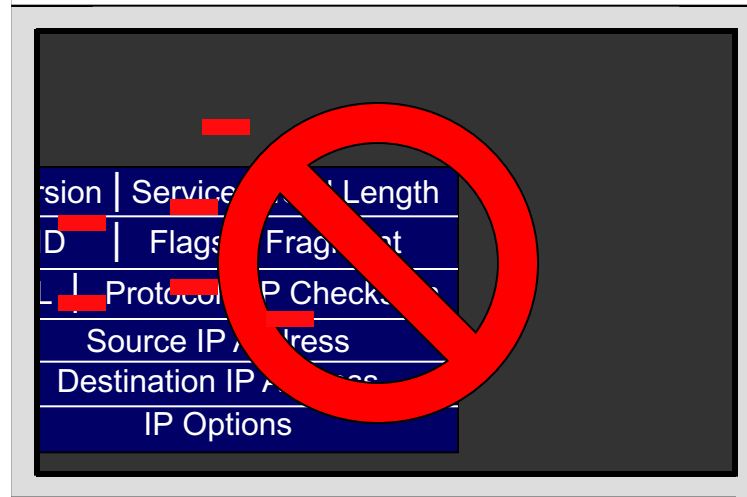
Firewall Traffic Path



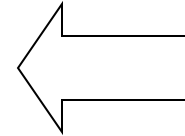
# Deep Packet Inspection / Prevention

## Signature Database

```
ATTACK-RESPONSES 14BACKDOOR
58BAD-TRAFFIC 15DDOS 33DNS
19DOS 18EXPLOIT >35FINGER
13FTP 50ICMP 115Instant
Messenger 25IMAP 16INFO
7Miscellaneous44MS-SQL 24MS-
SQL/SMB 19MULTIMEDIA 6MYSQL
2NETBIOS 25NNTP 2ORACLE
25P2P 51POLICY 21POP2 4POP3
18RPC 124RSERVICES 13SCAN
25SMTP 23SNMP 17TELNET
14TFTP 9VIRUS 3WEB-ATTACKS
47WEB-CGI 312WEB-CLIENT
```



Comparing...



Application Attack,  
Worm or Trojan  
Found !

Stateful  
Packet  
Inspection

Deep  
Packet  
Inspection

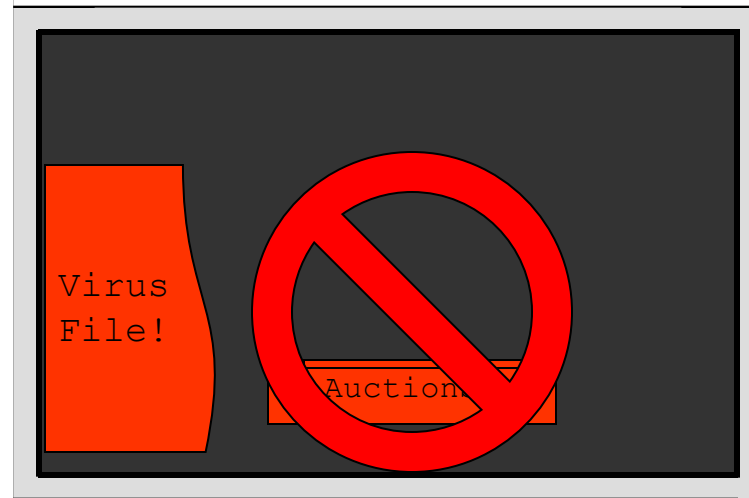
Deep Packet Inspection with  
Intrusion Prevention can find and  
block, application vulnerabilities,  
worms or Trojans.

Firewall Traffic Path

# Gateway Anti-Virus and Content Control

## Signature Database

```
ATTACK-RESPONSES 14BACKDOOR
58BAD-TRAFFIC 15DDOS 33DNS
19DOS 18EXPLOIT >35FINGER
13FTP 50ICMP 115Instant
Messenger 25IMAP 16INFO
7Miscellaneous44MS-SQL 24MS-
SQL/SMB 19MULTIMEDIA 6MYSQL
2NETBIOS 25NNTP 2ORACLE
25P2P 51POLICY 21POP2 4POP3
18RPC 124RSERVICES 13SCAN
25SMTP 23SNMP 17TELNET
14TFTP 9VIRUS 3WEB-ATTACKS
47WEB-CGI 312WEB-CLIENT
```



Stateful  
Packet  
Inspection

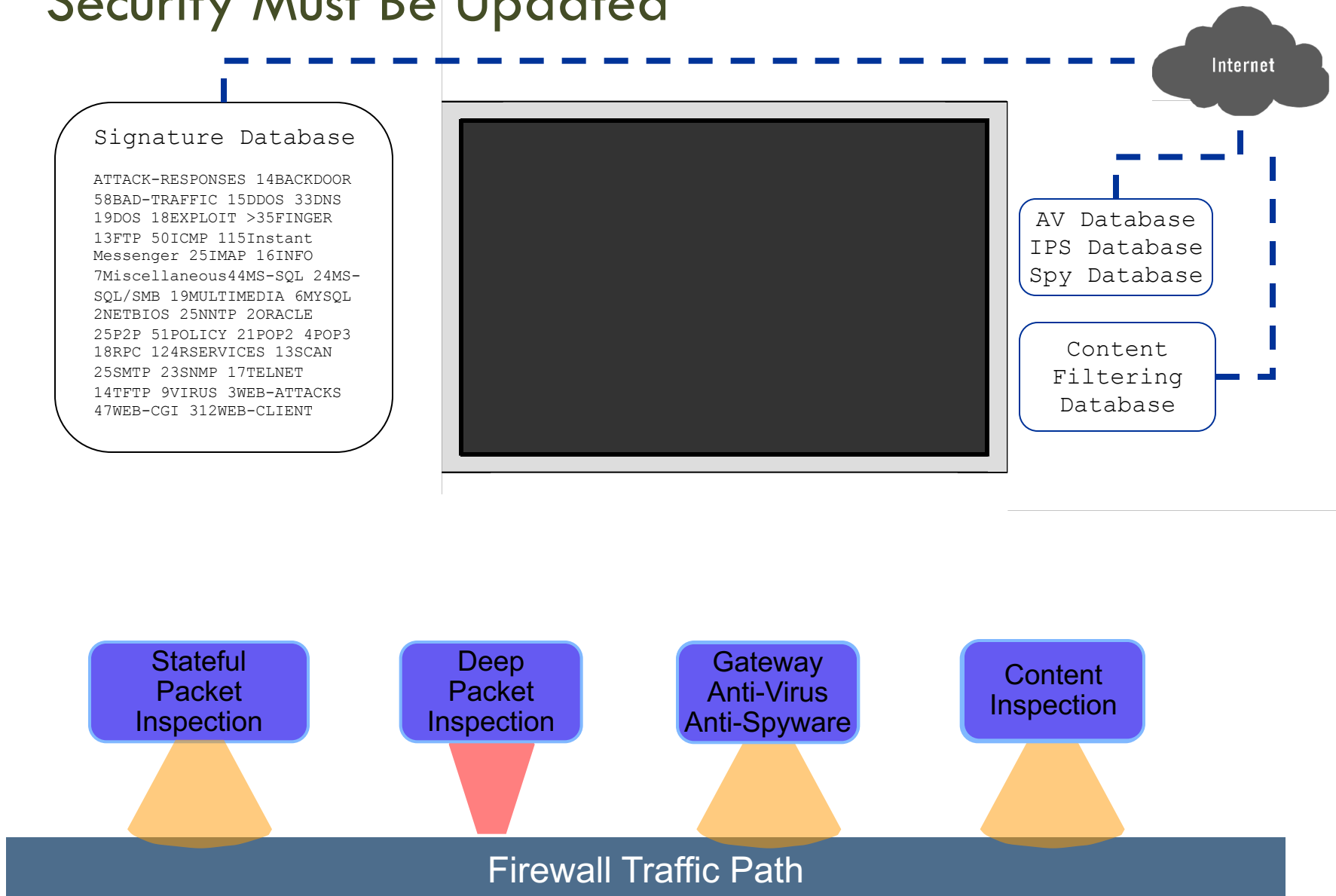
Deep  
Packet  
Inspection

Gateway  
Anti-Virus  
Anti-Spyware

Content  
Inspection

Firewall Traffic Path

# Security Must Be Updated





# Next Generation Firewall

25

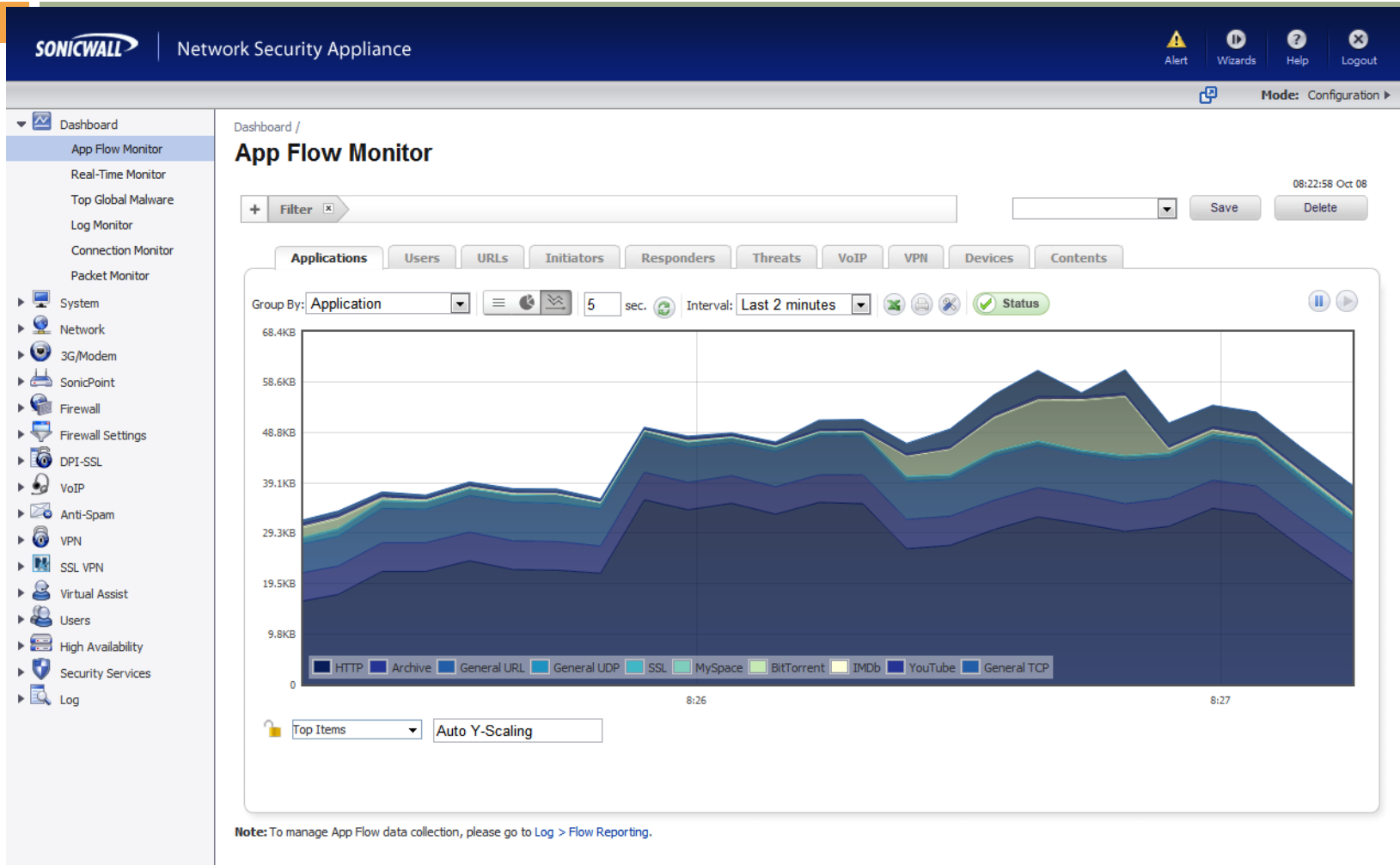
duyn@uit.edu.vn

**SECURITY**

**APPLICATION AWARENESS**

- **FINGERPRINT APPLICATIONS**
- **IDENTIFY USERS**
- **VISUALIZE TRAFFIC**

# Application Traffic Visualization



# Network Analysis Tools

# Do I have P2P on my Network?

Network Security Appliance

Dashboard

App Flow Monitor

Real-Time Monitor

Top Global Malware

Log Monitor

Connection Monitor

Packet Monitor

User Monitor

System

Network

3G/Modem

SonicPoint

Firewall

Firewall Settings

DPI-SSL

VoIP

Anti-Spam

VPN

SSL VPN

Users

High Availability

Security Services

WAN Acceleration

Log

Dashboard /

App Flow Monitor

Load Filter:

+

Filter View

x

Applications

Users

URLs

Initiators

Responders

Threats

VoIP

VPN

Devices

Contents

Create Rule

Filter View

Interval: Last 60 seconds

Group: Application

Status

	Application	Sessions	Total Packets	Total Bytes	Ave Rate (KBps)	Threat
<input type="checkbox"/>	BitTorrent/uTorrent	37	22,242	15,705,173	0.359	0
<input type="checkbox"/>	General HTTPS	7	23,833	4,388,049	0.984	0
<input type="checkbox"/>	Google Plus	1	890	231,846	-	0
<input type="checkbox"/>	Jabber (Google Talk)	2	1,013	76,022	-	0
<input type="checkbox"/>	Google	5	125	43,106	1.767	0
<input type="checkbox"/>	HTTP	3	50	27,846	-	0
<input type="checkbox"/>	General UDP	3	125	26,216	-	0
<input type="checkbox"/>	Google Safe Browsing	2	32	13,045	-	0
<input type="checkbox"/>	Gmail (Google Mail)	1	61	8,149	1.989	0
<input type="checkbox"/>	Service RPC Services (IANA)	1	84	7,312	-	0
<input type="checkbox"/>	DNS	8	16	1,905	0.114	0
<input type="checkbox"/>	ICMP	2	4	486	0.237	2

# Network Analysis Tools

Do I have P2P on my Network? **YES**

The screenshot displays the SonicWall Network Security Appliance interface, specifically the App Flow Monitor. The left sidebar shows a navigation menu with options like Dashboard, App Flow Monitor, Real-Time Monitor, Top Global Malware, Log Monitor, Connection Monitor, Packet Monitor, and User Monitor. The main content area is titled 'App Flow Monitor' and includes a 'Filter View' button. Below this, there are tabs for Applications, Users, URLs, Initiators, Responders, Threats, VoIP, VPN, Devices, and Contents. The 'Applications' tab is selected, showing a table of network applications. A red box highlights the 'BitTorrent/uTorrent' application, which has 37 sessions and 22,242 total packets. A black arrow points from the 'BitTorrent/uTorrent' entry in the left sidebar to the highlighted entry in the table.

Application	Sessions	Total Packets
BitTorrent/uTorrent	37	22,242
General HTTPS	7	23,833
Google Plus	1	890
Jabber (Google Talk)	2	1,013

# Immediate Application Control

Do I have P2P on my Network? **YES**

**SONICWALL** | Network Security Appliance

Dashboard / App Flow Monitor

Applications

Create Rule

Filter View

Interval: Last

Applications

- BitTorrent/uTorrent
- General HTTPS
- Google Plus
- Jabber (Google Talk)
- Google
- HTTP
- General UDP
- Google Safe Browsing
- Gmail (Google Mail)
- Service RPC Services (IAX)
- DNS
- ICMP

**Create Rule**

This creates a match object of items from the list below. You can block, bandwidth manage or monitor this match object.

BitTorrent/uTorrent

Please select an action:

- ☒ **Block**
- ☐ **Bandwidth Manage** [Configure](#)
  - BWM Global-Medium
  - BWM Global-Low
- ☐ **Packet Monitor**

Cancel Create Rule

Load Filter:

Contents

Status

Ave Rate (KBps)	Thr
0.359	0
0.984	0
-	0
-	0
1.767	0
-	0
-	0
-	0
1.989	0
-	0
0.114	0
0.237	2

# Network Analysis Tools

“Who’s watching YouTube?”

**SONICWALL** | Network Security Appliance

Alert | Wizards | Help | Logout

Mode: Configuration

Dashboard / **App Flow Monitor**

10:29:08 Oct 04

Filter [x]

Applications | Users | URLs | Initiators | Responders | Threats | VoIP | VPN | Devices | Contents

Group By: Application | 600 sec. | Interval: Last 5 minutes

Application	Sessions	Packets	Bytes	Rate (KBps)	Threats
HTTP	20	905	580640	431.664	0
unclassified	657	2835	339148	917.326	6
Archive	6	523	282565	16.646	0
BitTorrent	52	163	27517	103.826	0
<b>YouTube</b>	12	142	15428	17.247	0
DNS	82	164	13740	80.508	0
MySpace Video	4	41	10338	8.188	0
SSL	1	43	7446	12.346	0
MySpace	1	101	6519	0.874	0
IMDb	6	56	6282	3.132	0
Image	2	14	4404	1.568	0
RSS	1	10	2054	0.835	0

# Network Analysis Tools

## “Who’s watching YouTube?”

**SonicWall Network Security Appliance**

Alert | Wizards | Help | Logout

Mode: Configuration

Dashboard / **App Flow Monitor**

10:29:08 Oct 04

+ Filter x

Save Delete

**Applications** | Users | URLs | Initiators | Responders | Threats | VoIP | VPN | Devices | Contents

Group By: Application | 600 sec. | Interval: Last 5 minutes

Application	Sessions	Packets	Bytes	Rate (KBps)	Threats
HTTP	20	905	580640	431.664	0
unclassified	657	2835	339148	917.326	6
Archive	6	523	282565	16.646	0
BitTorrent	52	163	27517	103.826	0
<b>YouTube</b>	12	142	15428	17.247	0
DNS	82	164	13740	80.508	0
MySpace Video	4	41	10338	8.188	0
SSL	1	43	7446	12.346	0
MySpace	1	101	6519	0.874	0
IMDb	6	56	6282	3.132	0
Image	2	14	4404	1.568	0
RSS	1	10	2054	0.835	0

# User Identification

- Single Sign On (AD/LDAP Integration)
- Local Login
- Identify Top Bandwidth users

**SonicWall Network Security Appliance**

Dashboard / **App Flow Monitor**

Filter [x]

Applications Users URLs Initiators Responders Threats VoIP VPN Devices Contents

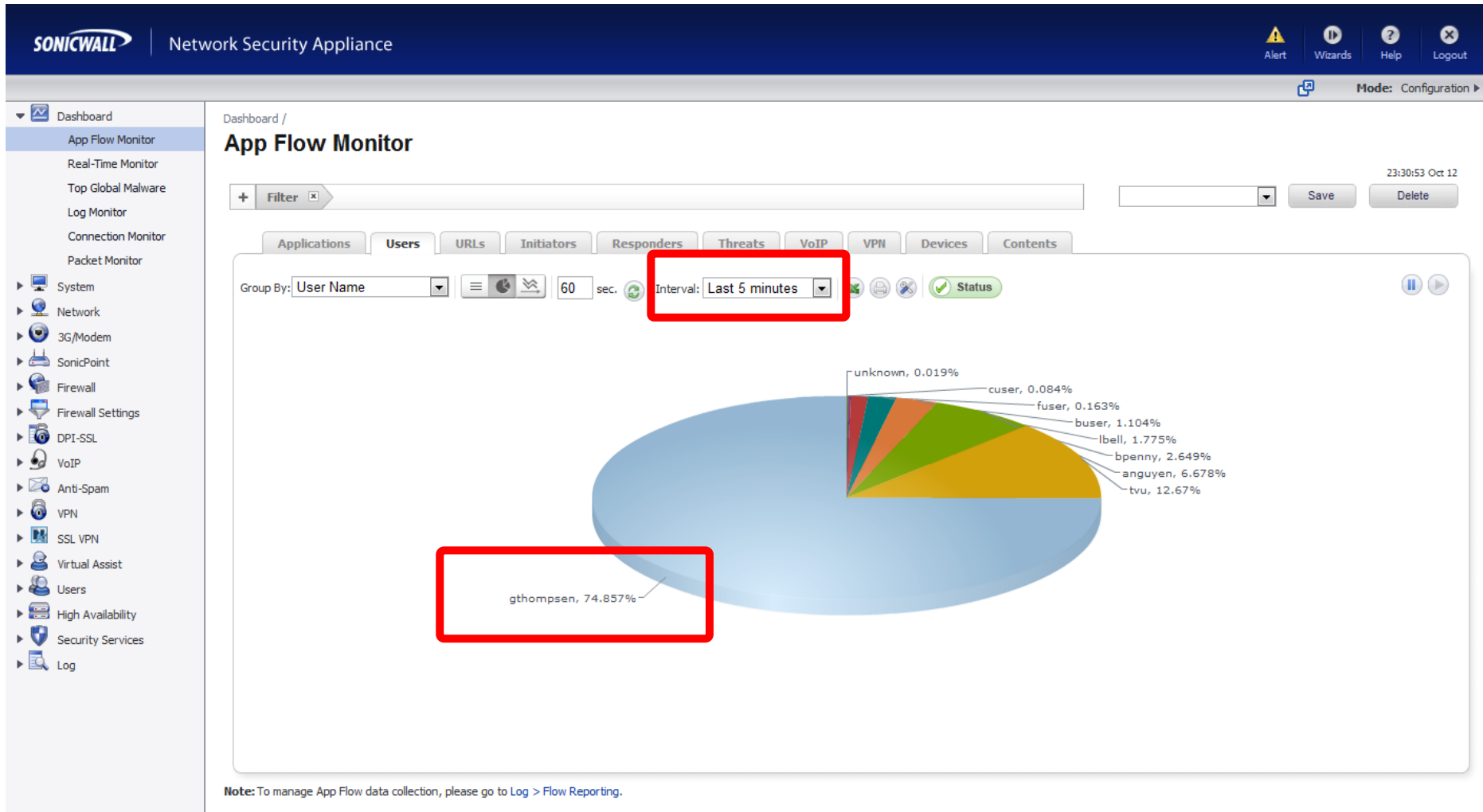
Group By: User Name [600 sec] Interval: Last 5 minutes [Status]

User	Sessions	Packets	Bytes	Rate (KBps)	Threats
bpenny	70	976	276514	250.363	0
lbell	68	911	266337	313.884	0
gthompson	107				
unknown	2				
euser	16				
epresley	1				
buser	54				
ldevore	4				
tvu	57				
anguyen	3				
sforrest	2				
cuser	2				
hholmes	9				
<b>Total:</b>	<b>400</b>				

Note: To manage App Flow data collection, please go to Log > Flow Reporting.



# Identify Top Bandwidth Users



# Connection Tracking by Country



Network Security Appliance



Mode: Configuration ▶

- Dashboard
- Real-Time Monitor
- App Flow Monitor
- Top Global Malware
- Log Monitor
- Connection Monitor
- Packet Monitor
- System
- Network
- 3G/Modem
- SonicPoint
- Firewall
- Firewall Settings
- DPI-SSL
- VoIP
- Anti-Spam
- VPN
- SSL VPN
- Virtual Assist
- Users
- High Availability
- Security Services
- Log

Dashboard /

## App Flow Monitor

+ Filter x

00:05:24 Oct 04

Save

Delete

Applications

Users

URLs

Initiators

Responders

Threats

VoIP

VPN

Devices

Contents

Group By: Country

600 sec.

Interval: Last 5 minutes

Status

Responder	Sessions	Packets	Bytes	Rate (KBps)	Threats
United Kingdom	14	98	11258	22.753	0
Canada	10	54	6935	16.046	0
Germany	4	29	2411	4.368	0
Afghanistan	3	26	2151	2.888	0
Denmark	3	22	2030	5.026	0
Russian Federation	4	8	1765	10.342	0
India	3	15	1405	3.320	0
Taiwan	4	6	1125	6.592	0
Austria	1	11	1052	1.438	0
Slovenia	2	4	872	5.109	0
Italy	2	4	863	5.057	0
Sweden	1	9	799	1.264	0
France	2	3	567	3.322	0
<b>Total:</b>	<b>465</b>	<b>5758</b>	<b>1775002</b>		

# Trace & Identify Network Connections

**SONICWALL** | Network Security Appliance

Alert | Wizards | Help | Logout

Mode: Configuration

Dashboard / App Flow Monitor

00:08:39 Oct 04

Filter Responders

Application Responders Threats VoIP VPN Devices Contents

Group By: Country 600 sec. Interval: Last 5 minutes Status

Responder	Sessions	Packets	Bytes	Rate (KBps)	Threats
<input type="checkbox"/> Russian Federation	3	5	2043	11.971	0
<input type="checkbox"/> Thailand	1	15	827	2.802	0
<input type="checkbox"/> Bahamas	1	2	366	2.145	0
<b>Total:</b>	<b>9</b>	<b>22</b>	<b>3236</b>		

# Next Generation Firewall

36

duyn@uit.edu.vn

**SECURITY**

**APPLICATION AWARENESS**

**PERFORMANCE**

- **HIGH THROUGHPUT**
- **NO LATENCY**
- **ANY SIZE NETWORK**

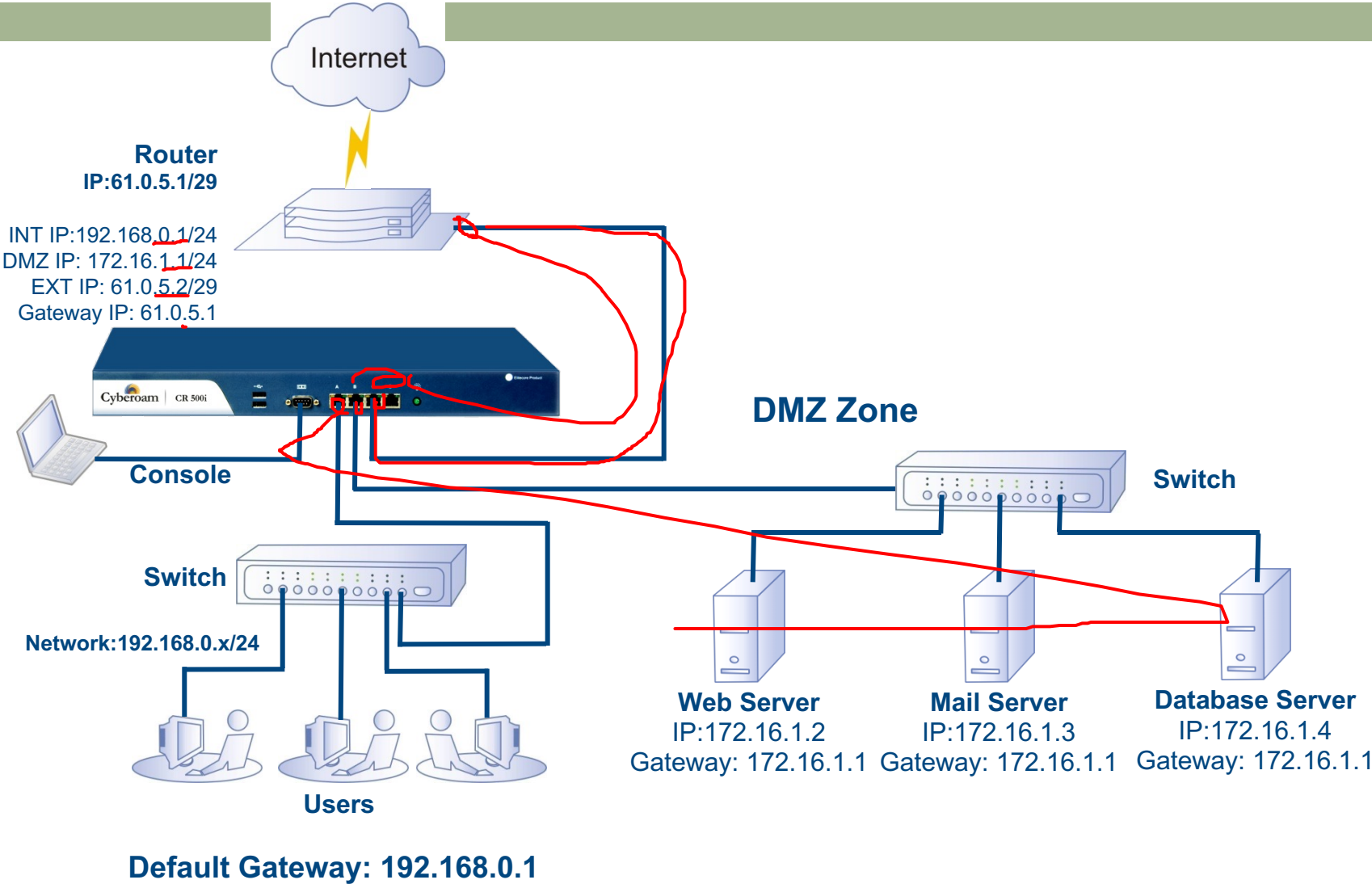
# Nội dung

37

duyn@uit.edu.vn

- Tường lửa là gì?
- Phân loại tường lửa?
- Tính năng của tường lửa thế hệ mới?
- **Mô hình triển khai tường lửa**

# Cyberoam in Gateway Mode



## Zone information when Cyberoam is in Gateway mode

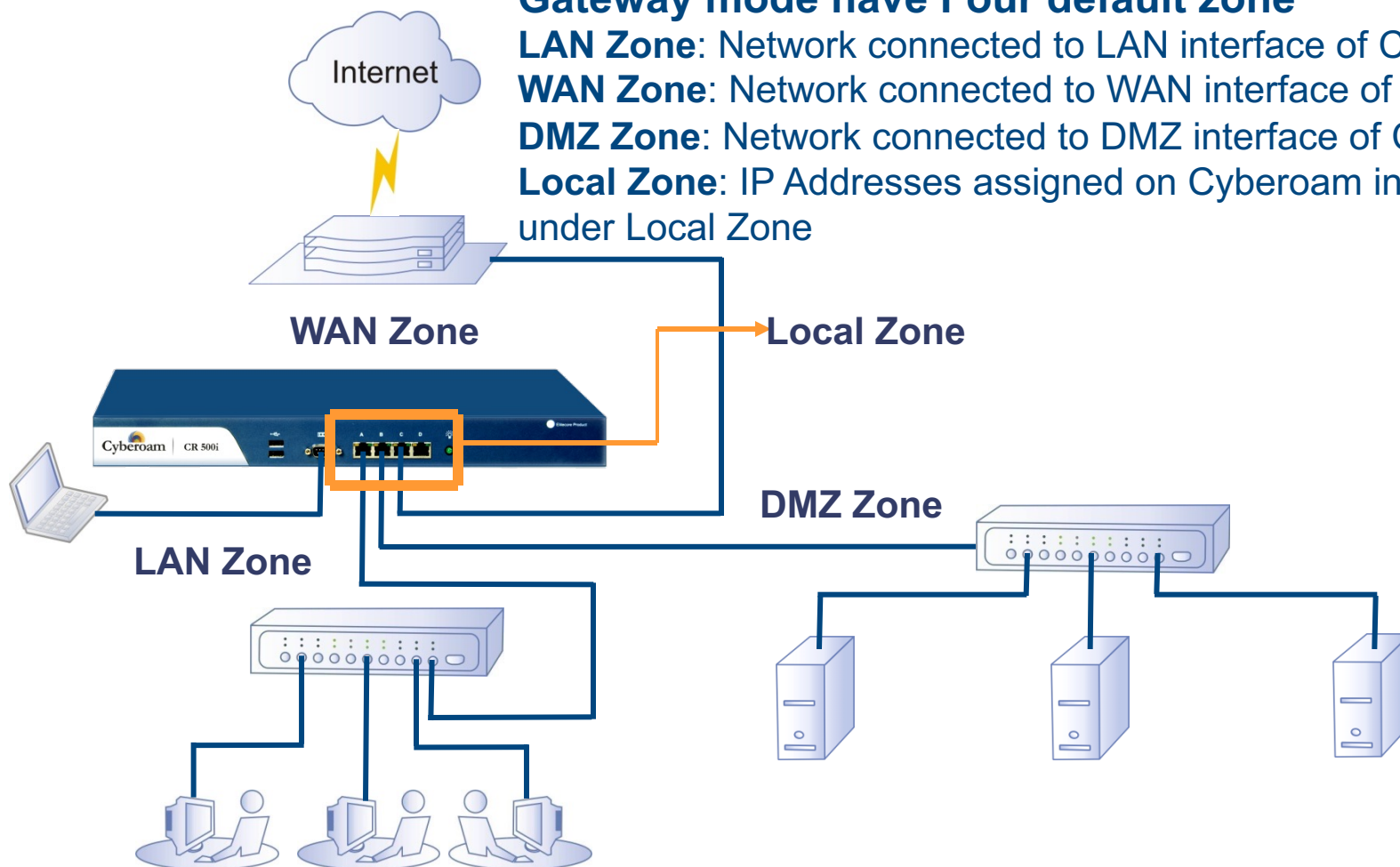
### Gateway mode have Four default zone

**LAN Zone:** Network connected to LAN interface of Cyberoam

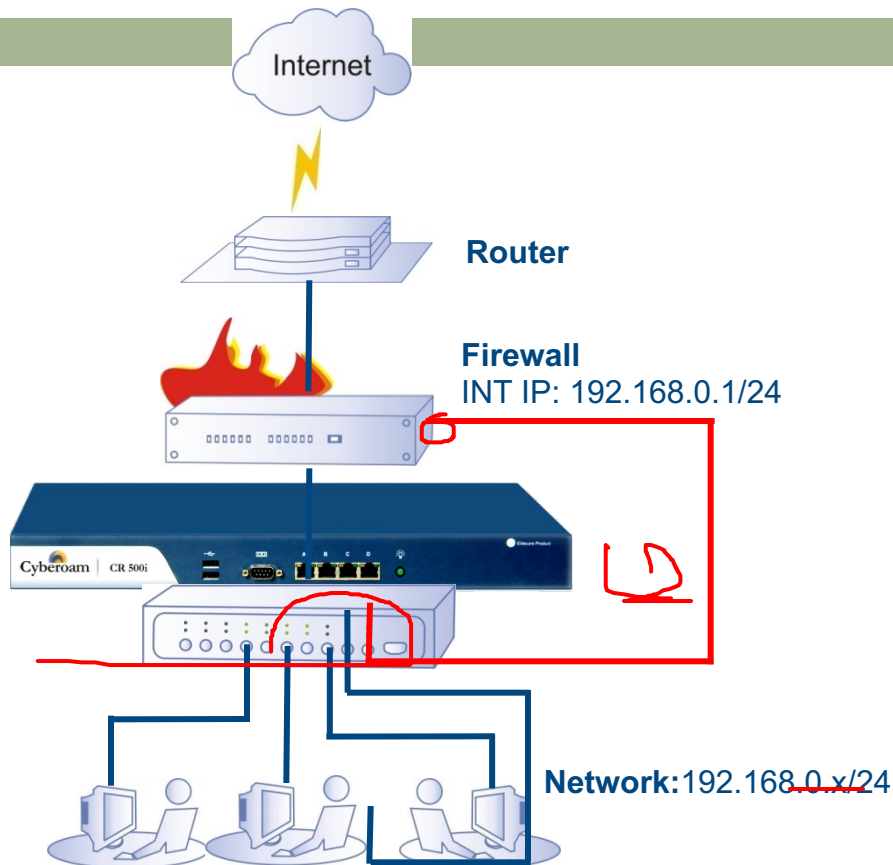
**WAN Zone:** Network connected to WAN interface of Cyberoam

**DMZ Zone:** Network connected to DMZ interface of Cyberoam

**Local Zone:** IP Addresses assigned on Cyberoam interfaces falls under Local Zone



# Cyberoam in Bridge Mode



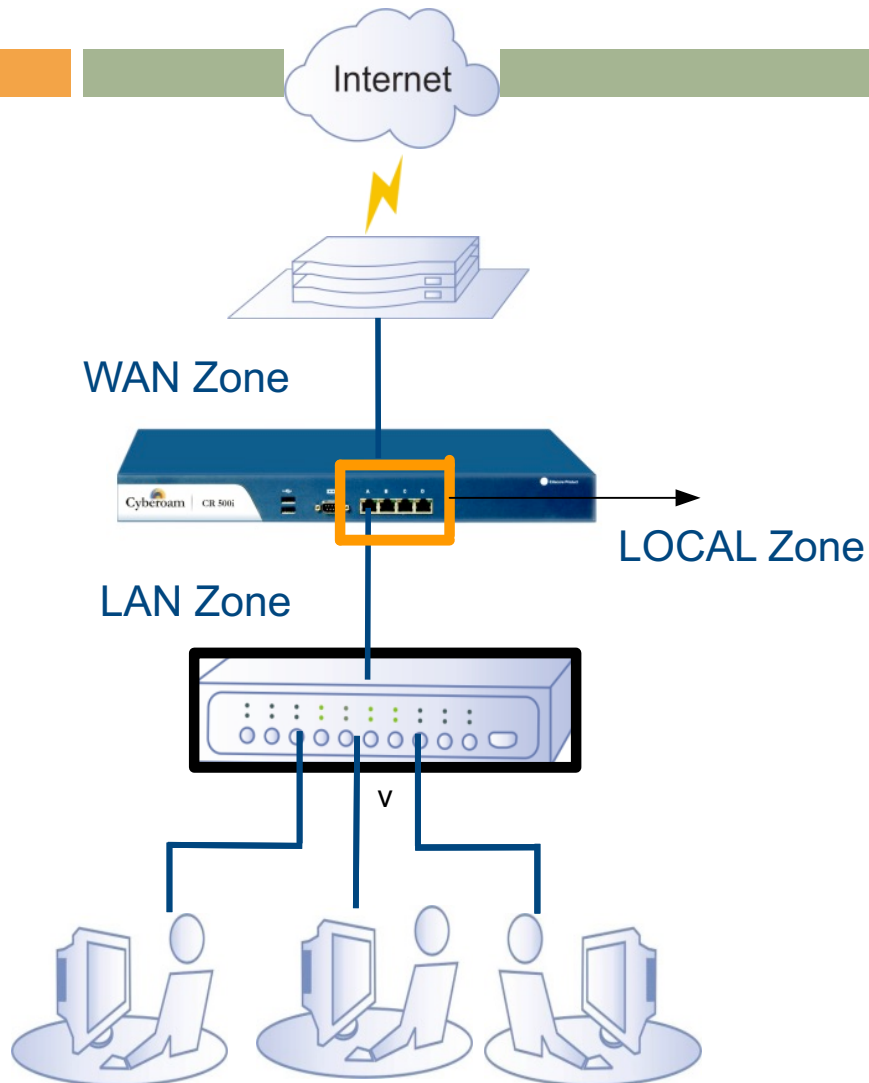
Bridge IP Address	<u>192.168.0.5</u>
Subnet Mask	<u>255.255.255.0</u>

IP address of the Default Gateway	<u>192.168.0.1</u>
DNS IP Address	<u>202.54.1.30</u>
System Time Zone	_____
System Date and Time	_____
Email ID of the administrator	_____

Default Gateway: 192.168.0.1



## Zone information when Cyberoam is in Transparent mode



Cyberoam in transparent mode have three default zone

**LAN Zone:** Network connected to LAN interface of Cyberoam

**WAN Zone:** Network connected to WAN interface of Cyberoam

**Local Zone:** IP Address assigned on the Bridge Interface falls under Local Zone

# Câu hỏi ôn tập

42

duyn@uit.edu.vn

- So sánh ACL, Firewall & NG-Firewall
  - Vị trí đặt trong hệ thống mạng
  - Filter được gì trong packets?
  - Connection?
  - Đối tượng kiểm soát?
  - Hiệu suất xử lý?
- Mô tả tính năng Identity authentication, Web Filtering, Application Control.
- Mô tả tính năng DPI.

Question ???