

## **Bài 14. Một số công cụ tấn công phòng thủ hiện đại**

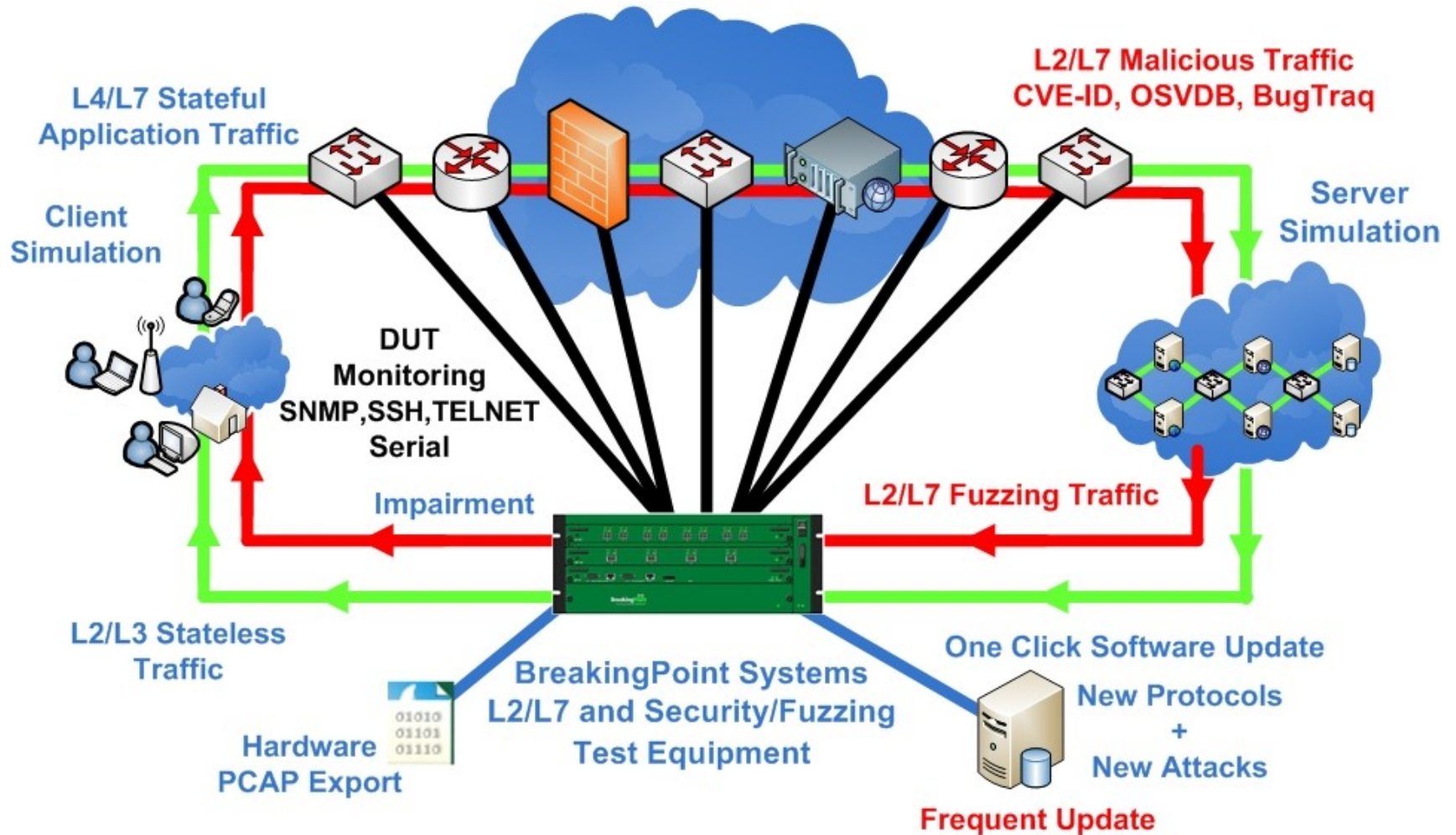
Học phần: ĐẢM BẢO VÀ AN TOÀN THÔNG TIN

# NỘI DUNG

---

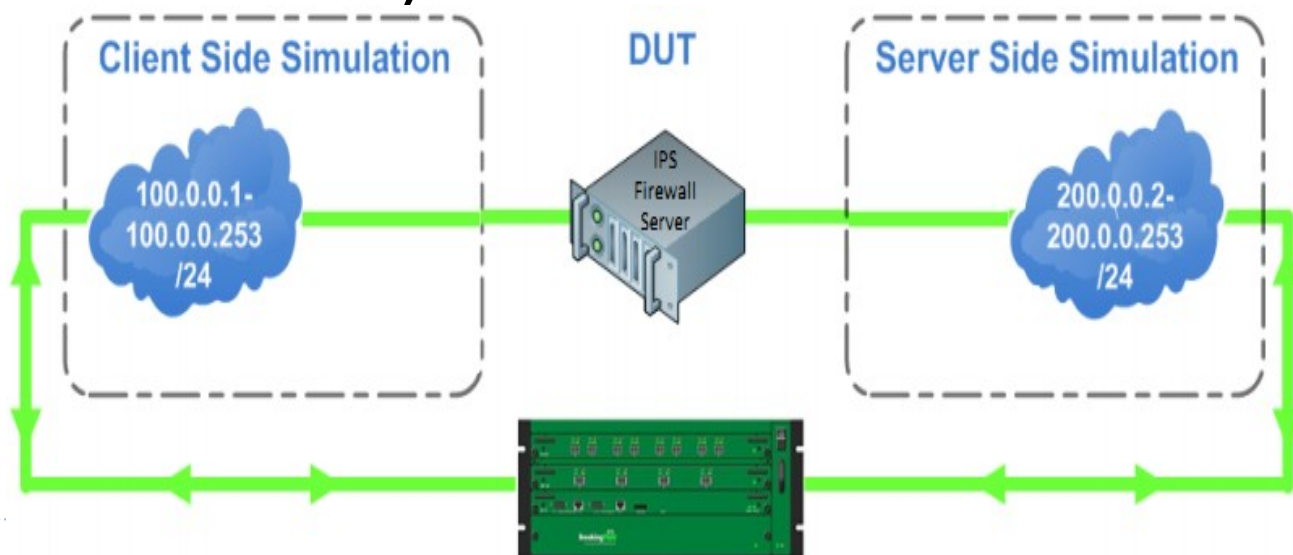
- 1. Hệ thống tấn công BPS**
- 2. Công cụ Burpsuit**
- 3. Hệ thống Flowmon**
- 4. Hệ thống Sonicwall TZ400**
- 5. Hệ thống addnet**
- 6. Hệ thống Logrythm**

# 1. Hệ thống tấn công BPS



# 1. Hệ thống tấn công BPS

BreakingPoint (BP) là thiết bị được sử dụng để kiểm tra tính năng bảo mật và hiệu năng phòng vệ của các thiết bị/hệ thống bảo mật như: Firewall, IPS/IDS,... bằng cách thực hiện các tấn công (DDoS, Malware, Virus, ...) với lưu lượng cực lớn vào thiết bị kiểm tra DUT (Device Under Test).



# 1. Hệ thống tấn công BPS

---

- Mô phỏng linh hoạt các tấn công an ninh mạng phức tạp theo các kịch bản dựng trước, với trên 100 kỹ thuật lảng tránh – evasions, cùng với hàng chục nghìn các phần mềm độc hại, botnets, tấn công DDoS, strike list, ...
- BP Firestorm có khả năng cung cấp trên 180 giao thức ứng dụng, bao gồm các ứng dụng phổ biến như Facebook, WebHTTP, IBM DB2, Microsoft CIFS/SMB, Google Mail, Skype,... Người dùng cũng có thể
- BP Firestorm cũng có thể được sử dụng để kiểm tra năng lực xử lý của các thiết bị mạng khác như Router, Switch, Server, ... bằng cách phát dữ liệu với lưu lượng lớn để kiểm tra

# 1. Hệ thống tấn công BPS

Màn hình đăng nhập:

ixia WEB APPS HELP ▾

ENTER YOUR CREDENTIALS

Username  
[input field]

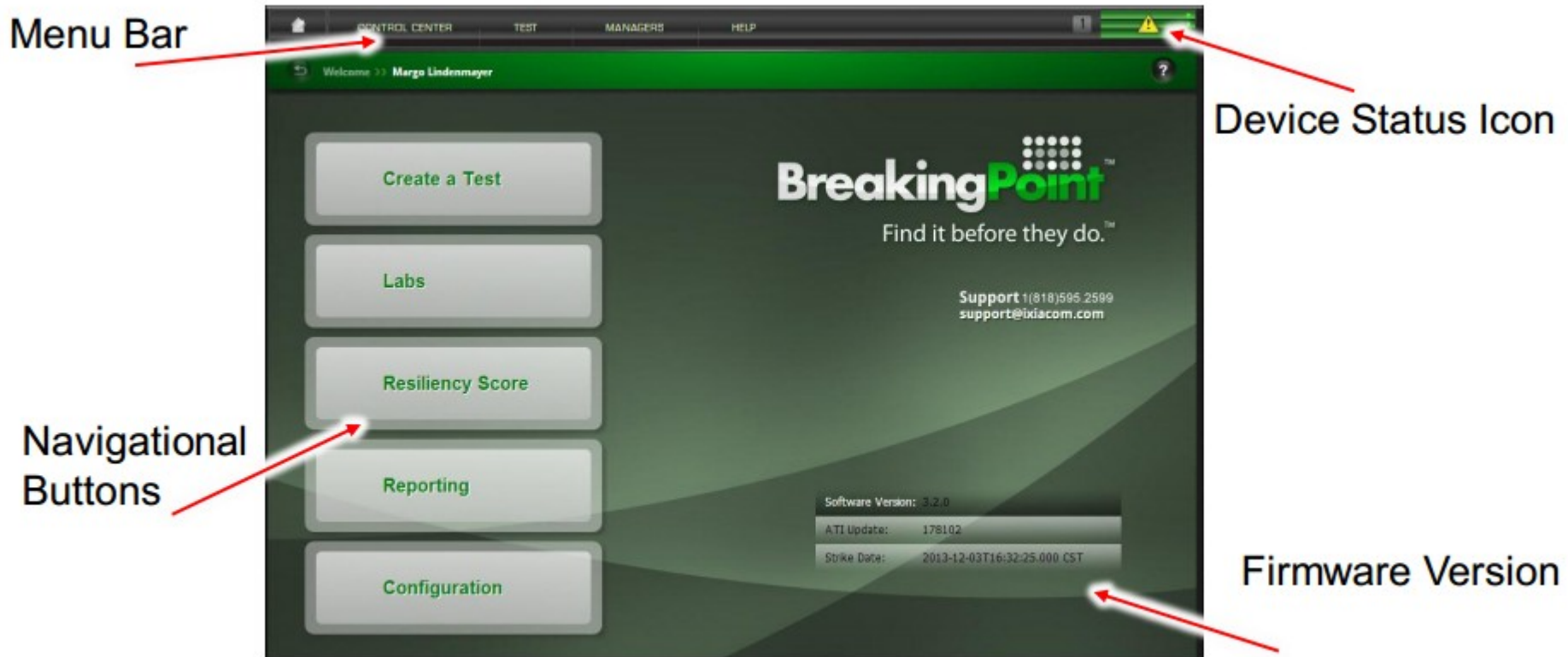
Password  
[input field]

☐ Remember me LOGIN

Copyright © Ixia 2013. All rights reserved

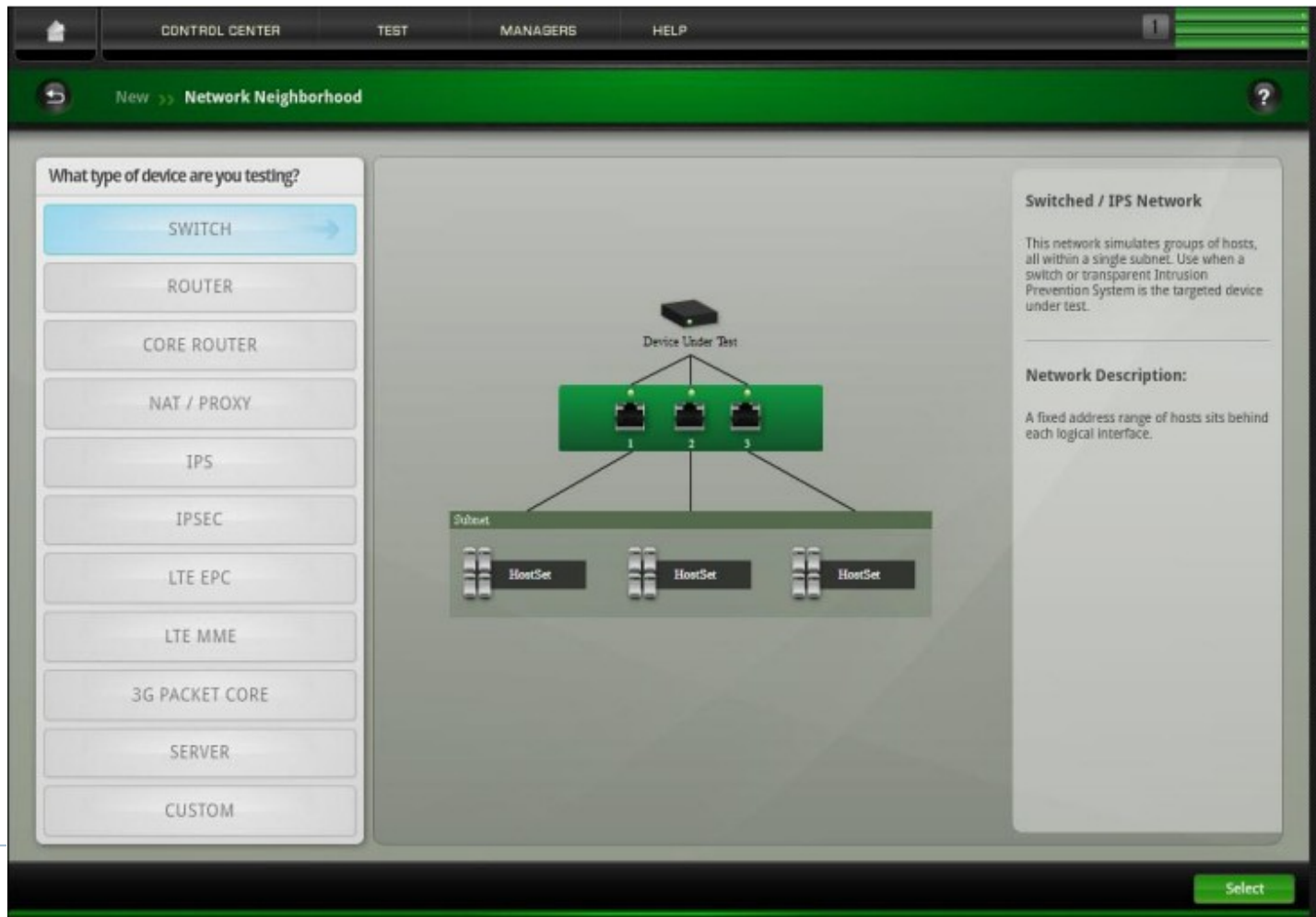
# 1. Hệ thống tấn công BPS

Giao diện của một phiên làm việc được chia thành các phần chính như hình sau:



# 1. Hệ thống tấn công BPS

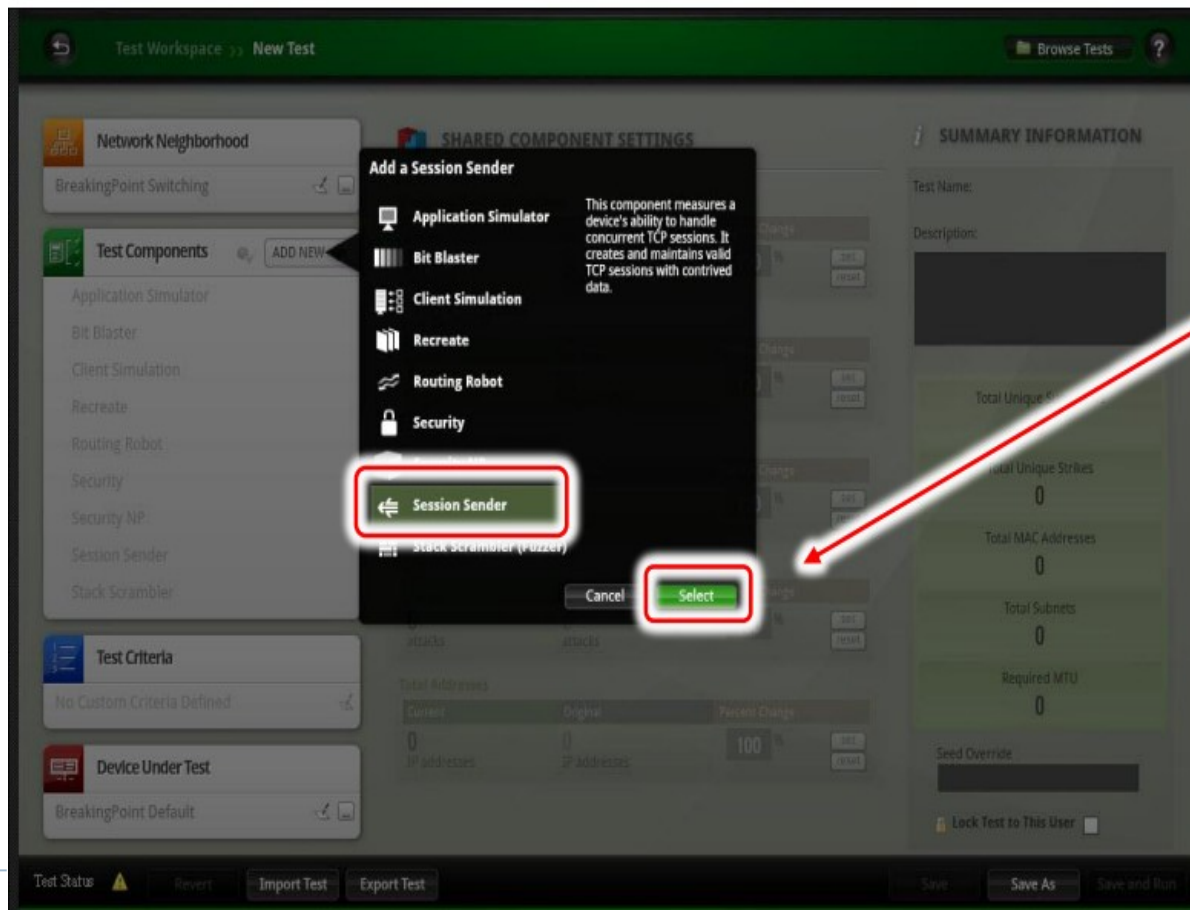
## Thiết lập sơ đồ mạng





# 1. Hệ thống tấn công BPS

Session Sender đo khả năng tải của thiết bị

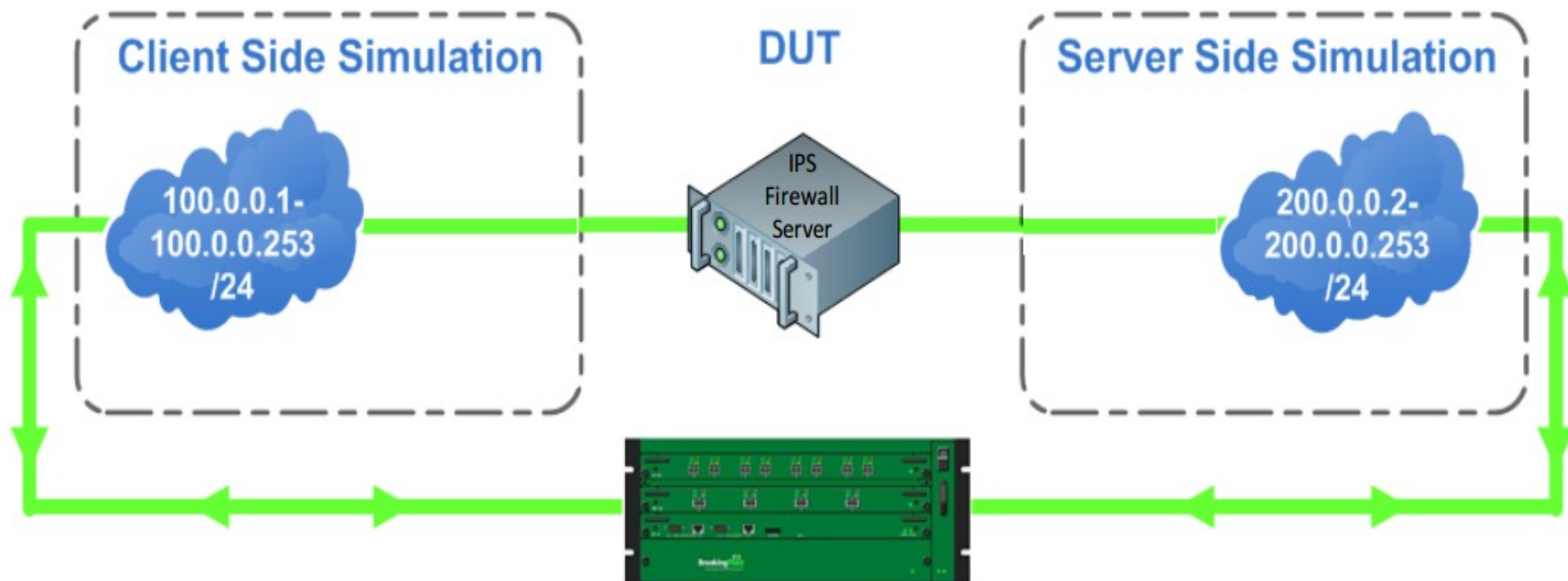


Choose  
Session  
Sender.

Click Select to  
move to the  
next step.

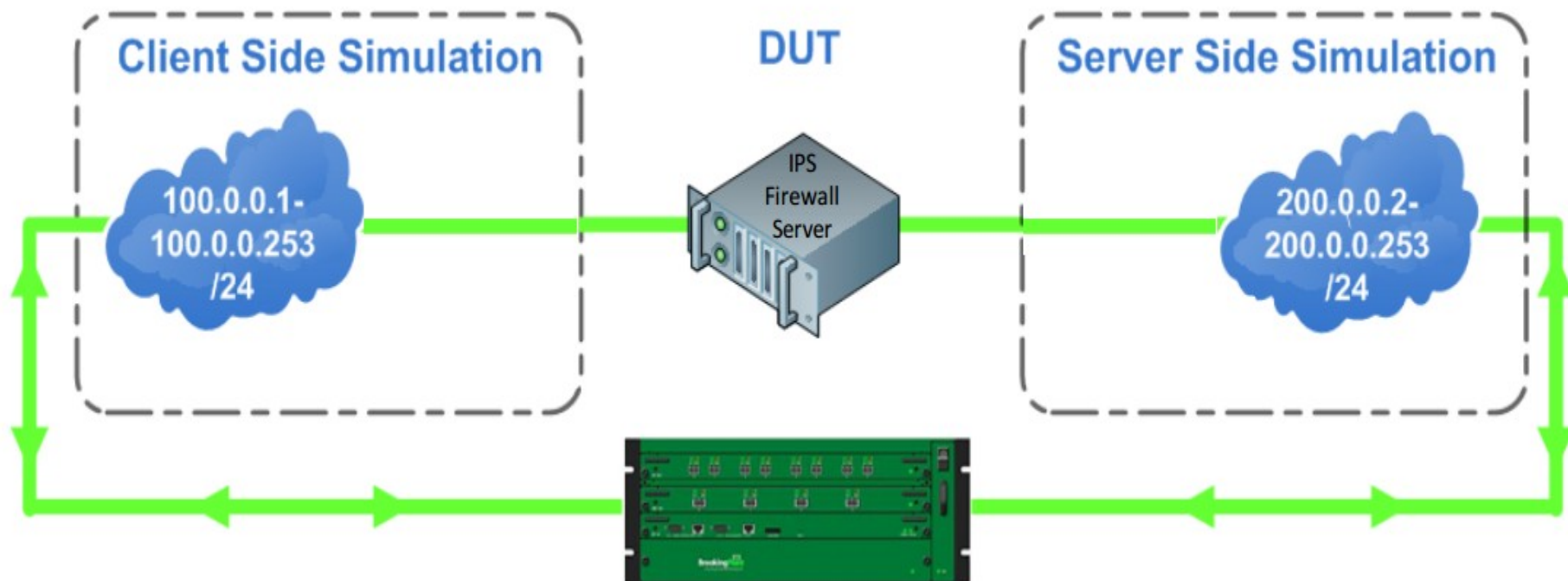
# 1. Hệ thống tấn công BPS

Sử dụng Stack Scrambler để kiểm tra hoạt động của IDS, Firewalls và các thiết bị bảo mật.



# 1. Hệ thống tấn công BPS

Dùng Strike để tạo 1 tấn công hoặc 1 luồng dữ liệu để khai thác hoặc tìm lỗ hổng thiết bị (CVE).



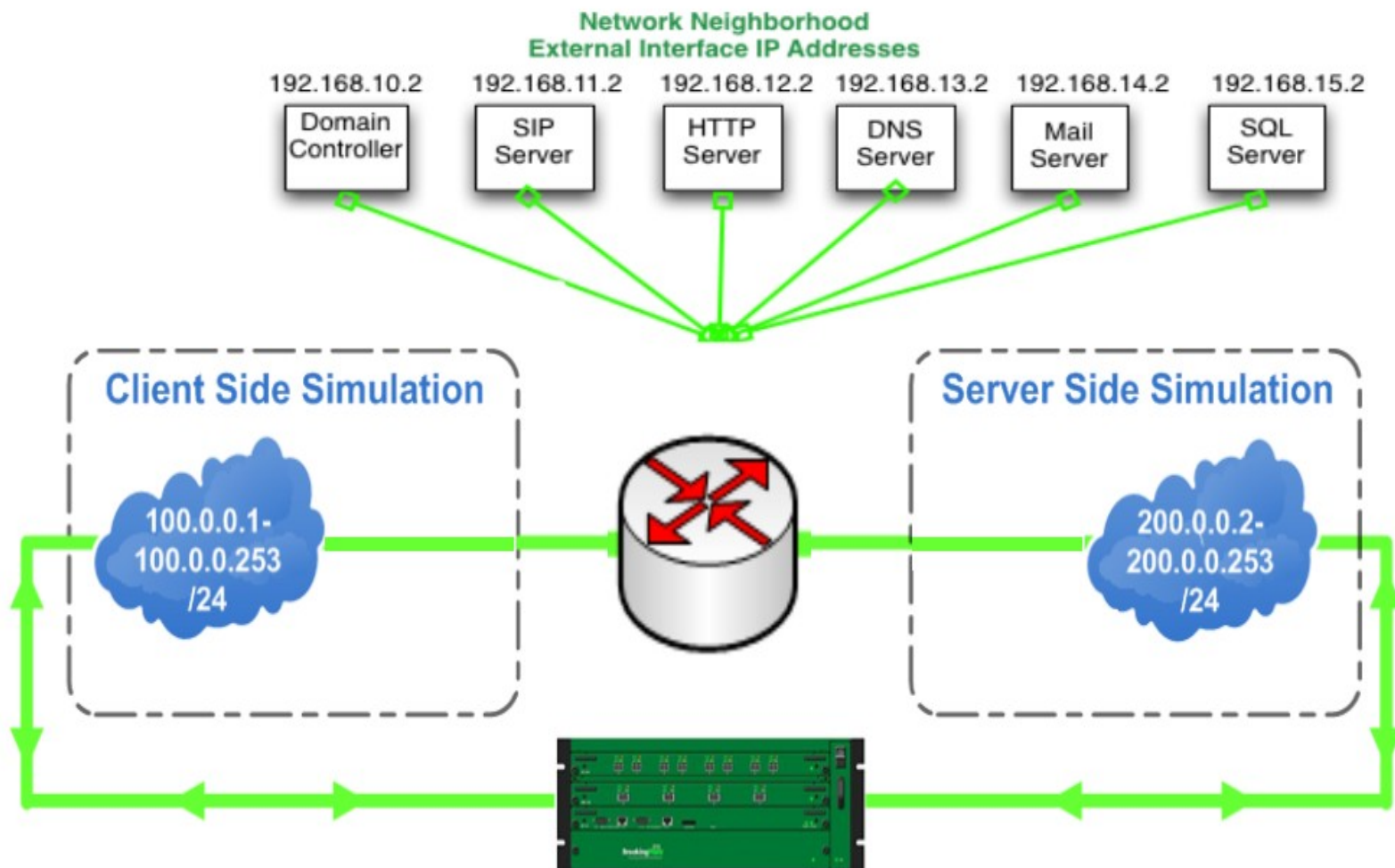
# 1. Hệ thống tấn công BPS

---

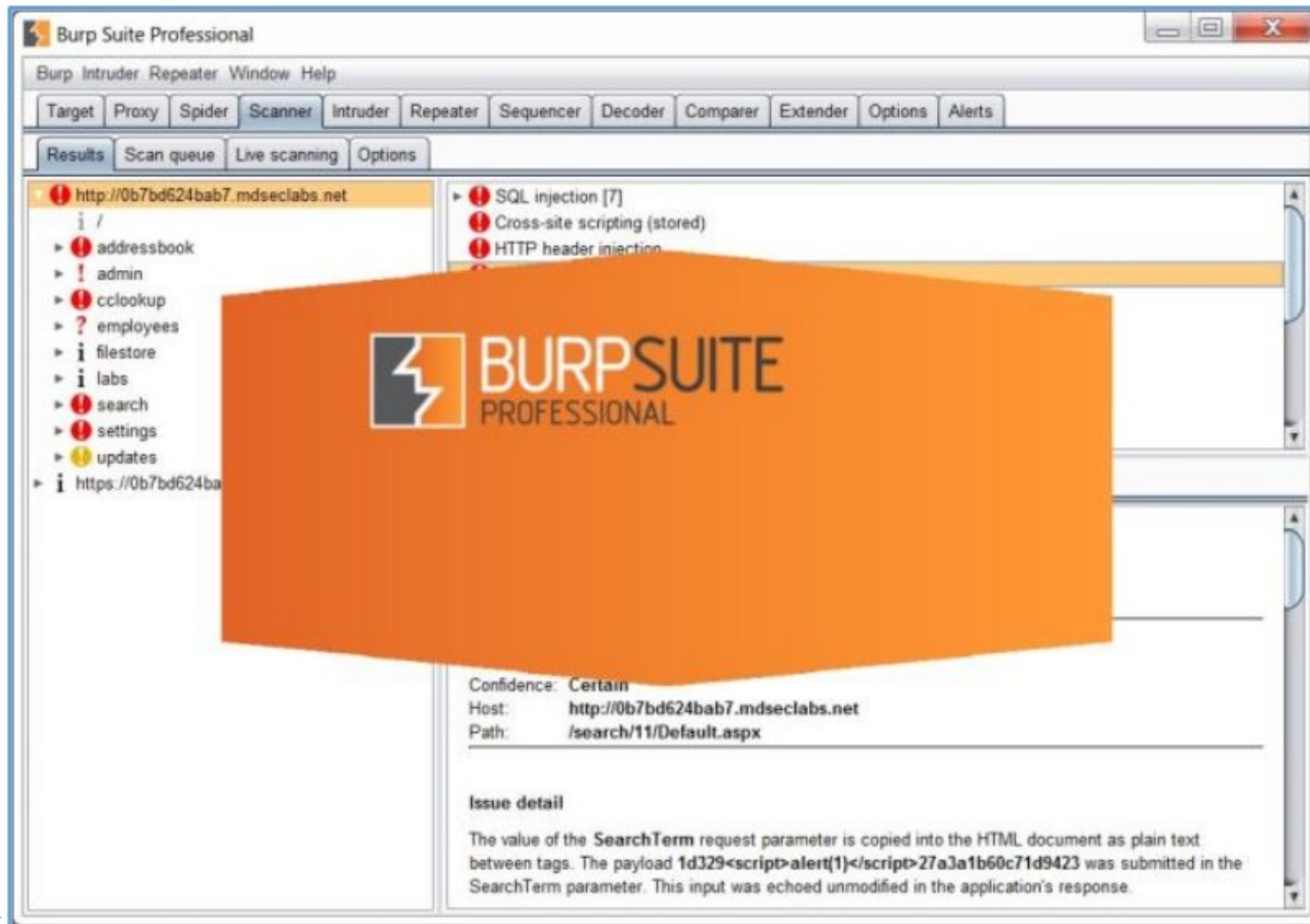
- Application Simulator mô phỏng làm thế nào mà hàng triệu người tương tác và trao đổi với người khác, và thực hiện các giao dịch điện tử sử dụng các ứng dụng Internet chẳng hạn như Facebook, Twitter, Skype, Netflix, Yahoo IM, Yahoo Mail, Gmail, Gtalk..
- Có thể tạo ra được 1 lượng lớn các requests bằng các flow

# 1. Hệ thống tấn công BPS

- Có thể tạo ra được 1 lượng lớn các requests bằng các flow



## 2. Công cụ Burpsuite



## 2. Công cụ Burpsuite

---

Burp suite là một ứng dụng java dùng để kiểm thử xâm nhập ứng dụng web

Các tính năng:

- Interception Proxy: được thiết kế để bắt các request gửi lên server.
- Repeater: cho phép sửa đổi nội dung request một cách nhanh chóng.
- Intruder: tự động hóa việc gửi các payloads lên server.
- Decoder: decode và encode string theo các format khác nhau (URL, Base64, HTML,...).

## 2. Công cụ Burpsuite

---

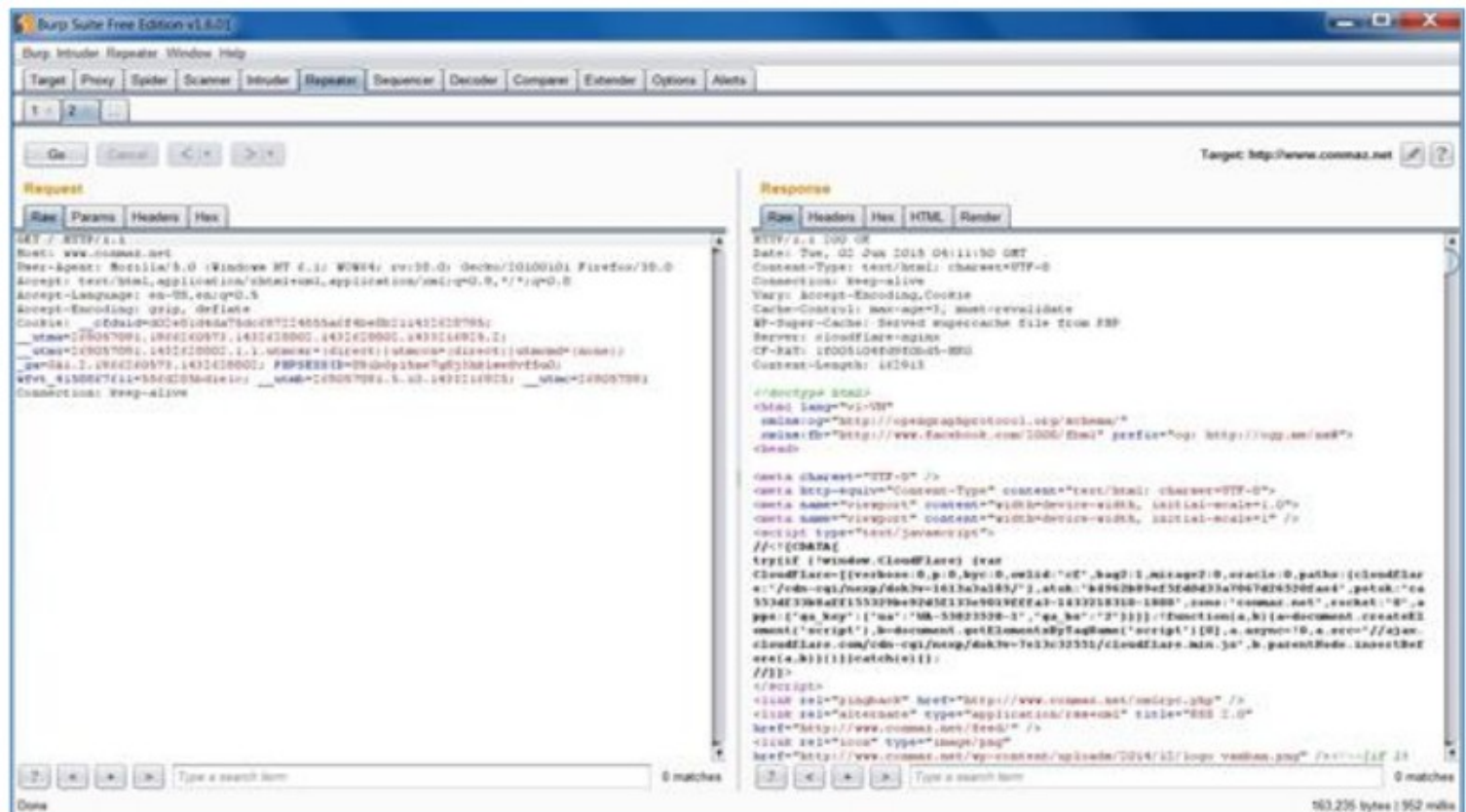
### Các tính năng:

- Comparer: chỉ ra sự khác nhau giữa các requests/responses
- Extender: API để mở rộng chức năng của Burp Suite. Bạn có thể download các extensions thông qua Bapp Store.
- Spider & Discover Content: crawl link có trong ứng dụng web.
- Scanner (chỉ có trong bản Pro): tự động quét các lỗ hổng trong ứng dụng web (XSS, SQLi, Command Injection, File Inclusion,...).

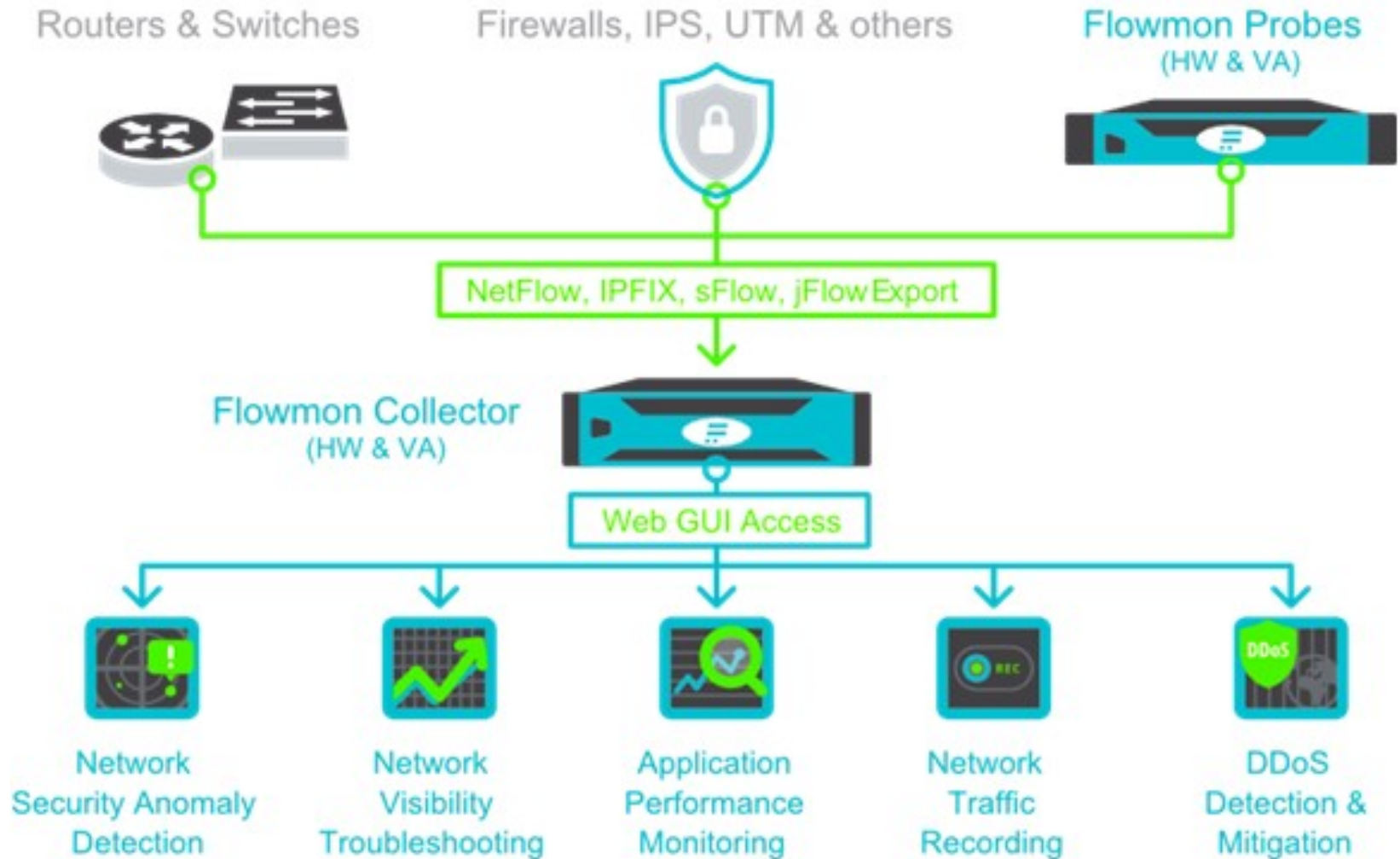


## 2. Công cụ Burpsuite

**Ví dụ chức năng Repeter:** dùng có thể tùy thay đổi và phát lại các yêu cầu HTTP khác nhau gửi tới server, phân tích các phản hồi từ phía server khi gửi các yêu cầu khác nhau.



### 3. Hệ thống Flowmon



### 3. Hệ thống Flowmon

---

- Giải pháp giám sát và phân tích luồng dữ liệu bất thường trên nền công nghệ NetFlown 9.0 (IPFIX) và Packet Capture sử dụng Probe và Collector
- Các module: Application Performance Monitoring, DDOS defender, Traffic recorder, Anomaly Detection & Network Behavior Analysis.

### 3. Hệ thống Flowmon

---

#### **FlowMon Probe**

- Thu thập toàn bộ lưu lượng mạng của doanh nghiệp, tổ chức
- Tập hợp thông tin gửi tới thiết bị FlowMon Collector
- Hỗ trợ NetFlow v5/v9, IPFIX, sFlow, NetStream, jFlow including NBAR2, SEL/NEL, MAC addresses, HTTP information, VoIP statistics support

### 3. Hệ thống Flowmon

---

#### **FlowMon Probe**

- Thông tin mở rộng WHOIS, IP reputation databases
- Hỗ trợ tích hợp SIEM: CEF (Syslog, SNMP)
- Khả năng thông báo qua E-mail, SMS, Syslog, SNMP
- Khả năng phát hiện bất thường qua SPAM, Port scan, DNS, ICMP, DoS, DDoS

### 3. Hệ thống Flowmon

---

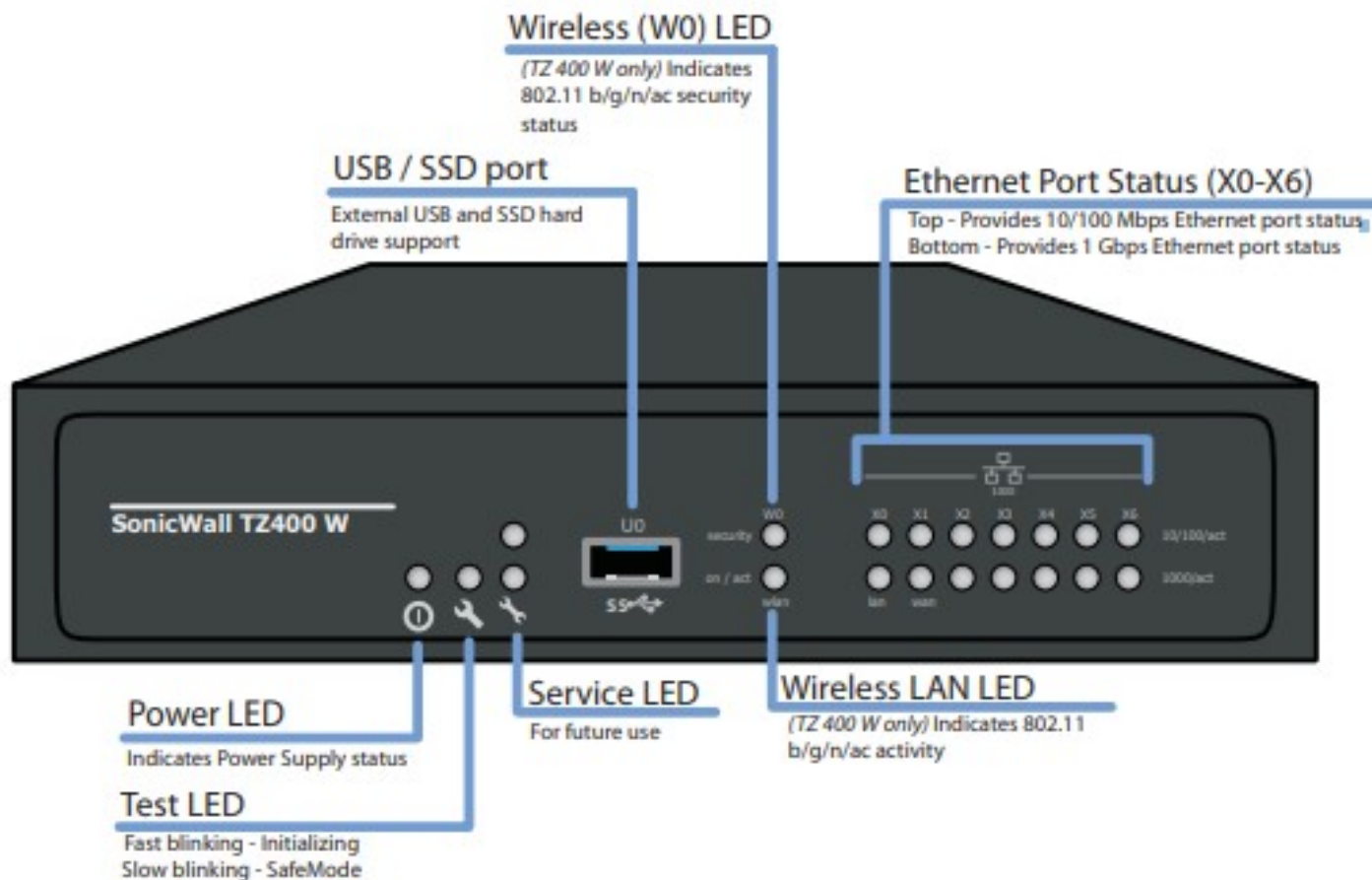
#### **FlowMon Collector**

- Tiếp nhận thông tin luồng dữ liệu từ các thiết bị Flowmon Probe
- Xử lý dữ liệu để hiển thị, cảnh báo bất thường
- Hỗ trợ thu thập flow: NetFlow v5/v9/IPFIX
- Hỗ trợ IPv4, IPv6, MAC, VLAN, MPLS
- Phân tích, dò ứng dụng HTTP & VoIP
- Giao diện quản trị web

### 3. Hệ thống Flowmon



## 4. Hệ thống Sonicwall TZ400





## 4. Hệ thống Sonicwall TZ400

---

- Là sản phẩm FireWall Next Generation với nhiều sản phẩm bảo mật được tích hợp sâu với nhau thành một khối thống nhất
- Quét files theo dạng stream base giúp tường lửa thế hệ mới có thể quét files với kích cỡ khác nhau và hỗ trợ nhiều giao thức.
- Nhiệm vụ: Cho phép, chặn lại, ghi lại hoạt động, giám sát, phân tích dữ liệu qua nó

## 4. Hệ thống Sonicwall TZ400

### Cấu hình block 1 địa chỉ web

The screenshot displays the SonicWall Network Security Appliance configuration interface. On the left, a navigation tree lists various system settings, with 'CFS Policies' highlighted under the 'CFS Exclusion' section. The main configuration area is titled 'CFS Policy' and contains the following fields:

- Name: Block\_Web
- Source Zone: Lan600
- Destination Zone: Lan1
- Source Address: Any
- User/Group: All
- Schedule: Always On
- Profile: Block\_Website
- Action: CFS Default Action

At the bottom of the configuration area, the status is 'Ready'. Below the configuration area, there are 'OK' and 'Cancel' buttons.

## 4. Hệ thống Sonicwall TZ400

Cấu hình chuyển log sang thiết bị khác để phân tích

The screenshot displays the Sonicwall log management interface. A table of logs is visible with columns for Action, Log Entity, Log Source Type, Log Source Name, and Collection Host. A context menu is open over the table, showing options like Associate, Check All, Check All Displayed, Uncheck All, Uncheck All Displayed, Clear Filters, Actions, View, Export Grid To File, Properties, Change Log Source Type, Resolve Log Source Hosts, Accept, Reject, and Delete. The 'Resolve Log Source Hosts' option is highlighted.

Action	Log Entity	Log Source Type	Log Source Name	Collection Host
<input type="checkbox"/>	HVKTQS	Syslog - Cisco Router	10.16.40.1 Cisco Router S...	Entity: ROOM 310 (MO), Host: Irhxm0
<input type="checkbox"/>	HVKTQS		10.16.41.1 Cisco Router S...	Entity: ROOM 310 (MO), Host: Irhxm0
<input type="checkbox"/>	HVKTQS		10.16.36.1 Cisco Router S...	Entity: ROOM 310 (MO), Host: Irhxm0
<input type="checkbox"/>	HVKTQS		10.16.33.1 Cisco Router S...	Entity: ROOM 310 (MO), Host: Irhxm0
<input type="checkbox"/>	HVKTQS		10.16.35.1 Cisco Router S...	Entity: ROOM 310 (MO), Host: Irhxm0
<input type="checkbox"/>	ROOM 308 (BO3)		10.0.22.105 Cisco Switch...	Entity: ROOM 310 (MO), Host: Irhxm0
<input type="checkbox"/>	ROOM 309 (BO3)	SW-3850-BO-03	10.0.23.105 Cisco Switch...	Entity: ROOM 310 (MO), Host: Irhxm0
<input type="checkbox"/>	ROOM 310 (MO)	10.0.23.105	10.0.23.105 Cisco Switch...	Entity: ROOM 310 (MO), Host: Irhxm0

## 4. Hệ thống Sonicwall TZ400

### Ngăn chặn Botnet Server C&C

☒ Accept

SettingsCustom Botnet ListWeb Block PageDiagnostics

☒ Block connections to/from Botnet Command and Control Servers  






















☐ All Connections☒ Firewall Rule-based Connections

☐ Block all connections to public IPs if BOTNET DB is not downloaded  
☐ Enable Custom Botnet List  
☒ Enable Logging

Botnet Exclusion Object:  
Default Geo-IP and Botnet Exclusion Group

## 4. Hệ thống Sonicwall TZ400

### Phát hiện và ngăn chặn tấn công DoS

Filter: 10.0.20.200 Display: Last 60 minutes                                      

## 5. Hệ thống addnet

Là hệ thống giúp quy hoạch hệ thống nhằm mục đích quản lý các thiết bị trong hệ thống dễ dàng hơn. Nhằm tăng cường an toàn an ninh hệ thống.

The screenshot displays the 'Users - Edit' page in a network management application. The top navigation bar includes tabs for Misc, Topology, DHCP options, MS AD, Radius, DNS, Switches, DHCP, Address planning, Imports and exports, Access, and Protocol. The 'Access' tab is selected.

The main content area is titled 'Users - Edit' and contains three tabs: 'User' (selected), 'Basic rights', and 'Limit to Radius user groups'.

Under the 'User' tab, the following fields are visible:

- ID: 6 (Valid from version 221 to Up to now)
- Login: admin
- Password: [empty field]
- Copy password: [empty field]
- First name: admin
- Surname: PAMA
- Password type: Database
- Enabled: Yes
- Language: ENG - English
- Per page: 50

Below these fields is the 'Assigned rules' section, which contains a table with one row:

Rule name
Full access

At the bottom of the 'Assigned rules' section, there is a dropdown menu showing '---' and a '+-' button.

The bottom of the page features five buttons: 'Update', 'Update and back', 'Save as', 'Delete', and 'Back'.

## 5. Hệ thống addnet

---

- Addnet sẽ được thiết lập với nhiều VLAN, mỗi VLAN có vai trò và ý nghĩa riêng, ứng với mỗi dải mạng và được chia thành các block khác nhau cho từng đối tượng thiết bị khác nhau. Ví dụ:
  - + VLAN 100: là Vlan quản lý
  - + VLAN 110: là VLAN dùng cho các Server
  - + VLAN 120 và VLAN 130: là VLAN cho người dùng
- ...
- Quy hoạch không gian địa chỉ IP, gán địa chỉ IP cho các thiết bị
- Quản lý về mặt vị trí địa lý của các thiết bị

## 5. Hệ thống addnet

Một số chức năng:

- Kiểm soát một thiết bị mới khi cắm vào hệ thống theo địa chỉ MAC

The screenshot displays the Addnet system interface. At the top, there is a navigation bar with tabs: Misc, Topology, DHCP options, MS AD, Radius, DNS, Switches, DHCP, Address planning, Imports and exports, Access, and Protocol. Below this, the 'Sniffer - Listing' section shows 'Records: 1-20/20' and 'Per page: 50'. It includes a search bar with the text 'Fulltext search (IPmask define IP pool)', a 'Search' button, and a 'Display' button. A 'Filter' section is visible, allowing users to filter by 'Current status' (All, Unknown, Forbidden, DHCP), 'Date' (with a date range and 'or the last' option), 'Records saved for audit only' (checkbox), 'Network' (set to 'Main\_Office\_Guest-10.255.160.0'), and 'Group by' (set to 'Group by MAC'). Below the filter section is an 'Audit' section with a 'Select records to keep for audit (in this page)' dropdown and buttons for 'All', 'None', and 'Set'. The main table lists 10 records with columns: #, .MAC., MAC DESCRIPTION, .IP., IP DESCRIPTION, ADD, .CURRENT STATUS, PORTS, .FROM., .TO., and AUDIT. The records are listed in a table with alternating green and white rows.

#	.MAC.	MAC DESCRIPTION	.IP.	IP DESCRIPTION	ADD	.CURRENT STATUS	PORTS	.FROM.	.TO.	AUDIT
1	AC:1F:8B:46:C9:39-		10.255.160.2	F S Y	Unknown			2018-09-13 06:46:00	2018-10-10 08:23:23	
2	AC:1F:8B:46:C9:71-		10.255.160.3	F S Y	Unknown			2018-09-13 06:44:14	2018-10-10 07:49:57	
3	8B:3C:8C:55:25:C6-		10.255.160.6	F S Y	Unknown			2018-09-04 18:21:06	2018-10-10 03:53:33	
4	AC:1F:8B:46:C9:70-		10.255.160.3	F S Y	Unknown			2018-10-09 12:12:19	2018-10-09 12:12:19	
5	AC:1F:8B:46:C9:38-		10.255.160.2	F S Y	Unknown			2018-10-09 12:12:18	2018-10-09 12:12:18	
6	74:A2:88:8B:2F:51-		10.255.160.254	F S Y	Unknown			2018-10-09 06:41:47	2018-10-10 10:35:03	
7	18:0B:F2:2F:8B:CA-		10.255.160.82	F S Y	Unknown			2018-09-18 09:17:38	2018-10-09 15:06:09	
8	18:0B:F2:2F:8B:8F-		10.255.160.85	F S Y	Unknown			2018-09-27 04:14:40	2018-10-08 09:32:42	
9	8B:C9:17:A4:8B:08-		10.255.160.90	F S Y	Unknown			2018-09-27 05:19:24	2018-09-27 10:12:17	
10	F8:1B:94:12:45:C4-		10.255.160.83	F S Y	Unknown			2018-09-26 03:26:10	2018-09-26 03:53:33	



## 5. Hệ thống addnet

Một số chức năng:

- Cập nhập 1 danh sách các địa chỉ IP của các thiết bị từ file

The screenshot displays the Novicom web interface for managing network rules. The main section is titled 'Import IP addresses from sniff log into rules - Listing'. It includes a search bar with the text '10.255.160.0/24' and a 'Search' button. Below the search bar, there are filters for 'Type of rule' (set to 'DHCP assignment'), 'Group of DHCP options' (set to 'None'), and 'VLAN ID' (set to '- not selected -'). The 'Fiber network' dropdown is set to 'Main\_Office\_Guest-10.255.160.0/24'. The table below lists 9 records with columns for ID, IP ADDRESS, MAC, NET FOUND, ACTION, and MARK. The 'MARK' column contains checkboxes, and the 'ACTION' column contains 'Add' buttons. The 'MARK' button in the table header is circled in red.

#	IP ADDRESS	MAC	NET FOUND	ACTION	MARK
1.	10.255.160.2	AC:1F:68:46:C9:38	Main_Office_Guest-10.255.160.0/24	Add	<input type="checkbox"/>
2.	10.255.160.2	AC:1F:68:46:C9:38	Main_Office_Guest-10.255.160.0/24	Add	<input type="checkbox"/>
3.	10.255.160.3	AC:1F:68:46:C9:78	Main_Office_Guest-10.255.160.0/24	Add	<input type="checkbox"/>
4.	10.255.160.3	AC:1F:68:46:C9:71	Main_Office_Guest-10.255.160.0/24	Add	<input type="checkbox"/>
5.	10.255.160.5	84:8A:8D:5D:A7:D2	Main_Office_Guest-10.255.160.0/24	Add	<input type="checkbox"/>
6.	10.255.160.6	88:8C:6D:F5:25:C8	Main_Office_Guest-10.255.160.0/24	Add	<input type="checkbox"/>
7.	10.255.160.50	18:0B:F2:2F:85:CA	Main_Office_Guest-10.255.160.0/24	Add	<input type="checkbox"/>
8.	10.255.160.51	18:0B:F2:2F:85:CA	Main_Office_Guest-10.255.160.0/24	Add	<input type="checkbox"/>
9.	10.255.160.62	88:E9:4C:53:44:58	Main_Office_Guest-10.255.160.0/24	Add	<input type="checkbox"/>

## 5. Hệ thống addnet

Một số chức năng:

- Giải phóng địa chỉ IP chết

The screenshot shows the Novicom DHCP management interface. The top navigation bar includes links for Dashboard, Locality, and various network services. The main content area is titled 'Last state via IP - Listing' and shows a list of IP addresses. The interface includes a search bar, a filter section, and a table of IP addresses.

Filter:

Base: [ ] - [ ] or older than: 3 Days or the last [ ] minutes

☐ Hide 0.0.0.0 addresses ☐ Hide link-local addresses ☐ Hide multicast addresses

Filter

Selection

Mark: All None Selection: Add Cancel 0 Selected records [Delete](#) - delete from rules and from address planning Show: All

#	MARK	IP	IP DESCRIPTION	MAC	MAC DESCRIPTION	LAST DHCP	LAST SEEN IN SNTPSR
1.	<input type="checkbox"/>	19.0.0.0		00-12-17-30-1A-5C			2018-09-21 11:35:06
2.	<input type="checkbox"/>	19.0.12.14		00-18-67-89-14-9B			2018-09-11 07:02:01
3.	<input type="checkbox"/>	19.0.28.1		FC-1E-3A-12-83-C4		2018-09-12 06:46:25	2018-09-20 11:35:31
4.	<input type="checkbox"/>	19.0.28.130		00-80-28-29-81-82			2018-10-02 08:29:04

## 5. Hệ thống addnet

Một số chức năng:




- Kiểm soát ngắt kết nối thiết bị

The screenshot displays the Novicom DHCP management interface. At the top, there's a navigation bar with tabs like Misc, Topology, DHCP options, etc. The 'DHCP' tab is active. Below the navigation bar, there's a search bar with fields for 'IP address' and 'MAC'. The MAC address '14 B3 1F 25 F5 0E' is entered and highlighted. A 'Search' button is next to it.



Below the search bar, the 'Overall information' section shows details for the selected MAC address:

IP address					
MAC	14:B3:1F:25:F5:0E	14-B3-1F-25-F5-0E	14B3.1F25.F50E	14B31F.25F50E	14B31F25F50E
Blacklisted	No				
Manufacturer NIC	Dell Inc.				
Resolved IP	No reverse found				

Below this, the 'Rules' section shows a table of DHCP rules:

Type	Enabled	Expired	Emerg	DHCP client	IP addresses	DNS	IP description
DHCP assignment	Yes <b>Disable</b>	No		14:B3:1F:25:F5:0E	10.255.130.60 <b>Change net</b>	MO-Student-14.mta.edu.vn	MO-Student-14   

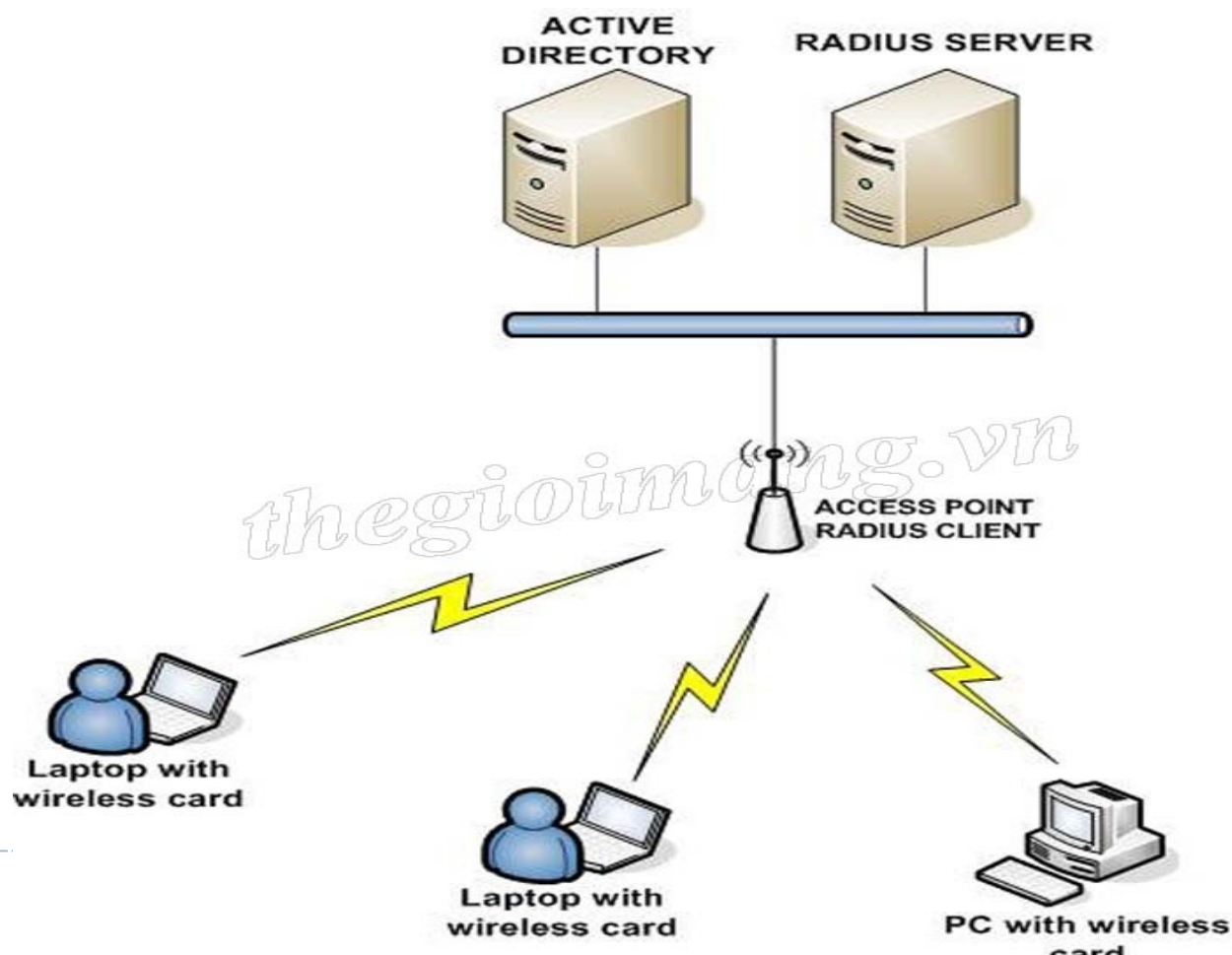
Below the rules table, the 'DHCP client' section shows a table of clients:

MAC and Idents	MAC description	VLAN ID
14 B3 1F 25 F5 0E	MO-Student-14	 

## 5. Hệ thống addnet

Một số chức năng:

- Xác thực kết nối thông qua Radius Server



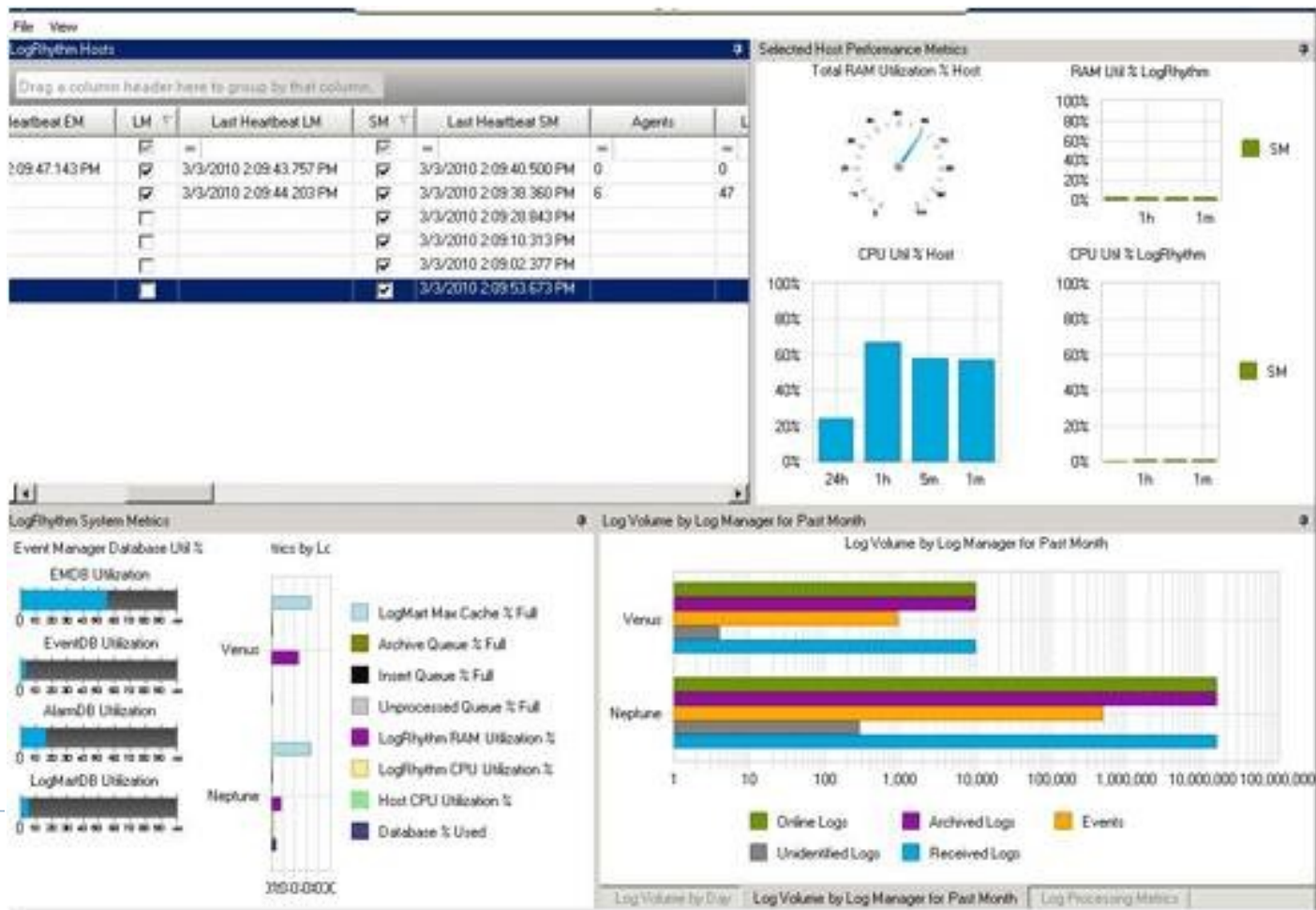
## 6. Hệ thống Logrhythm

Là một hệ thống giám sát mạng thông qua việc quản lý và phân tích hệ thống log từ các thiết bị trong 1 hệ thống mạng.



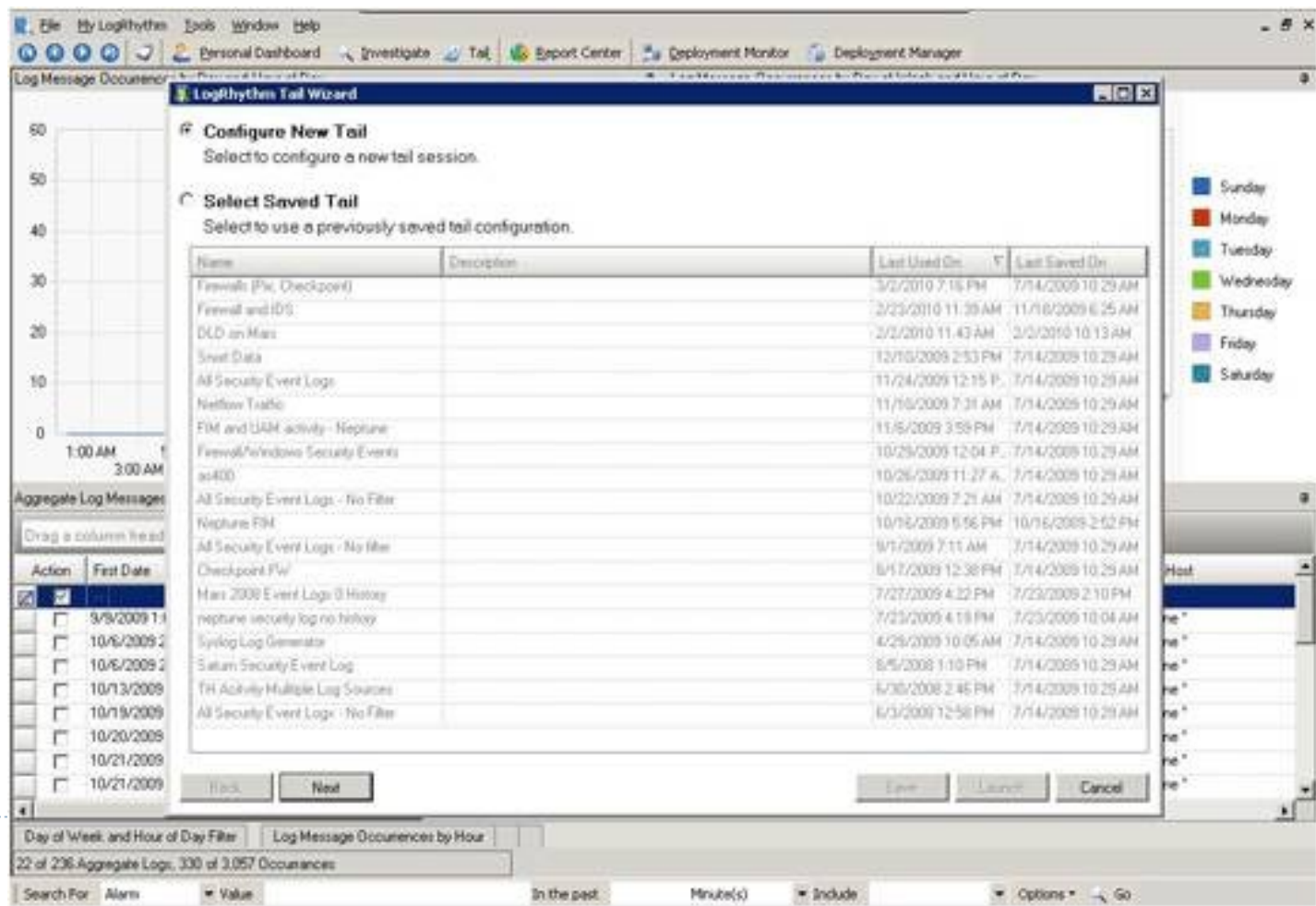
## 6. Hệ thống Logrhythm

- Hiển thị các sự kiện dưới định dạng số theo khoảng thời gian



## 6. Hệ thống Logrhythm

Dữ liệu thu thập được có thể được xem theo thời gian thực





## 6. Hệ thống Logrhythm

### Cấu hình cảnh báo các sự kiện bất thường

The screenshot displays the LogRhythm console interface. The main window shows a table of alarms with columns: Alarm Date, Alarm Status, Alarm Rule Name, Events, Avg RB, Max RB, Entity, and Last Update. The table lists various alarms, including Critical Errors, Suspicious Hosts, Failed Authentications, Invalid User Accounts, and Account Management activities. The status of all listed alarms is 'New'. The 'Entity' column consistently shows 'LogRhythm Labs'.

Alarm Date	Alarm Status	Alarm Rule Name	Events	Avg RB	Max RB	Entity	Last Update
3/2/2010 2:17:36 467 PM	New	Critical Error	1	42.00	42.00	LogRhythm Labs	
3/2/2010 2:20:14 290 PM	New	Suspicious Host..	4	52.00	58.00	LogRhythm Labs	
3/2/2010 2:26:51 930 PM	New	Critical Error	1	42.00	42.00	LogRhythm Labs	
3/2/2010 2:33:35 197 PM	New	Critical Error	1	42.00	42.00	LogRhythm Labs	
3/2/2010 2:35:05 803 PM	New	Critical Error	1	42.00	42.00	LogRhythm Labs	
3/2/2010 2:53:24 370 PM	New	Suspicious Host..	6	47.00	47.00	LogRhythm Labs	
3/2/2010 2:40:14 037 PM	New	Suspicious Host..	100	53.00	53.00	LogRhythm Labs	
3/2/2010 2:54:39 100 PM	New	Failed Authentic..	1	19.00	19.00	LogRhythm Labs	
3/2/2010 2:20:24 790 PM	New	Invalid User Acc..	5	4.00	6.00	LogRhythm Labs	
3/2/2010 2:34:14 303 PM	New	Suspicious Host..	7	28.00	20.00	LogRhythm Labs	
3/2/2010 2:35:36 410 PM	New	Account Manage..	28	3.00	10.00	LogRhythm Labs	
3/2/2010 3:09:44 143 PM	New	Device Shut down	1	8.00	8.00	LogRhythm Labs	
3/2/2010 3:10:24 753 PM	New	Critical Error	1	42.00	42.00	LogRhythm Labs	
3/2/2010 3:12:35 560 PM	New	Critical Error	1	42.00	42.00	LogRhythm Labs	
3/2/2010 3:16:37 487 PM	New	Device Shut down	1	8.00	8.00	LogRhythm Labs	
3/2/2010 2:18:44 073 PM	New	Suspicious Host..	30	28.00	31.00	LogRhythm Labs	
3/2/2010 2:49:14 397 PM	New	Suspicious Host..	6	28.00	28.00	LogRhythm Labs	
3/2/2010 2:49:54 003 PM	New	Device Shut down	2	8.00	8.00	LogRhythm Labs	
3/2/2010 3:24:44 043 PM	New	Suspicious Host..	4	47.00	47.00	LogRhythm Labs	
3/2/2010 3:25:11 953 PM	New	Failed Authentic..	1	19.00	19.00	LogRhythm Labs	
3/2/2010 3:07:42 930 PM	New	Account Manage..	20	4.00	10.00	LogRhythm Labs	
3/2/2010 3:33:16 560 PM	New	Kazza Alerts	1	19.00	19.00	LogRhythm Labs	
3/2/2010 3:27:53 680 PM	New	Critical Error	2	42.00	42.00	LogRhythm Labs	
3/2/2010 3:41:30 917 PM	New	Critical Error	1	42.00	42.00	LogRhythm Labs	
3/2/2010 3:45:02 030 PM	New	Critical Error	1	42.00	42.00	LogRhythm Labs	
3/2/2010 3:50:56 020 PM	New	Invalid User Acc..	2	6.00	6.00	LogRhythm Labs	
3/2/2010 3:56:29 100 PM	New	Suspicious Host..	3	40.00	47.00	LogRhythm Labs	
3/2/2010 3:21:04 917 PM	New	Suspicious Host..	10	28.00	28.00	LogRhythm Labs	

On the right side, the 'Alarm Properties' window is open for the selected alarm (Alarm ID: 220,244). It displays the following details:

- Alarm ID: 220,244
- Alarm Date: 3/2/2010 2:35:36 410 PM
- Alarm Name: Account Management Activity
- Alarm Description: General Access Granted..
- Common Events: 161, 200, 1, 4..
- Originating Systems: 161, 200, 1, 4..
- Impacted Systems: administrator..
- Impacted Applicatio..
- Logins

The bottom status bar indicates 'Alarms Loaded: 452'.



---

# HỎI VÀ ĐÁP