CHƯƠNG 2
NEXT GENERATION FIREWALL

ThS.Nguyễn Duy
duyn@uit.edu.vn

Nội dung

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

Nội dung

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

Nội dung

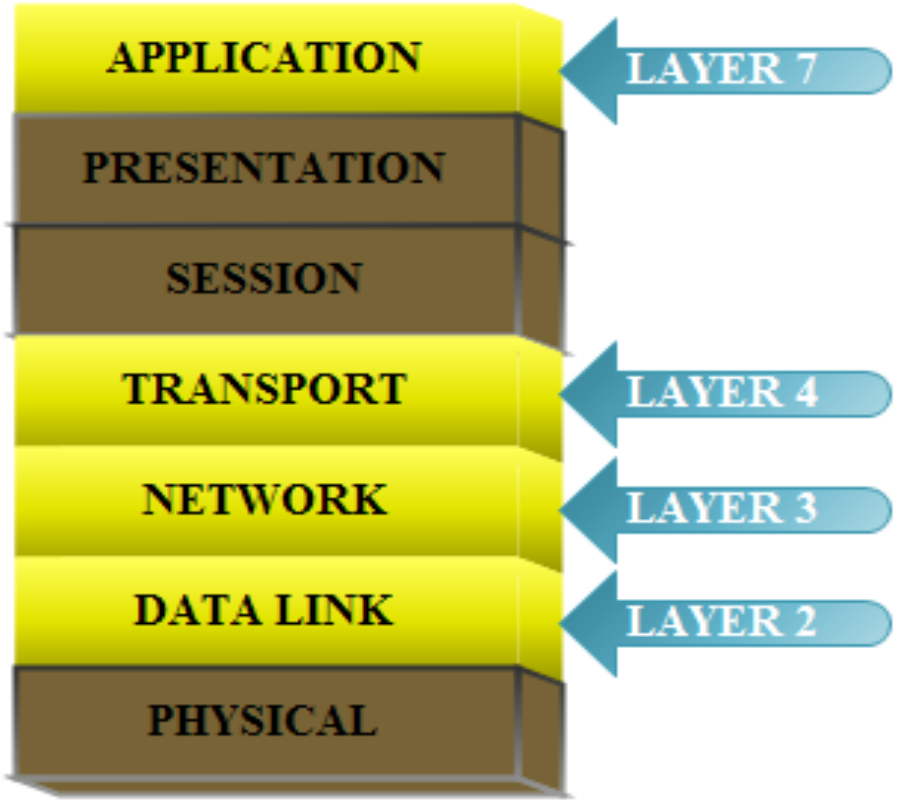
- Tường lửa là gì?
- **Phân loại tường lửa?**
- Tính năng của tường lửa thế hệ mới?
- Mô hình triển khai tường lửa

Phân loại tường lửa

- 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

- 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

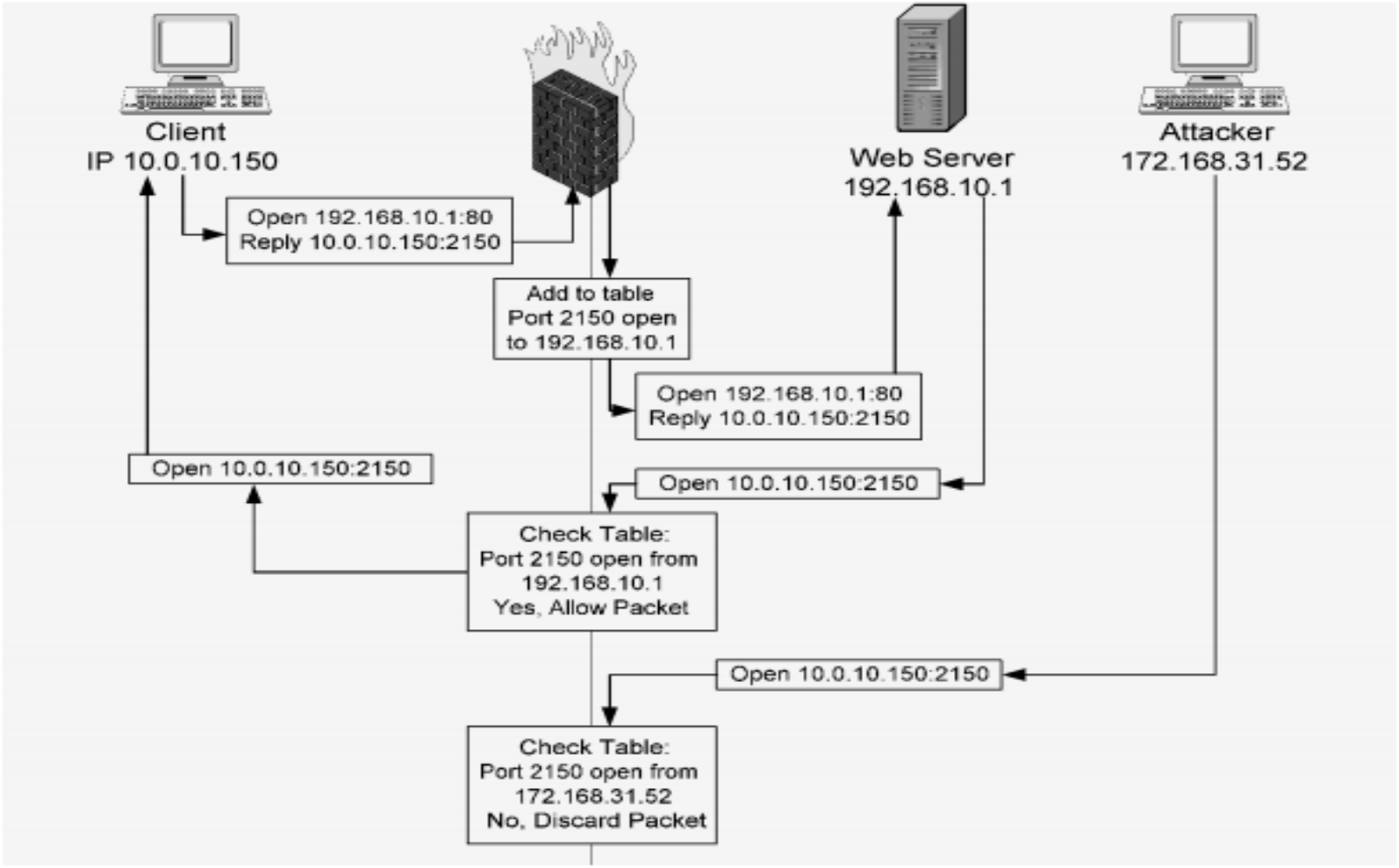
- **Simple Packet Filter Firewalls**
  - Kiểm tra gói tin qua firewall bằng cách so sánh nó với những nguyên tắc (Rule) đã được đặt ra, để quyết định gói tin đó được cho phép hay bị từ chối.
  - Những thông tin sẽ được kiểm tra :
    - IP Nguồn
    - IP Đích
    - Giao thức
    - Port Nguồn
    - Port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

Phân loại tường lửa

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

Phân loại tường lửa

- **Stateful Packet Filter Firewalls**



Phân loại tường lửa

- **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 tạm 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 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

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

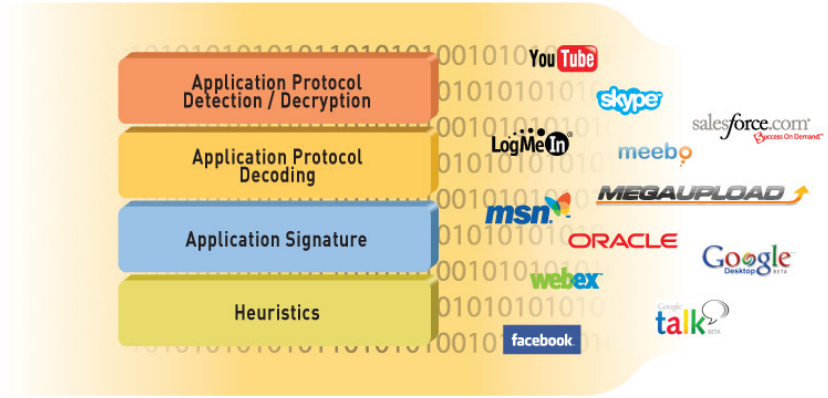
Next-Generation Firewall

New Requirements for the Firewall

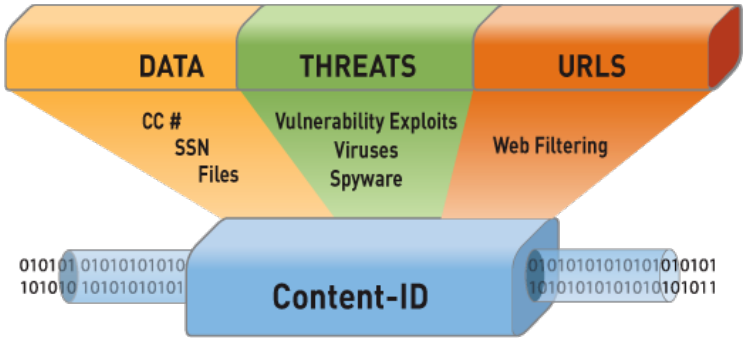
1. Identify applications regardless of port, protocol, evasive tactic or SSL
2. Identify users regardless of IP address
3. Granular visibility and policy control over application access / functionality
4. Protect in real-time against threats embedded across applications
5. Multi-gigabit, in-line deployment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

NG Firewall' Technology

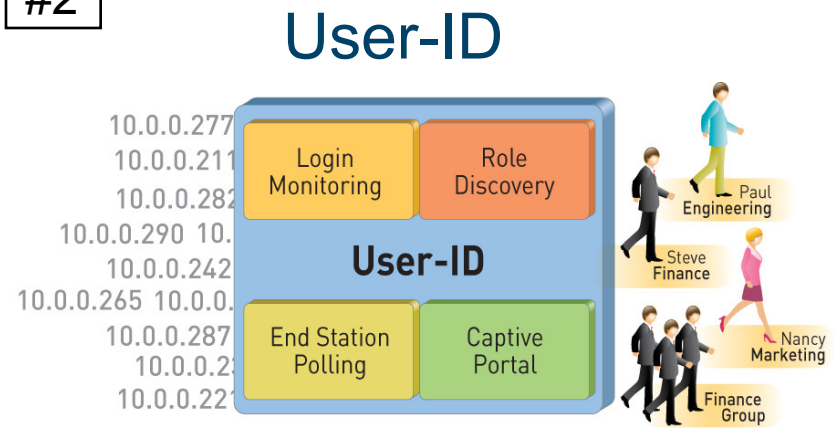
#1



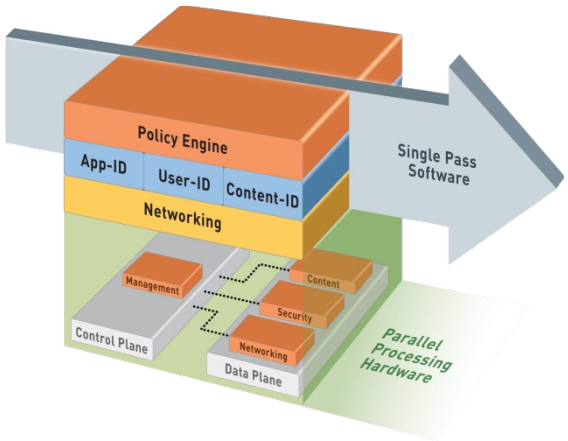
#3



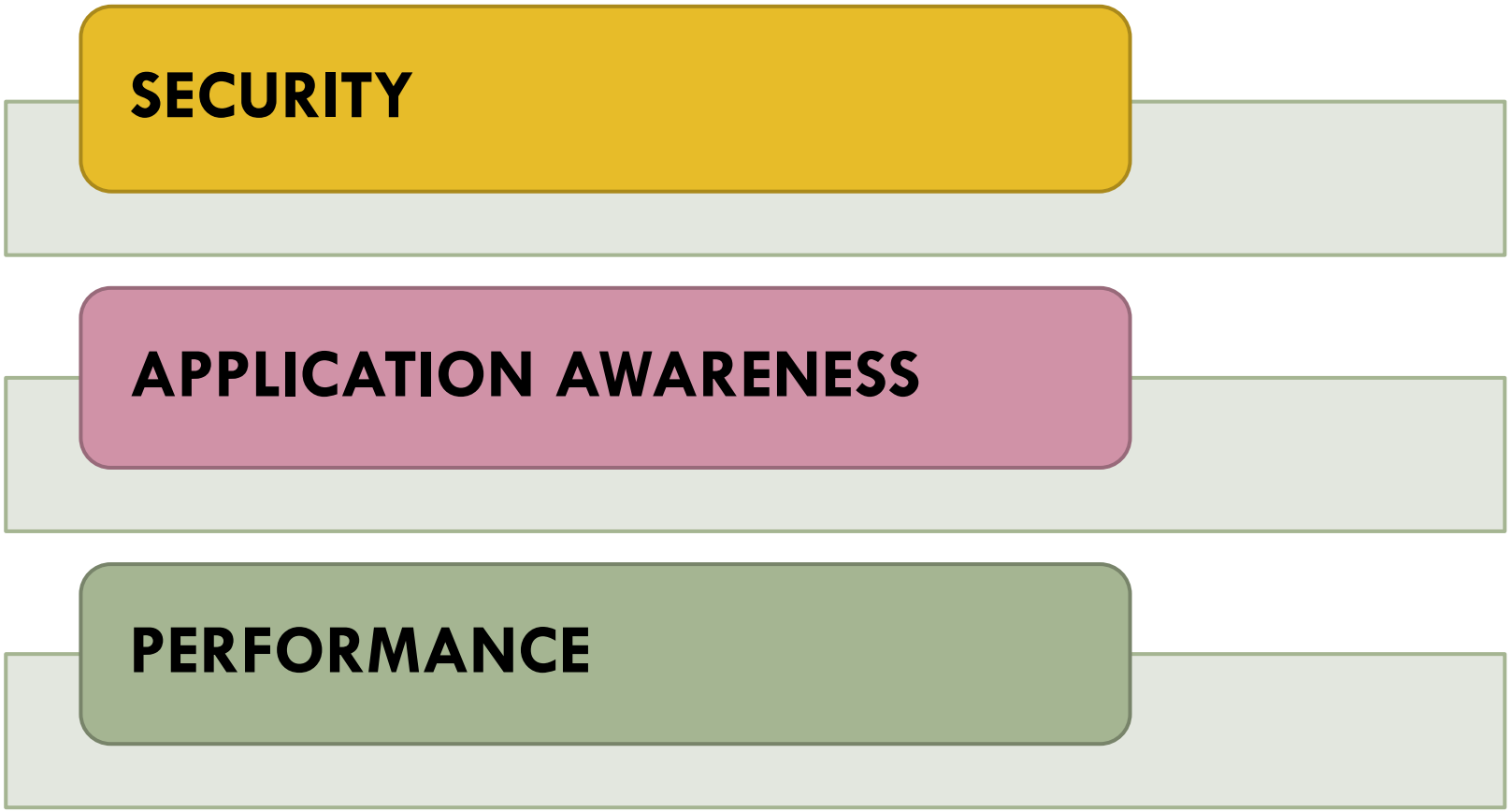
#2



#4



Next Generation Firewall



Next Generation Firewall

SECURITY

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

Stateful Packet Inspection

Stateful is limited inspection that can only block on ports

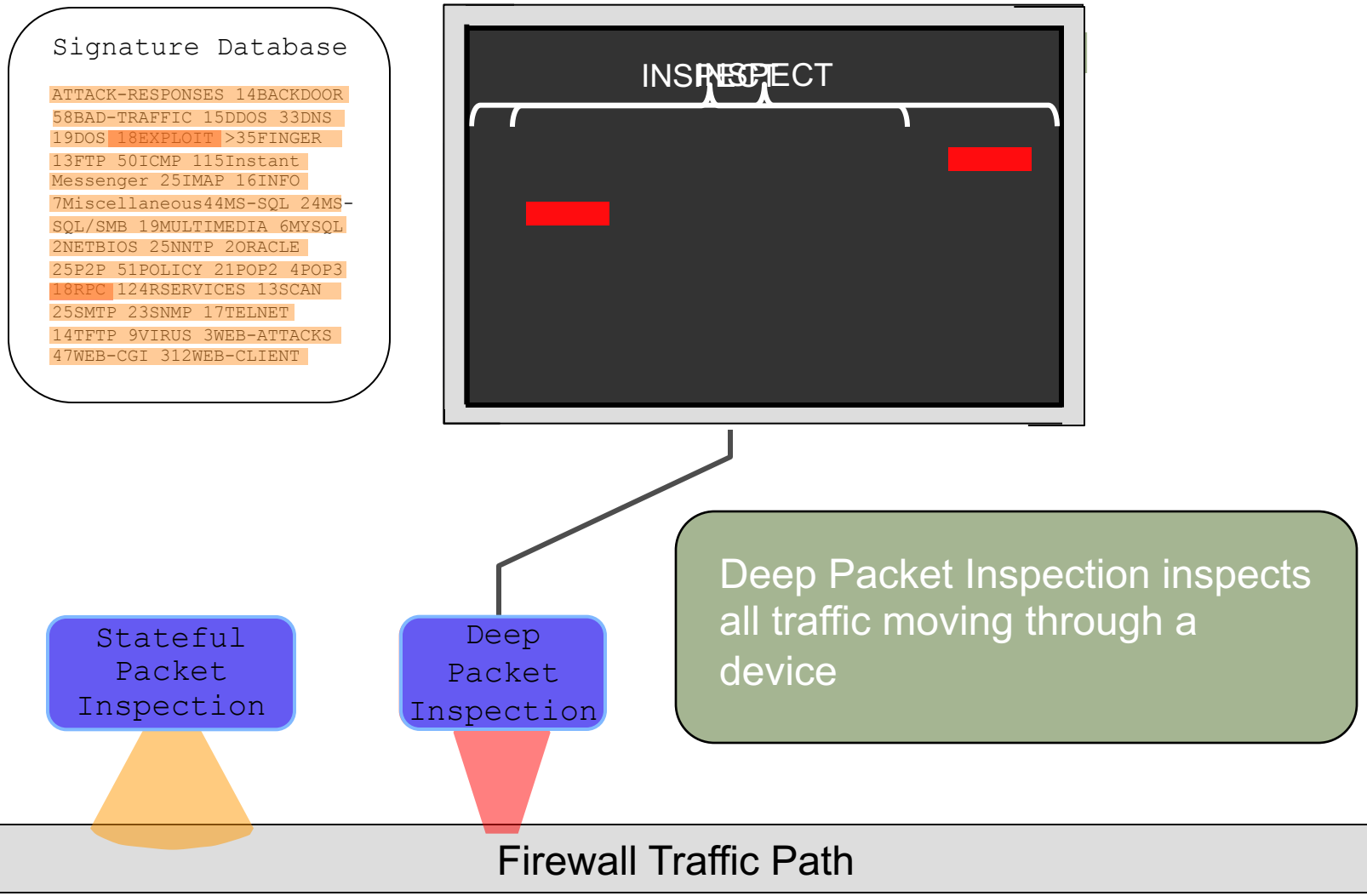
No Data Inspection!

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

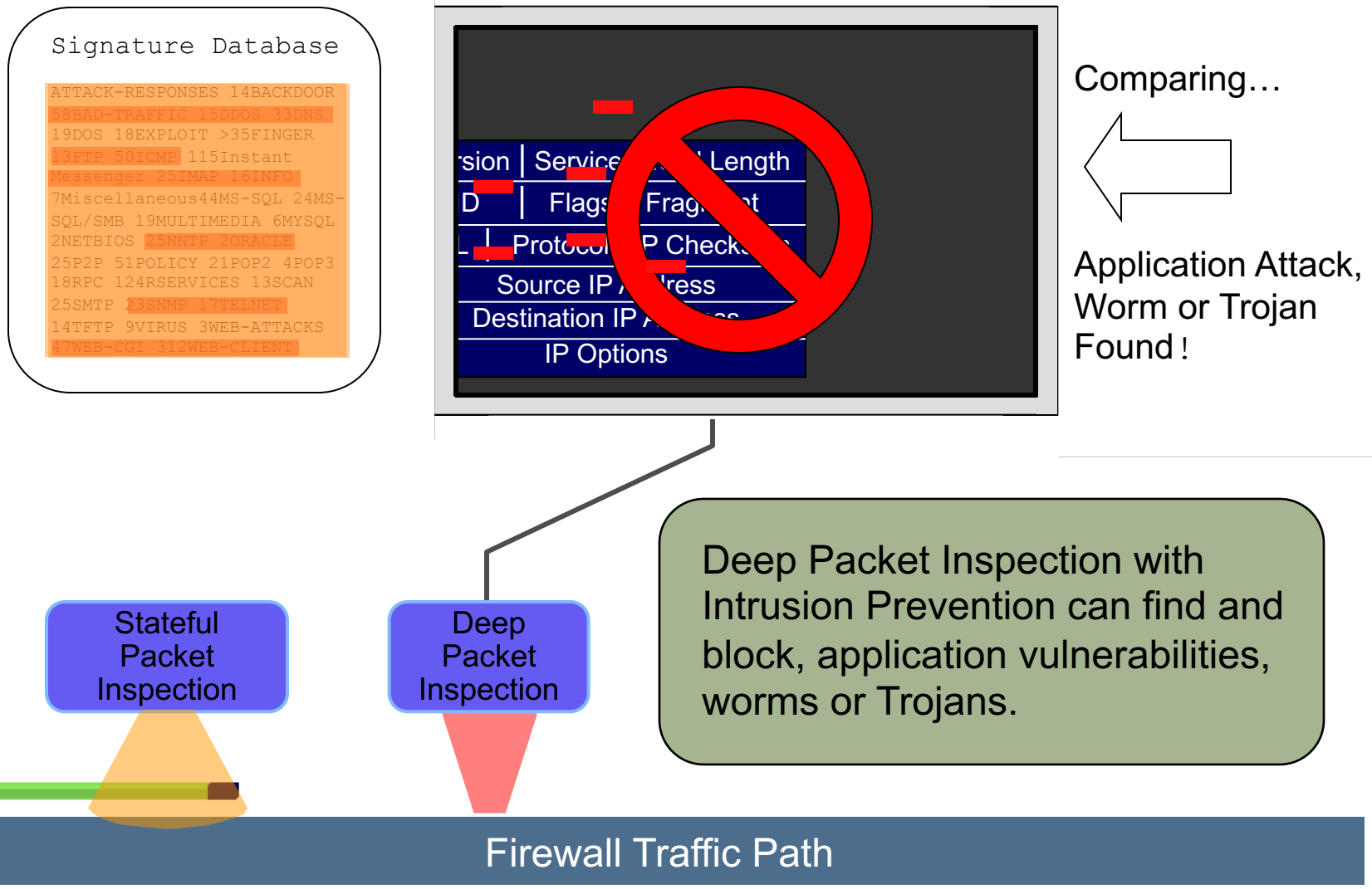
Stateful Packet Inspection

Firewall Traffic Path

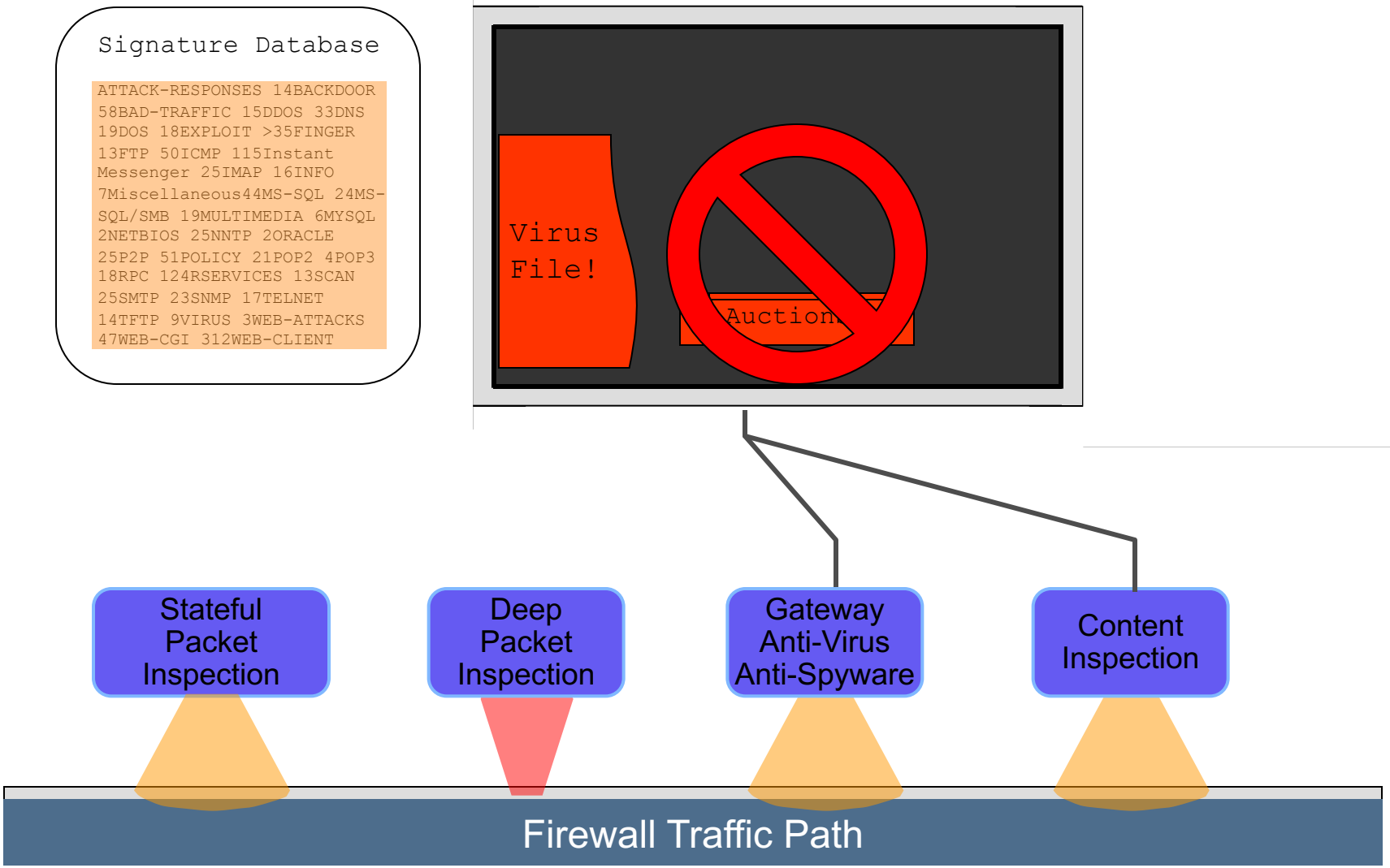
Deep Packet Inspection



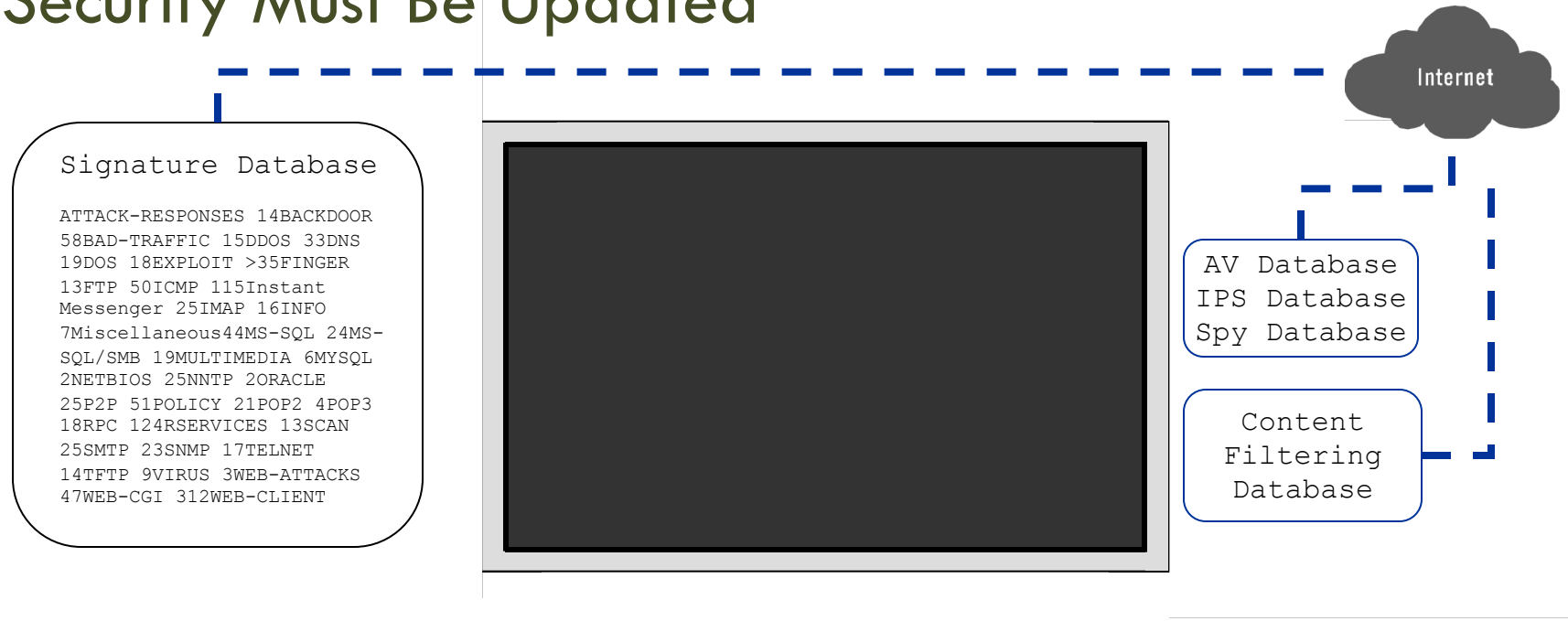
Deep Packet Inspection / Prevention

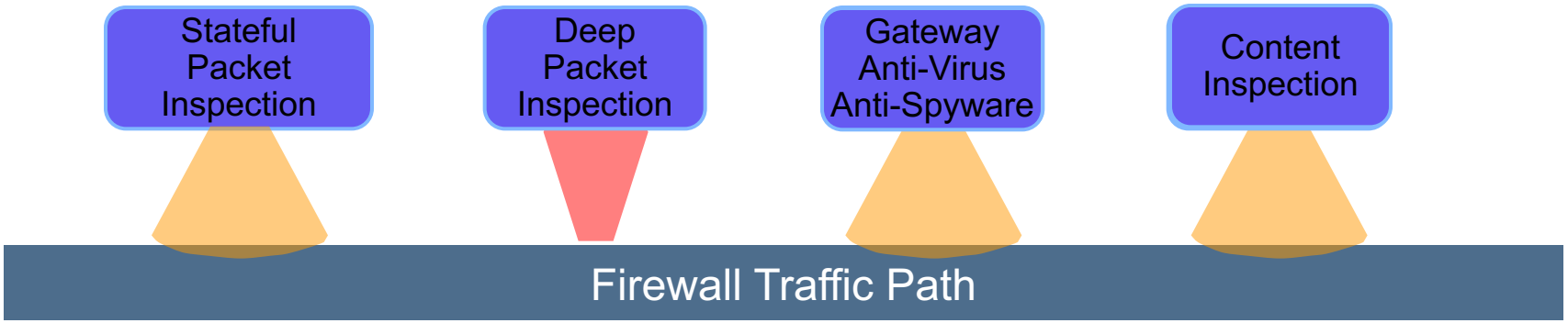


Gateway Anti-Virus and Content Control



Security Must Be Updated





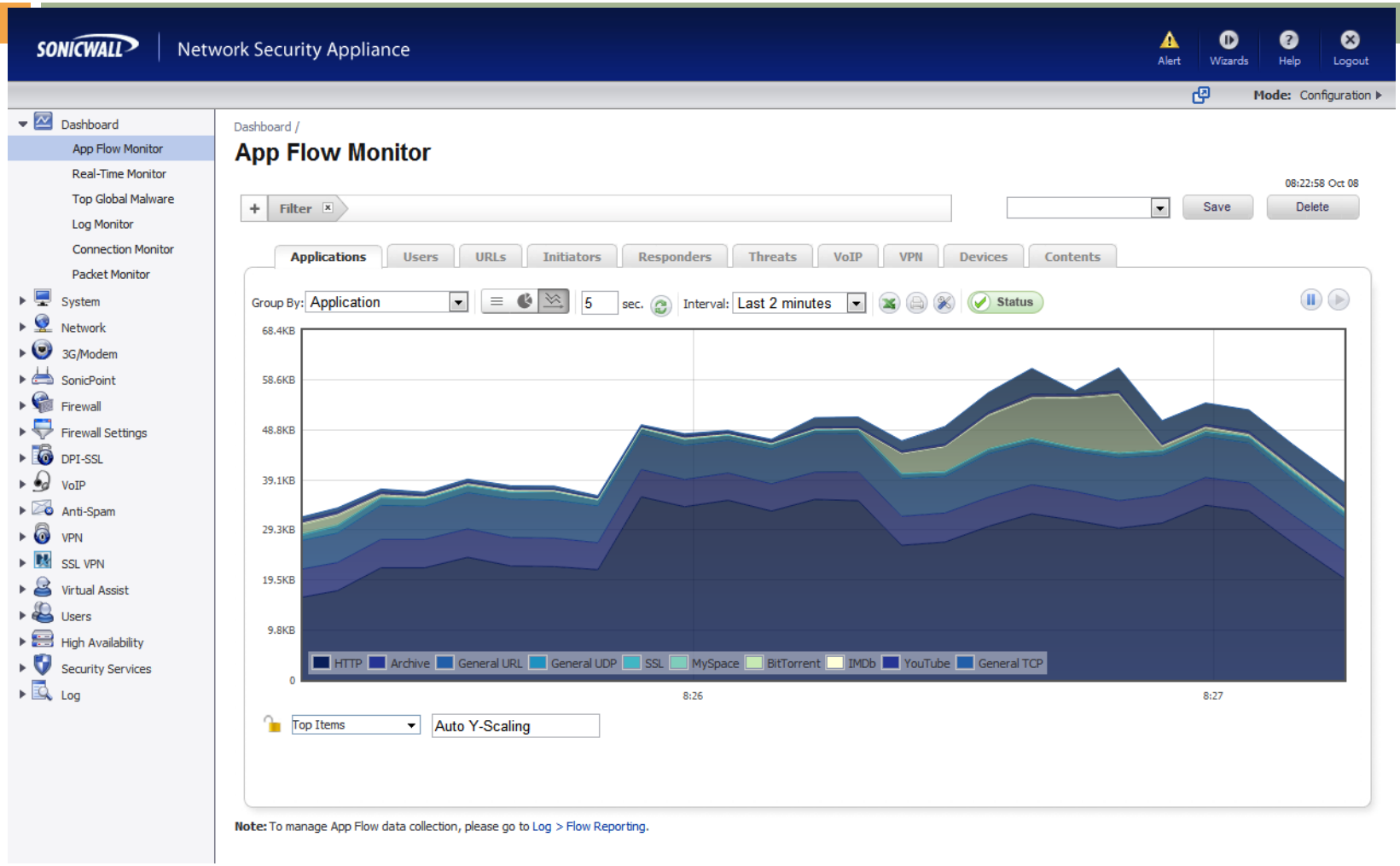
Next Generation Firewall

SECURITY

APPLICATION AWARENESS

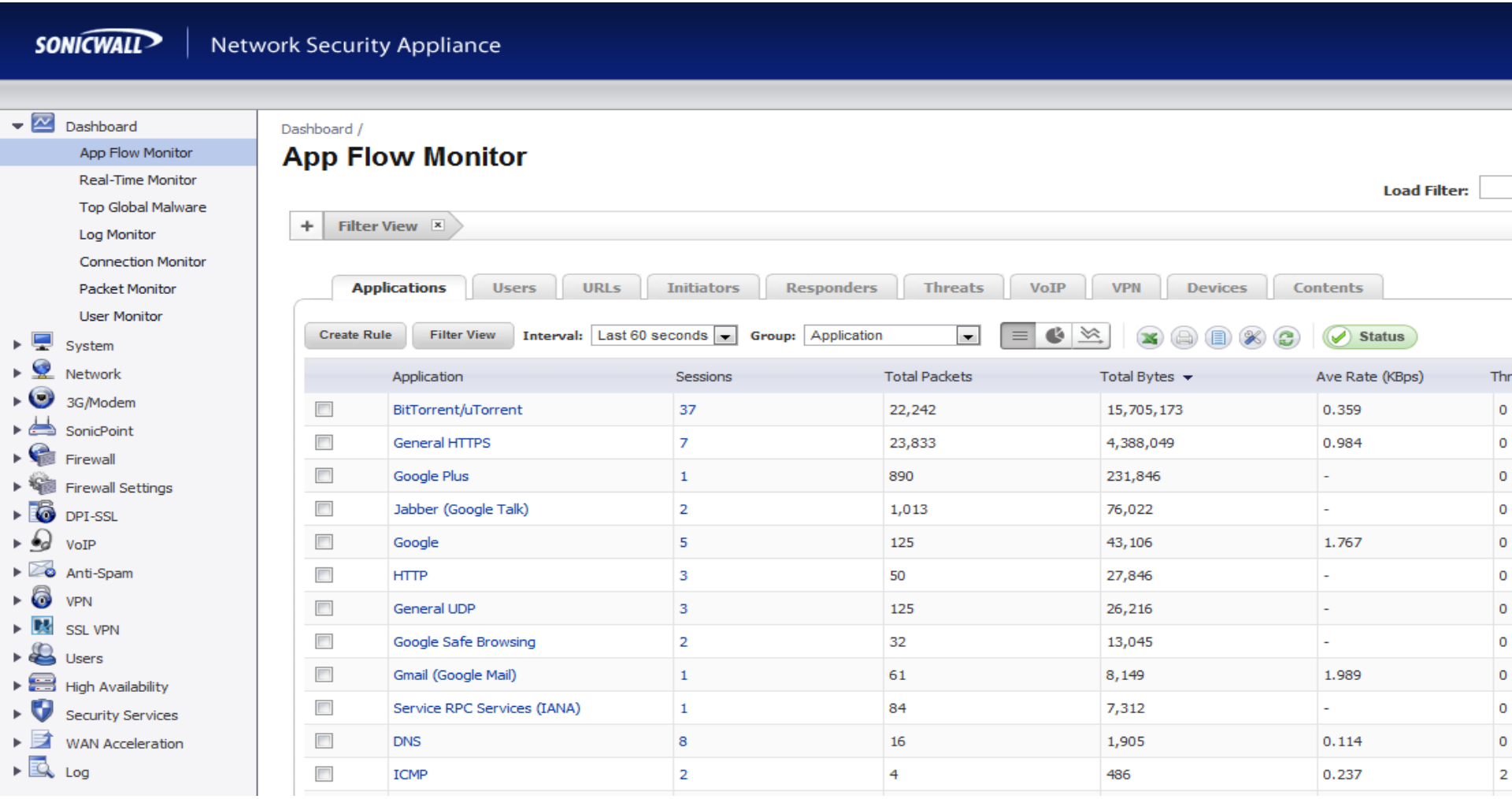
- **FINGERPRINT APPLICATIONS**
- **IDENTIFY USERS**
- **VISUALIZE TRAFFIC**

Application Traffic Visualization



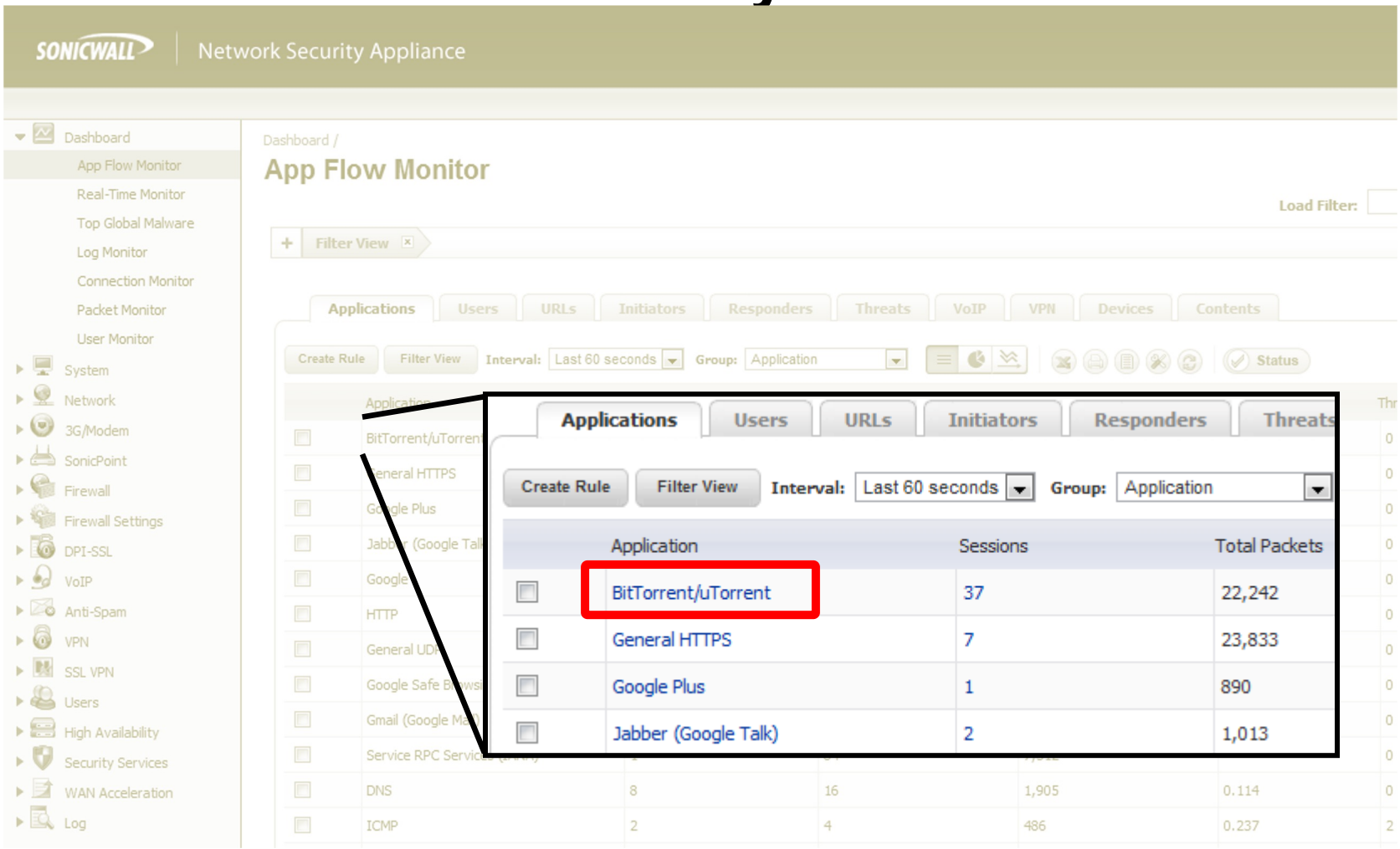
Network Analysis Tools

Do I have P2P on my Network?



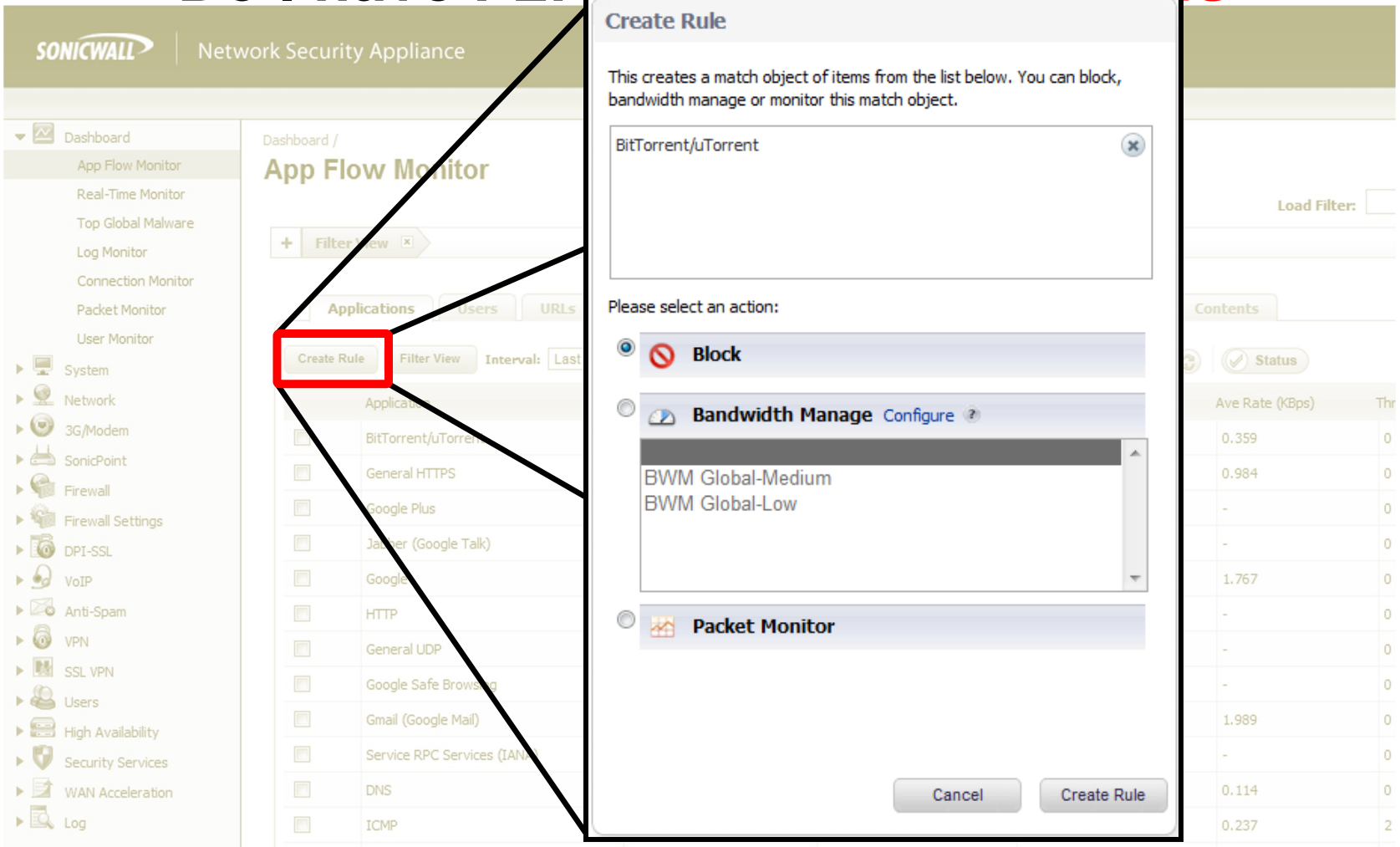
Network Analysis Tools

Do I have P2P on my Network? YES



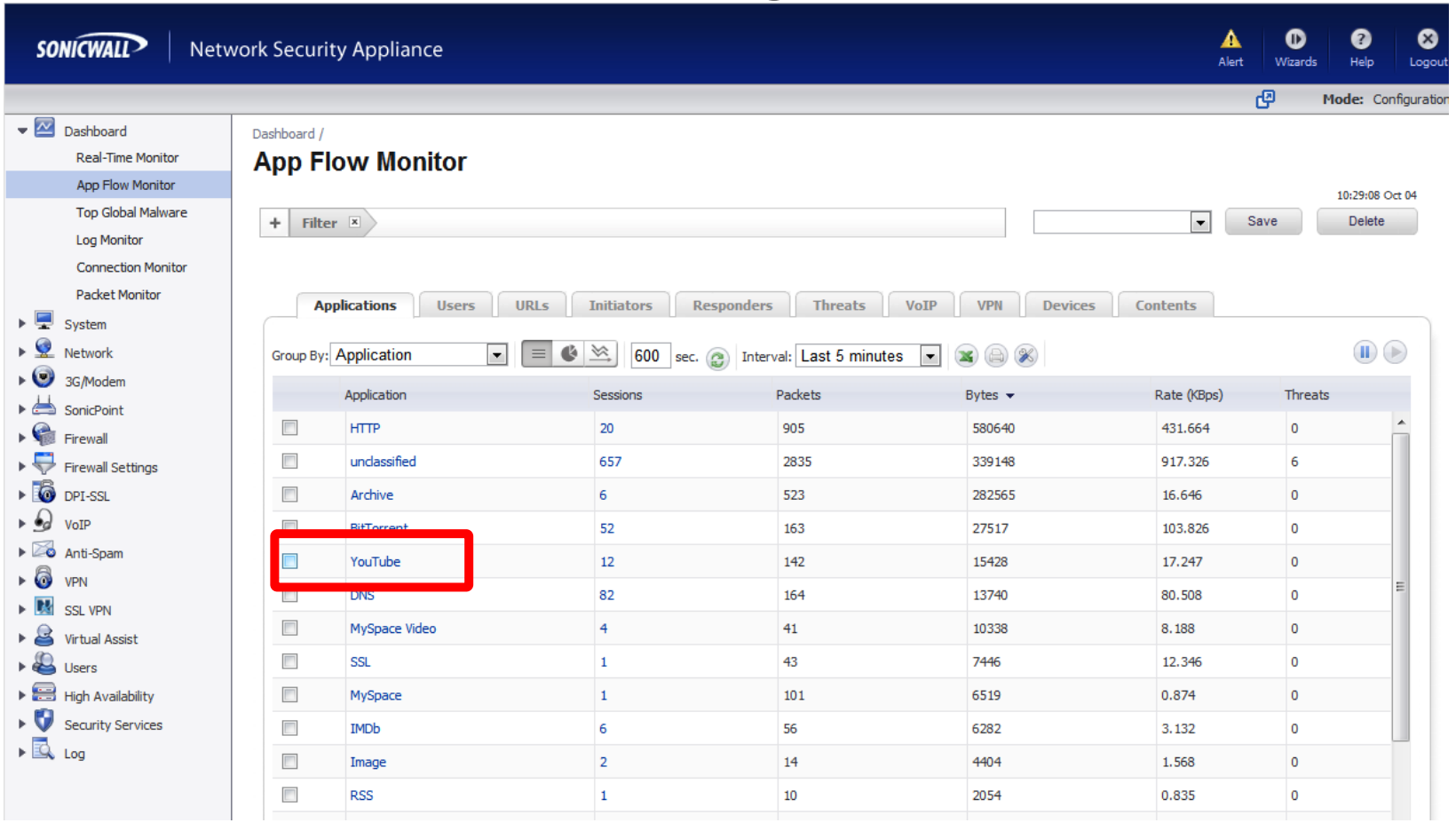
Immediate Application Control

Do I have P2P on my Network? YES



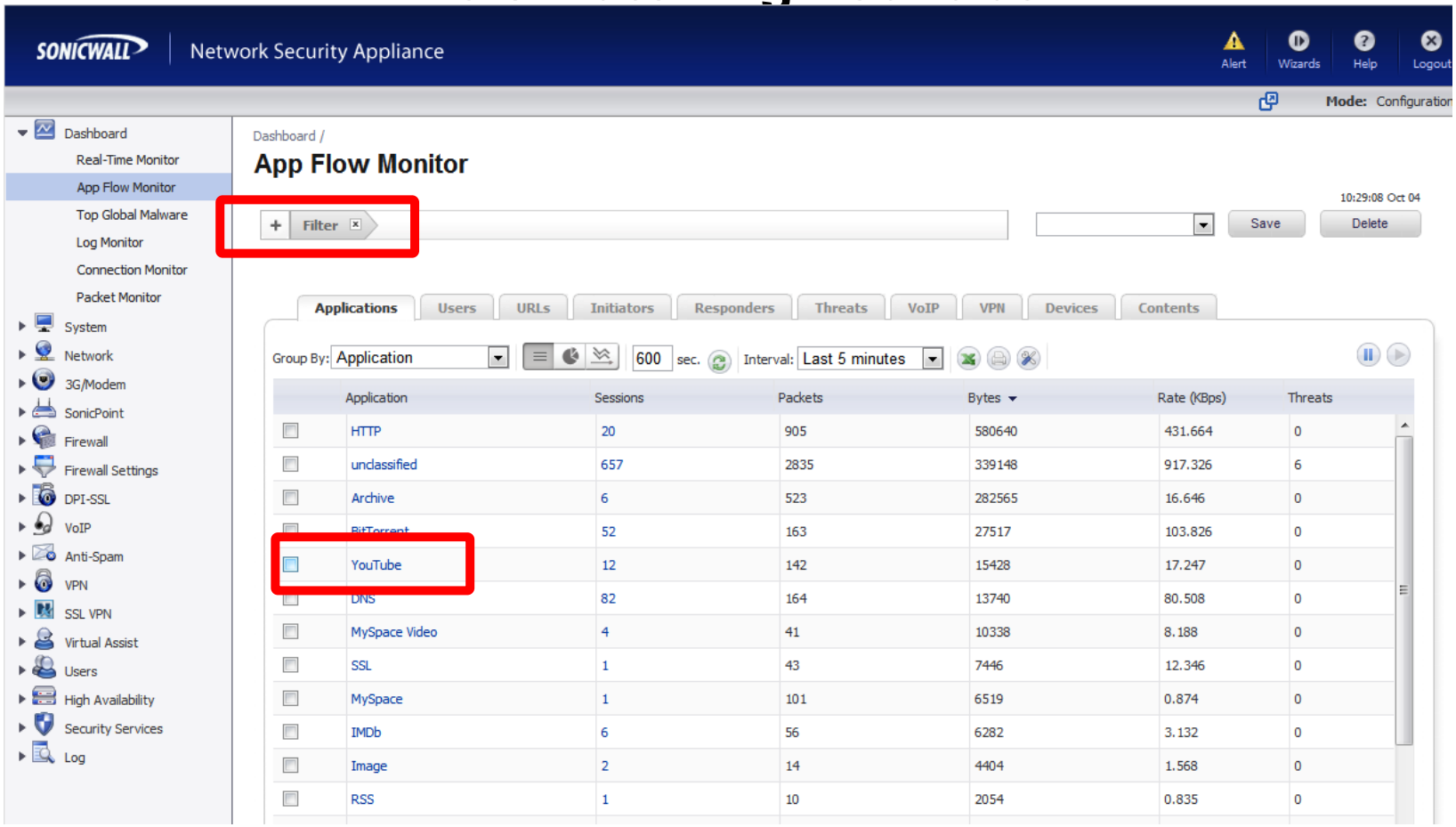
Network Analysis Tools

“Who’s watching YouTube?”



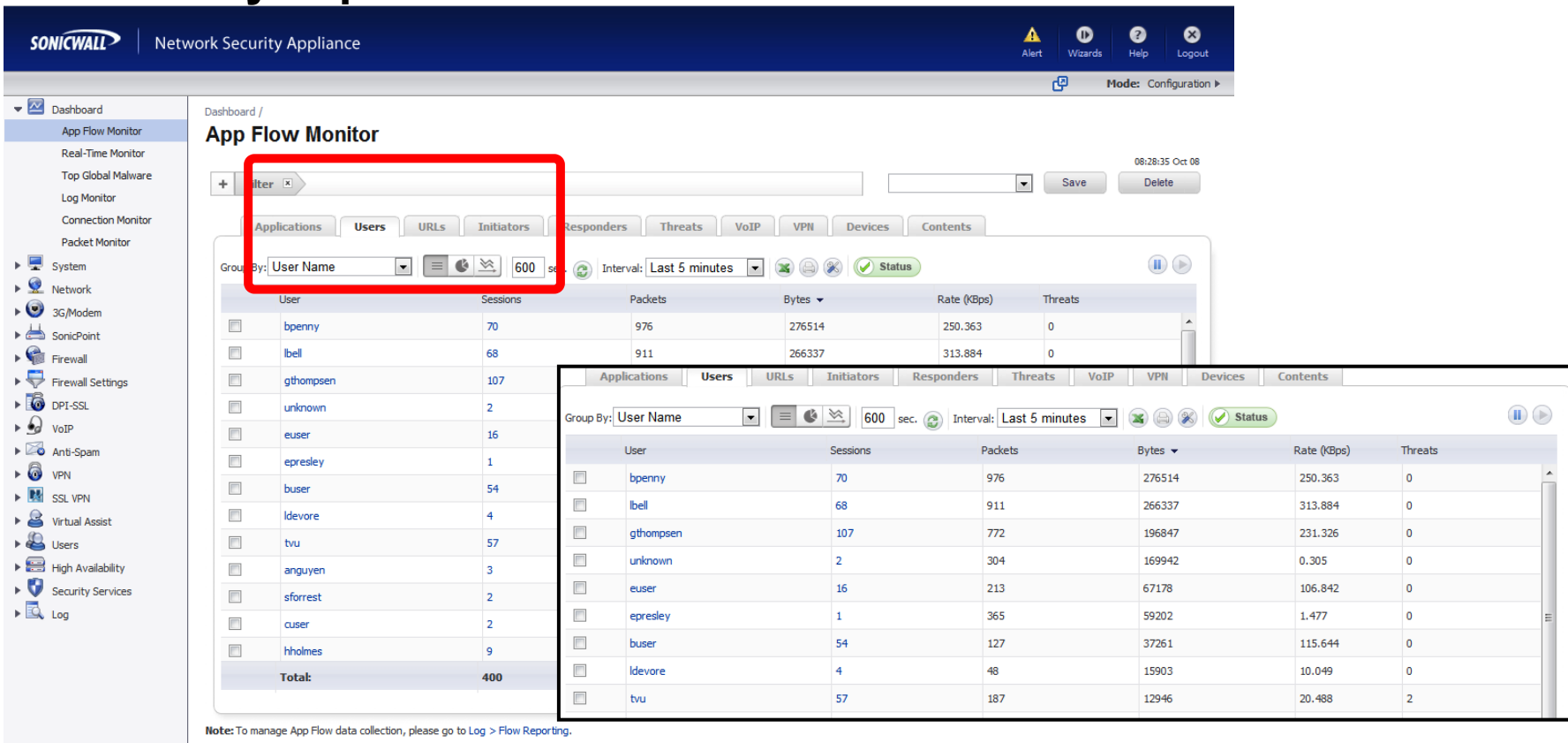
Network Analysis Tools

“Who’s watching YouTube?”

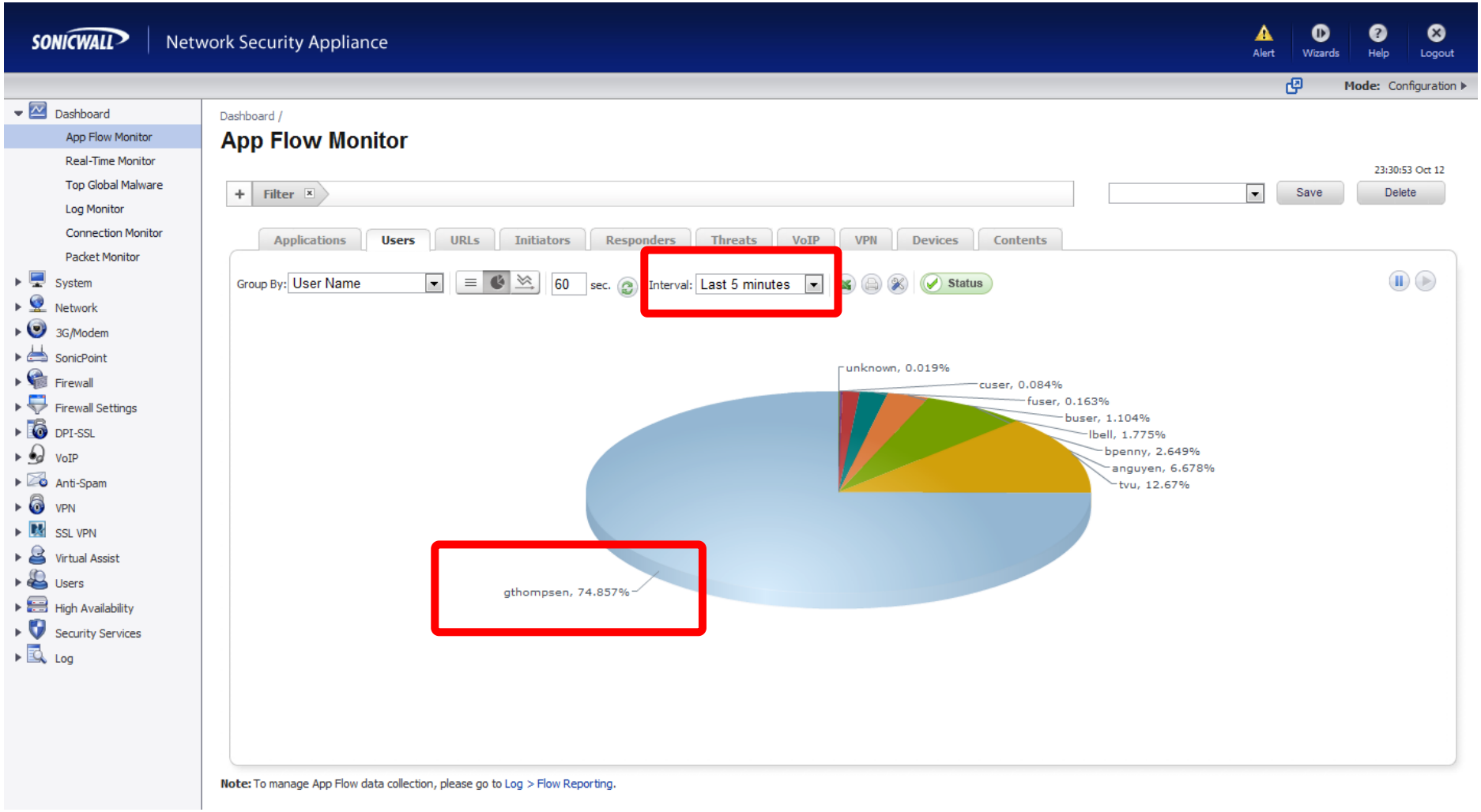


User Identification

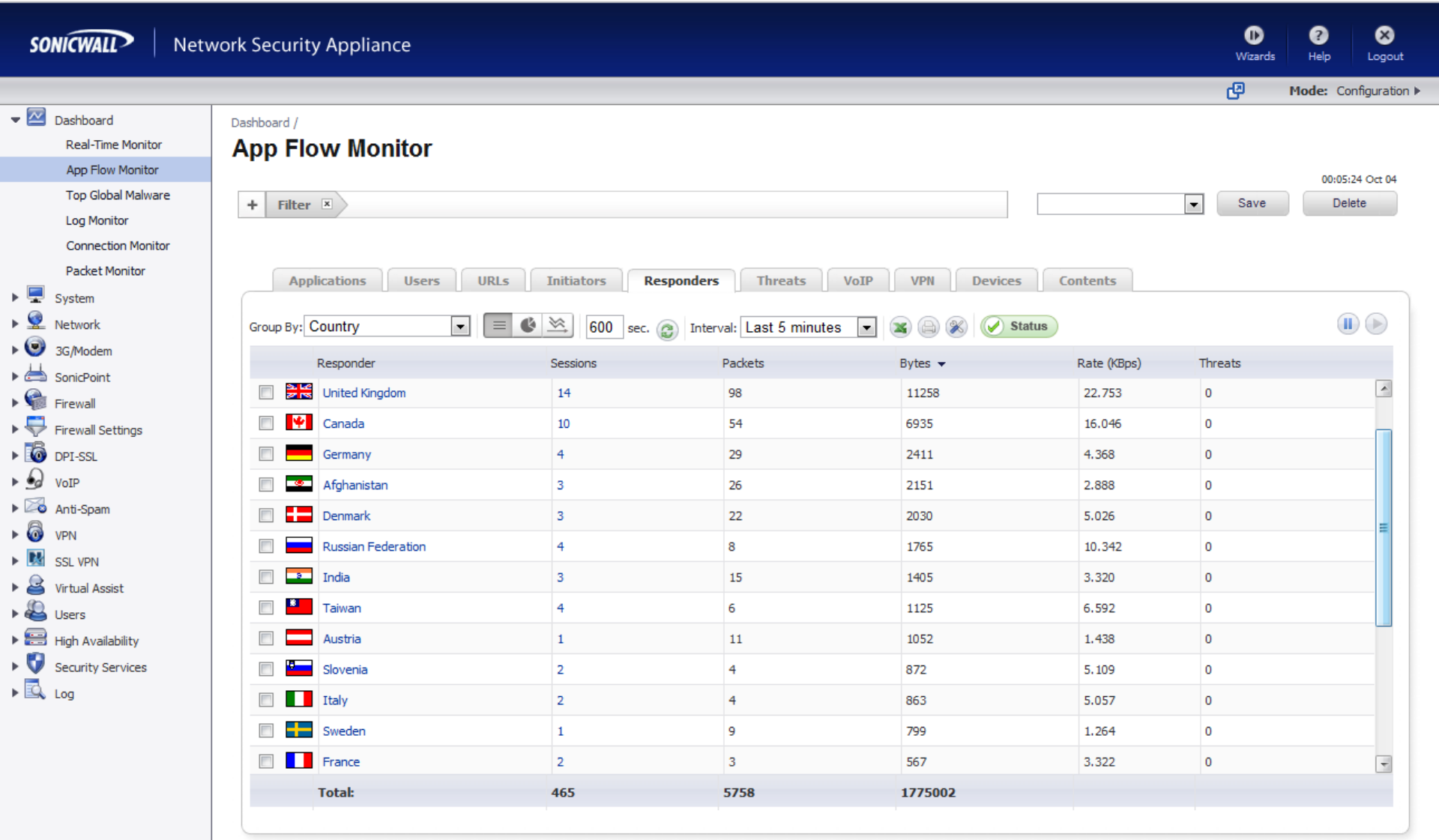
- **Single Sign On (AD/LDAP Integration)**
- **Local Login**
- **Identify Top Bandwidth users**



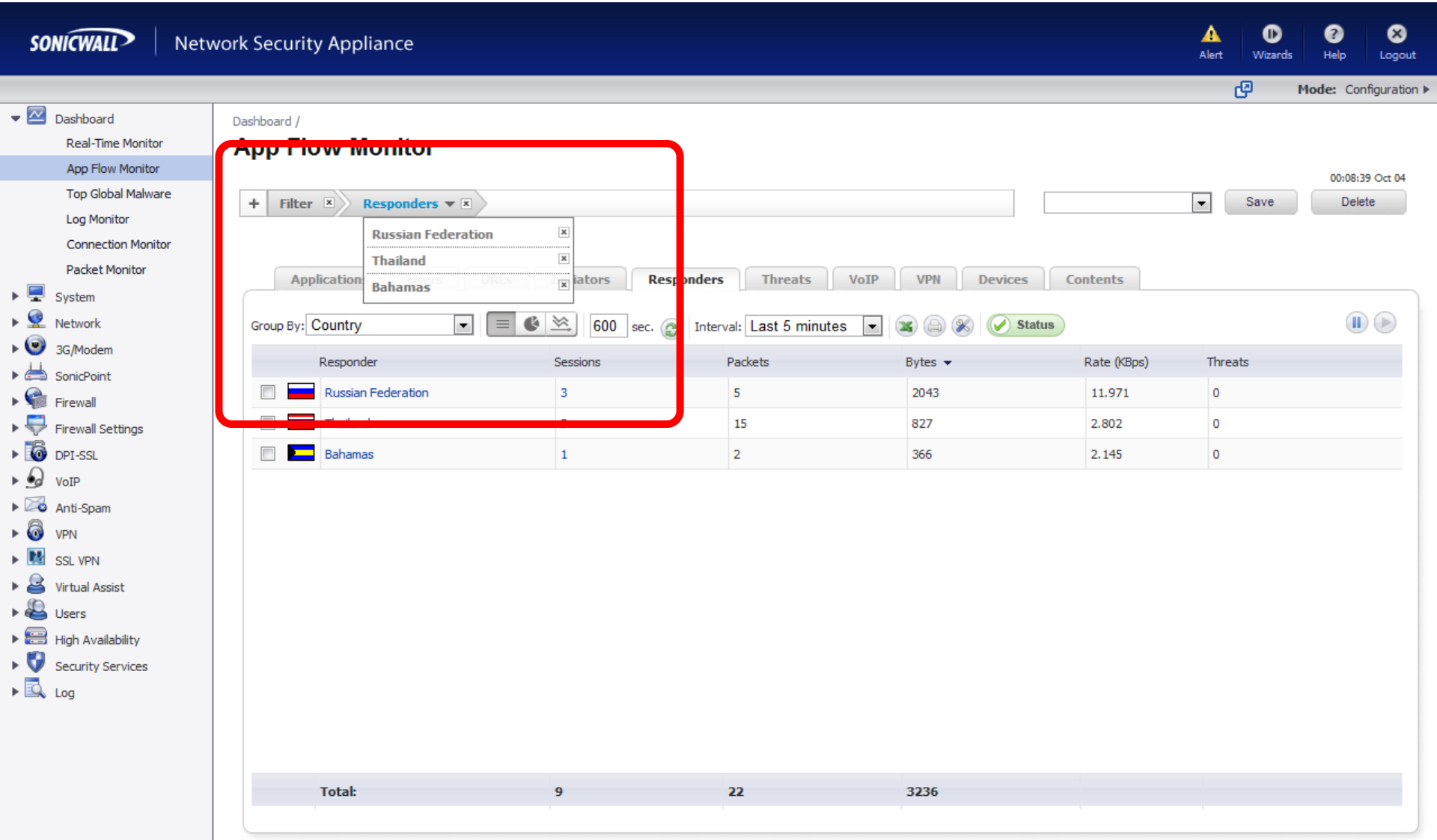
Identify Top Bandwidth Users



Connection Tracking by Country



Trace & Identify Network Connections



Next Generation Firewall

SECURITY

APPLICATION AWARENESS

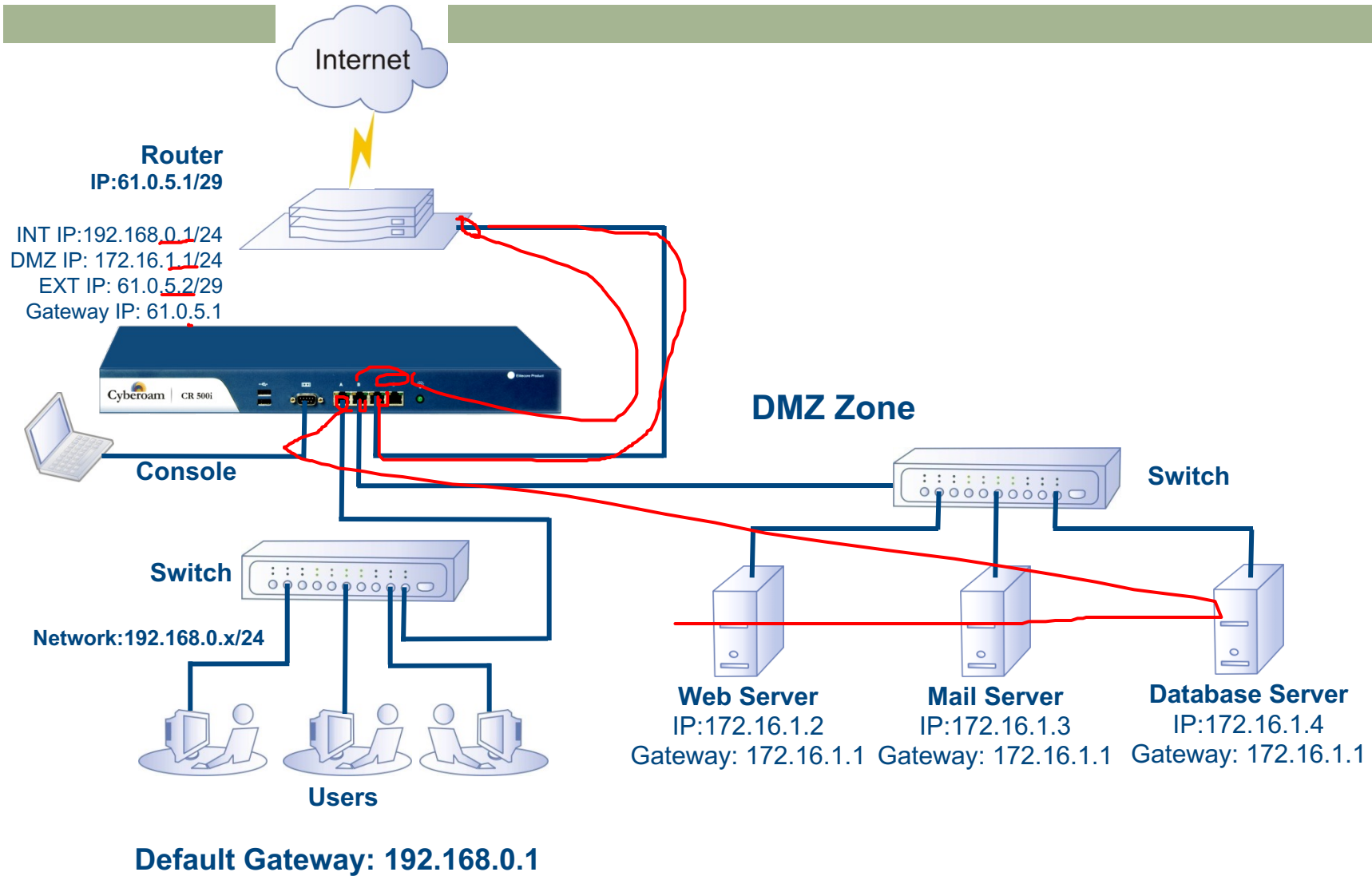
PERFORMANCE

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

Nội dung

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

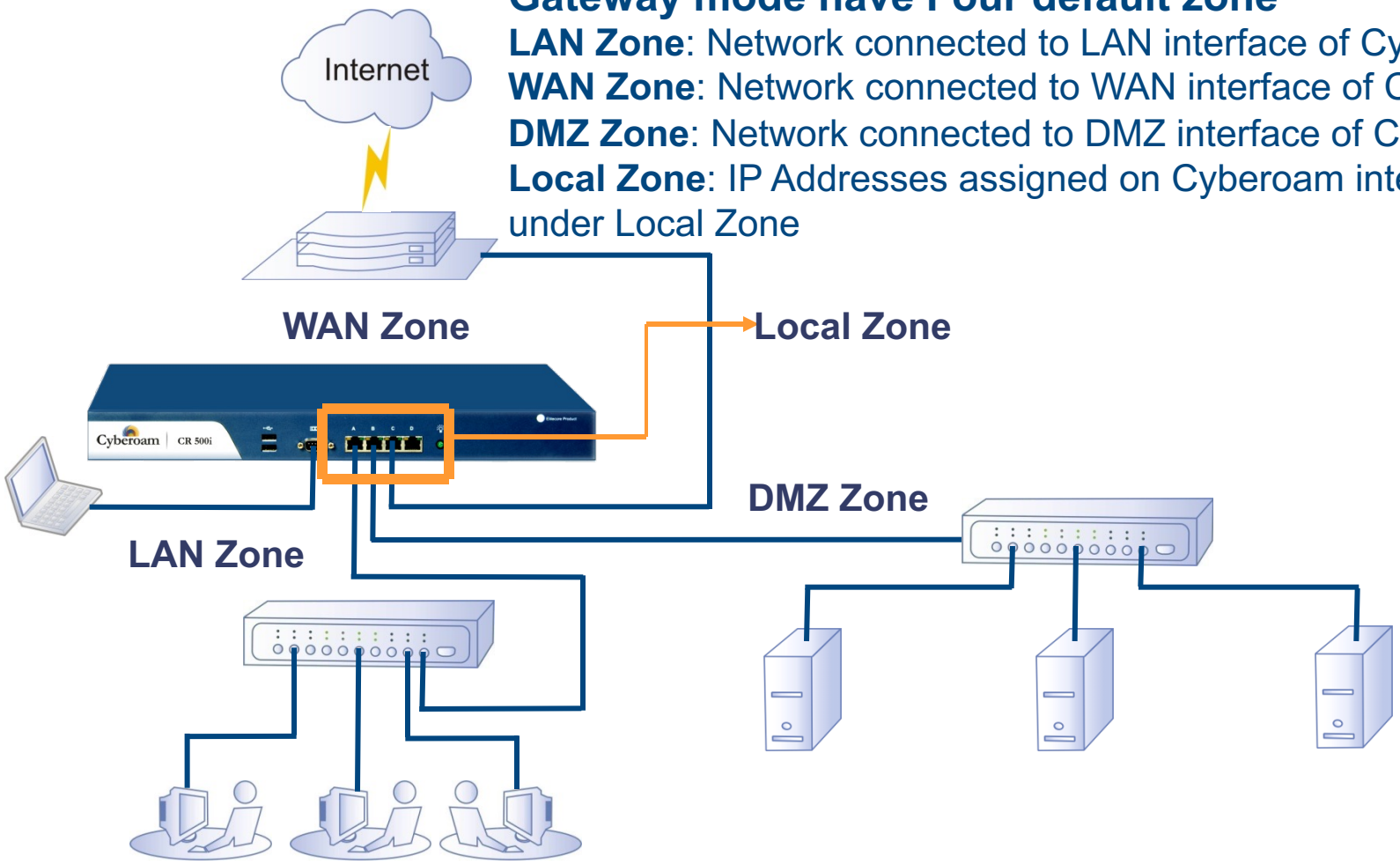
Cyberoam in Gateway Mode



Zone information when Cyberoam is in Gateway mode

Gateway mode have Four default zone

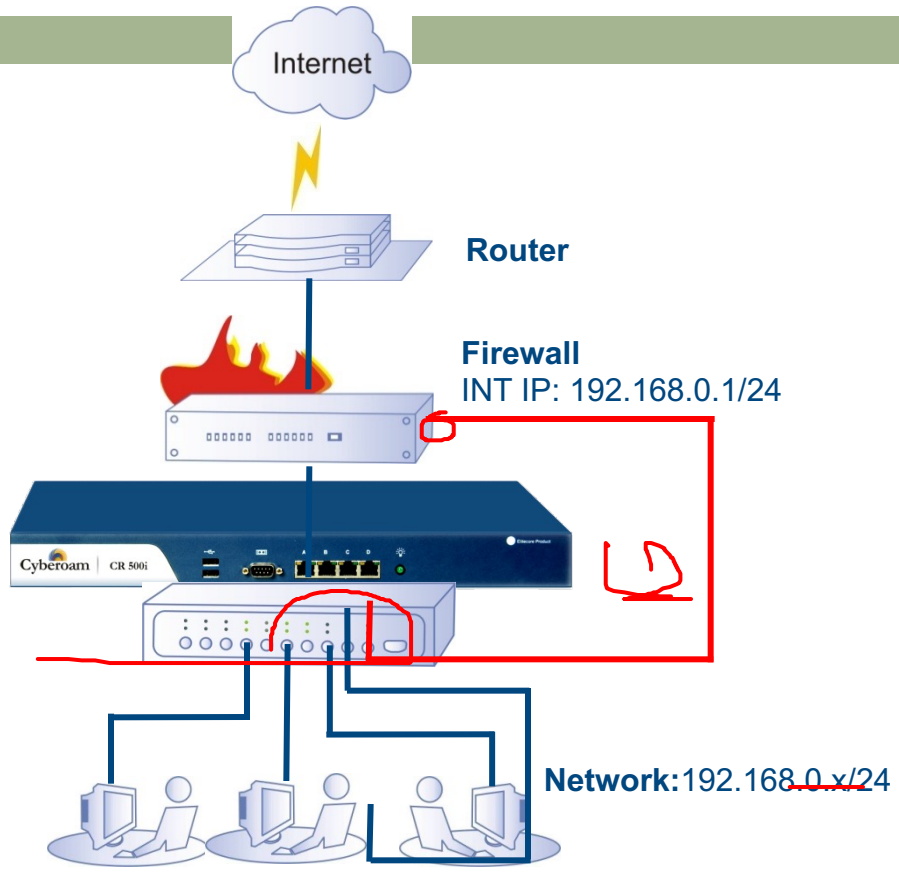
LAN Zone: Network connected to LAN interface of Cyberoam
WAN Zone: Network connected to WAN interface of Cyberoam
DMZ Zone: Network connected to DMZ interface of Cyberoam
Local Zone: IP Addresses assigned on Cyberoam interfaces falls under Local Zone



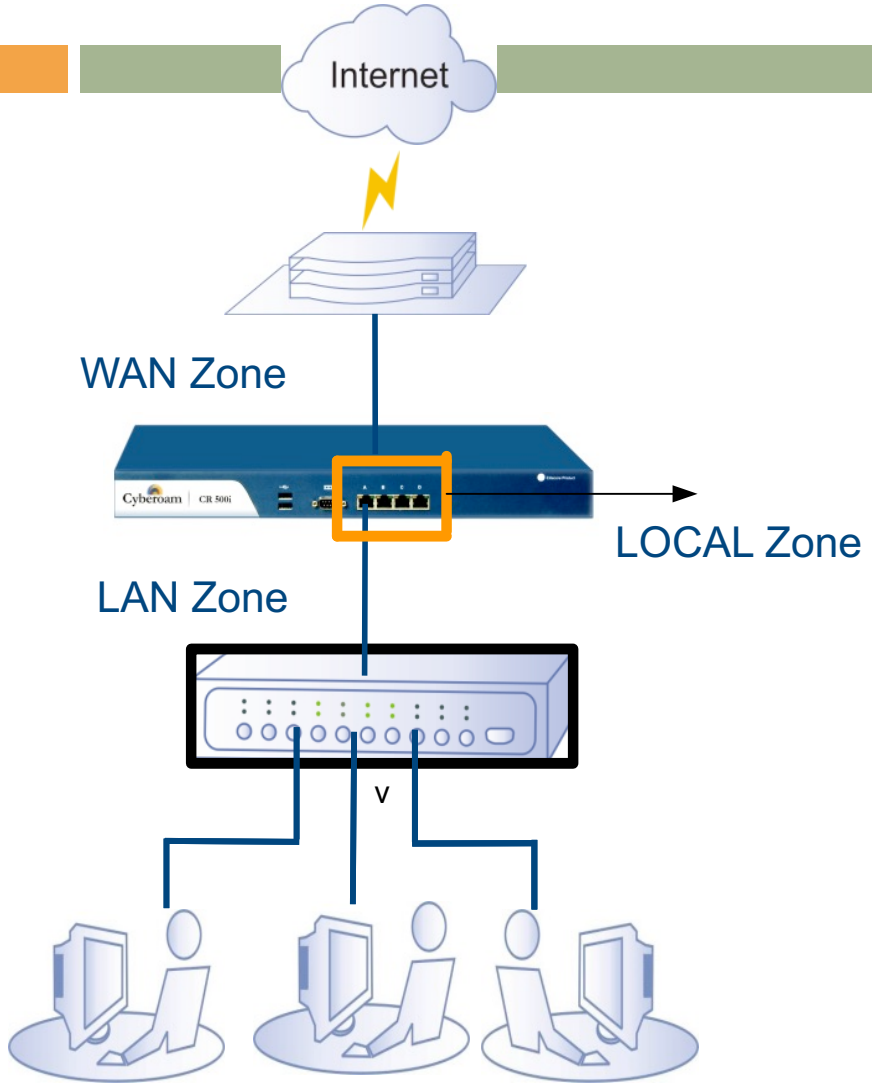
Cyberoam in Bridge Mode

Bridge IP Address	192.168. 0 . 5
Subnet Mask	255.255.255. 0

IP address of the Default Gateway	192.168. 0 . 1
DNS IP Address	202. 54 . 1 . 30
System Time Zone	_____
System Date and Time	_____
Email ID of the administrator	_____



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

- 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 ???