



Kyle Walsh,  
Sales Engineer Canadian  
Western Territory

**EPIC 2008**

**WatchGuard UTM Appliances  
and  
What's new in Fireware 10**

# Agenda

WatchGuard Product Families

Zero Day Protection

How WatchGuard Works

Unified Threat Management

What's New In Fireware Release 10

Live Demo

Questions



# WatchGuard Product Families

## Firebox X® e-Series Edge



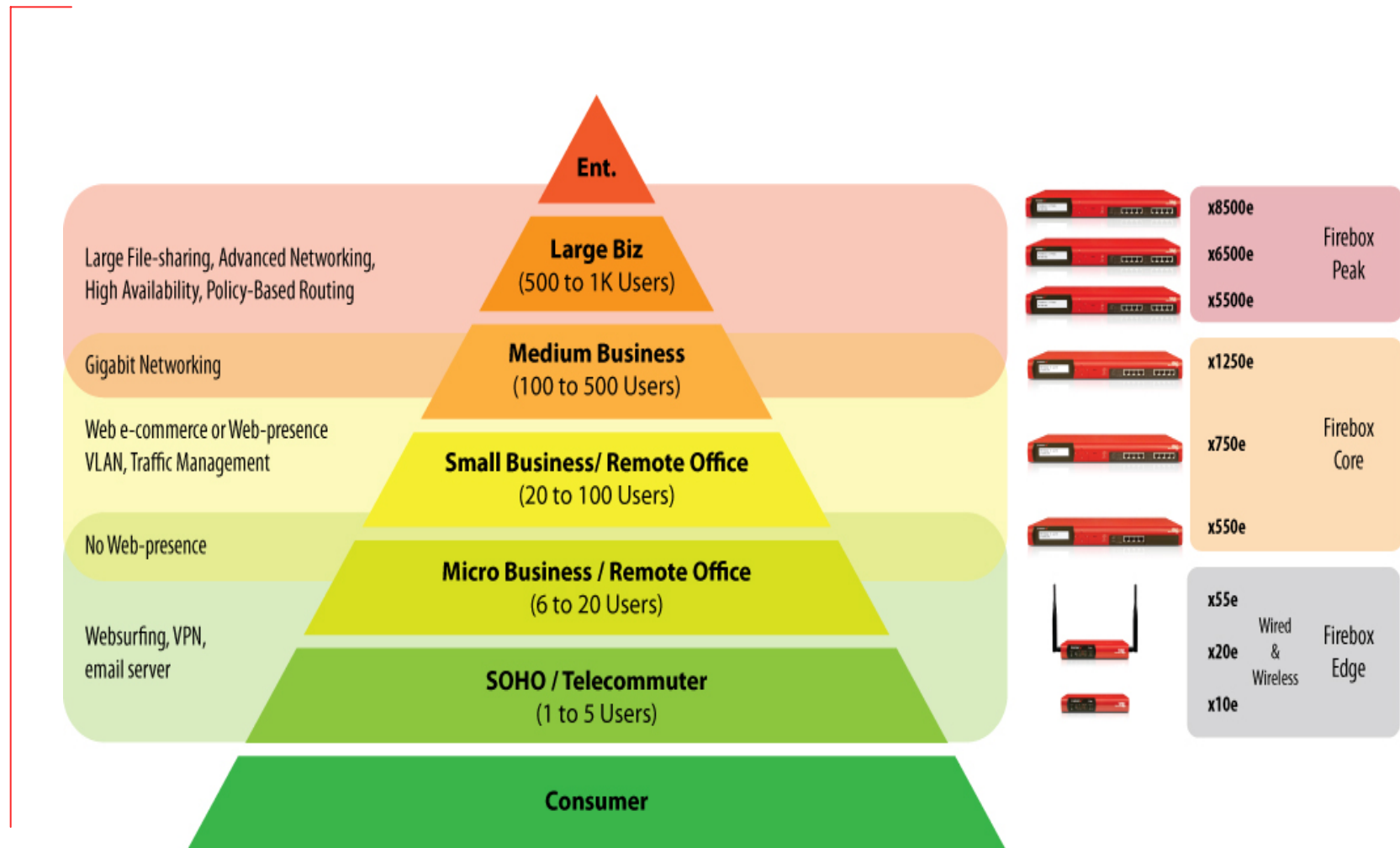
## Firebox X® e-Series Core



## Firebox X® e-Series Peak



# WatchGuard Product Families



## Fireware vs. Fireware Pro

| Feature                           | Fireware | Fireware Pro |
|-----------------------------------|----------|--------------|
| VPN Failover                      | Yes      | Yes          |
| Port Independence                 | Yes      | Yes          |
| VOIP & Video Conf. Support        | Yes      | Yes          |
| Multi-WAN Failover                | Yes      | Yes          |
| Traffic Management/Prioritization | No       | Yes          |
| Multi-WAN Load Sharing            | No       | Yes          |
| Multi-WAN Load Balancing          | No       | Yes          |
| High Availability                 | No       | Yes          |
| Dynamic Routing – BGP, RIP, OSPF  | No       | Yes          |
| Policy Based Routing              | No       | Yes          |
| Quality of Service (QOS)          | No       | Yes          |
| VLAN Support                      | No       | Yes          |
| Server Load Balancing             | No       | Yes          |
| Supports Maximum SSL VPN Tunnels  | No       | Yes          |

## Other Advanced Features

Built in Centralized Management, Logging & Reporting

- Centralized Management
  - Drag and Drop VPN Tunnel Creation
  - Centralized Policy Management (Edges)
  - Centralized Firmware Updates (Edges)
  - Support for Dynamic assigned IP's for remote appliances
  
- Centralized Logging & Reporting
  - Backend SQL server for Log Storage
  - Reports generated on demand without Admin intervention



# Zero Day Protection

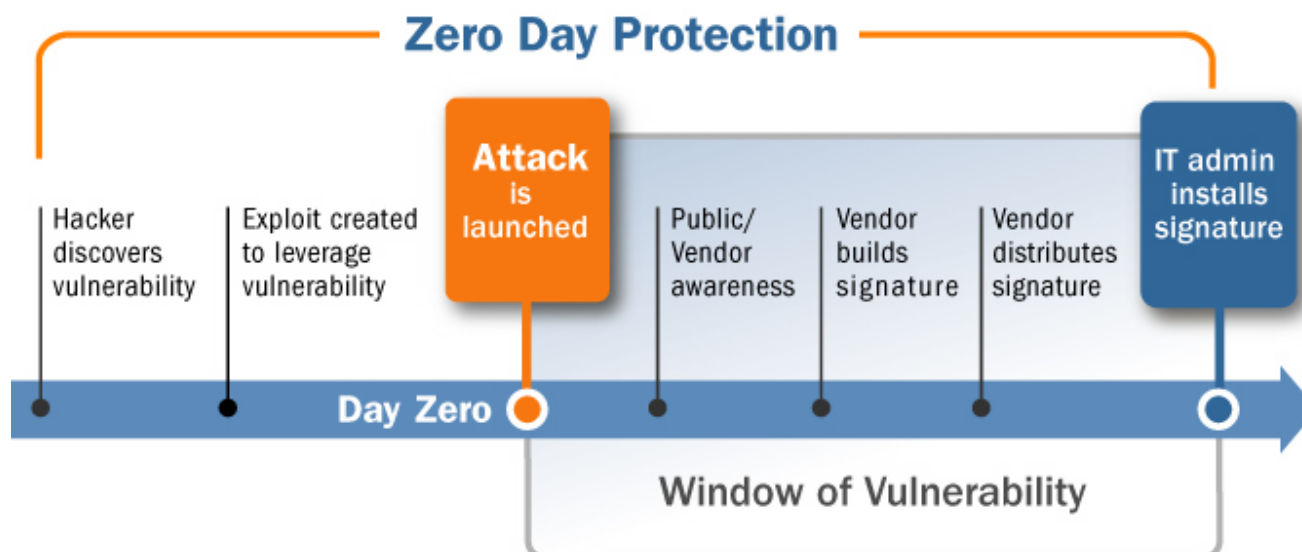
Since its inception in 1996 WatchGuard has been a  
Zero Day Protection Firewall

# Zero Day Protection

WatchGuard offers True Zero Day Protection right out of the box through its Intelligent Layered Security (ILS) architecture

Many vendors only provide signature-based protection, a reactive solution that leaves their customers exposed to threats until their signature is developed and deployed

WatchGuard protects against new and unknown threats before the vulnerability is discovered and the exploit is created and launched



## How does WatchGuard do this?

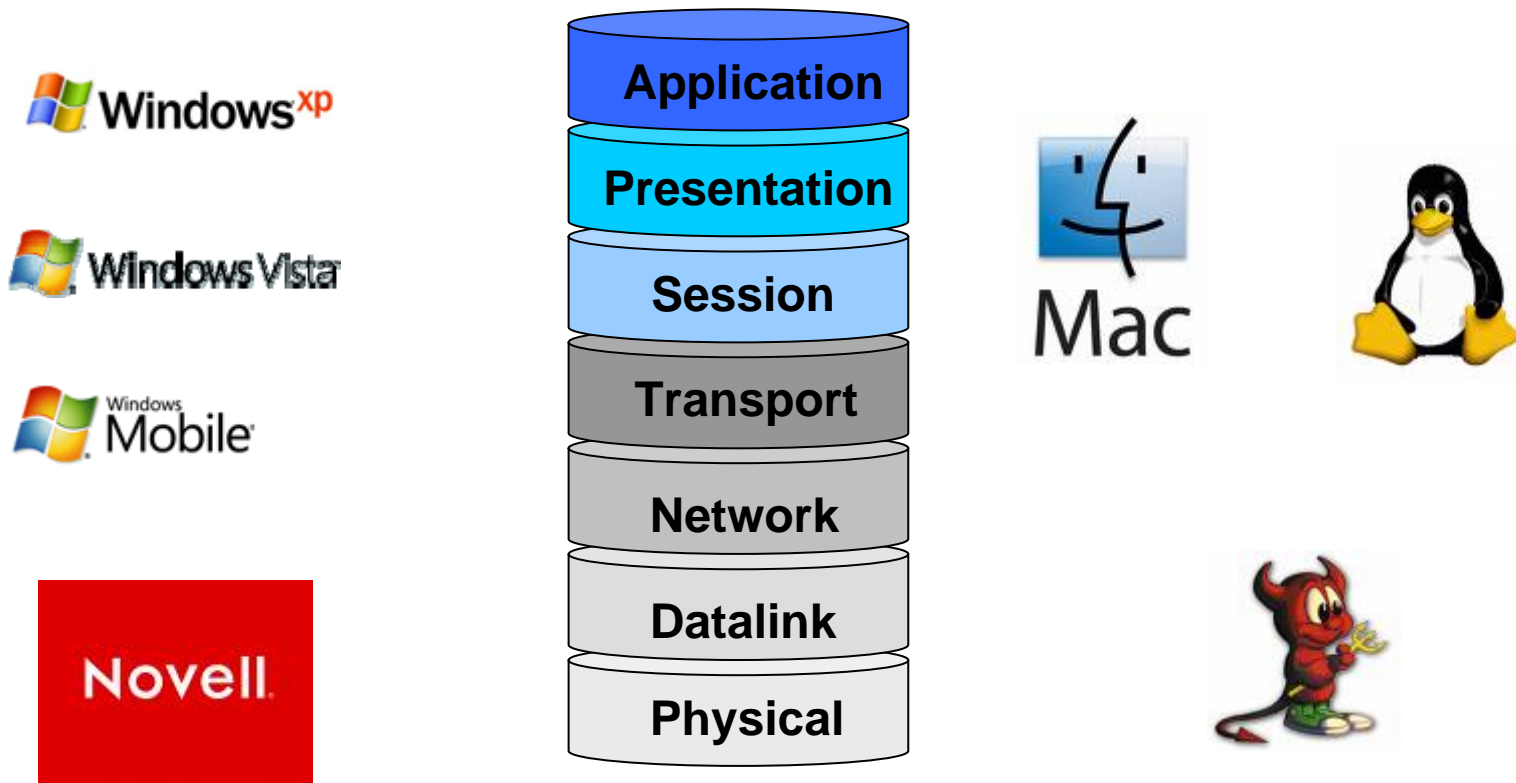
**To understand how Watchguard accomplishes zero day protection, you need to understand the basics.**

- There are two types of Firewalls in the industry today
  - Packet Filter Firewalls
  - Application Proxy Firewalls

# The Basics

## The 7 layer OSI model

For computers to communicate, they use what is known as the 7 layer OSI Model

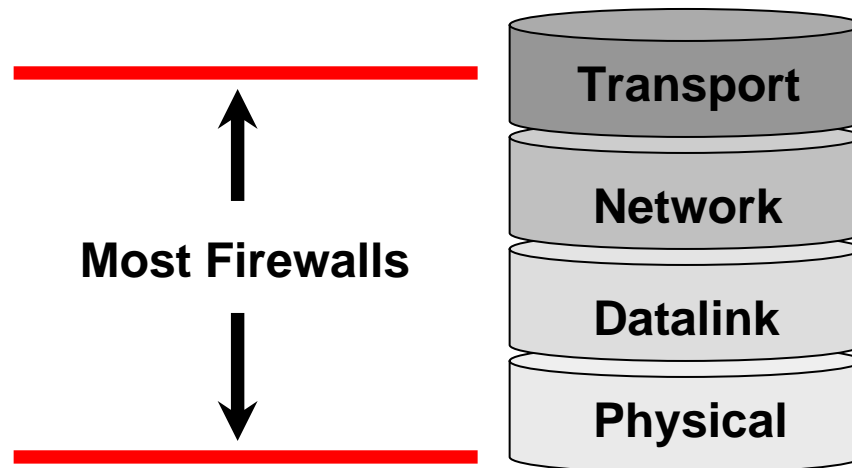


The OSI Model governs how data is “packaged” so that others can read it.

# Packet Filter

## Application Proxy Firewall vs. Packet Filtered Firewalls

**A Packet Filter Firewall inspects the bottom 3-4 layers of the OSI model.**

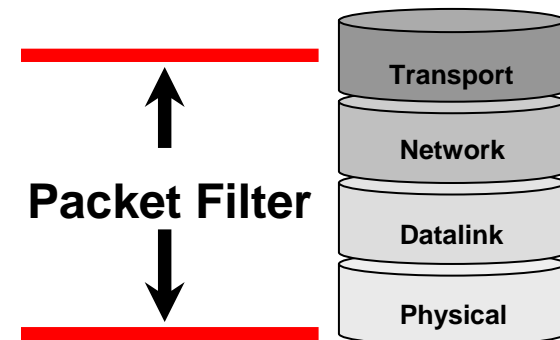


# How Packet Filter Firewalls Work

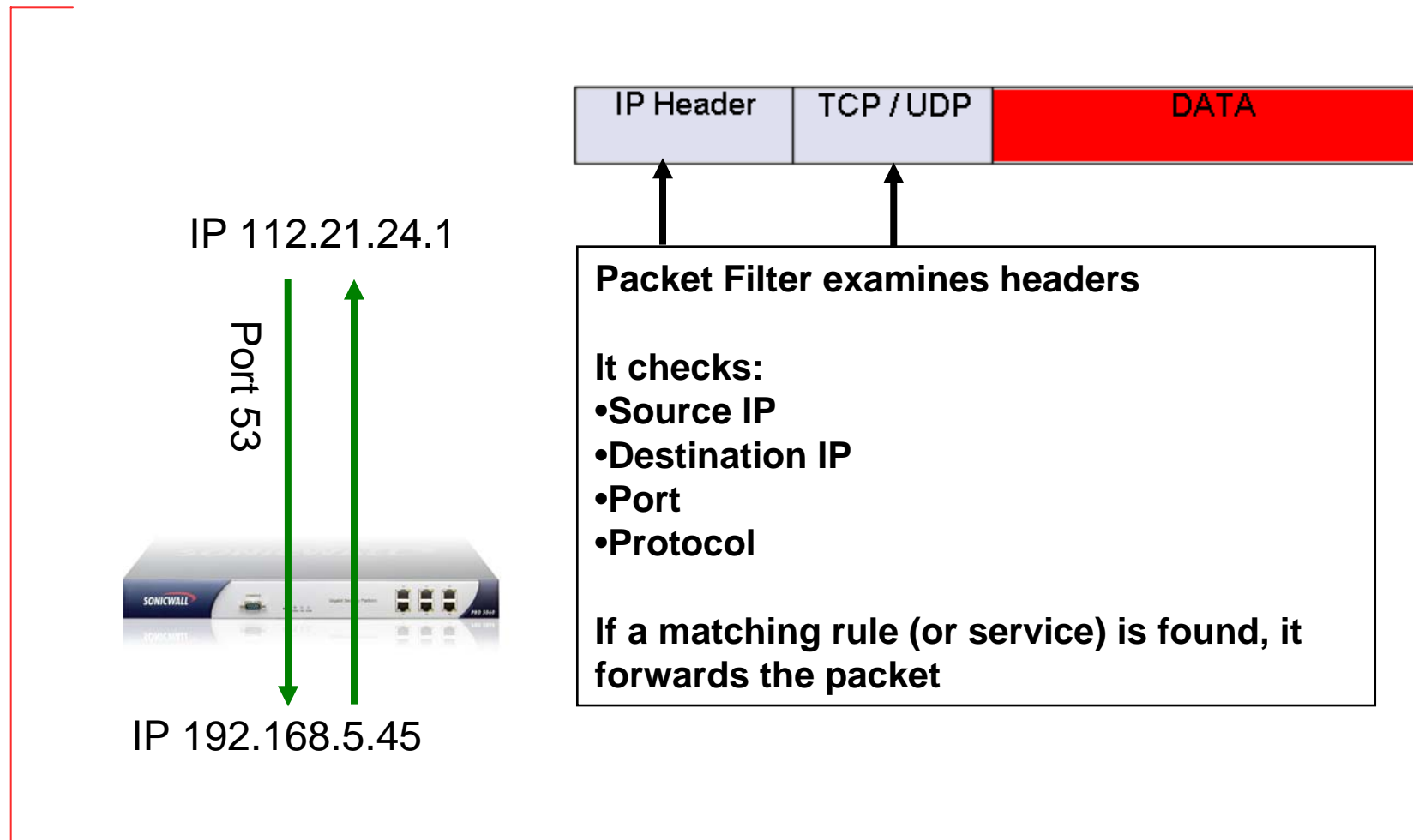
**A Packet Filter Firewall basically does 3 things:**

- 1. Monitor Connection State (Stateful Inspection)**
- 2. Compares traffic against Firewall Rules**
- 3. Compares allowed traffic against a list of Signatures**

Most Firewall vendors today are  
Packet Filter Firewalls.



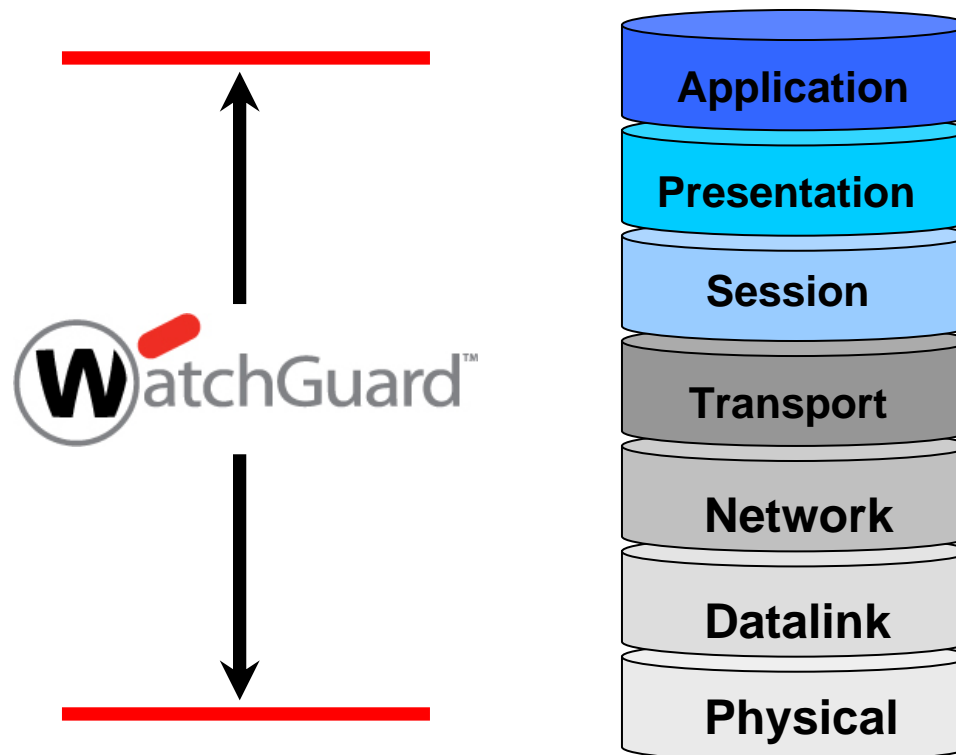
# Packet Filter in Action



# Application Proxy

Application Proxy Firewall vs. Packet Filtered Firewalls

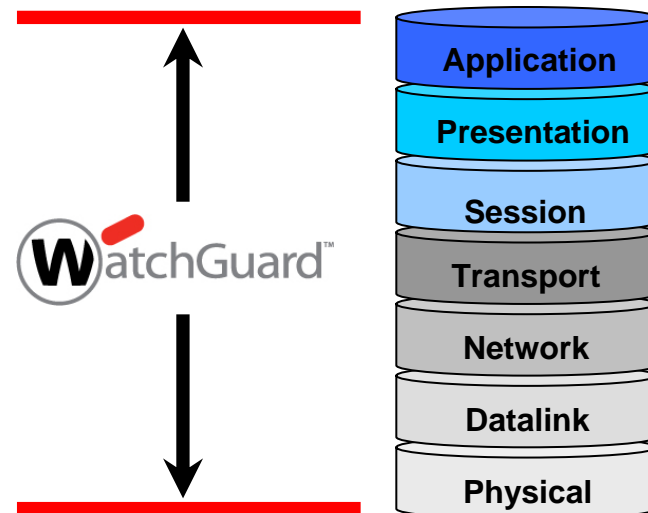
**Watchguard as an “Application Proxy” inspects all 7 layers of the OSI model.**



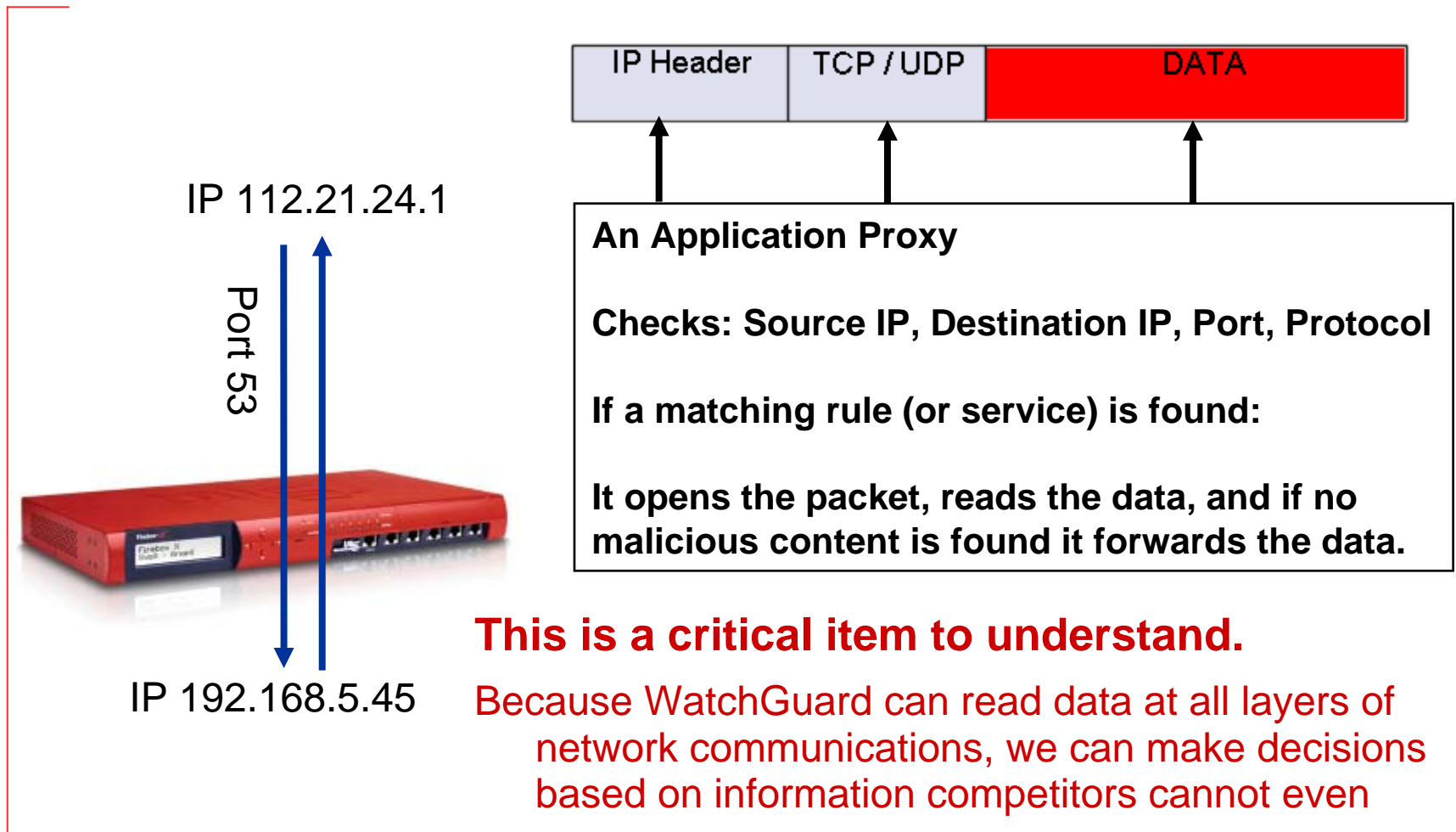
# How WatchGuard Works

**In its simplest form WatchGuard does much more:**

- 1. Monitor Connection State (Stateful Inspection)**
- 2. Compares traffic against Firewall Rules**
- 3. Inspects all aspects of the data**
- 4. Automatically blocks offenders**
- 5. Compares allowed traffic against a list of Signatures**



# Application Proxy in Action



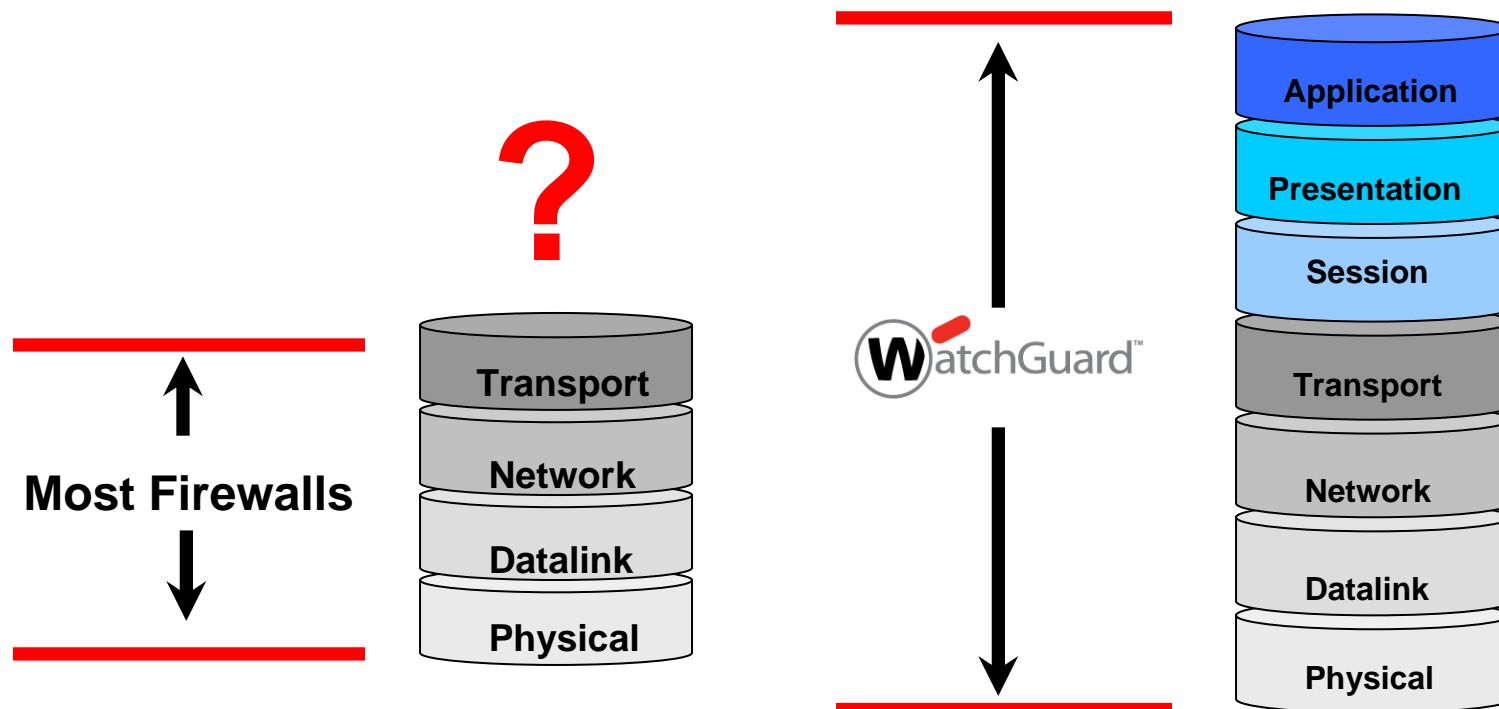
**This is a critical item to understand.**

Because WatchGuard can read data at all layers of network communications, we can make decisions based on information competitors cannot even see.

# Strong Security

## Application Proxy Firewall vs. Packet Filtered Firewalls

In a nutshell, WatchGuard inspects and makes decisions on data that other firewalls do not even look at.



## WatchGuard has tighter security

Because:

- WatchGuard does “everything” a packet filter firewall does and much more.
- WatchGuard inspects data other firewalls do not.
- Each connection must go through as many as hundreds of checks before being allowed.
- We enforce RFC compliance.
- We “Strip” bad data, and allow the good to pass.
- We take action on the data we see.
- We do not only rely on signatures.



A properly tuned WatchGuard is a “True” zero day firewall



# UTM (Unified Threat Management)

- **Due to our add-on services (GAV/IPS, WebBlocker, SpamBlocker)**
  - **WatchGuard is a Major Player for UTM Solutions in the Small to mid sized businesses of today**

## What is a UTM Solution?

▪ **Unified Threat Management** appliances have **evolved** from **traditional firewall** and **VPN appliances** into a solution that has additional capabilities previously handled by multiple systems including:

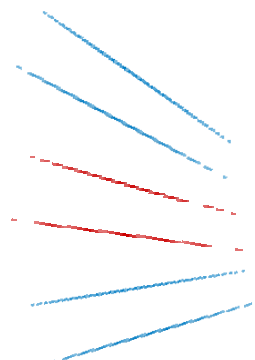
- URL filtering
  - Spam blocking
  - Spyware protection
  - Intrusion prevention,
  - Gateway antivirus
  - Integrated management, monitoring, and logging capabilities
- Why do UTMs make sense?
- Reduced TCO
  - Simplified administration
  - Inclusive: hardware & services
  - More efficient technology

# WatchGuard Security Services

spamBlocker®

WebBlocker®

GAV/IPS



**Full UTM capabilities available across all Firebox Appliances – Edge, Core and Peak**

## Security Services

spamBlocker®



- **What is it:**
  - **Real time spam blocking service for Firebox X appliances running Fireware or Fireware Pro**
  
- **Value:**
  - **It's the best service in the industry at distinguishing spam from legitimate communication, blocking >97% of unwanted e-mails. Very low false positive ratio.**
  - **Processing is done off the Fireware appliance so there is minimal impact to other network traffic processing**

**Partnered with CommTouch, an industry leader in spam prevention and mitigation**

## Security Services

### Gateway Antivirus/IPS



- **What is it?**
  - **Anti-spyware using multi layered inspection of inbound and outbound web and mail traffic for spyware, adware, keyloggers and dialers**
  - **Ability to enable/disable IPS signatures and individual IM/P2P applications**
  - **Ability to view and sort IPS signatures by ID, category, severity and status**
  - **streamlined configuration in Policy Manager**
- **Value:**
  - **Stronger security for web-surfing**
  - **Flexibility and Control over IM/P2P usage and IPS signatures**
  - **Protection against spyware while surfing the web and getting email**

## Security Services

### WebBlocker® (URL Filtering)



- **What's is it?**
  - **URL filtering via 54 categories (over 12 million URLs)**
  - **Configurable Exceptions (Whitelist / Blacklist)**
  - **Multiple policy deployment simple (Per user, per group, IP address, etc)**
  - **Details Reports can be generated on historical data**
  - **Pricing based on “Per Box” vs. “Per Seat”**
  - **Used in all industries “Very Popular in Schools”**
  
- **Value:**
  - **Flexibility to block specific site categories**
  - **Increased legal and regulatory protection**
  - **Protection against known spyware, internet scam and phishing sites**

**Partnered with SurfControl, industry leader in the Internet Content Filtering market**

## Options and add-ons

### LiveSecurity

- LiveSecurity Service
  - Award winning - *most comprehensive* support offering in the industry
  - Free Software updates (Software Assurance)
  - Technical support
  - Advanced hardware replacements (next day delivery)
  - Tools, expert advice on best security practices
  - Security alerts – text and video



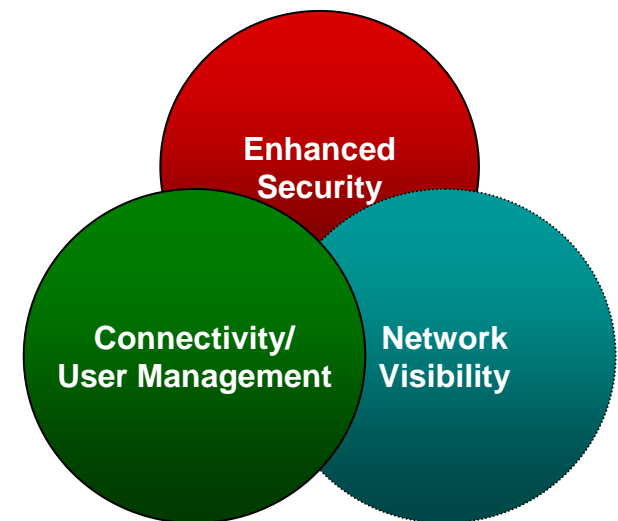
# What's New in Fireware 10

**Enhanced Security, Connectivity,  
User Management, Visibility**

## What's New in Fireware 10

### Enhanced Security, Connectivity/User Management, Network Visibility

- **Enhanced Security**
  - Virus Outbreak Detection
  - IPS Engine and Signatures
  - Quarantine for AntiVirus
  - HTTPS URL filtering
  - 54 WebBlocker Categories
- **Connectivity & User Management**
  - SSL VPN Integration
  - Single Sign-On Pass-Through Authentication
  - VoIP and Video Conferencing Support
  - Wireless Bridging
- **Network Visibility**
  - Reporting Engine and Report Content
  - SQL-Based log storage
  - LogViewer
  - LiveSecurity Alerts (RSS Feeds)
  - SNMPv3 support





**Questions?**



**Thank You!**