RSA CONFERENCE ASIA PACIFIC 2013

Security in knowledge

CUTTING THROUGH THE HYPE: WHAT IS TRUE “NEXT GENERATION” SECURITY?

Jennifer Ellard
HP

Session ID: SPO-W01B

Session Classification: General Interest

Agenda

- What is hype?
- What we hear from you?
- Separating the wheat from the chaff
- Moving forward “hypeless”
- Summary

Heard any hype lately??

SDN

Cyber Risk

End of the Mayan Calendar

Next Generation

Weapons of Mass Destruction

Bieber

Y2K

Encrypted traffic

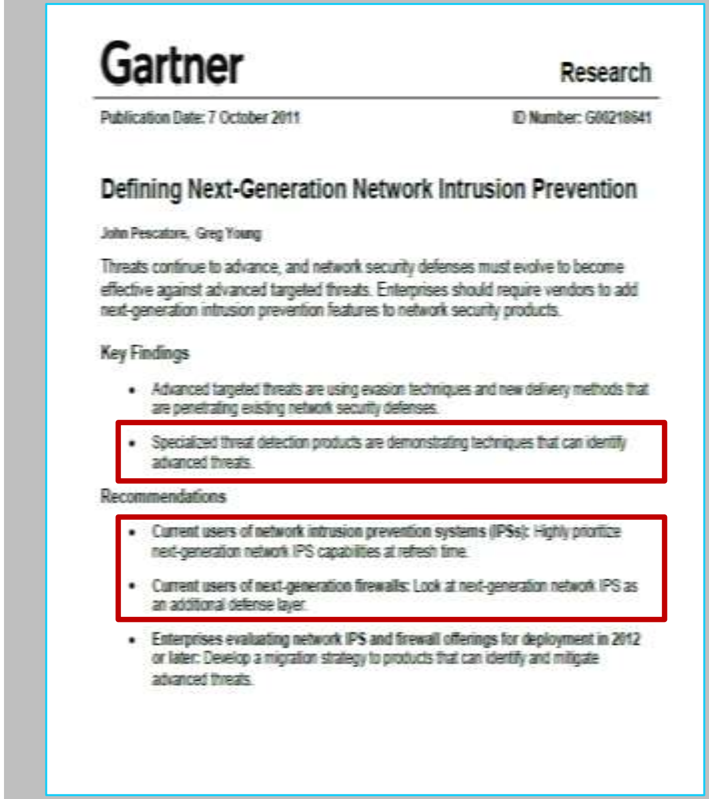
Insert latest threat

Kardasians

"I don't care about acronyms, I want to know that I am safe."

-- EMEA Customer

Next Generation Intrusion Prevention Defined



Gartner

Research

Publication Date: 7 October 2011

ID Number: G00218641

Defining Next-Generation Network Intrusion Prevention

John Pescatore, Greg Young

Threats continue to advance, and network security defenses must evolve to become effective against advanced targeted threats. Enterprises should require vendors to add next-generation intrusion prevention features to network security products.

Key Findings

- Advanced targeted threats are using evasion techniques and new delivery methods that are penetrating existing network security defenses.
- Specialized threat detection products are demonstrating techniques that can identify advanced threats.

Recommendations

- **Current users of network intrusion prevention systems (IPSs):** Highly prioritize next-generation network IPS capabilities at refresh time.
- **Current users of next-generation firewalls:** Look at next-generation network IPS as an additional defense layer.
- **Enterprises evaluating network IPS and firewall offerings for deployment in 2012 or later:** Develop a migration strategy to products that can identify and mitigate advanced threats.

Standard First Gen IPS Capabilities

Context Awareness

Content Awareness

Application Awareness and Visibility

Agile Engine

How are you addressing…

- **Virtual Security**
  - Cost/ efficiency
  - Performance degradation
- **Encrypted traffic**
  - Block it
  - Quarantine it
- **Software Defined Networks**
  - Planning for this
  - Considering it

How do you separate the wheat from the chaff?

Vulnerability Cold Hard Facts

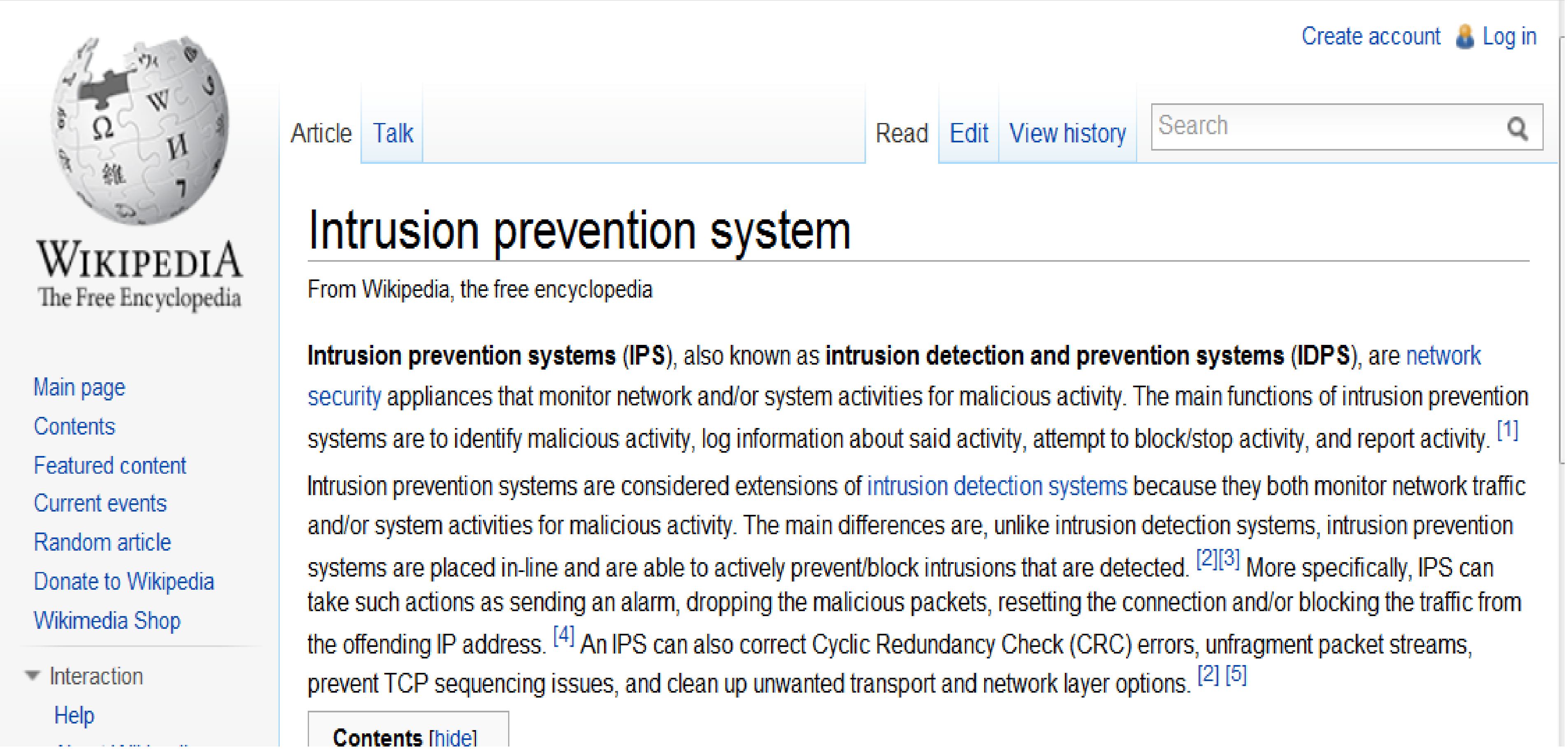
- The vulnerability arms race—total vulnerability disclosures in 2012 increased 19% from 2011.

- Evolving marketplaces and increasing complexity impact discovery and reporting

- Web applications continue to introduce significant technical risk to organizations

- The maturity of a technology does not govern its vulnerability profile – 700% increase

From the source of all knowledge…



Intrusion prevention system

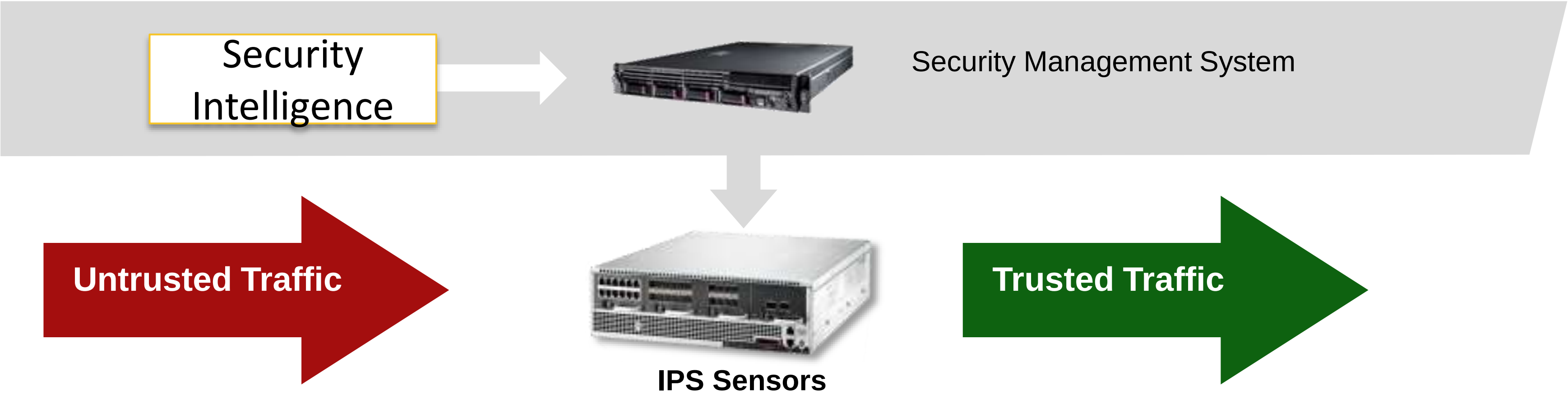
From Wikipedia, the free encyclopedia

Intrusion prevention systems (**IPS**), also known as **intrusion detection and prevention systems** (**IDPS**), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about said activity, attempt to block/stop activity, and report activity. [1]

Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected. [2][3] More specifically, IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address. [4] An IPS can also correct Cyclic Redundancy Check (CRC) errors, unfragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options. [2] [5]

Contents [hide]

Network Security Basics



Security Intelligence

Security Management System

Untrusted Traffic

IPS Sensors

Trusted Traffic

IPS Platform

Designed for future security demands and services

Proactive

- In-line reliability
- In-line performance (throughput/latency)
- Filter accuracy

Security

- Leading security research
- Fastest coverage
- Broadest coverage

↑

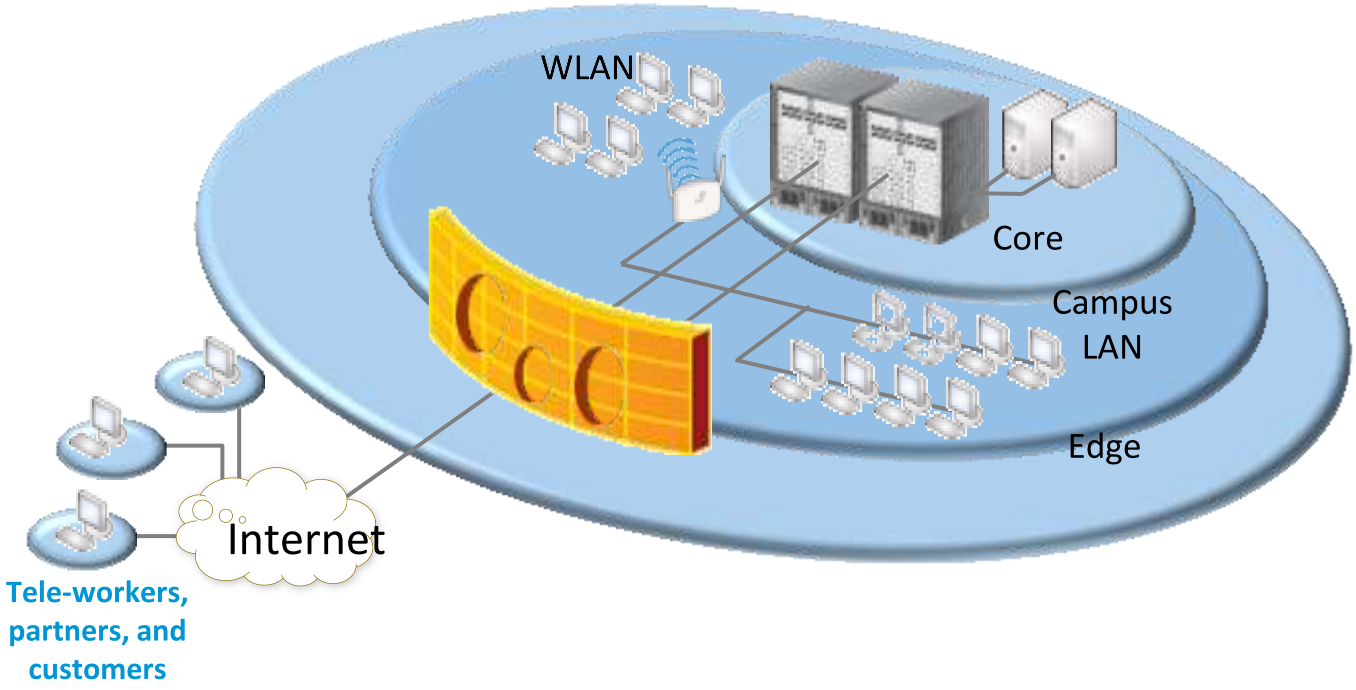
Costs

- Quick to deploy
- Automated threat blocking
- Easy to manage

↓

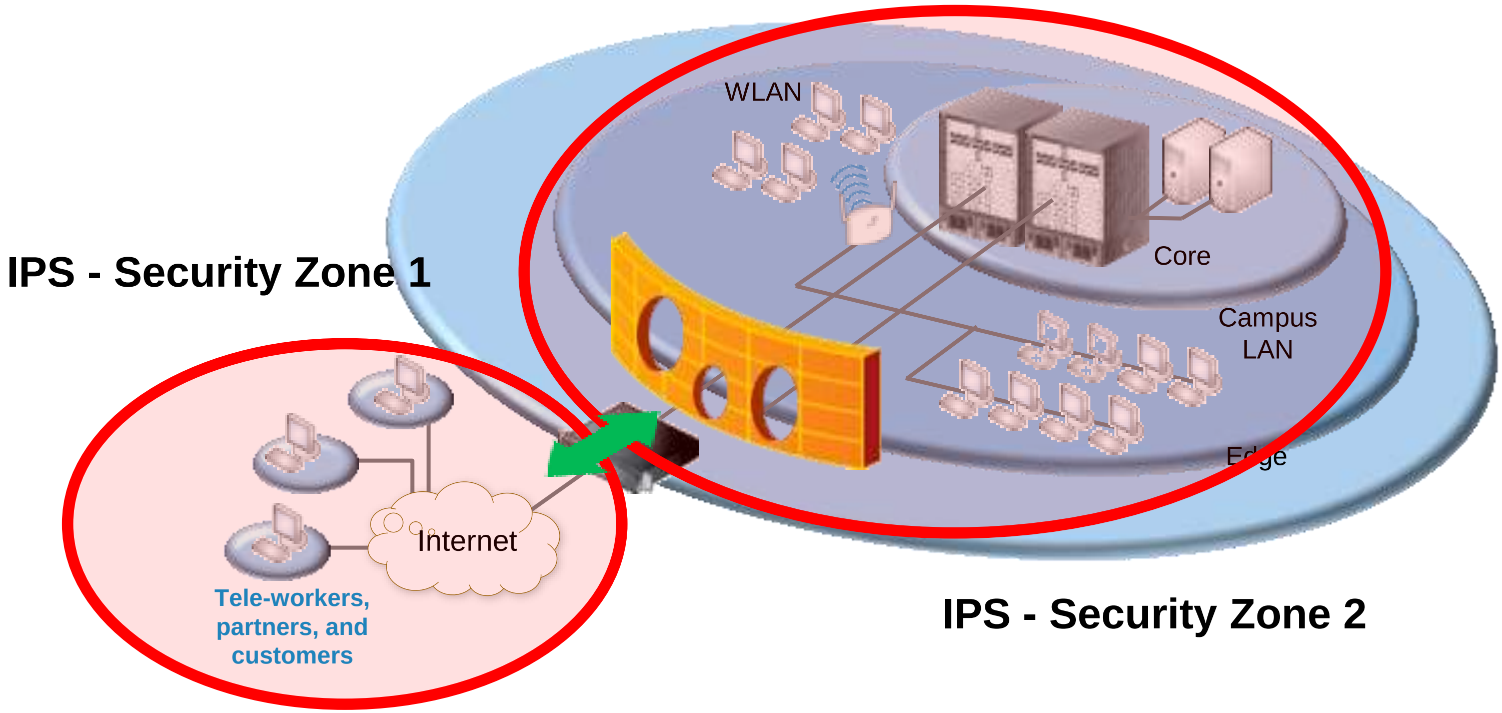
IPS devices can be deployed anywhere…

Just “wedge” an IPS segment into any place you want to inspect/enforce network security policy.



Like.. Between your Internet connection and your LAN (Local Area Network)

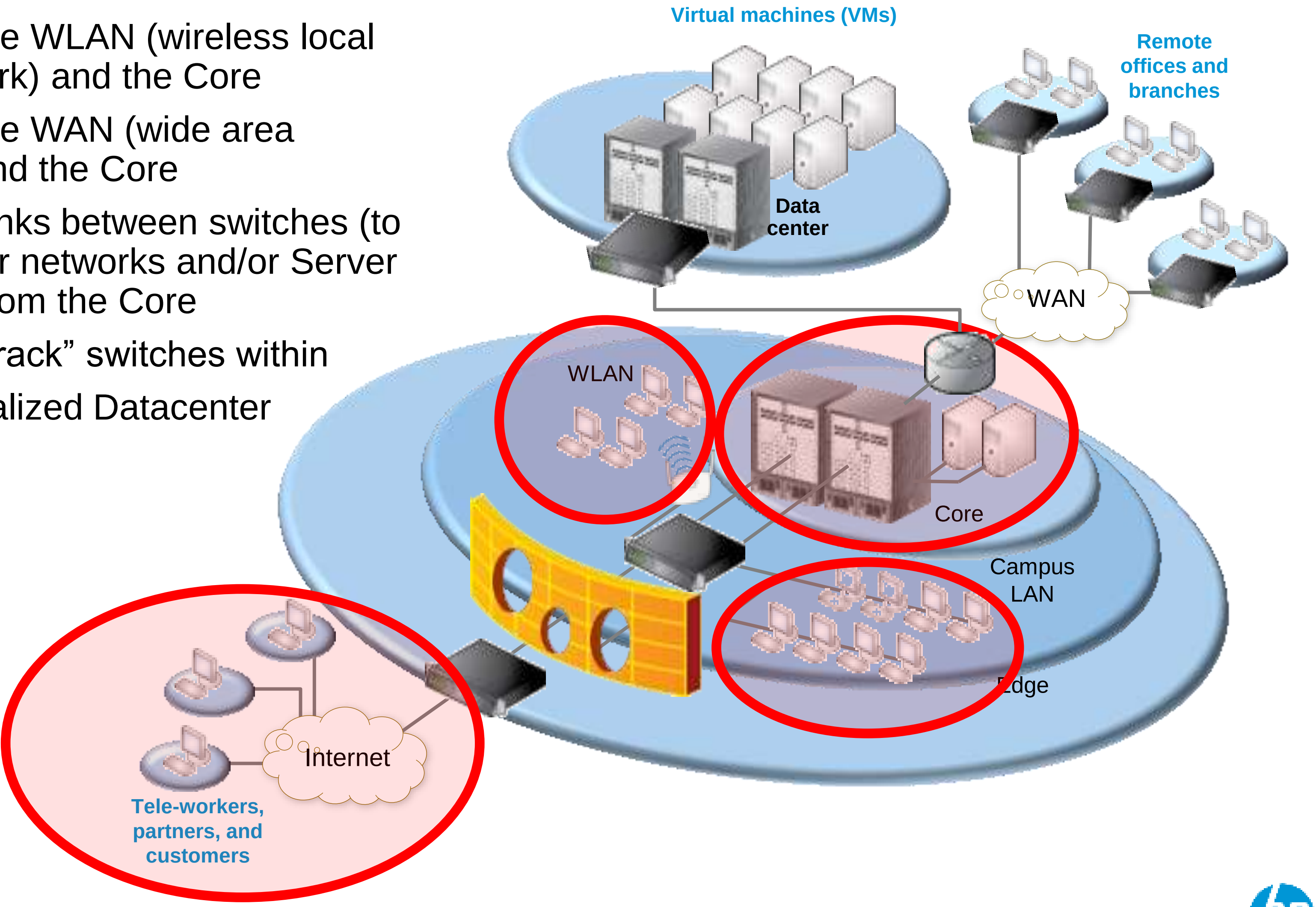
- Deploy inside the firewall (most common)
- Deploy outside the firewall (a fading trend)
- Deploy both inside and outside the firewall (a “firewall sandwich” – Also a fading trend)



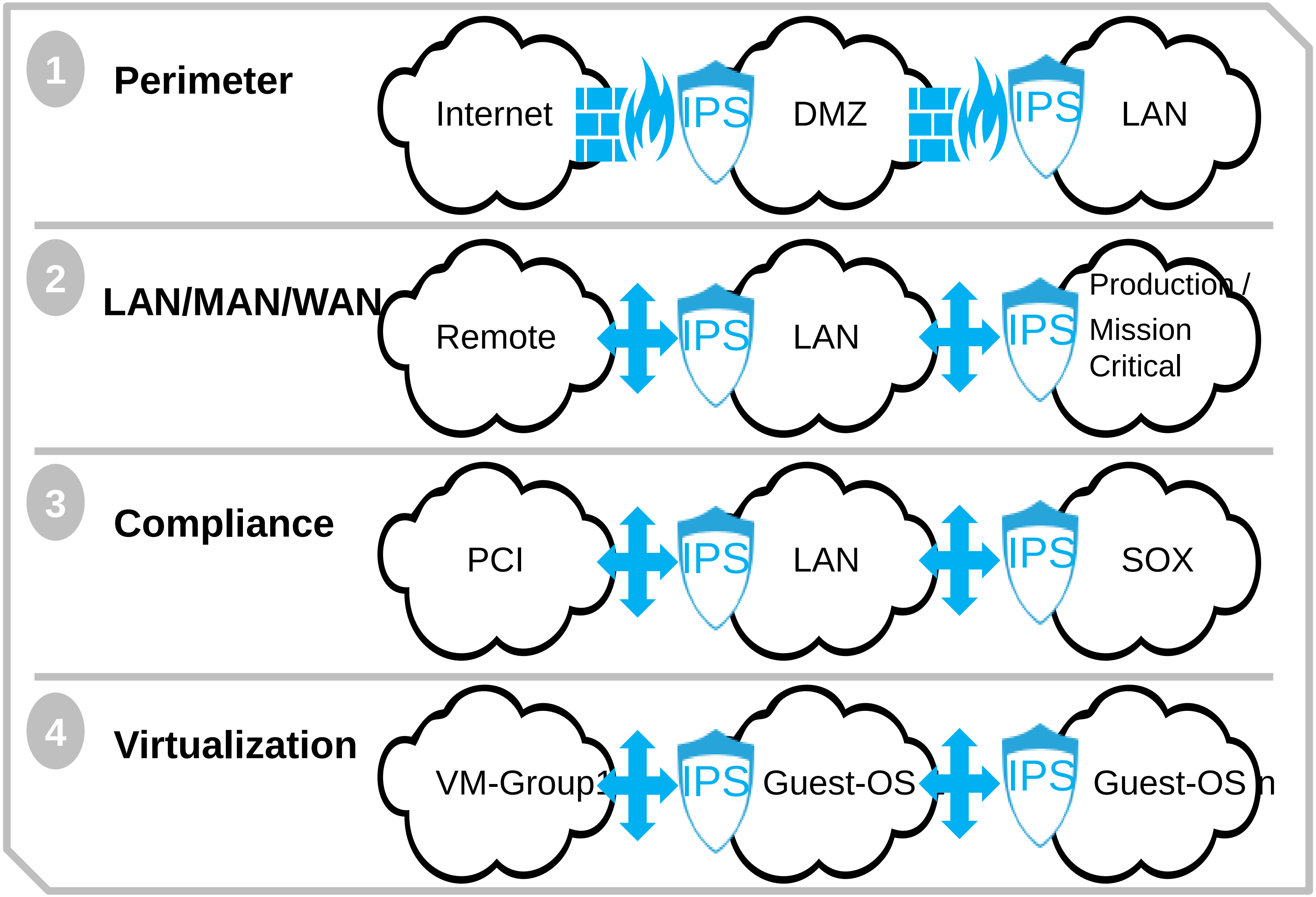
And/Or.. Deploy closer to the Core of the network

- Between the WLAN (wireless local area network) and the Core
- Between the WAN (wide area network) and the Core
- On Trunk links between switches (to isolate User networks and/or Server networks from the Core
- On "top-of-rack" switches within

  your virtualized Datacenter



Top Four Deployment Scenarios



Define settings & distribute to IPS devices

Availability

- Protocol Anomalies
- Denial-Of-Service
- (Distributed) Denial-Of-Service

...

Bandwidth Mgmt.

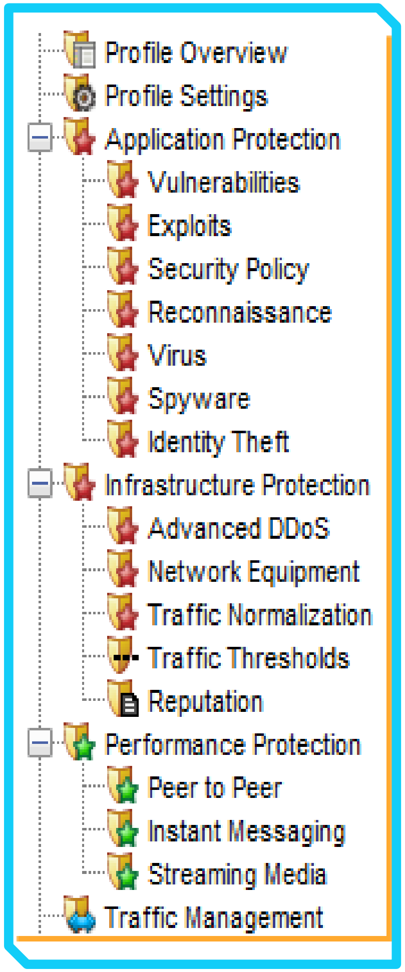
- App. Rate Limiter

Corporate-Policy

- Security Policy
- Access Validation
- Tunneling
- Rogue Applications
- Peer-to-Peer
- Streaming Media

...

Security Profile



- Profile Overview
- Profile Settings
- Application Protection
    - Vulnerabilities
    - Exploits
    - Security Policy
    - Reconnaissance
    - Virus
    - Spyware
    - Identity Theft
- Infrastructure Protection
    - Advanced DDoS
    - Network Equipment
    - Traffic Normalization
    - Traffic Thresholds
    - Reputation
- Performance Protection
    - Peer to Peer
    - Instant Messaging
    - Streaming Media
- Traffic Management

Cyber-Attacks

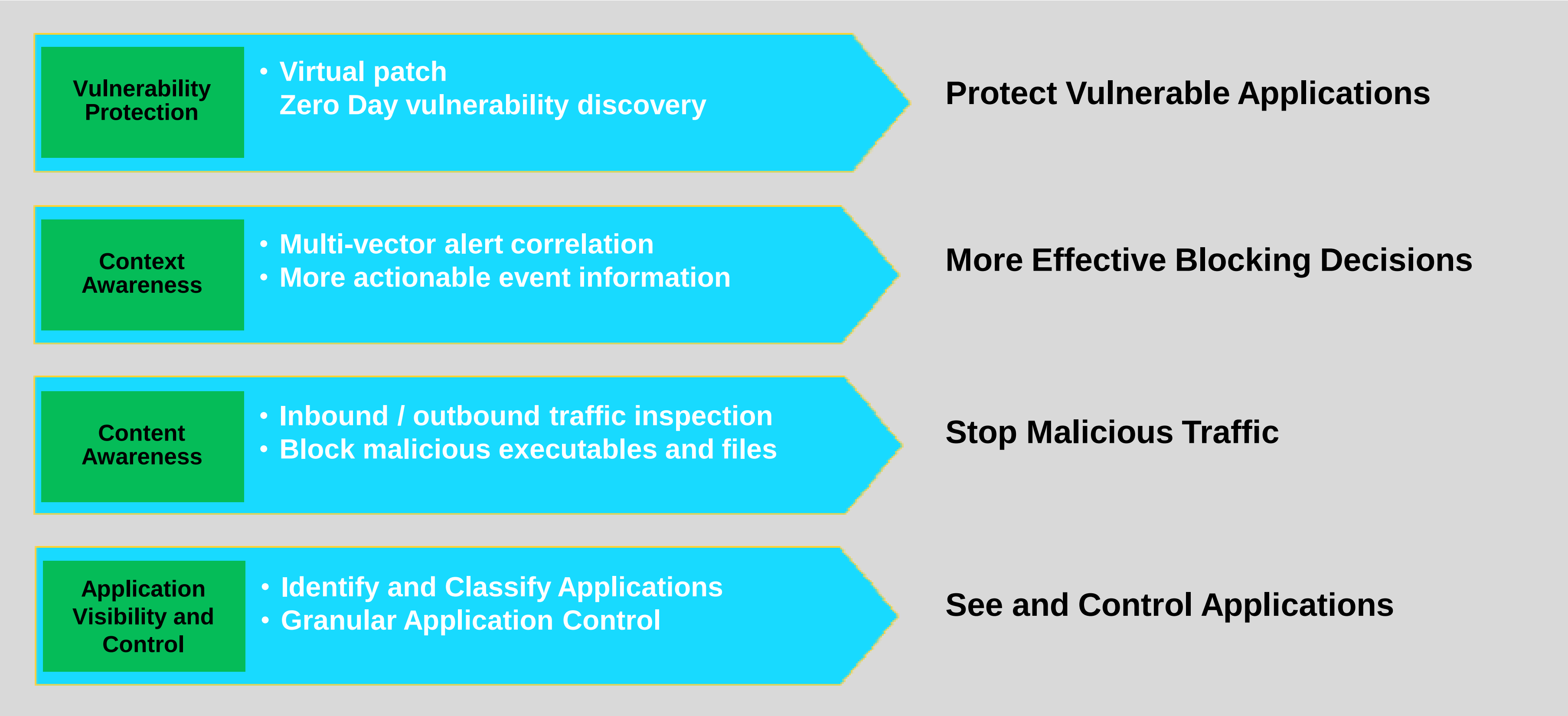
- Reconnaissance
- Trojan
- Backdoor
- Virus
- Worm
- Spyware
- Phishing
- Buffer Overflow
- Heap Heap Overflow
- SQL-Injection
- Cross-Site-Scripting
- Cross Site Rquest Forgery
- Malicious Documents

...

What do non-hyped Network Security offerings include?

- **Intelligence**
  - Up-to-date
  - Threat protection
- **Manageability**
  - Set and forget
  - 60% use the factory settings
  - Easy to use
- **Reliability**
  - Automated
  - Scalable to small and large enterprises

Your Network Deserves Full Security Coverage



	Key Feature and Capability	Benefit and Services
Vulnerability Protection	• Virtual patch Zero Day vulnerability discovery	Protect Vulnerable Applications
Context Awareness	• Multi-vector alert correlation • More actionable event information	More Effective Blocking Decisions
Content Awareness	• Inbound / outbound traffic inspection • Block malicious executables and files	Stop Malicious Traffic
Application Visibility and Control	• Identify and Classify Applications • Granular Application Control	See and Control Applications

"Before deploying {IPS device}, we had some security challenges. Every other day, tons of attacks were happening in our network. Sometimes they were blocked, but sometimes we could not manage the situation properly. We used to receive many complaints from students and faculty; but now, with {IPS device} in our environment, we can say that we have peace."

-- EMEA Educational Customer

See though the hype

- **Protect your network infrastructure**
  - Mobile Vulnerabilities
  - New Vulnerabilities
- **Control the policies and threat responses**
  - Set it and forget it
  - 60% of customers use factory-direct settings
- **Know what is going on in your environment**
  - Have visibility to threats
  - Take actions or automatically respond

Summary and Next Steps

Attend these sessions

- Tomorrow's keynote session – Learn how the criminal mind works.
- HP booth theatre – Learn how social media impacts your network

Visit these demos

- HP TippingPoint Intrusion Prevention Device demo
- HP ArcSight demo

After the event

- Visit the HP website at: www.hp.com/go/tippingpoint
- Download the Cyber Risk whitepaper at: www.hp.com/go/tippingpoint

Your feedback is important to us. Please take a few minutes to complete the session survey.

Thank you!