Academic Freedom or Application Chaos?

March 2012

paloalto NETWORKS

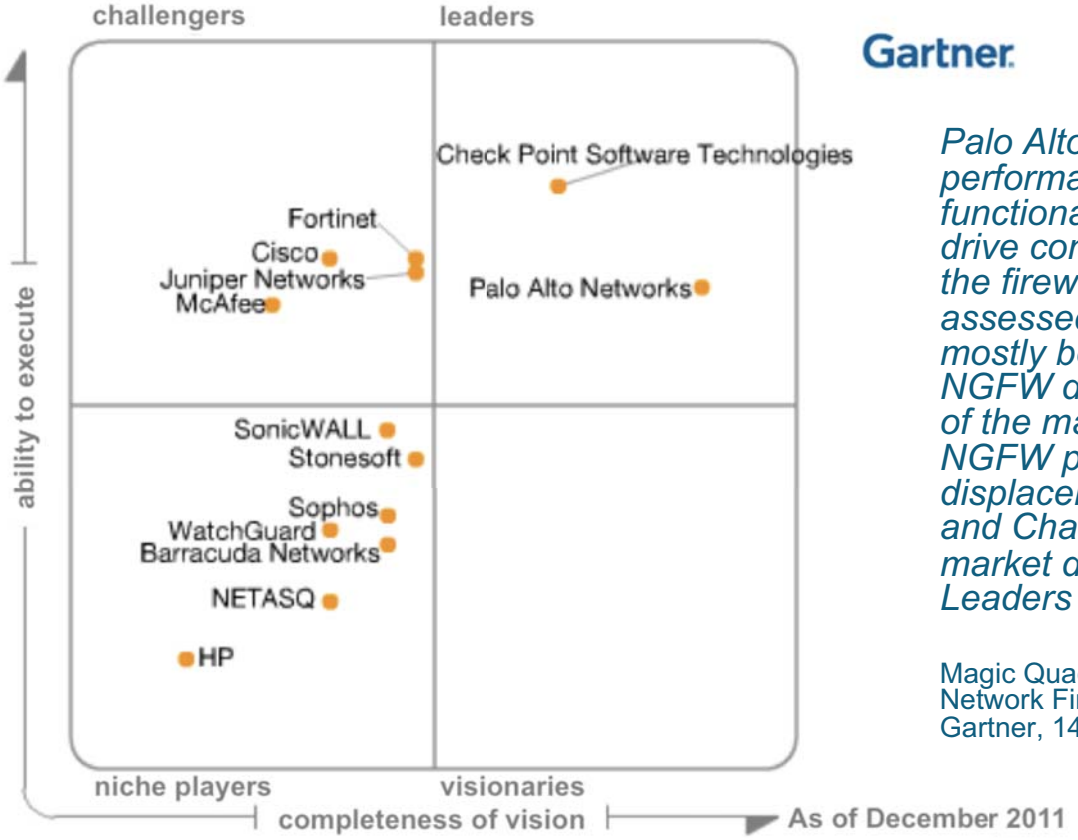
About Palo Alto Networks

- We are **the network security company**
- World-class team with strong security and networking experience
  - Founded in 2005, first customer July 2007
- We offer next-generation firewalls that safely enable 1,400+ applications
  - Restores the firewall as the core of the enterprise network security infrastructure
  - Innovations: App-ID™, User-ID, Content-ID, GlobalProtect™, WildFire™
- Global footprint: 6,300+ customers in 80+ countries

(*) Reported on August 1, 2011. Bookings run rate is defined as 4 (four) times the bookings amount of the most recently finished fiscal quarter. Bookings are defined as non-cancellable orders received during the fiscal period. Palo Alto Networks' fiscal year runs from August 1st until July 31st.

paloalto NETWORKS

2011 Magic Quadrant for Enterprise Network Firewalls



Gartner

Palo Alto Networks' high-performance NGFW functionality continues to drive competitors to react in the firewall market. It is assessed as a Leader mostly because of its NGFW design, redirection of the market along the NGFW path, consistent displacement of Leaders and Challengers, and market disruption forcing Leaders to react."

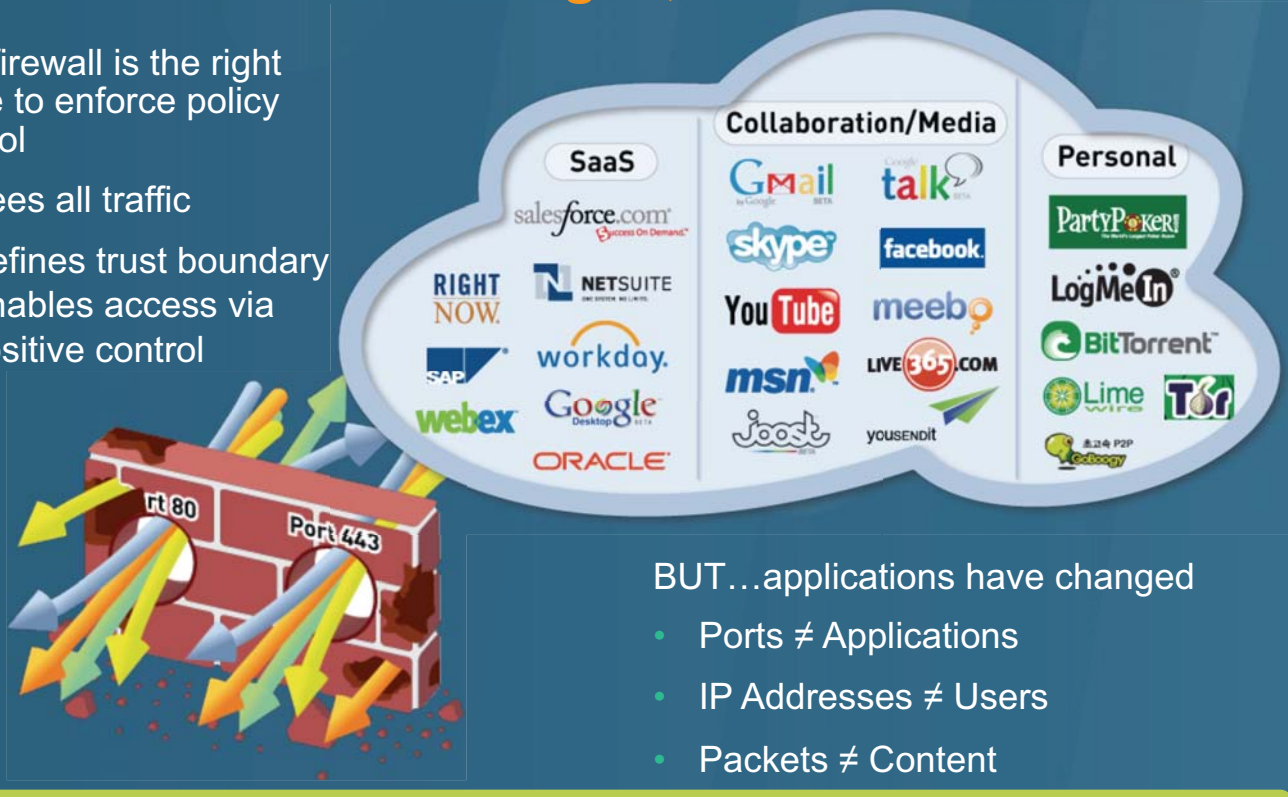
Magic Quadrant for Enterprise Network Firewalls
Gartner, 14 December 2011

paloalto NETWORKS

Applications Have Changed; Firewalls Have Not

The firewall is the right place to enforce policy control

- Sees all traffic
- Defines trust boundary
- Enables access via positive control



BUT…applications have changed

- Ports ≠ Applications
- IP Addresses ≠ Users
- Packets ≠ Content

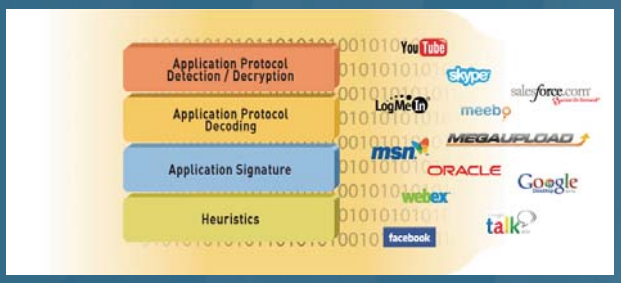
Need to restore visibility and control in the firewall

paloalto NETWORKS

Unique technologies transform the firewall

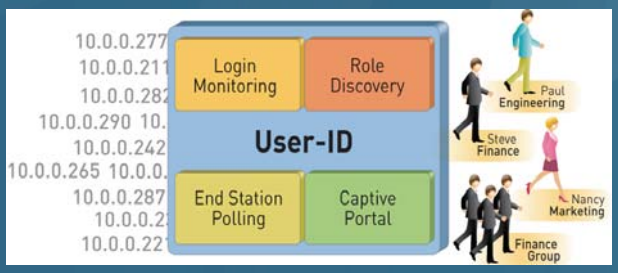
App-ID

Identify 1,400 applications



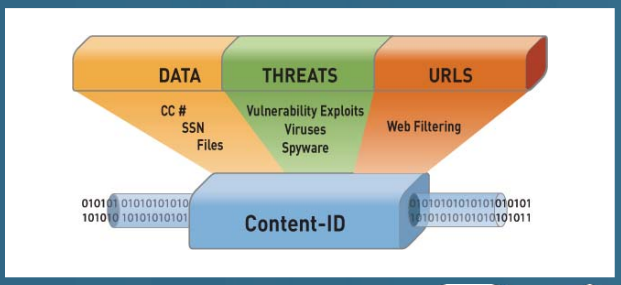
User-ID

Identify every user – by name



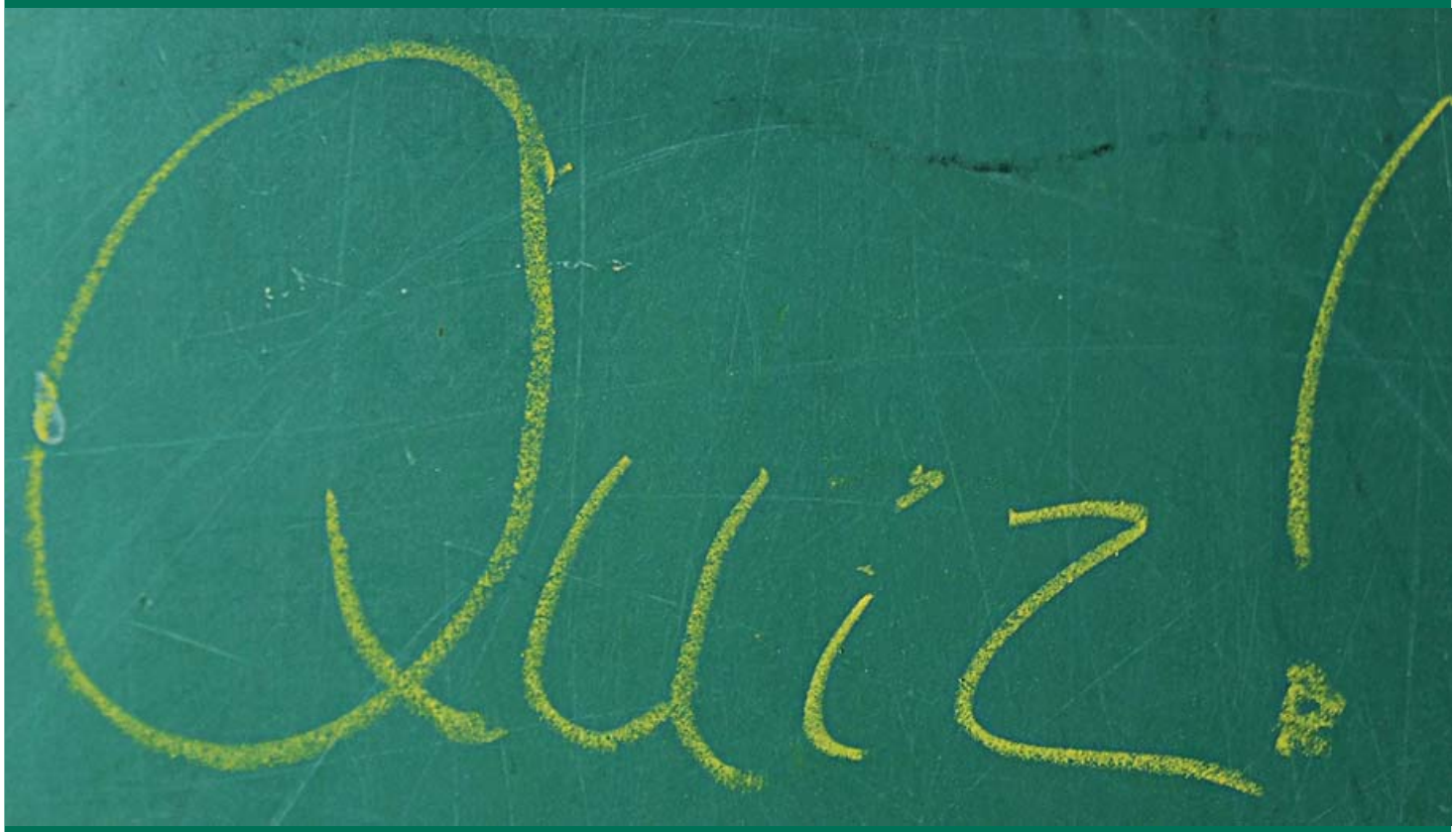
Content-ID

Scan and control all content



paloalto NETWORKS

What do you really know about your network?



Frequency that external proxies were found?

75%

Frequency is defined as a single instance found on a network (n=619).

paloalto NETWORKS

Frequency that external proxies were found?

85%

A total of **34 different proxies** were in use, with an average of five variants found on **85% of the 619 university networks**.

Frequency is defined as a single instance found on a network (n=619).

paloalto NETWORKS

Frequency that non-VPN related encrypted tunnels were found?

50%

Frequency is defined as a single instance found on a network (n=619).

paloalto NETWORKS

Frequency that non-VPN related encrypted tunnels were found?

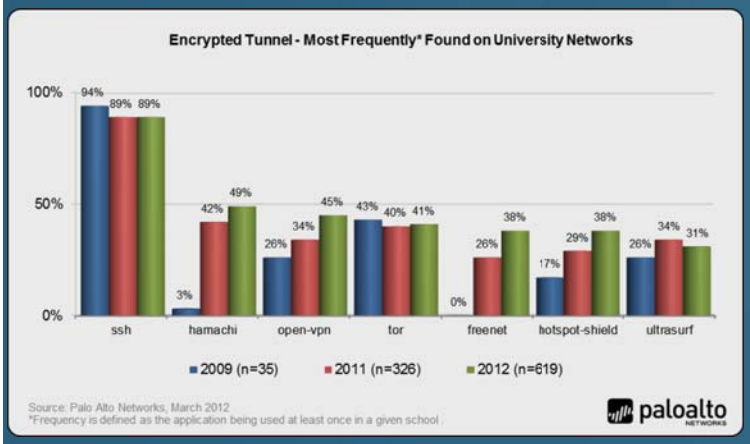
67%

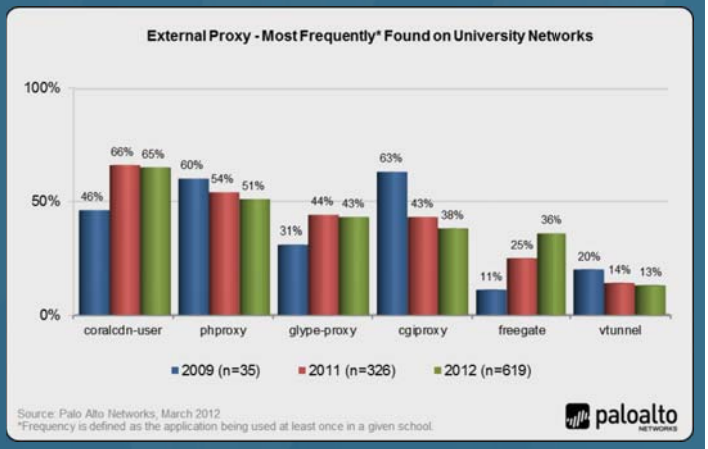
Non-VPN related tunnels **were found on 67%** of the University Networks – the question is what is the use case?

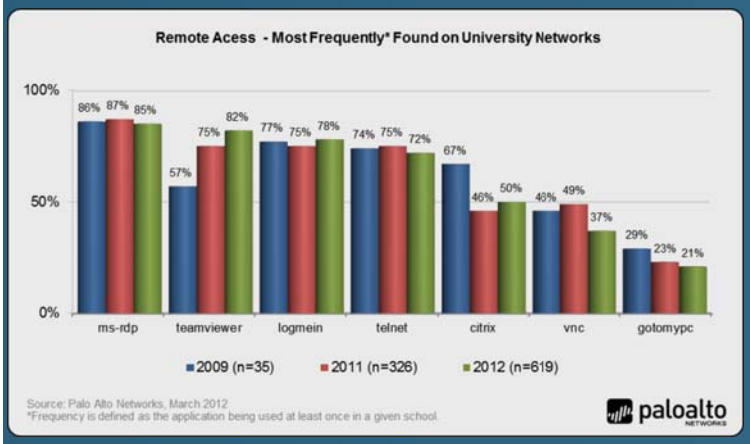
Frequency is defined as a single instance found on a network (n=619).

paloalto NETWORKS

Students find a way…







- Encrypted tunnels (Tor, UltraSurf, Hamachi) **used to "hide"**
- External proxies commonly used to **bypass URL filtering**
- Remote access commonly used to **evade controls; known as a cyber criminal target**

Average number of browser-based filesharing applications found per school?

Higher?

15

Lower?

paloalto NETWORKS

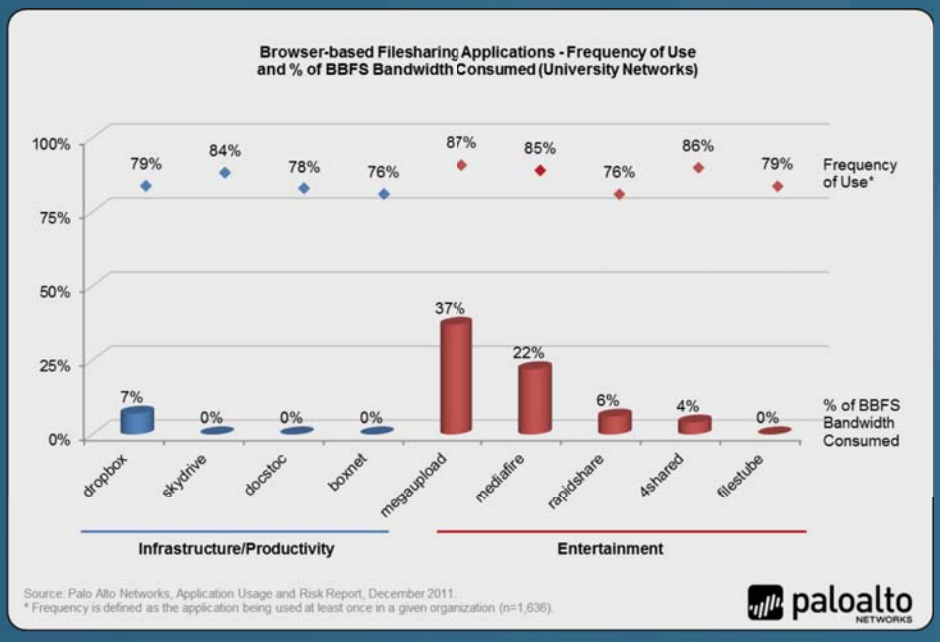
Average number of browser-based filesharing applications found per school?

18

There were **70 browser-based filesharing variants** found with an average of **11 discovered on 97%** of the participating universities.

paloalto NETWORKS

Browser-based file sharing: two use cases



Browser-based filesharing use cases: entertainment or productivity. Both uses have a common set of business and security risks that organizations must address.

paloalto NETWORKS

Percentage of total bandwidth consumed by file transfer of all types?

Higher?

25%

Lower?

paloalto NETWORKS

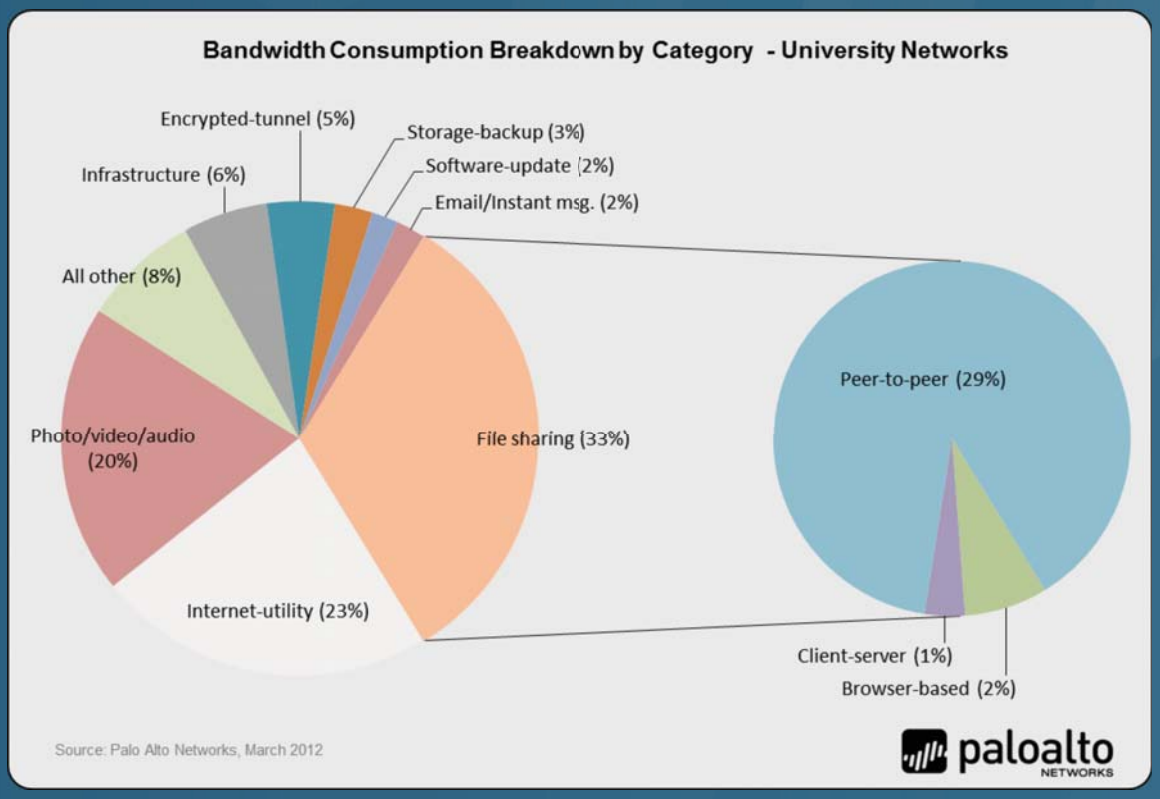
Percentage of total bandwidth consumed by file transfer of all types?

33%

P2P, browser-based and client-server filesharing applications **consumed 33%** of total bandwidth – **more that 3.5X** the same amount as viewed in the enterprise environments.

paloalto NETWORKS

P2P dwarfs all other application categories



paloalto NETWORKS

The number of applications using Port 80 only?

Higher?

300

Lower?

paloalto NETWORKS

The number of applications using Port 80 only?

307

The number of applications that **ONLY use Port 80 is 307 or 25% of the 1,248** applications found on participating university networks.

paloalto NETWORKS

The number of applications NOT using Port 80

Higher?

400

Lower?

paloalto NETWORKS

The number of applications NOT using Port 80

Higher?

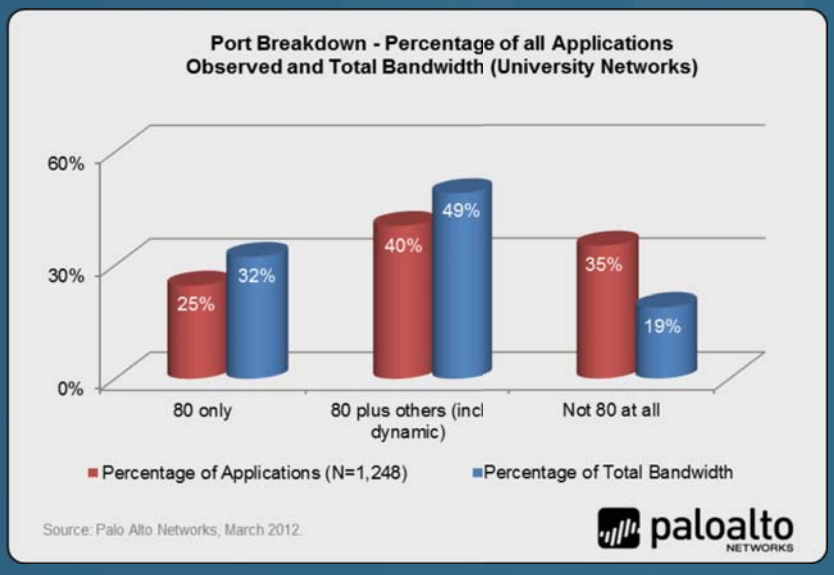
437

Lower?

The number of applications that **do not use Port 80 is 437 or 35% of the 1,248** applications found on participating university networks.

paloalto NETWORKS

Port 80 only security is shortsighted



Port 80 represents significant risks; yet too much emphasis can be shortsighted.

paloalto NETWORKS

Application Chaos Management Challenges

- The RIAA, P2P and browser-based file sharing
- Unable to identify many of the newer applications
- Cannot identify who is using the applications
- Must balance control with educational freedom
- Shrinking budgets and increased malware cleanup costs
- Increasingly complex security infrastructures
- The list goes on…

paloalto NETWORKS

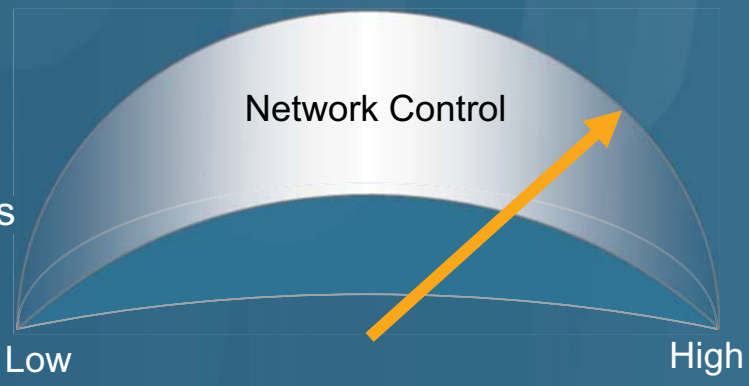
Enable academic freedom, minimize chaos

- Identify more than 1,400 applications including P2P, encrypted tunneling and proxies
- Determine who is using these applications through directory services integration
- Apply firewall policies to monitor and log, apply QoS or block where warranted
- Inspect and protect application traffic with high speed threat prevention

paloalto NETWORKS

You decide the levels of policy control

- Visibility enables more informed policy decisions
  - Allow
  - Allow but scan
  - Allow certain users
  - Allow certain functions
  - Deny known bad applications
  - Decrypt where appropriate
  - Shape (QoS)
  - …any combination



paloalto NETWORKS

Summary of Key Findings

- Circumvention tool use is high (but unchanged)
  - Contradicts the assumption that university networks are “open”.
- P2P filesharing and streaming media consumes 49% of overall bandwidth
  - P2P filesharing consumed a staggering 29%
  - Streaming media (video and audio) applications consumed 20% of the overall bandwidth
- Browser-based filesharing popularity forces use case segmentation
  - Productivity
  - Entertainment
- Securing port 80 does not equate to securing the network

paloalto NETWORKS


paloalto
NETWORKS
the network security company™