IBM Security Systems
Next Generation IPS

Paul Ashley
pashley@au1.ibm.com

Peter Param
pparam@stvincents.com.au

Pulse2012

Meet the Experts. Optimise your infrastructure.

May 31 – June1
Sheraton on the Park Hotel, Sydney

Trademarks and disclaimers

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

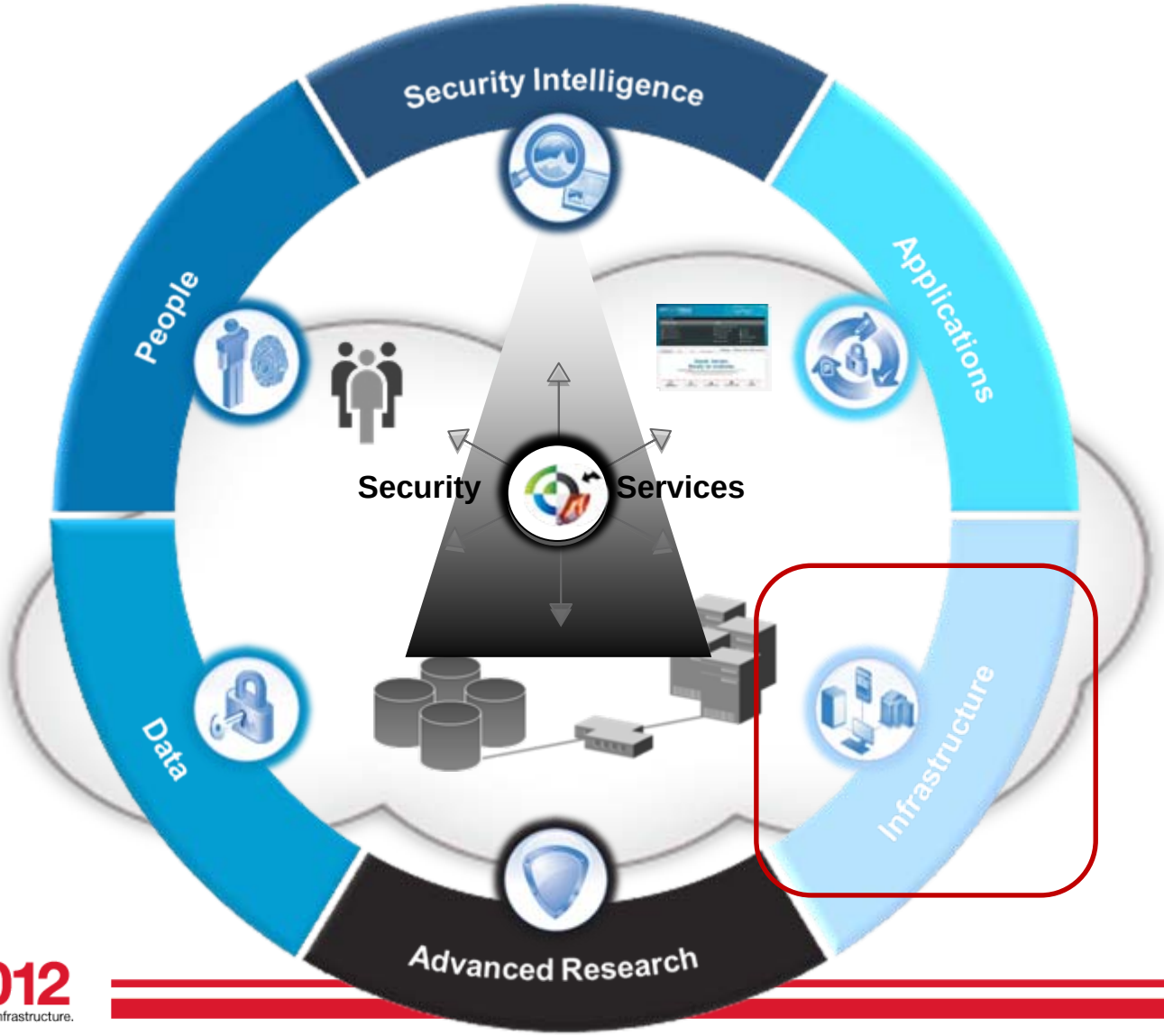
Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.

IBM Security: Delivering intelligence, integration and expertise across a comprehensive framework



IBM Security Network IPS Today

- Balance security and performance of business critical applications
- Address changing threats with limited expertise, resources, and budget
- Reduce cost and complexity of their security infrastructure
- Larger Enterprise/Service Providers require security at network core

IBM Protocol Analysis Modular Technology

Core Capabilities

Unmatched Performance delivering 20Gbps+ of throughput and 10GbE connectivity without compromising breadth and depth of security

Evolving protection powered by world renowned X-Force research to stay "ahead of the threat"

Reduced cost and complexity through consolidation of point solutions and integrations with other security tools

IBM Security Network IPS

	Remote	Perimeter			Core				
Model	GX4004 -200	GX4004	GX5008	GX5108	GX5208	GX7412 -5	GX7412 -10	GX7412	GX7800
Inspected Throughput	200 Mbps	800 Mbps	1.5 Gbps	2.5 Gbps	4 Gbps	5 Gbps	10 Gbps	15 Gbps	20 Gbps+
Protected Segments	2	2	4	4	4	8	8	8	4

What is a Next Generation IPS?

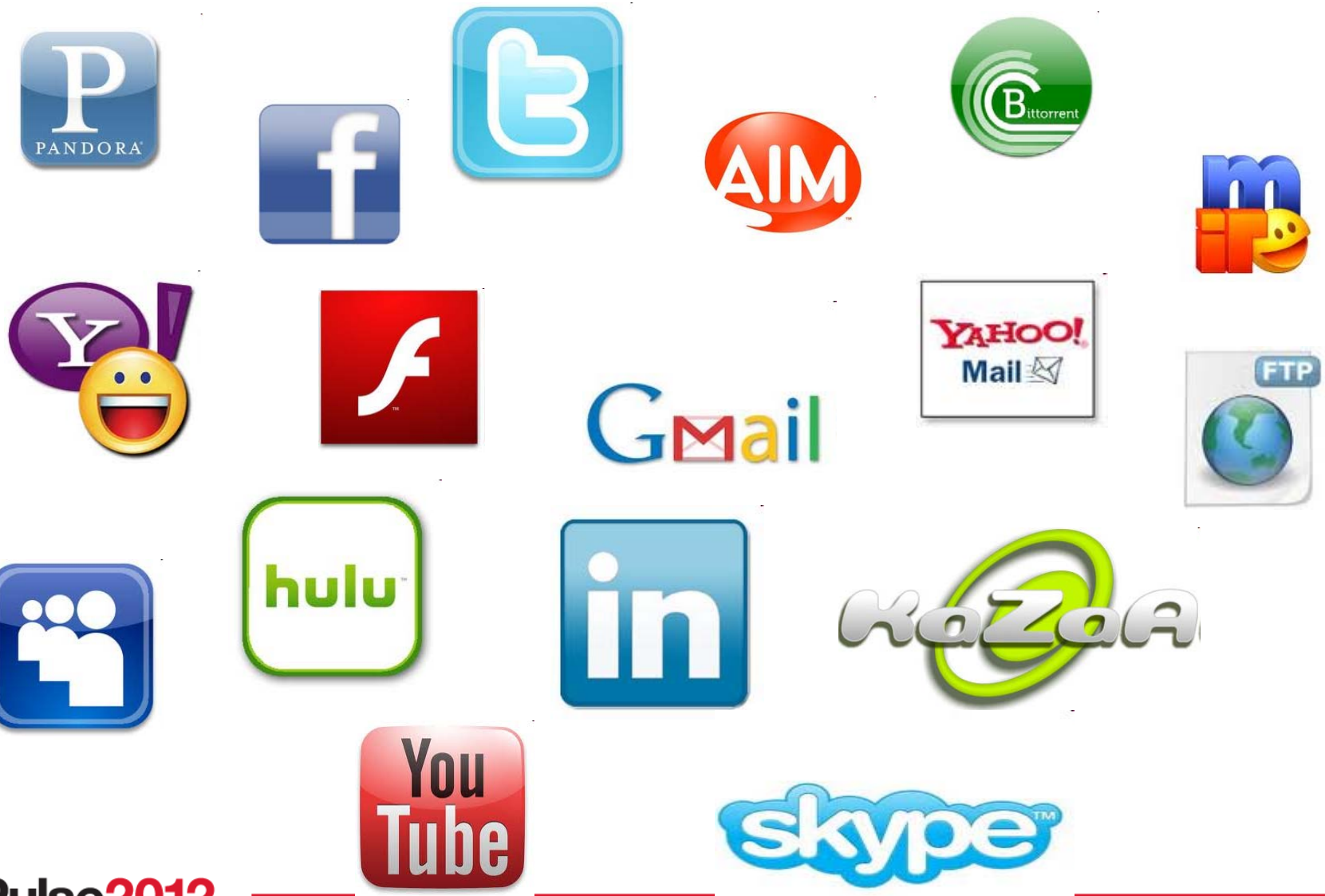
According to Gartner*…

- **Deployed as in-line device –** bump-in-the-wire solution
- **Complete First-generation IPS Capabilities** – vulnerability and threat signatures; Detection and blocking at wire speed; Signature Updates
- **Application Awareness** – Identify & Enforce network security policy at the application layer.
- **Context Awareness** –Use information from sources outside the IPS to make blocking decisions, or to modify the blocking rule base.
- **Agile Engine** – Provide an upgrade path for the integration of new information feeds and new techniques to address future threats.

Network Intrusion Prevention (GX)	❖ Vulnerability & Threat Protection (PAM) ❖ Inline deployment
Next Generation Intrusion Prevention (XGS)	❖ [Application] Protocol Analysis ❖ Content Awareness ❖ Reputation ❖ Application Control ❖ URL Filtering ❖ User Awareness ❖ Administrative Workflows
Next Generation Firewall (NGFW)	❖ Full Firewall Capabilities ❖ Integrated Intrusion Prevention ❖ VPN ❖ Network Malware ❖ Application Awareness

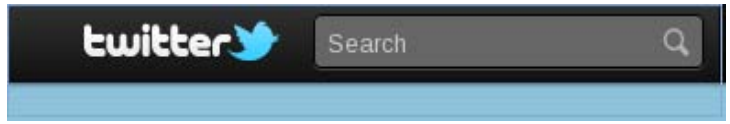
* Defining Next-Generation Network Intrusion Prevention, by John Pescatore and Greg Young, Gartner, G00218641

Consumerisation of the Enterprise



Consumerisation of the Enterprise

- Block completely?
  - Some applications are business relevant
  - Not a good look for employers
- Controlled access
  - Shouldn't the marketing department have unobstructed access to facebook and twitter
  - Perhaps we could let employees read their private Email accounts or Facebook between 12noon and 2pm each day?
    - Limit any private email to text only (not files)
    - Only allow “read” of Facebook
- Shouldn't employees be allowed to use Skype for contacting overseas offices?
  - How to handle “thick” client applications



Controlling Applications

- Some key questions
- How do I identify which applications my enterprise users are using?
- How much bandwidth is being consumed by each of these applications?
- Can I provide different users different application access?
  - Can I control specific application features?
- How do I control and know which web sites users should and shouldn't be accessing?
- How can I use my flow data for a greater understanding of my users?

Controlling Applications

- Firewalls cannot control applications
  - more communication through fewer ports (such as HTTP and HTTPS),
  - fewer protocols,
  - port/protocol-based policy has become less relevant and less effective.
- Applications themselves are actively deceptive
  - Non-standard ports
  - Port hopping and tunnelling
  - Protocol changes
  - Hide within SSL sessions
    - 30% of all applications now run exclusively over SSL
- Need to identify an application that is being deceptive

Controlling Applications

- What we need is convergence of multiple security technologies

- **User based Application Control** =

  Deep Packet Inspection (IPS) +

  Deep Packet Inspection (Application Identification) +

  Web Site Classification +

  User Identity +

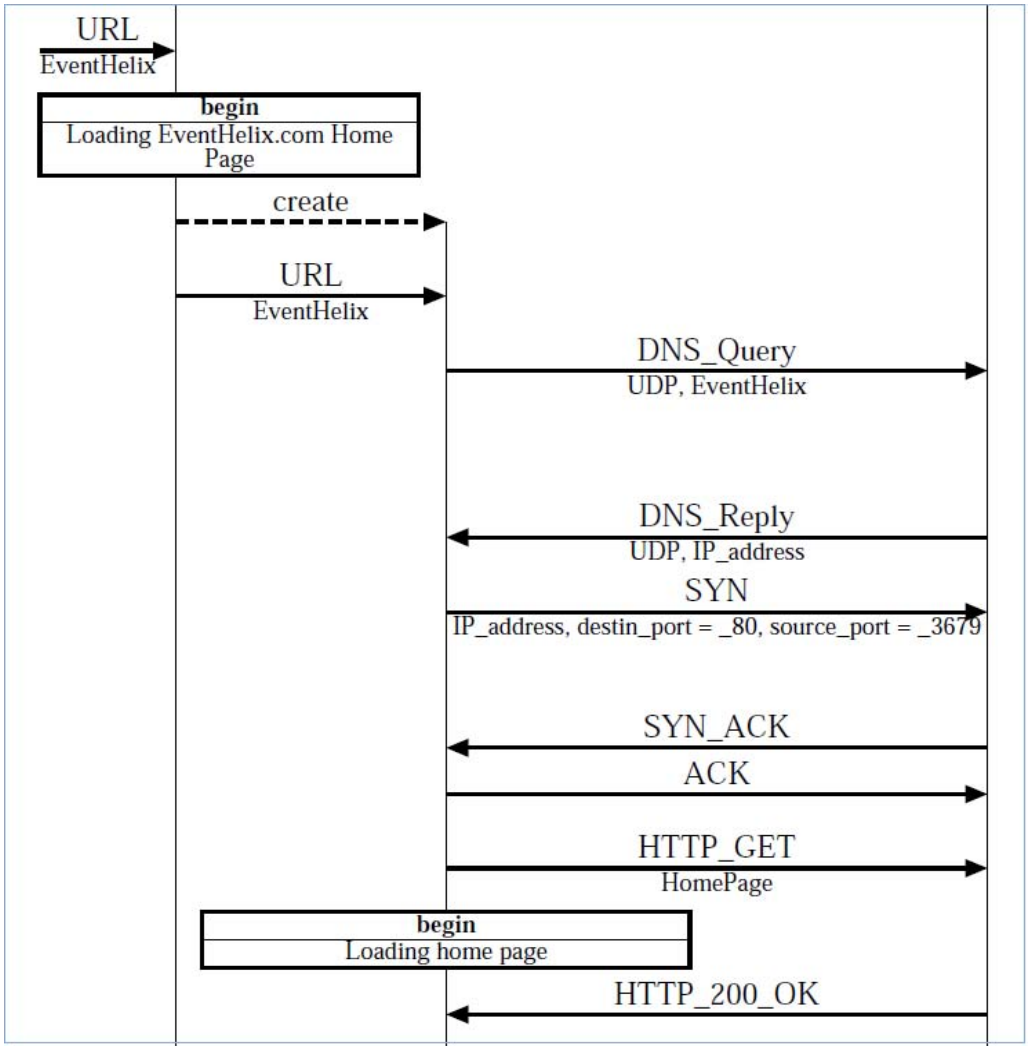
  Access Control +

Deep Packet Inspection (DPI)

- IBM has a highly respected DPI engine
  - Protocol Analysis Module (PAM)
  - Basis of first generation IPS products
  - Vulnerability and Signature based
  - Updates via eXPress Updates (XPUs bi-monthly)
  - Developed over the course of 14 years to a level of accuracy and intelligence that is unmatched.
- IBM has a long history of application identification
  - Experience in classifying traffic based on content rather than ports.
  - Today PAM is capable of identifying and understanding the state of over 300 non-web applications and the list is quickly growing

- A good DPI engine is the first ingredient of any application identification solution.

Deep Packet Inspection



- Application identification means following a sequence of packets before deciding which application is being used.

Web Classification

- Web sites create other risks

- Web sites are sources of malware / botnets
  - user visits an infected site
  - the malicious code (embedded Javascript, XSS attack, etc.) will be executed
  - the malware downloaded
  - may turn your client machine into a bot.

- Need also to protect the enterprise from content
  - Pornography
  - Gambling
  - Hate Sites
  - ...

Web Classification

- IBM has the most extensive web classification engine and infrastructure in the industry
  - Developed over the course of 13 years.
  - The web database has over 65 Million classified URLs in 68 categories.
  - We've analyzed over 15 Billion pages, we touch every public site in the world every few hours to every month, dynamically.
- 68 Categories
  - Criminal Activities
  - Drugs
  - Entertainment / Culture
  - Finance / Investment
  - Games / Gambling
  - General Business
  - ....

Web Classification

- Crawlers collect binary and text data from the Internet
  - 24 hours a day on 365 days, which adds up to 200 million pages each month
  - Every day, customers receive updates
- Learn feature in client products
- Analysis result
  - List of categories the URL belongs to
  - Web application and action identification
    - ApplicationID / ActionID
    - gmail/upload, googledocs/download, hotmail/sendmail, …
- A good Web classification engine is second ingredient of any application identification solution

IBM Security Network Protection

Home
Appliance Dashboard

Monitor
Analysis and Diagnostics

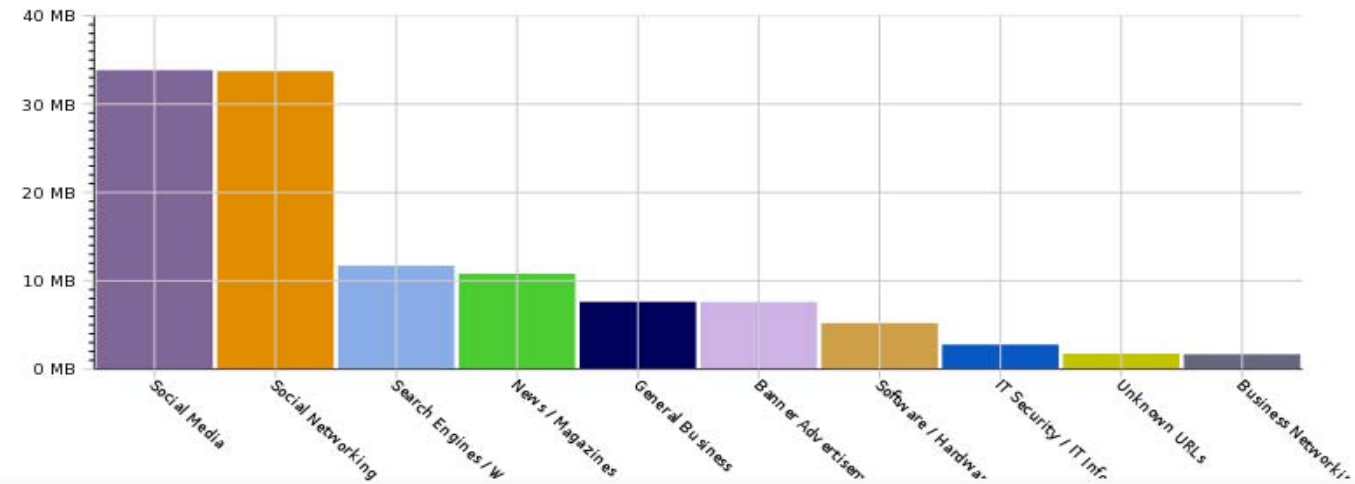
Secure
Policy Configuration

Manage
System Settings

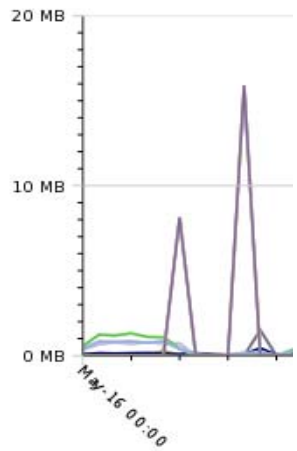
Web Traffic by Category

Date Range: 1 Day **Chart Type:** Columns and Lines

Total Bytes



Total Bytes Over Time



Traffic Details [Wed May 16 2012 00:00:30] .. [Thu May 17 2012 00:45:30]

Web Category
Social Media
Social Networking
Search Engines / Web Catalogs / Portals
News / Magazines
General Business
Banner Advertisements
Software / Hardware
IT Security / IT Information
Unknown URLs
Business Networking

User Identity and Access Control

- Control of users to applications is fundamentally an Identity and Access (I&A) Management problem

- This is about users and not IP addresses
  - First generation IPS's are typically unconcerned with users
  - Only understand low level protocols

- IBM Security Systems has been protecting the fortune 1000 with comprehensive I&A for over 15 years.
  - IBM Security Policy Manager, IBM Security Identity Manager, IBM Security Access Manager, IBM Security Directory Server …

- How to combine a First Generation IPS with I&A?

User Identity and Access Control

- The user must be first authenticated to allow control of their access
  - Integrate with existing enterprise directories e.g. Active Directory, LDAP Servers
  - Allow creation of Users “on the box” (for testing / smaller businesses)
- Allow definition of rule policy based on Users or Groups
  - Allow members of the marketing group unrestricted access to Facebook

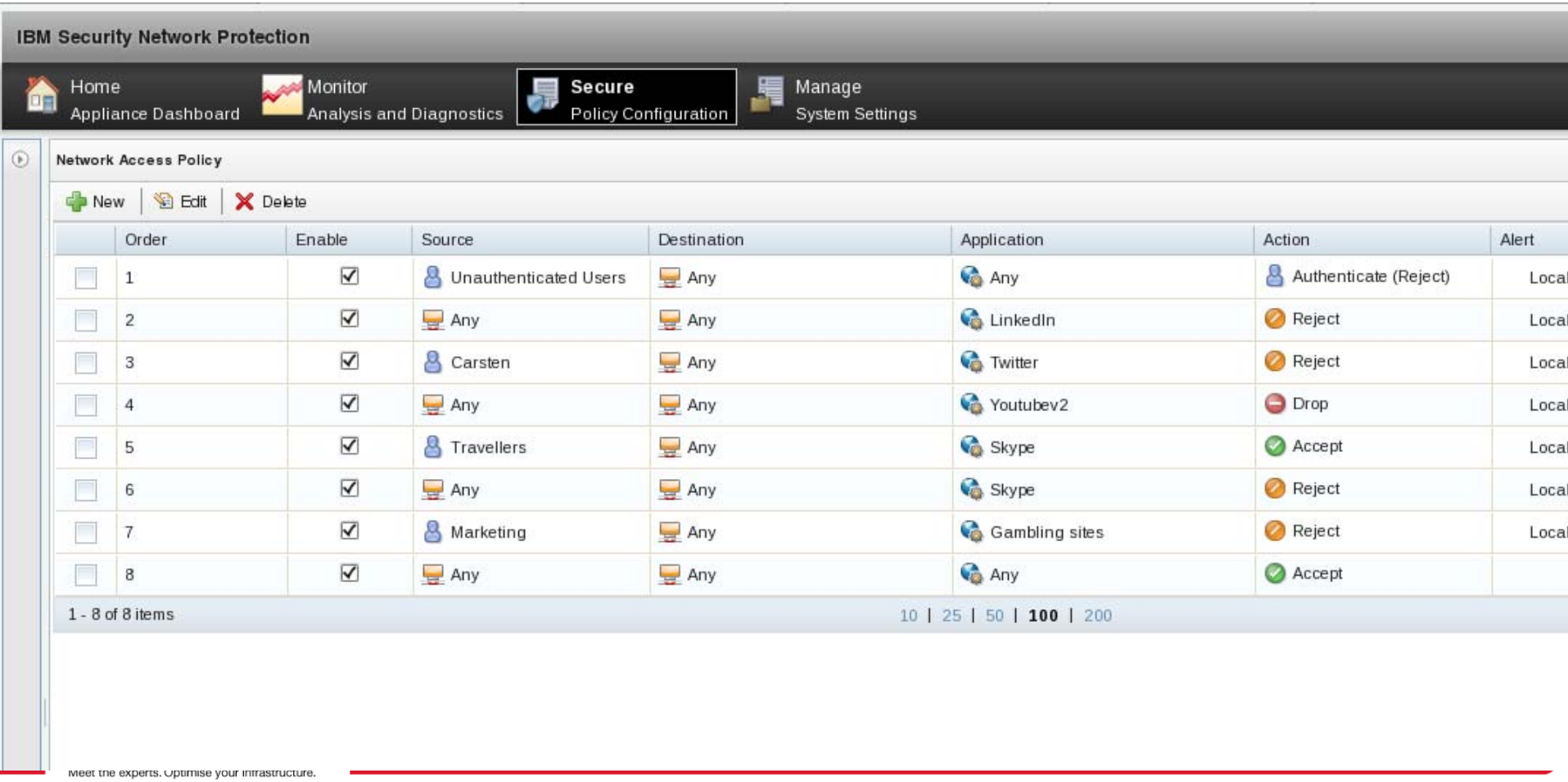
Leverage techniques for User to IP address relationship

- web re-direction (web applications)
- captive portal (non-web applications)
- Passive authentication (notice from trusted third party such as Active Directory login)

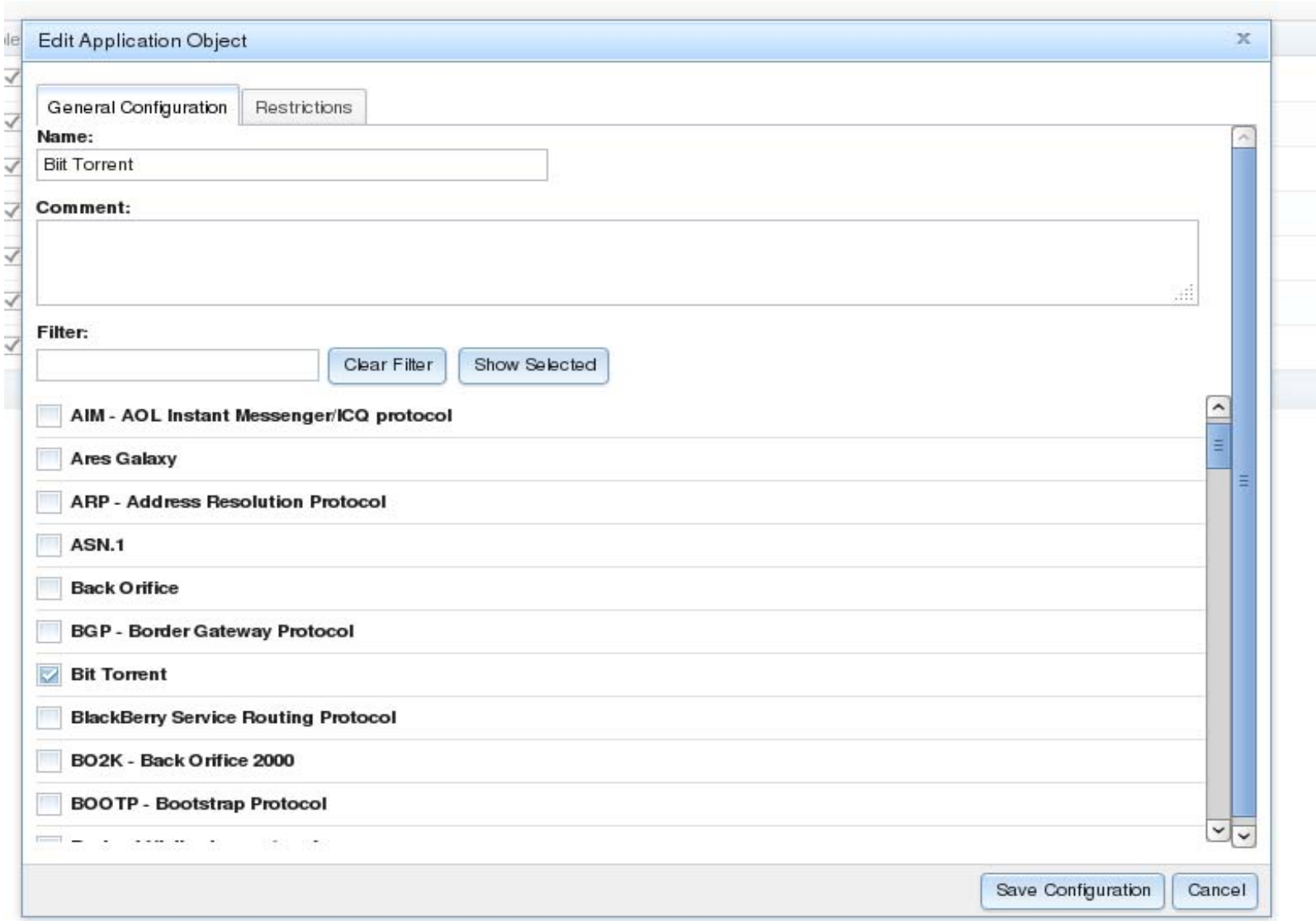
User Identity and Access Control are a fundamental ingredients of user based application control

User Identity and Access Control

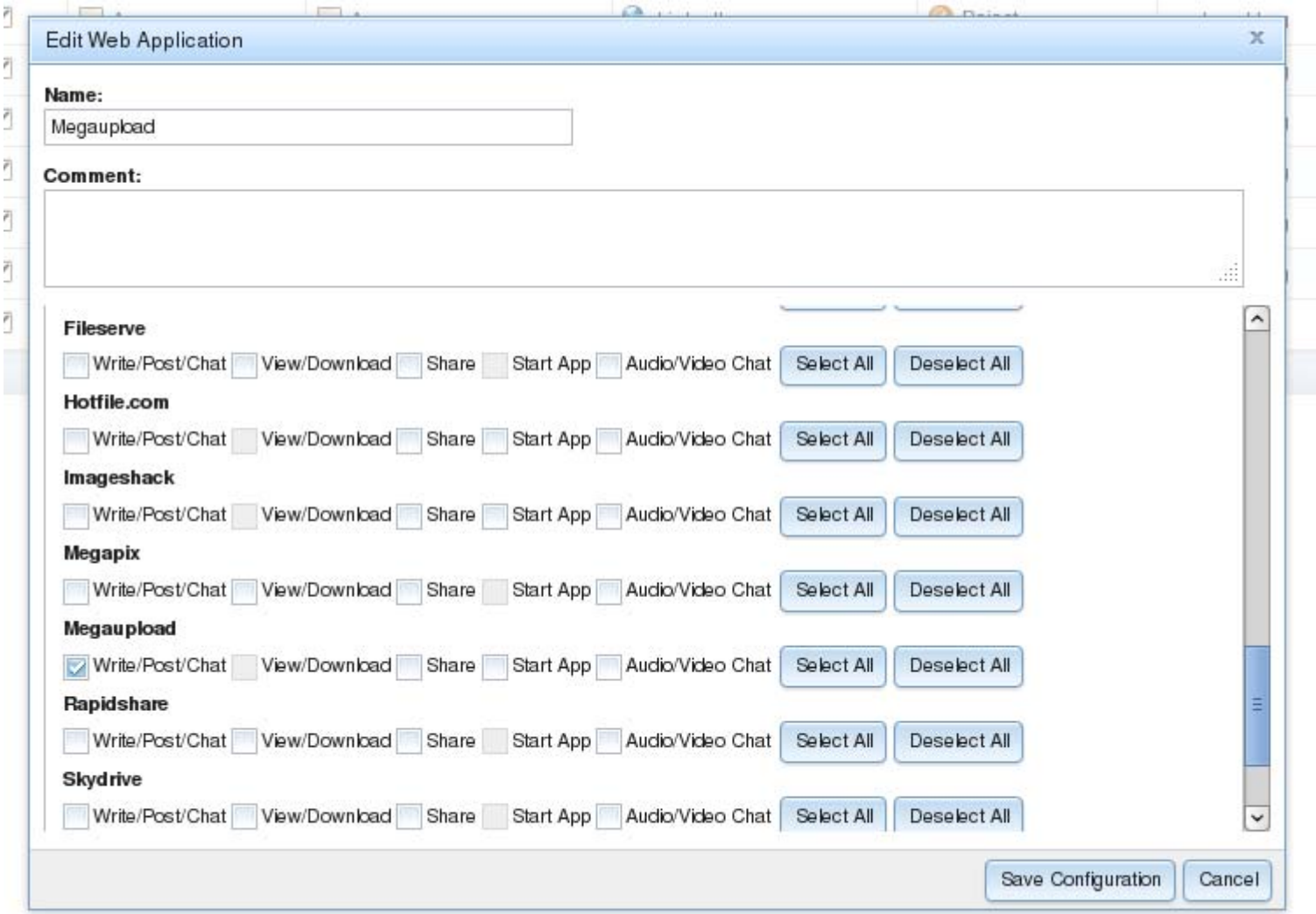
Access Control Policy is “firewall style”
Processing stops when first rule matches



Access Control



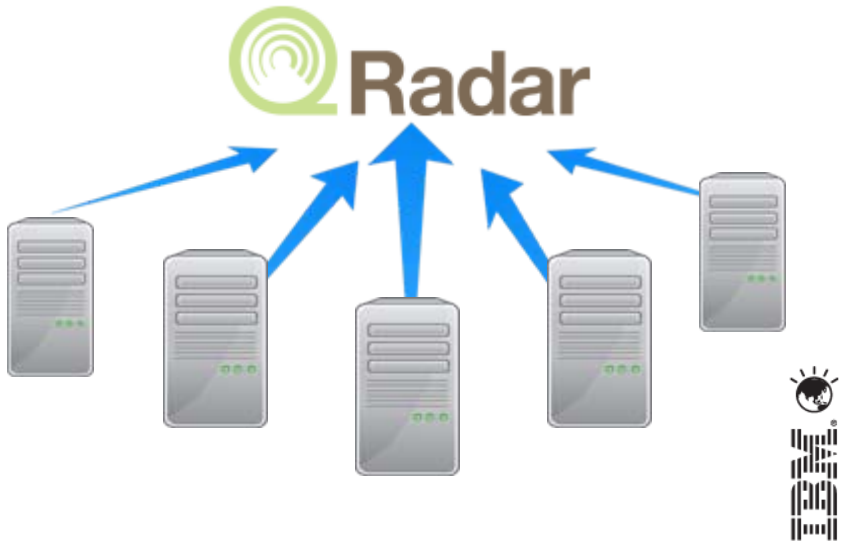
Access Control



Exporting of Flow Data

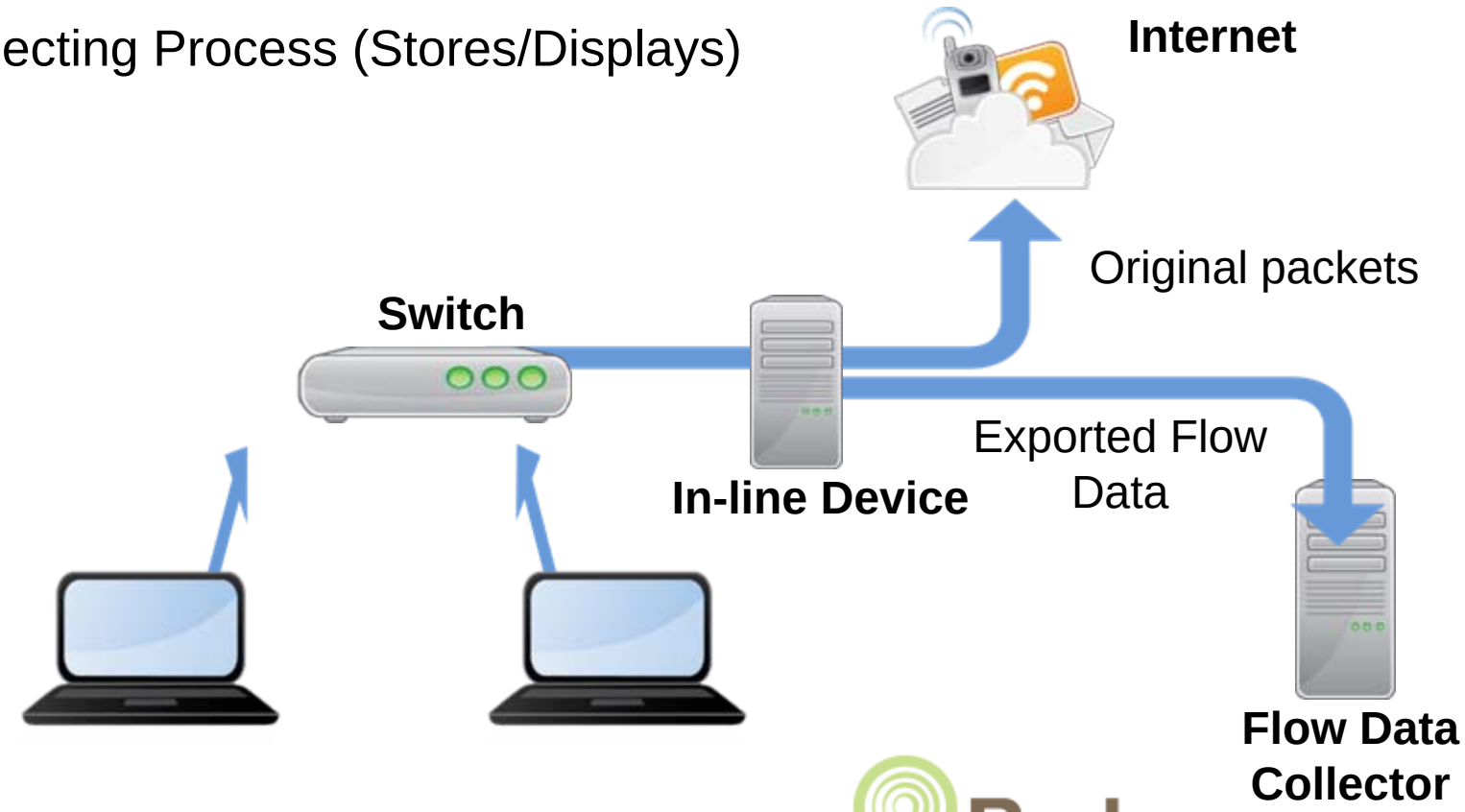
- An appliance can only store so much flow information
  - Typically around 20G only
  - This is summary data only
- There is a requirement to export flow data off the appliance to a “collector”
- Use standard IPFIX data
- Proposal: Enriched security by adding flow attributes
  - User
  - Application
  - Categories

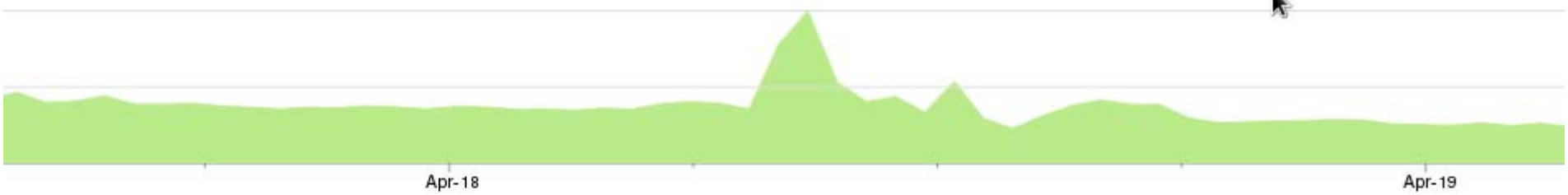
Central point
Flow Data traffic



Exporting of Flow Data

- Observation / Metering Process (Generates)
- Exporting Process (Pushes)
- Collecting Process (Stores/Displays)





Update Details

(Hide Charts)

Storage Time ▼	Source IP	Source Port	Destination IP	Destination Port	Source Bytes	Destination Bytes	Total Bytes	Source Packets	Destinati Packets	P
07:37	192.168.115.159	58108	9.17.136.83	1533	105 (C)	105 (C)	210	2	2	
07:37	192.168.115.155	49394	9.17.136.77	1533	216 (C)	168 (C)	384	4	3	
07:37	192.168.115.155	56917	216.218.132.82	80	1 193 (C)	3 787 (C)	4 980	9	9	
07:37	192.168.115.155	56915	216.218.132.82	80	1 307 (C)	6 662 (C)	7 969	11	11	

QRadar - Network Activity - Mozilla Firefox

File Edit View History Bookmarks Tools Help

QRadar - Network Activity

192.168.115.85 https://192.168.115.85/console/qradar/jsp/QRadar.jsp

Google

Welcome, admin [logout]

Dashboard | Offenses | Log Activity | Network Activity | Assets | Reports | Admin

QRadar

System Time: 15:09 | Preferences | Help

Search... ▾ Quick Searches ▾ Add Filter Save Criteria Save Results Cancel False Positive Rules ▾ Actions ▾ Quick Filter...

Viewing flows from 2012-03-26 15:09:00 to 2012-04-02 15:09:00 View: Select An Option: Display: Custom

Grouping By:

UserName (custom)

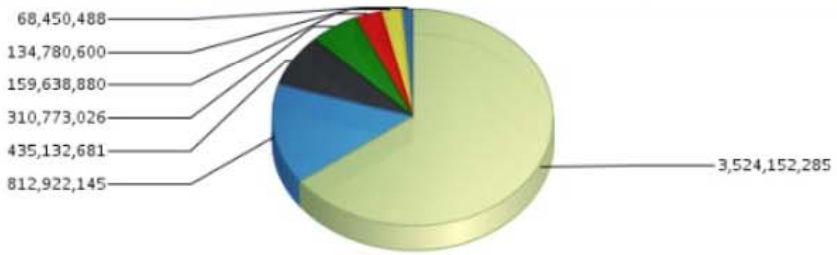
Using Search: NX-UserName

Completed

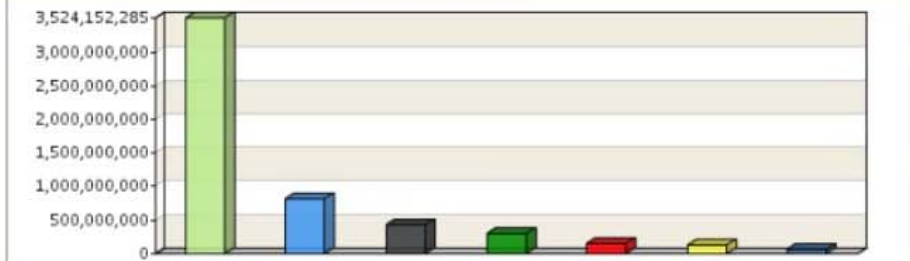
Current Statistics

Total Results	1 619 442	Compressed Data Files Searched	0 (0B Total)	Duration	17s 397ms
Data Files Searched	19 818 (896.8 MB Total)	Index File Count	0 (0B Total)		

Top 10 UserName (custom) Results By Total Bytes (Sum)



Top 10 UserName (custom) Results By Total Bytes (Sum)



(Hide Charts)

UserName (custom)	Flow Type (Unique Count)	First Packet Time (Minimum)	Storage Time (Minimum)	Source IP (Unique Count)	Source Port (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Source Bytes (Sum)	Destination Bytes (Sum)	Total Bytes (Sum) ▾	Sc Pa (S
kman	Standard Flow	07:01	15:09	Multiple (2)	Multiple (158...	Multiple (561)	Multiple (21)	3 095 556 407	428 595 878	3 524 152 285	
Unauthenticated Users	Standard Flow	15:13	15:12	Multiple (30)	Multiple (28 2...	Multiple (167)	Multiple (98)	370 603 369	442 318 776	812 922 145	
craig	Standard Flow	06:06	15:09	192.168.115.68	Multiple (148...	Multiple (592)	Multiple (10)	54 041 053	381 091 628	435 132 681	
johnwcrt@au1.ibm.com	Standard Flow	11:42	11:43	Multiple (2)	Multiple (17 7...	Multiple (150)	Multiple (11)	68 037 573	242 735 453	310 773 026	
john	Standard Flow	07:31	15:09	Multiple (2)	Multiple (8 132)	Multiple (131)	Multiple (10)	34 762 426	124 876 454	159 638 880	

Displaying 1 to 7 of 7 items (Elapsed time: 0:00:00.063)

Find: 155 Previous Next Highlight all Match case

QRadar - Network Activity - Mozilla Firefox

File Edit View History Bookmarks Tools Help

QRadar - Network Act

192.168.115.85

Welcome, admin [logout]

Dashboard Offenses Lo

Search... ▾ Quick Searches ▾

Display: Custom

erName (custom) Results By

2,285
0,000
0,000
0,000
0,000
0,000
0,000
0

Unauthenticated U
simon

Flow List - Mozilla Firefox

192.168.115.85 https://192.168.115.85/console/qradar/jsp/ArielSearchWrapper.jsp?url=do%2Fariel%2FarielSearch%3FappName%3DSurve

Search... ▾ Quick Searches ▾ Add Filter Save Criteria Save Results Cancel False Positive Rules ▾ Actions ▾ Quick Filter...

Viewing flows from 2012-03-26 15:09:00 to 2012-04-02 15:09:00 View: Select An Option:

Display: Custom

Grouping By:

Applications ID

Completed

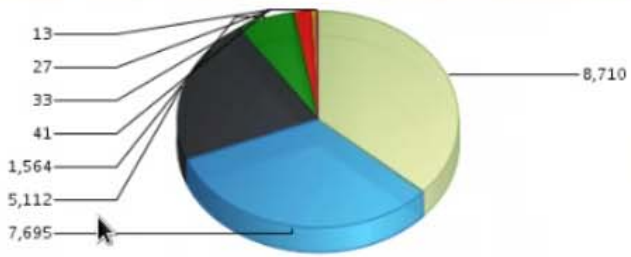
Current Filters:

UserName is kman (Clear Filter)

Current Statistics

Total Results	23 816	Compressed Data Files Searched	0 (0B Total)	Duration	4773ms
Data Files Searched	19 816 (696.6 MB Total)	Index File Count	0 (0B Total)		

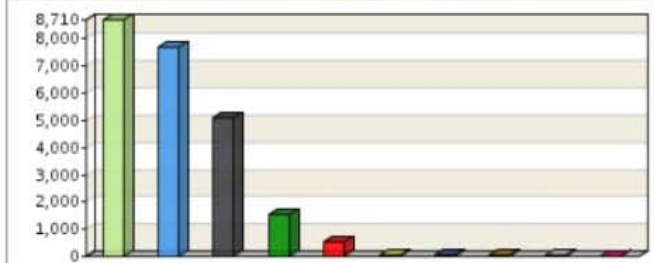
Top 10 Applications ID Results By Count



Legend

0x20000075 0x20000000 0x20000043
0x20000060 0x20000032 0x200000b5
0x200000E3 0x40010000 0x40050000
0x2000006a

Top 10 Applications ID Results By Count



Legend

0x20000075 0x20000000 0x20000043
0x20000060 0x20000032 0x200000b5
0x200000E3 0x40010000 0x40050000
0x2000006a

(Hide Charts)

First

Displaying 1 to 20 of 20 items (Elapsed time: 0:00:00.069)

rce Port nique ount)	Destination IP (Unique Count)	D Po									Count
ple (15 8...	Multiple (561)	Mu									23 816
ple (28 2...	Multiple (167)	Mu									1 513 168
ple (14 8...	Multiple (592)	Multiple (10)	54 041 053	381 091 628	435 132 681	416 659	404 682	821 341	Multiple (2)	qradar	qradar:Johns...	Multiple (19)	27 551
ple (17 7...	Multiple (150)	Multiple (11)	68 037 573	242 735 453	310 773 026	398 093	340 279	738 372	Multiple (2)	qradar	qradar:Johns...	Multiple (12)	32 650
ple (8 132)	Multiple (131)	Multiple (10)	34 762 426	124 876 454	159 638 880	192 579	172 320	364 899	Multiple (2)	qradar	qradar:Johns...	Multiple (11)	12 473

Displaying 1 to 7 of 7 items (Elapsed time: 0:00:00.063)

Find: 155 Previous Next Highlight all Match case

St Vincents Deployment

Endpoint System Life-cycle and Power Management – SV&MHS

❑ St Vincents & Mater Health Sydney

St Vincents & Mater Health Sydney (SV&MHS) is the NSW-based arm of St Vincent's Health Australia which, together with its partners, is one of Australia's leading Catholic not-for-profit diversified healthcare providers with more than 6,500 employees working in healthcare, management and support services.

As a major provider of public and private health and aged care services, the group's campuses include:

- St Vincent's Hospital Sydney Limited
- Sacred Heart Hospice Limited
- The Mater Hospital
- St Vincent's Private Hospital
- St Vincent's Clinic
- St Joseph's Hospital

Endpoint System Life-cycle and Power Management – SV&MHS

❑ Our Challenges

✓ Diverse user communities and needs, including support for cutting-edge medical technologies

✓ Malware security risk management and mitigation

✓Energy and PC Computing cost management yet with highly flexible schedules.

✓Patch and asset license compliance management to achieve budget parameters

✓ Responsibility for endpoint workstations

St Vincents – Plans for Deployment

- Appliance is placed initially in a “monitoring only” mode
- Understand:
  - Which applications are being used
  - How much bandwidth is being used by the applications
  - Who is using the applications
- Initially this mandates some automated IP address to User ID mapping
- Allow this to run for period of time
- Create an initial rule set
- Then convert to “enforcement” mode

St Vincents – Details of Deployment

- Deployment
  - On production network
  - Two in-line pairs
    - Wireless and Wired
  - > 1000 users
  - > 25Mbits/s constant throughput
  - Custom approach to Passive Authentication using RADIUS/LDAP and IBM Security Directory Integrator (ISDI) to identify users
- Learnings
  - Bandwidth consumption
  - Users
  - Applications
  - Categories

St Vincents – Next Steps of Deployment

- Creation of policy
  - Use LDAP groups to control access
- Flow Data Export to QRadar
  - IPFIX data with user, application
  - Analyze individual flows
  - Correlation with SIEM data

Thank You- Q&A