Pulse2011
Optimizing the World's Infrastructure

The Convergence of Identity, Access and Threat Management

Dr Paul Ashley
pashley@au1.ibm.com

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 pricesand 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.

Agenda

- Who am I?
- Consumerisation of the Enterprise
- Controlling Applications
- Threat Management
- Identity and Access Context
- Creation of Policy
- High Speed Appliance Based Solutions
- X-Force Research
- Summary

Who am I?

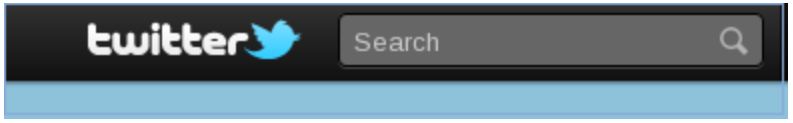
- Australia Development Laboratory
  - Gold Coast Security Lab
- 17 years security experience
  - Last 12 for IBM (USA, Australia)
- Worked on security projects in USA, Europe, Middle East, Asia, Australia
  - Identity and Access Management
  - Added SOA Security
- Now focussed on product development
  - Internet Security Systems
  - Appliance based Network Protection / X-Force Research

Consumerisation of the Enterprise

- Users expect to use any application (web or otherwise) at both home and work
  - "Without it my creativity, productivity is affected"
- There is a push toward more complex web applications
  - With AJAX more responsive web applications
  - Google Apps and Microsoft Office Live are examples of the newest generation of web applications

Consumerisation of the Enterprise

- Some of the applications are business relevant
- Shouldn't the marketing department have access to facebook or twitter?
- Perhaps we could let employees read their private email accounts between 12noon and 2pm each day?
  - But perhaps we should limit any private email to text only (not files)
- Shouldn't they be allowed to use Skype for contacting our overseas offices?



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
- 25% of all applications now run exclusively over SSL
- Need to identify an application that is being deceptive

Controlling Applications

- Web sites and Spam 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.
  - Spam emails are also a common way to supply malware to the clients computer
    - .exe, .pdf, .zip files commonly used
- Need also to protect the enterprise from content
  - Pornography
  - Gambling
  - Hate Sites

Controlling Applications

- Hacking is now a business
  - Government, criminals, mafia, commercial espionage
  - Examples: China – Google, Iran – StuxNet, Twitter attacks
- Enterprise gateways often at a strong security level
  - Attackers now may leave those alone and try other techniques
- Attack the user's client
  - Threats are focussing on getting vulnerable users to install malicious executables that attempt to avoid detection
  - Laptop, iPad, Android … as entry point
  - Stepping stone to get “inside” the enterprise
  - Sometimes starting point of an advanced persistent threat

Controlling Applications

- Enterprises are also finding use of network bandwidth is growing quickly
- Funding these bigger network pipes is expensive
- Enterprises need to know
  - Which applications are consuming my network bandwidth?
  - Which users are using those applications?
  - How do I to limit bandwidth consumption by application?

•Examples include the ability to

–allow Skype use but disable file sharing within Skype

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 limit bandwidth consumption by application and user?
- 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 do I stop data being leaked from my organization?
- How do I inspect traffic inside SSL pipes - both inbound and outbound?

Controlling Applications

- What we need is convergence of multiple security technologies

- **User based Application Control** =
  Threat +
  Identity +
  Access +
  (High Speed Appliances)

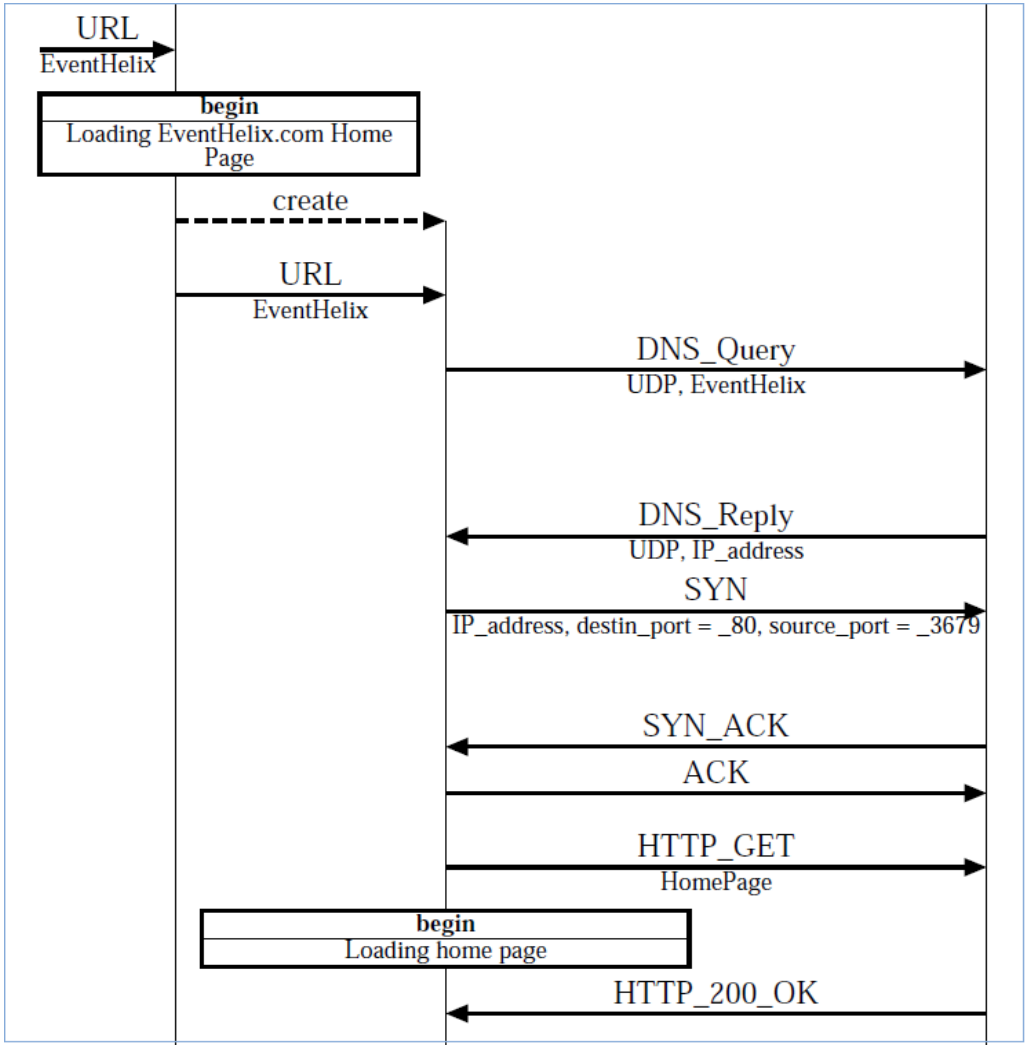
- IBM has more than a decade of experience in <u>all</u> four areas

Threat Management

- DPI/DSI - Deep packet and Deep Session Intelligence
  - ISS have a highly respected DPI/DSI engine
    - Protocol Analysis Module (PAM).
    - Developed over the course of 14 years to a level of accuracy and intelligence that is unmatched.
  - ISS have a long history of application identification experience in classifying traffic based on content rather than ports.
    - Today's PAM is capable of identifying and understanding the state of over 260+ web and non-web protocols and applications, and the list is quickly growing

- <u>A good DPI/DSI engine is the first ingredient of any application identification solution.</u>

Threat Management



- Application identification means following a <u>sequence of packets</u> before deciding which application is being used.
- Compare with traditional firewall which may need just <u>one</u> packet

Threat Management

- What is the Requirement for DPI?
  - Recent surveys of enterprises have shown 100s of applications (web and non-web) are in use
  - Extensive Library of Application Decodes
    - Social Networking (Facebook, LinkedIn, Twitter, YouTube ..)
    - Productivity Tools (Google Docs, Microsoft Live ...)
    - VoIP (Skype, Google Talk ...)
    - File Sharing (MegaUpload, BitTorrent ...)
    - Instant Messaging (AIM, Facebook, Yahoo …)
    - and numerous more
  - Categorize by
    - Application category (Social Networking, File Sharing ..)
    - Application (Facebook chat, Skype chat)
    - Destination (Geo-location)
    - Content (File, text only)

Threat Management

- Web classification engine
  - Many web applications can also be identified by URL/IP address being accessed
  - ISS 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.

- <u>A good Web classification engine is second ingredient of any application identification solution</u>

Threat Management

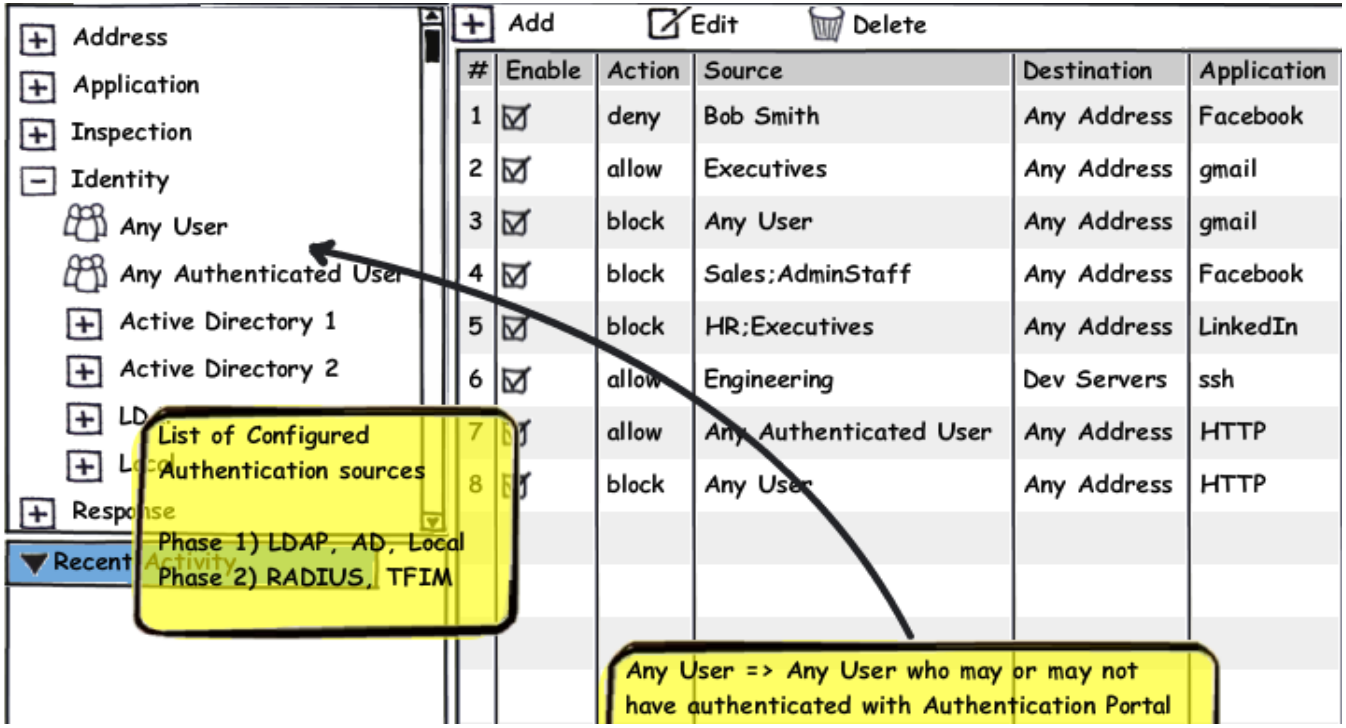
- ISS Web Classification Engine
  - Crawlers collect binary and text data from the Internet
    - 24 hours a day on 365 days, which adds up to 200 million pages each month
    - Every day, customers receive updates
  - Analysis result
    - List of categories the URL belongs to
    - ApplicationID / ActionID if applicable
      - gmail/upload, googledocs/download, hotmail/sendmail, ...

Identity and Access Context

- Identity and Access Context
  - Control of users to applications is fundamentally an I&A problem
  - This is about users and not IP addresses
    - Threat management is typically unconcerned with users
  - Tivoli security has been protecting the fortune 1000 with comprehensive I&A for over 15 years.
    - Tivoli Security Policy Manager, Tivoli Identity Manager, Tivoli Access Manager, Tivoli Federated Identity Manager, Tivoli Directory Integrator, Tivoli Directory Server ...

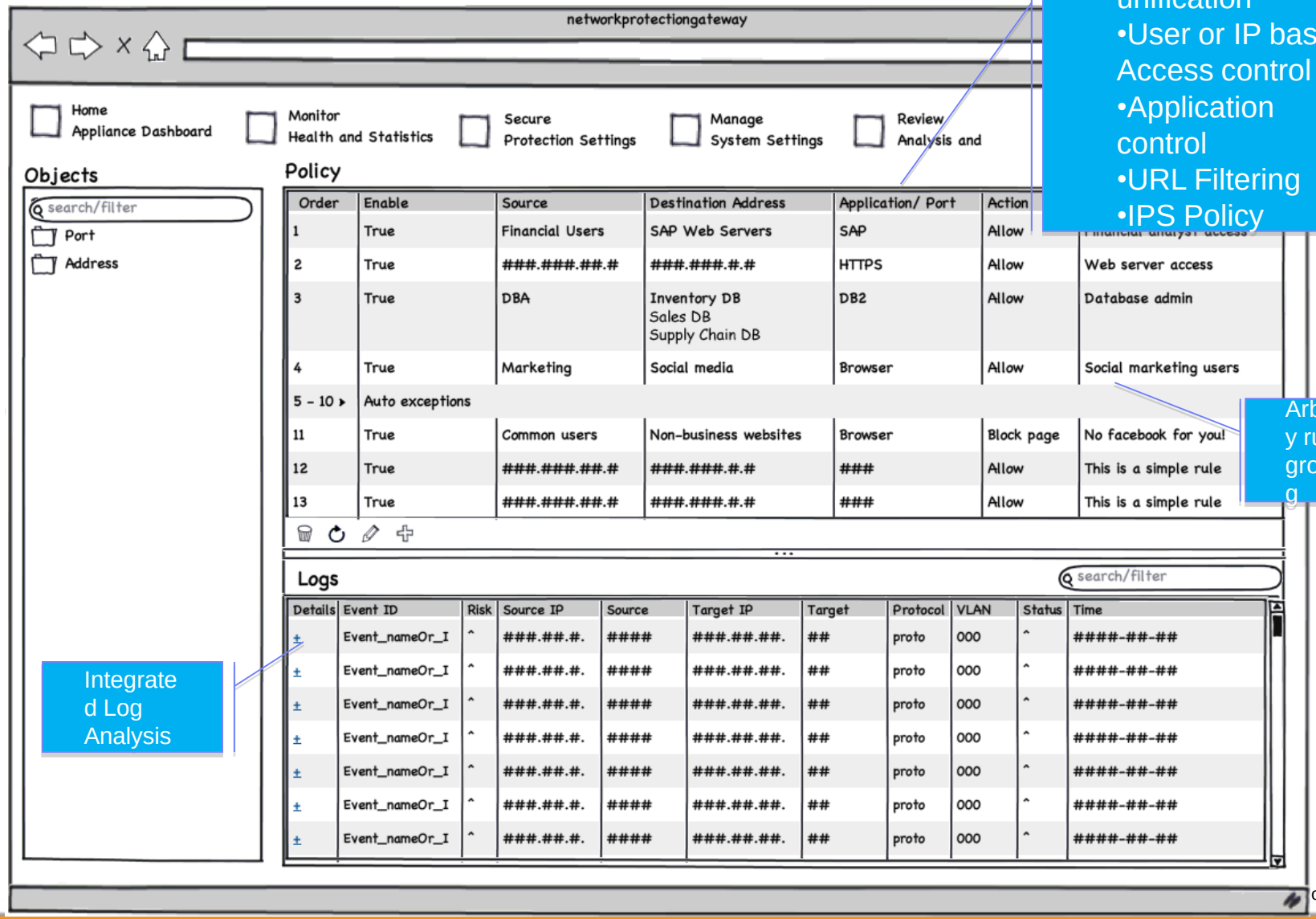
- Identity and access context is a fundamental ingredient of user based application control

Identity and Access Context



- Desired style is to write a set of rules
  - Allow Marketing to access Social Media Applications
  - Allow AnyUser to access Facebook between 12pm and 1pm
  - Allow AnyAuthUser to access Banking without decryption
  - Allow AnyAuthUser to access Webmail with SSL decryption

Identity and Access Context



Firewall-like unification
- User or IP based Access control
- Application control
- URL Filtering
- IPS Policy

Arbitrary rule grouping

Integrated Log Analysis

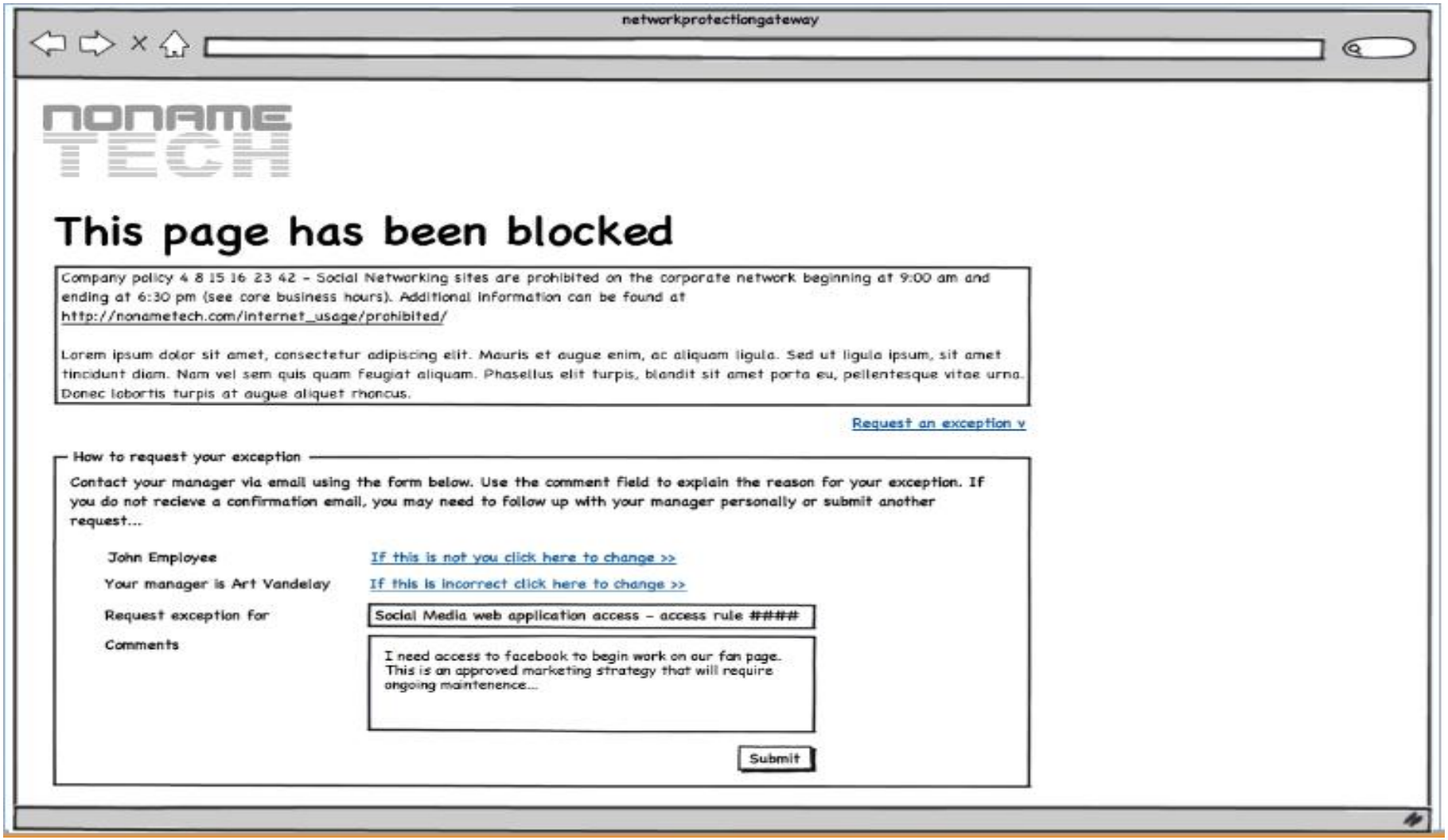
Identity and Access Context

- The user must be first authenticated to allow control of their access
  - Integrate with existing directories e.g. Active Directory, Tivoli Directory Server, RADIUS
  - Allow creation of Users “on the box”
- Allow definition of rule policy based on Users or Groups
- Leverage techniques for User to IP address relationship
  - web re-direction (web applications)
  - captive portal (non-web applications)
  - directory agent integration (infer from log)
  - client agent technology (most secure using IPSec or SSL)

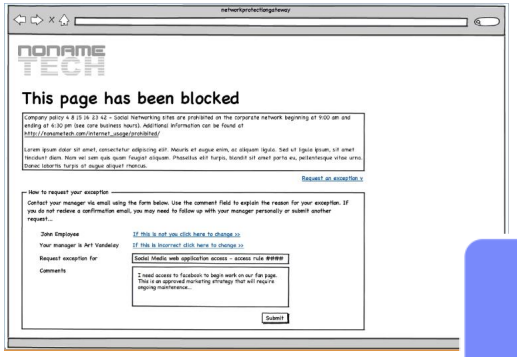
Creation of policy

- Appliance may be placed initially in a “monitoring only” mode
- Let the enterprise understand:
  - Which applications are being used
  - How much bandwidth is being used by the applications
  - Who is using the applications
    - This mandates some automated IP address to User ID mapping
- Allow this to run for several months
- Create an initial rule set
- Then convert to “enforcement” mode
  - The rule changes are then based on a request basis

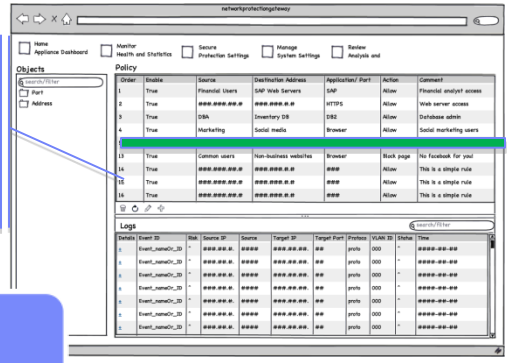
Creation of policy



Creation of policy



Exceptions Grouped above the rule that blocked the user. Business reason captured in comments!



User Block Page

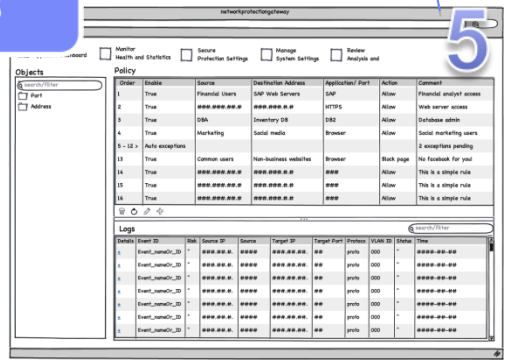
Creates Exception Request

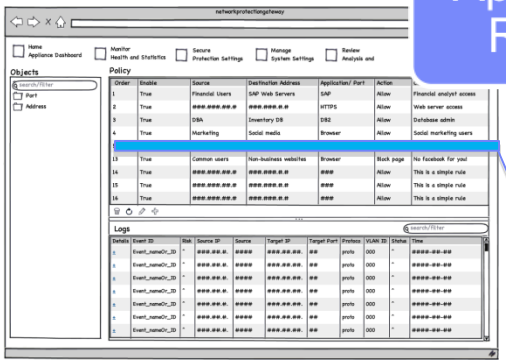
Email Notifications

Administrator views active requests

Exceptions Approved in Rule List

Admin sees how many user exceptions to process





Approved Exceptions are logically grouped in collapsed exception rows

High Speed Appliance Based Solutions

- Appliance Based Solutions
  - ISS has over 14 years experience in engineering specialized high-speed network security applications
    - aimed at providing intelligence and protection.
    - without sacrificing performance or scalability.
  - Today, ISS's Network Security products provide deep packet inspection
    - at speeds ranging from 23-40G,
    - easily more than double most competitors.
  - <u>Providing reliable, high-speed security intelligence through appliances is a basic ingredient of application control</u>

High Speed Appliance Based Solutions

GX7800

- Hardware configuration
  - IBM Industrial Design
  - FIPS Ready
  - Leverages Advantech platform
  - Solid State Drives (all future)
  - HIGH port density in supported network interfaces: copper, sfp(1GBe fiber), sfp+(10GBe fiber)
  - Tool-less rack mount installation
  - Health monitoring and reporting over SNMP

X-Force Research

The mission of the IBM X-Force® research and development team is to:

- Research and evaluate threat and protection issues
- Deliver security protection for today's security problems
- Develop new technology for tomorrow's security challenges
- Educate the media and user communities

X-Force

X-Force Research with IBM Managed Security Services

15B analyzed Web pages & images

40M spam & phishing attacks

54K Documented vulnerabilities

Provides Specific Analysis of:

- Applications
- Vulnerabilities & exploits
- Malicious/Unwanted websites
- Spam and Phishing
- Malware
- Other emerging trends

Summary: User based application control

- The enterprise has been “consumerised”
  - Users expect to use any application (web or otherwise) at both home and work
  - Skype, Facebook, Twitter, LinkedIn, GoogleDocs ..
- Application identification requires threat management technologies (deep packet inspection across any port/protocol)
- User based application control requires the additional technologies from identity and access
- Require speeds from specially built appliances
- IBM brings more than a decade of experience in all four areas as well as high speed appliance based solutions
- All backed by IBM's premier security research X-Force organization

Questions?