Dell Security
Next-Generation Firewalls

Agenda

- Evolution of Security Threats
- Next-Generation Firewall Features
- Multi-Core, Parallel Processing
- Reporting Tools
- Industry Reports
- Demo
- Q&A

The security threat continues to evolve

Notoriety

- Hackers used to just want their name in lights
- Usually an individual operating by oneself

Money-making business

- All aspects of a "normal" business exist
- Social media and virtual era aid this business plan

Strategic, well-planned attacks

- Highly coordinated & motivated… will keep at it
- Well-funded

The future

?

Vulnerabilities Will Continue to Persist

Vulnerabilities in the software everyone uses everyday …

It's Human Nature …

- Programmers make mistakes
- Malware exploits mistakes

LANDesk ThinkManagement File Deletion (April 27, 2012)

New ZBot variant discovered in the wild (Apr 26, 2012)

IBM Tivoli ActiveX Buffer Overflow (April 20, 2012)

Fire Safety emails lead to Gamarue Worm (Apr 18, 2012)

AryaN Botnet analysis - Part 2 (April 13, 2012)

Zeus Wire Transfer targeted attacks (April 12, 2012)

Microsoft Security Bulletin Coverage (April 10, 2012)

Stiniter Android Trojan uses new techniques (Mar 28, 2012)

AryaN IRC Botnet discovered in the wild (April 5, 2012)

Oracle JRE Sandbox Restriction Bypass - Flashback Trojan (Apr 5, 2012)

Microsoft Security Bulletin Coverage (March 14, 2012)

IBM Tivoli Provisioning Manager Express SQL Injection (Mar 29, 2012)

VideoLAN VLC Media Player mms Buffer Overflow (Mar 23, 2012)

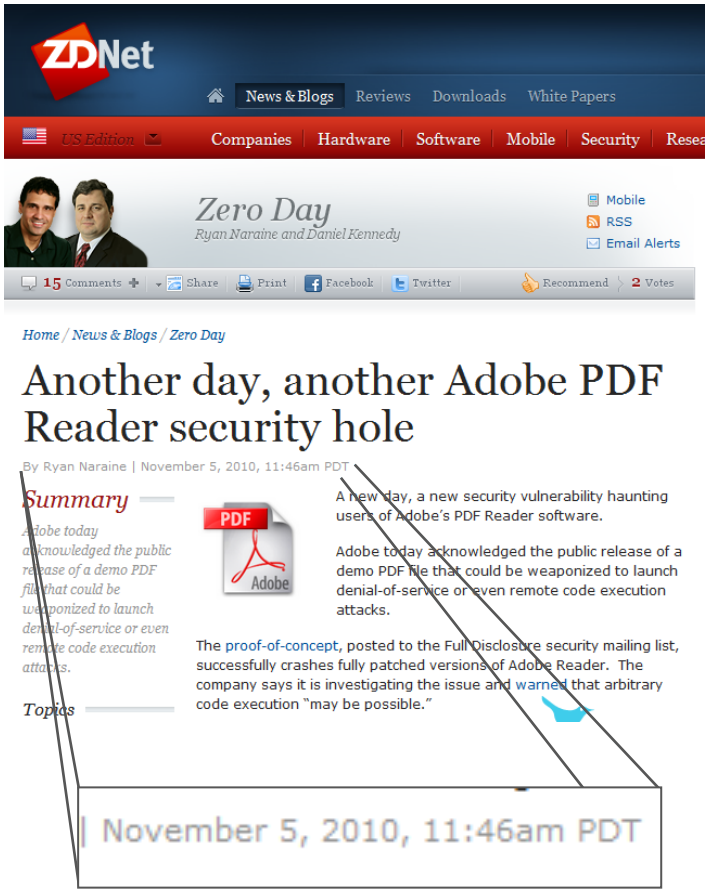
Wells Fargo Account Update Downloader Trojan (Mar 21, 2012)

New LockScreen Ransomware Trojan in the wild (Mar 15, 2012)

Oracle Java Runtime TTF BO (March 9, 2012)

Seemingly Safe Applications

Adobe PDF Reader



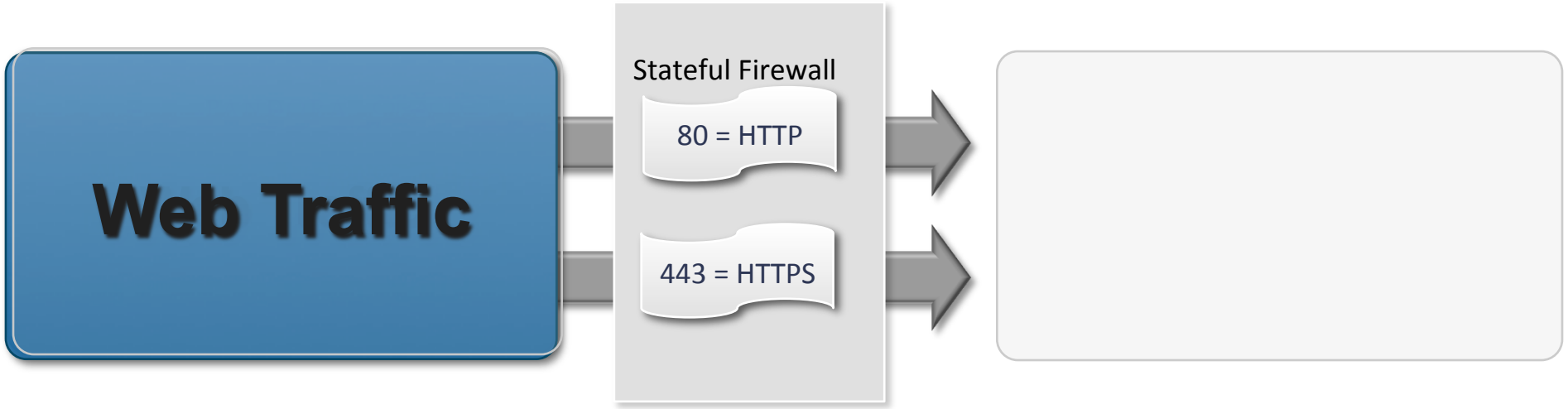
http://www.zdnet.com/blog/security/another-day-another-adobe-pdf-reader-security-hole/7693

Adobe Download Manager

http://glanceworld.com/the-worst-security-flaw-in-adobe-download-manager.html

Is my firewall good enough?

Traditional Firewalls



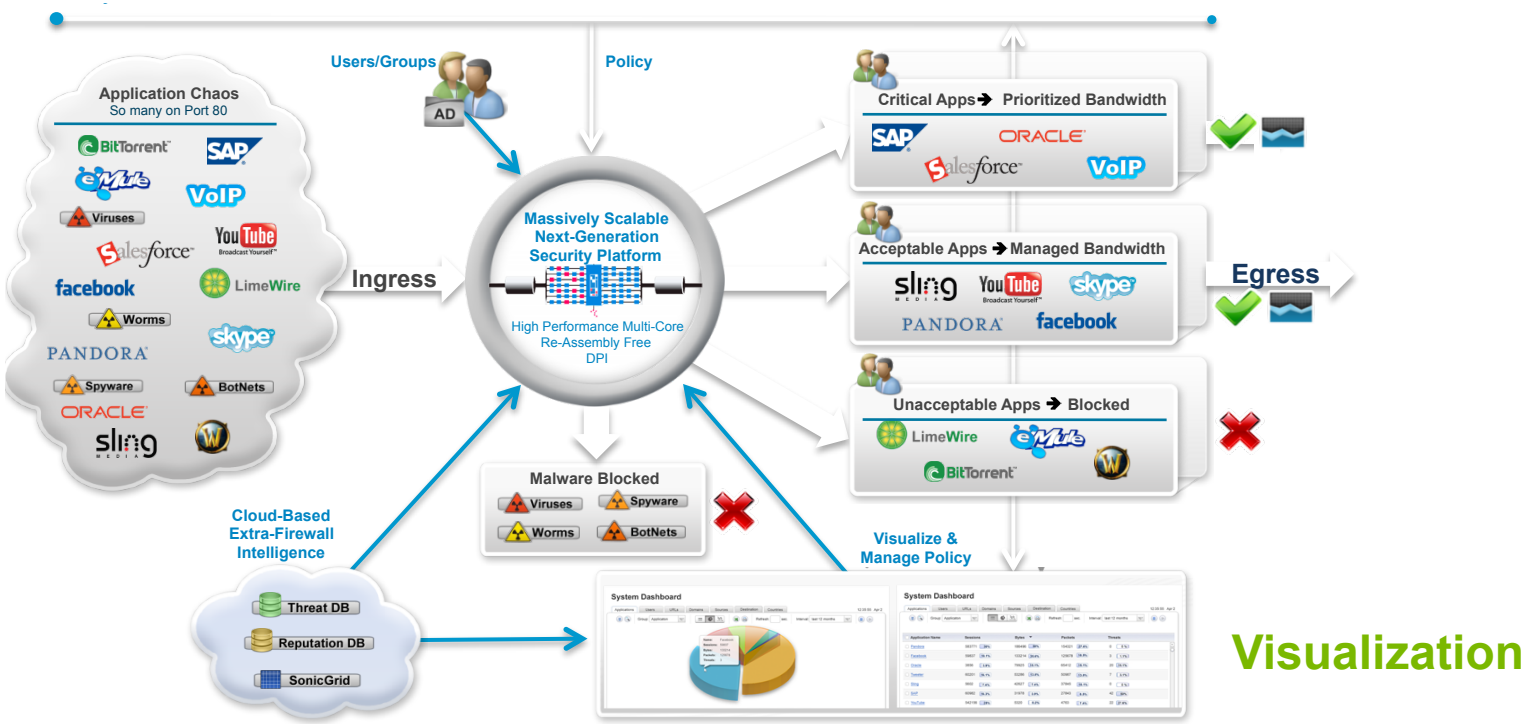
To a traditional firewall, all “web” traffic looks legitimate

Next-Generation Firewall Services

Next-Generation Firewall Features

First-Generation Firewall Capabilities	Supports Stateful Packet Inspection, NAT, Routing, & IPSec VPNs
Application Visibility and Control	Real-time visualization & granular control of applications running
Integrated IPS	Protects against a comprehensive array of network-based threats and vulnerabilities
SSL Decryption and Inspection	Decrypts and inspects SSL traffic for threats, applies application, URL and content control policies
AD/LDAP Integration (SSO)	User identification and activity are made available through seamless AD/LDAP SSO
Bump-In-the-Wire Deployment	Transparent mode deployment, in addition to Layer-3
Anti-Malware & Content Filtering	Gateway & Cloud AV, Anti-Spyware, Anti-Spam, & URL/Content Filtering

Application Visualization & Control



Identify

- 5000+ Application Signatures
- By Application
- By User/Group – LDAP/SSO
- By Content Inspection

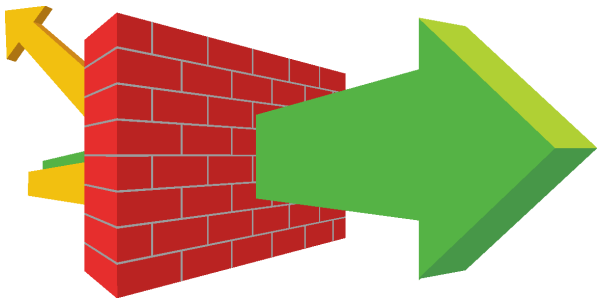
Categorize

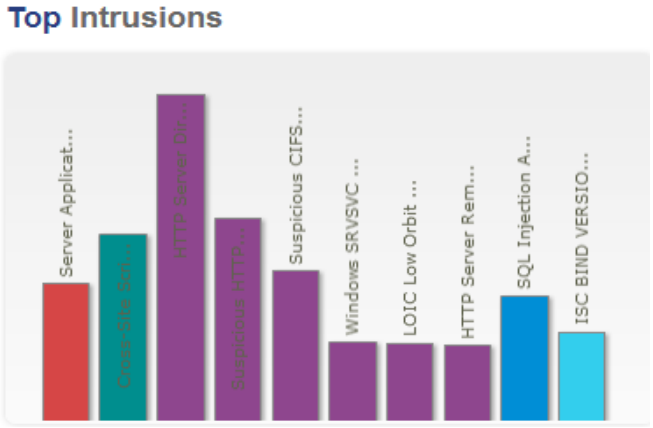
- By Application
- By Application Category
- By Destination
- By Content
- By User/Group

Control

- Prioritize Apps by Policy
- Manage Apps by Policy
- Block Apps by Policy
- Detect and Block Malware
- Manage network bandwidth

Intrusion Detection & Prevention





Detect & Prevent

Software vulnerabilities such as buffer overflows, peer-to-peer and instant messaging exploits, backdoor attacks, and other malware.

Comprehensive

- Pure Pattern Matching
- Buffer Overflow Detection
- Botnet detection & blocking
- DoS / Flood detection
- Geo IP monitoring & blocking
- SSL decryption & inspection

Reporting

- On-box reporting
- IPfix / Netflow exporting

SSL Decryption and Inspection

Deep Packet Inspection of Secure Socket Layer (DPI-SSL)

- SSL traffic decrypted, inspected, then re-encrypted
- Client DPI-SSL and Server DPI-SSL
- Inspects SSL sessions on all ports independent of protocol
- Content can be scanned as well as injected (e.g. HTTP/S block pages)
- Supports all Security Services

Extends

Deep Packet inspection to SSL traffic scanning both LAN and WAN traffic for threats and vulnerabilities

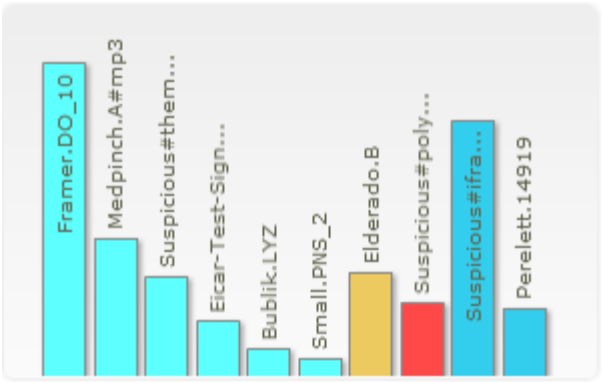
Inspects

Inspects SSL traffic across other security mechanisms, such as URL filtering, IPS & Gateway AV

Granular Control

Inclusion/Exclusion list to customize which traffic DPI-SSL inspects, which allows better management of CPU resources

Gateway Anti-Virus and Anti-Spyware



Scans & Prevents

Installation of malicious spyware and disrupts background communications from existing spyware programs that transmit confidential data

10M+

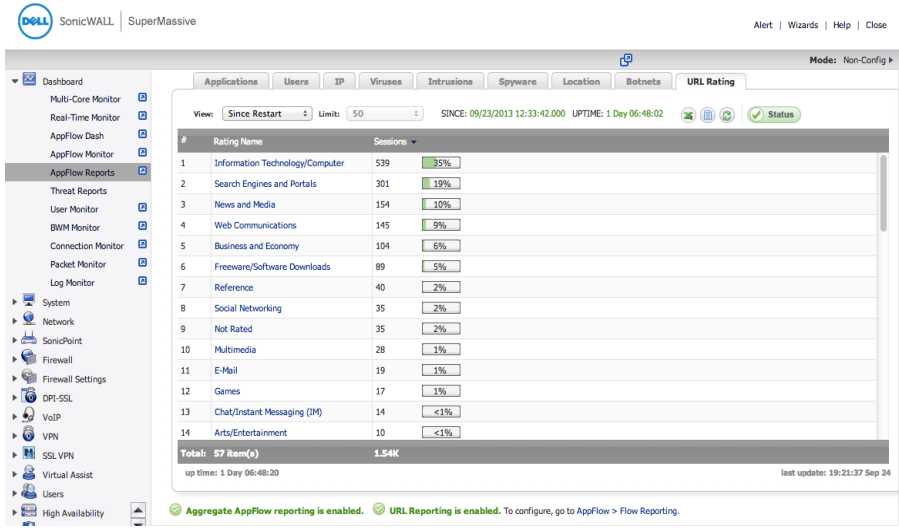
Signatures detecting millions of pieces of malware and intelligent enough to detect new variants providing effective **zero-day protection**

Unlimited

Dell SonicWALL **Reassembly-Free Deep Packet** Inspection engine scans analyze all files in real time—regardless of file size or compression.

Web Content Filtering

- Dynamically updated rating architecture
- Application traffic analytics
- Web-based management
- Enforced CFS Clients



16M+

Website rating database used to **block inappropriate and illegal content**, reduces organizational liability and **increases productivity**

56+

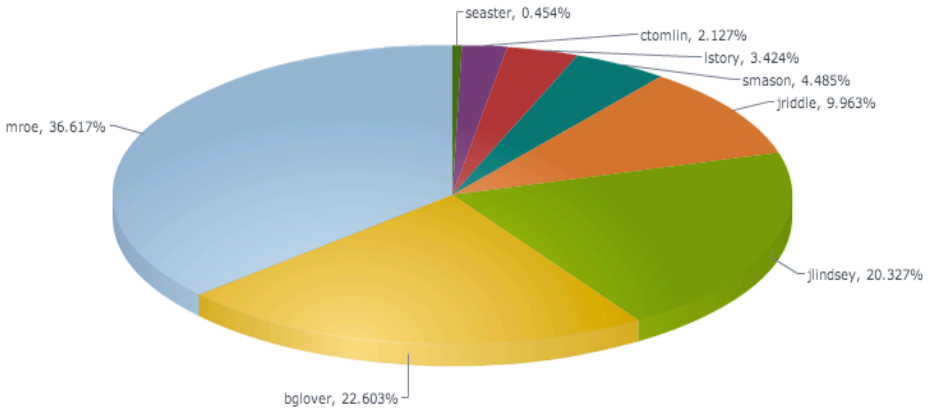
Granular level blocking based on pre-defined categories. IP-based HTTPS content filtering to **control user access** to web sites over encrypted HTTPS

Report & Analyze

Application traffic analytics suite - integration with Dell SonicWALL GMS®, Analyzer & Scrutinizer provides **real-time and historic analysis** of data transmitted through the firewall.

Single Sign-On

- Radius, AD, & LDAP Authentication
- Transparent User Authentication
- Per-Group Policies
- Per-User Policies
- Use Cases
  - Visibility & Reporting
  - CFS and Application Policies
  - Firewall Policies



SSO Agent

The Directory Connector SSO agent uses NetAPI, WMI, Domain Controller Logs, and the LogWatcher agent to identify users based on the workstation IP address

TSA Agent

The Terminal Services Agent (TSA) provides user-specific information required by the firewall for users accessing the network from multi-user systems

RADIUS Accounting

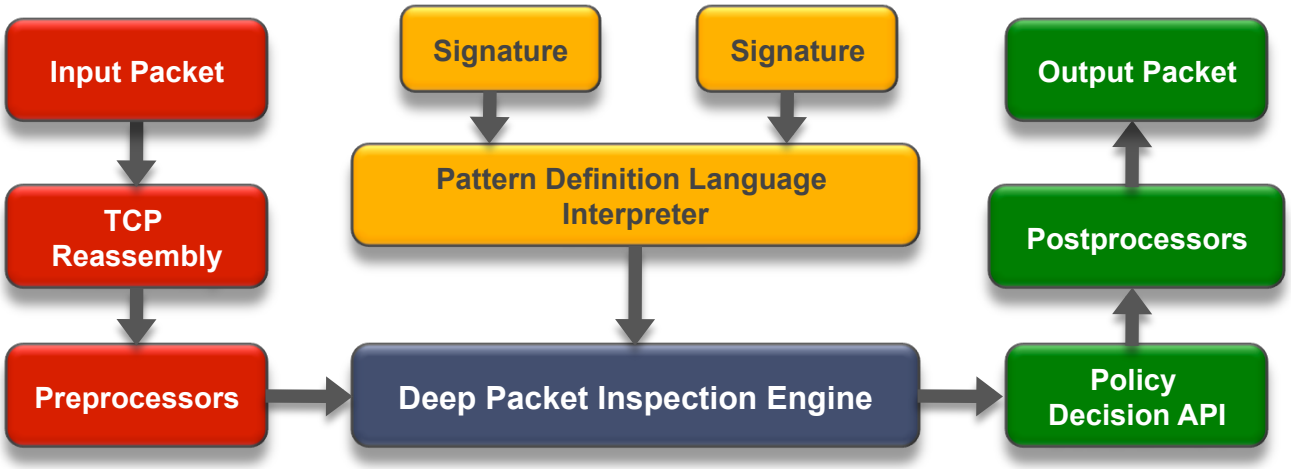
The Next-Generation Firewall appliances can function as a RADIUS accounting server, which enables RADIUS accounting message to be used for single sign-on

Multi-Core Parallel Processing Technology

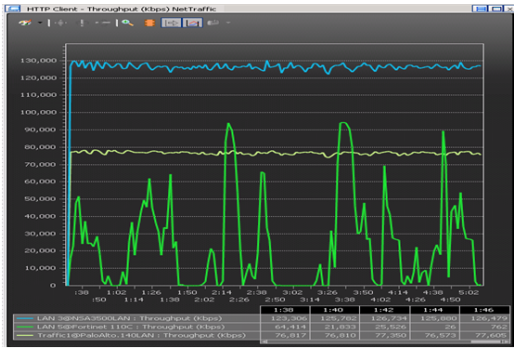
Single-Pass RFDPI Security Engine

Reassembly Free Deep Packet Inspection

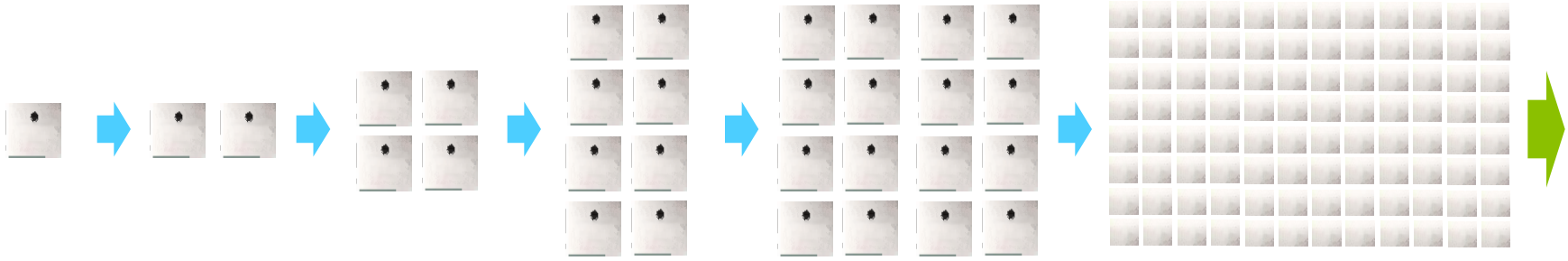
Low-Latency Ultra-Scalable Single Pass Deep Packet Inspection Engine



Stable Throughput vs. Buffering Proxy Engines



Linearly Scalable on a Massively Multi-Core Architecture



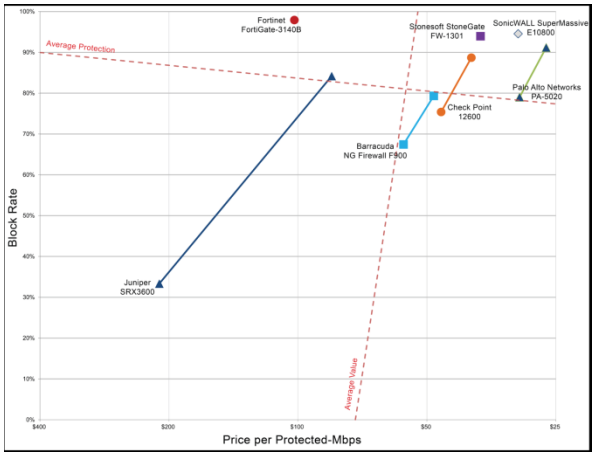
Dell Security
Global Response Intelligent Defense (GRID)

- 100% IP ownership of all signatures
- World-wide Intelligence from +2m end-points
- Advanced Tracking & Detection
  - 94% effectiveness rating from NSS for IPS and ICSA for Anti-Virus
- Industry Leading Responsiveness (MAPP leader)
  - Same day signatures, 1000's new/month
- Proactive Anti-Malware protection
- In-house security research team since 1999
- Active participant in leading research organizations (WildList, AVIEN, PIRT, APWG and more)
- Member of the Microsoft Active Protections Program (MAPP)

Industry Reports

Industry Reports

- NSS Labs Results –
  - Recommended NGFW
    - 2012 & 2013
  - Recommended IPS
    - 2012 & 2013



- Network World Firewall Challenge
  - Dell SonicWALL made the Cover of Network World as the Winner
  - Best Overall Performance for NGFW
  - Best Overall Performance for UTM
  - Best Overall Performance for SSL Decryption

NETWORKWORLD

Dell Security Next-Generation Firewall Appliances

Dell Security Next-Generation Firewalls

Enterprise, Data Center

SuperMassive Series

SuperMassive 9600
SuperMassive 9400
SuperMassive 9200

SuperMassive E10800
SuperMassive E10400
SuperMassive E10200

SMB/Campus/Branch

TZ Series

TZ 215/W
TZ 205/W
TZ 105/W

NSA Series

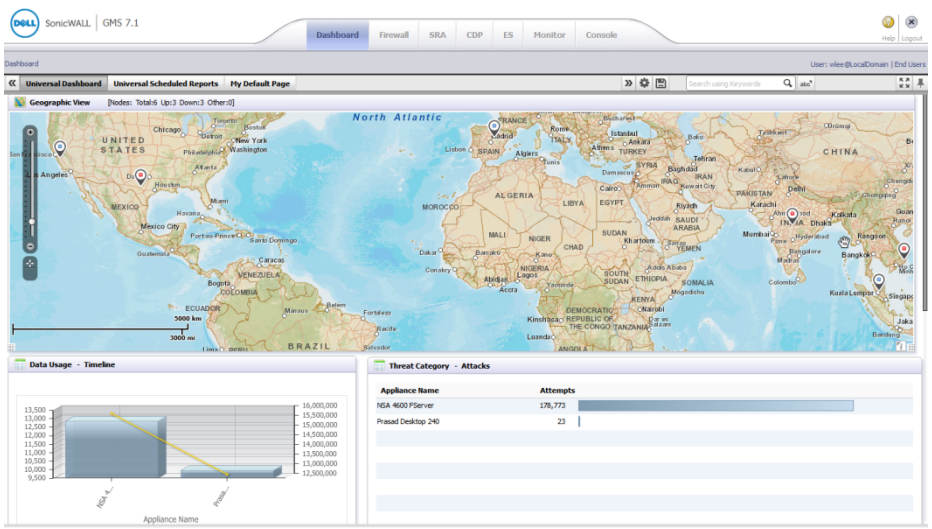
NSA 4600
NSA 3600
NSA 2600
NSA 220/250M

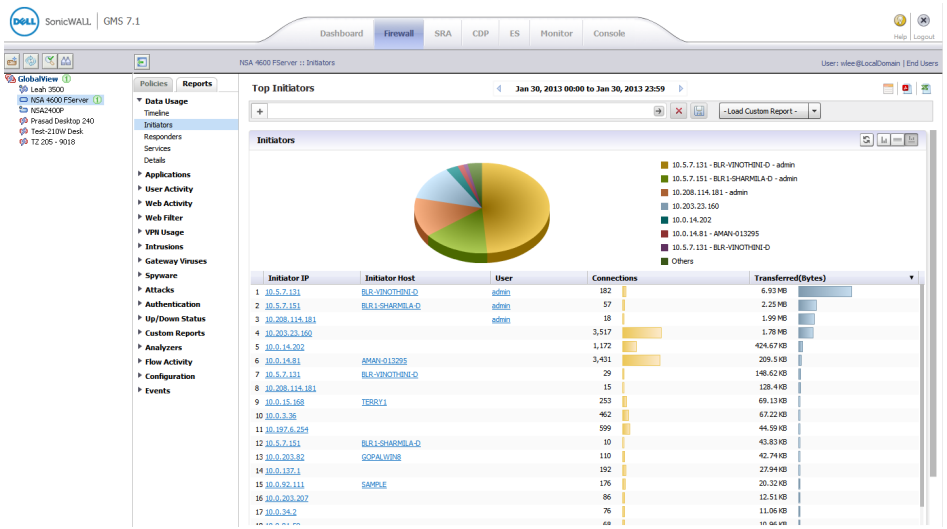
NSA 6600
NSA 5600

Dell Security Management & Reporting

Global Management System (GMS)

Dell Security Policy Management, Analytics, and Reporting





Issues

- **High cost of managing** complex security networks.
- **Difficulty capturing data**
- **Hard to identify disruptive** users.
- **Cumbersome license** management

Solution

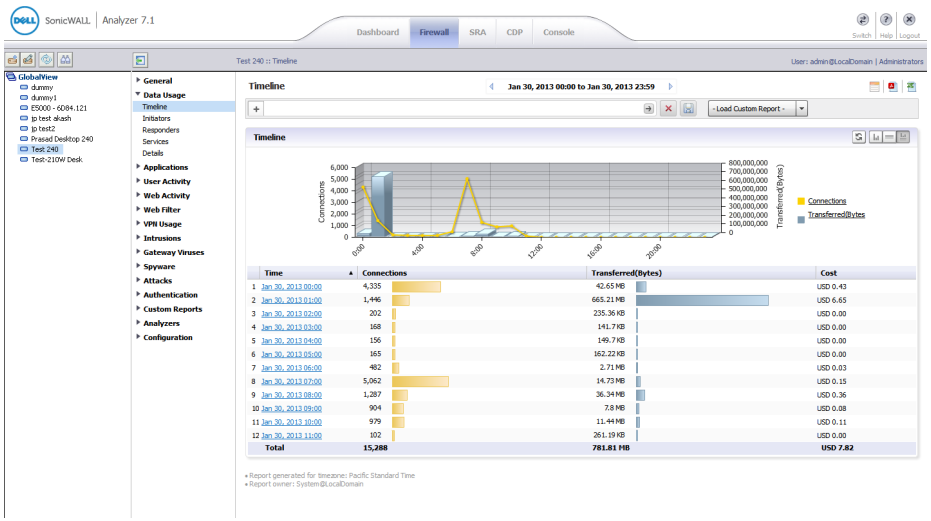
- **Centralized console** for managing, monitoring, and reporting.
- **Integrated features** incl. logging, analytics, change control, license tracking, and historical reporting.

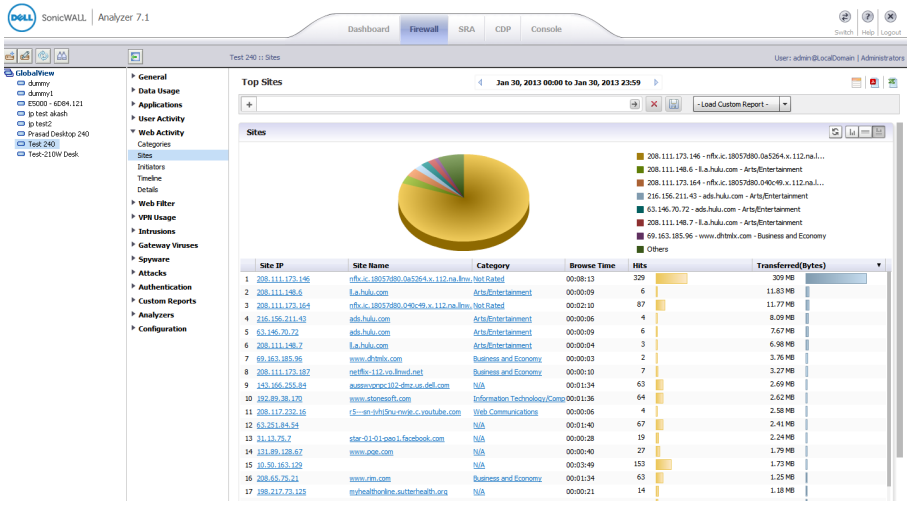
Benefits

- Greater efficiency via a streamlined console.
- Accurate compliance reports Higher productivity via user activity reporting.

Analyzer

Dell SonicWALL Analytics and Reporting





Issues

- **Difficulty capturing data** for regulatory compliance audits.
- **Hard to identify disruptive** users.
- **Hard to prove SLA** levels.

Solution

- **Centralized console** that is easy-to-use and affordable.
- **Integrated features** incl. logging, analytics, and historical reporting.

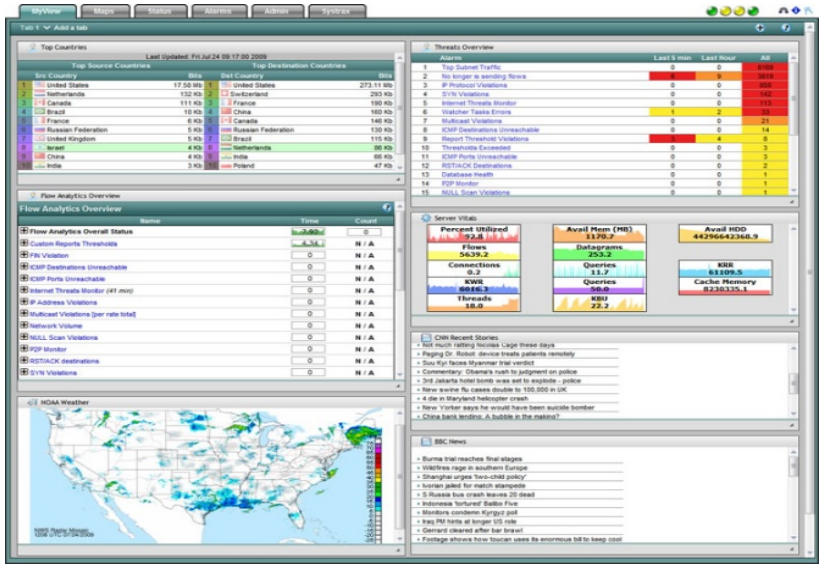
Benefits

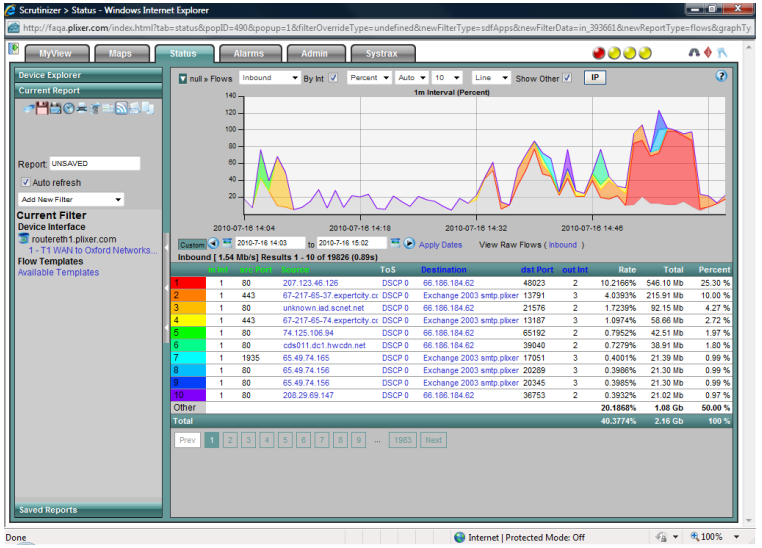
- Greater efficiency via a streamlined console.
- Accurate compliance reports via relevant data.
- Higher productivity via user activity reporting.

(1) IDC's Worldwide Mobile Worker Population 2009-2013 Forecast
(2) Cisco Connected World Technology Report, 2011

Scrutinizer

Multi-vendor IP Data Flow Analytics and Reporting





Issues

- Imprecise isolation of network performance issues
- Untraceable breaches from within a corporate data network.
- Non-business data traffic

Solution

- **Uncover bottlenecks and optimize network** design
- **Identify infected hosts**
- **Deliver granular reports** of user, website, and application usage activity.

Benefits

- **Lower network costs** via optimized, bandwidth utilization.
- **Proactive mitigation** of security threats
- **Higher productivity** by managing user activity.

Contacts

Dell Contacts

Dell Account Executive

- Peyton Biggs – peyton_biggs@dell.com

Security Sales Executive

- David Koch – david_koch@dell.com

Security Sales Engineer

- Rapatrick Murrell – rapatrick_murrell@dell.com

Dell Security Resources

Next-Generation Firewall Live Demo Site

- livedemo.sonicwall.com

Demos on Demand

- www.demosondemand.com/it/vendors/SonicWALL.asp

Dell Security – Next-Generation Firewalls

- www.sonicwall.com

Q&A