

McAfee Firewall Enterprise



Gerhard Pirkl
Senior Sales Engineer

May 6, 2010

"The information contained in this document is for informational purposes only and should not be deemed an offer by McAfee or create an obligation on McAfee. McAfee reserves the right to discontinue products at any time, add or subtract features or functionality, or modify its products, at its sole discretion, without notice and without incurring further obligations."



Secure Firewall (Sidewinder) 7.0 is the culmination of years of supporting governments



1995



Sidewinder

- Developed by the "Secure Computing" division of Honeywell for the U.S. Department of Defense
- First firewall to protect the firewall OS platform – uses our patented Type Enforcement technology
- Used to secure critical infrastructures all over the world

2002



Sidewinder (G2)

- Combination of Sidewinder and acquired TIS/NAI Gauntlet technologies
- First firewall to achieve Common Criteria at EAL4+ with the U.S. DoD Application Layer Protection Profiles
- Favorite firewall of many Enterprise financials and government organizations

2007



Secure Firewall (Sidewinder) 7.0

- Combination of Sidewinder G2 and acquired CyberGuard technologies
- The speed and usability of a stateful firewall with the security and UTM features of an application-layer gateway
- Delivers unprecedented application-layer performance

McAfee Firewall Enterprise: The Complete Security Solution



Security Appliances



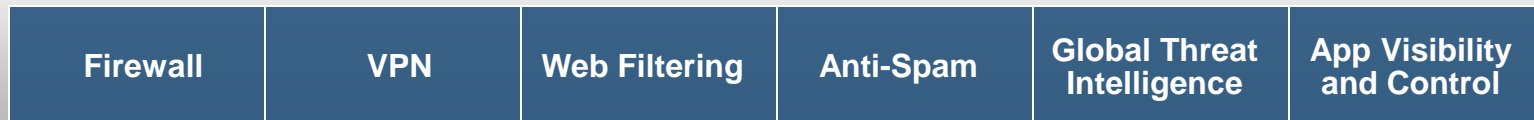
Comprehensive Security

- Application Inspection
- NAT
- HA
- Quality of Service
- VLAN

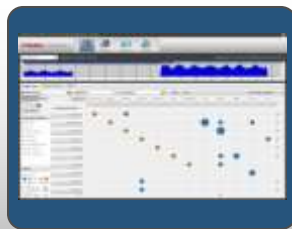
Flexible Deployments

- Standalone Appliances
- Multi-Firewall Appliances
- Virtual Firewall for VMware
- Riverbed Steelhead

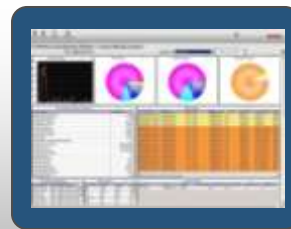
Networking and Security Service Integration



Management



McAfee Firewall Enterprise Profiler

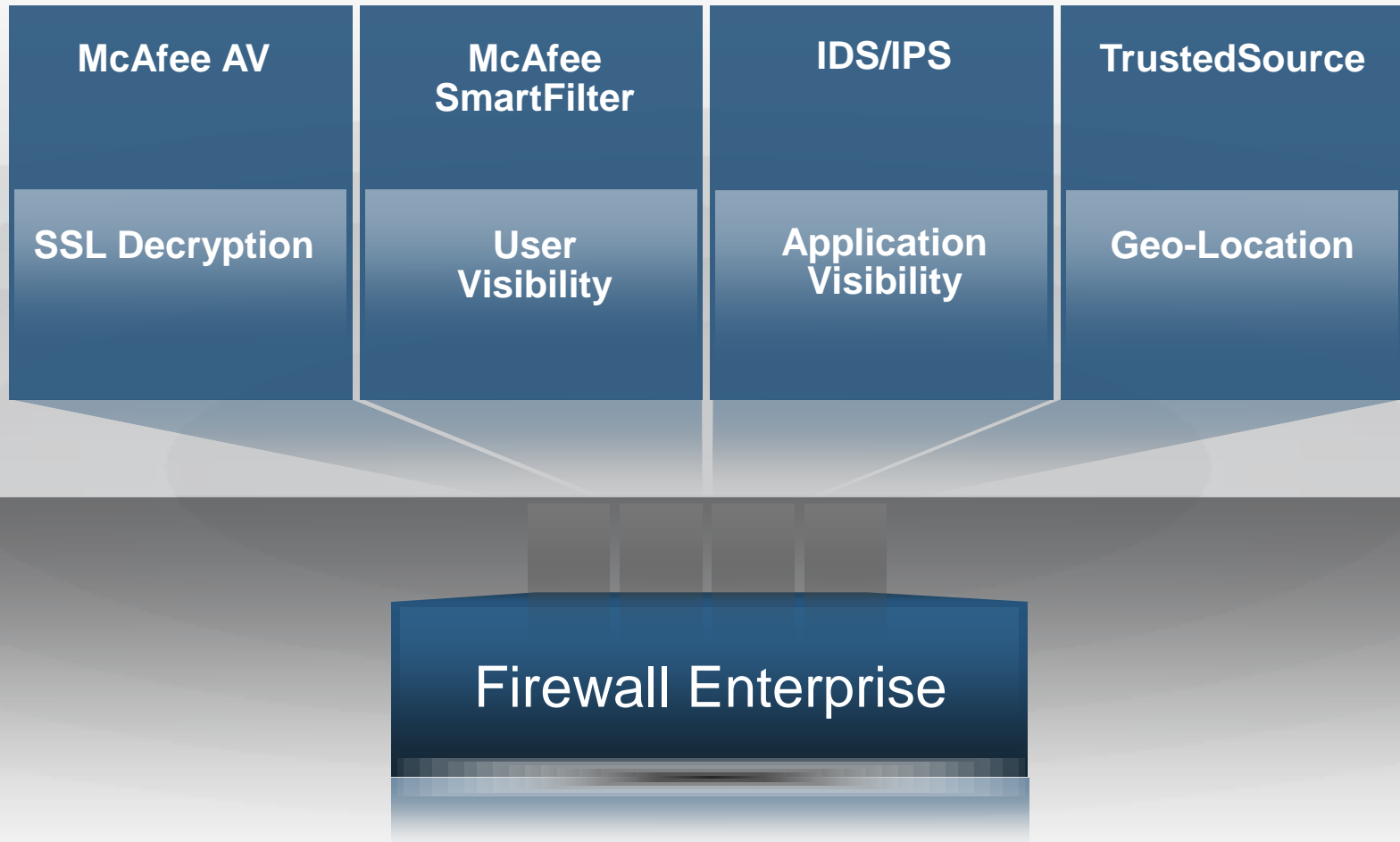


McAfee Firewall Reporter (included)



McAfee Firewall Enterprise Control Center

McAfee Firewall Enterprise: Consolidated, Best-in-Class Network Defenses



Flexible Deployment Options



Standard Appliances

- Designed for **traditional deployments**
- Levels of appliances sized for branch to data center deployments
- EAL4+ Certified, ICSA IPsec Certified



Rugged Platforms

- Designed for resiliency and availability **beyond commercial environments**
- Military Spec hardware quality metrics



Multi-firewall Appliance

- Multiple virtual firewalls within our turnkey firewall appliance
- Designed for **network segmentation and consolidation projects**



Virtual Appliance

- Firewalling within your ESX or V13 platform
- Designed for your **server consolidation projects**
- An easy way to evaluate and demonstrate McAfee Firewall

SecureOS / Firewall Software
Central Management and Reporting
Common Criteria EAL4+, ICSA Certified

Managing Firewalls Is Expensive



- Difficult to **provision** rules and firewall capacity to support application rollouts
- **Maintaining** and **optimizing** rules to support changes is extremely challenging
- **Compliance** data collection and **reporting** is painstaking



Reality Check—Troubleshooting and Changing Firewall Rules



- Finding source of firewall problems is difficult
- Completing firewall rule changes takes time
- All tasks are much more difficult with more firewall rules
- On average, how many actual hours or days does it take to track down and isolate a firewall-related issue?
- How long does it typically take to complete rule changes in your organization?

Source: “The State of Today’s Firewall Management Challenges.” IDC White Paper sponsored by McAfee, June 2009.



Market Requirements: Application and Identity Level Awareness



“Must block VOIP from trading floor that bypasses compliance mandated recording of communications. **Don’t want to track by IP addresses** of external call manager. We need to something to recognize that application.”

““The big challenge is the **port-agile** applications and the scheme they used to evade firewall rules”

“During the Olympics, **bandwidth was being sucked up**; traffic was going to Global Crossing. We blocked it. We ended up blocking NBC olympics video streaming. People were extremely unhappy, and we had a flurry of calls”

“Common changes in the firewall are due to IP address changes, whenever there is hardware refresh or when apps are upgraded to new versions that require **new ports**”

“I really want to be able to tie **identities** to my policies for our employees going to applications within our DMZ from our Internal network.”





Inadequate Protection

Without application visibility, firewalls cannot defend against increasingly port-agile, evasive, and ssl-tunneled application-layer attacks

Appliance Fatigue

The lack of quality, integrated threat prevention means too many appliances to manage, higher TCO, and greater risk

Inefficient, Frustrating Workflow

Firewall administrators need intelligent systems to ease administration, maintenance, and compliance tasks

McAfee Next Generation Firewall Vision

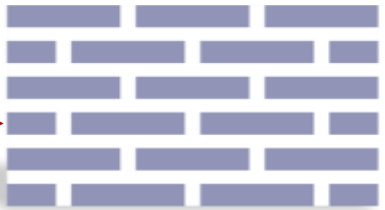


“McAfee next generation firewalls ease manageability and policy using the language of business: applications and users”

Avert Labs: Global Threat Intelligence



McAfee Firewall Enterprise



**Applications
Users / Roles**

Your Business



Broad, extra-firewall interlock

- GTI for application recognition, source reputation and dynamic threat identification
- Next Generation management framework for policy and event analysis

Consolidated, layered defense

- Integration of IPS, AV, URL filtering, DLP and other McAfee technologies
- Architecture for performance and deployment flexibility

Business level intelligence

- Application recognition and identity/role awareness for intuitive discovery and granular control
- Built-in visibility and analytics for efficient workflow

Application Recognition Plans



- Launch with 1500 application coverage
 - Updates backed by industry leading McAfee Labs
 - Intrushield and Secure Computing advantage on detecting evasive applications
- Coupled with innovative *visualization and analytics*, and *identity awareness* for intuitive workflow
- Unmatched threat research providing *application reputation or outbreak alerts* as well

- Anonymizer / Proxies
- Authentication Services
- Commercial Monitoring
- Collaboration / Content Mgt
- Database
- Director Services
- Encrypted Tunnels
- Work Group Email (GroupWise, Exchange, Lotus-notes)
- ERP/CRM
- File Sharing
- Gaming
- Instant Messaging
- VPN
- Infrastructure Services & Storage

- IT Utilities
- Mobile Software
- Personal Web Apps
- Peer to Peer (P2P)
- Remote Administration
- Remote Desktop / Terminal Services
- Social Networking
- Business Web Apps
- Software / System Updates
- Toolbars & PC Utilities
- Voice over IP (VOIP)
- Streaming Media
- Web Mail
- Web Browsing
- Web Conferencing
- Photo-video

“Teal” Release: Application Level Policy Control



Policies driven by identity not just endpoints

Start typing in any of these fields then they will start filtering

Policies include application not just port/service

All multi-selectable objects in 1 convenient place Endpoints, Applications, Zones, users, User Groups

Consolidated Management and Integration with ePolicy Orchestrator (ePO)



Firewall Management into ePO

(ePolicy Orchestrator v4.5)

- Monitor firewall appliance health
- See historical performance trends
- Track FW versions and patch levels

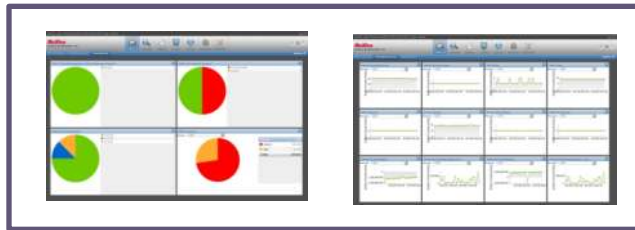


ePO into Firewall Management

(Control Center v4.0 with Profiler v1.5)

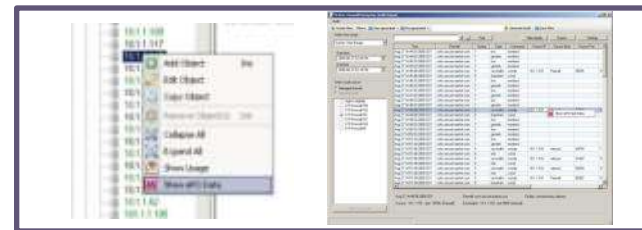
- Identify hosts and endpoints used in policies
- Access host profile information directly from visualization tools

Integrates network health with endpoint



EPO Admin

Aides troubleshooting & policy creation



Network Security Admin

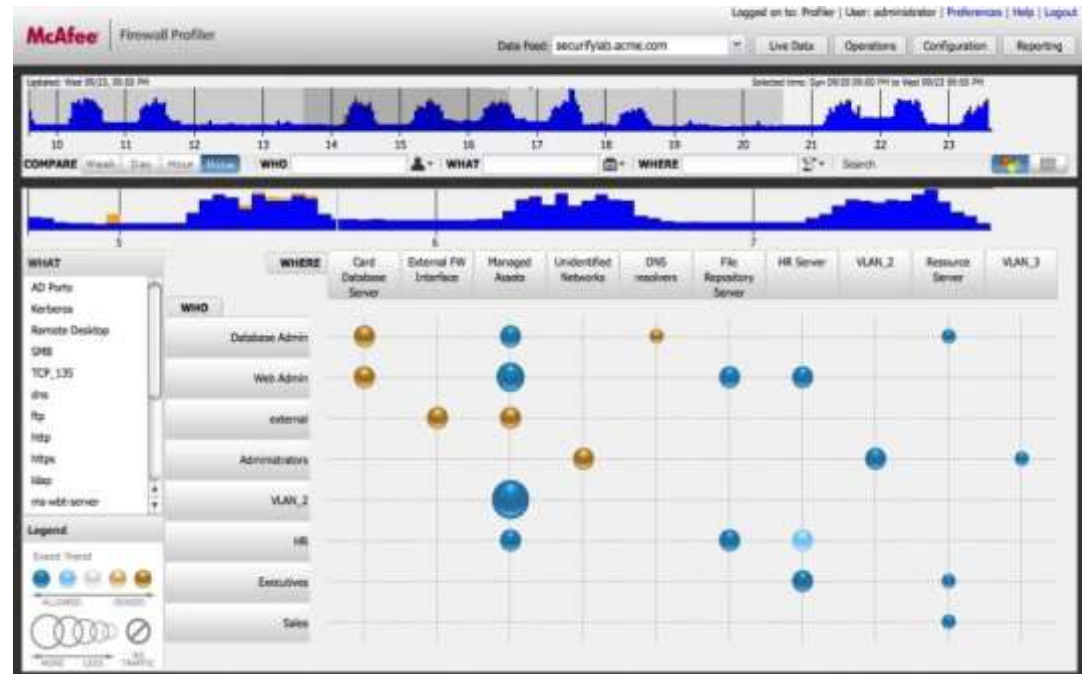
Introducing McAfee Firewall Profiler



- **Monitors all traffic that traverses the firewall and visualizes results in terms of user roles and assets.**
 - Discovery for properly addressing changes in the network and applications
- **Overlays all firewall actions including all allows and denies**
 - Record of all firewall actions to expedite troubleshooting and facilitate compliance
- **Correlates all observed traffic and actions to current Firewall Policy**
 - Visualization in the context of Policy for making efficient changes stopping the increasing complexity of the ruleset

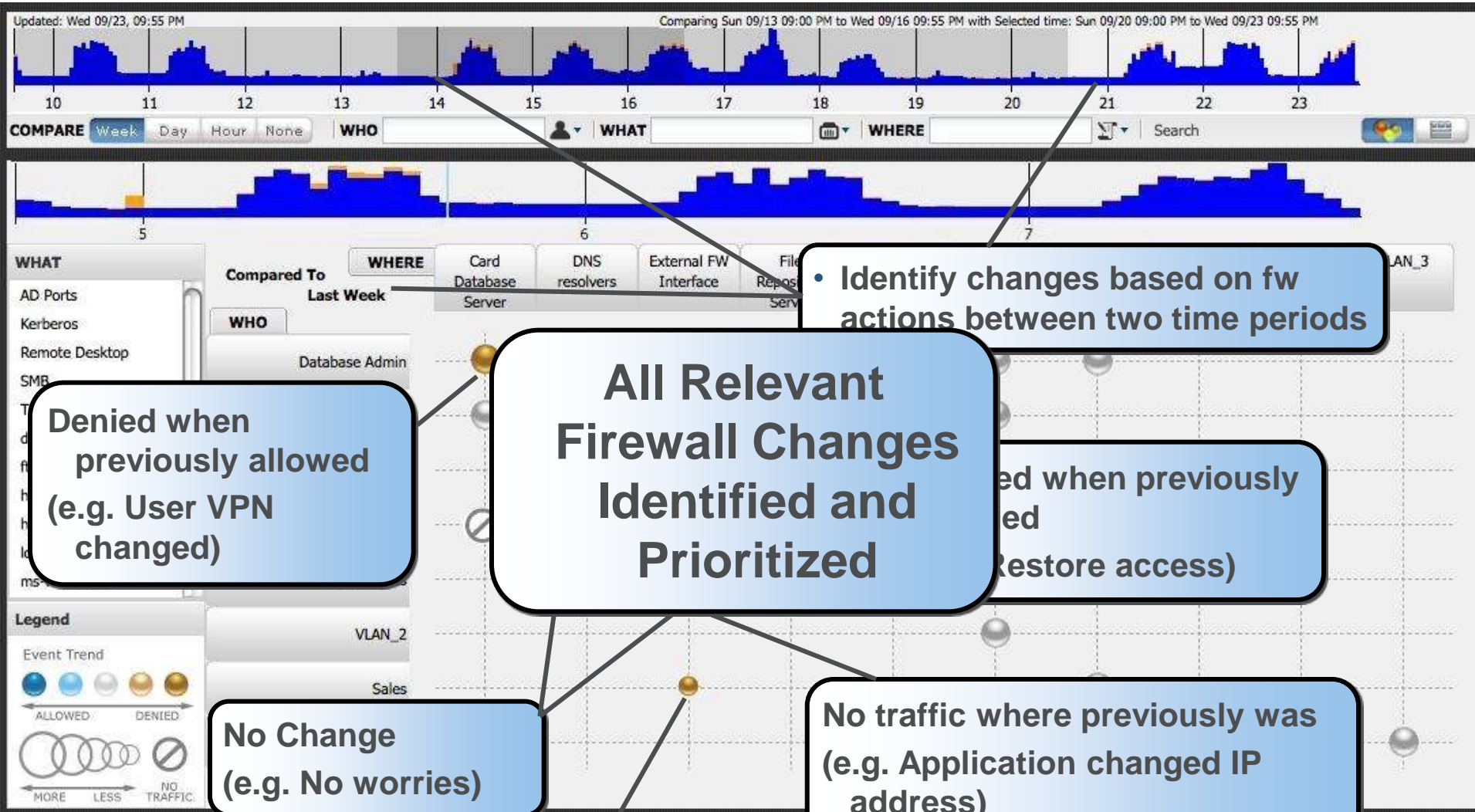
Turns Hours and Days of Work Into a Few Clicks

- All traffic that traverses the firewall
- In the context of users/roles and FW Policy objects
- Overlay of Firewall actions
- Aggregated view for high level context
- Intuitive drilldown for details



See and Know what rules are being used and for what

Profiler Visualization: Firewall Changes



Identify changes based on fw actions between two time periods

Denied when previously allowed (e.g. User VPN changed)

All Relevant Firewall Changes Identified and Prioritized

Restored when previously denied (e.g. Restore access)

No Change (e.g. No worries)

No traffic where previously was (e.g. Application changed IP address)

Reduced volume in traffic (e.g. Change in routing scheme)

Profiler Visualization: Root Cause Analysis



McAfee Firewall Profiler

Logged on to: Profiler | User: jcaldera | Preferences | Help | Logout

Data Feed: beach-a.sctc.com

Live Data Operations Configuration Reporting

Updated: Tue 07/07, 10:37 AM

Selected time: Sat 07/04 10:00 AM to Tue 07/07 10:37 AM

Root Cause for all Denied Events

COMPARE Week Day Hour None WHO WHAT WHERE Search

Remediation Summary

Details	Action	Source	Applicat...	Destination	Root Cause	Rule Name	Count
Denied	stpdco2	ntp	IPv4 link-local	Policy Violation: IPFilters	Drop any to IPv4 link-local	67	
Denied	stpdco2			Drop any to IPv4 link-local	Drop any to IPv4 link-local	1	
Denied	stpdco2			Drop any to IPv4 link-local	Drop any to IPv4 link-local	8	
Denied	external	isakmp	external	Policy Violation: Improper Source, Service or Destination	Deny All	1	
Denied	pt	http-alt	127.0.0.1	Policy Violation: Improper Source, Service or Destination	Deny All	3	
Denied	rick laptop	ssh	10.96.168.80	Policy Violation: Improper Source, Service or Destination	Deny All	1	
Denied	rick laptop	TCP 10...	10.96.168.80	Policy Violation: Improper Source, Service or Destination	Deny All	1	
Denied	thelonious	http	external	Policy Violation: Improper Source, Service or Destination	HTTP TrustedSource Deny	1	
Denied	blacknet	http-all	external	Protocol Violation	nt_http_out-nt_http_services-proxy-auth-internal	42	
Denied	blacknet	http-all	external	Protocol Violation	HTTP relaxed for some servers	1	
Denied	blacknet	https-all	external	Protocol Violation	_out-nt_http_services-proxy-auth-internal	97	
Denied	devnet-servers	http-all			without NTLM for some clients	108	
Denied	devnet-servers	https-al			HTTP without NTLM for some clients	13	
Denied	jim-c-ntlm	http-all	external	Protocol Violation	nt_http_out-nt_http_services-proxy-auth-internal	4	

FW Audit Categories

Access Rules

FW Objects

Proxy Security

Page 11 of 11

Displaying 501 - 539 of 539

Application & User Level Visualization



Logged on to: Profiler-80221 | User: administrator

Preferences | Help | Logout

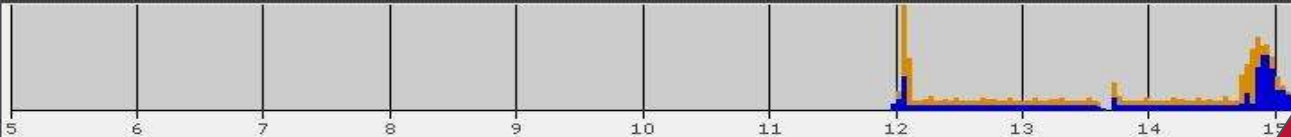
McAfee Firewall Profiler



sw80239.local

Updated: Sat 09/19, 12:16 AM

Selected ti



Discover what apps are your users accessing

Bubble Chart

Application Analysis

Details

Filter by Source: [] Application: [] Destination: [] Search Clear View Details For Bubbles

Application Category: Voice Over IP, Calendaring, Paul Custom Group, Peer to Peer, Video Games, Web Based, Business, Desktop Publishing

More Options

Destination Reporter

Combined 80237

Combined 80240

Firewall

IP2010

Inside 239 Subnet

Inside IP238

Inside IP23940

Pauls DC and DLC

Subnet 20

Subnet 50

internal

Source User Group

Santa Clara Employee_CN

Anonymous

Test Lab Employee_CN

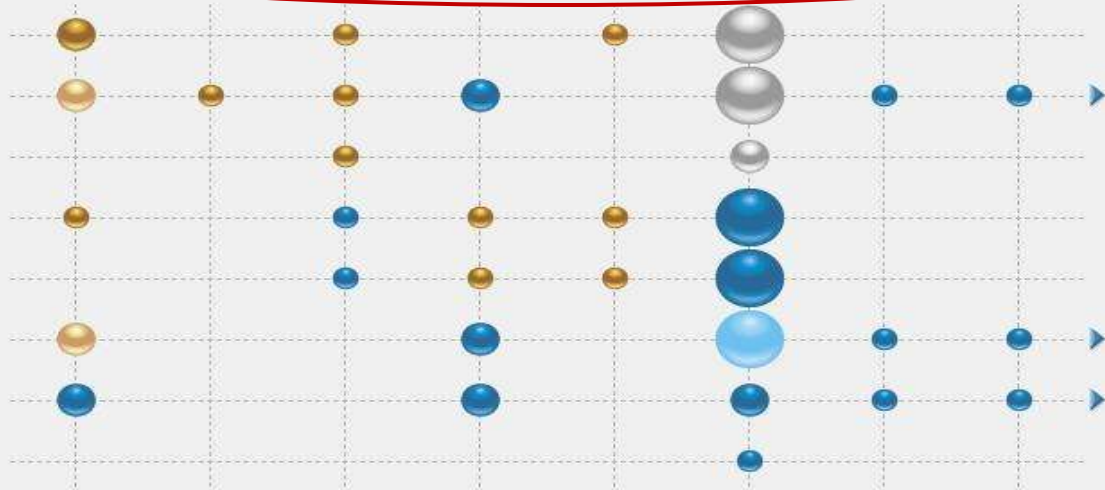
Domain Users_CN

Some User Group_CN

<no data>

Engineering_CN

Super Administrators_CN



Legend

Event Trend



ALLOWED DENIED



MORE NO

Including Geo Location



Logged on to: Profiler-80221 | User: administrator

Preferences | Help | Logout

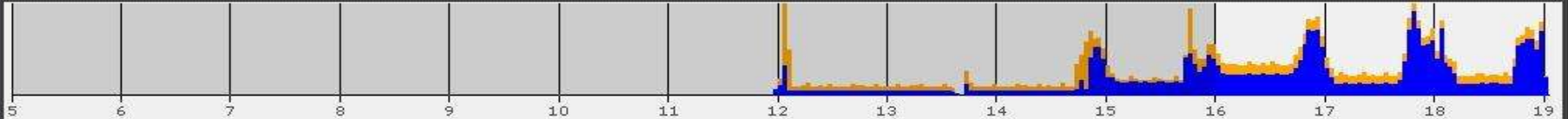
McAfee Firewall Profiler



sw80239.local

Updated: Sat 09/19, 12:16 AM

Selected time: Wed 09/16 12:00 AM to Sat 09/19 12:16 AM



Bubble Chart

Application Analysis

Details

Filter by Source: [] Application: [] Destination: [] Search Clear View Details For Bubbles

Compare: [] [] [] []
More Options

Application Category: Calendaring Video Games Voice Over IP Business Desktop Publishing High Risk Paul Custom Group Peer to Peer

- Destination Geo
- France
 - India
 - Japan
 - N/A
 - Russian Federati...
 - South Africa
 - South Georgia a...
 - Taiwan
 - United States
- Source Geo
- United States
 - Russian Federation
 - N/A
 - China
 - South Georgi...ch Is lands
 - United Arab Emirates
 - Germany
 - United Kingdom
 - Europe

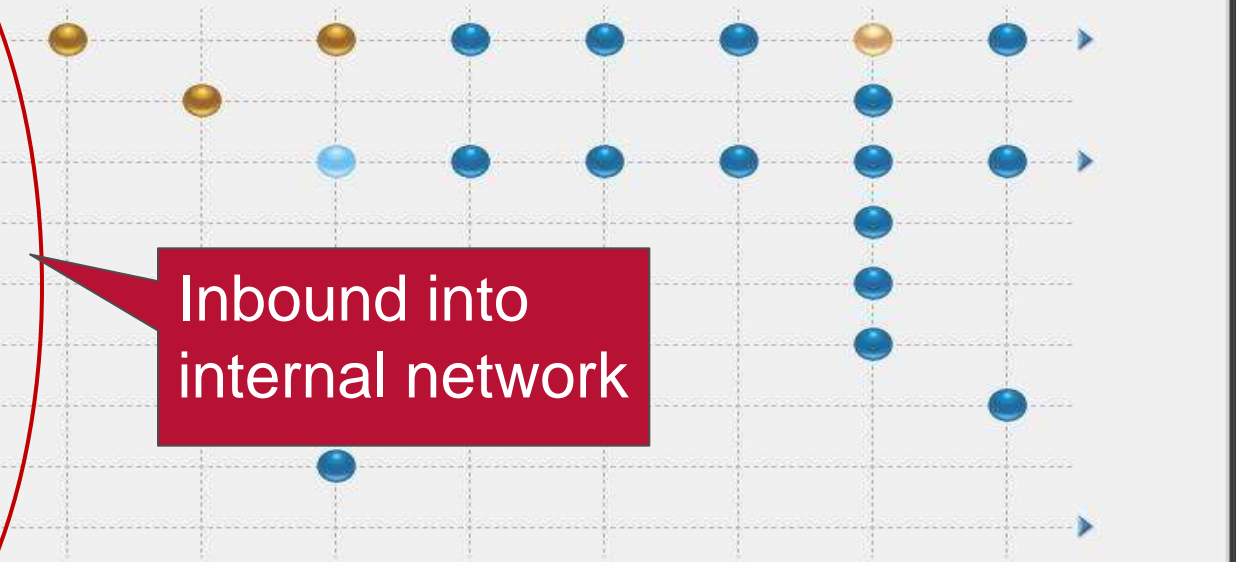
Legend

Event Trend

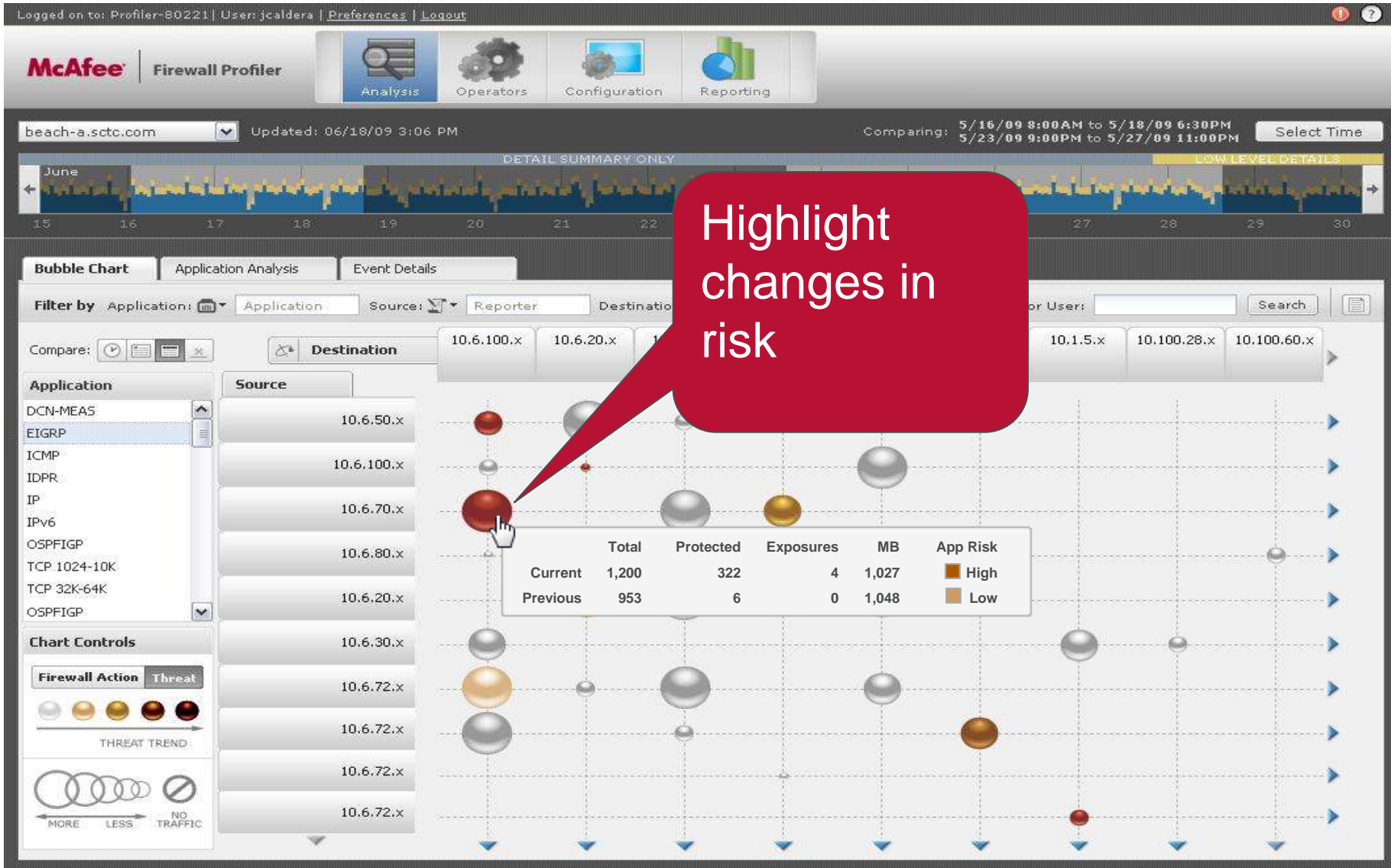
ALLOWED DENIED

MORE LESS NO TRAFFIC

Inbound into internal network



Threat Visualization (Teal)



Application Analysis integrated with Threat (Teal)



Logged on to: Profiler-80221 | User: jcaldera | Preferences | Logout

McAfee Firewall Profiler



Analysis



Operators



Configuration



Reporting

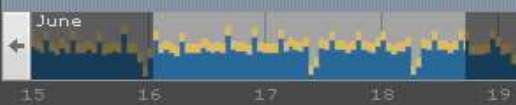
beach-a.sctc.com

Updated: 06/18/09 3

5/16/09 8:00AM to 5/18/09 6:30PM
5/23/09 9:00PM to 5/27/09 11:00PM

Select Time

Generate reports by BW, inbound, outbound, or by risk



Bubble Chart Application Analysis

View By: Application Category

Application Category	In (MB)	Out (MB)	Total (MB)	Risk
Communications				
Yahoo! IM	10,000	10,000	10,000	Critical
Gtalk	250	250	250	Critical
Pidgin	50,000	50,000	50,000	High
Trillian	10	10	10	Medium
(4 Applications)				
File Transfer				
(7 Applications)				
Games				
(2 Applications)				
Real-time				
(4 Applications)				
Photo-Video				
(5 Applications)	24,983	24,983	24,983	High
Graphics				
(13 Applications)	98,345	98,345	98,345	High
Management				
(11 Applications)	71,825	71,825	71,825	Medium

How security countermeasures are applied by app`

Communications

Application Risk **Critical**

Threat Summary

Security Countermeasure	Attack	Exposure	Protected	Bandwidth
IPS	140	140	0	7540
AV	0	0	0	0
URL Filter	0	0	0	0
Reputation	20	0	20	4000
Policy Violation	30	0	30	500
Protocol Violation	240	0	240	10000
SPAM	0	0	0	0
Buffer Overflow	0	0	0	0
DOS	0	0	0	0

Relationship Summary

User Group	Bandwidth	Allow	Deny
Marketing	250	50	4,000
Engineering	10,000	7,000	800
Finance	10	500	45



McAfee® | Global Threat Intelligence

Regulatory Compliance Research	Web Security Research Rated more than 25 million sites classified in more than 90 categories More than 400,000 zombies identified per day	McAfee Customers 50M enterprise nodes 100M consumer nodes	Malware Research 50,000 samples/day 1.5M malware detections in 2008	Vulnerability Research 100 sources monitored daily 20 vulnerabilities discovered	Email Security Research More than 10 billion messages every month	Network Security Research 10M IPS alerts monitored/analyzed daily 1000T traffic monitored/analyzed daily
---------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------	--------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------

McAfee is executing our Next Generation Firewall vision...
delivering visibility and control of applications & identities
new, innovative solutions to firewall workflow challenges
plus our integrated Global Threat Intelligence.

and those together
yield better, proactive support of the business,
savings/efficiencies for operations, and
better protection

F model update – Released Q3 09



- Increased Performance – Up to 200%
- McAfee Anti-Virus and McAfee SmartFilter URL Filtering included on all appliances by default
- Dell Remote Access Control – Out of band hardware control. Reboot, shutdown , boot and hardware diagnostics.

	410F	510F	1100F	2100F	2150F	4150F
Firewall Performance	1 Gb/Sec	2 Gb/Sec	6 Gb/Sec	6 Gb/Sec	10 Gb/Sec	12 Gb/Sec
Stateful Inspection Throughput	750 Mb/Sec	1.5 Gb/Sec	3 Gb/Sec	3 Gb/Sec	5 Gb/Sec	6.5 Gb/Sec
Application Filtering Throughput	600 Mb/Sec	1.2 Gb/Sec	2.5 Gb/Sec	2.5 Gb/Sec	3.5 Gb/Sec	5.0 Gb/Sec
AV	115 Mb/Sec	275 Mb/Sec	500 Mb/Sec	500 Mb/Sec	850 Mb/Sec	1 Gb/Sec
IPSec VPN Throughput	200 Mb/Sec	275 Mb/Sec	300 Mb/Sec	300 Mb/Sec	400 Mb/Sec	700 Mb/Sec



McAfee[®]