McAfee Web Gateway 7.0

Overview

Clive Lutley
McAfee System Engineer (NSU)

September 23, 2010
What will be covered

• Market Leading Technology
• Sample Rules
• Architecture Options
• The UI and Concepts
Market Leading Technology
Recognized Web Gateway Leader: Analyst reports

Gartner

“McAfee Web Gateway, backed by McAfee’s security expertise, is a solid choice for enterprise buyers looking for strong on-box malware protection…”

Forrester

“[McAfee] received the highest score on the technology portion of the evaluation...thanks to its innovative Web reputation technology and high-performing appliance,...”

IDC

IDC ranks McAfee #1 in Appliance Market Share – for web security appliances
Leading Independent Reviewers Rank McAfee Web Gateway a Leader

- Gartner: “Magic Quadrant Leader” three straight years
- Network World: “Clear Choice Winner” in their product reviews
- Forrester: “Leader” in its 2009 Web Filtering Wave
- IDC: “McAfee #1 in Market Share” in Web Security Appliances
- AV-TEST.org: “#1 ranking” 3 straight years, independent web gateway anti-malware testing
- SC Magazine: “Best Anti-Malware Solution 2010” Best Solution from 6 Finalists

Network World: “McAfee's Web Gateway appliance is our Clear Choice winner…McAfee's appliance thwarted more malware—with lower latency—than the other gateways.”
McAfee Web Gateway: Designed For Web 2.0

SECURITY
- Hybrid security
  - Local: Proactive anti-malware protection
  - Cloud-based: McAfee AV with Artemis, Web reputation
  - Deep content inspection including SSL traffic

CONTROL
- Inbound / outbound filtering of multiple Web protocols
- Productive use of Web 2.0: Application control
- Powerful policy engine
- Prevent data leakage
- Extensive reporting/auditing

PERFORMANCE
- Robust proxy / cache
- Enterprise scalability
- Flexible delivery: Appliances, VMware, blade
- Flexible deployment: Proxy, transparent bridge, transparent router
- Manage multiple Web security components
## McAfee Web Gateway

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware Proxy/Cache</strong></td>
<td>HTTP, HTTPs, FTP, RTSP, IM support, delegated and role based administration,</td>
</tr>
<tr>
<td></td>
<td>ePO integration, ICAP, Centralized Management, Flexible Network Options</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>Ensure proper Web access by users: AD/LDAP, NTLM, eDirectory, Kerberos, cookie, IP range, etc</td>
</tr>
<tr>
<td><strong>SSL-Scanner</strong></td>
<td>Unlocks encrypted traffic, enabling HTTPS content inspection, anti-malware scanning and company policy enforcement. Extensive Certificate Control.</td>
</tr>
<tr>
<td><strong>DLP</strong></td>
<td>Inspection Platform for McAfee Network DLP solutions for HTTP, FTP, HTTPS via ICAP</td>
</tr>
<tr>
<td><strong>Web filtering</strong></td>
<td>Multi-lingual URL filtering, Integrated Web Reputation powered by McAfee Labs, cloud look-up option for both categorization and reputation</td>
</tr>
<tr>
<td><strong>Anti-Virus</strong></td>
<td>Virus filtering at the gateway utilizing the McAfee anti-Virus engine and real-time Artemis look-ups. Separation of Desktop and Gateway engine technologies.</td>
</tr>
<tr>
<td><strong>Web 2.0 Security</strong></td>
<td>In-depth, Zero-Day Proactive protection against Viruses, Worms, Trojans, and Spyware at the Internet gateway.</td>
</tr>
<tr>
<td><strong>Reporting Solutions</strong></td>
<td>Enterprise-level reporting on Web traffic.</td>
</tr>
</tbody>
</table>
Filtering traffic with MWG can be broken down into three distinct cycles.

**Request**
- HTTP(S) requests (outbound)
- FTP requests (commands)
- All IM messages (see IM.Direction property)

**Response**
- HTTP(S) responses (inbound)
- FTP responses (command results)

**Embedded**
- Optionally after Request or Response cycle
- Only when request or response body contains embedded objects
- For example elements of a zip file or a HTML tag object

There are also non filtering cycles, e.g.:

**Log Cycle**
- Runs after all other cycles at the end of a transaction
- The Log Cycle is always executed
www.trustedsource.org
URL Filtering within 7.0

Local Database:
45 Million Entries
URLs as well as IP addresses
Web Reputation
Safe Search Enforcement

Cloud Database:
80% more data than what is locally stored on the appliance
URL Geolocation
Artemis Lookups
Real Time information

In the past (even with MWG 6.x) customers needed to schedule downloads of the URL database. While this gave the customer good coverage there was that delta timeframe between downloads where they were working with limited as well as potentially different data than was available.
Average Customer Download: Every 6 hours.
Web Reputation powered by Global Threat Intelligence

McAfee Labs

Point Products

McAfee Labs

Threat Intelligence Analysts & Proprietary Algorithms

File Reputation

Email Reputation

Network Reputation

Web Reputation
# Anti-Malware is More Than Anti-Virus

Signature based detection is not enough to cover today’s targeted Malware attacks

<table>
<thead>
<tr>
<th>Anti-Virus</th>
<th>Intent Analysis</th>
<th>Anti-Malware</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Signature based Anti-Virus is important part of Anti-malware protection&lt;br&gt;• Stops “known threats”&lt;br&gt;• However it is only a single aspect of the complete solution&lt;br&gt;• Signature based detection is not enough to cover today’s targeted Web 2.0 Malware attacks</td>
<td>• Code authentication – Checks for Digital Signature on active code&lt;br&gt;• Media Type Filter - verification via “magic byte” analysis not MIME&lt;br&gt;• Behavioral Malware detector - scans for malicious script intent and removes offending function calls&lt;br&gt;• Behavioral exploit detector – inspects code for hostile behavior like buffer overflows, etc.</td>
<td>• Prevents OS, browser and application exploits as a result of:&lt;br&gt;• Protects from known malicious code&lt;br&gt;• Protects from unknown malicious mobile code for which no signature exists</td>
</tr>
</tbody>
</table>

... Anti-Malware is a unique combination of Signature-based Anti-Virus PLUS intent analysis of mobile code
Anti-Malware Protection for Web 2.0

ActiveX Controls & Browser Helper Objects
Windows Executables & Dynamic Link Libraries
Java Applets & Applications
JavaScript (in HTML, Stand-alone, in PDF), Visual Basic Script
Visual Basic for Apps macros in Office documents

**Intent Analysis:**
- Buffer overflow exploit detection
- Generic Trojan downloader detection
- Shell code detection
- Several other detection algorithms

Active code Fragments extracted or blocked

Security Policy maps classification into action

Local Intent Analysis engines enforce the conditions set by the site’s reputation, protecting from malicious active scripts, determining Intent when a signature cannot exist.

“Local Enforcement of Global Reputation.”
AV-Test is one of the worldwide leading providers of test scenarios analyzing effectiveness, behavior and speed of IT-security solutions.

Quarterly tests on 36 anti-malware products

McAfee Web Gateway consistently leads
IM Proxy

Supported Clients

- Free IM Filtering Features!
  - Control of IM usage via Screen Names
  - AntiMalware Scanning of Attachments
  - Embedded URL Scanning of Chat
  - Keyword Scanning of messages
  - Logging of Chat Sessions (not the actual Chat!)
Helix Proxy by Real Networks

Included at no extra cost with 7.0!

Reduce Bandwidth Costs: By eliminating redundant data transmission between the server and proxy, you require less bandwidth to receive the same amount of content. Lower bandwidth usage translates into savings to your bottom line.

Manage the Network: Cap inbound and outbound bandwidth, ensuring that mission-critical applications are not adversely affected by streaming activities.

Control Content: Helix Proxy authenticates every client request at the origin, so control of the content always stays at the proxy.

Security: Helix Proxy masks the IP address of your internal users.

Improve End-User Playback: By caching and splitting content closer to the end-user, Helix Proxy reduces transmission problems that degrade the quality of the playback experience.
## Complete One Box Solution

### URL Filter
- Multi-vector reputation-based filtering including IP, Message, Content, URL, geo-location
  - Yes

### Anti-Malware
- Signature-based anti-virus
  - Yes
- Cloud-based anti-virus look-ups
  - Yes
- Industry-leading, 3rd party tested, pro-active filtering/protection for unknown attacks
  - Yes
- Unlimited file size scanning
  - Yes
- Single appliance integration
  - Yes

### Other Features
- Authenticode filter – digital signatures
  - Yes
- Flexible rules-based filtering engine
  - Yes
- Streaming proxy support
  - Yes
ePO integration
  - Yes
- App control including IM
  - Yes
- Flexible authentication (cookie auth, Kerberos)
  - Yes
Operation Aurora

**Infected Malicious Sites**

Destination of launch page denied by **TrustedSource** based on reputation and category.

**Inbound Content Protection**

**Blocked by Proactive Scanning**

Proactive protection from malicious code by **Gateway Anti-malware**

- **Heuristic.BehavesLike.JS.Obfuscated.E**
- **Heuristic.BehavesLike.HTML.Suspicious.B**
- Runs Exploit Code
- **Heuristic.Exploit.CodeExec.PGPG**

**Downloads Dropper**

Destination of downloader denied by **TrustedSource**

**Downloaded Trojan**

Caught at Gateway by media type

- Decodes To
- **Trojan.Spy.Gen**

**Infected Machine phones home**

Blocked by **SSL Decryption**

- Ad.jpg
- File does not contain correctly structured JPG content

**Inbound Content Protection**

- Blocked by **Magic Byte Mismatch**

**Blocked by Virus Alert**
Experience the Benefits

**Background**

- Fortune 100 US corporation
- Existing web proxy/gateway installation

**Scanned**

- Ninety-two million URLs
- 346,000 websites and web objects

**Results**

- 280,000 URLs categorized incorrectly by current proxy
- 16,000 discrete web objects containing malware
- 50,000 URLs with unacceptable reputations

**Savings:**

- 1,000 desktops saved from infection
- Remediation costs: $150-$200 per desktop
- During POC: $150,000-$200,000 savings
- Extrapolated to entire organization: $900k to 1.2M savings per month
Understand Traffic and Simplify Investigations

McAfee Web Reporter
Stand-Alone Windows, Linux Software

• Pre-built and customizable reports and dashboards
• Real-time views with extensive drill-down capability
• Scheduled reporting in multiple languages quickly process GBs of data
• Enterprise features: delegated reporting options
## MWG 7 features vs benefits

<table>
<thead>
<tr>
<th>Features</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Streaming Proxies</td>
<td>Provides additional access control and bandwidth savings for streaming as well as reduced latency. Eliminates the need to reconfigure each desktop.</td>
</tr>
<tr>
<td>IM Proxies</td>
<td>Allows DLP and compliance enforcement for IM, allows to apply all security features of MWG to IM traffic.</td>
</tr>
<tr>
<td>Trusted Source SDK</td>
<td>New TS SDK adds supports a hybrid (local database plus online queries) lookup, providing a significantly enhanced coverage and real-time lookup for new sites.</td>
</tr>
<tr>
<td>Artemis</td>
<td>Artemis adds online virus lookup for executables, resulting in improved detection rate.</td>
</tr>
<tr>
<td>Logfiles per policy</td>
<td>Adds multi-tenant logging capabilities, makes the product the perfect fit for MSP/Telco, education or large enterprise environments.</td>
</tr>
<tr>
<td>Rule tracing</td>
<td>Improved troubleshooting.</td>
</tr>
<tr>
<td>Rule engine</td>
<td>New rule based policy engine provides un-matched flexibility, and adds additional multi-tenancy features.</td>
</tr>
<tr>
<td>64bit OS</td>
<td>Improved scalability.</td>
</tr>
<tr>
<td>New proxy architecture</td>
<td>New internal architecture and re-designed connection handling, resulting in improved scalability and overall robustness.</td>
</tr>
<tr>
<td>Search function</td>
<td>Simplified and faster administration through product-wide search for content in rules, lists and settings.</td>
</tr>
<tr>
<td>Hierarchical rules</td>
<td>Additional multi-tenancy capabilities</td>
</tr>
</tbody>
</table>
## High Level Feature Comparison

<table>
<thead>
<tr>
<th>Feature</th>
<th>6.x</th>
<th>7.0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Proxy/Cache</strong> with complete AAA functionality, Auditable configuration management, and Cache.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>In-depth, ultra-high performance Proactive <strong>Anti Malware</strong> protection against Viruses, Worms, Trojans and Spyware at the gateway</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Anti Virus</strong> filtering at the gateway with the McAfee Scanning engine.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>SSL Scanner</strong> which unlocks encrypted traffic, enabling HTTPS content anti-virus scanning and company policy enforcement.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>IM Proxy</strong> for the most common IM protocols, such as ICQ, AIM, MSN, Yahoo.</td>
<td>❌</td>
<td>✓</td>
</tr>
<tr>
<td>Native <strong>Streaming Proxy</strong> with support for RTSP, MMS with split streaming and caching.</td>
<td>❌</td>
<td>✓</td>
</tr>
<tr>
<td>Flexible <strong>Rule-base Policy Engine</strong> with high granularity and object oriented approach</td>
<td>❌</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Installation and Startup wizards</strong> for easy setup</td>
<td>❌</td>
<td>✓</td>
</tr>
</tbody>
</table>
Architecture Options
McAfee Web Gateway

Performance, Scalability and Connectivity

Content Security Blade Server

WG5500

WG5000

WW1100

WW500

SaaS
Security as a Service

Branch Office

Corporate HQ
Architecture possibilities and preferences

• Explicit
  – Direct
  – Proxy.pac

• Transparent
  – Bridge mode
  – Router mode
  – WCCP

• Next hop

• ICAP
• Using an external hardware load balancer is MFE best practice for HA MWG cluster installs.
-however-

• MWG 7 has several built in load balancing setups
  – Proxy HA
  – Router Mode
  – Bridge Mode

*** throughput may be limited by the 1gb NIC unless you manually configure channel bonding which is not currently supported in the GUI

• Redundant directors are support via VRRP or STP
  – Directors are the appliances that are used also as load balancers
  – Scanning nodes are only used for scanning traffic
Proxy HA Mode

- Proxy HA Mode
  - proxy port on the director node
  - traffic is redirected to scanning nodes at kernel level
Transparent Bridge Mode

- **Bridge Mode**
  - director is plugged into the network path like a bridge
  - no proxy configuration on the client
  - selected destination ports are intercepted
  - transparent: director keeps IP and MAC
  - use Spanning Tree Protocol to switch redundant bridge(s) into blocking state
Transparent Router Mode

- **Router Mode**
  - director has to be in the routing path, e.g. as default gateway
  - no proxy configuration on the client
  - selected destination ports are intercepted
  - transparent: director keeps IP
Concepts – Find your way around

- The new java based web interface is separated into 5 main Sections

- Each Section might have tabs for sub-sections
- Settings are arranged in a tree structure for easy access
Concepts – Find your way around

• The Dashboard will give you a good overview of current system statistics

• If you have multiple MWGs in a cluster, you can view Dashboards from different appliances in one interface
Feature set of 7.0 (DashBoards)

11 Default Dashboards are available within 7.0

Example: Malware Statistics gives you an list of the Malware names as well as the URLs that delivered it.

Multiple MWGs Dashboards can be viewed directly through the single administrative gui
• Under “Policy” you will be able to configure ALL your filtering Rules
• You can find three tabs that will give you the options to configure everything you need for filtering
Concepts – Find your way around

• The “Configuration” section will show all the options to configure general settings and the appliance itself
  
  – Licensing
  – Clustering
  – Proxy mode and ports
  – Network settings
  – Monitoring/SNMP
  – General Log File settings like pushing and rotation
Concepts – Find your way around

• On the “Accounts” tab you will configure users and permissions for the administration of MWG
“Troubleshooting” will allow the MWG administrator to execute common tasks from the web interface

- Feedback.sh
- Tcpdump
- Log file viewing
- etc
Rule-Based in MWG7

Request Cycle

- URL is in Global Whitelist
  - Allow Whitelist Sites
  - Block

- URL is in Global Blacklist
  - Block

- Authenticate
  - isAuthenticated = false
  - Block

- Is URL High Risk Reputation?
  - Allowed Sites Only
  - Block

- User = jsmith
  - ClientIP is in Allowed IP List
    - Allowed Sites for jsmith only
    - Block

- Group = Webmail Users & URL in WebMail Category
  - Allow Webmail Sites

- Group = Domain Users
  - Allow Default Sites

Response Cycle

- Virus and Malware Scanning
- Cache this Content?
- Is SSL Certificate Valid?
- Zip File is Encrypted
- Body contains List of bad words
- Media Type = MP3?

- Block
- Cache
- Block
- Bypass AV Scanning
- Block
- Block
- Block MP3

• Every Rule is user-defined.
• No hard-coded sequence of events.
• Conditions can be added as needed.
• Multiple levels of nested rules.
• Infinite combinations of conditions.
Rule Sets

- **Rule Set**
  - Set of Rules
  - Applies to Requests, Responses & Embedded Cycle

- **Rules**
  - **Sequential evaluation of Rule Criteria**
    - Property, Operator, Operand
  - **Action**
    - Continue (go to next rule)
    - Block (display Block Page)
    - Redirect (to another page)
    - Stop Rule Set (go to next Rule Set)
    - Stop Cycle (stop further filtering-Allow traffic)
    - Authenticate
    - Remove (content from page)
  - **Events**
    - Perform a System Action, such as:
      - Send Alert
      - Manipulate Headers or Body
      - Next-Hop Proxy, etc.
    - Set Property (manipulate variables and counters)
    - Set Log Handler or Error Handler

- **Rule Criteria**
  - **Property**
    - Variables in the system to make decisions on. (URL, Client.IP, isInfected, etc)
  - **Operator**
    - Comparisons. (Equals, Greater than, Contains, Is in list, etc.)
  - **Operand**
    - Parameter to compare to. (Category, String, Boolean, Wildcard Expression, etc.)
Your requested URL has been blocked by the McAfee Web Gateway URL Filter database module. The URL is listed in categories that are not allowed by your administrator at this time.

**URL:** http://www.jimbeam.com/
**URL Categories:** Alcohol
**Reputation:** Minimal Risk
**Media Type:**

---

**Company Acceptable Use Policy**

This is an optional acceptable use disclaimer that appears on every page. You may change the wording or remove this section entirely in index.html.

---

**For assistance, please contact your system administrator.**
### Geographical Location

**URL.GeoLocation** is a string property that gets populated from a lookup to the Trusted Source Network.

**Embargoed Country List** is just a string list that was created with the two letter country codes for countries on the US Embargoed List.

By using the Operator “is in list” and a custom block page “Embargo Test” you can offer a level of control/protection that most others can’t do.

If you will notice there is also an AND statement with another rule based on self signed certificates that was added just to show how easy it is to create rules.

<table>
<thead>
<tr>
<th>Enabled</th>
<th>Name/Criteria</th>
<th>Action</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td><strong>Embargoed Countries restricted from using SSL with Self Signed Certificates</strong>&lt;br&gt;URL.Geolocation&lt;Default&gt; is in list&lt;br&gt;Embargoed Country List AND ssl.certificate.selfsigned equals true</td>
<td>Block   &lt;br&gt;<strong>Embargo Test</strong>&gt;</td>
<td></td>
</tr>
</tbody>
</table>
Other cool things? It's almost endless.

How about creating a clientless Site Advisor?
Other cool things? Its almost endless..

• Granular control over who uses the application and how it is used
  • Enabling or disabling specific functionality as needed
  • Allow Facebook, but block all Games or specific, e.g. Mafia Wars

• Example below: Using the policy engine to determine if a user can view YouTube videos, and what kind of Videos they may view!