Protect your internal users on the Internet with Secure Web Gateway

Richard Bible
EMEA Security Solution Architect
Identity and Access Management (IAM) Solution
Authentication, Authorization, and SSO to All Apps

- Cloud based web security
- True identity and context aware
- BIG-IQ Central management and reporting

Secure Web Gateway

- Internet Apps
- Internet
- Enterprise Apps
- Cloud, SaaS, and Partner Apps

- Mobile Apps
- Web Access Management
- Enterprise Mobility Management
- Remote Access and Application Access
- Federation
Employee personal web use at work is a problem

US workers spend between 60% - 80% of their time at work surfing non-work related websites.

- Surf news sites: 37%
- Update Facebook daily from work*: 15%
- Of “Cyber Monday 2013” purchases made from work: 49%

*Most visited non-work related website

Sources: Salary.com, InsideView, Forbes, Comscore
And, web-borne threats becoming more sophisticated and difficult to detect

- Watering Hole Attacks
- Drive-by Downloads
- Spearphishing
Why web defenses are a necessity today
However, most web defenses fail

- Primarily based on signature and reputation
- Lack of real-time inline content analysis
- Forward facing only, lacks outbound protection
- "More of the same" in new deployment options
- SSL lacks visibility
What is a secure web gateway

According Gartner, secure web gateway solutions protect Web-surfing PCs from infection and enforce company policies.

Filter unwanted software and malware from user-initiated web traffic

Enforce compliance with corporate and regulatory policies

Must include URL filtering, malicious code detection and filtering, web app controls, and limits bandwidth
F5 Secure Web Gateway Services

- Acceptable use policy and compliance controls
- Context-aware web security/protection
- Inbound and outbound malware protection
- Bandwidth control and preservation
F5 Secure Web Gateway Services consolidate infrastructure and maintenance costs

- Single integrated solution (BIG-IP, VIPRION) vs. two-box (ProxySG + Proxy-AV) solution
- Total cost of ownership savings between 29% - 72%, depending on service (URL Filtering or SWG Services), subscription length (1-year or 3-year), and number of users
F5 Secure Web Gateway Services
One-stop for all access policy, inbound and outbound

- Reduces chances of human error
- Strengthens policies
- Reduces overhead
- Increases security posture
- Deliver consolidated policy views – both inbound and outbound
F5 SWG Services Mitigate Threats, Cut Costs, and Increase Productivity and Availability

- Identify and eradicate malicious websites, web-based malware, and APTs
- Simply enforce corporate Web use policies and regulatory compliance
- Plug data leaks
- Restrict access to non-work related web sites based on policy, user, group, time, and more
- Increase bandwidth availability
Web access and activity visibility + the only web gateway to secure against inbound and outbound malware

- Maps and tracks user identity to network addresses
- Fully tracks activity by user identity and their device
- Enable transparent user-based security policies through F5 User Identity Agent
- Link user identity with endpoint integrity, assuring endpoint health prior to and after Web access
- F5 User Identity Agent runs on a Windows-based server, and pulls information from Active Directory domain controllers
Advanced Threat Protection

- Real-time threat analysis and intelligence
- Composite reputation scoring and predictive analysis
- Malware sandbox analysis
- Social app and video controls
- Graphical reporting and comprehensive logging

Robust malware database with over 10,000 web malware analytics and collection of signature and heuristic detection engines

Powerful URL categorization engine and database, constantly classifying over 40 million URLs

BIG-IP Platform

Devices

Data

APM with SWG
Flexible deployment options limit network change and churn

Explicit Proxy Mode

Proxy: `<f5swg_ip>:<f5swg_port>`

Connect: `<f5swg_ip>`
User: `user_id@<dest_host>`

Inline Transparent Proxy Mode

**Access Policy Management**
**URL Filtering (Outbound)**
**Social Media App Controls**

- **Client**
  - Tablet
  - Laptop
  - Desktop
  - Infected Laptop

- **Internet**

- **Web Surfing (HTTP/HTTPS)**
  - Off-premise web traffic
  - On-premise web traffic

- **Web App Servers**
Secure Web Gateway architecture diagram
Secure Web Gateway solution diagram

Customer Scenarios
- Context-Aware Web Security
- Bandwidth Controls
- Acceptable Use Policy Controls
- Compliance

Customer Functionality
- User Identification/Endpoint Inspection
- URL Filtering
- Web Access Policy Enforcement
- Malware Protection
- Identity Federation

Professional Services and Support
- Visibility (Logging)
  Human Resources
- Control (Reporting)
  IT/Security Admin

Corporate Network
- Contractor
- Employee
- PCI CDE

Remote Users
- Guest User
- Mobile User

Cloud-Based Threat Intelligence

Centralized Management

Secure WebGateway Services

Acceptable Websites
- Infected Executable Files
- Update Servers
- Infected Web Apps
- SaaS
- Inappropriate Websites

F5 Agility 2014
Secure Web Gateway solution diagram

Customer Scenarios:
- Context-Aware Web Security
- Bandwidth Controls
- Acceptable Use Policy Controls
- Compliance

Cloud-Based Threat Intelligence
Centralized Management

Secure WebGateway Services

Customer Functionality:
- User Identification/Endpoint Inspection
- URL Filtering
- Web Access Policy Enforcement
- Malware Protection
- Identity Federation

Professional Services and Support

Customer Functionality:
- Acceptable Websites
- Infected Executable Files
- Update Servers
- Infected Web Apps
- SaaS
- Inappropriate Websites

Corporate Network:
- Contractor
- Employee
- PCI CDE

Remote Users:
- Guest User
- Mobile User

Visibility (Logging):
- Human Resources

Control (Reporting):
- IT/Security Admin

F5 Agility 2014
Secure Web Gateway solution diagram

Customer Scenarios:
- Context-Aware Web Security
- Bandwidth Controls
- Acceptable Use Policy Controls
- Compliance

Customer Functionality:
- User Identification/Endpoint Inspection
- URL Filtering
- Web Access Policy Enforcement
- Malware Protection
- Identity Federation

Professional Services and Support:
- Visibility (Logging)
- Control (Reporting)

Corporate Network:
- Contractor
- Employee
- PCI CDE

Remote Users:
- Guest User
- Mobile User

Secure Web Gateway Services:

Cloud-Based Threat Intelligence
Centralized Management

Acceptable Websites
Infected Executable Files
Update Servers
Infected Web Apps
SaaS
Inappropriate Websites
Accommodating licensing models

- Annual Subscription services – 1-year or 3-year subscriptions
- Pricing ranges depending on platform – Virtual, BIG-IP or VIPRION – and number of filtering sessions (500 – 80,000)
- Only activated on top of F5 Access Policy Manager (APM) enabled platforms
- Session limits are defined and enforced on each platform ensuring future capacity and security service expansions
So let's look at the details…
Option #1: Secure Web Gateway
- URL classification and filtering (as defined)
- Support for custom URL categories (URL white/black lists)
- Connection to cloud-based threat intelligence infrastructure
- Web-based malware and advanced threat protection
- Granular social web applications detection and control
- User identification
- User based policy, graphical reporting and logging

Option #2: URL Filtering
- URL classification and filtering (as defined)
- Support for custom URL categories (URL white/black lists)
- Connection to cloud-based threat intelligence infrastructure
- Granular social web applications detection and control
- User identification
- User based policy, graphical reporting and logging
• **Real-Time Security Classification** – Empowers social web controls, and inspects all web content for malicious or suspicious code such as open or obfuscated scripts, exploit code and iframe tags

• **Real-Time Content Classification** – Employs advanced machine learning to quickly and accurately classify pages based on content including images, multimedia, and links

• **Real-Time Data Classification** – Classifies structured and unstructured data with paring and decoding support to address outbound data theft

• **Anti-Malware Engines** - Applies multiple anti-malware engines to identify both general and specialized malware

• **Reputation Analysis** - Considers more than twenty characteristics for detailed assessment and more accurate reputation scoring that encompasses contextual awareness

• **URL Classification** - Used independently and in conjunction with other defense assessments to apply current classification information for known pages, or to help assess new pages and links

• **Anti-Spam/Spear-Phishing** – Provides matchless, proactive protection against traditional and emerging threats in email
## Database Update Types

- Three types of updates

<table>
<thead>
<tr>
<th>Type of download</th>
<th>Schedule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master</td>
<td>Daily, sometime during the specified update window</td>
<td>Updates the categories and the URL's in them</td>
</tr>
<tr>
<td>RTSU</td>
<td>Every 5 Minutes, not configurable</td>
<td>Real time updates, that is the latest URLs that have been categorized</td>
</tr>
<tr>
<td>ACE</td>
<td>Every 5 Minutes, not configurable</td>
<td>Updates data that is used for Analysis, when necessary, to categorize a URL further</td>
</tr>
</tbody>
</table>
URL Categorization
URL Categories

- Custom categories may be added, in addition to the default categories that you want to block or allow.
- Custom Categories that you add become subcategories of Custom Categories.

![URL Categories Diagram]

- Name: F5-Custom
- Description: Customized pages to be blocked
- Associated URLs:
  - https://www.sitequest.com
  - http://www.sitequest.com:8080
Social Web Filters - Facebook

• **Facebook Posting**: Facebook function that enables a user to share a post, status or link.

• **Facebook Commenting**: Facebook function that enables a user to comment or like.

• **Facebook Friends**: Facebook function that enables a user to add a connection.

• **Facebook Photo Upload**: Facebook function that enables a user to upload a photo.

• **Facebook Mail**: Facebook function that enables a user to send an email within the Facebook community.

• **Facebook Events**: Facebook function that enables a user to create, modify or respond to an event within the Facebook community.

• **Facebook Apps**: Facebook function that enables a user to access or utilize an app.

• **Facebook Chat**: Facebook function that enables a user to chat within the Facebook community.

• **Facebook Questions**: Facebook function that enables a user to ask a question within the Facebook community.

• **Facebook Video Upload**: Facebook function that enables a user to upload a video.

• **Facebook Groups**: Facebook function that enables a user to create, modify or join a group within the Facebook community.

• **Facebook Games**: Facebook function that enables a user to access or play a game.
Social Web Filters – LinkedIn, Twitter, & YouTube

• LinkedIn:
  • LinkedIn Updates: LinkedIn function that enables a user to edit a profile or post an update.
  • LinkedIn Mail: LinkedIn function that enables a user to send an email within the LinkedIn community.
  • LinkedIn Connections: LinkedIn function that enables a user to add a connection.
  • LinkedIn Jobs: LinkedIn function that enables a user to perform activities related to job search

• Twitter:
  • Twitter Posting: Twitter function that enables a user to post an update.
  • Twitter Mail: Twitter function that enables a user to send an email within the Twitter community.
  • Twitter Follow: Twitter function that enables a user to add a connection.

• YouTube:
  • YouTube Commenting: YouTube function that enables a user to comment, like or dislike.
  • YouTube Video Upload: YouTube function that enables a user to upload a video.
  • YouTube Sharing: YouTube function that enables a user to share a video within and outside of the YouTube community.
SWG and Instant Messaging

- Secure Web Gateway (SWG) supports HTTP and HTTPS-based instant messaging protocols.

- As a result, when you use the Instant Messaging URL category to block messages, SWG can block messages to ICQ, for example, but cannot block messages from applications that use non-standard ports or tunneling over HTTP, such as, Yahoo Messenger, Skype, Google Talk, and so on.

- Similarly, SWG cannot block messages from file-sharing and peer-to-peer protocols that do not use HTTP or HTTPS; most do not.
URL Filtering
Default URL Filters

- Default URL Filters such as *block-all* and *basic-security* are available.
- You cannot delete any of the default filters, you can create new filters or copy existing ones.
Basic Security URL Filter

- Blocks the Security URL Category, and allows all other categories
URL Filters

• Custom URL Filters allow admin to **Allow** or **Block** any category or sub-category
URL Filters

- To block URLs that SWG cannot categorize, expand the category *Miscellaneous*, and select *Uncategorized*

- To use a URL Filter you must add it to a *Scheme*
Secure Web Gateway Schemes
Schemes

- You configure schemes to specify and schedule a group of URL filters that you want to apply to users.

<table>
<thead>
<tr>
<th>General Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Description</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Block</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default URL Filter</td>
<td>JIMS_CUSTOM_URLs</td>
</tr>
<tr>
<td>Content Scanning</td>
<td>Recommended</td>
</tr>
<tr>
<td>Max Buffer Size</td>
<td>1048576 bytes</td>
</tr>
<tr>
<td>Max Buffer Time</td>
<td>30 seconds</td>
</tr>
</tbody>
</table>

**What to do on uncategorized URL**

- Scan responses for malicious content.

**Schedule Settings**

- Time Range: 08:00 to 18:59
- Days Valid: Monday, Thursday, Friday

**Associated Schedules**

- JIMS_CUSTOM_URLs: 09:00 to 18:59, All Days of Week
Bringing it all together with APM VPE
Logging and Reporting
Sample Error/Blocking Messages

The hostname lookup was not successful.

Host: www.google.com

The proxy could not resolve the sitename you've requested. This site may not exist. Please check your spelling and try again if you feel you've encountered this message in error.

Click Go Back or use the browser's Back button to return to the previous page.

Access to this page is blocked.

Access was denied by a URL Filtering policy.

Click here to return to the previous page

The session reference number: d6148cbbd

The category reference is: Social Web - Twitter

This product is licensed from F5 Networks. © 1999-2013 F5 Networks. All rights reserved.
Policy, User Identity, Reports and Logs
Where to get more information

Follow up with your F5 channel partner and/or account manager

For detailed information, please go to f5.com/architectures

If I can be of further assistance please contact me:

r.bible@f5.com  |  +44 7919408772
Solutions for an application world.
Solutions for an application world.