Quick Start 2: Identifying and Troubleshooting filtering issues for Websense Web Security

Websense Support Webinar December 2012
Presenter

Greg Didier

Title:
– Support Specialist

Accomplishments:
– 9 years supporting Websense products

Qualifications:
– Technical Support Mentor
– Product Trainer
Goals And Objectives

• Understand how policies affect users
  – Filtering process
  – Understanding precedence
  – Exceptions to the rules

• Investigate policy enforcement issues
  – Where to start gathering information
  – How to analyze the data
    • Is the data correct?

• Take corrective action
Standalone Integration

- **Standalone mode**
  - Port spanning is required.
  - Filtering Service receives the lookup requests from Network Agent.
  - Filtering Service analyzes each lookup request and determines the appropriate security policy.
Third Party Integrations

• Integrated mode
  – Filtering Service receives the lookup requests from a third party integration.
  – Filtering Service analyzes each lookup request and determines the appropriate security policy.
Integration Modes

- **Independent of the integration type**, Filtering Service makes a policy determination.
- Some integration types can send additional information:
  - User name
  - URL for https traffic
Policies

- Websense policies enforce your company’s Internet use policy and consists of:
  - Category filters
  - Limited access filters
  - Protocol filters
  - Schedule (time and day the policy is active)

- Default policy has special use as a safety net:
  - Governs Internet access for all clients not assigned another policy
  - Initially, it permits all requests.
  - Always active
  - Cannot be deleted
To make sure a client does not fall through to the Default policy, assign another policy:

1. Create a policy (with predefined or custom category and protocol filters).
2. Define the time and day the policy applies.
3. Add one or more clients.
4. Assign the policy to the client.

Demonstration
• For any lookup request, the Websense Filtering Service:
  – Identifies the client object
  – Determines which policy applies
  – Determines if any policy restrictions apply

• Every block or permit action is the result of:
  – A single policy
  – A single specific restriction (blocked)
  – An absence of any restrictions (permitted)
To determine whether to block or permit a site, by default, exceptions or policies are applied in the following order:

1. Exception or policy assigned to the user
2. Exception or policy assigned to the IP address
3. Exception or policy assigned to the IP address range
4. Exception or policy assigned to groups
5. Exception or policy assigned to OU
6. The Default policy
   - Acts like a cleanup rule
   - Always applies when items 1 thru 5 are not matched
Client Considerations

• Optionally, configure directory policies to take precedence over IP address policies.
  – Modify the `UserGroupIpPrecedence` parameter and set it to `true`.

• When a user belongs to multiple groups or domains.
  – By default, the “least restrictive” policy applies.
  – Optionally, you may apply more restrictive blocking.
  – File Type blocking settings are ignored.
  – Limited access filter application may be counterintuitive.
To determine whether to permit or block a site, for the current day and time, Websense Web Security evaluates policy restrictions in the following order:

- **Exception**
- **Security Override**
- **Permit All or Block All category filter**
- **Limited Access Filter**
- **Protocol filter**
- **Recategorized URL**
- **Categorized in the Master Database**
- **Category filter**
- **Bandwidth restrictions**
- **File Type Restrictions**
- **Keyword blocking**
- **Quota Time**
- **Confirm**
Security Override

• In earlier versions, if a site was custom defined as an unfiltered URL or a recategorized URL in a permitted category, or if it appeared in a limited access filter, the site was permitted, even if the site was also assigned to a BLOCKED Security Risk category (like Malicious Web Sites, Spyware, or Phishing).

• Now, when Filtering Service determines a site belongs to a Security Risk category, the site is filtered based on the Security Risk status, even when it also resides in:
  – A recategorized URL
  – An unfiltered URL
  – A limited access filter

• Optionally, you may change the default behavior
• Filtering Service makes decisions based on a predefined list of rules.
  – The rules are conditional statements.
  – The applied policy is a result of a first-rule-match.
• Understanding these conditional rules will help you to identify and correct filtering issues quickly.
• Let’s explore these conditional rules.
Policy Enforcement Order

- Check whether an exception applies.
  - Note the **Security Override** check.

```
  Blocked by exception
   ^                  ^
   |                  |
  No                No
   v                  v
  Yes                Yes

  Security Override?
   ^                  ^
   |                  |
  Yes                No
   v                  v
  Permit             Permit
```
Policy Enforcement Order

• Check if a Permit All or Block All category filter, or a limited access filter applies.
  – Notice the second **Security Override** check.
Policy Enforcement Order

- Check the protocol filter (non-http), recategorized URLs, and Master Database.
Policy Enforcement Order

- Check the active category filter for:
  - Bandwidth Optimizer settings
  - File Type restrictions
  - Blocked Keywords
    - URL and CGI paths
Policy Enforcement Order

- Handles according to the action applied to the category (Permit, Limit by Quota, or Confirm).
To determine if a policy restriction exists, Filtering Service examines every lookup requests:

1. Client object
2. Policy
3. Filter
   - Either a category or protocol filter, or limited access filter

This determination processes continues until the request is either blocked or explicitly permitted.
Taking Corrective Action

• Filtering Service acts on the data provided.
  – Source IP address
  – Destination IP address
  – URL (http and ftp)
  – Protocol
  – User name

• Your actions:
  – Confirm the lookup request data
  – Identify the applicable client object
  – Identify the applicable policy
Taking Corrective Action

• End user must provide:
  – URL (or destination IP address)
  – Source IP address and user ID
  – Date and time of incident

• To examine filtering data:
  – Review the block page and hidden block page data.
    • Requires an active session with the end user.
  – Generate an Investigative Report.
  – Run Real-Time Monitor or the TestLogServer utility while recreating issue.
    • Requires an active session with the end user.
  – Toolbox
    • Determine affective category and policy
- Standalone versus third-party integrations
- Check for correct user name
- Investigative tools:
  - Reports (Real-Time Monitor and Investigative Reports)
  - Block page and hidden view source information
  - Toolbox options
  - TestLogServer utility
- Determine affective policy
- Allowing Web site access to:
  - A single user, multiple users, or all users
### Demonstration

<table>
<thead>
<tr>
<th>Filter Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block Exception</td>
<td></td>
</tr>
<tr>
<td>Security Override</td>
<td></td>
</tr>
<tr>
<td>Permit Exception</td>
<td></td>
</tr>
<tr>
<td>Permit All or Block All category filter</td>
<td></td>
</tr>
<tr>
<td>Limited Access Filter</td>
<td></td>
</tr>
<tr>
<td>Protocol filter</td>
<td></td>
</tr>
<tr>
<td>Recategorized URL</td>
<td></td>
</tr>
<tr>
<td>Categorized in the Master Database</td>
<td></td>
</tr>
<tr>
<td>Category filter</td>
<td></td>
</tr>
<tr>
<td>Bandwidth restrictions</td>
<td></td>
</tr>
<tr>
<td>File Type Restrictions</td>
<td></td>
</tr>
<tr>
<td>Keyword blocking</td>
<td></td>
</tr>
<tr>
<td>Quota Time</td>
<td></td>
</tr>
<tr>
<td>Confirm</td>
<td></td>
</tr>
</tbody>
</table>
Additional Information

• How do I know which policy my client is actually receiving?
• Where can I find information about why Filtering Service is blocking a page?
• Using How do I run TestLogServer without stopping the Log Server service?
• Prioritizing group and domain policies
• Limited access filters and filtering precedence
• Filtering a site
• Working with policies
• Lesson 12: Real-Time Monitor
Upcoming Webinar

Webinar Update

Title:
SSL Decryption: Benefits, Configuration, and Best Practices

Date:
January 25th, 2013

Time:
8:30 A.M. PST (UTC-8)

How to register:
http://www.websense.com/content/SupportWebinars.aspx
Training

• To find Websense classes offered by Authorized Training Partners in your area, visit: http://www.websense.com/findaclass

• Websense Training Partners offer classes online and onsite at your location.

• For more information, please send email to: readiness@websense.com