

# v7.5 Jump Start Part 2: Identifying and Troubleshooting Filtering Issues for Websense Web Security

**Webinar October 2010**



**Greg Didier**

- **Title:** Support Specialist
- **Accomplishments:**
  - 7 years supporting Websense products
- **Qualifications:**
  - Technical Support Mentor
  - Product Trainer

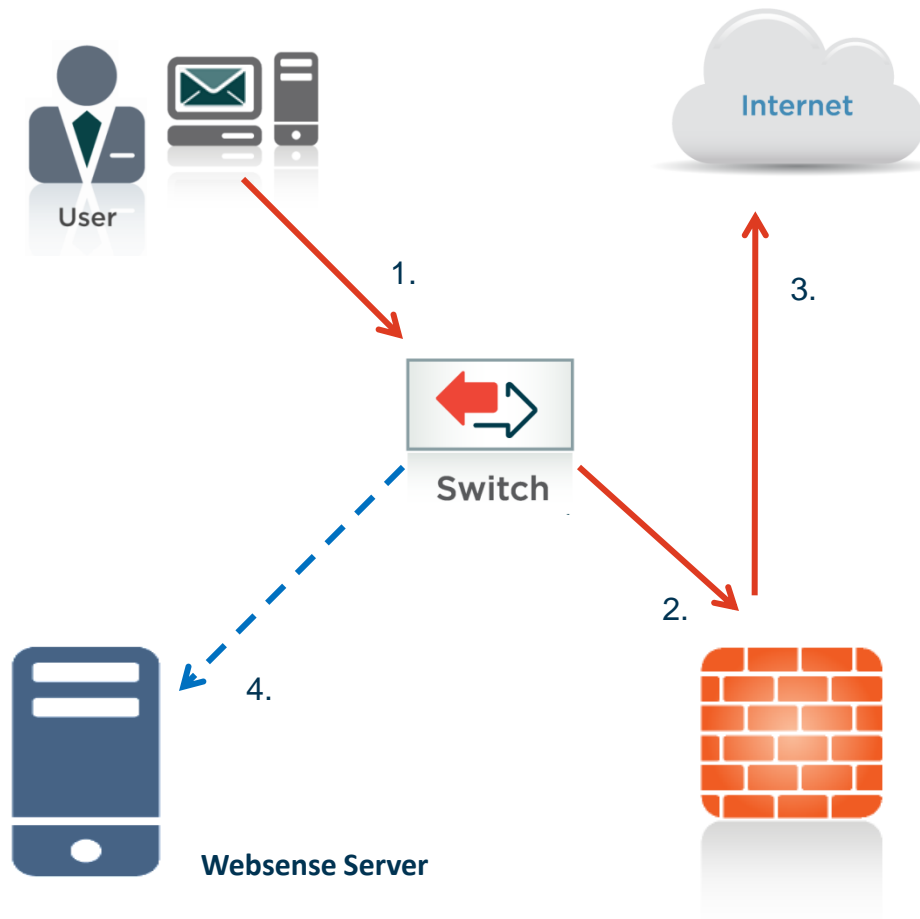
## ■ The filtering process

- How does a lookup request work?
- Websense component communication
- Precedence (filtering order)

## ■ Taking action

- Gather data
  - URL, time of issue, user name, source IP address
- Identify or confirm the policy being enforced
- Allowing site access
- Allowing file downloads

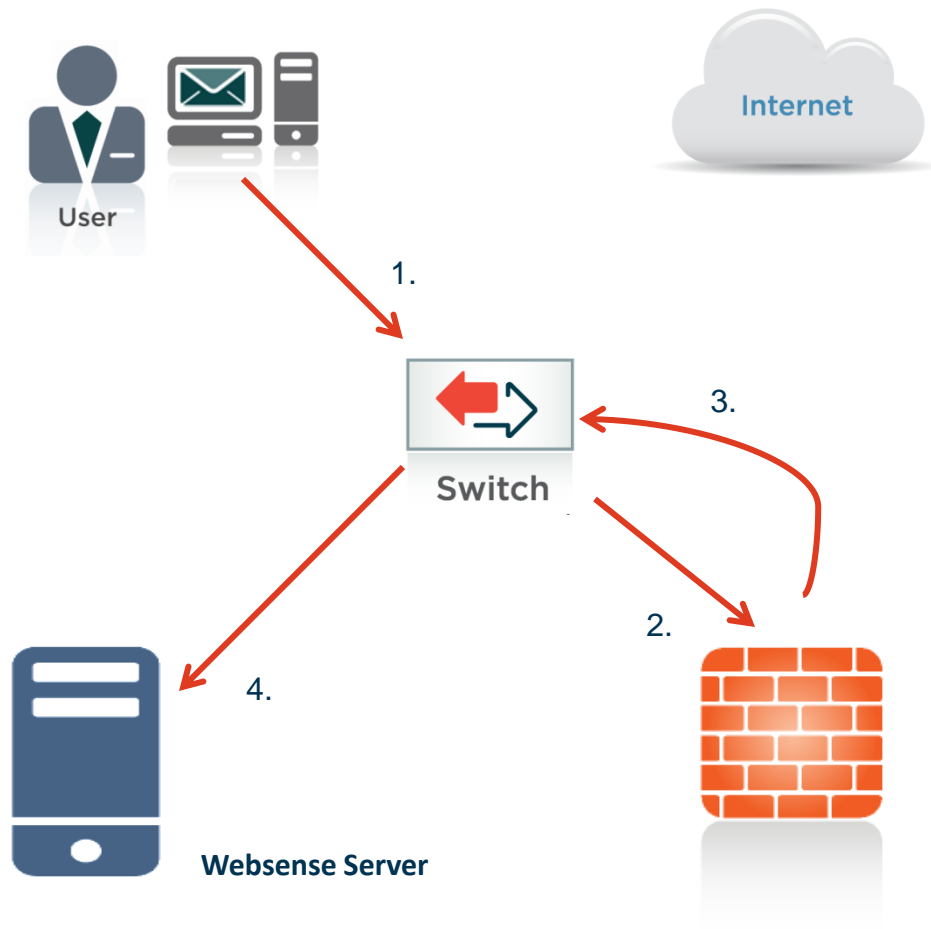
- Receiving lookup requests in standalone mode
  - Span, on the core switch, copies and sends all traffic to the Websense Network Agent service.



## Standalone mode

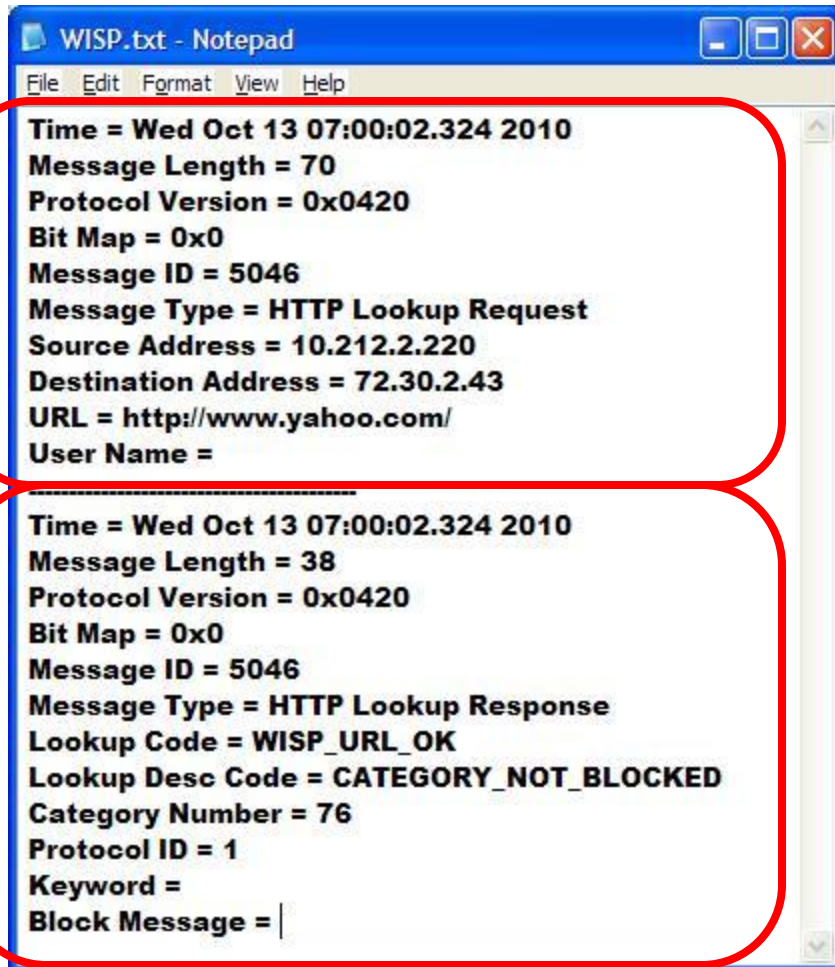
- The Network Agent, acting like a packet sniffer, generates and sends lookup requests to Websense Filtering Service.
- The Filtering Service analyzes each request and applies the appropriate filtering policy.

- Receiving lookup requests in integrated mode
  - A Firewall, proxy, or router generates and sends lookup requests to Websense Filtering Service.



## Integrated mode

- Filtering Service receives lookup request directly from the Integration.
- Filtering Service analyzes each lookup request and applies the appropriate filtering policy.



```
WISP.txt - Notepad
File Edit Format View Help
Time = Wed Oct 13 07:00:02.324 2010
Message Length = 70
Protocol Version = 0x0420
Bit Map = 0x0
Message ID = 5046
Message Type = HTTP Lookup Request
Source Address = 10.212.2.220
Destination Address = 72.30.2.43
URL = http://www.yahoo.com/
User Name =

-----
Time = Wed Oct 13 07:00:02.324 2010
Message Length = 38
Protocol Version = 0x0420
Bit Map = 0x0
Message ID = 5046
Message Type = HTTP Lookup Response
Lookup Code = WISP_URL_OK
Lookup Desc Code = CATEGORY_NOT_BLOCKED
Category Number = 76
Protocol ID = 1
Keyword =
Block Message = |
```

## Lookup Request

- URL
  - HTTP and FTP only
- Source IP address
- Destination IP address
- Protocol
- User name
  - From Proxy only

## Response

- Action
  - Block or Permit

- Filtering Service only sees:
  - Source IP address, destination IP address, URL (HTTP and FTP only), protocol, user name (proxy only)
- Filtering Service acts on the provided data
- Your response: permit or block
  - Identify and confirm the data
  - Identify the applicable filtering policy
  - Take action

- Site identified: needs to be permitted
- Use the provided URL
- Generate an investigative report
  - The user must provide you with the URL, source IP address, and time of incident.
- Examine the “view source” info on the block page
  - Hidden information on the Block Page
  - Requires active session with the end user
- Capture & examine the raw filtering data
  - Requires active session with the end user
  - Requires running the TestLogServer utility
- Demonstration

- To identify the data seen by Filtering Service
  - Use the provided URL
  - Generate an investigative report
    - Document: [Investigative Reporting Quick Start](#)
  - Examine the “view source” info
    - Help Guide: [Describes block page info, with an example](#)
  - Capture the raw filtering data
    - KB: [Step-by-step instructions for using TestLogServer](#)

## ■ Precedence

- Identifies the policy to enforce
  - Policies are associated with client objects
- Identify the filter to apply
  - A simple policy contains at least one category and one protocol filter
  - A single policy may contain multiple category and protocol filters
    - Each filter applies to a specific period of time
    - Time periods may represent, for example, before/after work hours, lunch, standard working hours, weekends, etc.

## ■ Filtering is determined by a “first match” method

## ■ Client objects

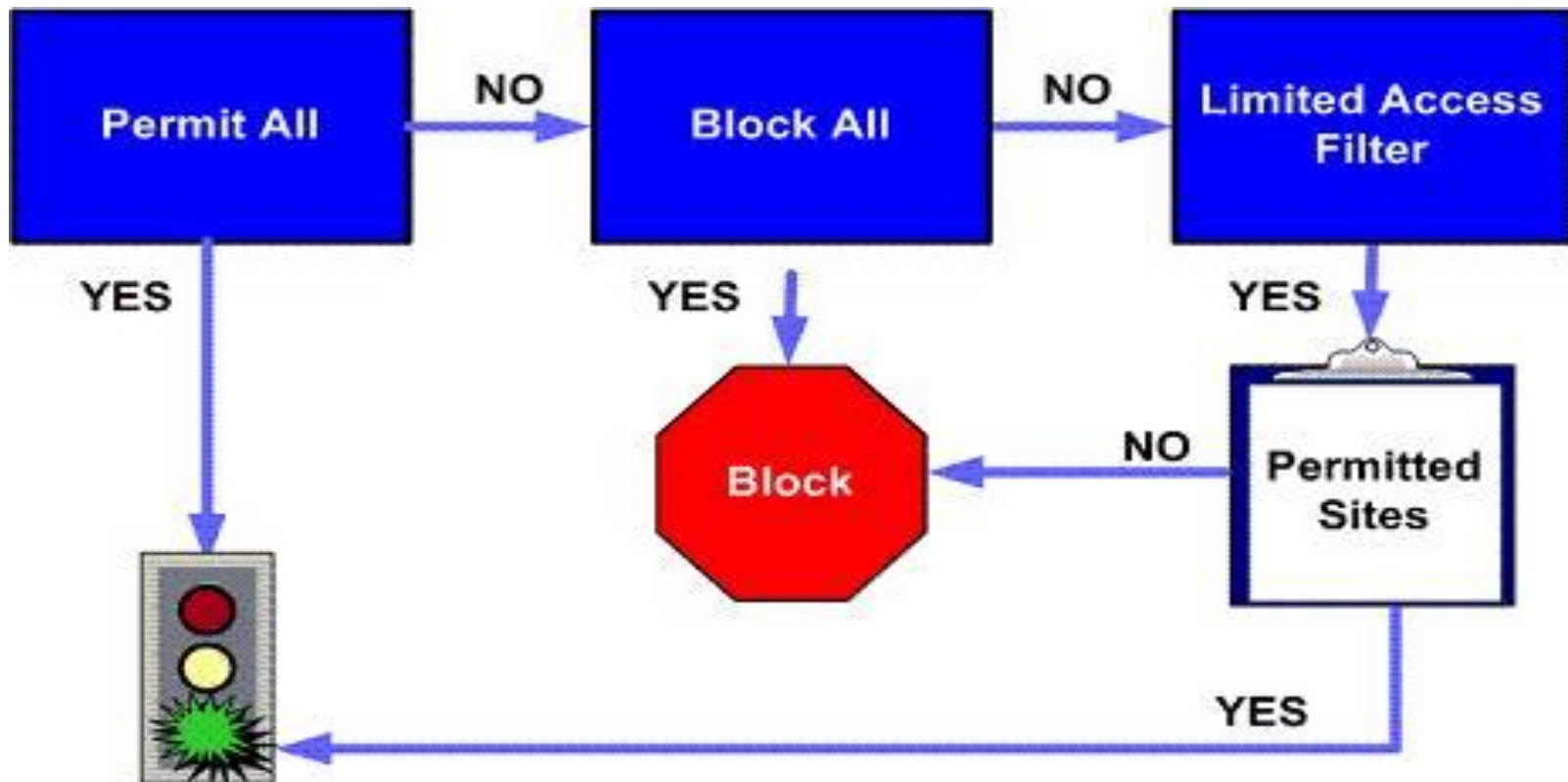
– Hierarchal (top down approach)

1. User
2. Computer (IP address)
3. Network IP (IP address range)
4. Group
5. OU (Organizational Unit)
6. Default Policy

– If items 1 thru 5 are not matched, then Default Policy always applies.

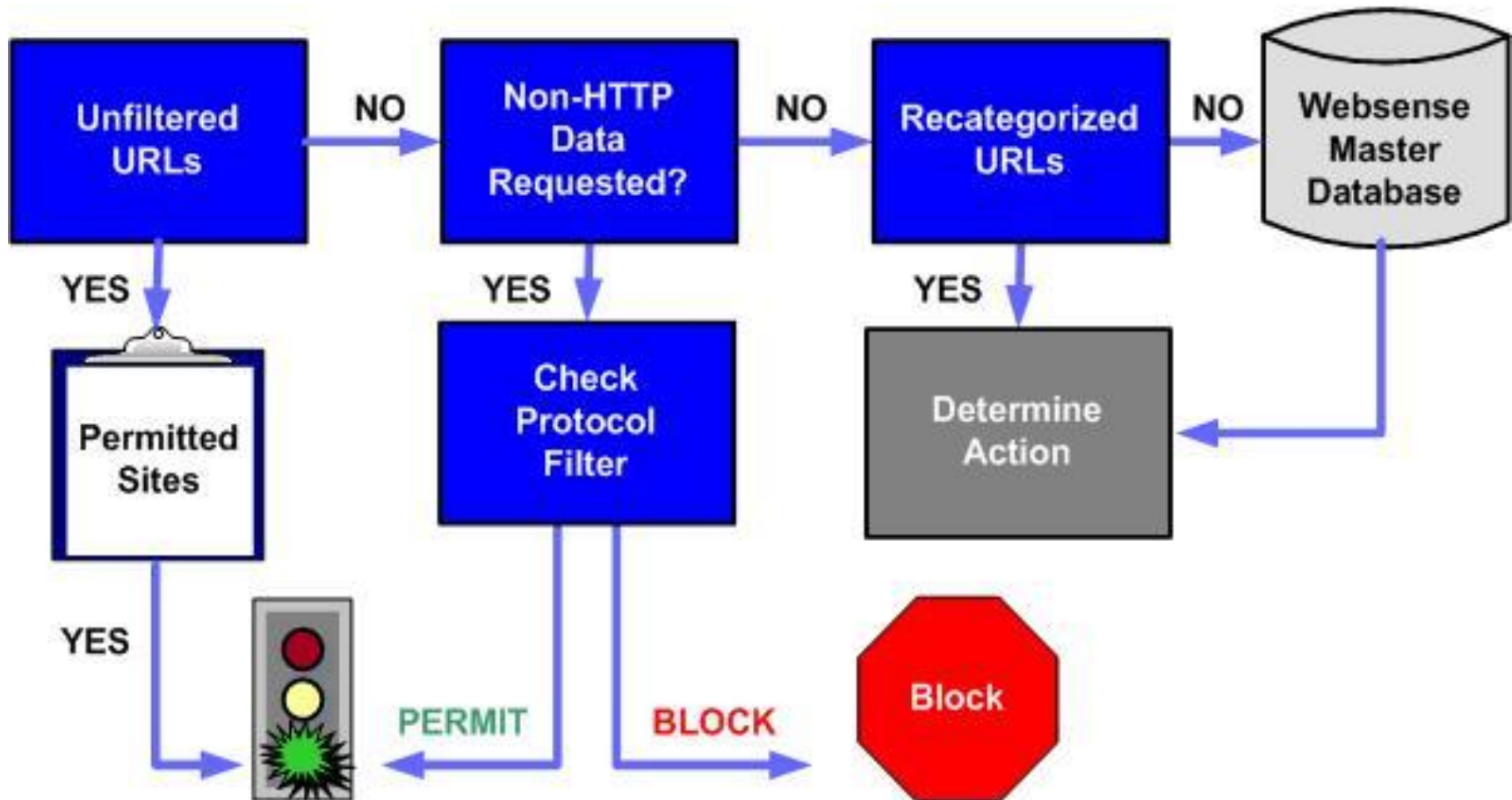
# Precedence – Indentify The Filter

- To determine whether to permit or block a site, Filtering Service does the following analysis:



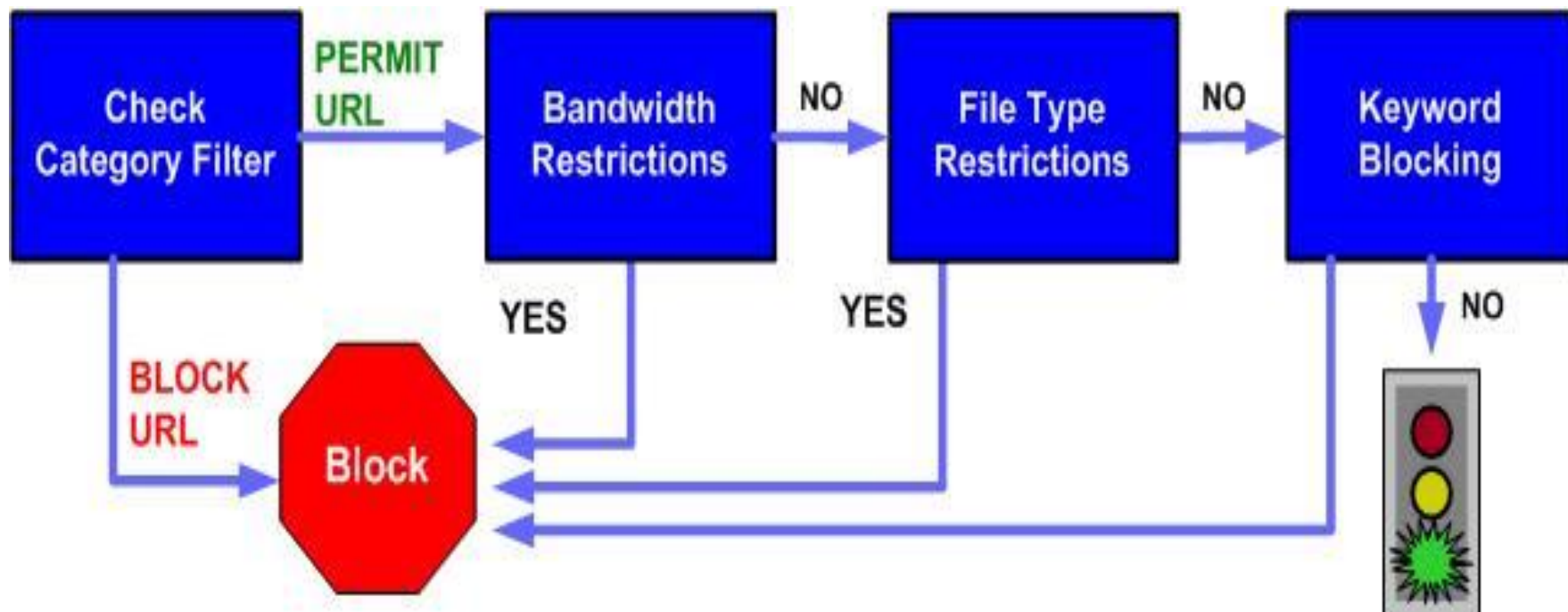
# Precedence – Indentify The Filter

- Filtering Service analysis continued:



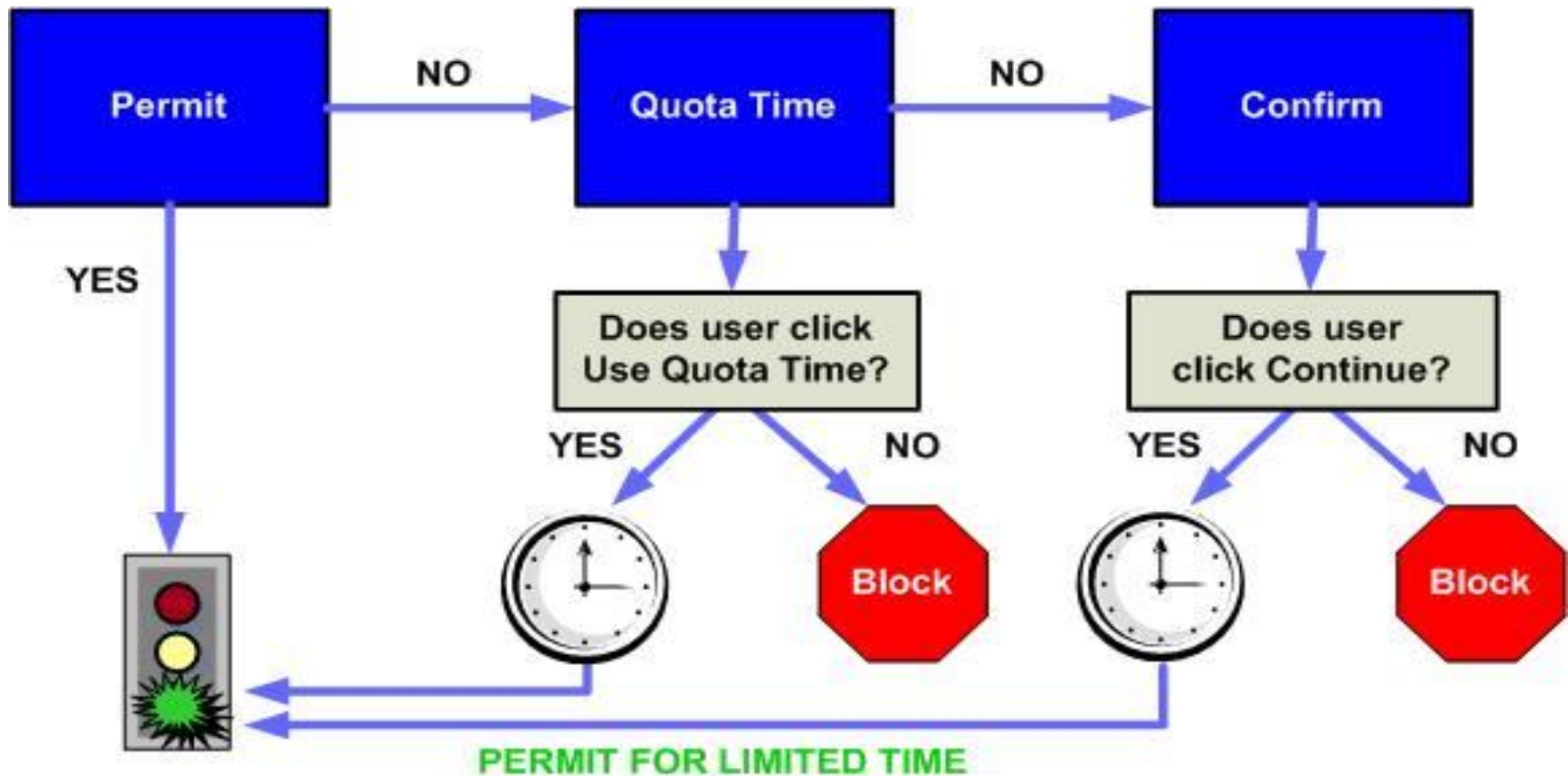
# Precedence – Indentify The Filter

- Filtering Service analysis continued:



# Precedence – Indentify The Filter

- Filtering Service analysis continued:



- To determine appropriate filtering, Filtering Service processes every lookup request using a top down approach.
  1. Client object
    - Client objects have an order of precedence
  2. Policy
  3. Filter
    - May be a category filter, protocol filter, or limited access filter.
    - Filters have an order of precedence
- Websense software processes the lookup request until it is either blocked or explicitly permitted.

## ■ Choices

- Unfiltered URLs
  - Permitted for all clients
- Recategorized URLs
  - Recategorize URLs to a different pre-defined category, or a custom category.
    - This allows for permitting access to some clients while blocking others
  - Allows for assigning keywords

## ■ Demonstration

- TRITON - Web Security: Main tab: Policy Management > Filter Components
  - Edit Categories
  - Edit Protocols
  - File Types
  - Unfiltered URLs

- To permit or block access
  - Unfiltered URLs
    - Permitted for all clients
  - Recategorize URLs
    - This allows for permitting access to some clients while blocking others

- Identify the enforced policy
  - Examine the “**view source**” info on the block page
- Examine filtering request
  - Run an **investigative report** on the user’s IP address
  - Run **TestLogServer** and examine the raw filtering data
- Automatically receive the view source data via email
  - [www.CustomBlockPages.com](http://www.CustomBlockPages.com)



**Websense Block Page Info**

File Edit View Insert Format Tools Message Help

Send Cut Copy Paste Undo Check Spelling Attach Priority Sign Encrypt Offline

To: wbsn\_admin@cns-test.com

Cc:

Subject: Websense Block Page Info

URL:<<http://testdatabasewebsense.com/adultmaterial>> <  
<!--  
User Name: [LDAP://192.168.1.118](#) CN=Users,DC=CNS-test,DC=local/Andrew Client Source IP Address: Current Time: 16:39  
This user is filtered by policy: role-8\*\*Headquarters. The policy includes a category or limited access filter for the current time.  
This policy is associated with role: Super Administrator.  
The request was categorized by: Master database.  
-->  
> Category:<Adult Material> CategoryID:<1> User Quota Time Available:<0>

**Troubleshooting Hot Spot:**  
Employees can hover over this spot to generate an email to the Websense® Administrator for Troubleshooting.

[www.CustomBlockPages.com](http://www.CustomBlockPages.com)

- TRITON - Web Security > Help > Help Contents > PDF
- Toolbox
  - URL Category
  - Check Policy
  - Test Filtering
  - URL Access
  - Investigate User

## Knowledge Base

- Search or browse the knowledge base for documentation, downloads, top knowledge base articles, and solutions specific to your product.

## Support Forums

- Share questions, offer solutions and suggestions with experienced Websense Customers regarding product Best Practices, Deployment, Installation, Configuration, and other product topics.

## Tech Alerts

- Subscribe to receive product specific alerts that automatically notify you anytime Websense issues new releases, critical hot-fixes, or other technical information.

## ask.websense.com

- Create and manage support service requests using our online portal.

# Customer Training Options

- To find Websense classes offered by Authorized Training Partners in your area, visit:  
<http://www.websense.com/findaclass>
- Websense Training Partners also offer classes online and onsite at your location.
- For more information, please send email to:  
[readiness@websense.com](mailto:readiness@websense.com)

**WEBSense®**  
**Authorized Training  
Partner**

**WEBSense®**  
**Certified Instructor**



## Webinar Update

Title: Troubleshooting Transparent Identification Agents for Websense TRITON – Web Security

Date: November 18, 2010

Time: 8:00 AM PDT (GMT -8)

How to register:

[http://www.websense.com/content/  
SupportWebinars.aspx](http://www.websense.com/content/SupportWebinars.aspx)

# Questions?

---

