finjan Vital Security™

securing your web

IBM URL Categories (Multiple Categories)

Vital Security 9.0 and 9.2

Copyright

For additional information, please visit www.finjan.com or contact one of our regional offices:

USA: San Jose 2025 Gateway Place Suite 180 San Jose, CA 95110, USA Toll Free: 1 888 FINJAN 8 Tel: +1 408 452 9700 Fax: +1 408 452 9701 salesna@finjan.com	Europe: UK 4th Floor, Westmead House, Westmead, Farnborough, GU14 7LP, UK Tel: +44 (0)1252 511118 Fax: +44 (0)1252 510888 salesuk@finjan.com
Israel/Asia Pacific Hamachshev St. 1, New Industrial Area Netanya, Israel 42504 Tel: +972 (0)9 864 8200 Fax: +972 (0)9 865 9441 salesint@finjan.com	Europe: Germany Alte Landstrasse 27, 85521 Ottobrun, Germany Tel: +49 (0)89 673 5970 Fax: +49 (0)89 673 597 50 salesce@finjan.com
General Information Email: support@finjan.com Internet: www.finjan.com	Europe: Netherlands Printerweg 56 3821 AD Amersfoort, Netherlands Tel: +31 334 543 555 Fax: +31 334 543 550 salesne@finjan.com

Table of Contents

1. Background 1

2. Methodology 1

3. Supported Solution 2

3.1 Example of Allow Rule in Outgoing Direction 3

3.2 Example of Related General Block Rule 4

1. Background

The IBM URL categorization engine in Finjan Vital Security categorizes approximately 20% of URLs with more than one category.

This approach easily addresses the requirements of Web 2.0.

The product currently features 68 categories. It would be impossible to map the Web closely to such a small number of categories.

The following example provides two approaches designed to address this issue:

There are several fine granular characteristics of a subject such as *Weapon*:

- Pages about shooting clubs
- Pages with military content
- Pages on which to buy weapons
- Pages with criminal backgrounds

2. Methodology

The first approach is to provide subcategories within a URL filter for each of these characteristics.

The second approach is to represent this fine granularity by combining different categories.

The disadvantage of the first approach is that there are, theoretically, an unlimited number of potential categories, which would make it necessary to update the static category list quite often.

On the other hand, combining different categories (as is done in Finjan's IBM URL categorization engine) results in the same fine granularity with much more flexibility. The following (IBM) category combinations represent the topical examples above:

- Weapons/Military; Sports
- Weapons/Military; Governmental Organizations
- Weapons/Military; Shopping
- Weapons/Military; Illegal Activities

The downside of this approach is that URLs in multiple categories can be blocked, even if they are part of an allowed category.

This will happen if the customer is working only with the standard URL Block Policy.

For more general details on the behavior of the Security Policy, see Security Policies In-Depth.

3. Supported Solution

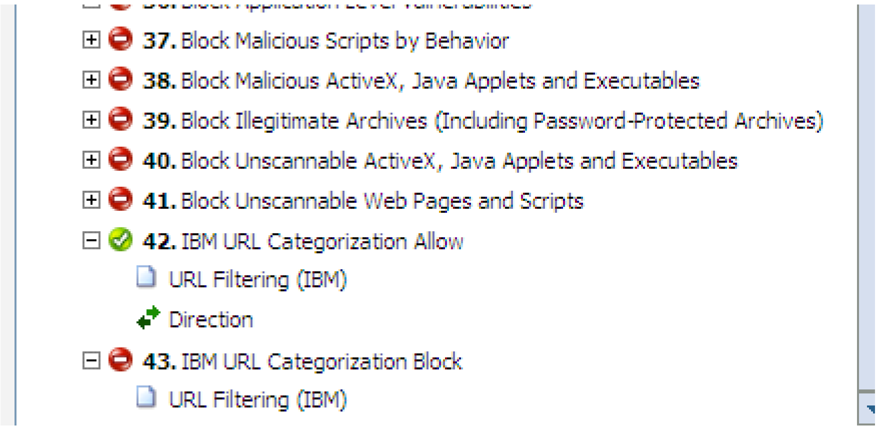
To ensure that customers do not have a significant increase in helpdesk calls, Finjan suggests the following workaround.

The normal setup with URL filter lists is a definition of the type of Web pages that are inappropriate based on company standards. Therefore, a policy with block-rules is normally used.

To ensure that all approved Categories can be processed by a multiple category engine (such as IBM's), the customer must whitelist all allowed categories before enabling the rule for blocked categories.

This assures that all URLs that have multiple categories, one of which is blocked, are still allowed by the Allow rule before they can be blocked.

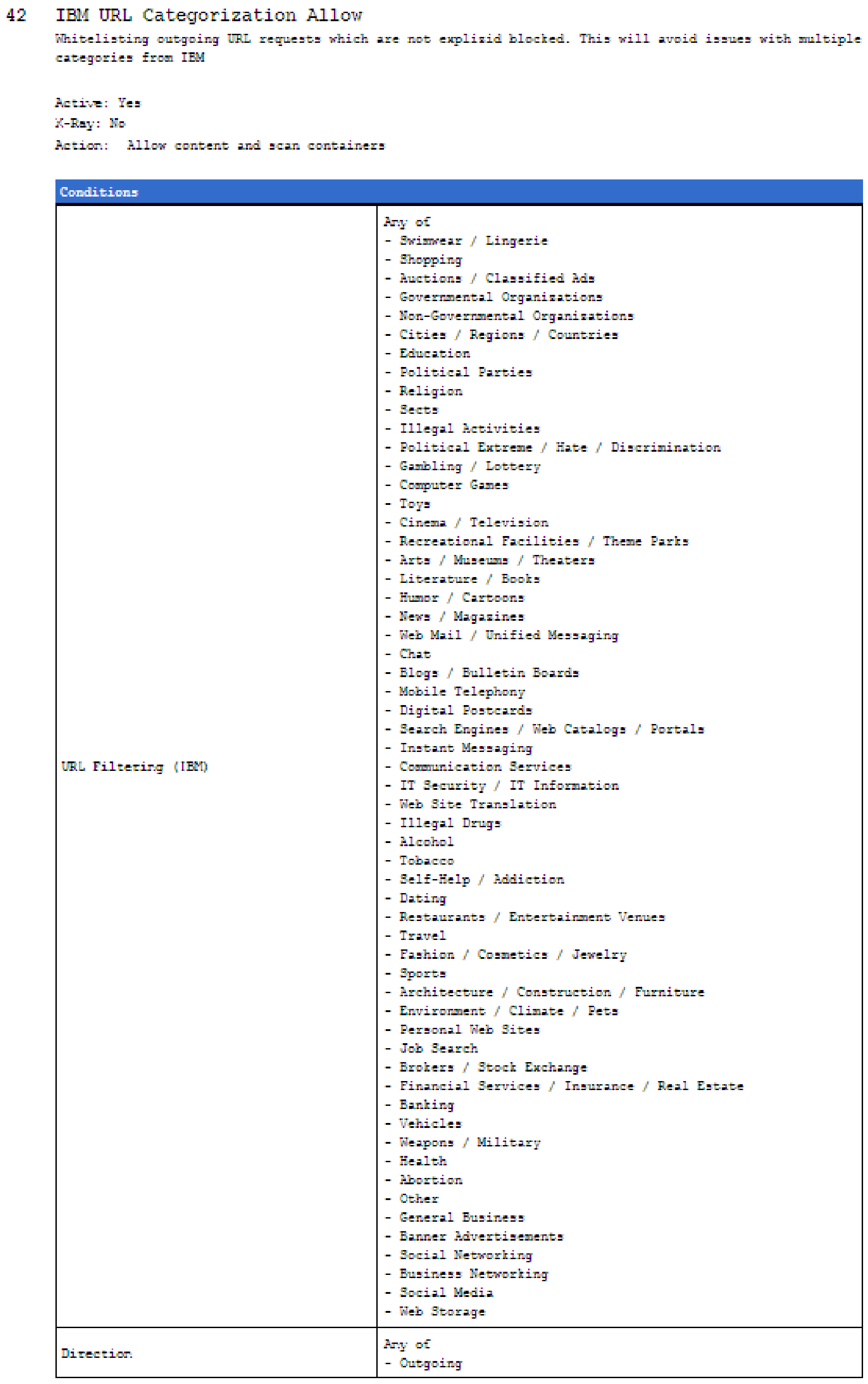
All other engines still work if this rule is placed at the end of the Policy (see the following example).



- ⊞ **36.** Block Application Level Vulnerabilities
- ⊞ **37.** Block Malicious Scripts by Behavior
- ⊞ **38.** Block Malicious ActiveX, Java Applets and Executables
- ⊞ **39.** Block Illegitimate Archives (Including Password-Protected Archives)
- ⊞ **40.** Block Unscannable ActiveX, Java Applets and Executables
- ⊞ **41.** Block Unscannable Web Pages and Scripts
- ⊟ ✓ **42.** IBM URL Categorization Allow
  - URL Filtering (IBM)
  - Direction
- ⊟ **43.** IBM URL Categorization Block
  - URL Filtering (IBM)

Note: The Allow rule must be defined for the outgoing direction (request phase) only.

3.1 Example of Allow Rule in Outgoing Direction



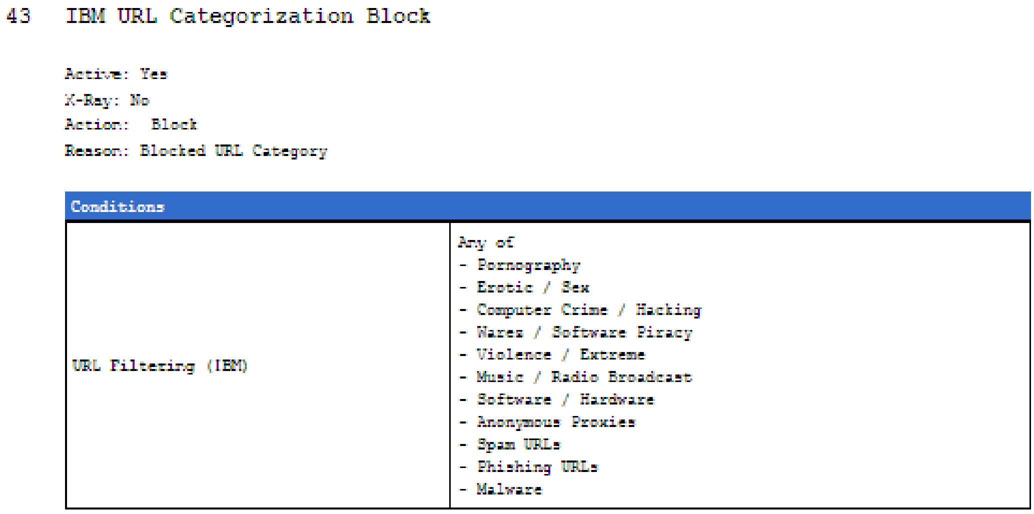
42 IBM URL Categorization Allow

Whitelisting outgoing URL requests which are not explizid blocked. This will avoid issues with multiple categories from IBM

Active: Yes
X-Ray: No
Action: Allow content and scan containers

Conditions	
URL Filtering (IBM)	Any of - Swimwear / Lingerie - Shopping - Auctions / Classified Ads - Governmental Organizations - Non-Governmental Organizations - Cities / Regions / Countries - Education - Political Parties - Religion - Sects - Illegal Activities - Political Extreme / Hate / Discrimination - Gambling / Lottery - Computer Games - Toys - Cinema / Television - Recreational Facilities / Theme Parks - Arts / Museums / Theaters - Literature / Books - Humor / Cartoons - News / Magazines - Web Mail / Unified Messaging - Chat - Blogs / Bulletin Boards - Mobile Telephony - Digital Postcards - Search Engines / Web Catalogs / Portals - Instant Messaging - Communication Services - IT Security / IT Information - Web Site Translation - Illegal Drugs - Alcohol - Tobacco - Self-Help / Addiction - Dating - Restaurants / Entertainment Venues - Travel - Fashion / Cosmetics / Jewelry - Sports - Architecture / Construction / Furniture - Environment / Climate / Pets - Personal Web Sites - Job Search - Brokers / Stock Exchange - Financial Services / Insurance / Real Estate - Banking - Vehicles - Weapons / Military - Health - Abortion - Other - General Business - Banner Advertisements - Social Networking - Business Networking - Social Media - Web Storage
Direction	Any of - Outgoing

3.2 Example of Related General Block Rule



43 IBM URL Categorization Block

Active: Yes
X-Ray: No
Action: Block
Reason: Blocked URL Category

Conditions	
URL Filtering (IBM)	Any of - Pornography - Erotic / Sex - Computer Crime / Hacking - Warez / Software Piracy - Violence / Extreme - Music / Radio Broadcast - Software / Hardware - Anonymous Proxies - Spam URLs - Phishing URLs - Malware