URL Filtering on a FireSIGHT System Configuration Example

Contents

Introduction

This document describes the steps to configure URL Filtering on FireSIGHT System. The URL filtering feature on FireSIGHT Management Center allows you to write a condition in an access control rule in order to determine the traffic that traverses a network based on non-encrypted URL requests by the monitored hosts.

Prerequisites

Requirements

This document has some some specific requirements for the URL Filtering License and the port.

Requirement of URL Filtering License

A FireSIGHT Management Center requires a URL Filtering license in order to contact the cloud periodically for an update on URL information. You can add category- and reputation-based URL conditions to access control rules without a URL Filtering license; however you cannot apply the access control policy until you first add a URL Filtering license to the FireSIGHT Management Center, then enable it on the devices targeted by the policy.

If a URL Filtering license expires, access control rules with category and reputation-based URL conditions stop filtering URLs, and the FireSIGHT Management Center no longer contacts the cloud service. Without a URL Filtering license, individual URLs or groups of URLs can be set to allow or block, but the URL category or reputation data cannot be used in order to filter the network traffic.

Port Requirement

A FireSIGHT System uses ports 443/HTTPS and 80/HTTP in order to communicate with the cloud service. Port 443/HTTPS must be opened bidirectionally, and inbound access to port 80/HTTP must be allowed on the FireSIGHT Management Center.

Components Used

The information in this document is based on these hardware and software versions:

- FirePOWER Appliances: 7000 Series, 8000 Series
- Next Generation Intrusion Prevention System (NGIPS) Virtual Appliance
- Adaptive Security Appliance (ASA) FirePOWER
- Sourcefire Software Version 5.2 or later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

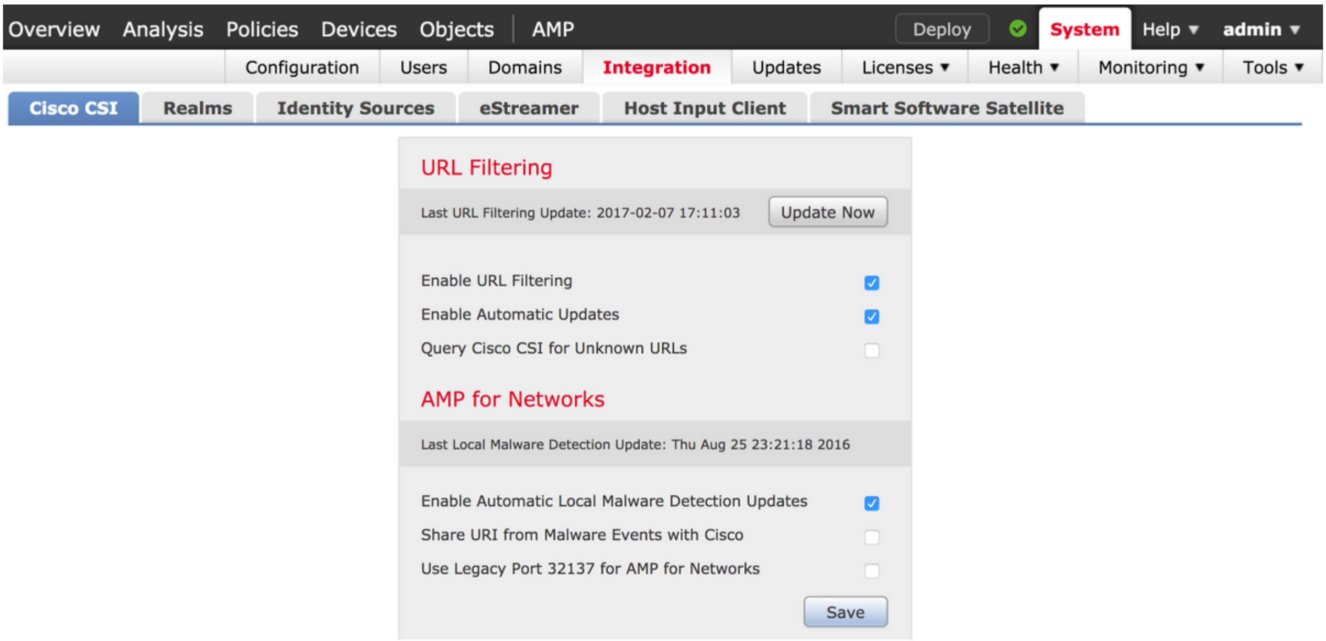
Enable URL Filtering on FireSIGHT Management Center

In order to enable URL Filtering, complete these steps:

1. Log into the web user interface of the FireSIGHT Management Center.

2. The navigation is different based on the software version that you run:

   On Version 6.1.x, choose **System > Integration > Cisco CSI**.



URL Filtering

Last URL Filtering Update: 2017-02-07 17:11:03

Enable URL Filtering ☑

Enable Automatic Updates ☑

Query Cisco CSI for Unknown URLs ☐

AMP for Networks

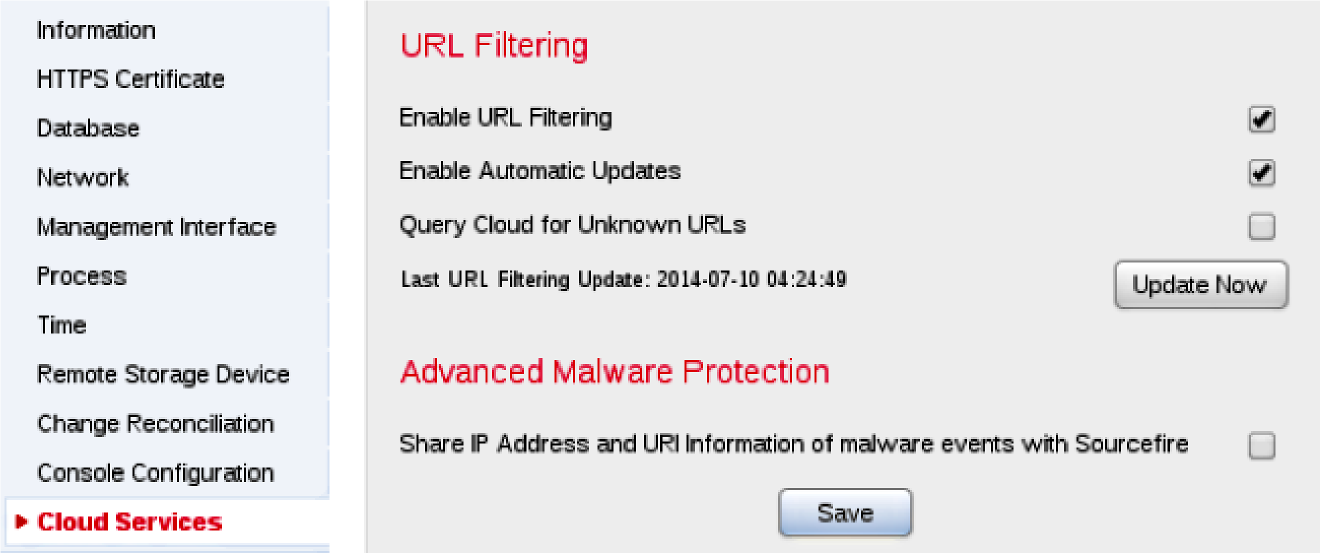
Last Local Malware Detection Update: Thu Aug 25 23:21:18 2016

Enable Automatic Local Malware Detection Updates ☑

Share URI from Malware Events with Cisco ☐

Use Legacy Port 32137 for AMP for Networks ☐

   On Version 5.x, choose **System > Local > Configuration**. Choose **Cloud Services**.



URL Filtering

Enable URL Filtering ☑

Enable Automatic Updates ☑

Query Cloud for Unknown URLs □

Last URL Filtering Update: 2014-07-10 04:24:49

Advanced Malware Protection

Share IP Address and URI Information of malware events with Sourcefire □

3. Check the **Enable URL Filtering** check box in order to enable URL Filtering.
4. Optionally, check the **Enable Automatic Updates** check box in order to enable automatic updates. This option allows the system to contact the cloud service on a regular basis in order to obtain updates to the URL data in the appliance's local data sets.

   Note: Although the cloud service typically updates its data once per day, if you enable automatic updates it forces the FireSIGHT Management Center to check every 30 minutes in order to make sure that the information is always current. Although daily updates tend to be small, if it has been more than five days since the last update, new URL filtering data might take up to 20 minutes to download. Once the updates have been downloaded, it might take up to 30 minutes to perform the update itself.

5. Optionally, check the **Query Cloud for Unknown URLs** for Unknown URLs check box in order to query the cloud service for unknown URLs. This option allows the system to query the Sourcefire cloud when someone on your monitored network attempts to browse to a URL that is not in the local data set. If the cloud does not know the category or reputation of a URL, or if the FireSIGHT Management Center cannot contact the cloud, the URL does not match access control rules with category or reputation-based URL conditions.

   Note: You cannot assign categories or reputations to URLs manually. Disable this option if you do not want your uncategorized URLs to be cataloged by the Sourcefire cloud, for example, for privacy reasons.

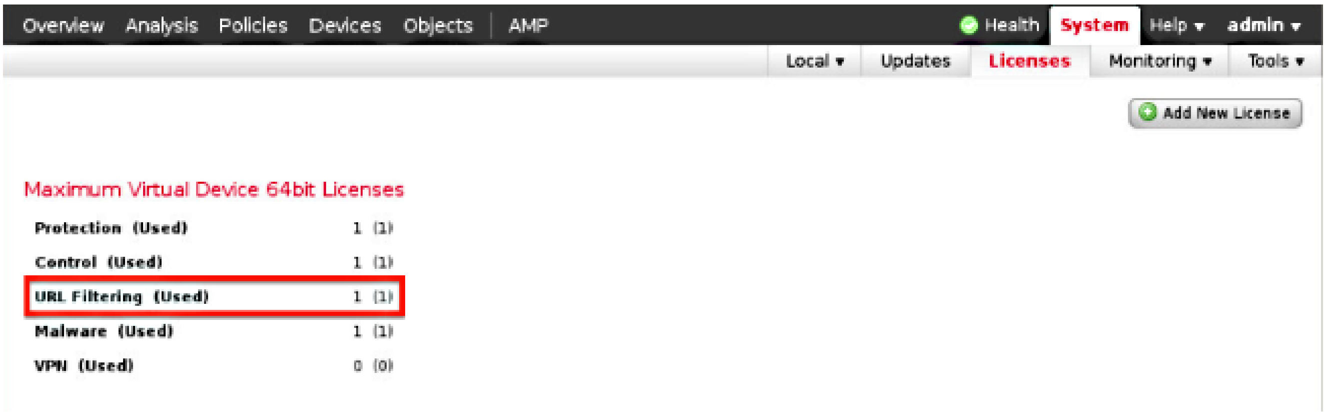
6. Click **Save**. URL Filtering settings are saved.

   Note: Based on the length of time since URL Filtering was last enabled, or if this is the first time you have enabled URL Filtering, a FireSIGHT Management Center retrieves the URL Filtering data from the cloud service.

Apply URL Filtering License on a Managed Device

1. Check if the URL Filtering license is installed on the FireSIGHT Management Center. Go to

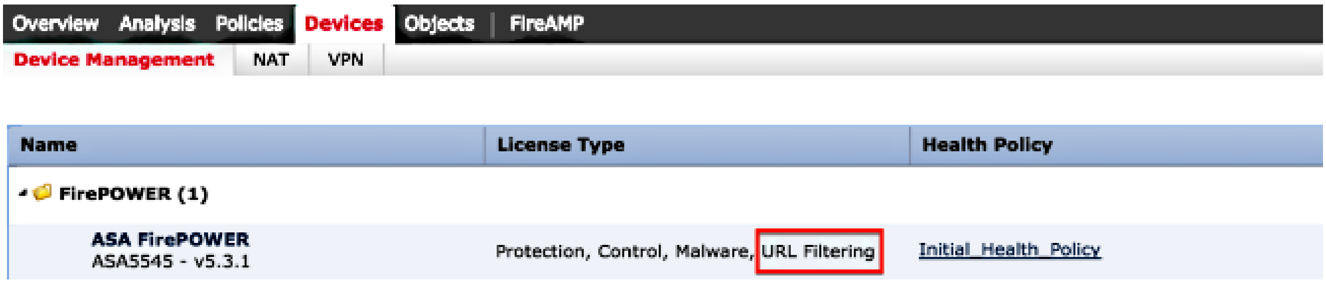
the **System > Licenses** page in order to find a list of licenses.



Maximum Virtual Device 64bit Licenses

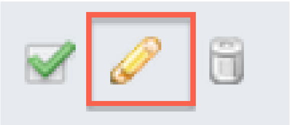
Protection (Used)	1 (1)
Control (Used)	1 (1)
URL Filtering (Used)	1 (1)
Malware (Used)	1 (1)
VPN (Used)	0 (0)

2. Go to the **Devices > Device Management** page, and verify if the URL Filtering license is applied on the device that monitors the traffic.

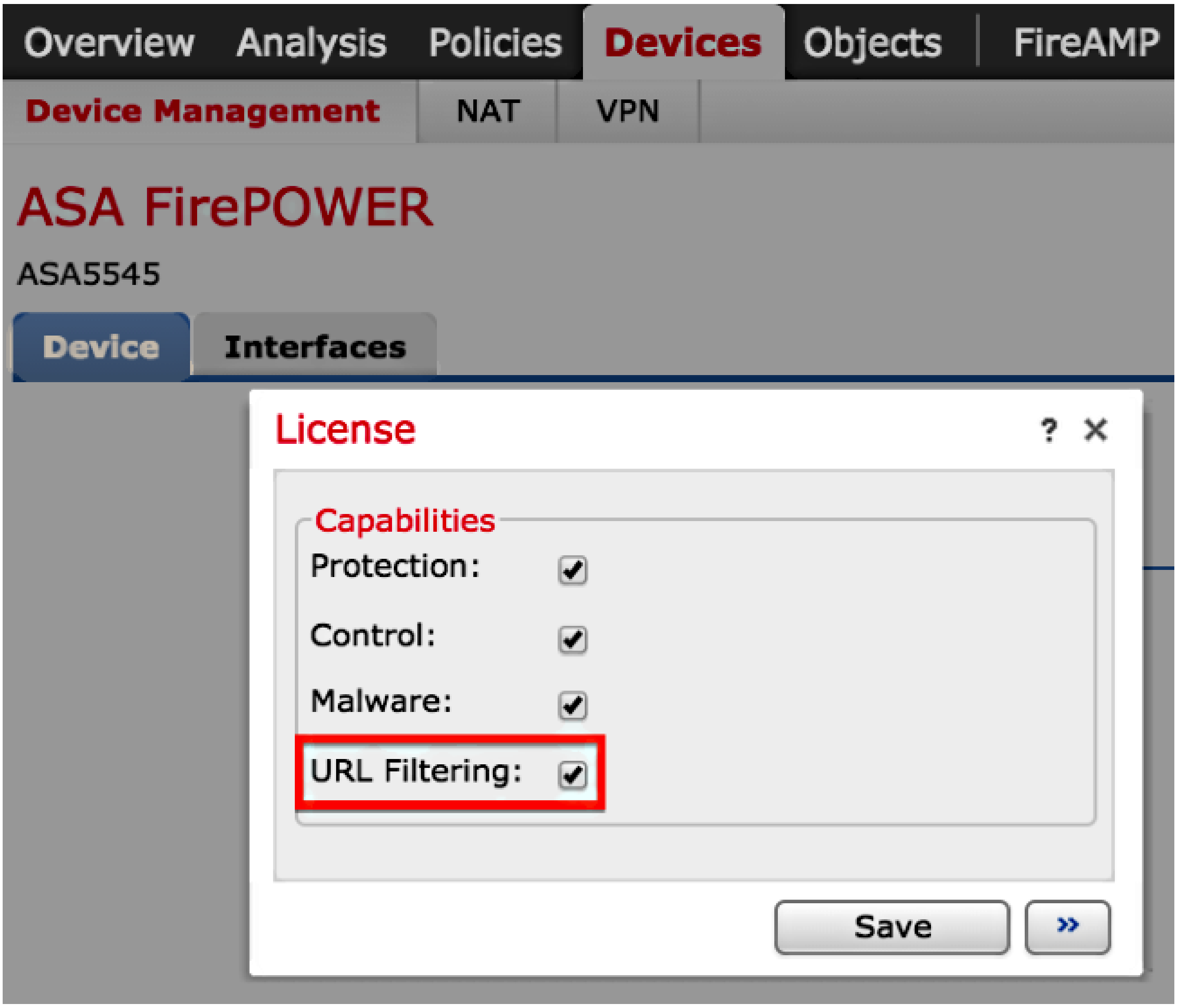


Name	License Type	Health Policy
FirePOWER (1)		
ASA FirePOWER ASA5545 - v5.3.1	Protection, Control, Malware, URL Filtering	Initial_Health_Policy

3. If the URL Filtering license is not applied on a device, click the **pencil** icon in order to edit the settings. The icon is located next to the device name.

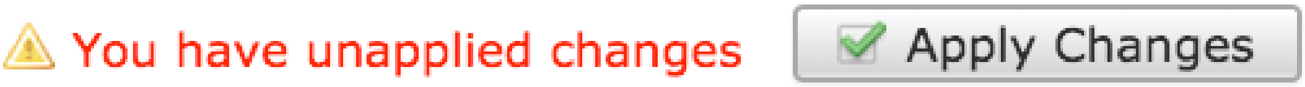


4. You can enable the URL Filtering license on a device from the **Devices** tab.



Capabilities
Protection: ☑
Control: ☑
Malware: ☑
URL Filtering: ☑

5. After you enable a license and save your changes, you also must click **Apply Changes** in order to apply the license on your managed device.



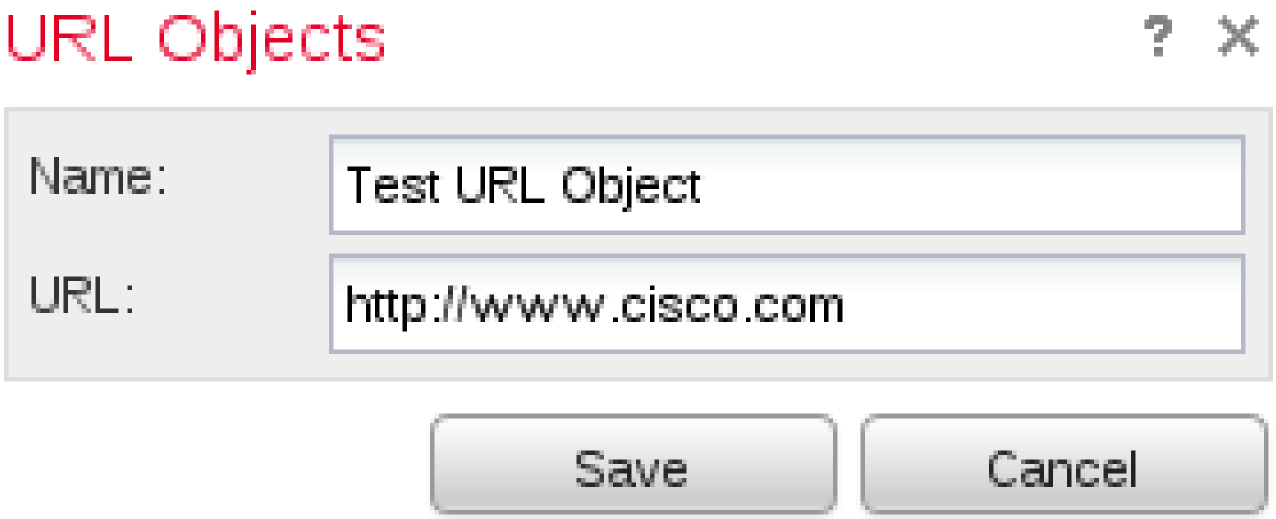
You have unapplied changes

Exclusion of a Specific Site from Blocked URL Category

FireSIGHT Management Center does not allow you to have a local rating of URLs that override the default Sourcefire provided category ratings. In order to accomplish this task, you must use an Access Control policy. These instructions describe how to use a URL object in an Access Control rule in order to exclude a specific site from a block category.

1. Go to the **Objects > Object Management** page.

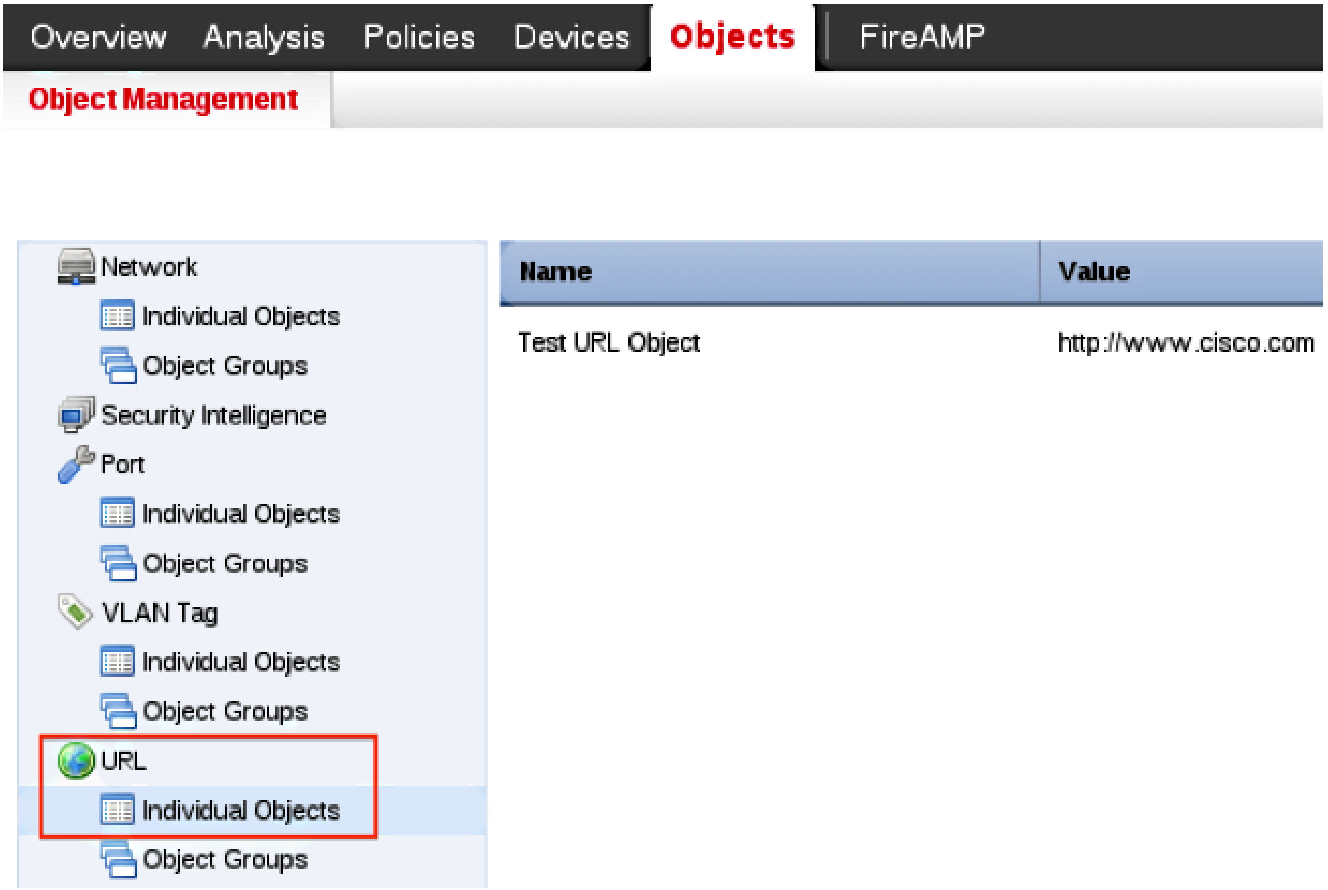
2. **Choose Individual Objects** for URL, and click the **Add URL** button. The **URL Objects** window appears.



URL Objects

Name: Test URL Object

URL: http://www.cisco.com

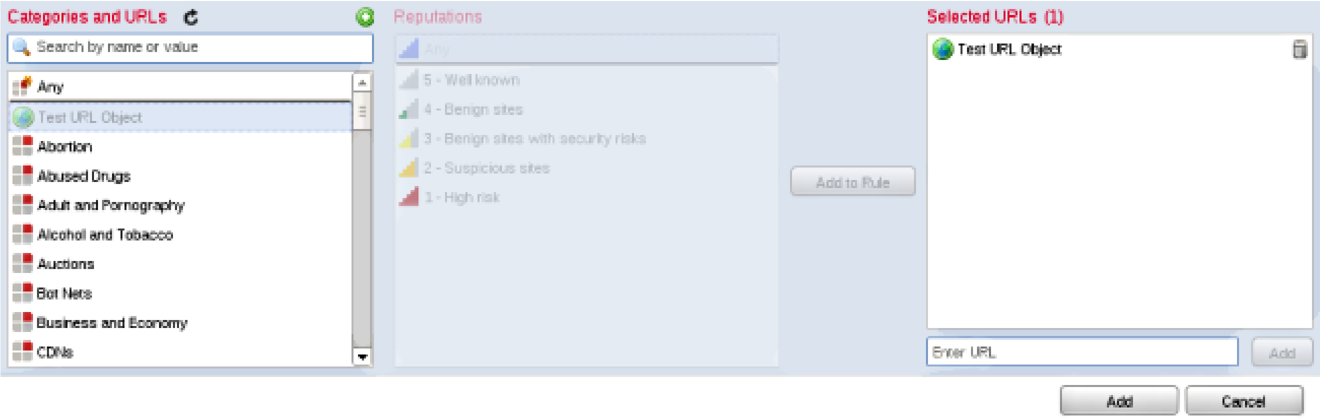


Name	Value
Test URL Object	http://www.cisco.com

3. After you save the changes, choose **Policies > Access Control** and click the **pencil** icon in order to edit the Access Control policy.

4. Click **Add Rule**.

5. Add your URL Object to the rule with the **Allow** action and place it above the URL Category rule, so that its rule action is evaluated first.



6. After you add the rule, click **Save and Apply**. It saves the new changes and applies the Access Control policy to managed appliances.

Verify

For Verify or Troubleshoot information, refer to the **Troubleshoot Issues with URL Filtering on FireSIGHT System** article linked in the Related Information section.

Troubleshoot

For Verify or Troubleshoot information, refer to the **Troubleshoot Issues with URL Filtering on FireSIGHT System** article linked in the Related Information section.

Related Information

- Troubleshoot Issues with URL Filtering on FireSIGHT System
- Technical Support & Documentation - Cisco Systems