

# Cisco ASA Connector Quick Configuration Guide

---

# Contents

<b>Cisco Cloud Web Security Account Creation and Initial Login to ScanCenter .....</b>	<b>3</b>
<b>Decision Tree for Creating Company or Group Key in Cisco ScanCenter .....</b>	<b>3</b>
Creating a Company Key .....	3
Creating a Group Key .....	4
<b>Cisco ASA Configuration for Redirection to CWS .....</b>	<b>5</b>
<b>Cisco ASA Configuration for Whitelisting (optional).....</b>	<b>7</b>
<b>Cisco ASA Configuration for Identity Firewall Integration (optional) .....</b>	<b>8</b>
<b>Verification of Traffic Redirection to CWS .....</b>	<b>9</b>
<b>Directory Groups Definition in Cisco ScanCenter (optional).....</b>	<b>10</b>
<b>Web Filtering Policy in Cisco ScanCenter .....</b>	<b>10</b>
Schedules .....	11
Filters .....	11
Rules.....	18
<b>Web Filtering Verification .....</b>	<b>21</b>
<b>Global Settings and Fine-Tuning of Web Filtering Policy .....</b>	<b>22</b>
Global Settings .....	22
User Messages .....	23
Email Alerts.....	24
<b>Basic User Reports in Cisco ScanCenter for User Traffic .....</b>	<b>24</b>
<b>Further Actions .....</b>	<b>27</b>

## Cisco Cloud Web Security Account Creation and Initial Login to ScanCenter

After subscribing to Cisco® Cloud Web Security (CWS), formerly known as Cisco ScanSafe, you will receive a provisioning email message that includes important information. In the provisioning email message you will find details about your primary and secondary web services proxy addresses. Keep these addresses because you will need them when configuring your Cisco Adaptive Security Appliance (ASA) Firewall.

In the message you will also find your credentials for logging in to the Cisco Web Security administrator portal, Cisco ScanCenter. The password supplied is a temporary password, so you must change it when you first log in. When you can successfully log in to your Cisco ScanCenter account, you are ready to start the configuration steps.

## Decision Tree for Creating Company or Group Key in Cisco ScanCenter

When traffic is redirected to the cloud, it needs to be identified in order to verify that the redirecting company is a licensed customer, and to recognize who that company is in order to apply the correct policy. This identification is achieved by generating a company or group key in your ScanCenter account; you then use this key in your ASA configuration settings. You should consider the following when deciding whether to use a company or a group key:

- You can create only one company key, which, as the name suggests, is used by the whole company. The company key is typically used when installing and configuring a single ASA to redirect to the Cloud Web Security (CWS) service, and in cases where one or more ASAs are integrated with a Microsoft Active Directory Network. Integrating the ASA with Active Directory enables you to apply policies according to group membership, and provides user granularity in reports.
- If you are configuring multiple ASAs (or an ASA in multiple context mode), you can create custom groups in ScanCenter and assign a group key to each group. You can then use separate group keys on each ASA device or context in order to associate them to your custom groups, and apply separate policy rules to the groups. This method can provide location granularity in cases where the ASA is not integrated with an AD, but users will not be named in reports (their IP addresses will be seen, however).

### Creating a Company Key

Because there is only one company key, the procedure is simple. This procedure is performed in ScanCenter.

1. Log in to ScanCenter and navigate to the Admin tab.
2. Under the Authentication menu, select Company Key.



3. If a key has already been created, you will see only the last four characters, so if you have not saved it elsewhere, you will have to revoke it and create a new one.

**Authentication key for Internal\_UK**

**Name:** Internal\_UK  
**Key Ref:** D589  
**State:** Active

[Deactivate](#) [Revoke](#)

**Note:** If you revoke a company key that is already in use, the new one will have to be updated in the configurations of all devices where it is already used.

4. To create a new company key, click **Create new**.
5. After you create a new company key, the full key is shown upon creation. You can send it to yourself in an email message from the page or copy and save it locally for use on the ASA configuration.

Authentication Keys

The following Authentication Keys have been created. You are advised to *immediately* copy these to a text file, save in a secure location, and email to the designated administrator for safe keeping. Key values are stored in an encrypted format, and it is not possible for them to be displayed again, after navigating away from this page.

Name	Authentication Key Type	Authentication Key
ScanSafe_Demo	Company	AS.SS.C.DEM-3UJ8Z9Y9F9E9T9H79B9L79U9

Send via email to the user  @ scansafe.com

## Creating a Group Key

Group keys are associated with custom groups, so first define your custom groups in ScanCenter:

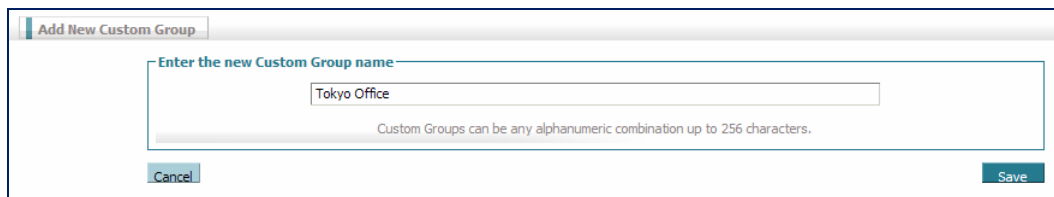
1. Navigate to the Admin tab and under the Management menu, select Groups.

The screenshot shows the 'Management' menu in the Cisco ISE GUI. The 'Groups' option is highlighted with a red rectangle. Other visible options include 'Users', 'Hosted Config', 'Dictionaries', 'File Info DBs', 'Import User List', and 'Authentication'.

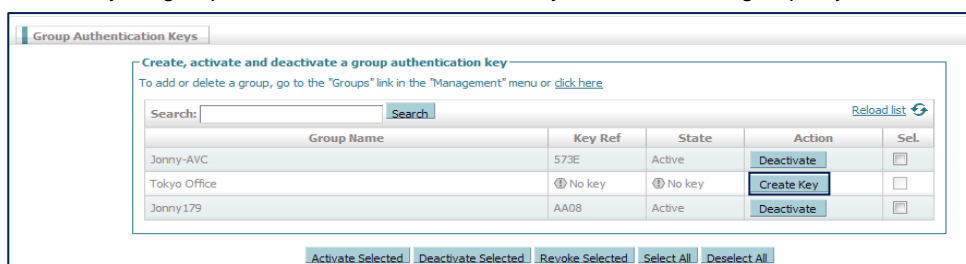
2. Click Add Custom Group from the foot of the page.

[Delete Selected](#)
[Add Custom Group](#)
[Add Directory Group](#)

3. The Add New Custom Group window will appear. Give your new custom group a name.



4. Next associate a group key with the custom group. Stay on the Admin tab and from the Authentication menu, select Group Keys.
5. Find your group on the list and click Create Key to create a new group key.



Group Name	Key Ref	State	Action	Sel.
Jonny-AVC	573E	Active	Deactivate	<input type="checkbox"/>
Tokyo Office	No key	No key	Create Key	<input type="checkbox"/>
Jonny 179	AA08	Active	Deactivate	<input type="checkbox"/>

6. As with the company key, the whole string is shown only once upon completion, and after that only the last four characters are shown, so be sure to save it.

## Cisco ASA Configuration for Redirection to CWS

Before you proceed with this step, make sure you have following information ready:

- Fully qualified domain name (FQDN) or IP address of the primary or backup CWS proxy servers
- License hex-keys

To configure ASA to send traffic, enter the following commands:

```
scansafe general-options
server primary ip 180.24.0.62 port 8080
retry-count 5
license 366CXXXXXXXXXXXXXXXXXXXX61E5
```

Configuration through the Cisco Adaptive Security Device Manager (ASDM) (native device manager) follows:

**Configuration > Device Management > Cloud Web Security**

Configure Cloud Web Security servers and license parameters  
Launch [Cloud Web Security Portal](#) to configure Web content scanning, filtering, malware protection services and retrieving reports.

**Primary Server**

IP Address/Domain Name:

HTTP Port:

**Backup Server**

IP Address/Domain Name:

HTTP Port:

**Other**

Retry Counter:

License Key:

Confirm License Key:

You can also verify the status of the CWS (ScanSafe) link as follows:

**Monitoring > Properties > Cloud Web Security**

**Cloud Web Security Status and Statistics**

**Server Status:**

Server	IP Address/FQDN	Status	Active
Primary	proxy197.scansafe.net(72.37.244.115)	REACHABLE	Active
Backup	proxy137.scansafe.net	80.254.152.99	Standby

**Server Connection Statistics:**

Server Connection	Value
Current HTTP sessions	0
Current HTTPS sessions	0
Total HTTP Sessions	0
Total HTTPS Sessions	0
Total Fail HTTP sessions	0
Total Fail HTTPS sessions	0
Total Bytes In	0
Total Bytes Out	0
HTTP session Connect Latency in ms(min/max/avg)	0/0/0
HTTPS session Connect Latency in ms(min/max/avg)	0/0/0

Last Updated: 8/10/12 3:19:02 PM

The next step is to identify the traffic pattern for which you want to redirect to the CWS proxy. This step requires some knowledge of the ASA modular policy framework (MPF). The details of MPF are available at: <http://tools.cisco.com/squish/eF3bE>.

In the following example, we will configure ASA to send all the port 80 traffic to CWS. You can use a similar approach to send port 443 traffic to CWS too. The configuration can be done by following a simple two-step process:

1. Create a policy map for CWS on the ASA.
2. Define the protocol (in this case HTTP).

The following configuration line items are required to achieve these steps:

```
hostname(config)# policy-map type inspect scansafe cws_inspect_pmap1
hostname(config-pmap)# parameters
hostname(config-pmap-p)# http
```

Now ASA is ready to send all the port 80 traffic to the CWS proxy.

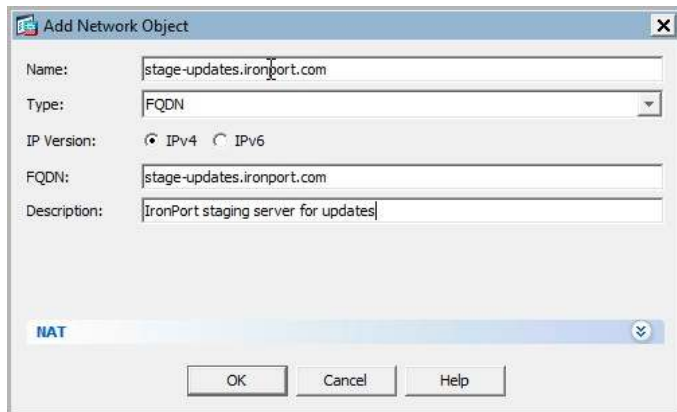
### Cisco ASA Configuration for Whitelisting (optional)

Customers can also selectively identify whitelisted websites for which the traffic should not get redirected through CWS proxy. Please note that this feature requires identification of source based on user and group. We highly recommend that you include in this list all URLs from which regular software updates originate, such as Microsoft, Apple, and Adobe, as well as antivirus signature update files that you regularly download from the Internet.

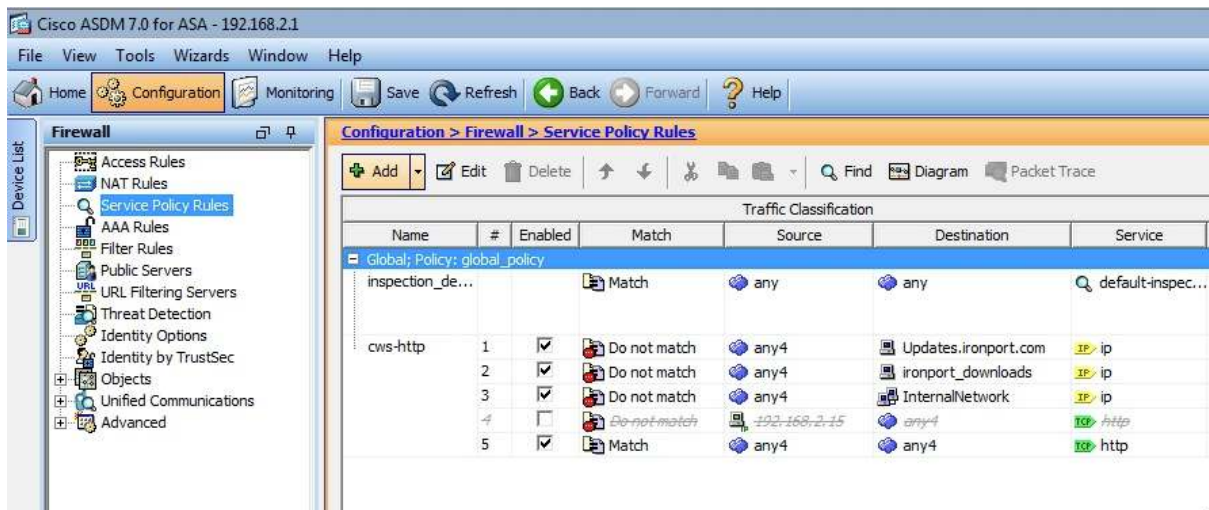
Following is an example of configuration of FQDN network objects for URLs that should be bypassed, and are set in the Service Access Policy to **not match**. In this example, the bypassed URLs are stage-updates.ironport.com and download.ironport.com:

Use the Add Network Object option to add the FQDN of the hosts that should be bypassed from CWS:

The screenshot shows a window titled "Add Network Object" with a close button (X) in the top right corner. Inside the window, there are several input fields and a dropdown menu. The "Name:" field contains the text "downloads.ironport.com". The "Type:" dropdown menu is set to "FQDN". The "IP Version:" section has two radio buttons, "IPv4" (which is selected) and "IPv6". The "FQDN:" field contains the text "downloads.ironport.com". The "Description:" field contains the text "IronPort download site". At the bottom of the window, there is a checkbox labeled "NAT" which is currently unchecked. Below the checkbox are three buttons: "OK", "Cancel", and "Help".



Add rules to the existing CWS service policy to exclude requests from any source to these hosts, and position them at the right priority in the list:



Full details of whitelisting configuration are available at:

[http://www.cisco.com/en/US/docs/security/asa/asa90/asdm70/configuration\\_guide/protect\\_cloud\\_web\\_security.html#wp1682939](http://www.cisco.com/en/US/docs/security/asa/asa90/asdm70/configuration_guide/protect_cloud_web_security.html#wp1682939).

### Cisco ASA Configuration for Identity Firewall Integration (optional)

ASA Identity Firewall (IDFW) over the Microsoft Active Directory Network provides Single Sign-On (SSO) within an Active Directory domain and embeds user and group identity in firewall access policies. This setup enables enterprises to configure policies and identify users directly by username or group name rather than through IP addresses. The advantages of this integration include:

- Increased flexibility and simplicity in policy creation by decoupling policy from topology
- Decreased costs of creating and maintaining security policies
- Better visibility on **who** is doing what
- Decoupling of policy from network topology
- Significant reduction of policy count



---

ASA Identity Firewall policies can be used in conjunction with CWS policies, and when used they will be carried to the CWS service, which can then use this identity information for the cloud policies.

For ASA Identity Firewall to be active, you must have an Active Directory domain-based network, and you must also have an Active Directory Agent (Cisco Directory Agent) installed in your network.

Following are the requirements:

**ASA Firewall:**

- Download the Active Directory group from the Active Directory domain controller with the Lightweight Directory Access Protocol (LDAP).
- Receive IP-user mappings from the Active Directory Agent with the RADIUS protocol.
- Report IP-user mappings from VPN or cut-through proxy to the Active Directory Agent.
- Apply policies (access control list [ACL] and Multi-Processor Forwarding [MPF]) based on user identity.

**Active Directory Agent:**

- Monitor the security logs of the Active Directory domain controllers with Windows Management Instrumentation (WMI).
- Push IP-user mappings to ASA with the RADIUS protocol.
- Receive IP-user mappings from ASA with the RADIUS protocol.

**Active Directory domain controller:**

- Authenticate users.
- Generate user logon security logs.
- Reply to the ASA LDAP query for user and group information.

Here is a link to the Identity Firewall Configuration Guide: <http://tools.cisco.com/squish/A0068>

## Verification of Traffic Redirection to CWS

There are various ways to test redirection to the CWS proxy. Perform the following steps to confirm that the web traffic of clients is being redirected to the proxy:

1. Open a web browser on a client machine that is behind the ASA.
2. In the URL window of your browser, type <http://whoami.scansafe.net>. Details such as your ScanCenter account name, group name(s), and usernames will be displayed. If a message is displayed stating "User is not currently using the service", then the client's web traffic is not being redirected to the cloud web proxy.
3. Try to browse to [www.gator.com](http://www.gator.com). The site should be blocked and you should see the default blocking page. Confirm that the reason for the block is identified spyware.
4. Browse to the homepage of one of the major search engines (Google, Yahoo, or Bing) and run a search. SearchAhead icons should be present next to the search results.

---

**Note:** If you do not see SearchAhead results, log in to ScanCenter, navigate to the Web Filtering tab, then the Management menu, and then under Global Settings ensure the Enable SearchAhead for all users checkbox is selected.

### Directory Groups Definition in Cisco ScanCenter (optional)

If you have integrated your ASA with an IDFW for group identification in rules and user granularity in reports, you need to define in ScanCenter any directory groups for use in web filtering rules.

1. Log in to ScanCenter and click the Admin tab.
2. Under the Management tab, click Groups. The list of defined groups will be shown.
3. Click Add Directory Group from the bottom of the page.
4. Type in the name of a directory group in the format of domain-name\group-name.
5. Click Save to save the directory group.
6. Repeat the previous three steps to add additional directory groups.

### Web Filtering Policy in Cisco ScanCenter

To get started, you need to create a basic web filtering policy in ScanCenter.

The policy is a set of rules that runs from top to bottom, checking each rule until it makes the first “match”, and applies the action of that rule and then stops. In order for a rule to make a match and apply an action, it must make a match on all three of the following entities:

- Groups, Users, or IP Addresses
- Filter
- Schedule

So the rule is actually asking “Can this user access this web content at this time?”

If no rule is matched, the Default rule at the bottom will always apply.

The following steps demonstrate how to set up a basic policy, which you can then build on and develop further.

**Note:** In a new account, no policy will be defined and all users can access all sites at all times, so all you will see is a default rule in the list.

In your ScanCenter account, click the Web Filtering tab to show the policy.

The screenshot shows the 'Web Filtering' tab selected in the top navigation bar. Below it, the 'Management' sub-tab is active. The breadcrumb trail is 'Web Filtering > Management > Policy > Manage policy'. There are three buttons: 'Manage policy', 'Edit a rule', and 'Create a rule'. A text block explains that rules higher in the list take priority and that there is a maximum of 100 enabled rules. Below this is a table titled 'Company policy'.

#	Move	Rules	Groups/Users/IPs	Filter	Schedule	Action	Active	Edit	Delete
1		<a href="#">Default</a>	Anyone	Anything	Anytime		<input checked="" type="checkbox"/>		

## Schedules

1. If you want rules to apply at all times, there is no need to create any schedules. A default schedule named Anytime already exists and cannot be edited. If you do not apply any schedule to a rule, it will also always be active.
2. If you need to create any schedules, under the Management menu, click Schedules.
3. You can create new schedules according to your needs. For instance, you can customize policies for lunch and working hours. Note that a schedule can apply to a certain time zone and be active on any combination of days.
4. Create and save any schedules as required.

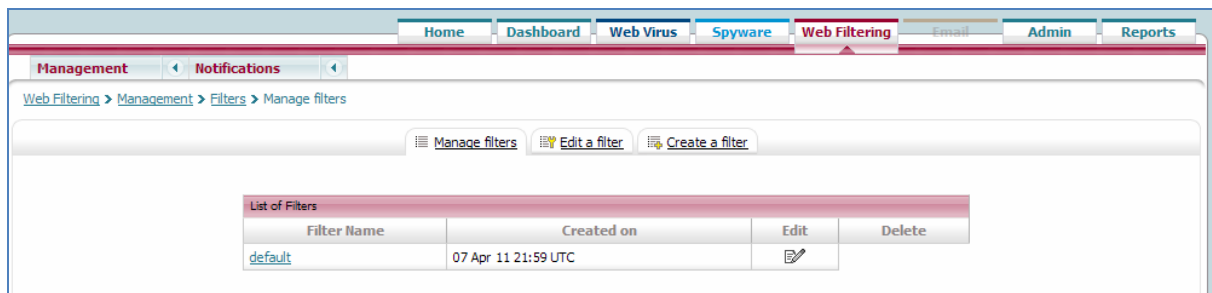
The screenshot shows the 'Web Filtering' tab selected, with the 'Schedules' sub-tab active under 'Management'. The breadcrumb trail is 'Web Filtering > Management > Schedules > Manage schedules'. There are three buttons: 'Manage schedules', 'Edit a schedule', and 'Create a schedule'. Below is a table titled 'List of Schedules'.

Schedule Name	Time	Time zone	Days	Edit	Delete
<a href="#">lunch</a>	From 12:00 to 14:00	US/Pacific	Mon-Tue-Wed-Thu-Fri		
<a href="#">working hours</a>	From 09:00 to 18:00	US/Pacific	Mon-Tue-Wed-Thu-Fri		
<a href="#">anytime</a>	From 00:00 to 00:00	US/Pacific	Everyday		

## Filters

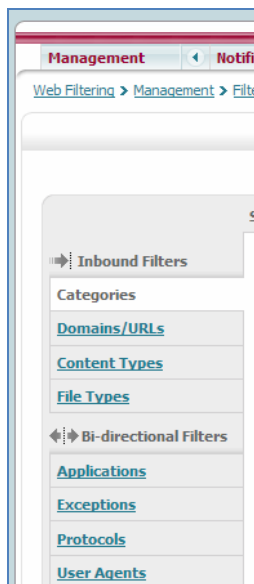
Filters are used for identifying the web content that you want to control. When creating a filter, think in advance what you want to achieve with the filter. Ask yourself questions such as “What action will be applied when this filter is matched?”, “To whom will this filter apply?”, and “What type of web content should this filter look for?” It is good practice to include numerous common web content types in the same filter if you plan to use them later to control the same users at the same time.

1. Under the Management menu, select Filters.



2. You will see a default filter in a new account. Create a new filter by clicking Create a filter. Give your new filter a name. It is good practice to use a meaningful name in line with what the filter will achieve. For example, "IT Allowed Sites".

When creating a filter for identifying users' web requests, you can identify the web content in many ways. You can identify all of the content through the various objects of the filter, all of which are listed down the left side of the filter.



Note that the logic between any objects in a filter is OR, meaning that it is enough that **any** of the objects is matched in order for the complete filter to be matched.

3. Click the various filter objects using the menu down the left side, starting with the Inbound Filters. Click Save after modifying a page, or click Save all settings at the end.

- On the Categories page, select the categories that you wish to control with this filter. Note that you can also select a category named Uncategorized.

The screenshot shows a web filter configuration interface. At the top, there are buttons for 'Manage filters', 'Edit a filter', and 'Create a filter'. Below these is a 'Filter name:' input field. The main section is titled 'Select the categories to be included in the filter'. On the left, there is a sidebar with 'Inbound Filters' and 'Bi-directional Filters' sections. Under 'Inbound Filters', there is a 'Categories' section with links for 'Domains/URLs', 'Content Types', 'File Types', 'Applications', 'Exceptions', 'Protocols', and 'User Agents'. The 'Categories' section is currently selected. The main area displays a list of categories with checkboxes next to them, including: Adult, Alcohol, Astrology, Business and Industry, Cheating and Plagiarism, Computers and Internet, Digital Postcards, Dynamic / Residential, Entertainment, Fashion, Filter Avoidance, Freeware and Shareware, Games, Advertisements, Arts, Auctions, Chat and Instant Messaging, Computer Security, Dating, Dining and Drinking, Education, Extreme, File Transfer Services, Finance, Gambling, and Government and Law.

- On the Domains/URLs page you can add a list of up to 1000 complete domains (for example, cnn.com) and specific URLs (for example, cnn.com/news).

The screenshot shows the 'Domains/URLs' page in a web filter configuration interface. The sidebar on the left is the same as in the previous screenshot, but the 'Domains/URLs' link is now selected. The main section is titled 'Enter the Domains/URLs/Networks/IPs to be included in the filter'. It contains two large text input areas. The top area is labeled 'Domains/URLs' and has a 'Sort Alphabetically' button below it. The bottom area is labeled 'Networks/IPs'. Below the 'Domains/URLs' input area, there is a note: 'Domains/URLs can be entered as an explicit URL or as domain names (without the "/" suffix). You must omit the "http://". You may specify sub-domains and paths.' Below the 'Networks/IPs' input area, there is a note: 'Networks/IPs can be entered as a specific network address or a single IP address(without the "/" suffix, the default netmask would be 32).

- On the same page, you have the option to add IP addresses or networks if you need to control them too.

7. Use the Content Types page to list any high-level content types that you want to control in this filter. Note that these types apply to a content type on requested webpages, and not to any outbound content that users post.

Select the Content Types to be included in the filter

**Application**

- ☐ Select All
- ☐ Word
- ☐ Excel
- ☐ Powerpoint
- ☐ pdf
- ☐ ppt-encrypted
- ☐ postscript
- ☐ x-gzip
- ☐ x-shockwave-flash
- ☐ octet-stream

**Audio**

- ☐ Select All
- ☐ basic
- ☐ mpeg
- ☐ wav
- ☐ x-msvideo
- ☐ x-midi
- ☐ x-realaudio
- ☐ x-wav

8. Use the File Types page to list any file types that you want to include in this filter. Note that these types apply to file types on requested webpages, and not to any outbound content that is posted by users.

Select the inbound File Types to be included in the filter

**Named file types**

- ☐ avi - Video file
- ☐ bin - Binary File
- ☐ cgi - CGI Script
- ☐ com - Executable Program
- ☐ doc - MS Word Program
- ☐ docx - Word 2007 file
- ☐ emu - Emulation
- ☐ ex\_ - Compressed exe
- ☐ ex\$ - Compressed exe
- ☐ exe - Executable File
- ☐ flv - Streaming media file
- ☐ gat - Gator File
- ☐ gif - Gif Image
- ☐ gz - Archive File
- ☐ hta - HTML Program
- ☐ jar - Java Archive File
- ☐ jpeg - JPEG Image
- ☐ jpg - JPEG Image
- ☐ js - Javascript File
- ☐ m4a - iTunes file
- ☐ mid - MIDI Music File
- ☐ moo - Quicktime Movie
- ☐ mov - Quicktime Movie
- ☐ mp3 - MPEG Audio Stream
- ☐ mpa - MPEG Audio Stream
- ☐ mpg - MPEG Audio Stream
- ☐ nzb - Newsgroup file
- ☐ pak - Archive File
- ☐ pdf - Adobe Acrobat File
- ☐ pif - Program Information
- ☐ pl - Perl Script
- ☐ ppt - PowerPoint 2007 file
- ☐ pptx - PowerPoint 2007 file

9. Under Bi-directional Filters, click Applications. Here you can control access to web applications and their activities.

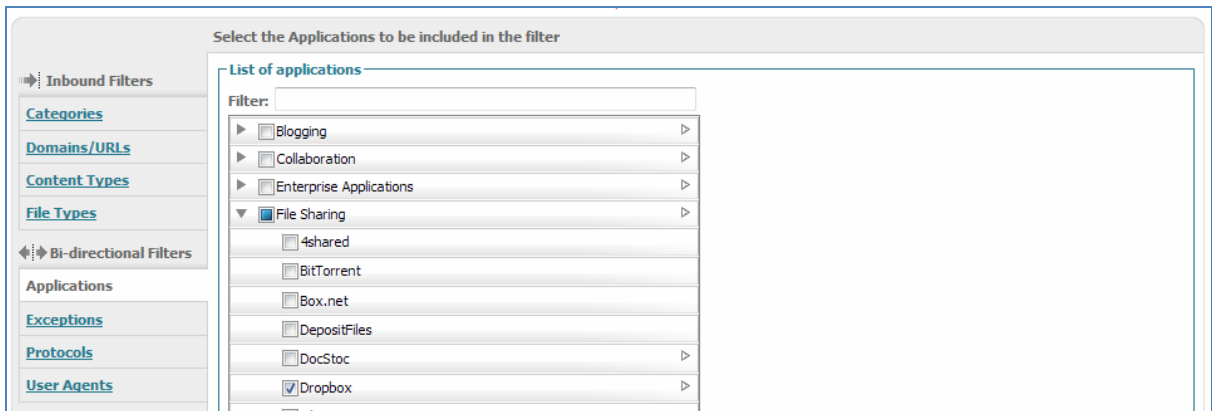
Select the Applications to be included in the filter

**List of applications**

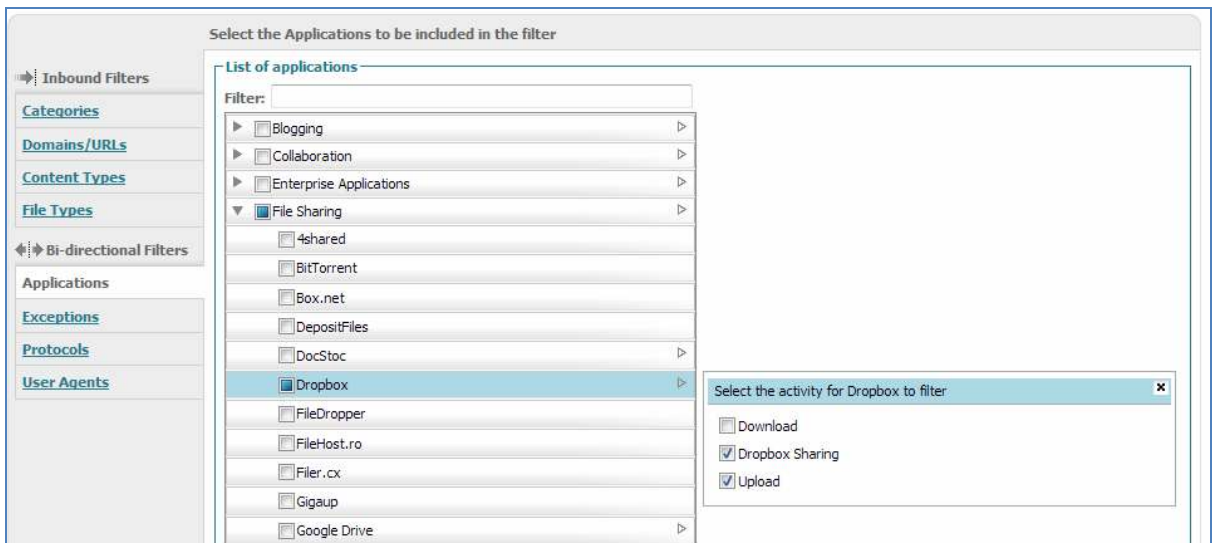
Filter:

- ☐ Blogging
- ☐ Collaboration
- ☐ Enterprise Applications
- ☐ File Sharing
- ☐ Games
- ☐ Instant Messaging
- ☐ Internet Utilities
- ☐ Media
- ☐ Myspace
- ☐ Presentation / Conferencing
- ☐ Proxies

10. Expand the tree to the level required. Use the checkboxes on the left to control application access. You can control this access at the level of a single application or at a higher level for the complete group of applications.



11. Use the arrows on the right to open the Activities panel and then use the checkboxes in those panels to control Activities Here too you can control these activities at the level of a single application or at a higher level for the complete group of applications.



12. Above the list of applications is a window for typing in search phrases; for example, “video”. The matching results will be filtered as you type. Note that after the applications are filtered, you should select the ones you want by checking the checkboxes, not by clicking Select All, because clicking Select All will select all applications, including the ones that are currently filtered from view.

Select the Applications to be included in the filter

Filter: video

- ☐ Media
  - ☐ Facebook Videos
  - ☐ Flash Video
- ☐ Myspace
  - ☐ Myspace Videos
- ☐ Social Networking
  - ☐ Google+
  - ☐ Google+ Videos

Revert Select All Deselect all Set to Default Show Selected Collapse All Expand All Save

13. Use the Exceptions window to list specific domains, URLs, IP addresses, and networks that should be excluded from the filter. Remember that anything listed here has higher priority than everything else in the filter.
14. In the Protocols window, you can select certain protocols to be included in this filter. The options available are HTTP, Secure HTTP (HTTPS), and FTP over HTTP. If nothing is selected, the filter will apply to all of these protocols.

Select the Protocols matches to be included in the filter

☐ FTP over HTTP ☐ HTTP

☐ HTTPS

Revert Set to Default Save



15. In the User Agents window you can choose to control certain web browsers.

The screenshot shows a web-based configuration interface for user agents. On the left is a sidebar with navigation links: Inbound Filters, Categories, Domains/URLs, Content Types, File Types, Bi-directional Filters, Applications, Exceptions, Protocols, and User Agents. The 'User Agents' section is selected. The main area is titled 'Select the user agents to be included in the filter'. It contains several sections for different browsers: Chrome (All Versions), Firefox (All Versions), Internet Explorer (All Versions, Internet Explorer 9, Internet Explorer 8, Internet Explorer 7), Safari (All Versions, Safari 5, Safari 4, Safari 3), and Custom User Agents. The Custom User Agents section has a text area for entering additional user agents, with a note: 'You can enter additional user agents below. Each user agent should be added on a separate line (An example is "1^Ubuntu"Firefox\$")'. At the bottom are buttons for Revert, Select All, Deselect all, Set to Default, and a Save button.

Select the user agents to be included in the filter

**Chrome**

☐ All Versions

**Firefox**

☐ All Versions

**Internet Explorer**

☐ All Versions ☐ Internet Explorer 9 ☐ Internet Explorer 8

☐ Internet Explorer 7

**Safari**

☐ All Versions ☐ Safari 5 ☐ Safari 4

☐ Safari 3

**Custom User Agents**

You can enter additional user agents below. Each user agent should be added on a separate line (An example is "1^Ubuntu"Firefox\$")

Revert Select All Deselect all Set to Default Save

## Rules

After you have created groups, schedules, and filters, you can create a rule for your policy.

1. Under the Management menu, select Policy. The policy will be shown again.
2. Click Create a rule at the top of the policy window.

The screenshot shows the 'Create a rule' window in the Web Filtering management interface. The window has a header with tabs: Home, Dashboard, Web Virus, Spyware, Web Filtering (selected), Email, Admin, and Reports. Below the header, there's a breadcrumb trail: Web Filtering > Management > Policy > Create a rule. The main content area has three buttons: Manage policy, Edit a rule, and Create a rule (selected). The form includes a Name field, a Rule Action dropdown (set to Block), and an Active checkbox. Below these are three sections: Define Group ("WHO"), Define Filters ("WHAT"), and Define Schedule ("WHEN"). Each section has instructions and a table to define exceptions. The 'Define Group' section has a table with columns Group, Set as an exception, and Delete. The 'Define Filters' section has a table with columns Filter, Set as an exception, and Delete. The 'Define Schedule' section has a table with columns Schedule, Set as an exception, and Delete. At the bottom, there are Reset and Create rule buttons.

3. Give your new rule a name. It is good practice to use a name that is meaningful, and in line with the filter that will be used in the rule; for example, "Warn Social Networking".

The screenshot shows the 'Create a rule' window with the rule 'Warn Social Networking' created. The Name field contains 'Warn Social Networking' and the Rule Action dropdown is set to Warn. The Active checkbox is checked. The buttons at the top are Manage policy, Edit a rule, and Create a rule.

## Rule Actions

4. Select the action that this rule should apply when matched. The following actions can be applied to a rule:
  - **Block:** The requested web content will be blocked.
  - **Allow:** The requested web content will be allowed.
  - **Anonymize:** Users' identities will be hidden in reports.
  - **Warn:** A warning page will be presented to users for their compliance before the requested site is allowed.

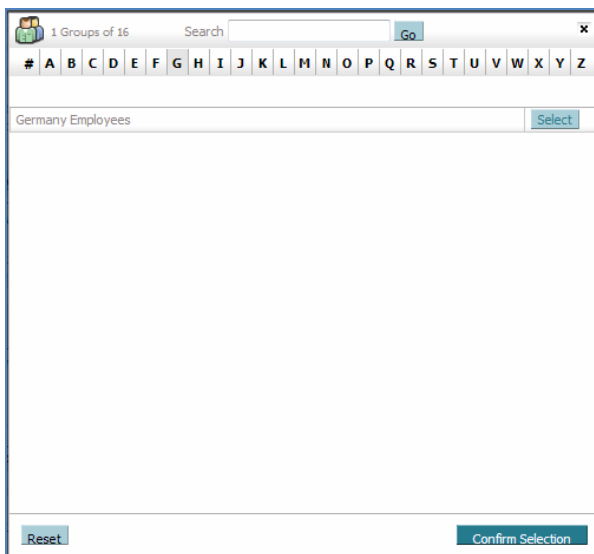
- **Authenticate:** This action triggers an authentication process. It is typically not used when configuring an ASA to redirect to the cloud.

Note that when using the anonymize action, the subsequent rules in the policy are still applied, but the users' identities will be stripped from the following reporting attributes in all data entries:

- **User:** Reports will show undisclosed.
- **Group:** Reports will show undisclosed.
- **Internal IP:** Reports will show 0.0.0.0.

#### Groups in Rules

5. If the rule is to apply to everyone, then there is no need to add any users. If you have defined groups, you can add them to your rules if you want to have different rules applied to different groups of users.
6. Click Add group to open the group selection window.
7. Click the first letter of a group to view certain groups.



8. You can type in the search window and click Go to search for a specific string. If you click Go without typing anything, all groups will be displayed.
9. Select the required group and then click Confirm selection. The selected group will be added to the rule.
10. You can add numerous groups to a rule. Click Add group and repeat the previous steps as necessary. You can add only one group at a time.

**Define Group ("WHO")**

Search for a group by clicking on "Add group". To set a group as an exception to the rule, select the corresponding "Set as exception" box (action of NOT).

If no group is selected, this rule will apply to anyone. Adding multiple groups has the action of "OR", so users will need to be in any of the groups listed for the rule to take effect.

Group	Set as an exception	Delete
Germany Employees	<input type="checkbox"/>	
Switzerland Employees	<input type="checkbox"/>	
Add group	<input type="checkbox"/>	

**Note:** You can add a group as an exception. For example, the Sales group should not be able to access Facebook, but if there are any users in that group who are also managers, then they should be allowed. In this case, add the Sales group to the rule and add the Management group to the rule as an exception.

**Note:** You can add a mixture of custom groups and directory groups to a rule. In case of a conflict, the directory rule will have priority, unless you included the word scansafe in the name of the custom group, in which case the custom group will have priority.

#### Filters in Rules

11. From the list of filters, select any filters you have created and then click Add. You must add a filter to a rule.

**Define Filters ("WHAT")**

Choose a Filter from the list and click "Add". To set a Filter as an exception to the rule, select the corresponding "Set as exception" box (action of NOT).

Add Filter:

Filter	Set as an exception	Delete
Always Blocked	<input type="checkbox"/>	

**Note:** As mentioned previously, when creating a rule it is enough that any of the objects in the filter is matched in order for the complete filter to be matched. It is also possible to use a set of two filters in a rule that must both be matched in order for the filter to apply. In order to have two conditions matched in a filter (the logical AND operation), add two separate filters to the rule, each with its own objects. You cannot add more than two filters to the rule. Remember to click Add after selecting each filter.

**Define Filters ("WHAT")**

Choose a Filter from the list and click "Add". To set a Filter as an exception to the rule, select the corresponding "Set as exception" box (action of NOT).

Add Filter:

Filter	Set as an exception	Delete
Firefox or IE	<input type="checkbox"/>	
Sporting Events	<input type="checkbox"/>	

#### Schedules in Rules

12. From the list of schedules, select any available schedules. If none are selected, then the rule will apply at all times.

13. You can add numerous schedules, and you can also set a schedule as an exception.

For example, a schedule for work hours is defined from 09:00 to 18:00 and another schedule for lunch is from 12:00 to 13:00. "Work hours" is added to the rule as a schedule and the lunch schedule is added as an exception. The rule will be active during work hours, but not during lunch time.

**Define Schedule ("WHEN")**  
Choose a Schedule from the list and click "Add". To set a Schedule as an exception to the rule, select the corresponding "Set as exception" box (action of NOT).  
Adding multiple schedule is not recommended unless one is going to be "Set as exception" (action of "AND NOT")

Schedule	Set as an exception	Delete
working hours	<input type="checkbox"/>	
lunch	<input checked="" type="checkbox"/>	

### Saving Rules

14. Use the Active checkbox to activate your rule now. You can activate your rule later from the policy.

15. Click Create rule at the bottom of the page to save your rule.

16. The policy page will be shown again and the new rule will be placed above the default rule. Use the up and down arrows to place the rule in the relevant priority in the policy, and click Apply changes to save the policy.

After you save changes in your policy, allow up to 5 minutes for the changes to come into effect, although it will usually happen within 1 or 2 minutes.

Note that any rules with the Anonymize action will be grouped together separately at the top of the policy.

Company policy									
#	Move	Rules	Groups/Users/IPs	Filter	Schedule	Action	Active	Edit	Delete
Privacy policy									
1	↑ ↓	<a href="#">Anonymize Switzerland</a>	"Switzerland Employees"	Anything	Anytime	Anonymize	<input checked="" type="checkbox"/>		
2	↑ ↓	<a href="#">Anonymize Germany</a>	"Germany Employees"	Anything	Anytime	Anonymize	<input checked="" type="checkbox"/>		
Internet usage policy									
3	↑ ↓	<a href="#">Always Blocked Content</a>	Anyone	"Always Blocked"	"anytime"	Block	<input checked="" type="checkbox"/>		
4	↑ ↓	<a href="#">Non Productive</a>	except "Management"	"Applications", "Non Productive"	"working hours", except "lunch"	Block	<input checked="" type="checkbox"/>		

### Web Filtering Verification

1. In order to test your web filtering policy, open a web browser on a client machine that is behind the ASA, and try to browse to websites that should be blocked for all users, if relevant.
2. If you have set any rules with warn actions, try to browse to these websites and confirm that you receive the warning message, and that you can access the site after you agree by pressing Accept.
3. If you have any rules that apply to certain groups, check to ensure that they apply to the relevant users in the groups.
4. If you have any "Anonymizing" rules for certain users or for certain websites, perform some test browsing to ensure the correct policy applies. Later you can confirm in reports that the traffic was anonymized.
5. If you have any rules that should apply according to schedules, you can also test them.

## Global Settings and Fine-Tuning of Web Filtering Policy

After you have defined your basic policy, you can expand it by adding additional rules and fine-tuning it to meet your requirements.

### Global Settings

On the Web Filtering tab, click the Global Settings menu under Management to define some additional settings. As the name suggests, these settings, when configured, are global for all users at all times.

- **SearchAhead:** This option will add icons next to all search results made in Google, Bing, and Yahoo! for all users, indicating to the users if the result will be allowed or blocked if clicked. Resulting websites will also be scanned for malware. As long as a user does not click a result, there will be no record of that user requesting to browse to this site (although the original search is recorded).

The screenshot shows the 'Global Settings' page for 'SearchAhead'. The page has a navigation bar with tabs: Home, Dashboard, Web Virus, Spyware, Web Filtering (selected), Email, Admin, and Reports. Under 'Web Filtering', there are sub-tabs: Management (selected), Notifications, and Reports. The 'Global Settings' section is active. It contains a description of SearchAhead, a checkbox labeled 'Enable SearchAhead for all users' which is checked, and a 'Save' button.

- **Separate HTTPS Restrictions:** When enabled, the list of categories in filters will be duplicated and there will be separate category lists for HTTP and HTTPS protocols that you can configure separately.

The screenshot shows the 'Separate HTTPS Restrictions' configuration page. It contains a description of the feature, a checkbox labeled 'Enable HTTP/HTTPS split' which is unchecked, and a 'Save' button.

- **Acceptable Usage Policy:** This option is not supported for use when integrating with the ASA.
- **Dynamic Classification Engine:** This engine will attempt to dynamically classify any uncategorized traffic to one of the six top extreme sites as listed by this feature in ScanCenter.

The screenshot shows the 'Dynamic Classification Engine' configuration page. It contains a description of the engine, a checkbox labeled 'Enable Dynamic Classification' which is checked, and a 'Save' button.

## User Messages

On the Web Filtering tab, click the User Messages menu under Notifications to customize alert and warn pages that users will see when getting blocked and warned. You can view the default pages, and you can also customize them in HTML. You can include the following variables in customized alert pages:

- #category
- #reason
- #url
- #username

In a similar way, you can also customize the block pages seen when users' requests are blocked because of malware (through the Web Virus tab) and spyware (through the Spyware tab).

The screenshot shows the Cisco Web Filtering configuration interface. The top navigation bar includes tabs for Home, Dashboard, Web Virus, Spyware, Web Filtering (selected), Email, Admin, and Reports. Below this, the 'Management' section is active, and the 'Notifications' sub-section is selected. The 'User Messages' menu is open, showing two main configuration areas:

- Customized Alert Page:** This section allows users to enter HTML for alert pages. It includes a text area for HTML, a checkbox to 'Include standard HTML page template for block page' (which is checked), and a 'Preview' button. Below the text area are 'Reset' and 'Save' buttons.
- Customized Warn Alert Page:** This section allows users to enter HTML for warning pages. It includes a 'Timeout value' dropdown set to '0' (0-24 hours), a text area for HTML, a checkbox to 'Include standard HTML page template for warning page' (which is checked), and a 'Preview' button. Below the text area are 'Reset' and 'Save' buttons.

## Email Alerts

On the Web Filtering tab, click the Email Alerts menu under Notifications to define email recipients who will receive email alerts when a page is blocked. You can define up to five email addresses (one of them could be a mailing list to reach a larger number of recipients). You can limit the number of email messages (1 to 20) per number of hours (1 to 24).

The screenshot shows the 'Email Alerts' configuration page within the 'Web Filtering' tab. The page has a navigation bar with 'Home', 'Dashboard', 'Web Virus', 'Spyware', 'Web Filtering', 'Email', 'Admin', and 'Reports'. Below the navigation bar, there's a 'Management' section with a 'Notifications' sub-section. The 'Email Alerts' settings are displayed in a box with the following fields:

- Email Alert Settings**
- Do you wish to be notified when a page is blocked? ☒ Yes
- Email address(es) for notifications to be sent to: (Four empty text input fields)
- Limit email alerts to: 3 per 1 hour(s).
- Buttons: Reset, Save

In a similar way, you can also define email message recipients who will receive email alerts when users' requests are blocked because of malware (through the Web Virus tab) and spyware (through the Spyware tab).

## Basic User Reports in Cisco ScanCenter for User Traffic

You can run reports on browsing activity roughly 2 to 4 minutes after you have browsed. Perform the following basic steps for verification of reporting:

1. Click the reports tab in ScanCenter.
2. Ensure the Time period at the top is set to Last 24 hours, and the Auto Run Report checkbox is selected.

The screenshot shows the 'Reports' configuration page within the 'Web Filtering' tab. The page has a navigation bar with 'Home', 'Dashboard', 'Web Virus', 'Spyware', 'Web Filtering', 'Email', 'Admin', and 'Reports'. Below the navigation bar, there's a 'Reports' section with the following fields:

- Time zone:** Europe/London
- Time period:** Last 24 hours
- From:** 5-10-2012 00:15
- To:** 6-10-2012 00:15
- Auto Run Report:** ☒



- From the list of Predefined reports, expand the Host Analysis folder and click one of the listed reports to run it.

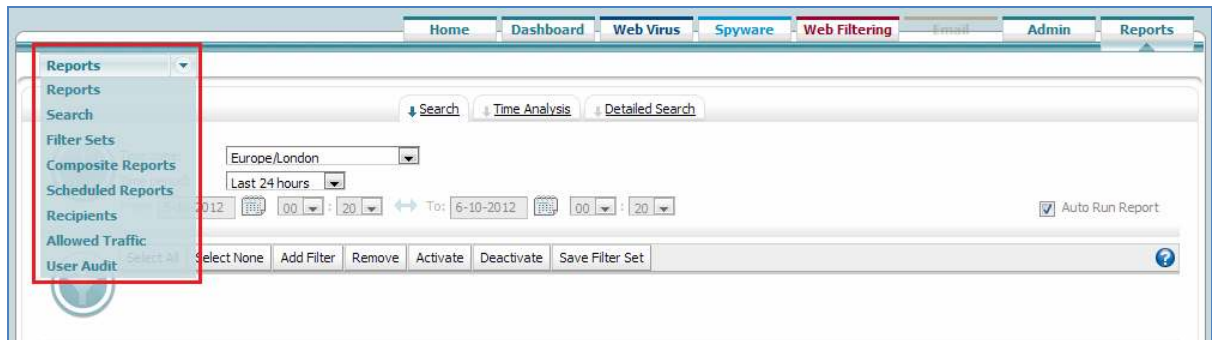
Predefined reports	Download	View as
Application Analysis		
Bandwidth Analysis		
Block Analysis		
Browse Time Analysis		
Browser Analysis		
Category Analysis		
Facebook Analysis		
Group Analysis		
Host Analysis		
What was the number of hits for each of the most popular hosts?		
		Grid
What were the top ten hosts by hits?		
		Grid
What were the top ten hosts visited for each category?		
		Grid
Legal Liability Analysis		
Malware Analysis		
Security Analysis		
User Analysis		

- The report will run in the Search page and results will be displayed within a few seconds.

View first <input type="text" value="10"/> Host sorted by Hits (descending), and their first <input type="text" value="10"/> Host sorted by Hits (descending)						
<a href="#">Launch search</a>						
What were the top ten hosts by hits?						
Show <input type="text" value="50"/> rows per page << first < prev 1 next > last >> 10 results						
	Host	Bandwidth (Bytes)	Browse Time (Min)	Bytes Received	Bytes Sent	Hits
	Totals for Host	1,287,577,665	6,844	1,287,551,214	26,451	11,974
	i.cdn.turner.com	2,086,373	8	2,086,373	0	333
	news.bbcimg.co.uk	1,220,907	5	1,220,907	0	194
	clients1.google.com	248,227	24	248,227	0	188
	safebrowsing-cache.google.com	451,241	50	451,241	0	185
	www.google.com	2,450,376	57	2,450,376	0	181
	i2.cdn.turner.com	1,517,790	7	1,517,790	0	142
	www.latenightwithjimmyfallon.com	1,346,139	2	1,346,139	0	135
	static.nfl.com	1,571,504	3	1,571,504	0	134
	www.nbc.com	1,666,878	2	1,666,878	0	131
	newsimg.bbc.co.uk	91,374	6	91,374	0	115
Show <input type="text" value="50"/> rows per page << first < prev 1 next > last >> 10 results						
Time range: Last 24 hours (from October 5, 2012 at 00:20 AM to October 6, 2012 at 00:20 AM)						
Download report as:  PDF  CSV						<a href="#">Save as</a>

- Scroll down and find the graphic output icons on the left below the results. Try clicking them to see the different ways the reports can be displayed.

- Use the Reports menu at the top left side of the page and select Reports to take you back to the list of Predefined reports.



- Try to run some additional reports from the Host Analysis, Group Analysis, and User Analysis folders, repeating the previous steps.
- If you have integrated your ASA with an Active Directory Network, ensure that group names and usernames are included in reports.

View first 10 Group sorted by Hits (descending), and their first 3 User sorted by Hits (descending) ☒

Launch search

What were the top ten hosts by hits?

Show 50 rows per page << first < prev 1 next > last >> 30 results

Group   User	Bandwidth (Bytes)	Browse Time (Min)	Bytes Received	Bytes Sent	Hits
Totals for Group	2,238,901,890	9,620	2,238,883,028	18,862	16,870
winnnt://demo\product	114,358,310	912	114,339,448	18,862	5,300
L winnt://demo\abby.murray	33,863,289	152	33,844,427	18,862	4,343
L winnt://demo\francesca.ch	614,165	102	614,165	0	152
L winnt://demo\andrew.norri	1,789,860	103	1,789,860	0	115
winnnt://demo\hr	78,010,282	922	78,010,282	0	1,311
L winnt://demo\charlie.day	3,152,555	101	3,152,555	0	150
L winnt://demo\holly.steele	12,714,156	83	12,714,156	0	140
L winnt://demo\kyle.doherty	15,559,893	98	15,559,893	0	134
winnnt://demo\management	418,560,061	643	418,560,061	0	928
L winnt://demo\ogon.fleming	2,335,942	70	2,335,942	0	138
L winnt://demo\chloe.whiteh	2,015,070	84	2,015,070	0	124
L winnt://demo\muhammad.bre	1,249,900	88	1,249,900	0	114
winnnt://demo\engineering	243,900,754	649	243,900,754	0	876
L winnt://demo\jaron.hought	27,558,319	92	27,558,319	0	152
L winnt://demo\samantha.cha	1,131,789	108	1,131,789	0	124
L winnt://demo\poppy.holden	192,132,526	88	192,132,526	0	113
winnnt://demo\paris	45,629,668	512	45,629,668	0	665
L winnt://demo\samantha.cha	1,131,789	108	1,131,789	0	124
L winnt://demo\alex.townsen	969,480	72	969,480	0	111
L winnt://demo\thomas.steph	2,267,151	89	2,267,151	0	100
winnnt://demo\bangkok	479,558,614	495	479,558,614	0	657
L winnt://demo\jodie.mitche	2,517,252	86	2,517,252	0	118
L winnt://demo\olivia.skinn	67,537,028	97	67,537,028	0	113
L winnt://demo\scarlett.de	405,666,255	63	405,666,255	0	110

9. If you have set any rules in your web filtering policy that apply the anonymize action, ensure that you can see results where the group and user attributes state Undisclosed, and the Internal IP attribute shows 0.0.0.0.

Who were the top ten users that browsed the most?

Show 50 rows per page << first < prev 1 next > last >> 1 result

	User   Internal IP	Bandwidth (Bytes)	Browse Time (Min)	Bytes Received	Bytes Sent	Hits
	Totals for User	3,262	42	3,262	0	42
	undisclosed	3,262	42	3,262	0	42
	L 0.0.0.0	3,262	42	3,262	0	42

## Further Actions

For full details of the administration tasks available in ScanCenter, please refer to the full Cisco ScanCenter Admin Guide available at:

[http://www.cisco.com/en/US/products/ps11720/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html).



Americas Headquarters  
Cisco Systems, Inc.  
San Jose, CA

Asia Pacific Headquarters  
Cisco Systems (USA) Pte. Ltd.  
Singapore

Europe Headquarters  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)