The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Notwithstanding any other warranty herein, all document files and software of these suppliers are provided "as is" with all faults. Cisco and the above-named suppliers disclaim all warranties, expressed or implied, including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement or arising from a course of dealing, usage, or trade practice.

In no event shall Cisco or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Cisco or its suppliers have been advised of the possibility of such damages.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

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: 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)
CONTENTS

CHAPTER 1
Introduction 1
  Pre-requisite 1
  Requirements 1
  Components Used 2
  Conventions 2

CHAPTER 2
Configurations Steps for Domain Filtering 3
  Domain Filtering Overview 3
    Considerations 4
  Configurations Steps for Domain Filtering 5
    Enabling Domain Filtering 5
      Enabling Domain Filtering using GUI 5
      Enabling Domain Filtering using CLI 6
  Access Control Lists and Rules 6
    Access Control Lists 6
      Access Control Lists using GUI 6
      Access Control Lists using CLI 8
    Rules—Blacklisting Example 8
      Rules Blacklisting using GUI 8
      Rules Blacklisting using CLI 10
    Rules—Whitelisting Example 11
      Rules Whitelisting using GUI 11
      Rules Whitelisting using CLI 12
  Enabling Hit Counters 13
    Enabling Hit Counters using GUI 13
    Enabling Hit Counters using CLI 14
  Applying Access Control Lists 15
    WLANs 15
Contents

Accessing WLANs using GUI 15
Accessing WLANs using CLI 16

Interfaces 17
Interfaces using GUI 17
Interfaces using CLI 17

Local Policies 18
Local Policies using GUI 18
Local Policies using CLI 19
Introduction

This document introduces the Domain Filtering feature and provides general guidelines for its deployment. The purpose of this document is to:

- Provide an overview of Domain Filtering
- Highlight supported key features and limitations
- Provide details on deploying and configuring Domain Filtering

- Pre-requisite, page 1
- Requirements, page 1
- Components Used, page 2
- Conventions, page 2

Pre-requisite

- Beta customers must have AireOS 8.3 release installed on a supported WLC (see requirements).
- For the beta, AVC Engine Version 23 / Protocol Pack Version 16 must be manually installed on the WLC for Domain Filtering to function (provided on the beta web site).
- Domain Filtering requires the WLAN traffic to be centrally forwarded through the WLC. For this beta Domain Filtering requires Access Points to be operating in Local Mode or FlexConnect WLANs to be configured for Central Switching.

Requirements

Domain Filtering will be supported on the following Wireless LAN Controller platforms:

- Cisco 5508 Wireless LAN Controller
- Cisco 5520 Wireless LAN Controller
- Cisco 8510 Wireless LAN Controller
Components Used

The information in this document was created from 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.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.
Domain Filtering Overview

Domain Filtering is a new enhancement that is being introduced as part of the 8.3 release. This enhancement complements the Application Visibility Control (AVC) filtering currently available on the WLC. AVC filtering only supports the protocols and applications that are defined in the Protocol Pack for a given AirOS release allowing specific applications to be dropped, marked or rate-limited.

Domain Filtering builds upon AVC by using the NBAR2 engine to look deeper into the application layer matching on both the application type (e.g. HTTP) and host (e.g. www.cisco.com). In the 8.3 release administrators can now define ACLs and rules which can be applied to WLANs, Interfaces or Local Policies to either permit or deny HTTP traffic destined to specific hosts providing greater flexibility and control.
Domain Filtering is based on the NBAR2 engines filtering capabilities using field extraction. The latest NBAR2 engine supports 120 custom applications. URLs can be defined as a custom application and be classified by the engine:

1. URLs are classified using ACLs defined on the WLC. Each ACL has rules defined that determine the URLs to be matched.
2. The NBAR2 engine is configured to extract the URL field (if present) in the packets passed to it. Field extraction is performed per flow to optimize performance.
3. The WLC passes HTTP packets to the NBAR2 engine to extract the URL. If present, the NBAR2 engine returns the host-name (for example www.cisco.com) as the URL to the WLC.
4. The WLC implements filtering logic for the extracted URLs and takes the appropriate forwarding action (i.e. permit or denies the flow).

**Considerations**

- This release supports a maximum of 100 x URL ACLs:
  - Each ACL supports a maximum of 64 rules.
  - Each rule has either a permit or deny action. At least one permit rule must be defined per URL ACL for traffic to be permitted.
  - Each ACL has an implicit "deny all rule" as the last rule. If a URL does not match any of the rules, it is dropped by the WLC.
  - Each rule is inspected in order of precedence (lowest to highest). The first rule in the ACL that is matched is applied to the flow.
  - Each rule supports a maximum length 32 characters.
Each rule must match the exact subdomain, domain and top level domain you wish to match (example www.cisco.com, tools.cisco.com or partners.cisco.com).

Partial matches using wildcards or regular expressions are not supported in this release (example www.c*.com or *.cisco.com).


One wildcard (*) rule with a permit or deny action is supported per ACL. The wildcard matches all URLs.

- No support for AVC Profiles for matched URLs is provided in this release. URL ACLs and rules are defined separately then applied to WLANs, Interfaces or Local Policies.
- No support for IPv6 in this release (IPv4 support only).
- No support for PI is provided in this release.

Note

This release supports HTTP URLs only. HTTPS URL support will be introduced in a later release.

Configurations Steps for Domain Filtering

Enabling Domain Filtering

Domain filtering is globally disabled on the WLC by default and must be enabled before the NBAR2 engine can inspect and filter HTTP based URLs. The following step demonstrates how to globally enable Domain Filtering on a WLC.

Enabling Domain Filtering using GUI

To enable domain filtering using GUI, perform the following steps:

Procedure

From the WLC main menu choose Security > Access Control Lists > URL ACLs. Select Enable URL Acl then click Apply.
Enabling Domain Filtering using CLI

To enable domain filtering using CLI, perform the following steps:

**Procedure**

Globally enable Domain Filtering:

(Cisco Controller) > config acl url-acl enable

Step 2: Verify enablement. The URL ACL Feature field will change from Disabled to Enabled:

(Cisco Controller) > show acl url-acl summary

<table>
<thead>
<tr>
<th>URL ACL Feature</th>
<th>ACL Counter Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

---

Access Control Lists and Rules

Domain filtering determines which HTTP based URLs to permit or deny using ACLs and rules that are assigned to WLANs, Interfaces or individual client sessions by way of Local Policies. The following steps demonstrate how to create URL based ACLs and rules for two common scenarios:

- Scenario 1—A ACL and rules are defined to deny access to specific HTTP URLs. This is commonly referred to as Blacklisting.
- Scenario 2—A ACL and rules are defined to only permit access to specific HTTP URLs. This is commonly referred to as Whitelisting.

Access Control Lists

**Access Control Lists using GUI**

To enable access control lists using GUI, perform the following steps:
Procedure

Step 1  From the WLC main menu choose SECURITY > Access Control Lists > URL ACLs and then click New.

Step 2  Enter the URL ACL Name and then click Apply.
In this example a ACL named BLOCK-HTTP-SITES has been defined.

Step 3  Click New to define additional ACLs.

Step 4  Enter the URL ACL Name and then click Apply.
In this example a second ACL named PERMIT-HTTP-SITES has been defined.
**Access Control Lists using CLI**

To enable access control lists using CLI, perform the following steps:

**Procedure**

**Step 1** Create the URL ACLs named BLOCK-HTTP-SITES and PERMIT-HTTP-SITES:

(Cisco Controller) > config acl url-acl create BLOCK-HTTP-SITES
(Cisco Controller) > config acl url-acl create PERMIT-HTTP-SITES

**Step 2** Verify ACL creation. Note the Applied status fields for both ACLs will display as No until rules are added and the ACLs are applied:

(Cisco Controller) > show acl url-acl summary
URL ACL Feature Enabled
ACL Counter Status Disabled

<table>
<thead>
<tr>
<th>URL ACL Name</th>
<th>Applied</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLOCK-HTTP-SITES</td>
<td>No</td>
</tr>
<tr>
<td>ALLOW-HTTP-SITES</td>
<td>No</td>
</tr>
</tbody>
</table>

**Rules–Blacklisting Example**

The following configuration steps demonstrate how to use rules to deny access to specific HTTP URLs (commonly referred to as blacklisting). In this example an ordered list of URLs is defined with a deny action to block access to specific requested HTTP based URLs. As the ACL itself has an implied deny, a wildcard permit rule is added as the last rule to provide access to all other requested HTTP URLs.

**Rules Blacklisting using GUI**

To enable rules blacklisting using GUI, perform the following steps:

**Procedure**

**Step 1** From the WLC main menu choose SECURITY > Access Control Lists > URL ACLs. Click on the URL ACL Name to add rules.
Step 2  Click Add New Rule.

Step 3  Enter a Rule Index then define a URL to match and Action. In this example, the URL www.cisco.com has been defined as the first rule with the action set to Deny. Click Apply. Add additional Deny rules as required.

Step 4  Define a final rule that permits access to all other HTTP sites. In this example, a wildcard URL * has been defined as the last rule with the action set to Permit. Click Apply.
**Step 5** Verify your rules are correct then click *Apply All*. The *Status* field will change from *Not Applied* to *Applied*.

**Rules Blacklisting using CLI**

To enable rules blacklisting using CLI, perform the following steps:

**Procedure**

**Step 1** Create rules for the ACL named `BLOCK-HTTP-SITES`.

(Cisco Controller) > config acl url-acl rule add BLOCK-HTTP-SITES 1
(Cisco Controller) > config acl url-acl rule url BLOCK-HTTP-SITES 1 www.cisco.local
(Cisco Controller) > config acl url-acl rule action BLOCK-HTTP-SITES 1 deny
(Cisco Controller) > config acl url-acl rule add BLOCK-HTTP-SITES 2
(Cisco Controller) > config acl url-acl rule url BLOCK-HTTP-SITES 2 www.nba.local
(Cisco Controller) > config acl url-acl rule action BLOCK-HTTP-SITES 2 deny

! Configuration Suppressed for rules 3 - 5

(Cisco Controller) > config acl url-acl rule add BLOCK-HTTP-SITES 6
(Cisco Controller) > config acl url-acl rule url BLOCK-HTTP-SITES 6 *
(Cisco Controller) > config acl url-acl rule action BLOCK-HTTP-SITES 6 permit

**Step 2** Apply the ACL.

(Cisco Controller) > config acl url-acl apply BLOCK-HTTP-SITES

**Step 3** Verify the ACL rules.

(Cisco Controller) > show acl url-acl detailed BLOCK-HTTP-SITES

<table>
<thead>
<tr>
<th>RuleIndex</th>
<th>Action</th>
<th>URL</th>
<th>Hit Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Deny</td>
<td><a href="http://www.cisco.com">www.cisco.com</a></td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>Deny</td>
<td><a href="http://www.nba.com">www.nba.com</a></td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>Deny</td>
<td><a href="http://www.disney.com">www.disney.com</a></td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>Deny</td>
<td><a href="http://www.nfl.com">www.nfl.com</a></td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>Deny</td>
<td><a href="http://www.united.com">www.united.com</a></td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>Permit</td>
<td>*</td>
<td>0</td>
</tr>
</tbody>
</table>
Steps

Step 4 Verify the ACL has been applied. The Applied status field for the BLOCK-HTTP-SITES ACL will change from No to Yes.

(Cisco Controller) > show acl url-acl summary

URL ACL Feature Enabled
ACL Counter Status Disabled

--------------------------------------------------------------
URL ACL Name  Applied
-------------  ------
BLOCK-HTTP-SITES Yes
ALLOW-HTTP-SITES No

Rules–Whitelisting Example

The following configuration steps demonstrate how to use rules to only permit access to specific HTTP URLs (commonly referred to as whitelisting). In this example an ordered list of URLs is defined with a permit action to allow access to specific requested HTTP based URLs. As the ACL has an implied deny, access to all other requested HTTP URLs will be blocked.

Rules Whitelisting using GUI

To enable rules whitelisting using GUI, perform the following steps:

Procedure

Step 1 From the WLC main menu choose SECURITY > Access Control Lists > URL ACLs. Click on the URL ACL Name to add rules.

Step 2 Click Add New Rule.
**Rules Whitelisting using CLI**

To enable rules whitelisting using CLI, perform the following steps:

**Procedure**

**Step 1** Create rules for the ACL named **ALLOW-HTTP-SITES**.

(Cisco Controller) > config acl url-acl rule add ALLOW-HTTP-SITES 1
(Cisco Controller) > config acl url-acl rule url ALLOW-HTTP-SITES 1 www.cisco.local
(Cisco Controller) > config acl url-acl rule action ALLOW-HTTP-SITES 1 permit
Step 2  Apply the ACL.
(Cisco Controller) > config acl url-acl apply ALLOW-HTTP-SITES

Step 3  Verify the ACL rules
(Cisco Controller) > show acl url-acl detailed ALLOW-HTTP-SITES
RuleIndex    Action       URL                Hit Count
------------- ----------- ------------------ --------------
            Permit       www.cisco.com          0

Step 4  Verify the ACL has been applied. The Applied status field for the ALLOW-HTTP-SITES ACL will change from No to Yes.
(Cisco Controller) > show acl url-acl summary
URL ACL Feature  Enabled
ACL Counter Status  Disabled
----------------------------------------
URL ACL Name  Applied
--------------- -------
BLOCK-HTTP-SITES  Yes
ALLOW-HTTP-SITES  Yes

Enabling Hit Counters

Hit counters can be optionally enabled to monitor the number of rule hits for each URL ACL. Hit counters are useful for troubleshooting ACLs as the counters are incremented by one as each rule is matched. The following step demonstrates how to globally enable ACL hit counters on a WLC.

Enabling Hit Counters using GUI

To enable hit counters using GUI, perform the following steps:

Procedure

Step 1  From the WLC main menu choose Security > Access Control Lists > Access Control Lists. Select Enable Counters and then click Apply.

Step 2  From the WLC main menu choose Security > Access Control Lists > URL ACLs. Click on the desired URL ACL Name to view the Hit Count for each matched URL.
Enabling Hit Counters using CLI

To enable hit counters using CLI, perform the following steps:

**Procedure**

**Step 1** Globally enable ACL Hit Counters.
(Cisco Controller) > config acl counter start

**Step 2** Verify enablement. The **ACL Counter Status** field changes from **Disabled** to **Enabled**.
(Cisco Controller) > show acl url-acl summary
URL ACL Feature Enabled
ACL Counter Status Enabled

<table>
<thead>
<tr>
<th>URL ACL Name</th>
<th>Applied</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLOCK-HTTP-SITES</td>
<td>Yes</td>
</tr>
<tr>
<td>ALLOW-HTTP-SITES</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Step 3** View the Hit Counters for a specific ACL. In this example the Hit Count for the ACL named **BLOCK-HTTP-SITES** is displayed.
(Cisco Controller) > show acl url-acl detailed BLOCK-HTTP-SITES

<table>
<thead>
<tr>
<th>RuleIndex</th>
<th>Action</th>
<th>URL</th>
<th>Hit Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Deny</td>
<td><a href="http://www.cisco.com">www.cisco.com</a></td>
<td>41</td>
</tr>
<tr>
<td>2</td>
<td>Deny</td>
<td><a href="http://www.nba.com">www.nba.com</a></td>
<td>24</td>
</tr>
<tr>
<td>3</td>
<td>Deny</td>
<td><a href="http://www.disney.com">www.disney.com</a></td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>Deny</td>
<td><a href="http://www.nfl.com">www.nfl.com</a></td>
<td>8</td>
</tr>
<tr>
<td>5</td>
<td>Deny</td>
<td><a href="http://www.united.com">www.united.com</a></td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>Permit</td>
<td>*</td>
<td>25</td>
</tr>
</tbody>
</table>
Applying Access Control Lists

URL ACLs can be assigned dynamically to clients using Local Policies or directly to WLANs or Interfaces:

- **Local Policy** – The URL ACL is applied to all clients assigned the Local Policy. URL ACLs assigned using Local Policies have the highest priority and will override URL ACLs assigned to the WLAN or Interface.

- **WLANs** – The URL ACL is applied to all clients associated to the WLAN (unless a URL ACL is assigned to a client using a Local Policy). URL ACLs assigned to a WLAN will override a URL ACL assigned to an Interface.

- **Interfaces** – The URL ACL is applied to all traffic forwarded specific interface.

The following steps demonstrate how to assign URL ACLs on a WLC to WLANs, Interfaces and Local Policies.

**WLANs**

**Accessing WLANs using GUI**

To access WLANs using GUI, perform the following steps:

**Procedure**

**Step 1** From the WLC main menu choose **WLANs > WLANs**. Select a **WLAN ID** to modify the access to the **QoS** tab. Verify **Application Visibility** is enabled.

**Step 2** Access the **Advanced Tab** then assign the desired **URL ACL**. Click **Apply**.
Application Visibility must be enabled on each WLAN for an assigned URL ACL.

**Note**

Accessing WLANs using CLI

To access WLANs using CLI, perform the following steps:

**Procedure**

**Step 1** Disable the target WLAN. In this example WLAN id 1 is disabled. The WLC does not allow you to assign the ACL if the target WLAN is enabled.

(Cisco Controller) > config wlan disable 1

**Step 2** Assign the URL ACL to the WLAN. In this example the ACL named **BLOCK-HTTP-SITES** is assigned to WLAN 1.

(Cisco Controller) > config wlan url-acl 1 BLOCK-HTTP-SITES

**Step 3** Re-enable the disabled WLAN.

(Cisco Controller) > config wlan enable 1

**Step 4** Verify the ACL assignment. If no ACL has been assigned to the WLAN, the **WLAN URL ACL** field will show **unconfigured**.

(Cisco Controller) > show wlan 1

```
WLAN Identifier.............................. 1
Profile Name.................................. TMELABS-PSK
Network Name (SSID).......................... TMELABS-PSK
Status........................................ Enabled
MAC Filtering................................. Disabled
```
Interfaces

Interfaces using GUI

To access interfaces using GUI, perform the following steps:

Procedure

From the WLC main menu choose CONTROLLER > Interfaces. Select an Interface Name to modify, then under Access Control List assign the desired URL ACL. Click Apply.

Interfaces using CLI

To access interfaces using CLI, perform the following steps:
Procedure

Step 1 Disable the WLANs using the target Interface. In this example WLAN id 3 is mapping clients vlan25. The WLC does not allow you to assign the ACL to an Interface if there are any active WLANs using the interface.

(Cisco Controller) > config wlan disable 3

Step 2 Assign the URL ACL to the WLAN. In this example the ACL named BLOCK-HTTP-SITES is assigned to WLAN 1.

(Cisco Controller) > config interface url-acl vlan25 BLOCK-HTTP-SITES

Step 3 Re-enable the disabled WLAN.

(Cisco Controller) > config wlan enable 3

Step 4 Verify the ACL assignment. Note if no ACL has been assigned to the Interface, the WLAN URL ACL field will show unconfigured.

(Cisco Controller) > show interface detailed vlan25

Interface Name................................. vlan25
MAC Address................................. 4c:00:82:71:4f:af
IP Address...................................... 192.168.25.22
IP Netmask..................................... 255.255.255.0
IP Gateway.................................... 192.168.25.1

! Output Suppressed

! IPv4 ACL...................................... Unconfigured
URL ACL........................................ BLOCK-HTTP-SITES

Note You can remove the ACL from a Interface by issuing the config interface url-acl <interface-name> none command.

Local Policies

Local Policies using GUI

To access local policies using GUI, perform the following steps:

Procedure

From the WLC main menu select SECURITY > Local Policies. Select a Policy Name to modify, then under Action assign the desired URL ACL. Click Apply.

**Local Policies using CLI**

To access local policies using CLI, perform the following steps:

**Procedure**

**Step 1** Assign the ACL to the target Local Policy. In this example the ACL named BLOCK-HTTP-SITES is assigned to a Local Policy named STUDENTS.

(Cisco Controller) > config policy STUDENTS action url-acl enable BLOCK-HTTP-SITES

**Step 2** Verify the ACL assignment.

(Cisco Controller) > config interface url-acl vlan25 BLOCK-HTTP-SITES

**Step 3** Re-enable the disabled WLAN.

(Cisco Controller) > config wlan enable 3

**Step 4** Verify the ACL assignment. Note if no ACL has been assigned to the Local Policy, the URL ACL field will show <none>.

(Cisco Controller) > show POLICY STUDENTS
Policy Index................................. 1
Match Role.................................. STUDENTS
Match Eap Type............................ <none>
IPV4 ACL.................................. <none>
URL ACL.................................. BLOCK-HTTP-SITES
FlexConnect Client ACL.................. <none>
QOS........................................ BRONZE

!
You can remove the ACL from a Local Policy by issuing the `config policy <policy-name> action url-acl disable` command.