Configuring an FQDN ACL

This document describes how to configure an access control lists (ACL) using a fully qualified domain name (FQDN). The Configuring an FQDN ACL feature allows you to configure and apply an ACL to a wireless session based on the domain name system (DNS). The domain names are resolved to IP addresses, the IP addresses are given to the client as part of the DNS response, and the FQDN is then mapped to an ACL based on the IP address.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Configuring FQDN ACL

The Configuring FQDN ACL feature is supported only on IPv4 wireless sessions.

Information About Configuring an FQDN ACL

Configuring an FQDN ACL

When access control lists (ACLs) are configured using a fully qualified domain name (FQDN), ACLs can be applied based on the destination domain name. The destination domain name is then resolved to an IP address, which is provided to the client as a part of the DNS response.

Guest users can log in using web authentication with a parameter map that consists of an FQDN ACL name.

Before you configure an FQDN ACL, complete the following tasks:

- Configure an IP access list.
- Configure an IP domain name list.
- Map an FQDN ACL with a domain name.

You can apply an access list to a specific domain by configuring the RADIUS server to send the **fqdn-acl-name** AAA attribute to the controller. The operating system checks for the passthrough domain list and its mapping, and permits the FQDN. The FQDN ACL allows clients to access only configured domains without authentication.

Note By default, an IP access list name is configured with the same name as the pass-through domain name. To override the default name, you can use the **access-session passthrou-access-group** *access-group-name* **passthrou-domain-list** *domain-list-name* command in global configuration mode.

How to Configure FQDN ACL

Configuring an IP Access List

SUMMARY STEPS

1. **configure terminal**
2. **ip access-list extended** *name*
3. **permit ip any any**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `# configure terminal`	Enters global configuration mode.
Step 2	**ip access-list extended** *name* **Example:** `(config)# ip access-list extended ABC`	Creates the IP access list.
Step 3	**permit ip any any** **Example:** `(config-ext-nacl)# permit ip any any`	Specifies the domains to be allowed for the wireless client. The domains are specified in the domain name list.
Step 4	**end** **Example:** `(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring a Domain Name List

You can configure a domain name list that contains a list of domain names that are allowed for DNS snooping by the access point. The DNS domain list name string must be identical to the extended access list name.

SUMMARY STEPS

1. **configure terminal**
2. **passthrou-domain-list** *name*
3. **match** *word*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose

Step 2	**passthrou-domain-list** *name*
	
	Example:
	`(config)# passthrou-domain-list abc`
	`(config-fqdn-acl-domains)#`
		Configures a passthrough domain name list.

Step 3	**match** *word*
	
	Example:
	`(config-fqdn-acl-domains)# match play.google.com`
	`(config-fqdn-acl-domains)# match www.yahoo.com`
		Configures a passthrough domain list. Adds a list of websites that the client is allowed to query for access without first being required to be authenticated through the RADIUS server.

Step 4	**end** **Example:** `(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Mapping the FQDN ACL with a Domain Name

SUMMARY STEPS

1. **configure terminal**
2. **access-session passthrou-access-group** *access-group-name* **passthrou-domain-list** *domain-list-name*
3. **parameter-map type webauth** *domain-list-name* and **login-auth-bypass fqdn-acl-name** *acl-name* **domain-name** *domain-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `# configure terminal`	Enters global configuration mode.
Step 2	**access-session passthrou-access-group** *access-group-name* **passthrou-domain-list** *domain-list-name* **Example:** `(config)# access-session passthrou-access-group abc passthrou-domain-list abc`	Maps the FQDN ACL AAA attribute name with the domain name list. Use this command when configuring central web authentication.

	Command or Action	Purpose

Step 3	**parameter-map type webauth** *domain-list-name* and **login-auth-bypass fqdn-acl-name** *acl-name* **domain-name** *domain-name*
	
	Example:
	`(config)# parameter-map type webauth abc`
	`(config-params-parameter-map)# login-auth-bypass fqdn-acl-name abc domain-name abc`
		Maps an FQDN ACL name with the domain name list. Use the command when configuring local authentication on the controller.
		
		The RADIUS server can be configured to return an FQDN ACL name as part of the authenticated user profile. The controller dynamically applies the FQDN ACL to the user if the FQDN ACL is defined on the controller.

Monitoring an FQDN ACL

The following commands can be used to monitor FQDN ACLs.

Command	Purpose
show access-session interface *interface-name* **details**	Displays the FQDN ACL information configured on the interface.
show access-session fqdn fqdn-maps	Displays the FQDN ACL mapped to the domain name list.
show access-session fqdn list-domain *domain-name*	Displays the domain names.
show access-session fqdn passthru-domain-list	Displays the domains that are configured.

Configuration Examples for an FQDN ACL

Examples: FQDN ACL Configuration

This example shows how to create IP access list:

```
# config terminal
(config)# ip access-list extended abc
(config-ext-nacl)# permit ip any any
(config-ext-nacl)# end
# show ip access-list abc
```

This example shows how to configure domain name list:

```
# config terminal
(config)# passthrou-domain-list abc
(config-fqdn-acl-domains)# match play.google.com
(config-fqdn-acl-domains)# end
# show access-session fqdn fqdn-maps
```

This example shows how to map FQDN ACL with domain name using central web authentication:

```
# config terminal
(config)# access-session passthrou-access-group abc passthrou-domain-list abc
(config)# end
# show access-session interface vlan 20
```

This example shows how to map FQDN ACL with domain name using local authentication:

```
# config terminal
(config)# parameter-map type webauth abc
(config-params-parameter-map)# login-auth-bypass fqdn-acl-name abc domain-name abc
(config-params-parameter-map)# end
# show access-session fqdn fqdn-maps
```

Additional References for Configuring FQDN ACL

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z
ACL configuration guide	*Security Configuration Guide: Access Control Lists*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring FQDN ACL

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Configuring FQDN ACL

Feature Name	Releases	Feature Information
Configuring an FQDN ACL	Cisco IOS 15.2(2)E	

Feature Name	Releases	Feature Information
		The Configuring an FQDN ACL feature allows you to configure and apply an access control lists (ACL) to a wireless session based on the domain name system (DNS). The domain names are resolved to IP addresses, where the IP addresses are given to the client as part of the DNS response; the FQDN is then mapped to an ACL based on the IP address. In Cisco IOS RElease 15.2(2)E or Cisco IOS XE 3.6E, this feature is supported on the following platforms: • Catalyst 4500E Supervisor Engine 7-E • Catalyst 4500E Supervisor Engine 7L-E • Catalyst 4500E Supervisor Engine 8-E • Catalyst 4500-X Series Switches • Catalyst 3850 Series Switches • Catalyst 3650 Series Switches • Cisco 5760 Wireless Controller • Cisco Industrial Ethernet 3000 Series Switches • Cisco Industrial Ethernet 2000 Series Switches • Cisco Catalyst 2960-S Series Switches (Stout) • Cisco Catalyst 2960-X Series Switches (Porter) • Cisco Catalyst 2960-X Series Switches (Kingfisher) The following commands were introduced or modified: **access**

Feature Name	Releases	Feature Information
		session passthrou access group, **login-auth-bypass**, **parameter-map type webauth global**, **pass throu domain list name**, **show access-session fqdn**.