FQDN ACL の設定

このドキュメントでは、完全修飾ドメイン名（FQDN）を使用したアクセス コントロール リスト（ACL ）を設定する方法について説明します。FQDN ACL 機能を設定することによって、ドメイン名システム（DNS ）に基づいて、ワイヤレス セッションに ACL を設定および適用することができます。ドメイン名を IP アドレスに解決されます。IP アドレスは、DNS 応答の一部としてクライアントに提供され、FQDN は、IP アドレスに基づいて、ACL にマッピングされます。

- 機能情報の確認 （1 ページ）
- FQDN ACL の設定に関する制約事項 （1 ページ）
- FQDN ACL の設定に関する情報 （2 ページ）
- FQDN ACL の設定方法 （2 ページ）
- FQDN ACL のモニタリング （5 ページ）
- FQDN ACL の設定例 （5 ページ）
- FQDN ACL の設定に関するその他の参考資料 （6 ページ）
- FQDN ACL の設定に関する機能情報 （6 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

FQDN ACL の設定に関する制約事項

FQDN ACL 機能の設定は、IPv4 ワイヤレス セッションでのみサポートされます。

FQDN ACL の設定に関する情報

FQDN ACL の設定

アクセス コントロール リスト（ACL）が、完全修飾ドメイン名（FQDN）を使用して設定されている場合、宛先ドメイン名に基づいて ACL を適用できます。宛先のドメイン名はその後、DNS 応答の一部としてクライアントに提供される IP アドレスに解決されます。

ゲスト ユーザは、FQDN ACL 名で構成されるパラメータ マップでネットワーク認証を使用してログインできます。

FQDN ACL を設定する前に、次の作業を実行してください。

- IP アクセス リストを設定します。
- IP ドメイン名のリストを設定します。
- ドメイン名と FQDN ACL をマッピングします。

コントローラに **fqdn-acl-name** AAA 属性を送信するように RADIUS サーバを設定して、アクセス リストを特定のドメインに適用できます。オペレーティング システムは、パススルー ドメイン リストとそのマッピングを確認し、FQDN を許可します。FQDN ACL により、クライアントは認証なしで設定されたドメインのみにアクセスできます。

（注） デフォルトでは、IPアクセスリスト名は、パススルードメイン名と同じ名前で設定されます。デフォルト名を上書きするために、グローバル コンフィギュレーション モードで**access-session passthrou-access-group** *access-group-name* **passthrou-domain-list** *domain-list-name* コマンドを使用できます。

FQDN ACL の設定方法

IP アクセス リストの設定

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip access-list extended** *name* 例： `(config)# ip access-list extended ABC`	IP アクセス リストを作成します。
ステップ 3	**permit ip any any** 例： `(config-ext-nacl)# permit ip any any`	ワイヤレス クライアントに許可されるドメインを指定します。ドメインはドメイン名リストで指定されます。
ステップ 4	**end** 例： `(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ドメイン名リストの設定

アクセス ポイントによる DNS スヌーピングが許可されたドメイン名のリストを含むドメイン名リストを設定できます。DNS ドメイン リスト名の文字列は、拡張アクセス リスト名と一致している必要があります。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**passthrou-domain-list** *name*
	例：
	`(config)# passthrou-domain-list abc`
	`(config-fqdn-acl-domains)#`
		パススルー ドメイン名リストを設定します。

	コマンドまたはアクション	目的

ステップ 3	**match** *word*
	例：
	`(config-fqdn-acl-domains)# match play.google.com`
	`(config-fqdn-acl-domains)# match www.yahoo.com`
		パススルー ドメイン リストを設定します。クライアントがRADIUSサーバを介して認証される必要なくアクセスの照会が許可されるWebサイトのリストを追加します。

ステップ 4	**end** 例： `(config)# end`	特権EXECモードに戻ります。また、Ctrl+Z キーを押しても、グローバルコンフィギュレーションモードを終了できます。

ドメイン名と FQDN ACL のマッピング

手順の概要

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*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-session passthrou-access-group** *access-group-name* **passthrou-domain-list** *domain-list-name* 例： `(config)# access-session passthrou-access-group abc passthrou-domain-list abc`	ドメイン名リストと FQDN ACL AAA 属性名をマッピングします。中央Web認証を設定する場合、このコマンドを使用します。

ステップ 3	**parameter-map type webauth** *domain-list-name* and **login-auth-bypass fqdn-acl-name** *acl-name* **domain-name** *domain-name*
	例：
	`(config)# parameter-map type webauth abc`
	`(config-params-parameter-map)# login-auth-bypass fqdn-acl-name abc domain-name abc`
		ドメイン名リストと FQDN ACL 名をマッピングします。コントローラでローカル認証を設定する場合、このコマンドを使用します。
		RADIUSサーバは、認証されたユーザプロファイルの一部として FQDN ACL 名を返すように設定できます。FQDN ACL がコントローラで定義される場合、コントローラは FQDN ACL をユーザに動的に適用します。

FQDN ACL のモニタリング

次のコマンドを使用して FQDN ACL をモニタできます。

コマンド	目的
show access-session interface *interface-name* **details**	インターフェイスに設定された FQDN ACL 情報を表示します。
show access-session fqdn fqdn-maps	ドメイン名リストにマッピングされた FQDN ACL を表示します。
show access-session fqdn list-domain *domain-name*	ドメイン名を表示します。
show access-session fqdn passthru-domain-list	設定されているドメインを表示します。

FQDN ACL の設定例

例：FQDN ACL の設定

次に、IP アクセス リストを作成する例を示します。

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

次に、ドメイン名のリストを設定する例を示します。

```
# 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
```

次に、中央集中型 Web 認証を使用してドメイン名と FQDN ACL をマッピングする例を示します。

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

次に、ローカル認証を使用してドメイン名と FQDN ACL をマッピングする例を示します。

```
# 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
```

FQDN ACL の設定に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	Cisco IOS Master Command List, All Releases
セキュリティ コマンド	• 『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 設定ガイド	『*Security Configuration Guide: Access Control Lists*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

FQDN ACL の設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

けを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : FQDN ACL* の設定に関する機能情報

機能名	リリース	機能情報
FQDN ACL の設定		FQDN ACL 機能を設定することで、ドメイン名システム（DNS）に基づいてワイヤレス セッションにアクセス コントロール リスト（ACL）を設定、適用することができます。ドメイン名が IP アドレスが DNS 応答の一部として、クライアントに割り当てるられる IP アドレスに解決されます。次に FQDN が IP アドレスに基づいて ACL にマッピングされます。 次のコマンドが導入または変更されました。**access session passthrou access group**、**login-auth-bypass**、**parameter-map type webauth global**、 **pass throu domain list name**、**show access-session fqdn**