



F コマンド

この章では、F で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

feature (ユーザ ロール機能グループ)

ユーザ ロール機能グループに機能を設定するには、**feature** コマンドを使用します。ユーザ ロール機能グループから機能を削除するには、このコマンドの **no** 形式を使用します。

feature *feature-name*

no feature *feature-name*

構文の説明	<i>feature-name</i>	show role feature コマンドの出力に表示される Cisco NX-OS 機能名。
デフォルト	なし	
コマンド モード	ユーザ ロール機能グループ コンフィギュレーション	
サポートされるユーザ ロール	network-admin vdc-admin	
コマンド履歴	リリース	変更箇所
	4.0(1)	このコマンドが追加されました。
使用上のガイドライン	このコマンドで使用できる有効な機能名を表示するには、 show role feature コマンドを使用します。このコマンドには、ライセンスは必要ありません。	
例	次に、ユーザ ロール機能グループに機能を追加する例を示します。 <pre>switch# configure terminal switch(config)# role feature-group name SecGroup switch(config-role-featuregrp)# feature aaa switch(config-role-featuregrp)# feature radius switch(config-role-featuregrp)# feature tacacs</pre> 次に、ユーザ ロール機能グループから機能を削除する例を示します。 <pre>switch# configure terminal switch(config)# role feature-group name MyGroup switch(config-role-featuregrp)# no feature callhome</pre>	
関連コマンド	コマンド	説明
	show role feature-group	ユーザ ロール機能グループを表示します。

feature cts

Cisco TrustSec 機能をイネーブルにするには、**feature cts** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

feature cts

no feature cts

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンドモード

グローバル コンフィギュレーション

サポートされるユーザロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature dot1x** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。



(注)

Cisco TrustSec 機能には、ライセンス猶予期間はありません。この機能を設定するには、アドバンスド サービス ライセンスをインストールする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、Cisco TrustSec 機能をイネーブルにする例を示します。

```
switch# configure terminal  
switch(config)# feature cts
```

次に、Cisco TrustSec 機能をディセーブルにする例を示します。

```
switch# configure terminal  
switch(config)# no feature cts
```

関連コマンド

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。
show cts	Cisco TrustSec のステータス情報を表示します。

feature dhcp

デバイス上で DHCP スヌーピング機能をイネーブルにするには、**feature dhcp** コマンドを使用します。DHCP スヌーピング機能をディセーブルにし、DHCP リレー、Dynamic ARP Inspection (DAI; ダイナミック ARP インスペクション)、IP ソース ガード設定を含む、DHCP スヌーピングに関連するすべての設定を削除するには、このコマンドの **no** 形式を使用します。

feature dhcp

no feature dhcp

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンドモード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

DHCP スヌーピング機能は、デフォルトではディセーブルです。

DHCP スヌーピング機能をイネーブルにしないと、DHCP スヌーピングの関連コマンドを使用できません。

ダイナミック APR インスペクションおよび IP ソース ガードは、DHCP スヌーピング機能に依存しません。

DHCP スヌーピング機能をディセーブルにすると、次の機能を含む、DHCP スヌーピング設定に関連するデバイス上のすべての設定が廃棄されます。

- DHCP スヌーピング
- DHCP リレー
- DAI
- IPSG

DHCP スヌーピング設定を保持したまま、DHCP スヌーピング機能をオフにしたい場合には、**no ip dhcp snooping** コマンドを使用して、DHCP スヌーピングをグローバルにディセーブルにします。

DHCP スヌーピング機能がイネーブルのときには、Access Control List (ACL; アクセス コントロール リスト) の統計情報はサポートされません。

このコマンドには、ライセンスは必要ありません。

例

次の例では、DHCP スヌーピングをイネーブルにする方法を示します。

```
switch# configure terminal
switch(config)# feature dhcp
switch(config)#'
```

関連コマンド

コマンド	説明
clear ip dhcp snooping binding	DHCP スヌーピング バインディング データベースを消去します。
ip dhcp snooping	デバイスの DHCP スヌーピングをグローバルにイネーブルにします。
service dhcp	DHCP リレー エージェントをイネーブルまたはディセーブルにします。
show ip dhcp snooping	DHCP スヌーピングに関する一般的な情報を表示します。
show running-config dhcp	IP ソース ガード設定を含めて、DHCP スヌーピング設定を表示します。

feature dot1x

802.1X 機能をイネーブルにするには、**feature dot1x** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

feature dot1x

no feature dot1x

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンドモード

グローバル コンフィギュレーション

サポートされるユーザロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

802.1X を設定する前に、**feature dot1x** コマンドを使用する必要があります。



(注)

802.1X 機能をディセーブルにすると、すべての 802.1X 設定が失われます。802.1X 認証をディセーブルにする場合は、**no dot1x system-auth-control** コマンドを使用します。

このコマンドには、ライセンスは必要ありません。

例

次に、802.1X をイネーブルにする例を示します。

```
switch# configure terminal  
switch(config)# feature dot1x
```

次に、802.1X をディセーブルにする例を示します。

```
switch# configure terminal  
switch(config)# no feature dot1x
```

関連コマンド

コマンド	説明
show dot1x	802.1X のステータス情報を表示します。

feature eou

Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) をイネーブルにするには、**feature eou** コマンドを使用します。EAPoUDP をディセーブルにするには、このコマンドの **no** 形式を使用します。

feature eou

no feature eou

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンドモード

グローバル コンフィギュレーション

サポートされるユーザロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

EAPoUDP を設定する前に、**feature eou** コマンドを使用する必要があります。



(注)

EAPoUDP をディセーブルにすると、Cisco NX-OS ソフトウェアにより EXPoUDP 設定が削除されます。

このコマンドには、ライセンスは必要ありません。

例

次に、EAPoUDP をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature eou
```

次に、EAPoUDP をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no feature eou
```

関連コマンド

コマンド	説明
<code>feature eou</code>	EAPoUDP をイネーブルにします。
<code>show eou</code>	EAPoUDP 情報を表示します。

feature ldap

Lightweight Directory Access Protocol (LDAP) をイネーブルにするには、**feature ldap** コマンドを使用します。LDAP をディセーブルにするには、このコマンドの **no** 形式を使用します。

feature ldap

no feature ldap

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンドモード

グローバル コンフィギュレーション

サポートされるユーザロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

LDAP を設定する前に、**feature ldap** コマンドを使用する必要があります。



(注)

LDAP をディセーブルにすると、Cisco NX-OS ソフトウェアにより LDAP 設定が削除されます。

このコマンドには、ライセンスは必要ありません。

例

次に、LDAP をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature ldap
```

次に、LDAP をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no feature ldap
```

関連コマンド

コマンド	説明
<code>show running-config ldap</code>	実行コンフィギュレーションの LDAP 設定を表示します。
<code>show startup-config ldap</code>	スタートアップ コンフィギュレーションの LDAP 設定を表示します。

feature password encryption aes

高度暗号化規格（AES）パスワード暗号化機能をイネーブルにするには、**feature password encryption aes** コマンドを使用します。AES パスワード暗号化機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

feature password encryption aes

no feature password encryption aes

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンドモード

グローバル コンフィギュレーション モード (config)

サポートされるユーザロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.2(1)	このコマンドが追加されました。

使用上のガイドライン

マスター キーがなくとも AES パスワード暗号化機能をイネーブルにできますが、マスター キーがシステムに存在する場合だけ暗号化が開始されます。マスター キーを設定するには、**key config-key** コマンドを使用します。

このコマンドには、ライセンスは必要ありません。

例

次に、AES パスワード暗号化機能をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature password encryption aes
switch(config)#
```

次に AES パスワード暗号化機能をディセーブルにする例を示します。

```
switch(config)# no feature password encryption aes
switch(config)#
```

関連コマンド

コマンド	説明
key config-key	タイプ 6 暗号化用のマスター キーを設定します。
show encryption service stat	暗号化サービスのステータスを表示します。

feature port-security

ポートセキュリティ機能をグローバルでイネーブルにするには、**feature port-security** コマンドを使用します。ポートセキュリティ機能をグローバルでディセーブルにするには、このコマンドの **no** 形式を使用します。

feature port-security

no feature port-security

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンドモード

グローバル コンフィギュレーション

サポートされるユーザロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトの設定では、ポートセキュリティはグローバルでディセーブルです。

ポートセキュリティは、各 Virtual Device Context (VDC; 仮想デバイス コンテキスト) に対してローカルです。必要な場合、このコマンドを使用する前に正しい VDC に切り替えます。

このコマンドには、ライセンスは必要ありません。

ポートセキュリティのイネーブル化

ポートセキュリティをグローバルでイネーブルにすると、ポートセキュリティに関連する他のすべてのコマンドが使用可能になります。

ポートセキュリティを再イネーブル化する場合、ポートセキュリティが最後にイネーブルだった時点のポートセキュリティ設定は復元されません。

ポートセキュリティのディセーブル化

ポートセキュリティをグローバルでディセーブルにすると、すべてのポートセキュリティ設定が削除されます。デバイスがアドレスをどのように学習したかに関係なく、ポートセキュリティのすべてのインターフェイス設定、およびすべてのセキュア MAC アドレスが削除されます。

例

次に、ポートセキュリティをグローバルでイネーブルにする例を示します。

```
switch# configure terminal
```

```
switch(config)# feature port-security  
switch(config)#
```

関連コマンド

コマンド	説明
clear port-security	ダイナミックに学習されたセキュア MAC アドレスをクリアします。
debug port-security	ポートセキュリティのデバッグ情報を提供します。
show port-security	ポートセキュリティに関する情報を表示します。
switchport port-security	レイヤ 2 インターフェイス上のポートセキュリティをイネーブルにします。

feature privilege

TACACS+ サーバでコマンド認可にロールの累積権限をイネーブルにするには、**feature privilege** コマンドを使用します。ロールの累積権限をディセーブルにするには、このコマンドの **no** 形式を使用します。

feature privilege

no feature privilege

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンドモード

グローバル コンフィギュレーション

サポートされるユーザロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

feature privilege コマンドをイネーブルにすると、権限ロールは低いレベルの権限ロールの権限を継承します。

例

次に、ロールの累積権限をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature privilege
```

次に、ロールの累積権限をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no feature privilege
2010 Feb 12 12:52:06 switch %FEATURE-MGR-2-FM_AUTOCKPT_IN_PROGRESS: AutoCheckpoint
system-fm-privilege's creation in progress...
switch(config)# 2010 Feb 12 12:52:06 switch %FEATURE-MGR-2-FM_AUTOCKPT_SUCCEEDED
AutoCheckpoint created successfully
```


関連コマンド

コマンド	説明
enable <i>level</i>	上位の特権レベルへのユーザの昇格をイネーブルにします。
enable secret <i>priv-lvl</i>	特定の権限レベルのシークレット パスワードをイネーブルにします。
show privilege	現在の特権レベル、ユーザ名、および累積権限サポートのステータスを表示します。
username <i>username</i> <i>priv-lvl</i>	ユーザが認可に権限レベルを使用できるようにします。

feature scp-server

リモート デバイスとの間でファイルをコピーするために、Cisco NX-OS デバイスでセキュア コピー (SCP) サーバを設定するには、**feature scp-server** コマンドを使用します。SCP サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

feature scp-server

no feature scp-server

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.1(1)	このコマンドが追加されました。

使用上のガイドライン

SCP サーバをイネーブルにした後、Cisco NX-OS デバイスとの間でファイルをコピーするために、リモート デバイスで SCP コマンドを実行できます。

arcfour および blowfish cipher オプションは SCP サーバではサポートされません。

このコマンドには、ライセンスは必要ありません。

例

次に、Cisco NX-OS デバイスで SCP サーバをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature scp-server
switch(config)#
```

次に、Cisco NX-OS デバイスで SCP サーバをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no feature scp-server
switch(config)#
```

関連コマンド

コマンド	説明
<code>feature sftp-server</code>	Cisco NX-OS デバイスで SFTP サーバをイネーブルにします。

feature sftp-server

リモート デバイスとの間でファイルをコピーするために、Cisco NX-OS デバイスで FTP (SFTP) サーバを設定するには、**feature sftp-server** コマンドを使用します。SFTP サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

feature sftp-server

no feature sftp-server

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.1(1)	このコマンドが追加されました。

使用上のガイドライン

SFTP サーバをイネーブルにした後、Cisco NX-OS デバイスとの間でファイルをコピーするために、リモート デバイスで SFTP コマンドを実行できます。

このコマンドには、ライセンスは必要ありません。

例

次に、Cisco NX-OS デバイスで SFTP サーバをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature sftp-server
switch(config)#
```

次に、Cisco NX-OS デバイスで SFTP サーバをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no feature sftp-server
switch(config)#
```

関連コマンド

コマンド	説明
<code>feature scp-server</code>	Cisco NX-OS デバイスで SCP サーバをイネーブルにします。

feature ssh

仮想デバイス コンテキスト (VDC) の Secure Shell (SSH; セキュア シェル) サーバをイネーブルにするには、**feature ssh** コマンドを使用します。SSH サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

feature ssh

no feature ssh

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

イネーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.1(2)	このコマンドは、 ssh server enable コマンドを置き換える目的で導入されました。

使用上のガイドライン

Cisco NX-OS ソフトウェアは、SSH バージョン 2 をサポートしています。
このコマンドには、ライセンスは必要ありません。

例

次に、SSH サーバをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature ssh
```

次に、SSH サーバをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
```

関連コマンド

コマンド	説明
show feature	機能のイネーブル ステータスを表示します。
show ssh server	SSH サーバ キーの情報を表示します。

feature tacacs+

TACACS+ をイネーブルにするには、**feature tacacs+** コマンドを使用します。TACACS+ をディセーブルにするには、このコマンドの **no** 形式を使用します。

feature tacacs+

no feature tacacs+

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンドモード

グローバル コンフィギュレーション

サポートされるユーザロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。



(注)

TACACS+ をディセーブルにすると、Cisco NX-OS ソフトウェアにより TACACS+ 設定が削除されます。

このコマンドには、ライセンスは必要ありません。

例

次に、TACACS+ をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature tacacs+
```

次に、TACACS+ をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no feature tacacs+
```

関連コマンド

コマンド	説明
show tacacs+	TACACS+ 情報を表示します。

feature telnet

仮想デバイス コンテキスト (VDC) の Telnet サーバをイネーブルにするには、**feature telnet** コマンドを使用します。Telnet サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

feature telnet

no feature telnet

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンドモード

グローバル コンフィギュレーション

サポートされるユーザロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.1(2)	このコマンドは、 telnet server enable コマンドを置き換える目的で導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、Telnet サーバをイネーブルにする例を示します。

```
switch# configure terminal  
switch(config)# feature telnet
```

次に、Telnet サーバをディセーブルにする例を示します。

```
switch# configure terminal  
switch(config)# no feature telnet  
XML interface to system may become unavailable since ssh is disabled
```

関連コマンド

コマンド	説明
show feature	機能のイネーブル ステータスを表示します。
show telnet server	SSH サーバ キーの情報を表示します。

filter

フィルタ マップ内に 1 つ以上の証明書マッピング フィルタを設定するには、**filter** コマンドを使用します。

filter [**subject-name** *subject-name* | **altname-email** *e-mail-ID* | **altname-upn** *user-principal-name*]

構文の説明

subject-name	(任意) 証明書のサブジェクト名を指定します。
<i>subject-name</i>	LDAP 識別名 (DN) ストリング フォーマットでの必要なサブジェクト名。次に例を示します。 cn=%username%,ou=PKI,o=Acme,c=US
altname-email	(任意) 代替名としてメール ID を指定します。
<i>e-mail-ID</i>	サブジェクト代替名として証明書に存在する必要があるメールアドレス。次に例を示します。 %username%@*
altname-upn	(任意) 代替名としてユーザ プリンシパル名を指定します。
<i>user-principal-name</i>	サブジェクト代替名として証明書に存在する必要があるプリンシパル名。次に例を示します。 %username-without-domain%@%hostname%

デフォルト

なし

コマンド モード

証明書マッピング フィルタ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、新しいフィルタ マップを作成する必要があります。
証明書は、マップで設定されたすべてのフィルタを通過した場合に検証にパスします。
このコマンドには、ライセンスは必要ありません。

例

次に、フィルタ マップ内に証明書マッピング フィルタを設定する例を示します。

```
switch# configure terminal
switch(config)# crypto certificatemap mapname filtermap1
switch(config-certmap-filter)# filter altname-email jsmith@acme.com
```

関連コマンド

コマンド	説明
crypto certificatemap mapname	フィルタ マップを作成します。
show crypto certificatemap	証明書マッピングのフィルタを表示します。

fips mode enable

連邦情報処理標準（FIPS）モードをイネーブルにするには、**fips mode enable** コマンドを使用します。FIPS モードをディセーブルにするには、このコマンドの **no** 形式を使用します。

fips mode enable

no fips mode enable

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンドモード

グローバル コンフィギュレーション (config)

サポートされるユーザロール

network-admin
network-operator

コマンド履歴

リリース	変更箇所
5.1(1)	このコマンドが追加されました。

使用上のガイドライン

FIPS モードをイネーブルにする前に、デフォルトの仮想デバイス コンテキスト（VDC）を使用していることを確認します。

FIPS には、次の前提条件があります。

- Telnet をディセーブルにします。ユーザのログインはセキュア シェル（SSH）だけで行ってください。
- SNMP v1 および v2 をディセーブルにしてください。SNMP v3 に対して設定された、デバイス上の既存ユーザ アカウントのいずれについても、認証およびプライバシー用 AES/3DES は SHA で設定されていなければなりません。
- SSH サーバの RSA1 キー ペアすべてを削除してください。
- Cisco TrustSec Security Association Protocol（SAP）ネゴシエーション中に使用する HMAC-SHA1 メッセージ整合性チェック（MIC）をイネーブルにします。そのためには、cts-manual または cts-dot1x モードで **sap hash-algorithm HMAC-SHA-1** コマンドを入力します。

このコマンドには、ライセンスは必要ありません。

例

次の例では、FIPS モードをイネーブルにする方法を示します。

```
switch# configure t  
switch(config)# fips mode enable  
FIPS mode is enabled
```

次に、FIPS モードをディセーブルにする例を示します。

```
switch# configure t  
switch(config)# no fips mode enable  
FIPS mode is disabled
```

関連コマンド

コマンド	説明
show fips status	連邦情報処理標準 (FIPS) モードのステータスを表示します。

fragments

ACL で明示的な **permit** コマンドまたは **deny** コマンドに一致しない非初期フラグメントを、IPv4 ACL または IPv6 ACL で許可するか拒否するかについて最適化するには、**fragments** コマンドを使用します。フラグメントの最適化をディセーブルにするには、このコマンドの **no** 形式を使用します。

fragments {**deny-all** | **permit-all**}

no fragments {**deny-all** | **permit-all**}

構文の説明

deny-all	ACL で一致するフローの非初期フラグメントが、常に破棄されるように指定します。
permit-all	フローの初期フラグメントが ACL で許可されたときに、フローの非初期フラグメントが許可されるように指定します。

デフォルト

なし

コマンドモード

IPv4 ACL コンフィギュレーション
IPv6 ACL コンフィギュレーション

サポートされるユーザロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.2(1)	このコマンドが追加されました。

使用上のガイドライン

ACL で明示的な **permit** コマンドまたは **deny** コマンドに一致しない非初期フラグメントを許可または拒否する場合、**fragments** コマンドを使用すると、IP ACL の設定を簡素化できます。**fragments** キーワードを指定した、数多くの **permit** コマンドまたは **deny** コマンドを使用して非初期フラグメントの処理を制御する代わりに、**fragments** コマンドを使用できます。

デバイスで、**fragments** コマンドが含まれる ACL がトラフィックに適用される場合、このコマンドは、ACL での明示的な **permit** コマンドまたは **deny** コマンドに一致しない非初期フラグメントだけに一致します。

このコマンドには、ライセンスは必要ありません。

例

次に、lab-acl という名前の IPv4 ACL で、フラグメントの最適化をイネーブルにする例を示します。**permit-all** キーワードは、**fragments** キーワードが含まれる **deny** コマンドに一致しないすべての非初期フラグメントを ACL で許可することを意味します。

```
switch# configure terminal
switch(config)# ip access-list lab-acl
switch(config-acl)# fragments permit-all
```

次の例では、**fragments** コマンドが含まれる lab-acl IPv4 ACL を表示する方法を示します。便宜上、**fragments** コマンドは ACL の最初に表示されます。ただし、非初期フラグメントがデバイスで許可されるのは、ACL で非初期フラグメントが他のすべての明示的なルールに一致しなくなったあとだけです。

```
switch(config-acl)# show ip access-lists lab-acl
```

```
IP access list lab-acl
  fragments permit-all
  10 permit tcp 10.0.0.0/8 172.28.254.254/24 eq tacacs
  20 permit tcp 10.0.0.0/8 172.28.254.154/24 eq tacacs
  30 permit tcp 10.0.0.0/8 172.28.254.54/24 eq tacacs
```

関連コマンド

コマンド	説明
deny (IPv4)	IPv4 ACL に拒否 (deny) ルールを設定します。
deny (IPv6)	IPv6 ACL に拒否 (deny) ルールを設定します。
permit (IPv4)	IPv4 ACL に許可 (permit) ルールを設定します。
permit (IPv6)	IPv6 ACL に許可 (permit) ルールを設定します。
show ip access-list	すべての IPv4 ACL または特定の IPv4 ACL を表示します。
show ipv6 access-list	すべての IPv6 ACL または特定の IPv6 ACL を表示します。

