IPv6 ファイアウォールの FTP66 ALG サポート

IPv6 ファイアウォールの FTP66 ALG サポート機能を使用すると、FTP は IPv6 ファイアウォールとともに機能することができます。 このモジュールでは、ファイアウォール、ネットワーク アドレス変換（NAT）、およびステートフル NAT64 が、FTP66 アプリケーション レベル ゲートウェイ（ALG）とともに機能するように設定する方法について説明します。

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。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある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。

IPv6 ファイアウォールの FTP66 ALG サポートの制約事項

FTP66 ALG は次をサポートしていません。

- ボックスツーボックス ハイ アベイラビリティ。
- 加入者単位のファイアウォール。
- ステートレス ネットワーク アドレス変換 64（NAT64）。
- ステートフル NAT64 が設定されている場合の仮想ルーティングおよび転送（VRF）。
- 仮想 TCP（vTCP）、または変換後の小さいパケットへのパケット分割。

IPv6 ファイアウォールの FTP66 ALG サポートについて

アプリケーション レベル ゲートウェイ

アプリケーション レベル ゲートウェイ（ALG）は、アプリケーション層ゲートウェイとも呼ばれ、アプリケーション パケットのペイロード内の IP アドレス情報を変換するアプリケーションです。 ALG は、アプリケーション層プロトコルを解釈し、ファイアウォールおよびネットワーク アドレス変換（NAT）アクションを実行するために使用されます。 これらのアクションは、ファイアウォールおよび NAT の設定に応じて次の 1 つまたは複数のアクションになります。

- クライアント アプリケーションが、ダイナミック TCP または UDP ポートを使用してサーバ アプリケーションと通信できるようにします。
- アプリケーション固有のコマンドを認識し、それらに対するきめ細かいセキュリティ制御を提供します。
- データ交換を行う 2 台のホスト間のデータの複数のストリームまたはセッションを同期します。
- アプリケーション ペイロードで使用できるネットワーク層アドレス情報を変換します。

ファイアウォールはピンホールを開き、NAT は、アプリケーション層データ ストリームの送信元および宛先 IP アドレスを伝送しない TCP または UDP トラフィックに対する変換サービスを実行します。 IP アドレス情報を埋め込む特定のプロトコルまたはアプリケーションには ALG のサポートが必要です。

FTP66 ALG サポートの概要

ファイアウォールは、IPv6 パケットおよびステートフル ネットワーク アドレス変換 64（NAT64）のインスペクションをサポートします。 IPv6 パケット インスペクションにおいて FTP が機能するには、アプリケーション層ゲートウェイ（ALG）（アプリケーション レベル ゲートウェイ（ALG）とも呼ばれます）、FTP66 が必要となります。 FTP66 ALG は、オールインワン FTP ALG および 1 つの FTP ALG とも呼ばれます。

FTP66 ALG は次のことをサポートします。

- ファイアウォール IPv4 パケット インスペクション

- ファイアウォール IPv6 パケット インスペクション
- NAT 設定
- NAT64 設定（FTP64 サポートとともに）
- NAT およびファイアウォール設定
- NAT64 およびファイアウォール設定

FTP66 ALG には次のセキュリティ脆弱性があります。

- パケットセグメンテーション攻撃：FTP ALG ステートマシンは、セグメント化されたパケットを検出でき、ステート マシンの処理は、完全なパケットを受信するまで停止します。
- バウンス攻撃：FTP ALG は、1024 より少ないデータ ポート番号を使用して（NAT 用の）ドアまたは（ファイアウォール用の）ピンホールを作成しません。 バウンス攻撃の防止は、ファイアウォールがイネーブルな場合にのみアクティブです。

FTP66 ALG でサポートされる FTP コマンド

FTP66 アプリケーション レベル ゲートウェイ（ALG）は、RFC 959 に基づいています。 ここでは、FTP66 ALG が処理する主要な RFC 959 と RFC 2428 の FTP コマンドおよび応答について説明します。

PORT コマンド

PORT コマンドは、アクティブ FTP モードで使用されます。 PORT コマンドでは、サーバが接続するアドレスとポート番号を指定します。 このコマンドを使用する場合、引数は、32 ビットのインターネット ホスト アドレスと 16 ビットの TCP ポートのアドレスを連結したものになります。 アドレス情報は 8 ビットのフィールドに分割され、各フィールドの値は 10 進数（文字列表記）として送信されます。 フィールドは、カンマで区切られます。

次に、*h1* がインターネット ホスト アドレスの最上位の 8 ビットである PORT コマンドの例を示します。

```
PORT h1,h2,h3,h4,p1,p2
```

PASV コマンド

PASV コマンドは、TRANSFER コマンドを受信した場合、サーバのデフォルト データ ポートではないデータ ポートをリッスンし、別の接続を開始するのではなく、接続を待機するようサーバに要求します。 PASV コマンドに対する応答には、サーバがリッスンするホストとポート アドレスが含まれます。

拡張 FTP コマンド

拡張 FTP コマンドは、FTP が IPv4 以外のネットワーク プロトコルのデータ接続エンドポイント情報をやり取りできる方法を提供します。 拡張FTP コマンドは、RFC 2428 で規定されています。 RFC 2428 では、拡張 FTP コマンドの EPRT および EPSV は、FTP コマンドの PORT および PASV をそれぞれ置き換えます。

EPRT コマンド

EPRT コマンドを使用すると、データ接続に拡張アドレスを指定できます。 拡張アドレスは、ネットワーク プロトコル、ネットワーク アドレス、および転送アドレスで構成されている必要があります。 EPRT のコマンドの形式は次のとおりです。

```
EPRT<space><d><net-prt><d><net-addr><d><tcp-port><d>
```

- <net-prt> 引数は、アドレス ファミリ番号である必要があり、次の表で説明するように定義される必要があります。

表 *1*：*<net-prt>* 引数の定義

アドレス ファミリ番号	プロトコル
1	IPv4（Pos81a）
2	IPv6（DH96）

- <net-addr> 引数は、ネットワーク アドレスのプロトコル固有文字列表記です。 上記の表で指定された 2 つのアドレス ファミリ番号（アドレス ファミリ番号 1 と 2）の場合、次の表に示すアドレス形式である必要があります。

アドレス ファミリ番号	アドレス フォーマット	例
1	ドット付き 10 進数	10.135.1.2
2	DH96 で定義された IPv6 文字列表記	2001:DB8:1::1

- <tcp-port> 引数は、ホストがデータ接続をリッスンする TCP ポートの番号の文字列表記である必要があります。
- 次のコマンドは、TCP ポート 6275 でホスト 10.235.1.2 へのデータ接続を開くために IPv4 アドレスを使用するようにサーバに指定する方法を示します。
  ```
  EPRT |1|10.235.1.2|6275|
  ```
- 次のコマンドは、ポート 5282 で TCP データ接続を開くために IPv6 ネットワーク プロトコルおよびネットワーク アドレスを使用するようにサーバに指定する方法を示します。
  ```
  EPRT |2|2001:DB8:2::2:417A|5282|
  ```
- <d> 引数は、デリミタ文字であり、33 ～ 126 の範囲の ASCII 形式である必要があります。

EPSV コマンド

EPSV コマンドは、サーバがデータ ポートでリッスンし、接続を待機するよう要求します。 このコマンドへの応答には、接続をリッスンする TCP ポート番号のみが含まれます。 拡張アドレスを使用してパッシブ モードを開始するための応答コードは、229 である必要があります。

EPSV コマンドへの応答で返されるテキストは、次の形式である必要があります。
`(<d><d><d><tcp-port><d>)`

- カッコで囲まれた文字列の一部は、データ接続を開くために EPRT コマンドで必要とされる正確な文字列である必要があります。

  カッコ内の最初の 2 つのフィールドは空白である必要があります。 3 番目のフィールドは、サーバがデータ接続のためにリッスンする TCP ポート番号の文字列表記である必要があります。 データ接続で使用されるネットワーク プロトコルは、制御接続で使用されるのと同じネットワーク プロトコルです。 データ接続を確立するために使用されるネットワーク アドレスは、制御接続で使用されるのと同じネットワーク アドレスです。

- 次に、応答文字列の例を示します。
  ```
  Entering Extended Passive Mode (|||6446|)
  ```

次の FTP 応答とコマンドも FTP66 ALG によって処理されます。 これらのコマンドの処理結果は、ステート マシンの状態遷移を駆動するために使用されます。

- 230 応答
- AUTH
- USER
- PASS

IPv6 ファイアウォールの FTP66 ALG サポートの設定方法

FTP66 ALG サポート用ファイアウォールの設定

match protocol ftp コマンドを使用して、FTP66 ALG を明示的にイネーブルにする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-any** *class-map-name*
4. **match protocol** *protocol-name*
5. **exit**
6. **policy-map type inspect** *policy-map-name*
7. **class type inspect** *class-map-name*
8. **inspect**
9. **exit**
10. **class class-default**
11. **exit**
12. **exit**
13. **zone security** *zone-name*
14. **exit**
15. **zone-pair security** *zone-pair* **source** *source-zone* **destination** *destination-zone*
16. **service-policy type inspect** *policy-map-name*
17. **exit**
18. **interface** *type number*
19. **no ip address**
20. **ip virtual-reassembly**
21. **zone-member security** *zone-name*
22. **negotiation auto**
23. **ipv6 address** *ipv6-address*/*prefix-length*
24. **cdp enable**
25. **exit**
26. **ipv6 route** *ipv6-prefix*/*prefix-length interface-type interface-number*
27. **ipv6 neighbor** *ipv6-address interface-type interface-number hardware-address*
28. **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	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# 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 3	**class-map type inspect match-any** *class-map-name* 例： `Device(config)# class-map type inspect match-any in2out-class`	検査タイプ クラス マップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 4	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol ftp`	指定されたプロトコルに基づくクラスマップの一致基準を設定します。
ステップ 5	**exit** 例： `Device(config-cmap)# exit`	QoS クラスマップ コンフィギュレーション モードを終了し、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 6	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect in-to-out`	検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 7	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect in2out-class`	アクションを実行するクラスを指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 8	**inspect** 例： `Device(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 9	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、QoS ポリシーマップ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 10	**class class-default** 例： `Device(config-pmap)# class class-default`	ポリシー マップ設定を定義済みのデフォルト クラスに適用して、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。 • 設定済みクラス マップの一致基準のいずれともトラフィックが一致しない場合、事前に定義されたデフォルト クラスに誘導されます。
ステップ 11	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 12	**exit** 例： `Device(config-pmap)# exit`	QoS ポリシーマップ コンフィギュレーション モードを終了し、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 13	**zone security** *zone-name* 例： `Device(config)# zone security inside`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • 設定には、ゾーン ペアを作成するために、2 つのセキュリティ ゾーン（送信元ゾーンと宛先ゾーン）が含まれている必要があります。 • ゾーン ペアでは、送信元ゾーンまたは宛先ゾーンとしてデフォルト ゾーンを使用できます。
ステップ 14	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、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 15	**zone-pair security** *zone-pair* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security in2out source inside destination outside`	セキュリティ ゾーンのペアを作成し、セキュリティ ゾーン ペア コンフィギュレーション モードを開始します。 • ポリシーを適用するには、ゾーン ペアを設定する必要があります。

	コマンドまたはアクション	目的
ステップ 16	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect in-to-out`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 • ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 17	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、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 18	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 19	**no ip address** 例： `Device(config-if)# no ip address`	IPアドレスを削除するか、IP処理をディセーブルにします。
ステップ 20	**ip virtual-reassembly** 例： `Device(config-if)# ip virtual-reassembly`	インターフェイスでの仮想フラグメンテーション再構成（VFR）をイネーブルにします。
ステップ 21	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security inside`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 • インターフェイスをセキュリティ ゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（デバイス宛のトラフィックまたはデバイス発信のトラフィックを除く）は、デフォルトでドロップされます。 トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。 ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 22	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビット イーサネット インターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーション プロトコルで設定できるようにします。

	コマンドまたはアクション	目的
ステップ 23	**ipv6 address** *ipv6-address/prefix-length* 例： `Device(config-if)# ipv6 address 2001:DB8:1::1/96`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 24	**cdp enable** 例： `Device(config-if)# cdp enable`	インターフェイス上で Cisco Discovery Protocol をイネーブルにします。
ステップ 25	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 26	**ipv6 route** *ipv6-prefix/prefix-length interface-type interface-number* 例： `Device(config)# ipv6 route 2001::/96 gigabitethernet 0/0/1`	スタティック IPv6 ルートを確立します。
ステップ 27	**ipv6 neighbor** *ipv6-address interface-type interface-number hardware-address* 例： `Device(config)# ipv6 neighbor 2001:DB8:1::1 gigabitethernet 0/0/1 0000.29f1.4841`	IPv6 ネイバー探索キャッシュのスタティック エントリを設定します。
ステップ 28	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

FTP66 ALG サポート用 NAT の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **ip nat inside**
6. **zone-member security** *zone-name*
7. **exit**
8. **interface** *type number*
9. **ip address** *ip-address mask*
10. **ip nat outside**
11. **zone-member security** *zone-name*
12. **exit**
13. **ip nat inside source static** *local-ip global-ip*
14. **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	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/2`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 10.1.1.1 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 5	**ip nat inside** 例： `Device(config-if)# ip nat inside`	インターフェイスが内部ネットワーク（NAT 変換の対象になるネットワーク）に接続されていることを示します。
ステップ 6	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security inside`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 • インターフェイスをセキュリティ ゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（デバイス宛のトラフィックまたはデバイス発信のトラフィックを除く）は、デフォルトでドロップされます。 トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。 ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 7	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 8	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 10.2.1.1 255.255.255.0`	インターフェイスが内部ネットワーク（NAT 変換の対象になるネットワーク）に接続されていることを示します。
ステップ 10	**ip nat outside** 例： `Device(config-if)# ip nat outside`	インターフェイスが外部ネットワークに接続されていることを示します。
ステップ 11	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security outside`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 • インターフェイスをセキュリティ ゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（デバイス宛のトラフィックまたはデバイス発信のトラフィックを除く）は、デフォルトでドロップされます。 トラフィックがインターフェイス通過するに

	コマンドまたはアクション	目的
		は、ゾーンをポリシーの適用先のゾーンペアの一部にする必要があります。ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 12	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 13	**ip nat inside source static** *local-ip global-ip* 例： `Device(config)# ip nat inside source static 10.1.1.10 10.1.1.80`	内部送信元アドレスの NAT をイネーブルにします。
ステップ 14	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

FTP66 ALG サポート用 NAT64 の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **interface** *type number*
5. **no ip address**
6. **ipv6 virtual-reassembly**
7. **zone-member security** *zone-name*
8. **negotiation auto**
9. **ipv6 address** *ipv6-address*
10. **ipv6 enable**
11. **nat64 enable**
12. **cdp enable**
13. **exit**
14. **interface** *type number*
15. **ip address** *type number*
16. **ip virtual-reassembly**
17. **zone member security** *zone-name*
18. **negotiation auto**
19. **nat64 enable**
20. **exit**
21. **ipv6 route** *ipv6-address interface-type interface-number*
22. **ipv6 neighbor** *ipv6-address interface-type interface-number hardware-address*
23. **nat64 v6v4 static** *ipv6-address ipv4-address*
24. **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	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。
ステップ 4	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**no ip address** 例： `Device(config-if)# no ip address`	IP アドレスを削除するか、IP 処理をディセーブルにします。
ステップ 6	**ipv6 virtual-reassembly** 例： `Device(config-if)# ipv6 virtual-reassembly`	インターフェイスでの仮想フラグメンテーション再構成（VFR）をイネーブルにします。
ステップ 7	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security inside`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 • インターフェイスをセキュリティ ゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（デバイス宛のトラフィックまたはデバイス発信のトラフィックを除く）は、デフォルトでドロップされます。トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。 ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 8	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビット イーサネット インターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーション プロトコルで設定できるようにします。
ステップ 9	**ipv6 address** *ipv6-address* 例： `Device(config-if)# ipv6 address 2001:DB8:1::2/96`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 10	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	明示的な IPv6 アドレスが設定されていないインターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 11	**nat64 enable** 例： `Device(config-if)# nat64 enable`	インターフェイスで NAT64 をイネーブルにします。
ステップ 12	**cdp enable** 例： `Device(config-if)# cdp enable`	インターフェイス上で Cisco Discovery Protocol をイネーブルにします。
ステップ 13	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 14	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 15	**ip address** *type number* 例： `Device(config-if)# ip address 209.165.201.25 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 16	**ip virtual-reassembly** 例： `Device(config-if)# ip virtual-reassembly`	インターフェイス上で VFR をイネーブルにします。
ステップ 17	**zone member security** *zone-name* 例： `Device(config-if)# zone member security outside`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 • インターフェイスをセキュリティ ゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（ルータ宛のトラフィックまたはルータ発信のトラフィックを除く）は、デフォルトでドロップされます。 トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。 ポリシーがトラ

	コマンドまたはアクション	目的
		フィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 18	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビット イーサネット インターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーション プロトコルで設定できるようにします。
ステップ 19	**nat64 enable** 例： `Device(config-if)# nat64 enable`	インターフェイスで NAT64 をイネーブルにします。
ステップ 20	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 21	**ipv6 route** *ipv6-address interface-type interface-number* 例： `Device(config)# ipv6 route 2001:DB8:1::2/96 gigabitethernet 0/0/0`	スタティック IPv6 ルートを確立し、指定したネットワークに到達するために使用可能なネクスト ホップの IPv6 アドレスを指定します。
ステップ 22	**ipv6 neighbor** *ipv6-address interface-type interface-number hardware-address* 例： `Device(config)# ipv6 neighbor 2001:DB8:1::103 gigabitethernet 0/0/0 0000.29f1.4841`	IPv6 ネイバー探索キャッシュのスタティック エントリを設定します。
ステップ 23	**nat64 v6v4 static** *ipv6-address ipv4-address* 例： `Device(config)# nat64 v6v4 static 2001:DB8:1::103 209.165.201.32`	NAT64 の IPv6 送信元アドレスを IPv4 送信元アドレスに、および IPv4 宛先アドレスを IPv6 宛先アドレスに変換します。
ステップ 24	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

IPv6 ファイアウォールの FTP66 ALG サポートの設定例

例：FTP66 ALG サポート用 IPv6 ファイアウォールの設定

```
Device# configure terminal
Device(config)# class-map type inspect match-any in2out-class
Device(config-cmap)# match protocol ftp
Device(config-cmap)# exit
Device(config)# policy-map type inspect in-to-out
Device(config-pmap)# class type inspect in2out-class
Device(config-pmap-c)# inspect
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# zone security inside
Device(config-sec-zone)# exit
Device(config)# zone security outside
Device(config-sec-zone)# exit
Device(config)# zone-pair security in2out source inside destination outside
Device(config-sec-zone-pair)# service-policy type inspect in-to-out
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/0/1
Device(config-if)# no ip address
Device(config-if)# ip virtual-reassembly
Device(config-if)# zone-member security inside
Device(config-if)# negotiation auto
Device(config-if)# ipv6 address 2001:DB8:1::1/96
Device(config-if)# cdp enable
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/1/1
Device(config-if)# no ip address
Device(config-if)# ip virtual-reassembly
Device(config-if)# zone-member security outside
Device(config-if)# negotiation auto
Device(config-if)# ipv6 address 2001:DB8:2::2/96
Device(config-if)# exit
Device(config)# ipv6 route 2001::/96 gigabitethernet 0/0/1
Device(config)# ipv6 route 2001::/96 gigabitethernet 0/1/1
Device(config)# ipv6 neighbor 2001:DB8:1::1 gigabitethernet 0/0/1 0000.29f1.4841
Device(config)# ipv6 neighbor 2001:DB8:2::2 gigabitethernet 0/1/1 0000.29f1.4842
Device(config)# end
```

例：FTP66 ALG サポート用 NAT の設定

```
Device# configure terminal
Device(config)# interface gigabitethernet 0/1/2
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# ip nat inside
Device(config-if)# zone-member security inside
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/1/1
Device(config-if)# ip address 10.2.1.1 255.255.255.0
Device(config-if)# ip nat outside
Device(config-if)# zone-member security outside
Device(config-if)# exit
Device(config-if)# ip nat inside source static 10.1.1.10 10.1.1.80
```

例：FTP66 ALG サポート用 NAT64 の設定

```
Device# configure terminal
Device(config)# ipv6 unicast-routing
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# no ip address
Device(config-if)# ipv6 virtual-reassembly
Device(config-if)# zone-member security inside
Device(config-if)# negotiation auto
Device(config-if)# ipv6 address 2001:DB8:1::2/96
Device(config-if)# ipv6 enable
Device(config-if)# nat64 enable
Device(config-if)# cdp enable
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/1/1
Device(config-if)# ip address 209.165.201.25 255.255.255.0
Device(config-if)# ip virtual-reassembly
Device(config-if)# zone member security outside
Device(config-if)# negotiation auto
Device(config-if)# nat64 enable
Device(config-if)# exit
Device(config)# ipv6 route 2001:DB8:1::2/96 gigabitethernet 0/0/0
Device(config)# 2001:DB8:1::103 gigabitethernet 0/0/0 0000.29f1.4841
Device(config)# nat64 v6v4 static 2001:DB8:1::103 209.165.201.32
```

IPv6 ファイアウォールの FTP66 ALG サポートの追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』
NAT コマンド	『IP Addressing Command Reference』

標準および RFC

標準/RFC	タイトル
RFC 959	『*File Transfer Protocol*』
RFC 2428	『*FTP Extensions for IPv6 and NATs*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 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

IPv6 ファイアウォールの FTP66 ALG サポートの機能情報

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 2：*IPv6* ファイアウォールの *FTP66 ALG* サポートの機能情報

機能名	リリース	機能情報
IPv6 ファイアウォールの FTP66 ALG サポート	Cisco IOS XE Release 3.7S	IPv6 ファイアウォールの FTP66 ALG サポート機能を使用すると、FTP は IPv6 ファイアウォールとともに機能することができます。 このモジュールでは、ファイアウォール、ネットワークアドレス変換（NAT）、および NAT64 が、FTP66 アプリケーション レベル ゲートウェイ（ALG）とともに機能するように設定する方法について説明します。