IPv6 ファイアウォールに対する FTP66 ALG サポート

IPv6 ファイアウォールの FTP66 ALG サポート機能により、FTP を IPv6 ファイアウォールと連動させることができます。このモジュールでは、FTP66 アプリケーション レベル ゲートウェイ（ALG）と連動するようにファイアウォール、ネットワーク アドレス変換（NAT）、およびステートフル NAT64 を設定する方法を説明します。

- IPv6 ファイアウォールに対する FTP66 ALG サポートに関する制約事項 （1 ページ）
- IPv6 ファイアウォールに対する FTP66 ALG サポートに関する情報 （2 ページ）
- IPv6 ファイアウォールに対する FTP66 ALG サポートの設定方法 （5 ページ）
- IPv6 ファイアウォールに対する FTP66 ALG サポートの設定例 （15 ページ）
- IPv6 ファイアウォールに対する FTP66 ALG サポートに関する追加情報 （17 ページ）
- IPv6 ファイアウォールに対する FTP66 ALG サポートに関する機能情報 （18 ページ）

IPv6 ファイアウォールに対する FTP66 ALG サポートに関する制約事項

FTP66 ALG は以下をサポートしません。

- ボックスツーボックス ハイアベイラビリティ。
- サブスクライバ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 Virtual Routing and Forwarding（VRF）。
- 仮想 TCP（vTCP）または変換後の小パケットへのパケット分割。

IPv6 ファイアウォールに対する FTP66 ALG サポートに関する情報

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 レイヤ 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 レイヤ 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、これらのコマンド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 つのホスト間の複数のデータ ストリームまたはデータ 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。

ファイアウォールがピンホールを開き、アプリケーション レイヤ データストリームの送信元 IP アドレスおよび宛先 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 NAT が実行します。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

ファイアウォールでは、IPv6 パケットとステートフル 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ています。FTP を IPv6 パケット インスペクションに基づいて機能させるには、アプリケーション層ゲートウェイ（ALG）（別名アプリケーション レベル ゲートウェイ（ALG））FTP66 が必要です。FTP66 ALG は、オールインワン FTP ALG およびワン FTP ALG とも呼ばれています。

FTP66 ALG では、次の機能をサポートしています。

- 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 の設定
- NAT64 の設定（FTP64 サポートを使用）

- NAT とファイアウォールの設定
- NAT64 とファイアウォールの設定

FTP66 ALG には、次のセキュリティ上の脆弱性があります。

- パケット セグメンテーション攻撃：FTP ALG ステート マシンではセグメント化されたパケットを検出できます。完全なパケットを受信するまで、ステートマシンの処理は停止します。
- バウンス攻撃：FTP ALG は、番号が 1024 未満のデータ ポートでドア（NAT の場合）やピンホール（ファイアウォールの場合）を作成しません。バウンス攻撃の防止がアクティブになるのは、ファイアウォールが有効にされている場合のみです。

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。この項では、FTP66 ALG が処理する、RFC 959 および RFC 2428 の主要な FTP コマンドと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、サーバの接続先と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際の引数は、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 ポートアドレスを連結したものです。このアドレス情報は 8 ビットのフィールドに分割されて、各フィールドの値が 10 進数（文字列表現）として送信されます。フィールドはカンマで区切ります。

次に示す PORT コマンドの例では、*h1* がインターネット ホスト アドレスの最上位 8 ビットです。

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

PASV コマンド

PASV コマンドは、サーバに対し、TRANSFER コマンドの受信時に別の接続を開始するのではなく、サーバのデフォルト以外のデータ ポートでリッスンして接続を待機するよう要求します。PASV コマンドへの応答には、サーバがリッスンしているホストおよびポート アドレスが組み込まれます。

拡張 FTP コマンド

拡張 FTP コマンドは、FTP で 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伝える手段になります。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 と EPSV が FTP コマンドの PORT と PASV にそれぞれ置き換わっています。

EPRT コマンド

EPRTコマンドでは、データ接続の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、トランスポートアドレスで構成する必要があります。EPRT 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 ファミリ番号であり、次の表に示すように定義する必要があります。

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、プロトコル固有のネットワーク アドレスの文字列表現です。上記の表で指定されているアドレス ファミリ番号（アドレス ファミリ番号1と2）は、次の表に記載するアドレス形式にする必要があります。

アドレス ファミリ番号	アドレス形式	例
1	ドット付き 10 進法	10.135.1.2
2	DH96 で定義されている IPv6 文字列形式	2001:DB8:1::1

- <tcp-port> 引数は、ホストがデータ接続をリッスンしている TCP ポート番号の文字列形式にする必要があります。
- 次のコマンドは、サーバに対し、IPv4 アドレスを使用してホスト 10.235.1.2 へのデータ接続を TCP ポート 6275 で開くように指示する方法を示しています。

```
EPRT |1|10.235.1.2|6275|
```

- 次のコマンドは、サーバに対し、IPv6 ネットワーク プロトコルとネットワーク アドレスを使用して TCP データ接続をポート 5282 で開くように指示する方法を示しています。

```
EPRT |2|2001:DB8:2::2:417A|5282|
```

- <d> 引数は区切り文字です。この引数は、ASCII 形式の 33 から 126 までの範囲の値にする必要があります。

EPSV コマンド

EPSV コマンドでは、サーバに対し、データ ポートでリッスンして接続を待機するよう要求します。このコマンドの応答には、リッスンする接続の TCP ポート番号だけが組み込まれます。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 です。

EPSV コマンドに対して返されるテキストは、次の形式になります。

```
(<d><d><d><tcp-port><d>)
```

- カッコで囲まれた文字列の部分は、EPRT コマンドでデータ接続を開くために必要な文字列と正確に一致する必要があります。

  カッコ内の最初の2つのフィールドは空白でなければなりません。3番目のフィールドは、サーバがデータ接続をリッスンしている TCP ポート番号の文字列表現でなければなりません。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ネットワーク プロトコルと同じです。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、制御接続に使用されるネットワーク アドレスと同じです。

- 次に、応答文字列の例を示します。

  ```
  Entering Extended Passive Mode (|||6446|)
  ```

次の FTP 応答およびコマンドも、FTP66 ALG によって処理されます。これらのコマンドの実行結果は、ステート マシンの遷移を操作するために使用されます。

- 230 応答メッセージ
- AUTH
- USER
- PASS

IPv6 ファイアウォールに対する FTP66 ALG サポートの設定方法

FTP66 ALG サポート用の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 モードを有効にします。 • 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	**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いて、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。

	コマンドまたはアクション	目的
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対象のクラスを指定し、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。
ステップ 10	**class class-default** 例： `Device(config-pmap)# class class-default`	定義済みのデフォルト クラスにポリシー マップ設定を適用して、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 マップのどの一致基準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。 • ゾーン ペアを作成するには2つのセキュリティ ゾーン（送信元ゾーンと宛先ゾーン）が設定に含まれる必要があります。 • 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。

	コマンドまたはアクション	目的
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て、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。 • 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。
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、そのインターフェイスを通して送受信されるすべてのトラフィックは、デフォルトでドロップされます（ただしデバイス宛のトラフィックとデバイス発のトラフィックを除く）。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

	コマンドまたはアクション	目的
		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。
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 サポート用の 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 モードを有効にします。 • 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。
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 変換の対象となるネットワーク）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、そのインターフェイスを通して送受信されるすべてのトラフィックは、デフォルトでドロップされます（ただしデバイス宛のトラフィックとデバイス発のトラフィックを除く）。トラフィックがインターフェイス通

	コマンドまたはアクション	目的
		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 変換の対象となるネットワーク）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、そのインターフェイスを通して送受信されるすべてのトラフィックは、デフォルトでドロップされます（ただしデバイス宛のトラフィックとデバイス発のトラフィックを除く）。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 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。

	コマンドまたはアクション	目的
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 モードを有効にします。 • 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	**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有効にします。
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、そのインターフェイスを通して送受信されるすべてのトラフィックは、デフォルトでドロップされます（ただしデバイス宛のトラフィックとデバイス発のトラフィックを除く）。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。

	コマンドまたはアクション	目的
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への到達に使用できるネクスト 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 ファイアウォールに対する FTP66 ALG サポートの設定例

例：FTP66 ALG サポート用の 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 サポート用の 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 サポート用の 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 ファイアウォールに対する FTP66 ALG サポートに関する追加情報

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*』

標準/RFC	タイトル
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
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

IPv6 ファイアウォールに対する FTP66 ALG サポートに関する機能情報

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 *2 : IPv6* ファイアウォールに対する *FTP66 ALG* サポートに関する機能情報

機能名	リリース	機能情報
IPv6 ファイアウォールに対する FTP66 ALG サポート	Cisco IOS XE リリース 3.7S	IPv6 ファイアウォールの FTP66 ALG サポート機能により、FTP を IPv6 ファイアウォールと連動させることができます。このモジュールでは、FTP66 アプリケーション レベル ゲートウェイ（ALG）と連動するように、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 を設定する方法について説明します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。