ゾーンベース ポリシー ファイアウォール IPv6 サポート

ゾーンベース ポリシー ファイアウォールでは、IPv4 パケットの高度なトラフィック フィルタリングまたはインスペクションを提供します。 IPv6 サポートによって、ゾーンベース ポリシー ファイアウォールは、IPv6 パケットのインスペクションをサポートします。 IPv6 サポートの前は、ファイアウォールがサポートしているのは IPv4 パケット インスペクションだけでした。 レイヤ 4 プロトコル、インターネット制御メッセージ プロトコル（ICMP）、TCP、および UDP パケットだけが、IPv6 パケット インスペクションの対象となります。

このモジュールでは、サポートされるファイアウォール機能、および IPv6 パケット インスペクション用にファイアウォールを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。

ゾーンベース ポリシー ファイアウォール IPv6 サポートの制約事項

次の機能はサポートされていません。

- アプリケーション レベル ゲートウェイ（ALG）
- ボックスツーボックス ハイ アベイラビリティ（HA）
- 分散型サービス拒否攻撃
- ファイアウォール リソース管理
- レイヤ 7 インスペクション
- マルチキャスト パケット
- 加入者単位のファイアウォールまたはブロードバンド ベース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）
- VRF-Aware Software インフラストラクチャ（VASI）
- Wide Area Application Services（WAAS）と Web Cache Communication Protocol（WCCP）

VASI インターフェイス経由の IPv6 ゾーンベース ファイアウォール サポートについて

ファイアウォール機能の IPv6 サポート

次の表で説明するファイアウォール機能は、IPv6 パケット インスペクションでサポートされます。

表 *1*：*IPv6* でサポートされるファイアウォール機能

機能	設定情報
クラス マップ	「ゾーンベース ポリシー ファイアウォール」モジュール。

機能	設定情報
インターネット制御メッセージ プロトコル バージョン 6（ICMPv6）、TCP、および UDP プロトコル	• 「*ICMP* のファイアウォール ステートフル インスペクション」モジュール。 • 「ゾーンベース ポリシー ファイアウォール」モジュール。
IP フラグメンテーション	「仮想フラグメンテーション再構成」モジュール。
シャーシ内 HA	—
エラー メッセージのロギング	「ゾーンベース ポリシー ファイアウォール」モジュール。
ネストされたクラス マップ	「ゾーンベース ポリシー ファイアウォールのネストされたクラス マップ サポート」モジュール。
Out-of-Order パケット処理	「ゾーンベース ポリシー ファイアウォール」モジュールの「Out-of-Order パケット処理」の項。
パラメータ マップ：検査タイプ パラメータ マップの場合、パラメータ マップで定義されたセッション数は、IPv4 と IPv6 セッションで累積されます	「ゾーンベース ポリシー ファイアウォール」モジュール。
ポリシー マップ	「ゾーンベース ポリシー ファイアウォール」モジュール。
ポートツーアプリケーション マッピング	—
ステートフル ネットワーク アドレス変換 64（NAT64）	『*IP Addressing: NAT Configuration Guide*』の「*Stateful Network Address Translation 64*」モジュール。
TCP SYN Cookie	「ファイアウォール *TCP SYN Cookie* の設定」モジュール。
VPN ルーティングおよび転送（VRF）認識ファイアウォール	「*VRF-Aware Cisco IOS XE* ファイアウォール」モジュール。
仮想フラグメンテーション再構成（VFR）	「仮想フラグメンテーション再構成」モジュール。
ゾーン、デフォルト ゾーン、およびゾーン ペア	「ゾーンベース ポリシー ファイアウォール」モジュール。

デュアル スタック ファイアウォール

デュアル スタック ファイアウォールは、IPv4 および IPv6 トラフィックを同時に実行するファイアウォールです。 デュアル スタック ファイアウォールは、次のシナリオで設定できます。

- IPv4 トラフィックを実行する 1 つのファイアウォール ゾーン、および IPv6 トラフィックを実行する別のファイアウォール ゾーン。
- IPv4 と IPv6 は、ステートフル ネットワーク アドレス変換 64（NAT64）を使用して展開している場合に共存します。 このシナリオでは、トラフィックは IPv6 から IPv4 へ、およびその逆に流れます。
- 同じゾーン ペアは、IPv4 および IPv6 トラフィックの両方を許可します。

IPv6 ヘッダー フィールドのファイアウォール アクション

IPv6 ヘッダー フィールドのファイアウォール アクションについては、（IPv6 ヘッダーで使用可能な順に）次の表で説明します。

表 *2*：*IPv6* ヘッダー フィールド

IPv6 ヘッダー フィールド	IPv6 ヘッダー フィールドの説明	ファイアウォール アクション
バージョン	IPv4 パケット ヘッダーのバージョン フィールドと同様ですが、IPv4 を意味する数字 4 の代わりに IPv6 を意味する数字 6 が示されます。	IPv6 である必要があります。
トラフィック クラス	IPv4 パケット ヘッダーのタイプ オブ サービス（ToS）フィールドと同様です。 トラフィック クラス フィールドは、差別化されたサービスで使用されるトラフィック クラスのタグをパケットに付けます。	検査されません。
フロー ラベル	IPv6 パケット ヘッダーの新しいフィールドです。 フロー ラベル フィールドは、ネットワーク層でパケットを差別化する特定のフローのタグをパケットに付けます。	検査されません。

IPv6 ヘッダー フィールド	IPv6 ヘッダー フィールドの説明	ファイアウォール アクション
ペイロード長	IPv4 パケット ヘッダーの合計長フィールドと同様です。 ペイロード長フィールドは、パケットのデータ部分の合計長を示します。	ファイアウォールはこのフィールドを限定的に使用して、ICMP、TCP などのレイヤ 4 プロトコルの一部の長さを計算します。
次ヘッダー長	IPv4 パケット ヘッダーのプロトコル フィールドと同様です。 次ヘッダー長フィールドの値により、基本 IPv6 ヘッダーに続く情報のタイプが決まります。 基本 IPv6 ヘッダーに続く情報のタイプは、TCP パケット、UDP パケット、または拡張ヘッダーなどのトランスポート層パケットです。	ファイアウォールは、セッションを作成するためにこのフィールドを認識する必要があります。
ホップ リミット	IPv4 パケット ヘッダーの存続可能時間（TTL）フィールドと同様です。 ホップ リミット フィールドの値は、IPv6 パケットが無効と見なされる前に通過できるデバイスの最大数です。 各デバイスでは、ホップ リミット値は 1 ずつ減少します。 IPv6 ヘッダーにはチェックサムがないため、デバイスはチェックサムを計算し直すことなく、値を減少できます。	検査されません。

IPv6 ファイアウォール セッション

トラフィックのステートフル インスペクションを実行するために、ファイアウォールは各トラフィック フローの内部セッションを作成します。 セッション情報には、IP 送信元アドレスと宛先アドレス、UDP または TCP の送信元ポートと宛先ポートまたは ICMP タイプ、レイヤ 4 プロトコル タイプ（ICMP、TCP、または UDP）、および VPN ルーティングおよび転送（VRF）ID が含まれます。 IPv6 ファイアウォールでは、送信元アドレスと宛先アドレスには IPv6 アドレスの 128 ビットが含まれます。

ファイアウォールは、パケットが設定済みのポリシーと一致した場合、最初のパケットの受信後に TCP セッションを作成します。 ファイアウォールは、TCP シーケンス番号を追跡し、TCP パケットのシーケンス番号が設定された範囲内にない場合、その TCP パケットをドロップします。セッションが削除されるのは、TCP アイドル タイマーが期限切れになった場合、またはリセット（RST）や終了確認応答（FIN-ACK）パケットを適切なシーケンス番号で受信した場合です。

ファイアウォールは、設定されたポリシーに一致する最初のUDPパケットが到着したときにUDPセッションを作成し、UDP アイドル タイマーが期限切れになった場合にセッションを削除します。 ファイアウォールは、マルチキャスト IPv6 アドレスまたは未知の IPv6 アドレスが含まれた IPv6 パケットの TCP または UDP セッションを作成しません。

フラグメント化されたパケットのファイアウォールインスペクション

ファイアウォールは、フラグメント化された IPv6 パケットのインスペクションをサポートします。 IP フラグメンテーションは、単一の IP データグラムを小さなサイズの複数のパケットに分割するプロセスです。 IPv6 では、エンド ノードはパス最大伝送単位（MTU）探索を実行して、送信されるパケットの最大サイズを判別し、MTUサイズよりも大きいパケットについて、フラグメント拡張ヘッダーが含まれる IPv6 パケットを生成します。

ファイアウォールは、仮想フラグメンテーション再構成（VFR）を使用して、フラグメント化されたパケットを検査します。 VFRは、シーケンス外のフラグメントのフラグメント拡張ヘッダーを調べ、インスペクションのためにそれらを正しい順序に配置します。 インターフェイスをゾーンに追加してインターフェイス上のファイアウォールをイネーブルにすると、VFRは同じインターフェイス上で自動的に設定されます。 明示的にVFRをディセーブルにした場合、ファイアウォールはレイヤ 4 ヘッダーを持つ最初のフラグメントだけを検査し、残りのフラグメントは検査なしで渡します。

フラグメント拡張ヘッダーは、次のヘッダー順で表示されます。

- IPv6 ヘッダー
- ホップバイホップ オプション ヘッダー
- 宛先オプション ヘッダー
- ルーティング ヘッダー
- フラグメント拡張ヘッダー

シスコ エクスプレス フォワーディングは、フラグメント拡張ヘッダーが含まれた IPv6 パケットを検査することで、ファイアウォールがパケットを処理する前にさらに検査する必要がないようにします。

ICMPv6 メッセージ

IPv6 は ICMPv6 を使用して、診断機能、エラー レポーティング、およびネイバー探索を実行します。 ICMPv6 メッセージは、情報およびエラー メッセージにグループ化されます。

ファイアウォールは、次の ICMPv6 メッセージのみを検査します。

- ECHO REQUEST
- ECHO REPLY
- DESTINATION UNREACHABLE
- PACKET TOO BIG

- PARAMETER PROBLEM
- TIME EXCEEDED

（注） ネイバー探索パケットが渡され、ファイアウォールによって検査されません。

ステートフル NAT64 のファイアウォール サポート

ゾーンベース ポリシー ファイアウォールは、ステートフル NAT64 をサポートします。 ステートフル NAT64 は、IPv6 パケットを IPv4 パケットに変換したり、その逆に変換したりします。 ファイアウォールおよびステートフル NAT64 の両方がルータで設定されている場合、そのファイアウォールはアクセス コントロール リスト（ACL）内の IP アドレスを使用して、パケットをフィルタリングします。 ただし、ACL は IPv4 アドレスと IPv6 アドレスの混在をサポートしません。ファイアウォールとステートフル NAT64 が連携して動作するには、IPv6 ACL を使用する必要があり、IPv4 アドレスは IPv6 ACL に組み込まれている必要があります。

（注） ステートフル NAT64 は VRF を認識しないため、VRF をファイアウォールおよびステートフル NAT64 設定とともに使用することはできません。

ファイアウォール クラス マップが ACL を使用する場合、ACL はホスト上で実際の IP アドレスを使用して、パケットフローを設定する必要があります。 送信元または宛先アドレスだけが必要な場合は、IPv4 アドレスまたは IPv6 アドレスがクラス マップ ACL で使用されます。 パケット フローが送信元アドレスと宛先アドレスの両方に基づいてフィルタリングできるようにするには、IPv6 アドレスが使用され、IPv4 アドレスが ACL に組み込まれている必要があります。 ACL は、IPv6 アドレスを使用して、ステートフル NAT64 パケットをフィルタリングする必要があります。

（注） ファイアウォールでのステートレス NAT64 はサポートされません。

ポートツーアプリケーション マッピング

ポートツーアプリケーション マッピング（PAM）を使用して、ネットワーク サービスやアプリケーション用の TCP または UDP ポート番号をカスタマイズできます。 ファイアウォールは PAM を使用して、TCP または UDP ポート番号を特定のネットワーク サービスやアプリケーションに関連付けます。 ポート番号をネットワーク サービスやアプリケーションにマッピングすることで、管理者は既知のポートを使用して定義されていないカスタム設定に対してファイアウォール インスペクションを強制適用できます。 **ip port-map** コマンドを使用して、PAM を設定します。

ハイ アベイラビリティおよび ISSU

IPv6 ファイアウォールはボックス内 HA をサポートします。 ファイアウォール セッションは、スイッチオーバーのためにスタンバイ組み込みサービス プロセッサ（ESP）に同期されます。 IPv6 ファイアウォールでは In Service Software Upgrade（ISSU）もサポートされます。

トラフィック クラスの pass アクション

ファイアウォールでは、トラフィック クラスはパケットの内容に基づいてパケットセットを識別します。 クラスを定義し、ポリシーを反映するアクションを識別されたトラフィックに適用できます。 アクションとは、トラフィック クラスに関連付けられる、特定の機能のことです。 クラスの inspect アクション、drop アクション、および pass アクションを設定できます。

pass アクションは、あるゾーンから別のゾーンにトラフィックを渡します。 pass アクションが設定されている場合、ファイアウォールはトラフィックを検査しません。つまり、トラフィックを渡します。IPv6 ファイアウォールでは、ゾーンペアおよび pass アクションに関するポリシーマップを定義して、リターン トラフィックの pass アクションを明示的に設定する必要があります。

次に、ポリシー マップの pass アクション、外部から内部へのポリシーと内部から外部へのポリシーを IPv6 トラフィックに設定する例を示します。

```
policy-map type inspect outside-to-inside-policy
 class type inspect ipv6-class
  pass (Defines pass action for the ipv6-class from the outside to the inside)
!
 class class-default
!
policy-map type inspect inside-to-outside-policy
 class type inspect ipv4-class
  inspect (Defines inspect action for ipv4-class)
 class type inspect v6_class
  pass (Defines pass action for ipv6-class from the inside to the outside)
 class class-default
!
!
zone security inside
!
zone security outside
!
zone-pair security in-out source inside destination outside
 service-policy type inspect inside-to-outside-policy
!
zone-pair security out-in source outside destination inside
 service-policy type inspect outside-to-inside-policy
```

ゾーンベース ポリシー ファイアウォール IPv6 サポートの設定方法

IPv6 ファイアウォールの設定

IPv4 ファイアウォールと IPv6 ファイアウォールを設定する手順は同じです。 IPv6 ファイアウォールを設定するには、IPv6 アドレスファミリだけが一致するようにクラスマップを設定する必要があります。

match protocol コマンドは、IPv4 トラフィックと IPv6 トラフィックの両方に適用され、IPv4 ポリシーまたは IPv6 ポリシーに含めることができます。

手順の概要

1. **enable**
2. **configure terminal**
3. **vrf-definition** *vrf-name*
4. **address-family ipv6**
5. **exit-address-family**
6. **exit**
7. **parameter-map type inspect** *parameter-map-name*
8. **sessions maximum** *sessions*
9. **exit**
10. **ipv6 unicast-routing**
11. **ip port-map** *appl-name* **port** *port-num* **list** *list-name*
12. **ipv6 access-list** *access-list-name*
13. **permit ipv6 any any**
14. **exit**
15. **class-map type inspect match-all** *class-map-name*
16. **match access-group name** *access-group-name*
17. **match protocol** *protocol-name*
18. **exit**
19. **policy-map type inspect** *policy-map-name*
20. **class type inspect** *class-map-name*
21. **inspect** [*parameter-map-name*]
22. **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 モードを開始します。 • 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	**vrf-definition** *vrf-name* 例： `Device(config)# vrf-definition VRF1`	仮想ルーティングおよび転送（VRF）ルーティング テーブル インスタンスを設定し、VRF 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	**address-family ipv6** 例： `Device(config-vrf)# address-family ipv6`	VRF アドレス ファミリ コンフィギュレーション モードを開始して、標準IPv6アドレスプレフィックスを伝送するセッションを設定します。
ステップ 5	**exit-address-family** 例： `Device(config-vrf-af)# exit-address-family`	VRF アドレス ファミリ コンフィギュレーション モードを終了し、VRF 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	**exit** 例： `Device(config-vrf)# exit`	VRF コンフィギュレーション モードを終了して、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 7	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect ipv6-param-map`	ファイアウォールのグローバル検査タイプ パラメータ マップを、検査アクションに関連するしきい値、タイムアウト、およびその他のパラメータに関連付けることができるようにし、パラメータ マップ タイプ検査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	**sessions maximum** *sessions* 例： `Device(config-profile)# sessions maximum 10000`	ゾーン ペア上に存在可能な最大許容セッション数を設定します。

	コマンドまたはアクション	目的
ステップ 9	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査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 10	**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 11	**ip port-map** *appl-name* **port** *port-num* **list** *list-name* 例： `Device(config)# ip port-map ftp port 8090 list ipv6-acl`	IPv6 アクセス コントロール リスト（ACL）を使用してポートツーアプリケーション マッピング（PAM）を確立します。
ステップ 12	**ipv6 access-list** *access-list-name* 例： `Device(config)# ipv6 access-list ipv6-acl`	IPv6 アクセス リストを定義し、IPv6 アクセス リスト 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	**permit ipv6 any any** 例： `Device(config-ipv6-acl)# permit ipv6 any any`	IPv6 アクセス リストに許可条件を設定します。
ステップ 14	**exit** 例： `Device(config-ipv6-acl)# exit`	IPv6 アクセス リスト 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	**class-map type inspect match-all** *class-map-name* 例： `Device(config)# class-map type inspect match-all ipv6-class`	アプリケーション固有検査タイプ 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 16	**match access-group name** *access-group-name* 例： `Device(config-cmap)# match access-group name ipv6-acl`	指定した ACL をベースにクラスマップに対して一致基準を設定します。

	コマンドまたはアクション	目的
ステップ 17	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol tcp`	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 18	**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 19	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect ipv6-policy`	プロトコル固有検査タイプ 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 20	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect ipv6-class`	アクションを実行する対象のトラフィック 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 21	**inspect** [*parameter-map-name*] 例： `Device(config-pmap-c)# inspect ipv6-param-map`	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 22	**end** 例： `Device(config-pmap-c)# end`	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、特権 EXEC モードを開始します。

ゾーンの設定およびインターフェイスへのゾーンの適用

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** *zone-name*
4. **exit**
5. **zone security** *zone-name*
6. **exit**
7. **zone-pair security** *zone-pair-name* [**source** *source-zone* **destination** *destination-zone*]
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **ipv6 address** *ipv6-address*/*prefix-length*
12. **encapsulation dot1q** *vlan-id*
13. **zone-member security** *zone-name*
14. **end**
15. **show policy-map type inspect zone-pair sessions**

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 モードを開始します。 • 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	**zone security** *zone-name* 例： `Device(config)# zone security z1`	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。
ステップ 4	**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。

	コマンドまたはアクション	目的
ステップ 5	**zone security** *zone-name* 例： `Device(config)# zone security z2`	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。
ステップ 6	**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 7	**zone-pair security** *zone-pair-name* [**source** *source-zone* **destination** *destination-zone*] 例： `Device(config)# zone-pair security in-2-out source z1 destination z2`	ゾーン 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。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect ipv6-policy`	ポリシー マップをトップレベル ポリシー マップに付加します。
ステップ 9	**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 10	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0.1`	サブインターフェイスを設定し、サブインターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**ipv6 address** *ipv6-address*/*prefix-length* 例： `Device(config-subif)# ipv6 address 2001:DB8:2222:7272::72/64`	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、インターフェイスまたはサブ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 12	**encapsulation dot1q** *vlan-id* 例： `Device(config-subif)# encapsulation dot1q 2`	インターフェイスで使用するカプセル化方式を設定します。

	コマンドまたはアクション	目的
ステップ 13	**zone-member security** *zone-name* 例： `Device(config-subif)# zone member security z1`	ゾーン メンバーとしてインターフェイスを設定します。 • *zone-name* 引数では、**zone security** コマンドを使用して設定したゾーンのいずれかを設定する必要があります。 • インターフェイスがセキュリティ ゾーンにある場合、そのインターフェイスを通るトラフィックはどちらの方向でもすべて（デバイス宛またはデバイス発信のトラフィックを除く）デフォルトでドロップされます。 ゾーン メンバーであるインターフェイスをトラフィックが通過することを許可するには、そのゾーンをゾーン ペアの一部にして、そのゾーンペアにポリシーを適用する必要があります。 ポリシーで、inspect または pass アクションを通してトラフィックが許可されると、トラフィックはインターフェイスを通過します。
ステップ 14	**end** 例： `Device(config-subif)# end`	サブインターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 15	**show policy-map type inspect zone-pair sessions** 例： `Device# show policy-map type inspect zone-pair sessions`	ポリシー マップが指定したゾーン ペアに適用されているため、作成されたステートフル パケット インスペクション セッションを表示します。 • このコマンドの出力は、IPv4 と IPv6 の両方のファイアウォール セッションを表示します。

例

show policy-map type inspect zone-pair sessions コマンドからの次のサンプル出力には、IPv6 アドレスと IPv4 アドレスの双方向のパケット変換が表示されます。

```
Device# show policy-map type inspect zone-pair sessions

  Zone-pair: in-to-out
  Service-policy inspect : in-to-out

    Class-map: ipv6-class (match-any)
      Match: protocol ftp
      Match: protocol tcp
      Match: protocol udp
      Inspect
        Established Sessions
         Session 110D930C [2001:DB8:1::103]:32847=>(209.165.201.2:21) ftp SIS_OPEN
          Created 00:00:00, Last heard 00:00:00
          Bytes sent (initiator:responder) [37:84]

        Half-open Sessions
```

```
        Session 110D930C [2001:DB8:1::104]:32848=>(209.165.201.2:21) ftp SIS_OPENING
         Created 00:00:00, Last heard 00:00:00
         Bytes sent (initiator:responder) [0:0]
```

show policy-map type inspect zone-pair sessions コマンドからの次のサンプル出力には、IPv6 アドレスから IPv6 アドレスへのパケットの変換が表示されます。

```
Device# show policy-map type inspect zone-pair sessions

  Zone-pair: in-to-out
  Service-policy inspect : in-to-out

    Class-map: ipv6-class (match-any)
      Match: protocol ftp
      Match: protocol tcp
      Match: protocol udp
      Inspect
        Established Sessions
         Session 110D930C [2001:DB8:1::103]:63=>[2001:DB8:2::102]:63 udp SIS_OPEN
          Created 00:00:02, Last heard 00:00:01
          Bytes sent (initiator:responder) [162:0]
```

IPv6 ファイアウォールおよびステートフル NAT64 ポート アドレス変換の設定

次の作業では、ステートフル NAT64 のダイナミック ポート アドレス変換（PAT）を使用した IPv6 ファイアウォールを設定します。

PAT 設定では、複数の IPv6 ホストを、使用可能な IPv4 アドレス プールに先着順でマッピングします。 ダイナミック PAT 設定は、IPv4 インターネットへの接続を提供しながら、不足している IPv4 アドレス空間の節約に直接役立ちます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **interface** *type number*
5. **no ip address**
6. **zone-member security** *zone-name*
7. **negotiation auto**
8. **ipv6 address** *ipv6-address*/*prefix-length*
9. **ipv6 enable**
10. **nat64 enable**
11. **exit**
12. **interface** *type number*
13. **ip address** *ip-address mask*
14. **zone member security** *zone-name*
15. **negotiation auto**
16. **nat64 enable**
17. **exit**
18. **ipv6 access-list** *access-list-name*
19. **permit ipv6 host** *source-ipv6-address* **host** *destination-ipv6-address*
20. **exit**
21. **ipv6 route** *ipv6-prefix*/*length interface-type interface-number*
22. **ipv6 neighbor** *ipv6-address interface-type interface-number hardware-address*
23. **nat64 v4 pool** *pool-name start-ip-address end-ip-address*
24. **nat64 v6v4 list** *access-list-name* **pool** *pool-name* **overload**
25. **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 モードを開始します。 • 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	**zone-member security** *zone-name* 例： `Device(config-if)# zone member security z1`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 7	**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 8	**ipv6 address** *ipv6-address/prefix-length* 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。
ステップ 9	**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 10	**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 11	**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。

	コマンドまたはアクション	目的
ステップ 12	**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 13	**ip address** *ip-address mask* 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 14	**zone member security** *zone-name* 例： `Device(config-if)# zone member security z2`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 15	**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 16	**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 17	**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 18	**ipv6 access-list** *access-list-name* 例： `Device(config)# ipv6 access-list ipv6-ipv4-pair`	IPv6 アクセス リストを定義し、IPv6 アクセス リスト 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	**permit ipv6 host** *source-ipv6-address* **host** *destination-ipv6-address* 例： `Device(config-ipv6-acl)# permit ipv6 host 2001:DB8:1::2 host 209.165:201.25`	IPv6 アクセス リスト、送信元 IPv6 ホスト アドレス、および宛先 IPv6 ホスト アドレスの許可条件を設定します。
ステップ 20	**exit** 例： `Device(config-ipv6-acl)# exit`	IPv6 アクセス リスト 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 21	**ipv6 route** *ipv6-prefix/length 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::2/96 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 v4 pool** *pool-name start-ip-address end-ip-address* 例： `Device(config)# nat64 v4 pool pool1 209.165.201.25 209.165.201.125`	ステートフル NAT64 IPv4 アドレス プールを定義します。
ステップ 24	**nat64 v6v4 list** *access-list-name* **pool** *pool-name* **overload** 例： `Device(config)# nat64 v6v4 list nat64-ipv6-any pool pool1 overload`	NAT64 PAT または過負荷アドレス変換をイネーブルにします。
ステップ 25	**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。

ゾーンベース ポリシー ファイアウォール IPv6 サポートの設定例

例：IPv6 ファイアウォールの設定

```
Device# configure terminal
Device(config)# vrf-definition VRF1
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# exit-address-family
```

```
Device(config-vrf)# exit
Device(config)# parameter-map type inspect ipv6-param-map
Device(config-profile)# sessions maximum 10000
Device(config-profile)# exit
Device(config)# ipv6 unicast-routing
Device(config)# ip port-map ftp port 8090 list ipv6-acl
Device(config)# ipv6 access-list ipv6-acl
Device(config-ipv6-acl)# permit ipv6 any any
Device(config-ipv6-acl)# exit
Device(config)# class-map type inspect match-all ipv6-class
Device(config-cmap)# match access-group name ipv6-acl
Device(config-cmap)# match protocol tcp
Device(config-cmap)# exit
Device(config)# policy-map type inspect ipv6-policy
Device(config-pmap)# class type inspect ipv6-class
Device(config-pmap-c)# inspect ipv6-param-map
Device(config-pmap-c)# end
```

例：ゾーンの設定およびインターフェイスへのゾーンの適用

```
Device# configure terminal
Device(config)# zone security z1
Device(config-sec-zone)# exit
Device(config)# zone security z2
Device(config-sec-zone)# exit
Device(config)# zone-pair security in-to-out source z1 destination z2
Device(config-sec-zone-pair)# service-policy type inspect ipv6-policy
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/0/0.1
Device(config-if)# ipv6 address 2001:DB8:2222:7272::72/64
Device(config-if)# encapsulation dot1q 2
Device(config-if)# zone member security z1
Device(config-if)# end
```

例：IPv6 ファイアウォールおよびステートフル NAT64 ポートアドレス変換の設定

```
configure terminal
 ipv6 unicast-routing
 interface gigabitethernet 0/0/0
  no ip address
  zone member security z1
  negotiation auto
  ipv6 address 2001:DB8:1::2/96
  ipv6 enable
  nat64 enable
!
 interface gigabitethernet 0/0/1
  ip address 209.165.201.25 255.255.255.0
  zone member security z2
  negotiation auto
  nat64 enable
!
 ipv6 access-list ipv6-ipv4-pair
  permit ipv6 host 2001:DB8:1::2 host 209.165:201.25
!
 ipv6 route 2001:DB8:1::2/96 gigabitethernet 0/0/0
 ipv6 neighbor 2001:DB8:1::2/96 gigabitethernet 0/0/0 0000.29f1.4841
 nat64 v4 pool pool1 209.165.201.25 209.165.201.125
 nat64 v6v4 list nat64-ipv6-any pool pool1 overload
```

ゾーンベース ポリシー ファイアウォール IPv6 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 Commands 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』
ステートフル NAT64	『Stateful Network Address Translation 64』

標準および RFC

標準/RFC	タイトル
RFC 2460	『*Internet Protocol, Version 6 (IPv6) Specification*』
RFC 2473	『*Generic Packet Tunneling in IPv6 Specification*』

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

ゾーンベース ポリシー ファイアウォール IPv6 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 *3*：ゾーンベース ポリシー ファイアウォール *IPv6* サポートの機能情報

機能名	リリース	機能情報
ゾーンベース ポリシー ファイアウォール IPv6 サポート	Cisco IOS XE Release 3.6S	ゾーンベース ポリシー ファイアウォール サポートは、IPv6 パケットのインスペクションをサポートします。 次のコマンドが導入または変更されました。**ip port-map** および **show policy-map type inspect zone-pair**。