ICMPのファイアウォールステートフルインスペクション

ICMP のファイアウォール ステートフル インスペクションは、Internet Control Management Protocol バージョン 4（ICMPv4）メッセージを悪意のあるメッセージまたは無害なメッセージのいずれかに分類する機能です。ファイアウォールではステートフルインスペクションを使用して、プライベートネットワーク内で生成された無害なICMPv4メッセージを信頼し、関連付けられた ICMP 応答がネットワーク内に入ることを許可します。ICMP のファイアウォール ステートフルインスペクション機能は、侵入者がネットワークに入り込まないようICMP を使用してネットワークの問題をデバッグするネットワーク管理者に役立ちます。

このモジュールでは、ICMPv4メッセージのファイアウォールステートフルインスペクションの概要を紹介し、ICMPv4 メッセージを検査するようにファイアウォールを設定する方法を説明します。

- ICMP のファイアウォール ステートフル インスペクションの前提条件 （1 ページ）
- ICMP のファイアウォール ステートフル インスペクションの制約事項 （2 ページ）
- ICMP のファイアウォール ステートフル インスペクションについて （2 ページ）
- ICMP のファイアウォール ステートフル インスペクションの設定方法 （4 ページ）
- ICMP のファイアウォール ステートフル インスペクションの設定例 （9 ページ）
- ICMP のファイアウォール ステートフル インスペクションに関する追加情報 （10 ページ）
- ICMP のファイアウォール ステートフル インスペクションに関する機能情報 （11 ページ）

ICMP のファイアウォール ステートフル インスペクションの前提条件

- ICMP のファイアウォール ステートフル インスペクション機能を設定するには、その前に、シスコ ファイアウォールを設定する必要があります。

- ネットワークで、すべての ICMP トラフィックにセキュリティ アプライアンス インターフェイスのパス スルーが許可される必要があります。
- セキュリティアプライアンスのインターフェイスで終端する ICMP トラフィックに対してアクセス ルールを設定する必要があります。

ICMP のファイアウォール ステートフル インスペクションの制約事項

この機能は UDP traceroute ユーティリティとは連動しません。この場合、ICMP パケットの代わりに UDP データグラムが送信されます。UDP traceroute は UNIX システムのデフォルトです。UNIX ホストでファイアウォールによって検査される ICMP traceroute パケットが生成されるようにするには、 **traceroute** コマンドで「-I」オプションを使用します。

ICMP のファイアウォール ステートフル インスペクションについて

ICMP のファイアウォール ステートフル インスペクションの概要

Internet Control Management Protocol（ICMP）は、ネットワークに関する情報を提供し、ネットワーク内のエラーを報告するネットワーク プロトコルです。ネットワーク管理者は ICMP を使用して、ネットワークの接続上の問題をデバッグします。ICMP を使用してプライベート ネットワークのトポロジを発見する可能性がある侵入者から保護するために、プライベート ネットワーク内に入らないように ICMPv4 メッセージをブロックすることはできますが、その場合、ネットワーク管理者がネットワークをデバッグできなくなります。

シスコ ルータでアクセス コントロール リスト（ACL）を使用することで、ICMPv4 メッセージを完全に許可または拒否するように設定できます。ICMPv4 メッセージに対して ACL を使用する場合、メッセージのインスペクションが、設定済みの allow または deny アクションよりも優先されます。

IP プロトコルを使用する ICMPv4 メッセージは、次の 2 つのタイプに分類することができます。

- 単純な要求/応答メカニズムを使用する情報メッセージ。
- IP パケットの配信中に何らかのエラーが発生したことを示すエラー メッセージ。

（注） ICMP 攻撃で宛先到達不能エラー メッセージが使用されないようにするために、1 つのセッションにつき 1 つの宛先到達不能メッセージだけがファイアウォールで許可されます。

ファイアウォールを経由する UDP セッションを処理しているホストが、宛先到達不能メッセージを含む ICMP エラー パケットを生成する場合があります。その場合、そのセッションでは 1 つの宛先到達不能メッセージだけがファイアウォールの通過を許可されます。

サポートされている ICMPv4 パケット タイプは以下のとおりです。

表 *1 : ICMPv4* パケット タイプ

パケット タイプ	名前	説明
0	エコー応答	エコー要求（タイプ 8）に対する応答。
3	到達不能	どの要求にも可能性のある応答。
8	エコー要求	ping または traceroute 要求。
11	時間超過	パケットの存続可能時間（TTL）のサイズがゼロの場合の応答。
13	タイムスタンプ要求	要求。
14	タイムスタンプ応答	タイムスタンプ要求（タイプ 13）に対する応答。

ICMPv4 パケット タイプ 0 と 8 は宛先に対する ping に使用されます。送信元がエコー要求パケットを送信すると、宛先はエコー応答パケットで応答します。パケット タイプ 0、8、および 11 は、ICMPv4 traceroute に使用されます（つまり、送信されるエコー要求パケットは、TTL サイズ 1 で開始されます）。TTL サイズはホップごとに増分されます。エコー要求パケットに対し、中間ホップは時間超過パケットで応答し、最終宛先はエコー応答パケットで応答します。

ICMPv4 エラー パケットが組み込みパケットである場合、その組み込みパケットは、該当するパケットに対して設定されたプロトコルとポリシーに応じて処理されます。たとえば、組み込みパケットが TCP パケットであり、そのパケットに対して drop アクションが設定されている場合、ICMPv4 では pass アクションを設定しているとしても、この組み込みパケットはドロップされます。

次のシナリオで、ICMPv4 パケットがファイアウォールをパス スルーするプロセスを説明します。

1. ICMPv4 パケットが送信元インターフェイスに到達します。ファイアウォールは、パケットの送信元アドレスと宛先アドレスを変更せずにそのまま使用して、パケット インスペクションを実行します。ファイアウォールは IP アドレス（送信元と宛先）、ICMP タイプ、およびプロトコルを使用してセッション キーの作成およびルックアップを行います。
2. パケットがファイアウォール インスペクションに合格します。
3. リターン トラフィックが宛先インターフェイスから戻ると、ファイアウォールは ICMPv4 メッセージ タイプに応じてセッション ルックアップ キーを作成します。
4. 1. 応答メッセージが情報メッセージの場合、ファイアウォールはパケットの送信元アドレスと宛先アドレスを変更せずにそのまま使用して、パケット インスペクションを実行します。ここで、宛先ポートは ICMPv4 メッセージの要求タイプです。
   2. 応答メッセージが ICMPv4 エラー メッセージの場合、ファイアウォールは ICMP エラー パケットに含まれるペイロード パケットを使用して、セッション ルックアップ用のセッション キーを作成します。
5. ファイアウォール セッション ルックアップが成功すると、パケットはファイアウォール インスペクションに合格します。

ICMP インスペクション チェック

ICMP の戻りパケットは、アクセス コントロール リスト（ACL）ではなくインスペクション コードによってチェックされます。インスペクション コードは各出力パケットの宛先アドレスをトラッキングし、返されるそれぞれのパケットをチェックします。エコー応答とタイムスタンプ応答のパケットについては、リターンアドレスがチェックされます。到達不能パケットおよび時間超過パケットについては、パケットデータから目的の宛先アドレスが抽出されてチェックされます。

ICMP のファイアウォール ステートフル インスペクションの設定方法

ICMP のファイアウォール ステートフル インスペクションの設定

次の項目を含む、ICMP のファイアウォール ステートフル インスペクションを設定しするには、この作業を実行します。

- ICMP トラフィックに一致するクラス マップ。
- 検査アクションを含むポリシー マップ。
- セキュリティ ゾーンおよびゾーン ペア（ファイアウォール ポリシー マップをゾーン ペアにアタッチするために必要）。

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny | permit**} **icmp** *source source-wildcard destination destination-wildcard*
4. **class-map type inspect** *class-map-name*
5. **match protocol** *protocol-name*
6. **exit**
7. **policy-map type inspect** *policy-map-name*
8. **class** *class-map-name*
9. **inspect**
10. **exit**
11. **exit**
12. **zone security** *zone-name*
13. **exit**
14. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
15. **service-policy type inspect** *policy-map-name*
16. **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	**access-list** *access-list-number* {**deny	permit**} **icmp** *source source-wildcard destination destination-wildcard* 例： `Device(config)# access-list 102 permit icmp 192.168.0.1 255.255.255.0 192.168.2.22 255.255.255.0`	拡張 IP アクセス リストを定義します。
ステップ 4	**class-map type inspect** *class-map-name* 例： `Device(config)# class-map type inspect c1`	アクションの実行対象となるクラスを定義し、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 5	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol icmp`	指定されたプロトコルに基づき、クラス マップの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 6	**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 7	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect p1`	プロトコル固有の検査タイプ 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 8	**class** *class-map-name* 例： `Device(config-pmap)# class c1`	アクションの実行対象となるクラスを定義し、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 9	**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 10	**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 11	**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 12	**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。 • 設定では送信元ゾーンと宛先ゾーンという、ゾーン ペアを作成するための 2 つのセキュリティ ゾーンが必要です。 • 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 13	**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 14	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security inout source z1 destination z2`	インターフェイスを割り当てることができる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。

	コマンドまたはアクション	目的
ステップ 15	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect p1`	ファイアウォール ポリシー マップをゾーン ペアに付加します。
ステップ 16	**end** 例： `Device(config-sec-zone-pair)# end`	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、特権EXECモードを開始します。

ICMP のファイアウォール ステートフル インスペクションの確認

次の **show** コマンドは任意の順序で使用できます。

手順の概要

1. **enable**
2. **show ip access-lists**
3. **show policy-map type inspect** *policy-map-name*
4. **show policy-map type inspect zone-pair** *zone-pair-name*
5. **show zone security** *zone-name*
6. **show zone-pair security** [**source** *source-zone* **destination** *destination-zone*]

手順の詳細

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 show ip access-lists

例：

```
Device# show ip access-lists
```

指定されたポリシー マップに関する情報を表示します。

ステップ 3 show policy-map type inspect *policy-map-name*

例：

```
Device# show policy-map type inspect p1
```

指定されたポリシー マップに関する情報を表示します。

ステップ 4 **show policy-map type inspect zone-pair** *zone-pair-name*

例：

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

ゾーン ペアのランタイム検査タイプ ポリシー マップ統計情報を表示します。

ステップ 5 **show zone security** *zone-name*

例：

```
Device# show zone security z1
```

ゾーン セキュリティ情報を表示します。

ステップ 6 **show zone-pair security** [**source** *source-zone* **destination** *destination-zone*]

例：

```
Device# show zone-pair security source z1 destination z2
```

送信元および宛先のゾーンとゾーン ペアに付加されたポリシーを表示します。

例：

次に示す **show ip access-lists** コマンドの出力例は、ホストから ping パケットのみが発行された ICMP セッションに対して ACL が作成されるしくみを示します。

```
Device# show ip access-lists

 Extended IP access list 102
     permit icmp any host 192.168.133.3 time-exceeded
     permit icmp any host 192.168.133.3 unreachable
     permit icmp any host 192.168.133.3 timestamp-reply
     permit icmp any host 192.168.133.3 echo-reply (4 matches)
```

次に、**show policy-map type inspect p1** コマンドの出力例を示します。

```
Device# show policy-map type inspect p1

 Policy Map type inspect p1
  Class c1
   Inspect
```

次に、**show policy-map type inspect zone-pair inout** コマンドの出力例を示します。

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

 Zone-pair: inout
  Service-policy : p1
   Class-map: c1 (match-all)
    Match: protocol icmp
    Inspect
     Session creations since subsystem startup or last reset 0
     Current session counts (estab/half-open/terminating) [0:0:0]
     Maxever session counts (estab/half-open/terminating) [0:0:0]
     Last session created never
     Last statistic reset never
```

```
    Last session creation rate 0
    half-open session total 0
  Class-map: class-default (match-any)
   Match: any
   Drop
    0 packets, 0 bytes
```

次に、**show zone security** コマンドの出力例を示します。

```
Device# show zone security

zone self
Description: System defined zone
```

次に、**show zone-pair security** コマンドの出力例を示します。

```
Device# show zone-pair security source z1 destination z2

zone-pair name inout
  Source-Zone z1  Destination-Zone z2
  service-policy p1
```

ICMP のファイアウォール ステートフル インスペクションの設定例

例：ICMP のファイアウォール ステートフル インスペクションの設定

```
Device# configure terminal
Device(config)# access-list 102 permit icmp 192.168.0.1 255.255.255.0 192.168.2.22
255.255.255.0
Device(config)# class-map type inspect c1
Device(config-cmap)# match protocol icmp
Device(config-cmap)# exit
Device(config)# policy-map type inspect p1
Device(config-pmap)# class c1
Device(config-pmap-c)# inspect
Device(config-pmap-c)# exit
Device(config-pmap)# exit
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 inout source z1 destination z2
Device(config-sec-zone-pair)# service-policy type inspect p1
Device(config-sec-zone-pair)# end
```

ICMP のファイアウォール ステートフル インスペクションに関する追加情報

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』、すべてのリリース
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』

標準と RFC

標準および RFC	タイトル
RFC 792	インターネット制御メッセージプロトコル（*ICMP*）
RFC 950	『*Internet Standard Subnetting Procedure*』
RFC 1700	『*Assigned Numbers*』

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

ICMP のファイアウォール ステートフル インスペクションに関する機能情報

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 : ICMP* のファイアウォール ステートフル インスペクションに関する機能情報

機能名	リリース	機能情報
ICMP のファイアウォール ステートフルインスペクション	Cisco IOS XE リリース 2.1 Cisco IOS XE リリース 3.2S	ICMP のファイアウォール ステートフル インスペクション機能は、ICMPv4 メッセージを「悪意のある」と「無害」のどちらかに分類します。ファイアウォールは、ステートフルインスペクションを使用して、プライベートネットワーク内で生成された無害の ICMP メッセージを信頼し、関連する ICMP 応答のエントリを許可します。

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。