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 インスペクション機能は、インターネット制御メッセージ プロトコル バージョン 4（ICMPv4）メッセージを悪意があるメッセージまたは良性メッセージとして分類します。 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良性 ICMPv4 メッセージを信頼し、関連する ICMP 応答のエントリがネットワークに入るのを許可します。 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を使用すると、ネットワーク管理者は ICMP を使用してネットワークの問題をデバッグすることができ、侵入者はネットワークに入れなくなります。

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、および 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について説明します。

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

- 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前に、Cisco 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トラフィックがセキュリティアプライアンスインターフェイスを通過できるようにする必要があります。
- セキュリティ アプライアンス インターフェイスで終端する ICMP トラフィックの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、ICMP パケットの代わりに UDP データグラムが送信される UDP traceroute ユーティリティでは機能しません。 UDP traceroute は、UNIX システムのデフォルトです。 ファイアウォールで検査される ICMP traceroute パケットを生成する UNIX ホストでは、**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

インターネット制御メッセージ プロトコル（ICMP）は、ネットワークに関する情報を提供し、ネットワークで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、ネットワーク接続の問題をデバッグします。プライベートネットワークのトポロジの検出にICMPを使用する潜在的な侵入者から保護するために、ICMPv4メッセージをブロックしてプライベート ネットワークに入れないようにすることができます。ただし、ネットワーク管理者はネットワークをデバッグできなくなる可能性があります。

アクセス コントロール リスト（ACL）を使用して ICMPv4 メッセージを完全に許可するか拒否するように Cisco ルータを設定できます。 ICMPv4 メッセージに ACL を使用すると、メッセージインスペクションは、設定済みの許可または拒否の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 種類に分類できます。

- 単純な要求/応答メカニズムを利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攻撃が宛先到達不能エラー メッセージを使用できないようにするには、セッションあたり1つの宛先到達不能エラー メッセージのみがファイアウォールで許可されるようにします。
ファイアウォールを通過する UDP セッションを処理しているホストは、宛先到達不能メッセージを使用して ICMP エラー パケットを生成する場合があります。 このような場合、そのセッションに対して1つの宛先到達不能メッセージのみがファイアウォールを通過できます。

次の ICMPv4 パケット タイプがサポートされます。

表 *1*：*ICMPv4* パケット タイプ

パケット タイプ	名前	説明
0	Echo Reply	エコー要求への応答（タイプ 8）。
3	Unreachable	任意の要求への考えられる応答。
8	Echo Request	ping または traceroute 要求。
11	Time Exceeded	パケットの存続可能時間（TTL）のサイズがゼロである場合の応答。
13	Timestamp Request	要求。
14	Timestamp Reply	タイムスタンプ要求への応答（タイプ13）。

ICMPv4 パケット タイプ 0 と 8 を使用して、宛先への ping を実行します。送信元は、エコー要求パケットを送信し、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 を ICMPv4 traceroute に使用し（つまり、送信されたエコー要求パケットは TTL サイズが 1 で始まります）、TTL のサイズはホップごとに増加します。 中間ホップでは時間超過パケットのエコー要求パケットに応答し、最終宛先が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の場合、組み込みパケットは、パケットに設定されたプロトコルとポリシーに基づいて処理されます。たとえば、組み込みパケットが TCP パケットで、パケットに drop アクションが設定されている場合、ICMPv4 に pass アクションが設定されている場合でも、パケットはドロップされます。

次のシナリオは、ICMPv4 パケットがファイアウォールを通過する方法を説明しています。

1 ICMPv4パケットは送信元インターフェイスに到着します。ファイアウォールは、パケットインスペクションを変更せずに、パケットの送信元および宛先アドレスを使用します。ファイアウォールは、セッション キーの作成および参照用に 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ます。

2 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。

3 リターン トラフィックは宛先インターフェイスで生じ、ICMPv4 メッセージ タイプに基づいて、ファイアウォールはセッション 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 インスペクションのためにパケットの送信元および宛先アドレスを変更なしで使用します。 ここで、宛先ポートは ICMPv4 メッセージ要求タイプです。

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 パケットに存在するペイロード 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した場合、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 インスペクションの確認

ICMP 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、検査コードによって検査されます。 検査コードは、各発信パケットからの宛先アドレスを追跡し、各戻りパケットをチェックします。エコー応答パケットおよびタイムスタンプ応答パケットでは、リターンアドレスが検査されます。 到達不能パケットおよび時間超過パケットの場合、意図した宛先アドレスが、パケット データから抽出され、検査されます。

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

この作業を実行して、次を含む、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ます。

- ICMP トラフィックと一致するクラス 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 ゾーンとゾーン ペア（ファイアウォール ポリシー マップをゾーン ペアに付加するため）。

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	**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。

	コマンドまたはアクション	目的
ステップ 4	**class-map type inspect** *class-map-name* 例： `Device(config)# class-map type inspect c1`	アクションを実行する対象のクラスを定義し、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くクラス マップの一致基準を設定します。
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`	アクションを実行する対象のクラスを定義し、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。

	コマンドまたはアクション	目的
		• 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。
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** コマンドを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 **show ip access-lists**

例：
```
Device# show ip access-lists
```
指定したポリシー マップ情報を表示します。

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

例：
```
Device# show policy-map type inspect p1
```
指定したポリシー マップ情報を表示します。

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
```
送信元ゾーンと宛先ゾーン、およびゾーン ペアに付加されたポリシーを表示します。

例：

show ip access-lists コマンドからの次のサンプル出力は、ping パケットだけがホストから発行された ICMP セッションに対して ACL がどのように作成されたかを示します。

```
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』

標準および RFC

標準/RFC	タイトル
RFC 792	『*Internet Control Message Protocol*』
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
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

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 インスペクションの機能情報

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 Release 2.1 Cisco IOS XE Release 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 メッセージを悪意があるメッセージまたは良性メッセージとして分類します。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良性 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。