ファイアウォールデバイスのセキュリティポリシーの設定

[Platform] > [Security] の [General] ページおよび [Timeouts] ページを使用して、デバイスの一般的なセキュリティ設定を行うことができます。インターフェイスでアンチスプーフィングをイネーブルにしたり、IP フラグメント設定を行ったり、デバイスのさまざまなタイムアウト値を設定したりできます。

この章は次のトピックで構成されています。

[一般（General）] ページ

[General] ページを使用して、悪意のあるパケット、スプーフィングされたパケット、フラグメント化されたパケット、および DoS 攻撃から保護するためのセキュリティ設定を行います。このページの設定の詳細については、 フラッドガード、アンチ スプーフィング、およびフラグメント値の設定 （3 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [セキュリティ（Security）] > [全般（General）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [セキュリティ（Security）] > [全般（General）] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- [Add/Edit General Security Configuration] ダイアログボックス （4 ページ）
- タイムアウトの設定 （5 ページ）

フィールド リファレンス

表 *1 : [*一般（*General***）*]* ページ**

要素	説明
Disable Floodguard（PIX 6.3 および FWSM 2.x だけ）	ファイアウォールデバイス上でフラッドガードをディセーブルにするには、このチェックボックスをオンにします。このオプションは、PIX 6.3 および FWSM 2.x デバイスでだけ使用できます。フラッドガード機能の詳細については、フラッドガード、アンチ スプーフィング、およびフラグメント値の設定 （3 ページ）を参照してください。
Global Fragment Settings 次のオプションを使用して、デバイスのグローバル フラグメント値を設定します。個々のインターフェイスに対するこれらの設定をオーバーライドできます。詳細については、[Add/Edit General Security Configuration] ダイアログボックス （4 ページ）を参照してください。	
Enable Default Settings	デフォルトのフラグメント設定フィールドをイネーブルにするには、このチェックボックスをオンにします。
サイズ	再構成を待機する IP 再構成データベースに格納できる最大フラグメント数を指定します。デフォルトは 200 です。
Chain	完全な IP パケットをフラグメント化する場合の最大フラグメント数を指定します。デフォルトは 24 パケットです。
タイムアウト（Timeout）	フラグメント化されたパケット全体が到着するのを待機する最大秒数を指定します。タイマーは、パケットの最初のフラグメントの到着後に開始されます。指定した秒数までに到着しなかったパケット フラグメントがある場合、到着済みのすべてのパケット フラグメントが廃棄されます。デフォルトは 5 秒です。
Interface Configuration Table このテーブルには、個々のアンチ スプーフィング設定およびフラグメント設定が定義されているすべてのインターフェイスが示されます。これらの設定の詳細については、フラッドガード、アンチ スプーフィング、およびフラグメント値の設定 （3 ページ）を参照してください。個々のインターフェイスにおけるこれらの値の設定の詳細については、[Add/Edit General Security Configuration] ダイアログボックス （4 ページ）を参照してください。	

フラッドガード、アンチスプーフィング、およびフラグメント値の設定

[Platform] > [Security] の [General] ページを使用して、（PIX 6.3 または FWSM 2.x デバイスの）フラッドガードをイネーブルまたはディセーブルにし、個々のインターフェイスでユニキャスト リバース パス転送（アンチ スプーフィング）をイネーブルにし、デバイスおよびデバイスの各インターフェイスの IP フラグメント値を設定します。

フラッドガード

フラッドガードを使用すると、ユーザ認証サブシステムでリソースが不足した場合にファイアウォール リソースを再要求できます。インバウンドまたはアウトバウンドの uauth 接続が攻撃を受けている場合または過剰に使用されている場合、ファイアウォールは TCP ユーザ リソースをアクティブに再要求します。

ユーザ認証サブシステムのリソースが枯渇すると、緊急性に応じて、次の順序で、さまざまな状態の TCP ユーザ リソースが再要求されます。

1. Timewait
2. LastAck
3. FinWait
4. Embryonic
5. Idle

フラッドガードは、デフォルトでイネーブルになっています。このオプションは、PIX 6.3 または FWSM 2.x デバイスにだけ適用されます。

アンチ スプーフィング

ユニキャスト Reverse Path Forwarding（RPF; リバース パス転送）は、すべてのパケットの送信元 IP アドレスが、ルーティング テーブルに基づく正しい送信元インターフェイスに一致することを確認することによって、IP スプーフィング（本来の送信元を隠すために不正な送信元 IP アドレスを使用するパケット）を防止します。

通常、セキュリティ アプライアンスは、パケットの転送先を決めるときに、宛先アドレスだけを確認します。ユニキャスト RPF は、送信元アドレスも確認することをセキュリティ アプライアンスに指示します。これが、リバース パス転送と呼ばれる理由です。セキュリティアプライアンスの通過を許可するすべてのトラフィックについて、送信元アドレスに戻るルートをセキュリティアプライアンスのルーティング テーブルに含める必要があります。詳細については、RFC 2267 を参照してください。

たとえば、外部トラフィックの場合、セキュリティアプライアンスは、デフォルトのルートを使用してユニキャスト RPF 保護を実現できます。トラフィックが外部インターフェイスから入り、その送信元アドレスをルーティング テーブルが認識できない場合、セキュリティ アプライアンスはデフォルトのルートを使用して、外部インターフェイスを送信元インターフェイスとして正しく識別します。

トラフィックが、ルーティングテーブルにとって既知であるが、内部インターフェイスに関連付けられているアドレスから外部インターフェイスに入る場合、セキュリティアプライアンスはそのパケットをドロップします。同様に、トラフィックが未知の送信元アドレスから内部インターフェイスに入る場合、一致するルート（デフォルトルート）は外部インターフェイスを示しているため、セキュリティ アプライアンスはそのパケットをドロップします。

ユニキャスト RPF は、次のように実装されます。

- ICMP パケットにはセッションがないため、個々のパケットはチェックされません。
- UDP および TCP にはセッションがあるため、初期パケットにはリバース ルート ルックアップが必要となります。セッション中に到着する後続のパケットは、セッションの一部として保持されている既存の状態を使用してチェックされます。最初のパケット以外のパケットは、最初のパケットと同じインターフェイスに到着したことを保証するためにチェックされます。

フラグメント設定

フラグメント設定によって、パケット フラグメンテーションの管理が提供され、Network File System（NFS; ネットワーク ファイル システム）との互換性が向上します。デフォルトでは、セキュリティ アプライアンスは、IP パケットごとに最大 24 のフラグメント、および再構成を待機する最大 200 のフラグメントを許可します。定期的にパケットをフラグメント化するアプリケーション（NFS over UDP など）がある場合は、ネットワーク上でフラグメントを許可する必要がある場合があります。ただし、トラフィックをフラグメント化するアプリケーションがない場合は、セキュリティアプライアンス経由でのフラグメントを許可しないことを推奨します。フラグメント化されたパケットは、DoS 攻撃として使用されることがあるためです。

関連項目

- [一般（General）] ページ （1 ページ）
- [Add/Edit General Security Configuration] ダイアログボックス （4 ページ）

[Add/Edit General Security Configuration] ダイアログボックス

[Add/Edit General Security Configuration] ダイアログボックスを使用して、アンチ スプーフィングをイネーブルまたはディセーブルにし、フラグメント オーバーライド設定値をインターフェイスに設定します。

ナビゲーション パス

[Add/Edit General Security Configuration] ダイアログボックスには、[Platform] > [Security] > [一般（General）] ページ （1 ページ）の [Anti-Spoofing and Fragment Interface Configuration] テーブルからアクセスできます。

関連項目

- フラッドガード、アンチ スプーフィング、およびフラグメント値の設定 （3 ページ）

フィールド リファレンス

表 2 : [Add/Edit General Security Configuration] ダイアログボックス

要素	説明
インターフェイス（Interface）	アンチスプーフィングまたはフラグメント値を設定するインターフェイスの名前を入力または選択します。
Enable Anti-Spoofing	指定したインターフェイスでユニキャストRPF（アンチスプーフィング）をイネーブルにするには、このチェックボックスをオンにします。
Override Default Fragment Settings	指定したインターフェイスのデフォルトのフラグメント設定をオーバーライドするには、このチェックボックスをオンにして次のフィールドをイネーブルにしてから、新しい値を入力します。デバイスのデフォルトのグローバルフラグメント設定値については、[一般（General）] ページ （1 ページ）を参照してください。
サイズ	指定したインターフェイスに関して、再構成を待機しているIP再構成データベースに格納できる最大フラグメント数を指定します。デフォルトは 200 です。
Chain	指定したインターフェイスに関して、完全なIPパケットをフラグメント化する場合の最大フラグメント数を指定します。デフォルトは24パケットです。
タイムアウト（Timeout）	フラグメント化されたパケット全体が、指定したインターフェイスに到着するのを待機する最大秒数を指定します。タイマーは、パケットの最初のフラグメントの到着後に開始されます。指定した秒数までに到着しなかったパケット フラグメントがある場合、到着済みのすべてのパケット フラグメントが廃棄されます。デフォルトは 5 秒です。

タイムアウトの設定

[Timeouts] ページを使用すると、セキュリティ アプライアンスでさまざまなタイムアウト値を設定できます。すべての時間が **hh:mm:ss** の形式になります。

これらの値は、さまざまなプロトコルの接続スロットと変換スロットのアイドルタイムアウトを表します。指定したアイドル時間中にスロットが使用されなかった場合、リソースはフリープールに戻されます。TCP 接続スロットは、通常の接続クローズ シーケンスの約 60 秒後に解放されます。

危険 これらの値は、カスタマー サポートに指示された場合を除き、変更しないことを推奨します。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [セキュリティ（Security）] > [タイムアウト（Timeouts）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [セキュリティ（Security）] > [タイムアウト（Timeouts）] を選択します。ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 *3 : [Timeouts]* ページ

要素	説明
パラメータのタイムアウト値を変更するには、そのパラメータ エントリの左にあるオプション ボタンをクリックしてアクティブ化してから、そのパラメータ フィールドに新しい値を入力します。値をデフォルトにリセットするには、関連する [Default] ボタンをクリックします。 [Disable] ボタン（提供されている場合）をクリックすると、値が 0:00:00 に設定され、そのタイムアウトがディセーブルになります。前の段落のいずれかの手順を実行して、ディセーブルになっている値を再度イネーブルにします。	
Translation Slot (xlate)	変換スロットが解放されるまでのアイドル時間。この値は 1 分以上である必要があります。デフォルトは 3 時間です。このタイムアウトをディセーブルにするには、0:00:00 を入力します。
Connection (conn)	接続スロットが解放されるまでのアイドル時間。この値は 5 分以上である必要があります。デフォルトは 1 時間です。このタイムアウトをディセーブルにするには、[無効（Disable）] をクリックするか 0:00:00 を入力します。
Half-Closed	TCP ハーフクローズ接続が閉じられるまでのアイドル時間。ASA 9.1.2 以降のデバイスの場合、最小値は 30 秒です。他のすべてのデバイスの場合、最小値は 5 分です。デフォルトは 10 分です。このタイムアウトをディセーブルにするには、[無効（Disable）] をクリックするか 0:00:00 を入力します。
UDP	UDP プロトコル接続が閉じられるまでのアイドル時間。この値は 1 分以上である必要があります。デフォルトは 2 分です。このタイムアウトをディセーブルにするには、[無効（Disable）] をクリックするか 0:00:00 を入力します。

要素	説明
SCTP	SCTP プロトコル接続が閉じられるまでのアイドル時間。この値は 1 分以上である必要があります。デフォルトは 2 分です。このタイムアウトをディセーブルにするには、[無効（Disable）] をクリックするか 0:00:00 を入力します。
接続ホールドダウン（Connection Holddown）	トラフィックが転送されるまでのアイドル時間。これは、ルートフラッピングを回避するために、トラフィックを転送する前に ASA が待機する時間です。この値は 1 秒以上にする必要があります。デフォルトは 15 秒です。このタイムアウトをディセーブルにするには、[無効（Disable）] をクリックするか 0:00:00 を入力します。
ICMP（PIX 7.x+、ASA、FWSM 3.x+）	全般的な ICMP 状態が終了するまでのアイドル時間。
RPC/Sun RPC	SunRPC スロットが解放されるまでのアイドル時間。この値は 1 分以上である必要があります。デフォルトは 10 分です。このタイムアウトをディセーブルにするには、[無効（Disable）] をクリックするか 0:00:00 を入力します。
H.225	H.225 シグナリング接続が閉じられるまでのアイドル時間。H.225 のデフォルトのタイムアウトは 1 時間（01:00:00）です。この値を 00:00:00 に設定すると、接続が閉じられなくなります。すべてのコールがクリアされた直後に接続を閉じるには、1 秒（0:00:01）を入力します。
H.323	H.323 メディア接続が閉じられるまでのアイドル時間。デフォルトは 5 分です。このタイムアウトをディセーブルにするには、[無効（Disable）] をクリックするか 0:00:00 を入力します。
MGCP	MGCP メディア ポートが閉じられるまでのアイドル時間。デフォルトは 5 分（0:05:00）です。このタイムアウトをディセーブルにするには、[無効（Disable）] をクリックするか 0:00:00 を入力します。
MGCP PAT（PIX 7.x+、ASA、FWSM 3.x+）	MGCP PAT 変換が削除されるまでのアイドル時間。最小時間は 30 秒です。デフォルトは 5 分（0:05:00）です。このタイムアウトをディセーブルにするには、[無効（Disable）] をクリックするか 0:00:00 を入力します。
SIP	SIP シグナリング ポート接続が閉じられるまでのアイドル時間。この値は 5 分以上である必要があります。デフォルトは 30 分です。このタイムアウトをディセーブルにするには、[無効（Disable）] をクリックするか 0:00:00 を入力します。

要素	説明
SIP Media	SIP メディア ポート接続が閉じられるまでのアイドル時間。この値は 1 分以上である必要があります。デフォルトは 2 分です。このタイムアウトをディセーブルにするには、[無効（Disable）] をクリックするか 0:00:00 を入力します。
SIP Disconnect（PIX 6.3(5)、PIX/ASA 7.2+、FWSM 3.2+）	CANCEL または BYE メッセージに対する 200 OK を受信しなかった場合に、SIP セッションが削除されるまでのアイドル時間。最小値は 0:00:01 です。最大値は 0:10:00 です。デフォルト値は 0:02:00 です。
SIP Invite（PIX 6.3(5)、PIX/ASA 7.2 以降、FWSM 3.2 以降）	暫定応答のピンホールおよびメディア xlate が終了するまでのアイドル時間。最小値は 0:01:00 です。最大値は 0:30:00 です。デフォルト値は 0:03:00 です。
SIP Provisional Media（PIX/ASA 7.2(3)+）	SIP プロビジョニングメディア接続のタイムアウト値。値の範囲は 0:01:00 ～ 1193:00:00 である必要があります。デフォルトは 2 分です。
承認タイプ(uath) Absolute	認証キャッシュがタイムアウトし、新しい接続の再認証が必要となるまでの時間。システムは、ユーザが新しい接続を開始するまで待機してから、再認証を要求します。この時間は、変換スロット値よりも短い必要があります。キャッシングをディセーブルにし、すべての新しい接続に対して再認証を要求するには、[無効（Disable）] をクリックするか、0:00:00 を入力します。 （注） 接続でパッシブ FTP を使用する場合は、この値を 0:00:00 に設定しないでください。 （注） この値を 0:00:00 に設定すると、 HTTPS 認証が機能しない場合があります。HTTPS 認証後に、ブラウザが複数の TCP 接続を開始して Web ページをロードすると、最初の接続は許可されますが、その後の接続では認証がトリガーされます。このため、ユーザーには、認証の成功後も常に認証ページが表示されます。これを回避するには、認証の絶対タイムアウトを 1 秒に設定します。ただし、この回避策では、同じ送信元 IP アドレスからアクセスした認証されていないユーザがファイアウォールを通過できる期間が 1 秒間発生します。
承認タイプ(uath) Inactivity	認証キャッシュがタイムアウトし、ユーザによる新しい接続の再認証が必要となるまでのアイドル時間。この期間は、変換スロット値よりも短い必要があります。

要素	説明
IGP	Cisco ASA は、ダイナミック ルーティング プロトコル（ボーダー ゲートウェイ プロトコル（BGP）および Open Shortest Path First（OSPF））について、ソフトウェアバージョン 9.3.1 以降でノンストップ フォワーディングをサポートします。Open Shortest Path First（OSPF）のコンバージェンス時間は、デフォルトで 70 秒です。 このフィールドを使用して、コンバージェンス時間を変更できます。この値は、10 秒から 1 時間 40 秒の範囲内である必要があります。IGP のデフォルト値は 0:01:10 です。

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。