DoS コマンド

この章は、次の項で構成されています。

security-suite deny fragmented

特定のインターフェイスから断片化された IP パケットを破棄するには、**security-suite deny fragmented** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。

断片化された IP パケットを許可するには、このコマンドの **no** 形式を使用します。

構文

security-suite deny fragmented *{[***add** *{ip-address* | **any***} {mask* | */prefix-length}]* | *[***remove** *{ip-address* | **any***} {mask* | */prefix-length}]}*

no security-suite deny fragmented

パラメータ

- **add** *ip-address* | *any*：宛先 IP アドレスを指定します。**any** を使用して、すべての IP アドレスを指定します。
- **mask**：IP アドレスのネットワーク マスクを指定します。
- **prefix-length**：IP アドレス プレフィックスを構成するビットの数を指定します。プレフィックス長は、スラッシュ（/）で開始する必要があります。

デフォルト設定

断片化されたパケットはすべてのインターフェイスから許可されます。

mask が指定されていない場合、デフォルトは 255.255.255.255 です。

prefix-length が指定されていない場合、デフォルトは 32 です。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

このコマンドが動作するためには、show security-suite configuration （18 ページ） がグローバルとインターフェイスの両方で有効である必要があります。

例

次の例では、インターフェイスからの断片化された IP パケットの破棄を試みています。

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# security-suite deny fragmented add any /32
To perform this command, DoS Prevention must be enabled in the per-interface mode.
```

security-suite deny icmp

（デバイスがネットワーク上にあることを攻撃者に知られることを防ぐために）特定のインターフェイスからの ICMP エコー要求を破棄するには、**security-suite deny icmp** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。

エコー要求を許可するには、このコマンドの **no** 形式を使用します。

構文

security-suite deny icmp *{[***add** *{ip-address* | **any***} {mask* | */prefix-length}]* | *[***remove** *{ip-address* | **any***} {mask* | */prefix-length}]}*

no security-suite deny icmp

パラメータ

- **ip-address** | **any**：宛先 IP アドレスを指定します。**any** を使用して、すべての IP アドレスを指定します。
- **mask**：IP アドレスのネットワーク マスクを指定します。
- **prefix-length**：IP アドレス プレフィックスを構成するビットの数を指定します。プレフィックス長は、スラッシュ（/）で開始する必要があります。

デフォルト設定

エコー要求はすべてのインターフェイスから許可されます。

mask が指定されていない場合、デフォルトは 255.255.255.255 です。

prefix-length が指定されていない場合、デフォルトは 32 です。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

このコマンドが動作するためには、show security-suite configuration （18 ページ） がグローバルとインターフェイスの両方で有効である必要があります。

このコマンドは、指定されたインターフェイスに入る、ICMP タイプがエコー要求の ICMP パケットを破棄します。

例

次の例では、インターフェイスからのエコー要求の破棄を試みています。

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# security-suite deny icmp add any /32
To perform this command, DoS Prevention must be enabled in the per-interface mode.
```

security-suite deny martian-addresses

システム予約済み IP アドレスまたはユーザ定義 IP アドレスを含むパケットを拒否するには、**security-suite deny martian-addresses** グローバル コンフィギュレーション モード コマンドを使用します。

デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

構文

security-suite deny martian-addresses *{***add** *{ip-address {mask | /prefix-length}} |* ***remove*** *{ip-address {mask | /prefix-length}}*（ユーザ指定 IP アドレスの追加または削除）

security-suite deny martian-addresses ***reserved*** *{***add** | **remove***}* *(*Add/remove system-reserved IP addresses, see tables below)

no security-suite deny martian-addresses（このコマンドは、**security-suite deny martian-addresses** *{***add** *{ip-address {mask | /prefix-length}} |* ***remove*** *{ip-address {mask | /prefix-length}}* により予約されたアドレスを削除し、ユーザにより追加されたすべてのエントリを削除します。**remove** *ip-address {mask | /prefix-length}* パラメータを使用することで、ユーザは特定のエントリを削除できます）。

security-suite deny martian-addresses ***reserved*** *{***add** | **remove***}* コマンドの **no** 形式はありません。保護を削除するには（そして、ハードウェア リソースを解放するには）、代わりに **security-suite deny martian-addresses reserved** *remove* コマンドを使用します。

パラメータ

- **reserved add/remove**：以下の予約済みアドレスの表に対して追加または削除を行います。
- **ip-address**：指定された IP 送信元または宛先アドレスを持つパケットを追加または破棄します。
- **mask**：IP アドレスのネットワーク マスクを指定します。
- **prefix-length**：IP アドレス プレフィックスを構成するビットの数を指定します。プレフィックス長は、スラッシュ（/）で開始する必要があります。
- **reserved**：予約済み（Martian）IP アドレスのブロック内の送信元または宛先 IP アドレスを持つパケットを破棄します。予約済みアドレスのリストについては、ユーザ ガイドラインを参照してください。

デフォルト設定

Martian アドレスは許可されます。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドが動作するためには、show security-suite configuration （18 ページ） がグローバルに有効である必要があります。

security-suite deny martian-addresses *reserved* は、次の表のアドレスを追加または削除します。

アドレス ブロック	現在の使用
0.0.0.0/8（0.0.0.0/32 が送信元アドレスの場合を除く）	このブロック内のアドレスは、「この」ネットワーク上の送信元ホストを参照します。
127.0.0.0/8	このブロックは、インターネット ホスト ループバック アドレスとして使用するために割り当てられています。
192.0.2.0/24	このブロックは、ドキュメンテーションとサンプル コードで使用するための「TEST-NET」として割り当てられています。
224.0.0.0/4（送信元として）	以前はクラス D アドレス空間として知られていたこのブロックは、IPv4 マルチキャスト アドレス割り当てで使用するために割り当てられています。
240.0.0.0/4（255.255.255.255/32 が宛先アドレスの場合を除く）	以前はクラス E アドレス空間として知られていたこのブロックは、予約済みです。

（注） 予約済みのアドレスが含まれている場合は、個々の予約済みのアドレスは削除できません。

例

次の例では、予約済み IP アドレスのブロック内の送信元または宛先アドレスを持つ、すべてのパケットを破棄しています。

```
switchxxxxxx(config)# security-suite deny martian-addresses reserved add
```

security-suite deny syn

特定のインターフェイスからの TCP 接続の作成をブロックするには、**security-suite deny syn** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。このコマンドは、これらの接続を完全にブロックします。

TCP 接続の作成を許可するには、このコマンドの **no** 形式を使用します。

構文

security-suite deny syn {*[***add** *{tcp-port* | **any***} {ip-address* | **any***} {mask* | */prefix-length}]* | *[***remove** *{tcp-port* | **any***} {ip-address* | **any***} {mask* | */prefix-length}]}*

no security-suite deny syn

パラメータ

- **ip-address** | **any**：宛先 IP アドレスを指定します。**any** を使用して、すべての IP アドレスを指定します。
- **mask**：宛先 IP アドレスのネットワーク マスクを指定します。
- **prefix-length**：宛先IPアドレスプレフィックスを構成するビットの数を指定します。プレフィックス長は、スラッシュ（/）で開始する必要があります。
- **tcp-port** | **any**：宛先 TCP ポートを指定します。使用できる値は、**http**、**ftp-control**、**ftp-data**、**ssh**、**telnet**、**smtp**、または **port number** です。すべてのポートを指定するには **any** を使用します。

デフォルト設定

TCP 接続の作成は、すべてのインターフェイスから許可されます。

mask が指定されていない場合、デフォルトは 255.255.255.255 です。

prefix-length を指定しない場合は、デフォルトで 32 が使用されます。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

このコマンドが動作するためには、show security-suite configuration （18 ページ） がグローバルとインターフェイスの両方で有効である必要があります。

インターフェイスからの TCP 接続の作成のブロックは、指定された宛先 IP アドレスと宛先 TCP ポートについて、「SYN=1」、「ACK=0」、および「FIN=0」の入力 TCP パケットを破棄することで行われます。

例

次の例では、インターフェイスからの TCP 接続の作成のブロックを試みています。これは、セキュリティ スイートがインターフェイスごとではなく、グローバルに有効になっているため、失敗します。

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# security-suite deny syn add any /32 any
To perform this command, DoS Prevention must be enabled in the per-interface mode.
```

security-suite deny syn-fin

SYN と FIN の両方が設定されているすべての入力 TCP パケットをドロップするには、**security-suite deny syn-fin** グローバル コンフィギュレーション モード コマンドを使用します。

SYN と FIN の両方が設定されている TCP パケットを許可するには、このコマンドの **no** 形式を使用します。

構文

security-suite deny syn-fin

no security-suite deny syn-fin

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

この機能は、デフォルトで有効に設定されています。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、SYN フラグと FIN フラグの両方が設定されている TCP パケットをブロックしています。

```
switchxxxxxx(config)# security-suite deny syn-fin
```

security-suite dos protect

特定の既知のサービス妨害（DoS）攻撃からシステムを保護するには、**security-suite dos protect** グローバル コンフィギュレーション モード コマンドを使用します。3 つのタイプの攻撃に保護を提供できます（以下のパラメータを参照）。

DoS 保護を無効にするには、このコマンドの **no** 形式を使用します。

構文

security-suite dos protect {**add** *attack* | **remove** *attack*}

no security-suite dos protect

パラメータ

add/remove *attack*：追加または削除する攻撃タイプを指定します。攻撃を追加すると、その攻撃に対する保護が提供されます。攻撃を削除すると、保護が削除されます。

使用できる攻撃タイプは次のとおりです。

- **stacheldraht**：送信元 TCP ポートが 16660 の TCP パケットを破棄します。
- **invasor-trojan**：宛先 TCP ポートが 2140、送信元 TCP ポートが 1024 の TCP パケットを破棄します。
- **back-orifice-trojan**：宛先 UDP ポートが 31337、送信元 UDP ポートが 1024 の UDP パケットを破棄します。

デフォルト設定

保護は設定されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドが動作するためには、show security-suite configuration （18 ページ） がグローバルに有効である必要があります。

例

次の例では、Invasor トロイの木馬 DoS 攻撃からシステムを保護しています。

```
switchxxxxxx(config)# security-suite dos protect add invasor-trojan
```

security-suite dos syn-attack

サービス妨害（DoS）SYN 攻撃をレート制限するには、**security-suite dos syn-attack** インターフェイス コンフィギュレーション モード コマンドを使用します。このコマンドにより、SNY パケットが部分的にブロックされます（最大で、ユーザが指定したレートまで）。

レート制限を無効にするには、このコマンドの **no** 形式を使用します。

構文

security-suite dos syn-attack *syn-rate* {***any*** **|** *ip-address*} {*mask* | *prefix-length*}

no security-suite dos syn-attack {***any*** **|** *ip-address*} {*mask* | *prefix-length*}

パラメータ

- **syn-rate**：1 秒あたりの最大接続数を指定します。（範囲：199 ～ 1000）
- **any | ip-address**：宛先 IP アドレスを指定します。**any** を使用して、すべての IP アドレスを指定します。
- **mask**：宛先 IP アドレスのネットワーク マスクを指定します。
- **prefix-length**：宛先 IP アドレス プレフィックスを構成するビットの数を指定します。プレフィックス長は、スラッシュ（/）で開始する必要があります。

デフォルト設定

レート制限は設定されていません。

ip-address が指定されていない場合、デフォルトは 255.255.255.255 です。

prefix-length が指定されていない場合、デフォルトは 32 です。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

このコマンドが動作するためには、show security-suite configuration （18 ページ） がグローバルとインターフェイスの両方で有効である必要があります。このコマンドは、指定された宛先 IP アドレスについて、「SYN=1」、「ACK=0」、および「FIN=0」の入力 TCP パケットをレート制限します。SYN 攻撃のレート制限は、セキュリティ スイートのルールがパケットに適用された後に実装されます。ACL ルールと QoS ルールは、これらのパケットには適用されません。ハードウェア レート制限はバイト数をカウントするため、「SYN」パケットのサイズは短いと見なされます。

例

次の例では、ポートでの DoS SYN 攻撃のレート制限を試みています。これは、セキュリティスイートがインターフェイスごとではなく、グローバルに有効になっているため、失敗します。

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# security-suite dos syn-attack 199 any /10
To perform this command, DoS Prevention must be enabled in the per-interface mode.
```

security-suite enable

セキュリティスイート機能と設定を有効にするには、**security-suite enable** グローバル コンフィギュレーション モード コマンドを使用します。セキュリティスイート機能は、さまざまなタイプの攻撃に対する保護をサポートします。デフォルト設定を復元するには、このコマンドの **no** 形式を使用します。

構文

security-suite enable [**global-rules-only | interface-rules-only**]

no security-suite enable

パラメータ

- **global-rules-only**：（オプション）デバイスがグローバルレベル（インターフェイスレベルではない）のセキュリティスイートコマンドのみをサポートするように指定します。この設定により、Ternary Content Addressable Memory（TCAM）のスペースを節約できます。このキーワードを使用しない場合、security-suite コマンドはグローバルに使用することもインターフェイスごとに使用することもできます。
- **interface-rules-only**：（オプション）デバイスがインターフェイスレベルのセキュリティスイート コマンドのみをサポートするように指定します（詳細については、次のユーザガイドラインを参照してください）。このモードは、デバイス上のいずれかのインターフェイスに ACL が適用されている場合は有効にできません。
- **(none)**：キーワードを使用しない場合、セキュリティスイートのコマンドはグローバルにもインターフェイスごとにも使用できます。このモードは、ACLがデバイス上のインターフェイスに適用されている場合は有効にできません。

デフォルト設定

セキュリティ スイート機能は無効になっています。

global-rules-only または **interface-rules-only** のいずれも指定されていない場合、デフォルトではセキュリティスイートをグローバルとインターフェイスごとに有効にします。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

セキュリティスイートの設定を定義し、有効にできる設定のタイプ（グローバルレベルルールのみ、インターフェイス レベル ルールのみ、または両方のタイプ）を決定する機能を有効にするには、このコマンドを使用します。セキュリティスイートが有効になっている場合、ユーザが設定したモードに応じて、次のコマンドを使用できます。

このコマンドを使用すると、ハードウェア リソースが予約されます。予約するリソースの数はコマンドに指定したモード（**global-rules-only**、**interface-rules-only**、または no mode（両方のタイプ））によって異なります。リソースは、**no security-suite enable** コマンドが入力されると解放されます。

セキュリティ スイートを有効にする前に、MAC ACL を削除する必要があります。このルールは、セキュリティ スイートを有効にした後に再入力できます。インターフェイスに ACL またはポリシー マップが割り当てられている場合は、インターフェイスのセキュリティ スイートのルールごとに有効にすることはできません。

例 1：次の例では、セキュリティ スイート機能を有効にし、security-suite コマンドがグローバル コマンドのみであることを指定しています。ポート上でセキュリティ スイートを設定しようとすると失敗します。

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# security-suite dos syn-attack 199 any /10
To perform this command, DoS Prevention must be enabled in the per-interface mode.
```

例 2：次の例では、セキュリティ スイート機能をグローバルに、およびインターフェイスで有効にしています。ポートに対する security-suite コマンドは成功します。

```
switchxxxxxx(config)# security-suite enable
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# security-suite dos syn-attack 199 any /10
switchxxxxxx(config-if)#
```

security-suite syn protection mode

TCP SYN 保護モードを設定するには、**security-suite syn protection mode** グローバル コンフィギュレーション モード コマンドを使用します。

TCP SYN 保護モードをデフォルトに設定するには、このコマンドの **no** 形式を使用します。

構文

security-suite syn protection mode {disabled | report | block}

no security-suite syn protection mode

パラメータ

- **disabled**：この機能が無効になります。
- **report**：この機能でポートごとの TCP SYN トラフィックに関して報告されます（攻撃が識別された場合のレート制限 SYSLOG メッセージを含む）。
- **block**：ローカル システム宛ての攻撃ポートからの TCP SYN トラフィックがブロックされ、レート制限 SYSLOG メッセージ（1 分ごとに 1 回）が生成されます。

デフォルト設定

デフォルト モードは block です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

（ユーザ定義 ACL などの）ACL が定義されているポートでは、この機能は TCP SYN パケットをブロックできません。保護モードがブロックされて SYN トラフィックをブロックできない場合、関連する SYSLOG メッセージ（port gi1/0/1 is under TCP SYN attack など）が作成されます。TCP SYN traffic cannot be blocked on this port since the port is bound to an ACL.」というメッセージが作成されます。

例 1：次の例では、ポートから攻撃が識別された場合に、ポートに対する TCP SYN 攻撃を報告するように TCP SYN 保護機能を設定しています。

```
switchxxxxxx(config)# security-suite syn protection mode report
```

例 2：次の例では、ポートから攻撃が識別された場合に、ポートに対する TCP SYN 攻撃をブロックするように TCP SYN 保護機能を設定しています。

```
switchxxxxxx(config)# security-suite syn protection mode block
```

security-suite syn protection recovery

攻撃されたインターフェイスをSYN保護機能がブロックする期間を設定するには、**security-suite syn protection period** グローバル コンフィギュレーション モード コマンドを使用します。

期間をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

構文

security-suite syn protection recovery timeout

no security-suite syn protection recovery

パラメータ

timeout：SYN パケットのブロック元のインターフェイスでブロックを解除するタイムアウト（秒単位）を定義します。このインターフェイスで SYN 攻撃が引き続きアクティブな場合には、再度ブロックされる可能性があることに注意してください。（範囲：10 ～ 600）

デフォルト設定

デフォルトのタイムアウト値は 60 秒です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

タイムアウトが変更された場合、新しい値は現在攻撃を受けていないインターフェイスでのみ使用されます。

例

次の例では、TCP SYN 期間を 100 秒に設定しています。

```
switchxxxxxx(config)# security-suite syn protection recovery 100
```

security-suite syn protection threshold

SYN 保護機能のしきい値を設定するには、**security-suite syn protection threshold** グローバル コンフィギュレーション モード コマンドを使用します。

しきい値をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

構文

security-suite syn protection threshold syn-packet-rate

no security-suite syn protection threshold

パラメータ

syn-packet-rate：TCP SYN 攻撃の識別をトリガーする、特定の各ポートからのレート（1 秒あたりのパケット数）を定義します。（範囲：20 ～ 200）

デフォルト設定

デフォルトのしきい値は 80 pps（1 秒あたりのパケット数）です。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、TCP SYN 保護のしきい値を 40 pps に設定しています。

```
switchxxxxxx(config)# security-suite syn protection threshold 40
```

show security-suite configuration

セキュリティスイート設定を表示するには、**show security-suite configuration** switchxxxxxx> コマンドを使用します。

構文

show security-suite configuration

コマンド モード

ユーザ EXEC モード

例

次の例では、セキュリティ スイート設定を表示しています。

```
switchxxxxxx# show security-suite configuration
```

セキュリティスイートが有効になっています（インターフェイスごとのルールが有効になっている）。

```
Denial Of Service Protect: stacheldraht, invasor-trojan, back-office-trojan.
Denial Of Service SYN-FIN Attack is enabled
Denial Of Service SYN Attack
```

Interface ---------- gi1/0/1	IP Address ---------- 176.16.23.0\24	SYN Rate (pps) ---------- 100

```
Martian addresses filtering
Reserved addresses: enabled.
Configured addresses: 10.0.0.0/8, 192.168.0.0/16
SYN filtering
```

Interface ---------- gi1/0/2	IP Address ---------- 176.16.23.0\24	TCP port ---------- FTP

```
ICMP filtering
```

Interface ---------- gi1/0/2	IP Address ---------- 176.16.23.0\24	

```
Fragmented packets filtering
```

Interface ---------- gi1/0/2	IP Address ---------- 176.16.23.0\24	

show security-suite syn protection

SYN 保護機能の設定と、インターフェイスごとの最後の攻撃の時間を含むインターフェイス ID ごとの動作ステータスを表示するには、**show security-suite syn protection** switchxxxxxx> コマンドを使用します。

構文

show security-suite syn protection [interface-id]

パラメータ

interface-id：（オプション）インターフェイス ID を指定します。インターフェイス ID には、イーサネット ポートまたはポート チャネルのいずれかのタイプを指定できます。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

インターフェイス ID を使用して、特定のインターフェイスに関する情報を表示します。

例

次の例では、TCP SYN 保護機能の設定と、すべてのインターフェイスの現在のステータスを表示しています。この例では、ポート gi1/0/2 が攻撃されていますが、このポートにはユーザ ACL が存在するため、ブロックできません。そのため、ステータスは Blocked and Reported ではなく Reported になっています。

```
switchxxxxxx# show security-suite syn protection
Protection Mode: Block
Threshold: 40 Packets Per Second
Period: 100 Seconds
```

Interface Name	Current Status	Last Attack
gi1/0/1	Attacked	19:58:22.289 PDT Feb 19 2012 Blocked and Reported
gi1/0/2	Attacked	19:58:22.289 PDT Feb 19 2012 Reported
gi1/0/3	Attacked	19:58:22.289 PDT Feb 19 2012 Blocked and Reported

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。