Cisco IOS Classic Firewall/IPS：Denial of Service（DoS）を防止するためのコンテキストベース アクセス コントロール（CBAC）の設定

内容

概要

このドキュメントでは、CBAC を使用する Cisco IOS® Classic Firewall でのサービス拒否（DoS）パラメータの調整手順について説明します。

CBAC は、高度なトラフィック フィルタリング機能を提供し、ネットワーク ファイアウォールの不可欠な要素として使用されます。

通常、DoS は意図的か否かにかかわらず、WAN リンク帯域幅、ファイアウォール接続テーブル、エンド ホスト メモリ、CPU、サービス機能などのネットワーク リソースを制圧するネットワーク アクティビティを指します。最悪のシナリオの場合、DoS アクティビティは、該当するリソースが利用不能になるまで脆弱な（または標的とする）リソースを制圧し、正規ユーザへの WAN 接続またはサービス アクセスを禁止します。

Cisco IOS Firewall は、Classic Firewall（**ip inspect**）および Zone-Based Policy Firewall の両方で、ファイアウォールおよび侵入防御ソフトウェアを通じて、「ハーフオープン」TCP 接続数のカウンタおよび合計接続レートを維持する場合、DoS アクティビティの軽減に役立ちます。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

ハーフオープン接続とは、相互接続のパラメータをネゴシエートするために、常に TCP ピアで使用される 3 方向 SYN-SYN/ACK-ACK ハンドシェイクが完了していない TCP 接続です。大量のハーフオープン接続は、DoS または分散型サービス拒否（DDoS）攻撃など、悪意のあるアクティビティを示唆する可能性があります。DoS 攻撃の 1 つのタイプの例は、インターネット上で複数のホストに感染し、大量の SYN 接続がインターネット上または組織のプライベート ネットワーク内の複数のホストによってサーバに送信される、SYN 攻撃によって特定のインターネット サーバを制圧を試みるワームやウイルスなど、悪意のある、意図的に開発されたソフトウェアによって実行されます。SYN 攻撃は、サーバが新しい接続に対処可能になるよりも早く到達する「偽」の SYN 接続試行によってサーバの接続テーブルをロードできるため、インターネット サーバへの危害を示します。これは、攻撃を受けるサーバの TCP 接続リスト内の大量の接続によって、正規ユーザによる攻撃を受けるインターネット サーバへのアクセスが妨害されるため、DoS 攻撃の 1 つのタイプです。

トランスポート用に UDP を使用する多くのアプリケーションがデータの受信を確認するので、Cisco IOS Firewall は、1 方向のみのトラフィックを持つ User Datagram Protocol（ユーザ データグラム プロトコル）セッションも「ハーフオープン」と見なします。リターン トラフィックのない UDP セッションは、DoS アクティビティを示唆する可能性があり、ホストのうちの 1 つが応答しなくなった 2 つのホスト間の接続を試みます。ログ メッセージ、SNMP ネットワーク管理トラフィック、音声およびビデオ メディアのストリーミング、シグナリング トラフィックなど、多くの UDP トラフィックのタイプは、トラフィックを伝送するために 1 方向のトラフィックのみを使用します。これらのタイプのトラフィックの多くは、1 方向トラフィック パターンがファイアウォールや IPS DoS 動作に悪影響を及ぼさないようにするために、アプリケーション固有のインテリジェンスを適用します。

Cisco IOS ソフトウェア リリース 12.4(11)T および 12.4(10) の前に、Cisco IOS ステートフル パケット インスペクションは、インスペクション規則が適用された時点で、デフォルトで DoS 攻撃からの保護を提供しています。Cisco IOS ソフトウェア リリース 12.4(11)T および 12.4(10) は、DoS 保護は自動的には適用されないが、接続アクティビティ カウンタが引き続きアクティブになるように、デフォルトの DoS 設定を変更しています。DoS 保護がアクティブな場合、つまりデフォルト値が以前のソフトウェア リリースで使用されている場合、または値がトラフィックに影響を与える範囲に調整されている場合、DoS 保護は、ファイアウォールが適用される方向で、ファイアウォール ポリシー設定プロトコルが検査するために、インスペクションが適用されるイ

ンターフェイスで有効になります。DoS 保護は、トラフィックが TCP 接続または UDP セッションの最初のトラフィック（SYN パケットまたは最初の UDP パケット）の同じ方向に適用されるインスペクションによってインターフェイスに入るか、離れるネットワーク トラフィックでのみ有効になります。

Cisco IOS ファイアウォール インスペクションは、DoS 攻撃から保護するために調整可能な複数の値を備えています。12.4(11)T および 12.4(10) より前の Cisco IOS ソフトウェア リリースには、接続レートがデフォルト値を超えるネットワークで適切なレベルのネットワーク アクティビティに対応するように設定されていない場合、適切なネットワーク操作を妨げる可能性があるデフォルト値があります。これらのパラメータにより、ファイアウォール ルータの DoS 保護が有効になる開始ポイントを設定することができます。ルータの DoS カウンタがデフォルト値または設定値を上回ると、ルータは、ハーフオープン セッションの数が max-incomplete の下位値を下回るまで、設定された max-incomplete または 1 分間の上限値を超える新しい接続ごとに 1 つの古いハーフオープン接続をリセットします。ロギングが有効な場合、ルータは Syslog メッセージを送信し、ルータに侵入防御システム（IPS）が設定されている場合、ファイアウォール ルータは Security Device Event Exchange（SDEE）を通じて DoS シグニチャ メッセージを送信します。DoS パラメータがネットワークの通常動作に対応していない場合、通常のネットワーク アクティビティは、Cisco IOS ファイアウォール ルータ上でアプリケーション障害、ネットワーク パフォーマンスの低下、および CPU の高使用率を引き起こす DoS 保護メカニズムをトリガーする場合があります。

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

Cisco IOS Software Classic（IP Inspect）Firewall および侵入防御システム対応サービス攻撃の調整

Classic Cisco IOS Firewall は、ルータの DoS カウンタのグローバル設定を維持し、すべてのインターフェイス上のすべてのファイアウォール ポリシーに対するすべてのファイアウォール セッションがファイアウォール カウンタのグローバル設定に適用されます。

Cisco IOS Classic Firewall インスペクションは、Classic Firewall が適用されるときに、デフォルトで DoS 攻撃からの保護を提供します。DoS 保護は、ファイアウォールが適用される方向で、ファイアウォール ポリシーが検査するように設定されている各サービスまたはプロトコルに対して、インスペクションが適用されるすべてのインターフェイスで有効になります。Classic Firewall は、DoS 攻撃から保護するために調整可能な複数の値を備えています。接続レートがデフォルトを超えるネットワークで適切なレベルのネットワーク アクティビティに対応するように設定されていない場合、表 1 に示すレガシー デフォルト設定（リリース 12.4(11)T より前のソフトウェア イメージによる）は、正しいネットワーク操作を妨げる可能性があります。DoS の設定は、実行コマンド **show ip inspect config** によって確認することでき、設定は **sh ip inspect all** の出力に含まれています。

CBAC は、タイムアウトとしきい値を使用して、セッションのステート情報を管理する時間を特定し、完全に確立されていないセッションを破棄する時期を決定します。これらのタイムアウトとしきい値は、すべてのセッションにグローバルに適用されます。

表 1 Classic Firewall のデフォルトの DoS 保護の制限		
DoS 保護値	**12.4(11)T/12.4(10) より前**	**12.4(11)T/12.4(10) 以降**
max-incomplete の上限値	500	無制限
max-incomplete の下限値	400	無制限
1 分間の上限値	500	無制限
1 分間の下限値	400	無制限
tcp max-incomplete ホストの *値*	50	無制限

Cisco IOS VRF 対応ファイアウォールを適用するように設定されたルータは、VRF ごとに 1 セットのカウンタを保持します。

「ip inspect one-minute high」および「ip inspect one-minute low」のカウンタは、接続が正常に行われているかどうかにかかわらず、ルータが動作する前の瞬間におけるすべての TCP、UDP、インターネット制御メッセージ プロトコル（ICMP）の接続試行の合計を維持します。接続レートの増加は、プライベート ネットワーク上のワームの感染、またはサーバに対する DoS 攻撃の試行を示唆する可能性があります。

ファイアウォールの DoS 保護を「無効」にすることはできませんが、大量のハーフオープン接続がファイアウォール ルータのセッション テーブルに存在しない限り、DoS 保護が有効にならないように DoS 保護の調整できます。

DoS ファイアウォールの保護

ファイアウォールの DoS 保護をネットワークのアクティビティに合うように調整するには、次の手順を実行します。

1. ネットワークが、誤って大量のハーフオープン接続値や接続レートの試行を引き起こす可能性があるワームやウイルスに感染していないことを確認します。ネットワークが「クリーン」ではない場合、ファイアウォールの DoS 保護を適切に調整する方法はありません。通常のアクティビティの間に、ネットワークのアクティビティを監視する必要があります。ネットワーク アクティビティが低下またはアイドル状態になっている時間内にネットワークの DoS 保護設定を調整すると、通常のアクティビティ レベルが DoS 保護設定を超える場合があります。
2. max-incomplete の上限値をきわめて高い値にします。

```
ip inspect max-incomplete high 20000000
ip inspect one-minute high 100000000
ip inspect tcp max-incomplete host 100000 block-time 0
```

これにより、ネットワークの接続パターンを監視する間、ルータは DoS 保護を提供できなくなります。DoS 保護を無効な状態のままにしたい場合は、ここでこの手順を中止します。**注：ルータで**Cisco IOSソフトウェアリリース12.4(11)T以降、または12.4(10)以降が稼働している場合は、デフォルトのDoS保護値を上げる必要はありません。これらは、デフォルトで最大限度に設定されています。**注：ホストへの接続開始のブロックを含む、より積極的なTCPホスト固有のDoS防御を有効にする場合**は、ip inspect tcp max-incomplete hostコマン

ドで指定されたブロック時間を設定する必要があります

3. このコマンドを使用して、Cisco IOS Firewall の統計情報を消去します。

```
show ip inspect statistics reset
```

4. 設定したルータをしばらくの間（おそらく 24 ~ 48 時間）この状態のままにして、通常のネットワーク アクティビティ サイクルの少なくとも丸 1 日以上、ネットワーク パターンを確認できようにします。**注：値は非常に高いレベルに調整さ**れますが、ネットワークはCisco IOS FirewallやIPS DoS保護の恩恵を受けません。
5. 監視期間経過後に、次のコマンドで DoS カウンタを確認します。

```
show ip inspect statistics
```

DoS 保護を調整するために監視する必要があるパラメータは、**bold** でハイライトされています。

```
Packet inspection statistics
   [process switch:fast switch]
  tcp packets: [218314:7878692]
  udp packets: [501498:65322]
   packets: [376676:80455]
   packets: [5738:4042411]
  smtp packets: [11:11077]
  ftp packets: [2291:0]
Interfaces configured for inspection 2
Session creations since subsystem
   startup or last reset 688030
Current session counts
   (estab/half-open/terminating) [0:0:0]
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
Last session created 00:00:05
Last statistic reset never
Last session creation rate 1
Maxever session creation rate 330
Last half-open session total 0
TCP reassembly statistics
  received 46591 packets out-of-order; dropped 16454
  peak memory usage 48 KB; current usage: 0 KB
  peak queue length 16
```

6. **ip inspect max-incomplete high を、ルータの指定された maxever セッション カウントのハーフオープン値より 25 パーセント高い値に設定します。**1.25 の乗数は、観察された動作を上回る 25 パーセントの余裕を提供します。次に例を示します。

```
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
56 * 1.25 = 70
```

設定例:

```
router(config)
   #ip inspect max-incomplete high 70
```

注：このドキュメントでは、ネットワークの一般的なアクティビティの1.25倍の乗数を使用して、DoS保護を行うための制限を設定する方法について説明します。通常のネットワークアクティビティのピーク内のネットワークを監視する場合、特殊な状況を除くすべての状況で、ルータの DoS 保護のアクティブ化を回避するために十分な余裕を提供する必要があります。この値を超える正当なネットワーク アクティビティの大規模なバーストがネットワークに定期的に発生する場合、ルータは一部のネットワーク トラフィックに悪影響を及ぼ

す可能性のある DoS 保護機能を実施します。正当なネットワーク アクティビティの結果として限度がもたらされたと判断した場合、DoS アクティビティを検出するためのルータ ログをモニタし、**ip inspect max-incomplete high および ip inspect one-minute high またはそのいずれかの限度を調整し、DoS のトリガーを防ぎます。**次のようなログ メッセージの存在によって、DoS 保護アプリケーションを確認できます。

7. **ip inspect max-incomplete low を、ルータが maxever セッション カウントのハーフオープン値に対して表示した値に設定します。次に例を示します。**

```
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
```

設定例:

```
router(config)
   #ip inspect max-incomplete low 56
```

8. **ip inspect one-minute high および one-minute low のカウンタは、接続が正常に行われているかどうかにかかわらルータが動作する前の瞬間におけるすべての TCP、UDP、インターネット制御メッセージ プロトコル（ICMP）の接続試行の合計を維持します。**接続レートの増加は、プライベート ネットワーク上のワームの感染、またはサーバに対する DoS 攻撃の試行を示唆する可能性があります。追加インスペクション統計情報は、セッション作成率の最高水準を明らかにするために、12.4(11)T および 12.4(10) で **show ip inspect statistics の出力に追加されました。**12.4(11)T または 12.4(10) より前の Cisco IOS ソフトウェア リリースを実行している場合、インスペクション統計情報に次の行は含まれません。

```
Maxever session creation rate [value]
```

12.4(11)T および 12.4(10) より前の Cisco IOS ソフトウェア リリースは、インスペクション maxever の 1 分間の接続レートの値を維持しないため、監視された「maxever セッション カウント」値に基づいて適用する値を計算します。実稼働環境で Cisco IOS Firewall Release 12.4(11) T のステートフル インスペクションを使用する複数のネットワークの監視によって、Maxever のセッション作成率が約 10 パーセントの「maxever セッション カウント」の 3 つの値（確立、ハーフオープン、および終了）の合計を超過する傾向があることが確認されています。ip inspect の 1 分間の下限値を計算するには、1.1 によって示された「確立」値を乗算します。次に例を示します。

```
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
(207 + 56 + 35) * 1.1 = 328
```

設定例:

```
ip inspect one-minute low 328
```

ルータが Cisco IOS ソフトウェア リリース 12.4(11)T 以降、または 12.4(10) 以降を実行している場合、単に「Maxever セッション作成率」インスペクションの統計情報に表示される値を適用できます。

```
Maxever session creation rate 330
```

設定例:

```
ip inspect one-minute low 330
```

9. **ip inspect one-minute high** を計算し、設定します。ip inspect の 1 分間の上限値は、計算された 1 分間の下限値より高い 25 パーセントである必要があります。次に例を示します。

```
ip inspect one-minute low (330) * 1.25 = 413
```

設定例:

```
ip inspect one-minute high 413
```

注：このドキュメントでは、ネットワークの一般的なアクティビティの1.25倍の乗数を使用して、DoS保護を行うための制限を設定する方法について説明します。通常のネットワークアクティビティのピーク内のネットワークを監視する場合、特殊な状況を除くすべての状況で、ルータの DoS 保護のアクティブ化を回避するために十分な余裕を提供する必要があります。この値を超える正当なネットワーク アクティビティの大規模なバーストがネットワ

ークに定期的に発生する場合、ルータは一部のネットワーク トラフィックに悪影響を及ぼす可能性のある DoS 保護機能を実施します。正当なネットワーク アクティビティの結果として限度がもたらされたと判断した場合、DoS アクティビティを検出するためのルータ ログをモニタし、**ip inspect max-incomplete high および ip inspect one-minute high またはそのいずれかの限度を調整し、DoS のトリガーを防ぎます。**次のようなログ メッセージの存在によって、DoS 保護アプリケーションを確認できます。

10. サーバの機能の知識に基づいて、**ip inspect tcp max-incomplete host の値を定義する必要があります。**このドキュメントでは、この値がエンド ホストのハードウェアおよびソフトウェア パフォーマンスに基づいて大幅に変動するため、ホストごとの DoS 保護設定のためのガイドラインを提供できません。DoS 保護を設定するための適切な限度について確信が持てない場合は、DoS の限度を定義する次の 2 つのオプションが役に立ちます。望ましいオプションは、ルータ ベースのホストごとの DoS 保護を上限値（最大値 4,294,967,295 以下）に設定し、各ホストのオペレーティング システムや Cisco Security Agent（CSA）などの外部ホスト ベースの侵入防御システムで提供されるホスト固有の保護を適用することです。ネットワーク ホストのアクティビティおよびパフォーマンス ログインを検査し、ピーク時に持続可能な接続レートを決定します。Classic Firewall のみが 1 台のグローバル カウンタを提供するので、すべてのネットワーク ホストが最大接続レート率であるかどうかを確認した後で、最大値を適用する必要があります。ここでも、OS 固有のアクティビティの限度と CSA などのホスト ベースの IPS の使用がお勧めします。**注：Cisco** IOS **Firewall**は、特定のオペレーティングシステムおよびアプリケーションの脆弱性に対する直接攻撃に対して限定的な保護を提供します。Cisco IOS Firewall の DoS 保護は、潜在的に対立する環境に露出されるエンド ホスト サービスの侵害の保護を保証しません。
11. ネットワーク上の DoS 保護アクティビティをモニタします。DoS 攻撃検出の発生を記録するには、理想的には、Syslog サーバを使用するか、Cisco Monitoring and Reporting Stations（MARS）を使用します。検出が非常に頻繁に発生する場合は、DoS 保護パラメータをモニタし、調整する必要があります。TCP SYN の DoS 攻撃に関する詳細については、「TCP SYN サービス拒否攻撃から保護するための戦略の定義」を参照してください。

確認

現在、この設定に使用できる確認手順はありません。

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- Cisco PIX Firewall ソフトウェア
- Cisco Secure PIX ファイアウォール コマンド リファレンス
- セキュリティ製品に関する Field Notice（PIX を含む）
- Requests for Comments (RFCs)

- テクニカル サポートとドキュメント – Cisco Systems