ログインブロックの設定

ログインの拡張機能に関する情報：ログインブロック

ログインの拡張機能：ログインブロックの概要

ログインの拡張機能（ログインブロック）機能により、ユーザーはサービス拒絶（DoS）攻撃と思われる攻撃が検出された場合、ログイン試行を自動的にブロックするオプションを設定して、デバイスのセキュリティを強化できます。

この機能により導入された Login Block オプションおよび Login Delay オプションで、Telnet または SSH 仮想接続を設定できます。この機能をイネーブルにすると、接続試行の失敗が複数回検出された場合に、「待機時間」を強制して「辞書攻撃」をスローダウンし、ルーティングデバイスをサービス拒絶（DoS）攻撃攻撃から保護できます。

サービス拒絶攻撃および辞書ログイン攻撃からの保護

ユーザーまたは経営幹部レベルで、デバイスを管理する目的によるデバイスへの接続は、リモートコンソール（PC など）から Telnet または SSH（セキュアシェル）を使用して最も頻繁に実行されます。ユーザのデバイスと管理デバイスとの間の通信トラフィックが暗号化されるため、SSH では、よりセキュアな接続オプションが提供されます。Login Block 機能をイネーブルにすると、Telnet 接続と SSH 接続の両方に適用されます。12.3(33)SRB2、12.2(33)SXH2、および 12.4(15)T1 以降のリリースバージョンでは、ログインブロック機能は HTTP 接続にも適用されます。

この機能によって導入される自動アクティベーション、および Login Block 機能および Quiet Period 機能のロギングは、個人が使用するとネットワーク デバイスを阻害したり、損なう可能

性のある2つの既知の方法に特に対処したりすることでデバイスのセキュリティをさらに強化するように設計されています。

デバイスの接続アドレスが検出され、到達可能である場合、悪意あるユーザが接続要求のフラッディングによってデバイスの通常の動作を妨げようとする可能性があります。通常のルーティングサービスを適切に処理しようとして、繰り返し行われるログイン接続試行を処理しようとしたり、デバイスがビジーになったり、正規のシステム管理者に通常のログインサービスを提供できなくなる可能性があるため、この種の攻撃は、サービス拒絶（DoS）攻撃の試行と呼ばれます。

辞書攻撃の主な意図は、一般的な DoS 攻撃とは異なり、デバイスへの管理アクセスを実際に取得することです。辞書攻撃とは、数千、時には数百万ものユーザ名/パスワードの組み合わせでログインを試行する自動プロセスです（このタイプの攻撃は、まず最初に、有効なパスワードとして一般的な辞書で見られるあらゆる言葉が使用されるため、「辞書攻撃」と呼ばれています）。このアクセスを試行するためにスクリプトやプログラムが使用されていて、このような試みのプロファイルは通常、DoS試行のものと同じです。短期間で複数のログインを試行します。

検出プロファイルをイネーブルにすることにより、ログイン試行の失敗が反復する場合は、以降の接続要求（ログインブロッキング）を拒否して対応するように、デバイスを設定できます。このブロックには「待機時間」と呼ばれる、一定の時間を設定できます。システム管理者との関連付けが把握されているアドレスを使用してアクセスリスト（ACL）を設定し、待機時間中でも正規の接続試行を許可できます。

連続するログイン試行間の遅延

デバイスは、仮想接続をできる限り高速で処理して受け入れることができます。ログイン試行間に遅延を導入すると、デバイスを辞書攻撃や DoS 攻撃などの悪意あるログイン接続から保護することができます。遅延は次のいずれかの方法でイネーブルにできます。

- **auto secure** コマンドを使用します。AutoSecure機能をイネーブルにすると、デフォルトで1秒のログイン遅延時間が自動的に強制されます。
- **login block-for** コマンドを使用します。**login delay** コマンドを発行する前に、このコマンドを入力する必要があります。**login block-for** コマンドのみを入力すると、デフォルトで1秒のログイン遅延時間が自動的に強制されます。
- グローバル コンフィギュレーション モード コマンド **login delay** を使用すると、強制されるログイン遅延時間を秒単位で指定できます。

DoS 攻撃が疑われる場合のログイン シャットダウン

設定された接続試行回数が指定された期間内に失敗した場合、デバイスは「待機時間」の間、追加接続を受け付けません。（事前定義されたアクセス コントロール リスト（ACL）によって許可されたホストは待機時間から除外されます）。

待機時間を発生させる接続試行の失敗回数は、新しいグローバルコンフィギュレーションモード コマンド **login block-for** で指定できます。待機時間から除外される定義済みの ACL は、新

しいグローバル コンフィギュレーション モード コマンド **login quiet-mode access-class** で指定できます。

この機能は、デフォルトではディセーブルです。AutoSecureがイネーブルの場合はイネーブルになりません。

ログイン拡張機能の設定方法：ログインブロック

ログイン パラメータの設定

デバイスへのDoS攻撃の疑いを検出し、辞書攻撃による影響の緩和に役立つログインパラメータを設定するには、ここに示す手順を実行します。

すべてのログインパラメータは、デフォルトではディセーブルです。他のログインコマンドを使用する前に、デフォルトのログイン機能を有効にする **login block-for** コマンドを発行する必要があります。**login block-for** コマンドをイネーブルにすると、次のデフォルトが強制されます。

- デフォルトの 1 秒のログイン遅延
- TelnetまたはSSHを通じて行われるすべてのログイン試行は、待機時間中拒否されます。つまり、**login quiet-mode access-class** コマンドが発行されるまで、ACL はログイン時間から除外されません。

手順

	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	**login block-for** *seconds* **attempts** *tries* **within** *seconds* **例**： `Device(config)# login block-for 100 attempts 2 within 100`	DoS 検出の提供に役立つログインパラメータ用にデバイスを設定します。 （注） このコマンドは、その他のログイン コマンドを使用する前に発行する必要があります。

	コマンドまたはアクション	目的

ステップ 4	**login quiet-mode access-class** {*acl-name* | *acl-number*}
	例：
	`Device(config)# login quiet-mode access-class myacl`
		（任意）このコマンドはオプションですが、デバイスが静音モードに切り替わるときにデバイスに適用される ACL を指定するように設定することを推奨します。デバイスが待機モードになっている間は、すべてのログイン要求が拒否され、使用できる接続はコンソール経由の接続のみになります。
		このコマンドを設定しない限り、デフォルトの ACL **sl_def_acl** はデバイス上に作成されます。この ACL は実行コンフィギュレーションでは非表示です。デフォルトの ACL のパラメータを表示するには、**show access-list sl_def_acl** を使用します。
		次に例を示します。
		`Device# show access-lists sl_def_acl`
		`Extended IP access list sl_def_acl`
		`10 deny tcp any any eq telnet`
		`20 deny tcp any any eq www`
		`30 deny tcp any any eq 22`
		`40 permit ip any any`

ステップ 5	**login delay** *seconds* 例： `Device(config)# login delay 10`	（任意）連続するログイン試行間の遅延を設定します。
ステップ 6	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**show login failures** 例： `Device# show login`	ログイン パラメータを表示します。 • **failures** ：失敗したログイン試行に関連する情報のみを表示します。

ログイン パラメータの確認

デバイスに適用されたログイン設定と現在のログインステータスを確認するには、次の作業を実行します。

手順

	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	**show login failures** 例： `Device# show login`	ログイン パラメータを表示します。 • **failures** ：失敗したログイン試行に関連する情報のみを表示します。

例

show login コマンドからの次のサンプル出力は、ログインパラメータが指定されていないことを確認します。

```
Device# show login

No login delay has been applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps
Router NOT enabled to watch for login Attacks
```

show login コマンドからの次のサンプル出力は、**login block-for** コマンドが発行されたことを確認します。この例で、コマンドは100秒以内に16回以上のログイン要求が失敗した場合、ログイン ホストを100秒ブロックするように設定されています。すでに5回のログイン要求が失敗しています。

```
Device# show login

A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.
Router enabled to watch for login Attacks.
If more than 15 login failures occur in 100 seconds or less, logins will be disabled for
 100 seconds.
Router presently in Watch-Mode, will remain in Watch-Mode for 95 seconds.
Present login failure count 5.
```

show login コマンドからの次のサンプル出力は、デバイスが待機モードになっていることを確認します。この例で、**login block-for** コマンドは、100 秒以内に 3 回以上のログイン要求が失敗した場合、ログインホストを 100 秒ブロックするように設定されています。

```
Device# show login

A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.
Router enabled to watch for login Attacks.
If more than 2 login failures occur in 100 seconds or less, logins will be disabled for
 100 seconds.
Router presently in Quiet-Mode, will remain in Quiet-Mode for 93 seconds.
Denying logins from all sources.
```

show login failures コマンドからの次のサンプル出力は、デバイス上で失敗したすべてのログイン試行を表示します。

```
Device# show login failures

Information about login failure's with the device
Username      Source IPAddr  lPort Count  TimeStamp
try1          10.1.1.1        23    1     21:52:49 UTC Sun Feb 24 2019
try2          10.1.1.2        23    1     21:52:52 UTC Sun Feb 23 2019
```

show login failures コマンドからの次のサンプル出力は、現在記録されている情報がないことを確認します。

```
Device# show login failures

*** No logged failed login attempts with the device.***
```

ログイン拡張機能の設定例：ログインブロック

例：ログインパラメータの設定

次に、100 秒以内に 15 回ログイン要求が失敗した場合に 100 秒の待機モードに入るようにデバイスを設定する例を示します。待機時間中、ACL「myacl」からのホスト以外、すべてのログイン要求が拒否されます。

```
Device> enable
Device# configure terminal
Device(config)# login block-for 100 attempts 15 within 100
Device(config)# login quiet-mode access-class myacl
Device(config)# end
```

ログイン拡張機能の機能履歴：ログインブロック

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Gibraltar 16.11.1	ログイン拡張機能: ログインブロック	ログイン拡張機能であるログインブロック機能により、ユーザーは、DoS 攻撃の可能性が検出されたときに、それ以降のログイン試行を自動的にブロックするオプションを設定することにより、ルータのセキュリティを強化できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。

ログイン拡張機能の機能履歴：ログインブロック