

セキュアファイアウォールASAでのリモートアクセスVPNの脅威検出の設定

内容

[はじめに](#)

[背景説明](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[内部のみの\(無効な\)VPNサービスへの接続試行の脅威の検出](#)

[リモートアクセスVPNクライアント開始攻撃の脅威検出](#)

[リモートアクセスVPN認証障害の脅威検出](#)

[確認](#)

[関連情報](#)

はじめに

このドキュメントでは、Cisco Secure Firewall ASAでリモートアクセスVPN(RVPN)の脅威検出機能を設定するプロセスについて説明します。

背景説明

リモートアクセスVPNサービスの脅威検出機能を使用すると、次のシナリオから保護できます。

1. リモートアクセスVPNサービスを無効にしようとしています。つまり、内部使用のみを目的としたサービスへの接続が試行されます。
2. クライアント開始攻撃。攻撃者が開始するが、リモートアクセスVPNヘッドエンドへの接続試行を完了しない場合に、1台のホストから何度も攻撃を受けます。
3. VPNサービスにリモートアクセスするための認証の試みが繰り返し失敗する(ユーザ名/パスワードのブルートフォーススキャン攻撃)。

これらの攻撃は、アクセスの試行が失敗した場合でも、計算リソースを消費し、有効なユーザがリモートアクセスVPNサービスに接続できなくなる可能性があります。

これらのサービスを有効にすると、設定されたしきい値を超えたホスト(IPアドレス)は、セキュアファイアウォールによって自動的に排除され、IPアドレスの排除を手動で削除するまで、それ以上の試行は行われません。

 **注:** リモートアクセスVPNのすべての脅威検出サービスは、デフォルトで無効になっています。

前提条件

次の項目に関する知識があることが推奨されます。

- Ciscoセキュアファイアウォール適応型セキュリティアプライアンス(ASA)
- ASAでのリモートアクセスVPN(RAVPN)

要件

これらの脅威検出機能は、次に示すバージョンのCisco Secure Firewall ASAでサポートされています。

- 9.16バージョン群 -> 9.16(4)67以降でサポート
- 9.20バージョン群 -> 9.20(3)以降でサポート

使用するコンポーネント

このドキュメントで説明する情報は、次のハードウェアとソフトウェアのバージョンに基づくものです。

- Cisco Secure Firewall ASAバージョン9.20(3)

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、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

グローバルコンフィギュレーションモードでSecure Firewallコマンドラインインターフェイス (CLI)にログインし、リモートアクセスVPNで利用可能な1つ以上の脅威検出サービスを有効にします。

内部のみの（無効な）VPNサービスへの接続試行の脅威の検出

このサービスを有効にするには、`threat detection service invalid-vpn-access`コマンドを実行します。

リモートアクセスVPNクライアント開始攻撃の脅威検出

このサービスを有効にするには、`threat detection service remote-access-client-initiations hold-down <minutes> threshold <count>`コマンドを実行します。値は次のとおりです。

- hold-down <minutes>は、最後の開始試行の後、連続する接続試行がカウントされる期間を定義します。この時間内に連続する接続試行回数が設定されたしきい値を満たすと、攻撃者のIPv4アドレスは排除されます。この期間は1 ~ 1440分の間で設定できます。
- threshold <count>は、ホールドダウン期間に回避をトリガーするために必要な接続試行数です。しきい値は5 ~ 100の間で設定できます。

たとえば、ホールドダウン期間が10分で、しきい値が20の場合、任意の10分のスパン内で20回連続して接続試行が行われると、IPv4アドレスは自動的に排除されます。

 注：ホールドダウンおよびしきい値を設定する際には、NATの使用率を考慮してください。同じIPアドレスからの多くの要求を許可するPATを使用する場合は、より大きい値を考慮します。これにより、有効なユーザが接続するのに十分な時間が確保されます。たとえば、ホテルでは、多数のユーザが短期間で接続を試みるすることができます。

リモートアクセスVPN認証障害の脅威検出

このサービスを有効にするには、threat detection service remote-access-authentication hold-down<minutes> threshold <count>コマンドを実行します。値は次のとおりです。

- hold-down <minutes>は、最後に失敗した試行の後、連続する失敗がカウントされる期間を定義します。この期間内に連続する認証の失敗回数が、設定されたしきい値を満たした場合、攻撃者のIPv4アドレスは排除されます。この期間は1 ~ 1440分の間で設定できます。
- threshold <count>は、ホールドダウン期間中に回避をトリガーするために必要な、認証の試行の失敗回数です。しきい値は1 ~ 100の間で設定できます。

たとえば、ホールドダウン期間が10分で、しきい値が20の場合、いずれかの10分スパンで20回連続して認証が失敗すると、IPv4アドレスは自動的に排除されます。

 注：ホールドダウンおよびしきい値を設定する際には、NATの使用率を考慮してください。同じIPアドレスからの多くの要求を許可するPATを使用する場合は、より大きい値を考慮します。これにより、有効なユーザが接続するのに十分な時間が確保されます。たとえば、ホテルでは、多数のユーザが短期間で接続を試みるすることができます。

 注:SAMLによる認証の失敗はまだサポートされていません。

次の設定例では、クライアントの開始と失敗した認証の試行に対して、ホールドダウン期間が10分、しきい値が20のリモートアクセスVPNに使用できる3つの脅威検出サービスを有効にします。

```
threat-detection service invalid-vpn-access
threat-detection service remote-access-client-initiations hold-down 10 threshold 20
threat-detection service remote-access-authentication hold-down 10 threshold 20
```

確認

脅威検出RAVPNサービスの統計情報を表示するには、`show threat-detection service [service] [entries|details]`コマンドを実行します。このサービスが`remote-access-authentication`、`remote-access-client-initiations`、または`invalid-vpn-access`のいずれかである場合。

次のパラメータを追加して、ビューをさらに制限できます。

- `entries` : 脅威検出サービスによって追跡されているエントリのみを表示します。たとえば、認証の試行に失敗したIPアドレスなどです。
- `details` : サービスの詳細とサービスエントリの両方を表示します。

有効になっているすべての脅威検出サービスの統計情報を表示するには、`show threat-detection service`コマンドを実行します。

```
ciscoasa# show threat-detection service
Service: invalid-vpn-access
  State      : Enabled
  Hold-down  : 1 minutes
  Threshold  : 1
  Stats:
    failed    :          0
    blocking  :          0
    recording :          0
    unsupported :          0
    disabled  :          0
  Total entries: 0
Service: remote-access-authentication
  State      : Enabled
  Hold-down  : 10 minutes
  Threshold  : 20
  Stats:
    failed    :          0
    blocking  :          1
    recording :          4
    unsupported :          0
    disabled  :          0
  Total entries: 2
Name: remote-access-client-initiations
  State      : Enabled
  Hold-down  : 10 minutes
  Threshold  : 20
  Stats:
    failed    :          0
    blocking  :          0
    recording :          0
    unsupported :          0
    disabled  :          0
  Total entries: 0
```

リモートアクセス認証サービスで追跡される潜在的な攻撃者の詳細を表示するには、show threat-detection service <service> entriesコマンドを実行します。

```
ciscoasa# show threat-detection service remote-access-authentication entries
Service: remote-access-authentication
Total entries: 2
```

Idx	Source	Interface	Count	Age	Hold-down	
1	192.168.100.101/ 32	outside		1	721	0
2	192.168.100.102/ 32	outside		2	486	114

Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.

特定の脅威検出リモートアクセスVPNサービスの一般的な統計情報と詳細を表示するには、show threat-detection service <service> detailsコマンドを実行します。

```
ciscoasa# show threat-detection service remote-access-authentication details
Service: remote-access-authentication
```

```
State      : Enabled
Hold-down  : 10 minutes
Threshold  : 20
```

Stats:

```
failed      : 0
blocking    : 1
recording    : 4
unsupported  : 0
disabled    : 0
```

Total entries: 2

Idx	Source	Interface	Count	Age	Hold-down	
1	192.168.100.101/ 32	outside		1	721	0
2	192.168.100.102/ 32	outside		2	486	114

Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.

 注：エントリは、脅威検出サービスによって追跡されているIPアドレスのみを表示します。IPアドレスが排除する条件を満たしていると、ブロッキングカウントが増加し、IPアドレスはエントリとして表示されなくなります。

さらに、次のコマンドを使用して、VPNサービスによって適用される排除をモニタし、単一のIPアドレスまたはすべてのIPアドレスの排除を実行できます。

- `show shun [ip_address]`

排除されたホストを表示します。これには、VPNサービスの脅威検出によって自動的に排除されたホストや、shunコマンドを使用して手動で排除されたホストも含まれます。オプションで、指定したIPアドレスにビューを制限できます。

- `no shun ip_address [インターフェイスif_name]`

指定したIPアドレスからのみ回避を削除します。アドレスが複数のインターフェイスで回避され、一部のインターフェイスで回避を設定しておく場合は、回避のインターフェイス名をオプションで指定できます。

- `clear shun`

すべてのIPアドレスおよびすべてのインターフェイスから回避を削除します。

 注:VPNサービスの脅威検出によって排除されたIPアドレスは、`show threat-detection shun`コマンドでは表示されません。これはスキャンの脅威検出だけに適用されます。

リモートアクセスVPNの脅威検出サービスに関連する各コマンド出力と利用可能なsyslogメッセージの詳細については、『[Cisco Secure Firewall ASA Firewall CLIコンフィギュレーションガイド、9.20](#)』を参照してください。 [章：脅威検出](#) 文書

関連情報

- 詳細については、Technical Assistance Center(TAC)にお問い合わせください。有効なサポート契約([シスコワールドワイドサポートの連絡先](#))が必要です。
- また、Cisco VPN [コミュニティ](#)にもアクセスできます。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。