Application Visibility and Control

以下のトピックでは、Application Visibility and Control（AVC）を有効にして設定する方法について説明します。AVC を使用すると、IP アドレスとポートだけでなく、アプリケーションに基づいてアクセス制御ルールを作成できます。また、拡張アクセス制御リスト（ACL）を使用する機能でも AVC を使用できます。

Application Visibility and Control について

アクセス コントロール ルールを使用すると、接続で使用されるアプリケーションに基づいてトラフィックをフィルタリングできます。これは Application Visibility and Control と呼ばれます。このシステムはさまざまアプリケーションを認識できるため、すべての Web アプリケーションをブロックせずに 1 つの Web アプリケーションをブロックする方法を探す必要はありません。

脆弱性データベースおよびネットワークサービス オブジェクト

Application Visibility and Control を有効にすると、Threat Defense デバイスで使用されるものと同じ脆弱性データベース（VDB）がダウンロードされます。ダウンロードされると、システムによって以下が自動的に作成されます。

- 各アプリケーションのネットワークサービス オブジェクト。VDB には通常、4,000 を超える定義済みアプリケーションが含まれています。各アプリケーションには、名前、アプリケーションカテゴリ、説明、アプリケーション ID、および関連するドメイン名のリストが含まれています。

- 各アプリケーションカテゴリのネットワークサービス オブジェクト グループ。VDB には通常、60 を超える定義済みカテゴリが含まれています。

AVC オブジェクトはダイナミック ネットワークサービス オブジェクトまたはグループとして作成されるため、実行コンフィギュレーションには保存されません。VDB で作成されたダイナミックオブジェクトを組み込むカスタム ネットワークサービス グループを作成することで、独自のカテゴリを作成することも可能です。

その後、アクセス制御ルールかその他の拡張 ACL で AVC またはカスタム ネットワークサービス グループを使用できます。

システムは更新された VDB を毎週ダウンロードします。いつでも強制的にダウンロードを実行できます。ダウンロードすると既存のオブジェクトが更新されます。これらのオブジェクトを使用するアクセス制御ルールかその他の ACL は、更新されたオブジェクトを自動的に使用します。

接続におけるアプリケーションの決定

システムは運用上、接続を AVC ベースのアクセス制御エントリと正しく照合できるように、次の手法を使用して、接続で使用されるアプリケーションをドメイン名に基づいて決定します。システムはこれらの手法を使用して、IPアドレスとアプリケーションを照合するために必要なIPからドメインへのマッピングキャッシュを構築します。高可用性グループでは、キャッシュはスタンバイユニットで複製されます。

- DNS 要求/応答スヌーピング：DNS 要求/応答クエリは、ポート UDP/53 上にあり、暗号化されていない必要があります。これらのクエリはデバイスを通過する必要があります。ASA をバイパスするパスで DNS 解決が行われる場合、DNS 応答はスヌーピングできません。接続の宛先 IP アドレス/プロトコル/ポートが DNS の IP からドメインへのキャッシュにある場合、接続の最初のパケットにある適切な AVC ベースのアクセス制御エントリと一致させることができます。

- HTTPS 接続用の TLS Client Hello スヌーピング：HTTPS 要求の場合、オプションの SNI フィールドには要求されたサーバーのドメイン名が含まれます。この名前を取得するためのスヌーピングでは、SNI フィールドが存在し、暗号化されていない必要があります。スヌーピングでは、ドメイン名が抽出されて TLS Client Hello パケットの IP アドレスに関連付けられ、DNS スヌーピングキャッシュに追加されます。SNI フィールドは Client Hello ではオプションであるため、スヌーピングに使用できない場合があることに注意してください。このタイプのスヌーピングを使用する場合、アプリケーションIDは接続先サーバーに対する初回接続の最初のパケットではまだ使用できませんが、後続の接続は正しいAVCベースのアクセスルールと一致する必要があります。

- HTTP リクエストヘッダーのホスト名のスヌーピング：HTTP ホストヘッダーにはドメイン名が含まれています。スヌーピングでは、ドメイン名が抽出され、HTTP パケットの接続先の IP アドレスに関連付けられます。このタイプのスヌーピングを使用する場合、アプリケーション ID は接続先サーバーに対する初回接続の最初のパケットではまだ使用できませんが、後続の接続は正しい AVC ベースのアクセスルールと一致する必要があります。

これらの項目を使用できない場合、AVC の分類はできず、すべてのアプリケーションのヒット数がゼロになります。この場合、AVC ルールは正しく機能しません。

（注） コンテンツ配信ネットワーク（CDN）では、IP アドレスが複数のドメインにマッピングされる場合があります。これにより、アプリケーショントラフィックが誤って分類される可能性があるため、接続が誤ったアクセス制御ルールに一致し、誤ってブロックまたは許可されることがあります。DNS スヌーピングキャッシュを表示して、IP アドレスが複数のドメインに一致するかどうかを判断できます。DNS スヌーピングキャッシュのモニタリング （17 ページ） を参照してください。

AVC をサポートする機能

拡張アクセス制御リスト（ACL）をサポートする任意のポリシーで AVC ネットワークサービス オブジェクト グループを使用できます。これには、アクセス制御ルール、QoS ポリシングサービスポリシー規則、その他のサービスポリシー規則、ルートマップなどが含まれます。

ブロックされた接続に関してユーザーに表示される内容

アクセス拒否制御ルールでブロックしているドメイン名にユーザーがアクセスしようとすると、ブラウザに一般的な接続不可エラーページが表示されます。このメッセージで接続の再試行を提案される場合があります。サービスコールを回避するために、ネットワーク上で許可されるアプリケーションと許可されないアプリケーションに関するユーザーの期待事項を設定することをお勧めします。

ユーザーが接続にアプリケーションを使用している場合、表示されるエラーはアプリケーションの動作によって異なります。ユーザーに表示されるエラーページまたはメッセージはカスタマイズできません。

アクセス制御以外のサービスに使用される拡張 ACL に対する AVC ベースの拒否ルールでは、サービスからそれらの接続を単に除外します。これらのアクションは、エンドユーザーに対して透過的である必要があります。

Application Visibility and Control のライセンス

Application Visibility and Control には、次のライセンスが必要です。

- キャリア
- 強力な暗号化（3DES）。スマート ライセンス アカウントで輸出規制対象の機能が許可されている必要があります。

Application Visibility and Control の前提条件

モデルの要件

- Cisco Secure Firewall 6100

Application Visibility and Control のガイドラインと制限事項

ファイアウォール モードのガイドライン

マルチコンテキストモードでは、VDB と関連ファイルがすべてのコンテキストで共有されます。ただし、AVC ネットワークサービス オブジェクトやグループ、およびその他のデータ構造は各コンテキストで作成されます。ユーザーコンテキストごとに AVC を有効にします。

VDB ダウンロードのガイドライン

- 脆弱性データベース（VDB）をダウンロードできるように、support.sourcefire.com に連絡できるインターフェイスで DNS および DNS ルックアップを設定する必要があります。また、そのサーバーへのルートも使用可能である必要があります。
- 高可用性グループでは、スタンバイユニットがデータインターフェイスを介してトラフィックを渡すことができないため、VDB ダウンロードは管理インターフェイスを介して実行できる必要があります。スタンバイユニットは VDB 更新を自らダウンロードします。
- クラスターでは、各ユニットが VDB を個別にダウンロードします。
- マルチコンテキストモードでは、1 つのユーザーコンテキストのみが VDB をダウンロードし、AVC が有効になっているコンテキストと共有します。
- VDB ダウンロードでは HTTPS が使用されるため、セキュアな接続を確保するには、サードパーティ認証局からの信頼できる CA 証明書がデバイスにインストールされている必要があります。
- VDB 更新をダウンロードする場合、ダウンロードが完了すると、既存の AVC ネットワークサービス オブジェクトとグループ、およびその他の AVC ファイルがクリアされ、再構築されます。AVC ベースのポリシーは、更新が完了するまで機能を停止します。
- VDB ダウンロードファイルは約 70 MB です。抽出された VDB には、少なくとも 450 MB のディスク容量が必要です。VDB をダウンロードして抽出するための十分な空き領域がデバイスにあることを確認します。

その他のガイドライン

- DNS スヌーピングに基づく AVC トラフィック分類を機能させるには、DNS インスペクション（デフォルトで有効）を有効にし、DNS の信頼できる送信元を設定する必要があります（**dns trusted-source** コマンド）。
- DNScrypt を有効にしてはなりません。DNScrypt が有効になっている場合、DNS 接続が暗号化されるため、DNS スヌーピングはできません。DNS インスペクションポリシーで **dnscrypt** コマンドが有効になっていないことを確認します。
- DNS スヌーピングは、UDP/53 を介した DNS 要求のみをサポートします。DNS スヌーピングは、TCP/53 または HTTP/HTTPS を介した DNS 要求では機能しません。
- TLS Client Hello および HTTP ヘッダーのスヌーピングでは、トラフィック分類は新たに確認されたアプリケーションの最初のパケットでは完了しません。ただし、アプリケーションを使用する後続の接続は、期待されるルールに一致する必要があります。
- QUIC および DTLS 接続では、IP からドメインへのマッピング情報をスヌーピングできません。

Application Visibility and Control の設定

Application Visibility and Control（AVC）には初期セットアップが必要ですが、機能を有効にすると、通常どおりネットワークサービス オブジェクト グループを使用してアクセス制御ルールと拡張 ACL を作成できます。次の手順では、AVC の有効化と使用に関するすべての側面について説明します。

手順

ステップ 1 キャリア ライセンスを設定し、スマート ライセンス アカウントで輸出規制対象の機能が有効になっていることを確認します。

詳細については、『『ASA General Operations ASDM Configuration Guide』の適切なリリース』の「Licensing」の章を参照してください。

ステップ 2 インターフェイス上で DNS サーバーと DNS ルックアップを設定します。

DefaultDNS グループ（またはカスタムグループ）に DNS サーバーを追加し、アプリケーションの使用状況を検出する各インターフェイスで DNS ルックアップを有効にします。

詳細については、『『ASA General Operations ASDM Configuration Guide』の適切なリリース』の「Basic Settings」の章にある「Configure the DNS Server」の情報を参照してください。

ステップ 3 DNS スヌーピング用の信頼できる DNS サーバーを設定します。

ネットワークサービス オブジェクトに DNS 名が含められると、DNS 要求/応答トラフィックのスヌーピングによって DNS ドメイン名に対応する IP アドレスが収集され、その結果がキャッシュされます。すべての DNS 要求/応答をスヌーピングできます。

セキュリティ上の理由から、信頼する DNS サーバーを定義することで DNS スヌーピングの範囲を制限できます。信頼されていない DNS サーバーへの DNS トラフィックは無視され、ネットワークサービス オブジェクトのマッピングの取得に使用されません。

デフォルトでは、設定および学習されたすべての DNS サーバーが信頼されます。信頼できるリストを制限する場合のみ変更が必要になります。**show dns** コマンドを使用して、現在の DNS の信頼できる送信元設定を確認します。

具体的には、クライアントがドメイン名を解決するために使用する DNS サーバーが信頼できるリストに含まれるようにする必要があります。デフォルト設定では、ユーザー DNS サーバーが DHCP を介して設定される状況に対処できます。ただし、クライアント DNS サーバーを明示的に設定する場合は、それらのサーバーの IP アドレスが信頼できるリストに含まれるようにしてください。

詳細については、「信頼できる DNS サーバの構成」を参照してください。

ステップ 4 DNS インスペクションを設定します。

DNS インスペクションはデフォルトでイネーブルになっています。オフになっている場合は、再度有効にする必要があります。デフォルトの DNS インスペクションのグローバル設定は、AVC に適しています。DNS インスペクションの詳細については、「DNS インスペクション」を参照してください。

ステップ 5 support.sourcefire.com へのルートを設定します。

スタティックルート、またはルーティングプロトコルからの更新に脆弱性データベース（VDB）のダウンロードに使用されるサーバーへのパスが含まれるようにします。HA ユニットの場合、このルートは管理インターフェイスからアクセスできる必要があります。不明な場合は、**ping** を使用してルートが存在することを確認してください。

スタティックルートとルーティングプロトコルの設定方法については、『『ASA General Operations ASDM Configuration Guide』の適切なリリース』を参照してください。

（注）
この機能は、エアギャップネットワークでは動作しません。AVC は、インターネットにアクセスできるネットワークに対してのみ有効です。

ステップ 6 デバイスでサードパーティ CA からの有効なデバイスアイデンティティ証明書を設定します。証明書は、デバイスと VDB ダウンロードサーバー間の接続を検証するために必要です。

ステップ 7 Application Visibility and Control の有効化 （7 ページ）

ステップ 8 カスタム アプリケーション カテゴリの作成 （8 ページ）

ステップ 9 AVC アクセスルールの設定 （9 ページ）

ステップ 10 （オプション）アプリケーション制御が必要な他の機能で AVC オブジェクトを使用します。

任意の拡張 ACL で AVC ベースのネットワークサービス オブジェクト グループを使用できます。それらの ACL は、サービス ポリシー クラス マップ、ルートマップなど、拡張 ACL を使用する任意の機能で使用できます。

拡張 ACL オブジェクトの設定については、「拡張 ACL の設定」を参照してください。また、「AVC アクセスルールの設定 （9 ページ）」で説明されている有意義なルールの設定に関する情報は、一般的な AVC ベースの ACL に適用されます。

ステップ 11 （オプション） VDB の手動ダウンロード （10 ページ）

Application Visibility and Control の有効化

脆弱性データベース（VDB）をダウンロードし、アクセス制御ルールと拡張 ACL で使用できるネットワークサービス オブジェクトおよびグループを作成するには、Application Visibility and Control（AVC）を有効にする必要があります。

（注） 後で AVC を無効化すると、ダウンロードして抽出したすべてのファイルと AVC ネットワークサービス オブジェクトおよびグループが削除されます。

始める前に

「Application Visibility and Control のガイドラインと制限事項 （4 ページ）」に記載されている要件を満たしていることを確認します。要件を満たしていなければ、VDB ダウンロードが失敗する可能性があります。

手順

ステップ 1 **[設定（Configuration）] > [ファイアウォール（Firewall）] > [詳細（Advanced）] > [AVCの有効化（Enable AVC）]** の順に選択します。

ステップ 2 [AVCの有効化（Enable AVC）] を選択します。

ステップ 3 [適用（Apply）] をクリックして、変更内容をデバイスに適用します。

ステップ 4 [AVCステータス（AVC Status）] リンクをクリックして、ステータスページに移動します。VDB がダウンロードされて抽出され、ネットワークサービス オブジェクトおよびグループが作成されるのを待ちます。

モニタリングページには、**[モニタリング（Monitoring）]>[プロパティ（Properties）]>[AVC]>[ステータス（Status）]** の順に選択することでもアクセスできます。

たとえば、次の出力は、システムの準備ができおり、VDB が最新バージョンであることを示しています。

```
AVC (Application Visibility and Control): ENABLED : READY
VDB (containing app definition) download status: UP-TO-DATE
VDB version: current 397, last 0
VDB last update at 15:29:57 UTC Apr 29 2025; last update attempt at 15:27:36 UTC Apr 29
 2025; next update at 15:30:55 UTC May 6 2025.
VDB download link:
```

https://50.19.123.95/auto-update/auto-dl.cgi/Download/files/Cisco_VDB_Fingerprint_Database-4.5.0-397.sh.REL.tar

また、syslog メッセージを使用してステータスを追跡できます。AVC syslog メッセージのモニタリング （18 ページ） を参照してください。

カスタム アプリケーション カテゴリの作成

VDB ダウンロードから作成されたアプリケーションの動的なネットワークサービス オブジェクトを組み込む、新しいネットワークサービス オブジェクト グループを作成できます。他の AVC ネットワークサービス オブジェクト グループと同様に使用します。

カスタム アプリケーション カテゴリの作成は、事前定義済みの AVC カテゴリの一部を許可またはブロックする場合に役に立ちます。たとえば、_gaming_ AVC カテゴリ内のほとんどのアプリケーションをブロックし、カテゴリ内のいくつかのアプリケーションを許可する場合、許可可能なアプリケーションのカスタムカテゴリを作成します。そうすると、カスタムカテゴリを許可するアクセス制御ルールを作成してから AVC _gaming_ カテゴリを許可しないルールを加えることができます。

アクセス制御ルールと拡張ACLでは、ネットワークサービスオブジェクトではなくネットワークサービス グループのみを使用できるため、既存の AVC カテゴリに準拠しないルールを作成する場合は、カスタムカテゴリを作成する必要があります。

手順

ステップ 1 **[構成（Configuration）]>[ファイアウォール（Firewall）]>[オブジェクト（Objects）]>[ネットワークサービスオブジェクト/グループ（Network Services Objects/Groups）]**を選択します。

ステップ 2 次のいずれかを実行します。

- **[追加（Add）] > [ネットワークサービスグループ（Network Service Group）]**を選択し、新しいオブジェクトを追加します。名前を入力し、任意で説明を入力します。
- 既存のオブジェクトを選択し、**[編集（Edit）]** をクリックします。

ステップ 3 既存のサービスオブジェクトをグループに追加します。

a) **[既存のネットワーク サービス オブジェクト（Existing Network-Services Objects）]**を選択します。

b) **[追加（Add）]** をクリックしてオブジェクトをグループに追加します。オブジェクトを削除するには、そのオブジェクトを選択して [削除（Delete）] をクリックします。

c) 必要なすべてのオブジェクトがグループに追加されるまで、このプロセスを繰り返します。

ステップ 4 [OK] をクリックします。

AVC アクセスルールの設定

AVC ネットワークサービス ダイナミック オブジェクト グループと作成するカスタム ネットワークサービス オブジェクト グループを使用して、アクセス コントロール ポリシーで許可ルールとブロックルールを設定します。VDB ダウンロードによってダイナミックオブジェクトおよびグループが変更されると、アクセス制御ルールで自動的に変更が選択され、一致する接続に適用されます。

アプリケーションのルールの一致を判断するために、システムでは接続の送信元と接続先の IP アドレスを使用して、IP アドレスからドメインへのキャッシュ内の関連するドメイン名を検索します。単一の IP アドレスが複数のドメインにマッピングされる場合があることに注意してください。

システムはこの情報をプロトコル/ポートとともに使用して、アプリケーションが含まれているネットワークサービス グループを特定します。次に、アクセス制御ルール（またはアクセス制御以外の機能の一般的な拡張 ACL エントリ）がそれらのグループで検索され、最初の一致が優先されます。したがって、アプリケーションが複数のカテゴリに表示される場合は、ルールセットでそのアプリケーションに目的のアクションが適用されるようにしてください。

始める前に

ルールで使用する AVC ネットワークサービス グループを指定するか、必要なカスタム ネットワークサービス オブジェクト グループを作成します。

この手順は、グローバルアクセス制御ルールまたはインターフェイスベースのアクセス制御ルールがすでに定義されており、既存のアクセスグループにルールを追加することを前提としています。代わりに新たに開始する場合は、「アクセス ルール」を参照してください。

手順

ステップ 1 **[設定（Configuration）]** > **[ファイアウォール（Firewall）]** > **[アクセスルール（Access Rules）]** の順に選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを追加するには、**[追加（Add）]** > **[アクセスルールの追加（Add Access Rule）]** の順に選択します。
- コンテナ内の特定の場所にルールを挿入するには、追加する場所の下にある既存のルールを選択して **[追加（Add）]** > **[挿入（Insert）]** の順に選択するか、**[追加（Add）]** > **[後に挿入（Insert After）]** の順に選択します。
- ルールを編集するには、ルールを選択し、[Edit] をクリックします。

ステップ 3 ルールのプロパティを入力します。選択する主なオプションを次に示します。

- [Interface]：ルールを適用するインターフェイスを指定します。 グローバル ルールを作成する場合は [Any] を選択します。ルーテッド モードのブリッジ グループでは、ブリッジ

仮想インターフェイス（BVI）と各ブリッジグループ メンバーのインターフェイスの両方にアクセス ルールを作成できます。

- [Action]：[Permit] または [Deny]：対象のトラフィックを許可するか拒否（破棄）するかを指定します。
- [Source/Destination criteria]： 送信元（発信アドレス）と宛先（トラフィック フローのターゲット アドレス）を定義します。

  AVC ベースのアクセス制御ルールでは通常、宛先アドレスとしてネットワークサービス オブジェクト グループが使用されます。これは、アプリケーションへの内部ユーザーのアクセスを制御します。

  その他のアドレスには、許可または拒否するアクセスに応じて、**any**、またはより具体的なホストもしくはネットワークのアドレスを使用できます。

ステップ 4 [OK] をクリックします。

VDB の手動ダウンロード

AVC を有効にすると、脆弱性データベース（VDB）が自動的にダウンロードされます。その後、毎週自動的に更新されます。ただし、強制的に更新する必要がある場合は、最新の VDB を手動でダウンロードできます。

始める前に

「Application Visibility and Control のガイドラインと制限事項 （4 ページ）」に記載されている要件を満たしていることを確認します。要件を満たしていなければ、VDB ダウンロードが失敗する可能性があります。

手順

ステップ 1 VDB のダウンロードを開始します。

avc download vdb

例：

```
ciscoasa(config)# avc download vdb
```

ステップ 2 VDB がダウンロードされて抽出され、ネットワークサービス オブジェクトおよびグループが作成されるのを待ちます。

AVC システムのステータスを表示するには、**show avc status** コマンドを使用します。たとえば、次の出力は、システムの準備ができており、VDB が最新バージョンであることを示しています。

```
ciscoasa(config)# show avc status
AVC (Application Visibility and Control): ENABLED : READY
VDB (containing app definition) download status: UP-TO-DATE
VDB version: current 397, last 0
VDB last update at 15:29:57 UTC Apr 29 2025;
last update attempt at 15:27:36 UTC Apr 29 2025; next update at 15:30:55 UTC May 6 2025.
VDB download link: https://50.19.123.95/auto-update/auto-dl.cgi/Download/
files/Cisco_VDB_Fingerprint_Database-4.5.0-397.sh.REL.tar
```

また、syslog メッセージを使用してステータスを追跡できます。AVC syslog メッセージのモニタリング （18 ページ） を参照してください。

Application Visibility and Control のモニタリングとトラブルシューティング

以下のトピックでは、AVC のモニタリングおよびトラブルシューティング方法について説明します。

AVC および VDB ダウンロードステータスのモニタリングとトラブルシューティング

AVC システムのステータスを表示するには、**[モニタリング（Monitoring）]** > **[プロパティ（Properties）]** > **[AVC]** > **[ステータス（Status）]** の順に選択します。

次に例を示します。

```
AVC (Application Visibility and Control): ENABLED : READY
VDB (containing app definition) download status: UP-TO-DATE
VDB version: current 397, last 0
VDB last update at 15:29:57 UTC Apr 29 2025; last update attempt
  at 15:27:36 UTC Apr 29 2025; next update at 15:30:55 UTC May 6 2025.
VDB download link: https://50.19.123.95/auto-update/auto-dl.cgi/
Download/files/Cisco_VDB_Fingerprint_Database-4.5.0-397.sh.REL.tar
```

考えられる AVC のステータスは次のとおりです。

- ENABLED/DISABLED：AVC 機能がオンになっているかどうか。
- READY：脆弱性データベース（VDB）のダウンロードが成功し、アプリケーションとカテゴリが正常に作成されました。AVC を使用できるようになりました。
- NOT READY：VDB のダウンロードまたはアプリケーションとカテゴリの作成で問題が発生しました。VDB ステータスを確認してください。

考えられる VDB ダウンロードのステータスは次のとおりです。

- UP-TO-DATE。VDB のダウンロードが成功し、最新バージョンがインストールされました。

- INITIALIZATION。ダウンロードを開始しています。
- PROGRESSING。ダウンロードが進行中です。
- RETRY。ダウンロードに失敗し、再試行中です。
- FAILED。VDB のダウンロードを 6 回試行しましたが、ダウンロードを実行できませんでした。syslog メッセージで 861003 などの問題の兆候を確認してください。障害の主な理由は次のとおりです。
  - VDB サーバーのドメインが解決されていない。DNS 設定をチェックし、更新が試行されたインターフェイスでドメインのルックアップが有効になっていることを確認します。copy コマンドを試して、ドメイン名が解決されていないことを示す方法で失敗するかどうかを確認します。

```
ciscoasa(config)# copy https://support.sourcefire.com/index.html index.html
Address or name of remote host [support.sourcefire.com]?
?Invalid host address or name
%Error parsing filename (No such device)
```

  - VDB サーバーに到達できない。ルーティング設定を確認し、必要に応じてスタティックルートをインストールします。ルートのインターフェイスが稼働しており、ダウンロードホストへの ping が機能していることを確認します。
  - SSL 検証に失敗した。接続の検証に使用できるサードパーティの CA 証明書をインストールします。ダウンロードが機能していた場合は、使用した証明書の有効期限が切れているかどうかを確認します。
  - デバイスライセンスが強力な暗号化をサポートしていない。この場合、AVC を使用できません。

アプリケーションの使用状況のモニタリング

アプリケーションを使用してアクセスを制御していない場合でも、ネットワークで使用されているアプリケーションを監視できます。

次のページでは、デバイスによって処理された接続で表示されるアプリケーションに関するヒット数の情報を提示できます。

- 最もヒットしたアプリケーションの上位 *n* 個を表示するには、**[モニタリング（Monitoring）] > [プロパティ（Propertie）] > [AVC] > [上位N（Top N）]** の順に選択します。表示するアプリケーションの数を入力し、[OK] をクリックします。
- すべてのアプリケーションのヒット数情報を表示するには、**[モニタリング（Monitoring）] > [プロパティ（Properties）] > [ネットワークオブジェクト（Network Object）] > [オブジェクトグループネットワークサービス（Object Group Network Service）]** の順に選択し、オブジェクト名 _avc_visibility_nsg_ を入力して [検索（Search）] をクリックします。

  次の項目でフィルタ処理できます。

- [すべてのオブジェクト（All Objects）]。ヒット数を問いません。
- [ゼロ以外のオブジェクト（Non-Zero Objects）]。許可されているのかブロックされているのかに関係なく、接続が確認されたアプリケーションのみが表示されます。

  他のネットワークサービス オブジェクト グループ名でも検索できます。

- サービスポリシー規則の一致条件として使用する拡張 ACL でネットワークサービス オブジェクト グループを使用した場合、**[モニタリング（Monitoring）]** > **[プロパティ（Properties）]** > **[サービスポリシー（Service Policy）]** ページでヒット数を表示できます。

アプリケーションの分類のトラブルシューティング

AVC を有効にして VDB が正常にダウンロードされ、AVC ネットワークサービス オブジェクトおよびグループが作成されると、システムがスヌーピングと IP アドレスからドメイン名へのキャッシュの構築を開始します。キャッシュに表示されるアドレスまたはドメインを含む接続が試行/確立されると、アプリケーションのヒット数が増加します。その結果、各接続は、IP アドレスとドメイン名のマッピングに基づいて、特定のアプリケーションに属するように分類されます。

デバイスでトラフィックのスヌーピング、キャッシュの構築、ヒット数に関する情報の収集を行う時間を設けます。そうすると、ヒット数からデバイスが制御するネットワークセグメントでどのアプリケーションが使用されているのかを把握できます。

次のトピックでは、アプリケーションの分類で発生する可能性のある主な問題について説明します。

アプリケーション分類が行われていることの確認

AVC を機能させるには、アプリケーションを分類する必要があります。つまり、IP アドレスをドメイン名にマッピングするために、DNS スヌーピングキャッシュを構築する必要があります。

show avc top *n* コマンドを使用して、一部のアプリケーションにヒット数があることを確認します。たとえば、次のように上位 3 つのアプリケーションを表示することができます。ASDM では、**[モニタリング（Monitoring）]** > **[プロパティ（Properties）]** > **[AVC]** > **[上位N（Top N）]** ページでテーブル内の情報を確認できます。

```
ciscoasa: show avc top 3
AVC: Top 3 App hits
  Application: TikTok, Hit Count: 33950
  Application: GameSpot, Hit Count: 14400
  Application: Facebook, Hit Count: 980
```

どのアプリケーションにもヒット数がない場合、何も分類されず、AVC ベースのルールは動作しなくなります。たとえば、次の場合はアプリケーションが分類されていないことを示しています。

```
ciscoasa# show avc top
```

```
AVC: Top 20 App hits
  Application: ADrive, Hit Count: 0
  Application: Amazon, Hit Count: 0
  ...
  ...
  Application: Dropbox, Hit Count: 0
  Application: eBay, Hit Count: 0
  Application: eBay Bid, Hit Count: 0
```

また、DNS スヌーピングキャッシュで空かどうかを確認することもできます。ASDM では、**[モニタリング（Monitoring）]** > **[プロパティ（Properties）]** > **[DNSキャッシュ（DNS Cache）]** で情報を表示します。

```
ciscoasa# show dns ip-cache
DNS snooping IP cache: 0 in use, 0 most used
Address          Domain                    Idle(sec) Timeout   Hit-count  Source
```

ヒット数がゼロの状況をトラブルシュートするには、次の手順を実行します。

手順

ステップ 1 DNSインスペクションが有効になっており、パケット数がゼロ以外であることを確認します。

```
ciscoasa# show service-policy inspect dns
  Global policy:
   Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns migrated_dns_map_1, packet 0, lock fail 0,
        drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0
        sctp-drop-override 0 message-length maximum client auto, drop 0
```

inspect dns があっても、パケット数がゼロの場合、それはUDP/53のDNS要求/応答トラフィックがデバイスを通過しておらず、スヌーピングするDNSクエリがあることを意味します。

DNS インスペクションが有効になっていない場合は、ここで有効にし、システムが DNS をスヌーピングする時間を設けてから、**show avc top** コマンドを再試行します。

ステップ 2 DNS インスペクションが有効になっており、パケット数がゼロでない場合は、DSNcrypt が有効になっていないことを確認します。

show service-policy inspect dns の出力に次のようなDNScrypt行が含まれている場合、DNScryptは有効です。**dnscrypt** コマンドを **inspect dns** 設定から削除します。

```
DNScrypt egress: rcvd 402, encrypt 402, bypass 0, inject 402
DNScrypt ingress: rcvd 804, decrypt 402, bypass 402, inject 402
DNScrypt: Certificate Update: completion 10, failure 1
```

ステップ 3 DNSインスペクションが有効になっており、パケット数がゼロでない場合は、信頼できるDNSサーバーにクライアントが使用するサーバーが含まれていることを確認します。信頼できるサーバーのリストにクライアントが使用するサーバーが含まれていない場合は、ここで追加します。

show dns コマンドにより、DNS 信頼の現在の状況が表示されます。次の出力は、DNS 信頼がデフォルト設定で設定されていることを示しています。

```
ciscoasa# show dns
INFO: no activated FQDN
DNS Trusted Source enabled for DHCP Server Configured
DNS Trusted Source enabled for DHCP Client Learned
DNS Trusted Source enabled for DHCP Relay Learned
DNS Trusted Source enabled for DNS Server Configured
DNS Trusted Source not enabled for Trust-any
DNS Trusted Source: Type: IPs : Interface : Idle/Timeout (sec)
…
```

デフォルト以外の設定で **dns trusted-source** コマンドを設定している場合は、実行コンフィギュレーションに表示されます。たとえば、次のシンプルなポリシーはすべての DNS サーバーを信頼します。

```
ciscoasa# show running-config dns
  dns domain-lookup management
  DNS server-group DefaultDNS
   name-server 171.70.168.183 management
  dns trusted-source any
```

ステップ 4 DNS サーバー、ルックアップ、およびインスペクションの設定が正しく、DNS クエリがデバイスを通過していないためにインスペクションパケット数がゼロのままの場合、DNS スヌーピングからトラフィック分類を取得できません。代わりに、TLS Client Hello および HTTP リクエスト ホスト ヘッダー スヌーピングに依存する必要があります。

DNS キャッシュが空のままの場合、TLS/HTTP スヌーピングは失敗します。入力インターフェイスでパケットキャプチャを実行し、TLS Client Hello パケットに暗号化されていない SNI フィールドが存在すること、または HTTP トラフィックにホストヘッダーが存在することをチェックすることによって問題を確認できます。

DNS キャッシュが空のままの場合は、DNS クエリがデバイスを通過するようにネットワークを再設計する必要があります。それ以外の場合、このデバイスでは役に立たないため AVC をオフにしてください。

トラフィックの誤分類のトラブルシューティング

アプリケーションが一貫して許可またはブロックされていない場合は、トラフィックの誤分類の問題が起きている可能性があります。この問題は、特定の IP アドレスが異なるドメイン名にマッピングされている可能性があるコンテンツ配信ネットワーク（CDN）で発生する可能性があります。

この問題が発生しているかどうかを確認するには、**show dns ip-cache** コマンドを使用して、IP アドレスが複数のドメインで共有されているかどうかを確認します。ASDM では、**[モニタリング（Monitoring）] > [プロパティ（Properties）] > [DNSキャッシュ（DNS Cache）]** でキャッシュを表示できます。

たとえば、次の出力は、tiktok.com と fidelity.com が同じ IP アドレスにマッピングされていることを示しています。アクセス制御ルールは最終的に IP アドレスによって照合されるため、

あるアプリケーションをブロックする一方で別のアプリケーションを許可する個別のルールがある場合、そのルールは期待どおりに機能しません。別のルールで両方のアプリケーションを許可した場合でも、ルールとアプリケーションのヒット数にはアプリケーションの使用状況は反映されません。

```
ciscoasa(config)# show dns ip-cache
DNS snooping IP cache: 81 in use, 98 most used
Address            Domain                  Idle(sec) Timeout   Hit-count  Source
23.1.106.133       salesforce.com.         2         120       0          DNS
23.67.33.42        fidelity.com.           1         120       42         DNS
                   tiktok.com.             1         120       52         DNS
99.83.221.176      gamespot.com.           8         1495      10         DNS
```

異なる方法で処理する複数のアプリケーションにマッピングされている多数のアドレスがある場合、特定のネットワークで AVC が役に立たない可能性があります。AVC の使用を続行する必要があるかどうかを評価します。

許可されたアプリケーションとブロックされたアプリケーションのモニタリング

アクセス制御ルールによって許可またはブロックされたアプリケーション、およびそのアプリケーションのヒット数を表示するには、**[モニタリング（Monitoring）] > [プロパティ（Properties）] > [AVC] > [許可されたアプリケーションとブロックされたアプリケーション（Allowed and Blocked Applications）]** の順に選択します。[許可（Allowed）] または [ブロック（Blocked）] のオプションボタンをクリックして、関連するアプリケーションのリストを表示します。

アプリケーションのアプリケーションカテゴリの決定

アプリケーションは複数のカテゴリに表示される場合があります。特定のアプリケーションに関しては、**show object network-service** コマンドを使用してカテゴリを確認できます。カテゴリがわかれば、アクセス制御の許可およびブロックルールを設計し、予期しない許可/ブロックの結果をトラブルシュートできます。

たとえば、「Fox News」アプリケーションを表示すると、それが 3 つのカテゴリに属していることが示されます（これは次の VDB のダウンロードで変更される可能性があり、この例は説明のみを目的としています）。

```
ciscoasa# show object network-service "Fox News"
object network-service "Fox News" dynamic (hitcnt=30)
 description Web Portal for news update.
 app-id 1366
 member of: "_multimedia_(tb/video)_" "_web_services_provider_" "_news_"
…
```

アプリケーションカテゴリの表示

ネットワークサービス オブジェクト グループとして定義されているアプリケーションカテゴリのリストを表示するには、**[モニタリング（Monitoring）]** > **[プロパティ（Properties）]** > **[AVC]** > **[アプリケーションカテゴリ（App Category）]** の順に選択します。出力には、行ごとに 1 つのカテゴリが表示されます。リストをフィルタ処理して以下を表示できます。

- [すべてのオブジェクトグループ（All Object Groups）]。ヒット数を問いません。
- [ゼロ以外のオブジェクトグループ（Non-Zero Object Groups）]。許可されているのかブロックされているのかに関係なく、接続が確認されたカテゴリのみが表示されます。

DNS スヌーピングキャッシュのモニタリング

DNS スヌーピングによって作成された DNS IP からドメインへのキャッシュの内容を監視できます。

キャッシュが空の場合、デバイスで DNS スヌーピングが行われていないことを示しています。この問題をトラブルシュートするには、「アプリケーション分類が行われていることの確認（13 ページ）」を参照してください。

キャッシュを監視するには、**[モニタリング（Monitoring）]** > **[プロパティ（Properties）]** > **[DNSキャッシュ（DNS Cache）]** の順に選択します。

各キャッシュエントリの存続可能時間（TTL）は、2 分～ 24 時間の制限内です。DNS 解決で返される TTL が 2 分未満の場合、キャッシュエントリの TTL は 2 分です。DNS TTL が 24 時間を超える場合、キャッシュエントリは 24 時間後に期限切れになります。これらの制限により、一方ではキャッシュ内で過剰に変化することがなくなり、他方ではエントリが失効しなくなります。

AVC ネットワークサービス オブジェクトのリロード

新しいバージョンの VDB がダウンロードされると、AVC ネットワークサービス オブジェクトが再設定されます。AVC ネットワークサービス オブジェクトに問題があると思われる場合は、システムでそれらのオブジェクトを強制的にリロードできます。定義をリロードするには、次のコマンドを使用します。

network-service reload

次に例を示します。

```
ciscoasa# network-service reload
```

システム定義（AVC）とユーザー設定両方のすべてのネットワークサービス オブジェクトを表示するには、**show object network-service detail** コマンドを使用します。

AVC のヒット数と統計のリセット

次の clear コマンドを使用して、AVC を無効にせずにヒット数とその他の統計を 0 にリセットできます。統計をリセットすると、システムで使用されているアプリケーションの新たなビューが表示されます。

- **clear avc**

  ネットワークサービス オブジェクトおよびグループのカウンタを含む、すべての AVC 関連のカウンタをクリアします。次に例を示します。

```
ciscoasa# clear avc
```

- **clear object** ［**id** *object_name* | **network-service**］

  ユーザー定義と AVC 定義両方のネットワークサービス オブジェクトのカウンタをクリアします。名前でオブジェクトを指定するには、**id** キーワードを使用します。**network-service** キーワードを使用すると、パラメータを使用しない場合と同じ結果が得られます。次に例を示します。

```
ciscoasa# clear object network-service
ciscoasa# clear object id ns
```

- **clear object-group** ［**id** *object_name* | **network-service**］

  ユーザー定義と AVC 定義両方のオブジェクトグループのカウンタをクリアします。名前でオブジェクトを指定するには、**id** キーワードを使用します。**network-service** キーワードを使用して、範囲をすべてのネットワークサービス オブジェクト グループに制限します。次に例を示します。

```
ciscoasa# clear object-group network-service
ciscoasa# clear object-group id nsg
```

AVC syslog メッセージのモニタリング

次に、AVC 機能に関連する syslog メッセージを示します。

- 861001: AVC：AVCアプリケーションディレクトリ.app_dataの作成に失敗しました。無効なディレクトリです。（Creating AVC app directory .app_data failed; Invalid directory.）

  AVC データ用のディレクトリを作成できませんでした。テクニカルサポートまでお問い合わせください。

- 861002: AVC：リンクURL_linkからディレクトリ.app_dataへのファイルのダウンロードに成功しました。（Downloading file from link *URL_link* to directory .app_data succeeded.）

  VDB のダウンロードが成功しました。対処不要です。

- 861003: AVC：リンクURL_linkからディレクトリ.app_dataへのファイルのダウンロードに失敗しました。そのようなデバイスはありません。（Downloading file from link *URL_link* to directory .app_data failed; no such device.）

サーバーへのルートがなかったため、VDB のダウンロードに失敗しました。DNS 設定とルーティングテーブルをチェックし、名前を解決できることとルートが存在することを確認します。

- 861004: AVC：ファイルsf.xmlからVDBバージョンを取得できませんでした。VDBバージョンを取得するためのVDB更新署名が見つかりません。（Getting VDB version from file sf.xml failed; Cannot locate the VDB update signature to get VDB version.）

  システムはバージョンファイルをダウンロードし、ダウンロード可能な新しい VDB があるかどうかを確認します。バージョンファイルが破損している可能性があり、システムはファイルからバージョン番号を抽出できません。テクニカルサポートまでお問い合わせください。

- 861005: AVC：ファイルsf.xmlからVDBファイルパスを取得できませんでした。VDBファイルパスを取得するためのVDBファイルパス署名が見つかりません。（Getting VDB file path from file sf.xml failed; Cannot locate the VDB file path signature to get VDB file path.）

  VDB ファイルパス署名が見つかりませんでした。ファイルが破損している可能性があります。テクニカルサポートまでお問い合わせください。

- 861006: AVC：ファイルsf.xmlからVDBファイル名を取得できませんでした。VDBファイル名を取得するためのVDBファイル名トレーラーが見つかりません。（Getting VDB file name from file sf.xml failed; Cannot locate the VDB file name trailer to get VDB file name.）

  VDB ファイル名を抽出できませんでした。ファイルが破損している可能性があります。テクニカルサポートまでお問い合わせください。

- 861007: AVC：ネットワークサービス（アプリケーション）定義ファイル（dynamic-config.json）のロードに失敗しました。ファイルが見つかりません。（Loading network service (app) definition file (dynamic-config.json) failed; file not found.）

  アプリケーションのネットワークサービス オブジェクトを作成できませんでした。VDB のダウンロードを再試行してください。問題が解決しない場合は、テクニカル サポートに問い合わせてください。

- 861008: AVC：ネットワークサービス（アプリケーション）定義ファイル（dynamic-config.json）のロードに成功しました。（Loading network service (app) definition file (dynamic-config.json) success.）

  アプリケーションのネットワークサービス オブジェクトが正常に作成されました。対処不要です。

- 861009: AVC：アプリケーションカテゴリ定義ファイルのロードに失敗しました。VDB sqlite.vdbを開いているときにエラーが発生しました。（Loading app category definition file failed; Opening VDB sqlite.vdb error.）

  アプリケーションカテゴリ定義ファイルを開けませんでした。VDB のダウンロードを再試行してください。問題が解決しない場合は、テクニカル サポートに問い合わせてください。

- 861010: AVC：アプリケーションカテゴリ定義ファイルのロードに関する警告。カテゴリ名アプリケーションID番号に対応するNSが見つかりません。（AVC: Loading app category definition file warning; No corresponding NS found for category *name* app id *number*.）

  アプリケーションカテゴリで指定されたアプリケーション ID を持つアプリケーションが見つかりませんでした。アプリケーションが廃止されている可能性があります。対処不要です。

- 861011: AVC：アプリケーションカテゴリ定義ファイルのロードに成功しました。（Loading app category definition file success.）

  アプリケーションカテゴリ定義ファイルが正常にロードされました。対処不要です。

- 861012: AVC：可視性NSGのインストールに失敗しました。エラー：内部可視性NSGを作成できません。error_string。（AVC: Installing visibility NSG failed; ERROR: cannot create internal visibility NSG; *error_string*.）

  _avc_visibility_nsg_ という名前のアプリケーション可視性ネットワークサービス オブジェクト グループを作成できなかったか、可視性ネットワークサービス グループ（NSG）へのメンバーアプリケーションの追加中にエラーが発生しました。エラー文字列には、エラーの詳細な説明が表示されます。テクニカルサポートまでお問い合わせください。

- 861013: AVC：可視性NSGのインストールに成功しました。（Installing visibility NSG success.）

  アプリケーションカテゴリのネットワークサービス オブジェクト グループが正常に作成されました。処置は不要です。

Application Visibility and Control の履歴

機能名	プラットフォームリリース	説明
Cisco Secure Firewall 6100 の Application Visibility and Control	9.24(1)	アプリケーションの可視性と制御（AVC）を使用すると、IP アドレスとポートだけでなく、アプリケーションに基づいてアクセス制御ルールを作成できます。AVC は脆弱性データベース（VDB）をダウンロードします。このデータベースでは、アクセス制御ルールで使用できるネットワークサービスオブジェクトとグループが作成されます。オブジェクトはさまざまなアプリケーションを定義し、グループはアプリケーションカテゴリを定義します。これにより、IPアドレスやポートを指定せずに、アプリケーションまたは接続のクラス全体を簡単にブロックできます。 次の画面を導入しました。[**Configuration** > **Firewall** > **Advanced** > **Enable AVC**]、[**Monitoring** > **Properties** > **AVC** > **Status**]、[**Monitoring** > **Properties** > **AVC** > **Top N**]、[**Monitoring** > **Properties** > **AVC** > **App Category**]、[**Monitoring** > **Properties** > **AVC** > **Allowed/Blocked Applications**]、[**Monitoring** > **Properties** > **Service Policy**]、[**Monitoring** > **Properties** > **Network Object** > **Object Group Network Service**] サポートされているプラットフォーム： Cisco Secure Firewall 6100

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。

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。

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。

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。