ASA/PIX： ACS を使用している VPN クライアントのパススルー トラフィック アカウンティングの設定例

目次

概要

このドキュメントでは、PIX/ASA と ACS を使用して、VPN Client（IPSec/SSL）をアカウンティングするための設定例を紹介します。 適応型セキュリティ アプライアンスは、適応型セキュリティ アプライアンスを通過する TCP または UDP トラフィックに関するアカウンティング情報を RADIUS または TACACS+ サーバに送信できます。 そのトラフィックがまた認証される場合、AAAサーバはユーザ名によってアカウンティング 情報を維持できます。 トラフィックが認証されない場合、AAAサーバは IP アドレスによってアカウンティング 情報を維持できます。 アカウンティング 情報はとパススルーがセッションのための適応性があるセキュリティ アプライアンス モデル、サービス使用した、および各セッションの期間含んでいますセッション 開始するおよび停止、ユーザ名、バイト数。

このコマンドを使用できる前に最初に **aaa-server コマンド**で AAAサーバを指定して下さい。 アカウンティング 情報はサーバグループのアクティブなサーバにだけ aaa-server プロトコル 設定モードの会計**モード** コマンドを使用して同時会計をイネーブルにしなければ送信 されます。

AAA 会計が exclude コマンド含んでいると同時に同じ 設定で **aaaアカウント一致** コマンドを使用できないし。 **含**および **exclude コマンド**の代りに **match コマンドを**使用することを提案します; **含**および **exclude コマンドは** ASDM によってサポートされません。

この資料は認証のための ACS の IPSec VPN Client/SSL VPN クライアント（Anyconnect）設定の ASA/PIX を使用してリモートアクセス VPN が既になされている仮定し、ときちんとはたらきます。 この資料は方法に ACS で ASA セキュリティ アプライアンス モデルの VPN クライアントのための AAA 会計を設定する焦点を合わせます。

拡大認証（XAUTH）のための Cisco Secure Access Control Server（ACS バージョン 3.2）を使用して Cisco VPN Client（Windows のための 4.x）と PIX 500 シリーズ セキュリティ アプライアンス モデル 7.x 間のリモートアクセスVPN接続を設定する方法について詳細を学ぶために Cisco Secure ACS 認証 の 設定例のための PIX/ASA 7.x および Cisco VPN Client 4.x を参照して下さい。

ASA 8.x を参照して下さい: 棒設定例の公衆インターネット VPN のための AnyConnect VPN Client 詳細を（ASA）8.0.2 を Cisco AnyConnect VPN Client と棒の SSL VPN を行うために適応型セキュリティ アプライアンス（ASA）ソフトウェア設定する方法について学ぶため。

前提条件

要件

VPN クライアントが接続を確立し、エンドツーエンド達できるきちんとことを確かめて下さい。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco ASA 5500 シリーズ 7.x およびそれ以降を実行する
- Cisco Secure ACS 4.x

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たものです。 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。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

関連製品

この資料もソフトウェア バージョン 7.x およびそれ以降の Cisco PIX 500 シリーズ セキュリティ アプライアンス モデルと使用することができます。

表記法

ドキュメント表記の詳細は、『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。

設定

ASA の設定

会計を設定するために、これらのステップを実行して下さい:

1. 適応性があるセキュリティ アプライアンス モデルにユーザ 1 人あたりのアカウント データを提供してほしい場合認証を有効に して下さい。 適応性があるセキュリティ アプライアンス モデルに IP アドレスごとのアカウント データを提供してほしい場合認証を有効に することは必要ではないし、ステップ 2.に進むことができます。
2. **access-list コマンド**を使用する、送信元アドレスを識別し、ほしいトラフィックの宛先アドレスが説明したアクセス リストを作成して下さい。**注:** 認証を設定し、認証されるすべての

トラフィックのためのアカウント データをほしいと思う場合 **AAA認証一致** コマンドと併用するため作成した同じアクセス リストを使用できます。

3. 会計をイネーブルにするために、このコマンドを入力して下さい:`hostname(config)# aaa accounting match` *acl_name interface_name server_group* 各記号の意味は次のとおりです。
   acl_name 引数は **access-list コマンド**で設定 される アクセス リスト名前です。
   interface_name 引数は **nameif** コマンドで設定 される インターフェイス名です。
   server_group 引数は **aaa-server コマンド**で設定 される サーバグループ名前です。**注:** また、使用コマンド内のトラフィックを識別する ） **AAA 会計 include コマンド**（ できますが、同じ 設定で両方のメソッドを使用できません。 詳細については Cisco ASA 5580 適応型セキュリティ アプライアンス コマンドレファレンスを参照して下さい。

これらのコマンドは送信 トラフィックを認証し、承認し、説明します:

ASA

```
!--- Using the aaa-server command, identify your AAA
servers. If you have already !--- identified your AAA
servers, continue to the next step. hostname(config)#
aaa-server AuthOutbound protocol RADIUS hostname(config-
aaa-server-group)# exit !--- Identify the server,
including the AAA server group it belongs to and !---
enter the IP address, Shared key of the AAA Server.
hostname(config)# aaa-server AuthOutbound (inside) host
10.1.1.1 hostname(config-aaa-server-host)# key
TACPlusUauthKey hostname(config-aaa-server-host)# exit
!--- Using the access-list command, create an access
list that identifies the source !--- addresses
anddestination addresses of traffic you want to
authenticate. hostname(config)# access-list TELNET_AUTH
extended permit tcp any any eq telnet !--- Using the
access-list command, create an access list that
identifies the source !--- addresses anddestination
addresses of traffic you want to Authorize and
Accounting. hostname(config)# access-list SERVER_AUTH
extended permit tcp any any !--- configure
authentication, enter this command: hostname(config)#
aaa authentication match TELNET_AUTH inside AuthOutbound
!--- configure authorization, enter this command:
hostname(config)# aaa authorization match SERVER_AUTH
inside AuthOutbound
!--- This command causes the PIX Firewall to send !---
RADIUS accounting packets for RADIUS-authenticated
outbound sessions to the AAA !--- server group named
"AuthOutbound": hostname(config)# aaa accounting match
SERVER_AUTH inside AuthOutbound
```

ACS 設定を使用して説明する RADIUS

CSV ロガーはカンマで分かれるカラムの属性の記録のデータを記録します（ 、 ）。 Microsoft Excel または Microsoft Access のようないろいろなサードパーティ製のアプリケ– ションにこの形式を、インポートできます。 そのようなアプリケーションへの CSV ファイルからのデータのインポート、グラフを準備するか、またはクエリを行うことができた後何時間にユーザがある特定の期間の間にネットワーク ログイン されたか判別のような。 Microsoft Excel のようなサードパーティ製のアプリケ– ションで CSV ファイルを使用する方法についての情報に関してはサードパーティベンダーからのドキュメントを参照して下さい。

ACS サーバ ハード ドライブの CSV ファイルにアクセスできますまたは Webインターフェイス

から CSV ファイルをダウンロードできます。

デフォルトで、ACS はログにユニークであるディレクトリでログファイルを保存します。 CSV ログのログファイルの場所を設定できます。 すべてのログのためのデフォルト ディレクトリは **sysdrive** に常駐します: **\プログラム ファイル\ CiscoSecure ACS vx.x。**

CiscoSecure ACS を CSV を使用して説明する RADIUS を行うために設定するためにこれらのステップを実行して下さい:

1. ナビゲーション バーで System Configuration をクリックします。
2. [Logging] をクリックします。 ログコンフィギュレーション ページは提示されます。
3. **CSV RADIUS 会計を**選択して下さい。
4. **CSV RADIUS 説明 Report チェックボックスへのログが**選択されることを確認して下さい。 それが選択されない場合、それを今選択して下さい。
5. **ログ テーブルへの『Attributes』 を選択**では、RADIUS アカウントログで見たいと思う RADIUS特性が**記録 された Attributes リスト**に現われることを確かめて下さい。 標準 RADIUS属性に加えて、CiscoSecure ACS によって、本名のような、ExtDB 情報提供され、リモートで 記録 される複数の特別な口ギング属性があります。
6. CiscoSecure ACS for Windows サーバを使用している場合（オプションの）、大きい RADIUS 課金ファイルどのくらいの間保たれるか何判別するログファイル 管理を規定できます、ある場合もあり、どこでどのように保存されるか。
7. RADIUS 説明設定への変更を行なう場合、『SUBMIT』 をクリック して下さい。 CiscoSecure ACS は RADIUS に説明設定を作成した変更を保存し、実装されています。

これらのトピックは ACS CSV レポートを表示しダウンロードする方法を記述します:

- CSV ログファイル名前
- CSV レポートの表示
- CSV レポートのダウンロード

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在のところ、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 Secure Access Control Server 4.2 のためのユーザガイド-ロギングおよびレポート
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスに関するサポート ページ
- PIX/ASA： TACACS+ および RADIUS サーバを使用したネットワーク アクセスのカットスルー プロキシの設定例
- Cisco Secure Access Control Server for Windows
- Cisco PIX 500 シリーズ セキュリティ アプライアンス
- テクニカルサポートとドキュメント - Cisco Systems