

ASA/PIX: Pass-through Traffic Accounting for VPN Clients Using ACS Configuration Example

Document ID: 111134

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Related Products
- Conventions

Configure

- ASA Configuration
- RADIUS Accounting Using ACS Configuration

Verify

Troubleshoot

Related Information

Introduction

This document provides a sample configuration for Accounting for VPN Clients (IPsec/SSL) using PIX/ASA with ACS. The adaptive security appliance can send accounting information to a RADIUS or TACACS+ server about any TCP or UDP traffic that passes through the adaptive security appliance. If that traffic is also authenticated, then the AAA server can maintain accounting information by username. If the traffic is not authenticated, the AAA server can maintain accounting information by IP address. Accounting information includes when sessions start and stop, username, the number of bytes that pass through the adaptive security appliance for the session, the service used, and the duration of each session.

Before you can use this command, you must first designate an AAA server with the **aaa-server** command. Accounting information is sent only to the active server in a server group unless you enable simultaneous accounting using the **accounting-mode** command in **aaa-server** protocol configuration mode.

You cannot use the **aaa accounting match** command in the same configuration as the **aaa accounting include** and **exclude** commands. We suggest that you use the **match** command instead of the **include** and **exclude** commands; the **include** and **exclude** commands are not supported by ASDM.

This document assumes that Remote Access VPN using ASA/PIX with IPsec VPN Client/SSL VPN Client (Anyconnect) configuration with ACS for authentication is already made and works properly. This document focuses on how to configure AAA Accounting for VPN Clients on ASA Security Appliance with ACS.

Refer to PIX/ASA 7.x and Cisco VPN Client 4.x for Cisco Secure ACS Authentication Configuration Example in order to learn more about how to set up a remote access VPN connection between a Cisco VPN Client (4.x for Windows) and the PIX 500 Series Security Appliance 7.x using a Cisco Secure Access Control Server (ACS version 3.2) for extended authentication (Xauth).

Refer to ASA 8.x: AnyConnect VPN Client for Public Internet VPN on a Stick Configuration Example in order to learn more about how to set up an Adaptive Security Appliance (ASA) 8.0.2 to perform SSL VPN on a stick with Cisco AnyConnect VPN Client.

Prerequisites

Requirements

Make sure the VPN client is able to establish the connection and reach end to end properly.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ASA 5500 Series that runs 7.x and later
- Cisco Secure ACS 4.x

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Related Products

This document can also be used with the Cisco PIX 500 Series Security Appliance with Software Version 7.x and later.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure

ASA Configuration

To configure accounting, perform these steps:

1. If you want the adaptive security appliance to provide accounting data per user, you must enable authentication. If you want the adaptive security appliance to provide accounting data per IP address, enabling authentication is not necessary and you can continue to step 2.
2. Using the **access-list** command, create an access list that identifies the source addresses and destination addresses of traffic you want accounted.

Note: If you have configured authentication and want accounting data for all the traffic being authenticated, you can use the same access list you created for use with the **aaa authentication match** command.

3. In order to enable accounting, enter this command:

```
hostname(config)# aaa accounting match acl_name interface_name server_group
```

Where:

- ◆ The *acl_name* argument is the access list name set in the **access-list** command.
- ◆ The *interface_name* argument is the interface name set in the **nameif** command.
- ◆ The *server_group* argument is the server group name set in the **aaa-server** command.

Note: Alternatively, you can use the **aaa accounting include** command (which identifies traffic within the command), but you cannot use both methods in the same configuration. See the Cisco ASA 5580 Adaptive Security Appliance Command Reference for more information.

These commands authenticate, authorize, and account for outbound traffic:

```
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 and destination 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 and destination 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
```

RADIUS Accounting Using ACS Configuration

The CSV logger records data for logging attributes in columns separated by commas (.). You can import this format into a variety of third-party applications, such as Microsoft Excel or Microsoft Access. After you import data from a CSV file into such applications, you can prepare charts or perform queries, such as determining how many hours a user was logged into the network during a given period. For information about how to use a CSV file in a third-party application such as Microsoft Excel, see the documentation from the third-party vendor.

You can access the CSV files on the ACS server hard drive or you can download the CSV file from the web interface.

By default, ACS keeps log files in directories that are unique to the log. You can configure the log file location of CSV logs. The default directories for all logs reside in **sysdrive:\Program Files\CiscoSecure ACS vx.x**.

In order to configure CiscoSecure ACS to perform RADIUS accounting using CSV, perform these steps:

1. In the navigation bar, click **System Configuration**.
2. Click **Logging**. The Logging Configuration page appears.
3. Select **CSV RADIUS Accounting**.
4. Confirm that the **Log to CSV RADIUS Accounting report** check box is selected. If it is not selected, select it now.
5. In the **Select Attributes To Log** table, make sure that the RADIUS attributes you want to see in the RADIUS accounting log appear in the **Logged Attributes** list. In addition to the standard RADIUS attributes, there are several special logging attributes provided by CiscoSecure ACS, such as Real Name, ExtDB Info, and Logged Remotely.
6. (Optional) If you are using CiscoSecure ACS for Windows Server, you can specify log file management, which determines how large RADIUS account files can be, how many are retained, for how long, and where they are stored.
7. If you have made changes to RADIUS accounting configuration, click **Submit**. CiscoSecure ACS saves and implements the changes you made to its RADIUS accounting configuration.

These topics describe how to view and download ACS CSV reports:

- [CSV Log File Names](#)
- [Viewing a CSV Report](#)
- [Downloading a CSV Report](#)

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- [User Guide for Cisco Secure Access Control Server 4.2 – Logging and Reports](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances Support Page](#)
- [PIX/ASA : Cut-through Proxy for Network Access using TACACS+ and RADIUS Server Configuration Example](#)
- [Cisco Secure Access Control Server for Windows](#)
- [Cisco PIX 500 Series Security Appliances](#)
- [Technical Support & Documentation – Cisco Systems](#)

