RADIUS Attribute Screening

The RADIUS Attribute Screening feature allows users to configure a list of "accept" or "reject" RADIUS attributes on the network access server (NAS) for purposes such as authorization or accounting.

If a NAS accepts and processes all RADIUS attributes received in an Access-Accept packet, unwanted attributes may be processed, creating a problem for wholesale providers who do not control their customers' authentication, authorization, and accounting (AAA) servers. For example, there may be attributes that specify services to which the customer has not subscribed, or there may be attributes that may degrade service for other wholesale dial users. The ability to configure the NAS to restrict the use of specific attributes has therefore become a requirement for many users.

The RADIUS Attribute Screening feature should be implemented in one of the following ways:

- To allow the NAS to accept and process all standard RADIUS attributes for a particular purpose, except for those on a configured reject list
- To allow the NAS to reject (filter out) all standard RADIUS attributes for a particular purpose, except for those on a configured accept list

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To

find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for RADIUS Attribute Screening

Before configuring a RADIUS accept or reject list, you must enable AAA by using the **aaa new-model**command in global configuration mode.

Restrictions for RADIUS Attribute Screening

NAS Requirements

To enable this feature, your NAS should be configured for authorization with RADIUS groups.

Accept or Reject Lists Limitations

The two filters used to configure accept or reject lists are mutually exclusive; therefore, a user can configure only one access list or one reject list for each purpose, per server group.

Vendor-Specific Attributes

This feature does not support vendor-specific attribute (VSA) screening; however, a user can specify attribute 26 (Vendor-Specific) in an accept or reject list, which accepts or reject all VSAs.

Required Attributes Screening Recommendation

It is recommended that users do not reject the following required attributes:

- For authorization:
  - 6 (Service-Type)
  - 7 (Framed-Protocol)
- For accounting:
  - 4 (NAS-IP-Address)
  - 40 (Acct-Status-Type)
  - 41 (Acct-Delay-Time)
  - 44 (Acct-Session-ID)

If an attribute is required, the rejection is refused, and the attribute is allowed to pass through.

Note The user does not receive an error at the point of configuring a reject list for required attributes because the list does not specify a purpose--authorization or accounting. The server determines whether an attribute is required when it is known what the attribute is to be used for.

Information About RADIUS Attribute Screening

The RADIUS Attribute Screening feature provides the following benefits:

- Users can configure an accept or reject list consisting of a selection of attributes on the NAS for a specific purpose so unwanted attributes are not accepted and processed.
- Users may wish to configure an accept list that includes only relevant accounting attributes, thereby reducing unnecessary traffic and allowing users to customize their accounting data.

How to Screen RADIUS Attributes

Configuring RADIUS Attribute Screening

To configure a RADIUS attribute accept or reject list for authorization or accounting, use the following commands:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authentication ppp default**
4. **aaa authorization network default group** *group-name*
5. **aaa group server radius** *group-name*
6. **server** *ip-address*
7. **authorization** [**accept** | **reject**] *listname*
8. Router(config-sg-radius)# **exit**
9. **radius-server host** {*hostname* | *ip-address*} [**key** *string*
10. **radius-server attribute list** *listname*
11. **attribute** *number number* [*number...*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa authentication ppp default** **Example:** **group** *group-name* **Example:** `Router(config)# aaa authentication ppp default group radius-sg`	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
Step 4	**aaa authorization network default group** *group-name* **Example:** `Router(config)# aaa authorization network default group radius-sg`	Sets parameters that restrict network access to the user.
Step 5	**aaa group server radius** *group-name* **Example:** `Router(config)# aaa group server radius radius-sg`	Groups different RADIUS server hosts into distinct lists and distinct methods.
Step 6	**server** *ip-address* **Example:** `Router(config-sg-radius)# server 10.1.1.1`	Configures the IP address of the RADIUS server for the group server,
Step 7	**authorization** [**accept** | **reject**] *listname* **Example:** `and/or`	Specifies a filter for the attributes that are returned in an Access-Accept packet from the RADIUS server. and/or Specifies a filter for the attributes that are to be sent to the RADIUS server in an accounting request.

	Command or Action	Purpose
	Example: **accounting** [**accept** | **reject**] *listname* **Example:** `Router(config-sg-radius)# authorization accept min-author`	**Note** The **accept** keyword indicates that all attributes are rejected except for the attributes specified in the *listname*. The **reject** keyword indicates that all attributes are accepted except for the attributes specified in the *listname* and all standard attributes.
Step 8	Router(config-sg-radius)# **exit**	Exits server-group configuration mode.
Step 9	**radius-server host** {*hostname* | *ip-address*} [**key** *string* **Example:** `Router(config)# radius-server host 10.1.1.1 key mykey1`	Specifies a RADIUS server host.
Step 10	**radius-server attribute list** *listname* **Example:** `Router(config)# radius-server attribute list min-author`	Defines the list name given to the set of attributes defined in the **attribute** command and enters server-group configuration mode. **Note** The *listname* must be the same as the *listname* defined in Step 5.
Step 11	**attribute** *number number* [*number...*]] **Example:** `Router(config-sg-radius)# attribute 6-7`	Adds RADIUS attributes to the configured accept or reject list. See the " RADIUS Attributes Overview and RADIUS IETF Attributes " feature module for more information. **Note** This command can be used multiple times to add attributes to an accept or reject list. **Note** The user-password (RADIUS attribute 2) and nas-ip (RADIUS attribute 4) attributes can be filtered together successfully in the access request if they are configured to be filtered. An access request must contain either a user-password or a CHAP password or a state. Also, either a NAS IP address or NAS identifier must be present in a RADIUS accounting request.

Verifying RADIUS Attribute Screening

To verify an accept or reject list, use one of the following commands in privileged EXEC mode:

Command	Purpose
`Router#` **debug aaa accounting**	Displays information on accountable events as they occur.
`Router#` **debug aaa authentication**	Displays information on AAA authentication.
`Router#` **show radius statistics**	Displays the RADIUS statistics for accounting and authentication packets.

Configuration Examples for RADIUS Attribute Screening

Authorization Accept Example

The following example shows how to configure an accept list for attribute 6 (Service-Type) and attribute 7 (Framed-Protocol); all other attributes (including VSAs) are rejected for RADIUS authorization.

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
server 10.1.1.1
authorization accept min-author
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list min-author
attribute 6-7
```

Accounting Reject Example

The following example shows how to configure a reject list for attribute 66 (Tunnel-Client-Endpoint) and attribute 67 (Tunnel-Server-Endpoint); all other attributes (including VSAs) are accepted for RADIUS accounting.

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
server 10.1.1.1
accounting reject tnl-x-endpoint
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list tnl-x-endpoint
attribute 66-67
```

Authorization Reject and Accounting Accept Example

The following example shows how to configure a reject list for RADIUS authorization and configure an accept list for RADIUS accounting. Although you cannot configure more than one accept or reject list per server group for authorization or accounting, you can configure one list for authorization and one list for accounting per server group.

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
server 10.1.1.1
authorization reject bad-author
accounting accept usage-only
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list usage-only
attribute 1,40,42-43,46
!
radius-server attribute list bad-author
attribute 22,27-28,56-59
```

Rejecting Required Attributes Example

The following example shows debug output for the **debug aaa accounting** command. In this example, required attributes 44, 40, and 41 have been added to the reject list “standard.”

```
Router# debug aaa authorization
AAA/ACCT(6): Accounting method=radius-sg (radius)
RADIUS: attribute 44 cannot be rejected
RADIUS: attribute 61 rejected
RADIUS: attribute 31 rejected
RADIUS: attribute 40 cannot be rejected
RADIUS: attribute 41 cannot be rejected
```

Additional References

The following sections provide references related to the RADIUS Attribute Screening feature.

Related Documents

Related Topic	Document Title
IOS AAA security features	*Cisco IOS Security Configuration Guide: Securing User Services* , Release 12.4T.
Cisco IOS Security Commands	*Cisco IOS Security Command Reference*
RADIUS	“ Configuring RADIUS ” module.

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this release.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for RADIUS Attribute Screening

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for RADIUS Attribute Screening

Feature Name	Releases	Feature Information
RADIUS Attribute Screening	12.2(1)DX 12.2(2)DD 12.2(4)B 12.2(4)T 12.2(13)T 12.2(33)SRC	The RADIUS Attribute Screening feature allows users to configure a list of "accept" or "reject" RADIUS attributes on the network access server (NAS) for purposes such as authorization or accounting. This feature was introduced in 12.2(1)DX. This feature was integrated into Cisco IOS Release 12.2(2)DD. This feature was integrated into Cisco IOS Release 12.2(4)B. This feature was integrated into 12.2(4)T. This feature was integrated into Cisco IOS Release 12.2(33)SRC. Platform support was added for the Cisco 7401 ASR router. The Cisco 7200 series platform applies to the Cisco IOS Releases 12.2(1)DX, 12.2(2)DD, 12.2(4)B, 12.2(4)T, and 12.2(13)T. The Cisco 7401 ASR platform applies to Cisco IOS Release 12.2(13)T only. The following commands were introduced or modified by this feature: **accounting (server-group configuration), authorization (server-group configuration), attribute (server-group configuration), radius-server attribute list**

Glossary

AAA --authentication, authorization, and accounting. Suite of network security services that provide the primary framework through which access control can be set up on your Cisco router or access server.

attribute --RADIUS Internet Engineering Task Force (IETF) attributes are the original set of 255 standard attributes that are used to communicate AAA information between a client and a server. Because IETF attributes are standard, the attribute data is predefined and well known; thus all clients and servers who exchange AAA information via IETF attributes must agree on attribute data such as the exact meaning of the attributes and the general bounds of the values for each attribute.

NAS --network access server. A Cisco platform (or collection of platforms, such as an AccessPath system) that interfaces between the packet world (for example, the Internet) and the circuit world (for example, the Public Switched Telephone Network).

RADIUS --Remote Authentication Dial-In User Service. RADIUS is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

VSA --vendor-specific attribute. VSAs are derived from one IETF attribute--vendor-specific (attribute 26). Attribute 26 allows a vendor to create and implement an additional 255 attributes. That is, a vendor can create an attribute that does not match the data of any IETF attribute and encapsulate it behind attribute 26: essentially, Vendor-Specific ="protocol:attribute=value".

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.