RADIUS Attribute Value Screening

Last Updated: January 17, 2012

The RADIUS Attribute Value 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 Value 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 feature information and caveats, see 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 document.

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.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for RADIUS Attribute Value Screening

Before configuring a RADIUS accept or reject list, you must enable AAA.

Restrictions for RADIUS Attribute Value 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 Value Screening

The RADIUS Attribute Value 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 Value 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. Router(config)# **aaa authentication ppp default**
4. Router(config)# **aaa authorization network default group** *group-name*
5. Router(config)# **aaa group server radius** *group-name*
6. Router(config-sg-radius)# **server** *ip-address*
7. Router(config-sg-radius)# **authorization** [**accept** | **reject**] *listname*
8. Router(config-sg-radius)# **exit**
9. Router(config)# **radius-server host** {*hostname* | *ip-address*} [**key** *string*
10. Router(config)# **radius-server attribute list** *listname*
11. Router(config-sg-radius)# **attribute** *value1* [*value2* [*value3...*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	Router(config)# **aaa authentication ppp default** **Example:** **group** *group-name*	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
Step 4	Router(config)# **aaa authorization network default group** *group-name*	Sets parameters that restrict network access to the user.
Step 5	Router(config)# **aaa group server radius** *group-name*	Groups different RADIUS server hosts into distinct lists and distinct methods.
Step 6	Router(config-sg-radius)# **server** *ip-address*	Configures the IP address of the RADIUS server for the group server,
Step 7	Router(config-sg-radius)# **authorization** [**accept** | **reject**] *listname* **Example:** `and/or` **Example:** `Router(config-sg-radius)#` **accounting** [**accept** | **reject**] *listname*	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. **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	Router(config)# **radius-server host** {*hostname* | *ip-address*} [**key** *string*	Specifies a RADIUS server host.
Step 10	Router(config)# **radius-server attribute list** *listname*	Defines the list name given to the set of attributes defined in the **attribute** command. **Note** The *listname* must be the same as the *listname* defined in Step 5.
Step 11	Router(config-sg-radius)# **attribute** *value1* [*value2* [*value3...*]]	Adds attributes to the configured accept or reject list. **Note** This command can be used multiple times to add attributes to an accept or reject list.

Verifying RADIUS Attribute Value 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 Value 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 Value Screening feature.

Related Documents

Related Topic	Document Title
RADIUS	“ Configuring RADIUS ” feature module.
Other security features	*Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2
Security commands	*Cisco IOS Security Command Reference*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
None.	To locate and download MIBs for selected platforms, Cisco software 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 feature, and support for existing RFCs has not been modified by this feature.	--

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/cisco/web/support/index.html

Feature Information for RADIUS Attribute Value 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 Value Screening

Feature Name	Releases	Feature Information
RADIUS Attribute Value Screening	Cisco IOS XE Release 2.1	The RADIUS Attribute Value 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. In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers The following commands were introduced or modified by this feature: **accounting (server-group), authorization (server-group), attribute (server-group), radius-server attribute list**