Attribute Screening for Access Requests

The Attribute Screening for Access Requests feature allows you to configure your network access server (NAS) to filter attributes in outbound Access Requests to the RADIUS server for purposes of authentication or authorization.

- Finding Feature Information, page 1
- Prerequisites for Attribute Screening for Access Requests, page 1
- Restrictions for Attribute Screening for Access Requests, page 2
- Information About Attribute Screening for Access Requests, page 2
- How to Configure Attribute Screening for Access Requests, page 2
- Configuration Examples for Attribute Filtering for Access Requests, page 6
- Additional References, page 7
- Feature Information for Attribute Screening for Access Requests, page 9

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.

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 Attribute Screening for Access Requests

- You must be familiar with configuring attribute lists.

Restrictions for Attribute Screening for Access Requests

- Attributes 1 (Username), 2 (User-Password), and 3 (Chap-Password) cannot be filtered.

Information About Attribute Screening for Access Requests

Configuring an NAS to Filter Attributes in Outbound Access Requests

The Attribute Screening for Access Requests feature allows you to configure your NAS to filter attributes in outbound Access Requests to the RADIUS server for purposes of authentication or authorization. The filters can be configured on the NAS, or they can be downloaded via downloadable vendor-specific attributes (VSAs) from the authentication, authorization, and accounting (AAA) server.

The following are some examples of the downloadable VSAs:

```
Cisco:Cisco-Avpair="ppp-authen-type=chap"
Cisco:Cisco-Avpair="ppp-authen-list=group 1"
Cisco:Cisco-Avpair="ppp-author-list=group 1"
Cisco:Cisco-Avpair="vpdn:tunnel-id=B53"
Cisco:Cisco-Avpair="vpdn:ip-addresses=10.0.58.35"
```

Note You must be aware of which attributes you want to filter. Filtering certain key attributes can result in authentication failure (for example, attribute 60 should not be filtered).

How to Configure Attribute Screening for Access Requests

Configuring Attribute Screening for Access Requests

or

accounting [**request** | **reply**] [**accept** | **reject**] *listname*

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server attribute list** *listname*
4. **attribute** *value1* [*value2*[*value3* **...**]]
5. **aaa group server radius** *group-name*
6. Do one of the following:
   - **authorization** [**request** | **reply**][**accept** | **reject**] *listname*
   -
   -
   - **accounting** [**request** | **reply**] [**accept** | **reject**] *listname*

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.
Step 3	**radius-server attribute list** *listname* **Example:** `Router (config)# radius-server attribute list attrlist`	Defines an attribute list.
Step 4	**attribute** *value1* [*value2*[*value3* **...**]] **Example:** `Router (config)# attribute 6-10, 12`	Adds attributes to an accept or reject list.
Step 5	**aaa group server radius** *group-name* **Example:** `Router (config)# aaa group server radius rad1`	Applies the attribute list to the AAA server group and enters server-group configuration mode.

	Command or Action	Purpose

Step 6	Do one of the following:
	• **authorization** [**request** | **reply**][**accept** | **reject**] *listname*
	•
	•
	• **accounting** [**request** | **reply**] [**accept** | **reject**] *listname*
	Example:
	`Router (config-sg-radius)# authorization request accept attrlist`
	Example:
	Example:
	Example:
	`Router (config-sg-radius)# accounting request accept attrlist`
		Filters attributes in outbound Access Requests to the RADIUS server for purposes of authentication or authorization.
		• The **request** keyword defines filters for outgoing authorization Access Requests.
		• The **reply** keyword defines filters for incoming authorization Accept and Reject packets and for outgoing accounting requests.

Configuring a Router to Support Downloadable Filters

To configure your router to support downloadable filters, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authorization template**
4. **aaa authorization network default group radius**
5. **radius-server attribute list** *list-name*
6. **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.
Step 3	**aaa authorization template** **Example:** `Router (config)# aaa authorization template`	Enables usage of a local or remote customer template on the basis of Virtual Private Network (VPN) routing and forwarding (VRF).
Step 4	**aaa authorization network default group radius** **Example:** `Router (config)# aaa authorization network default group radius`	Sets parameters that restrict user access to a network.
Step 5	**radius-server attribute list** *list-name* **Example:** `Router (config)# radius-server attribute list attlist`	Defines an accept or reject list name.
Step 6	**attribute** *value1* [*value2* [*value3*...]] **Example:** `Router (config)# attribute 10-14, 24`	Adds attributes to an accept or reject list.

Troubleshooting Tips

If attribute filtering is not working, ensure that the attribute list is properly defined.

Monitoring and Maintaining Attribute Filtering for Access Requests

To monitor and maintain attribute filtering, you can use the **debug radius**command.

SUMMARY STEPS

1. **enable**
2. **debug radius**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug radius** **Example:** `Router# debug radius`	Displays information associated with RADIUS, including filtering information.

Configuration Examples for Attribute Filtering for Access Requests

Attribute Filtering for Access Requests Example

The following example shows that the attributes 30-31 that are defined in “all-attr” will be rejected in all outbound Access Request messages:

```
aaa group server radius ras
 server 172.19.192.238 auth-port 1745 acct-port 1746
 authorization request reject all-attr
!
.
.
.
radius-server attribute list all-attr
 attribute 30-31
!
.
.
.
```

Attribute Filtering User Profile Example

The following is a sample user profile after attribute filtering has been configured for Access Requests:

```
cisco.com Password = "cisco"
Service-Type = Framed,
Framed-Protocol = PPP,
Cisco:Cisco-Avpair = :1:"rad-serv=172.19.192.87 key rad123",
Cisco:Cisco-Avpair = :1:"rad-serv-filter=authorization request reject range1",
Cisco:Cisco-Avpair = :1:"rad-serv-filter=accounting request reject range1",
Cisco:Cisco-Avpair = "ppp-authen-type=chap"
Cisco:Cisco-Avpair = "ppp-authen-list=group 1",
Cisco:Cisco-Avpair = "ppp-author-list=group 1",
Cisco:Cisco-Avpair = "ppp-acct-list=start-stop group 1",
Cisco:Cisco-Avpair = "vpdn:tunnel-id=B53",
Cisco:Cisco-Avpair = "vpdn:tunnel-type=l2tp",
Cisco:Cisco-Avpair = "vpdn:ip-addresses=10.0.58.35",
Cisco:Cisco-Avpair = "vpdn:l2tp-tunnel-password=cisco"
user2@cisco.com
Service-Type = Outbound,
Cisco:Cisco-Avpair = "vpdn:tunnel-id=B53",
Cisco:Cisco-Avpair = "vpdn:tunnel-type=l2tp",
Cisco:Cisco-Avpair = "vpdn:ip-addresses=10.0.58.35",
Cisco:Cisco-Avpair = "vpdn:l2tp-tunnel-password=cisco"
```

When a session for user2@cisco.com “comes up” at the Layer 2 Tunneling Protocol (L2TP) Network Server (LNS)--as is shown above--because the **aaa authorization template** command has been configured, a RADIUS request is sent to the server for Cisco.com. The server then sends an Access Accept message if authentication is successful, along with the VSAs that are configured as part of the Cisco.com profile. If filters are configured as part of the Cisco.com profile, these filters will be parsed and applied to the RADIUS requests for user2@cisco.com.

In the above profile example, filter range1 has been applied to the authorization and accounting requests.

debug radius Command Example

If the attribute you are trying to filter is rejected, you will see an **debug radius** output statement similar to the following:

```
RADIUS: attribute 31 rejected
```

If you try to filter an attribute that cannot be filtered, you will see an output statement similar to the following:

```
RADIUS: attribute 1 cannot be rejected
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Configuring RADIUS	Configuring RADIUS feature module.
Security commands	*Cisco IOS Security Command Reference*

Standards

Standards	Title
None.	--

MIBs

MIBs	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

RFCs	Title
None	--

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 Attribute Screening for Access Requests

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 Attribute Screening for Access Requests

Feature Name	Releases	Feature Information
Attribute Screening for Access Requests	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.3S	This feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The Attribute Screening for Access Requests feature allows a network access server (NAS) to be configured to filter attributes in outbound Access Requests to the RADIUS server for purposes of authentication or authorization. The following commands were introduced or modified by this feature: **authorization (server-group)**.