

RADIUS Centralized Filter Management

The RADIUS Centralized Filter Management feature introduces a filter-server to simplify ACL configuration and management. This filter-server serves as a centralized RADIUS repository and administration point, which users can centrally manage and configure access control list (ACL) filters.

- Prerequisites for RADIUS Centralized Filter Management, on page 1
- Restrictions for RADIUS Centralized Filter Management, on page 1
- Information About RADIUS Centralized Filter Management, on page 1
- How to Configure Centralized Filter Management for RADIUS, on page 3
- Configuration Examples for RADIUS Centralized Filter Management, on page 6
- Additional References, on page 7
- Feature Information for RADIUS Centralized Filter Management, on page 8

Prerequisites for RADIUS Centralized Filter Management

- You may need to add a dictionary file to your server if it does not support the new RADIUS VSAs. For a sample dictionary and vendors file, see the section “RADIUS Dictionary and Vendors File Example” later in this document.

If you need to add a dictionary file, ensure that your RADIUS server is nonstandard and that it can send the newly introduced VSAs.

- You want to set up RADIUS network authentication so a remote user can dial in and get IP connectivity.

Restrictions for RADIUS Centralized Filter Management

Multiple method lists are not supported in this feature; only a single global filter method list can be configured.

Information About RADIUS Centralized Filter Management

Before the RADIUS Centralized Filter Management feature, wholesale providers (who provide premium charges for customer services such as access control lists [ACLs]) were unable to prevent customers from applying exhaustive ACLs, which could impact router performance and other customers. This feature introduces

a centralized administration point--a filter server--for ACL management. The filter server acts as a centralized RADIUS repository for ACL configuration.

Whether or not the RADIUS server that is used as the filter server is the same server that is used for access authentication, the network access server (NAS) will initiate a second access request to the filter server. If configured, the NAS will use the filter-ID name as the authentication username and the filter server password for the second access request. The RADIUS server will attempt to authenticate the filter-ID name, returning any required filtering configuration in the access-accept response.

Because downloading ACLs is time consuming, a local cache is maintained on the NAS. If an ACL name exists on the local cache, that configuration will be used without consulting the filter server.



Note An appropriately configured cache should minimize delays; however, the first dialin user to require a filter will always experience a longer delay because the ACL configuration is retrieved for the first time.

Cache Management

A global filter cache is maintained on the NAS of recently downloaded ACLs; thus, users no longer have to repeatedly request the same ACL configuration information from a potentially overloaded RADIUS server. Users are required to flush the cache when the following criteria have been met:

- After an entry becomes associated with a newly active call, the idle timer that is associated with that entry will be reset, if configured to do so.
- After the idle-time stamp of an entry expires, the entry will be removed.
- After the global cache of entries reaches a specified maximum number, the entry whose idle-timer is closest to the idle time limit will be removed.

A single timer is responsible for managing all cache entries. The timer is started after the first cache entry is created, and it runs periodically until reboot. The period of the timer will correspond to the minimum granularity offered when configuring cache idle timers, which is one expiration per minute. A single timer prevents users from having to manage individual timers per cache entry.



Note The single timer introduces a lack of precision in timer expiration. There is an average error of approximately 50 percent of the timer granularity. Although decreasing the timer granularity will decrease the average error, the decreased timer granularity will negatively impact performance. Because precise timing is not required for cache management, the error delay should be acceptable.

New Vendor-Specific Attribute Support

This feature introduces support for three new vendor-specific attributes (VSAs), which can be divided into the following two categories:

- User profile extensions

- Filter-Required (50)--Specifies whether the call should be permitted if the specified filter is not found. If present, this attribute will be applied after any authentication, authorization, and accounting (AAA) filter method-list.

- Pseudo-user profile extensions
  - Cache-Refresh (56)--Specifies whether cache entries should be refreshed each time an entry is referenced by a new session. This attribute corresponds to the **cache refresh** command.
  - Cache-Time (57)--Specifies the idle time out, in minutes, for cache entries. This attribute corresponds to the **cache clear age** command.

Note All RADIUS attributes will override any command-line interface (CLI) configurations.

How to Configure Centralized Filter Management for RADIUS

Configuring the RADIUS ACL Filter Server

To enable the RADIUS ACL filter server, use the following command in global configuration mode:

Command	Purpose
`Router(config)# aaa authorization cache filterserver default methodlist[methodlist2...]`	Enables AAA authorization caches and the downloading of an ACL configuration from a RADIUS filter server. • **default** --The default authorization list. • *methodlist* [*methodlist2...*]--One of the keywords listed on the **password** command page.

Configuring the Filter Cache

Follow the steps in this section to configure the AAA filter cache.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Router(config)# **aaa cache filter**
4. Router(config-aaa-filter)# **password 0 7**} *password*
5. Router(config-aaa-filter)# **cache disable**
6. Router(config-aaa-filter)# **cache clear age** *minutes*
7. Router(config-aaa-filter)# **cache refresh**
8. Router(config-aaa-filter)# **cache max** *number*

DETAILED STEPS

Procedure

	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	Router(config)# **aaa cache filter**	Enables filter cache configuration and enters AAA filter configuration mode.
Step 4	Router(config-aaa-filter)# **password 0 7**} *password*	(Optional) Specifies the optional password that is to be used for filter server authentication requests. **0** --Specifies that an unencrypted password will follow. **7** --Specifies that a hidden password will follow. *password* --The unencrypted (clear text) password. **Note** If a password is not specified, the default password ("cisco") is enabled. **Important** This feature is identified as insecure and is a security risk for Cisco devices. Existing deployments continue to function, but new installations require intentional enablement. For more information on remediation, see *Cisco IOS XE Routing Playbook for Resilient Infrastructure*.
Step 5	Router(config-aaa-filter)# **cache disable**	(Optional) Disables the cache.
Step 6	Router(config-aaa-filter)# **cache clear age** *minutes*	(Optional) Specifies, in minutes, when cache entries expire and the cache is cleared. *minutes* --Any value between 0 to 4294967295. **Note** If a time is not specified, the default (1400 minutes [1 day]) is enabled.
Step 7	Router(config-aaa-filter)# **cache refresh**	(Optional) Refreshes a cache entry when a new session begins. This command is enabled by default. To disable this functionality, use the **no cache refresh**command.

	Command or Action	Purpose
Step 8	Router(config-aaa-filter)# **cache max** *number*	(Optional) Limits the absolute number of entries the cache can maintain for a particular server. *number* --The maximum number of entries the cache can contain. Any value between 0 to 4294967295. **Note** If a number is not specified, the default (100 entries) is enabled.

Verifying the Filter Cache

To display the cache status, use the **show aaa cache filterserver** EXEC command. The following is sample output for the **show aaa cache filterserver** command:

```
Router# show aaa cache filterserver
Filter     Server          Age Expires Refresh Access-Control-Lists
-------------------------------------------------------------------------------
aol        10.2.3.4          0    1440     100 ip in icmp drop
                                               ip out icmp drop
                                               ip out forward tcp dstip 1.2.3...
msn        10.3.3.4        N/A   Never       2 ip in tcp drop
msn2       10.4.3.4        N/A   Never       2 ip in tcp drop
vone       10.5.3.4        N/A   Never       0 ip in tcp drop
```

Note The **show aaa cache filterserver** command shows how many times a particular filter has been referenced or refreshed. This function may be used in administration to determine which filters are actually being used.

Troubleshooting Tips

To help troubleshoot your filter cache configurations, use the privileged EXEC **debug aaa cache filterserver** command. To view sample output for the **debug aaa cache filterserver** command, refer to the section "Debug Output Example" later in this document.

Monitoring and Maintaining the Filter Cache

To monitor and maintain filter caches, use at least one of the following EXEC commands:

Command	Purpose
Router# **clear aaa cache filterserver acl** [*filter-name*	Clears the cache status for a particular filter or all filters.
Router# **show aaa cache filterserver**	Displays the cache status.

Configuration Examples for RADIUS Centralized Filter Management

NAS Configuration Example

The following example shows how to configure the NAS for cache filtering. In this example, the server group "mygroup" in contacted first. If there is no response, the default RADIUS server will then be contacted. If there still is no response, the local filters care contacted. Finally, the call is accepted if the filter cannot be resolved.

```
aaa authorization cache filterserver group mygroup group radius local none
!
aaa group server radius mygroup
 server 10.2.3.4
 server 10.2.3.5
!
radius-server host 10.1.3.4
!
aaa cache filter
 password mycisco
 no cache refresh
 cache max 100
!
```

RADIUS Server Configuration Example

The following example is a sample RADIUS configuration that is for a remote user "user1" dialing into the NAS:

```
myfilter Password = "cisco"
Service-Type = Outbound,
Ascend:Ascend-Call-Filter = "ip in drop srcip 10.0.0.1/32 dstip 10.0.0.10/32 icmp",
Ascend:Ascend-Call-Filter = "ip in drop srcip 10.0.0.1/32 dstip 10.0.0.10/32 tcp dstport =
 telnet",
Ascend:Ascend-Cache-Refresh = Refresh-No,
Ascend:Ascend-Cache-Time = 15
user1 Password = "cisco"
Service-Type = Framed,
Filter-Id = "myfilter",
Ascend:Ascend-Filter-Required = Filter-Required-Yes,
```

RADIUS Dictionary and Vendors File Example

The following example is a sample RADIUS dictionary file for the new VSAs. In this example, the dictionary file is for a Merit server.

```
dictionary file:
Ascend.attr Ascend-Filter-Required 50 integer (*, 0, NOENCAPS)
Ascend.attr Ascend-Cache-Refresh   56 integer (*, 0, NOENCAPS)
Ascend.attr Ascend-Cache-Time      57 integer (*, 0, NOENCAPS)
Ascend.value Ascend-Cache-Refresh Refresh-No  0
```

```
Ascend.value Ascend-Cache-Refresh Refresh-Yes 1
Ascend.value Ascend-Filter-Required  Filter-Required-No  0
Ascend.value Ascend-Filter-Required  Filter-Required-Yes 1
vendors file:
50     50
56     56
57     57
```

Debug Output Example

The following is sample output from the **debug aaa cache filterserver** command:

```
Router# debug aaa cache filterserver

AAA/FLTSV: need "myfilter" (fetch), call 0x612DAC64
AAA/FLTSV: send req, call 0x612DAC50
AAA/FLTSV: method SERVER_GROUP myradius
AAA/FLTSV: recv reply, call 0x612DAC50 (PASS)
AAA/FLTSV: create cache
AAA/FLTSV: add attr "call-inacl"
AAA/FLTSV: add attr "call-inacl"
AAA/FLTSV: add attr "call-inacl"
AAA/FLTSV: skip attr "filter-cache-refresh"
AAA/FLTSV: skip attr "filter-cache-time"
AAA/CACHE: set "AAA filtserv cache" entry "myfilter" refresh? no
AAA/CACHE: set "AAA filtserv cache" entry "myfilter" cachetime 15
AAA/FLTSV: add attr to list "call-inacl" call 0x612DAC64
AAA/FLTSV: add attr to list "call-inacl" call 0x612DAC64
AAA/FLTSV: add attr to list "call-inacl" call 0x612DAC64
AAA/FLTSV: PASS call 0x612DAC64
AAA/CACHE: timer "AAA filtserv cache", next in 10 secs (0 entries)
AAA/CACHE: timer "AAA filtserv cache", next in 10 secs (1 entry)
AAA/CACHE: destroy "AAA filtserv cache" entry "myfilter"
AAA/CACHE: timer "AAA filtserv cache", next in 10 secs (0 entries)
```

Additional References

The following sections provide references related to RADIUS Centralized Filter Management.

Related Documents

Related Topic	Document Title
Configuring Authorization	“ Configuring Authorization ” feature module.
Configuring RADIUS	“ Configuring RADIUS ” feature module
Authorization Commands	*Cisco IOS Security Command Reference*

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
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/techsupport

Feature Information for RADIUS Centralized Filter Management

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 Centralized Filter Management

Feature Name	Releases	Feature Information
RADIUS Centralized Filter Management	Cisco IOS XE Release 3.9S	The RADIUS Centralized Filter Management feature introduces a filter-server to simplify ACL configuration and management. This filter-server serves as a centralized RADIUS repository and administration point, which users can centrally manage and configure access control list (ACL) filters. The following commands were introduced or modified by this feature: **aaa authorization cache filterserver**, **aaa cache filter, cache clear age, cache disable, cache refresh**,**clear aaa cache filterserver acl**, **debug aaa cache filterserver**, **password**, **show aaa cache filterserver.**