

Network Access Restrictions

Abstract

Network access restrictions (NARs) provide authorization conditions that have to be met before a user can gain access to the network. Cisco® Secure Access Control Server (ACS) applies these conditions using information from attributes sent by authentication, authorization, and accounting (AAA) clients. Although you may set up NARs in several ways, they all are based on matching attribute information sent by a AAA client. Therefore, you must understand the format and content of the attributes that your AAA clients send if you want to employ NARs effectively.

In setting up a NAR, you must choose whether the filter operates positively or negatively (Table 1). That is, you specify in the NAR whether to permit or deny access from AAA clients that send information that matches the information stored in the NAR. However, if a NAR encounters insufficient information to operate, it defaults to denied access.

Table 1 NAR Permit and Deny Conditions

	Match	No Match	Insufficient Information
Permit	Access granted	Access denied	Access denied
Deny	Access denied	Access granted	Access denied

Cisco Secure ACS supports two basic types of NARs:

- IP-based restrictions in which the originating request relates to an existing IP address
- Non-IP-based filters for all other cases in which automatic number identification (ANI) may be used

IP-based restrictions are based on one of the following attribute fields, depending on the protocol the AAA client uses:

- If you are using TACACS+—The `rem_addr` field is used
- If you are using RADIUS IETF—The `calling-station-id` (attribute 31) and `called-station-id` (attribute 30) fields are used

More information about NAR field interpretation is provided in the TACACS+ and RADIUS sections later in this document.

AAA clients that do not provide sufficient IP-address information (for example, some types of firewalls) do not support all NAR functions.



A non-IP-based NAR is a list of permitted or denied “calling” or “point of access” locations that you may employ in restricting a AAA client when an IP-based connection is not established. The non-IP-based NAR generally uses the calling line ID (CLID) number and the Digital Number Identification Service (DNIS) number (Figures 1 and 2).

However, by entering an IP address instead of the CLI, you may use the non-IP-based filter even when the AAA client does not use a Cisco IOS® Software release that supports CLI or DNIS. In another exception to entering a CLI, you may enter a MAC address to permit or deny access when you are using a Cisco Aironet® AAA client. Likewise, you could enter the Cisco Aironet access point MAC address instead of the DNIS number. The format of what you specify in the CLI box—CLI, IP address, or MAC address—must match the format of what you receive from your AAA client. You can determine this format from your RADIUS accounting log.

When specifying a NAR, you may use an asterisk (*) as a wildcard for any value, or as part of any value, to establish a range. All the values and conditions in a NAR specification must be met for the NAR to restrict access. That is, the values are “ANDed.”

Figure 1
User Interface Snapshot of IP-Based Access Restriction

AAA Client	Port	Address
NDG:ng2-rad	*	*



Figure 2
User Interface Snapshot of DNIS/CLI Access Restriction

Define CL/DNIS-based access restrictions

Table Defines: Permitted Calling/Point of Access Locations

AAA Client	Port	CLI	DNIS
All AAA Clients	*	*	*

AAA Client: All AAA Clients

Port:

CLI:

DNIS:

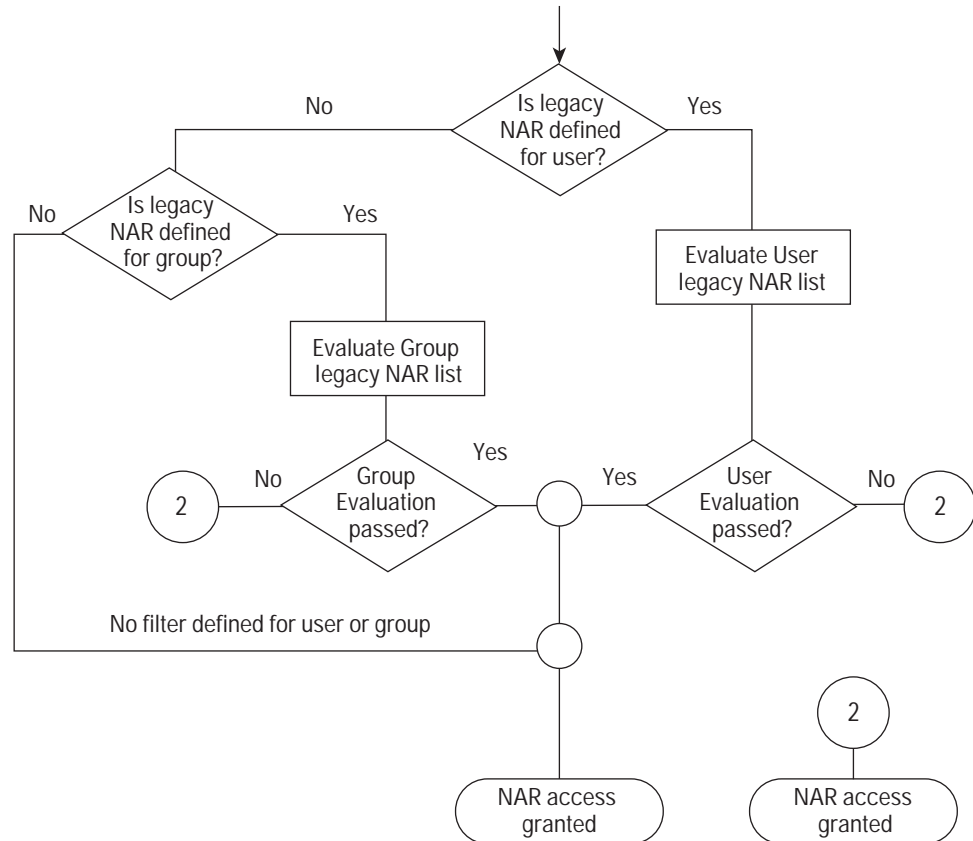
NAR Types

You may define a NAR for, and apply it to, a specific user or user group. For more information about this approach, see [Setting Network Access Restrictions for a User or Setting Network Access Restrictions for a User Group in Cisco Secures ACS online documentation](#). This NAR definition method will be referred to in this document as existing NAR definitions. However, in the Shared Profile Components section of Cisco Secure ACS, you may create and name a shared NAR without directly citing any user or user group. You give the shared NAR a name that can be referenced in other parts of the Cisco Secure ACS HTML interface. Then, when you set up users or user groups, you may select none, one, or multiple shared restrictions to be applied. When you specify the application of multiple shared NARs to a user or user group, choose one of two access criteria: either “All selected filters must permit” or “Any one selected filter must permit.”

The following tables describe the NAR evaluation process result when using Shared Profile Component (SPC). Table 2 describes the result when one or more SPC NARs return “Access granted.” Table 3 describes the result when one or more SPC NAR return access denied.

Table 2 SPC (Shared Profile Component) NAR Conditions when Specific Filter Reports “Access Granted” Results

	Match All (Default Is Success)	Match Any (Default Is Failure)
Permit filter reports Access granted (match at least one entry)	Need to evaluate next filter	Success
Deny filter reports Access granted (did not match all entries)	Failure	Need to evaluate next filter



Logging and Debugging Information

Use failed-attempts or passed-authentications reports to understand why access was or was not granted to a certain user. Usually, the caller ID, network access server (NAS) port, and NAS IP address fields are available and can be used to debug the session.

When the reason for acceptance or denial is unclear, you can add the Filter Information field to these reports (both to failed attempts and passed authentications). This field will provide additional data only when using SPC NARs. (All existing NARs can be easily replaced with SPC NARs.) When you use existing NARs, this field will show the first message (No Filter Activated) regardless of the results.



Table 4 describes all available messages in the Filter-Information-field.

Table 4 Explanation of Messages in Filter Information Field

Messages for SPC NARs in Filter-Information-Field	Success ¹ / Failure	Description
No Filters activated	Success	The Shared Network Access Restrictions was not activated for this user/group (this message doesn't indicate that NAR SPC NAR definition is also not activated)
No Access Filters Passed	Failure	The Shared Network Access Restrictions function was activated for this user or group. The matching policy is that "any one selected NAR results in permit," but none of the NAR filters in the list matched.
All Access Filters Passed	Success	The Shared Network Access Restrictions function was activated for this user or group. The matching policy is that "all selected NARs result in permit," and all NAR filters in the list matched.
No Filters Selected	Success	The Shared Network Access Restrictions function was activated for this user or group, but the filter list is empty.
Failed to evaluate <filter name> <filter entry>	Failure	Evaluation of filter entry <filter entry> in filter <filter name> failed.
Access Filter <filter name> from <id> permitted on Filter Line: <filter entry>. This is sufficient to satisfy an "Any Selected" SPC NAR config.	Success	The Shared Network Access Restrictions function was activated for this user or group. The matching policy is that "any one selected NAR results in permit," where the filter entry <filter entry> matched in filter <filter name> for user/group <id> (and the filter policy is permit). These conditions cause the entire evaluation to pass.
Access Filter <filter name> from <id> did not fail any criteria. This is sufficient to satisfy an "Any Selected" SPC NAR config.	Success	The Shared Network Access Restrictions function was activated for this user or group. The matching policy is that "any one selected NAR results in permit," where the filter entries matched in filter <filter name> for user/group <id> (and the filter policy is deny). These conditions cause the entire evaluation to pass.
Access Filter <filter name> from <id> denied on Filter Line: <line>. This is sufficient to reject an "All Selected" SPC NAR config	Failure	The Shared Network Access Restrictions function was activated for this user or group. The matching policy is that "all selected NARs result in permit," where filter entry <filter entry> matched in filter <filter name> for user/group <id> (and the filter policy is deny). These conditions cause the entire evaluation to fail.
Access Filter <filter name> from <id> did not permit any criteria. This is sufficient to reject an "All Selected" SPC NAR config.	Failure	The Shared Network Access Restrictions function was activated for this user or group. The matching policy is that "all selected NARs result in permit," where none of the filter entries matched in filter <filter name> for user/group <id> (and the filter policy is permit). These conditions cause the entire evaluation to fail.
Access Filter <filter name> from <id> denied Because of lack of required attributes. This is sufficient to reject an "All Selected" SPC NAR config.	Failure	The Shared Network Access Restrictions function was activated for this user or group. The matching policy is that "all selected NARs result in permit," where some of the attributes were missing when matching filter <filter name> for user/group <id>. These conditions cause the entire evaluation to fail.

1. The success/failure result is relevant only to the SPC NAR evaluation process. It might be that if both existing NAR and SPC NAR are used simultaneously, a NAR success message can appear in a failed-attempts report, in which the user passed evaluation for SPC NAR but was denied based on an existing NAR. (The latter determines the result as described in the priority algorithm.)



Filter Selection for TACACS+ Protocol

A TACACS+ session can be matched against IP-based NAR or DNIS/CLI-based NARs. Depending on the user session information, Cisco Secure ACS chooses:

- IP-based NAR when the rem_addr field in the TACACS+ start packet body contains a valid IP address
- DNIS/CLI-based NAR in all other cases

NAR Field Interpretation for TACACS+ Protocol

Tables 5 and 6 describe how Cisco Secure ACS interoperates the different NAR fields when using TACACS+.

Table 5 IP-Based NAR

NAR Field	TACACS+ fields used when evaluating
AAA client	NAS IP address (taken from the source address in the socket between Cisco Secure ACS and the TACACS+ client)
Port	Taken from port field in the TACACS+ start packet body
Address	Taken from the rem_addr field in TACACS+ start packet body

Table 6 DNIS/CLI-Based NAR

NAR entry	TACACS+ fields used when evaluating:
AAA client	NAS IP address (taken from the source address in the socket between Cisco Secure ACS and the TACACS+ client)
Port	Taken from port field in the TACACS+ start packet body
CLI	Taken from the rem_addr field in TACACS+ start packet body
DNIS	Taken from the rem_addr field in TACACS+ start packet body. In cases in which the rem_addr data begins with "/" the DNIS field will contain the rem_addr data without the "/" character

Reference

TACACS+ protocol

Filter Selection for RADIUS Protocol

A RADIUS session can be matched against IP-based NAR or DNIS/CLI-based NARs. Depending on the user session information, Cisco Secure ACS chooses:

- IP-based NAR when the calling-station-id (RADIUS attribute 31) contains a valid IP address
- DNIS/CLI-based NAR in all other cases



NAR Field Interpretation for RADIUS Protocol

Tables 7 and 8 describe how Cisco Secure ACS interoperates the different NAR fields when using RADIUS protocol.

Table 7 IP-Based NAR

NAR Field	Radius fields used when evaluating
AAA client	NAS-IP-Address (RADIUS attribute 4) or, if NAS-IP-Address does not exist, NAS-Identifier (RADIUS attribute 32)
Port	NAS-Port (RADIUS attribute 5) or, if NAS-Port does not exist, NAS-Port-Id (RADIUS attribute 87)
Address	Calling-Station-Id (RADIUS attribute 31)

Table 8 DNIS/CLI-Based NAR

NAR Entry	Radius fields used when evaluating
AAA client	NAS-IP-Address (RADIUS attribute 4) or, if NAS-IP-Address does not exist, NAS-Identifier (RADIUS attribute 32)
Port	NAS-Port (RADIUS attribute 5) or, if NAS-Port does not exist, NAS-Port-Id (RADIUS attribute 87)
CLI	Calling-Station-Id (RADIUS attribute 31)
DNIS	Called-Station-Id (RADIUS attribute 30)

References

RADIUS protocol—RFC2865

RADIUS protocol extensions—RFC2869

List of RADIUS attributes—<http://www.iana.org/assignments/radius-types>

Known Issues with NAR

CSCea35303—Changing the network device group for network access server causes undetermined results

CSCea63816—NAR list size and field size limitation

CSCdz84451—Defining two NAS entries with identical IP address

CSCea28987—Enhancement request to NAR: Use nonsequential IP address definition

CSCea87466—Enhancement request to NAR: Use RADIUS attribute 66/67 in NAR



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, Aironet, and Cisco IOS are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.
(0304R) 203110/ETMG_07/03