NETCONF and RESTCONF Service-Level ACLs

This module describes the service-levels ACLs supported on NETCONF and RESTCONF, and how to configure it.

Information About NETCONF and RESTCONF Service-Level ACLs

Overview of NETCONF and RESTCONF Service-Level ACLs

You can configure an IPv4 or IPv6 access control list (ACL) for NETCONF and RESTCONF sessions. Clients that do not conform to the configured ACLs are not allowed to access the NETCONF or RESTCONF subsystems. When service-level ACLs are configured, NETCONF-YANG and RESTCONF connection requests are filtered based on the source IP address.

If no service-level ACLs are configured, all NETCONF-YANG and RESTCONF connection requests are permitted into the subsystems.

Note Only named ACLs are supported; numbered ACLs are not supported.

How to Configure NETCONF and RESTCONF Service-Level ACLs

Configuring an ACL for a NETCONF-YANG Session

You can either configure an IP access-list or an IPv6 access list for your NETCONF-YANG session.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. • **ip access-list** {**standard** | **extended**} *access-list-name*
   • **ipv6 access-list** *access-list-name*
4. **permit** {*host-address* | *host-name* | **any**} [*wildcard*]
5. **deny** {*host-address* | *host-name* | **any**} [*wildcard*]
6. **exit**
7. **netconf-yang ssh** {{**ipv4** | **ipv6** }**access-list name** *access-list-name*} | **port** *port-number*}
8. **end**

DETAILED STEPS

Procedure

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

Step 3	• **ip access-list** {**standard**	**extended**} *access-list-name*
		• **ipv6 access-list** *access-list-name*
		Example:
		`Device(config)# ip access-list standard acl1_permit`
		`Device(config)# ipv6 access-list ipv6-acl1_permit`
			• Specifies a standard IP access list and enters standard access-list configuration mode.
			• Specifies an IPv6 access list and enters IPv6 access-list configuration mode.

Step 4	**permit** {*host-address*	*host-name*	**any**} [*wildcard*] **Example:** `Device(config-std-nacl)# permit 192.168.255.0 0.0.0.255`	Sets conditions in an IP/IPv6 access list that will permit packets.
Step 5	**deny** {*host-address*	*host-name*	**any**} [*wildcard*] **Example:** `Device(config-std-nacl)# deny any`	Sets conditions in an IP or IPv6 access list that will deny packets.
Step 6	**exit** **Example:** `Device(config-std-nacl)# exit`	Exits standard access-list configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 7	**netconf-yang ssh** {{**ipv4** | **ipv6** }**access-list name** *access-list-name*} | **port** *port-number*} **Example:** `Device(config)# netconf-yang ssh ipv4 access-list name acl1_permit`	Configures an ACL for the NETCONF-YANG session.
Step 8	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring an ACL for a RESTCONF Session

You can either configure an IP access list or an IPv6 access list for your RESTCONF session.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. • **ip access-list** {**standard** \| **extended**} *access-list-name*
   • **ipv6 access-list** *access-list-name*
4. **permit** {*protocol-number* \| *ipv6-source-address* \| *ipv6-source-prefix* \| *protocol*}**any**
5. **deny** {*protocol-number* \| *ipv6-source-address* \| *ipv6-source-prefix* \| *protocol*}**any any**
6. **exit**
7. **restconf** {**ipv4** \| **ipv6** }**access-list name** *access-list-name*
8. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	• **ip access-list** {**standard** | **extended**} *access-list-name* • **ipv6 access-list** *access-list-name* **Example:**	• Specifies a standard IP access list and enters standard access-list configuration mode. • Specifes an IPv6 access list and enters IPv6 access list configuration mode.

	Command or Action	Purpose

	`Device(config)# ip access-list standard acl1_permit`
	
	`Device(config)# ipv6 access-list ipv6-acl1_permit`	

Step 4	**permit** {*protocol-number* | *ipv6-source-address* | *ipv6-source-prefix* | *protocol*} **any** **Example:** `Device(config-ipv6-acl)# permit ipv6 2001:db8::1/32 any`	Sets conditions in an IPv6 access list that will permit packets.
Step 5	**deny** {*protocol-number* | *ipv6-source-address* | *ipv6-source-prefix* | *protocol*} **any any** **Example:** `Device(config-ipv6-acl)# deny ipv6 any any`	Sets conditions in an IPv6 access list that will deny packets.
Step 6	**exit** **Example:** `Device(config-ipv6-acl)# exit`	Exits IPv6 access list configuration mode and returns to global configuration mode.
Step 7	**restconf** {**ipv4** | **ipv6** } **access-list name** *access-list-name* **Example:** `Device(config)# restconf ipv6 access-list name ipv6-acl1_permit`	Configures an ACL for the RESTCONF session.
Step 8	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuration Examples for NETCONF and RESTCONF Service-Level ACLs

Example: Configuring an ACL for a NETCONF Session

```
Device# enable
Device# configure terminal
Device(config)# ip access-list standard acl1_permit
Device(config-std-nacl)# permit 192.168.255.0 0.0.0.255
Device(config-std-nacl)# deny any
Device(config-std-nacl)# exit
Device(config)# netconf-yang ssh ipv4 access-list name acl1_permit
Device(config)# end
```

Example: Configuring an ACL for a RESTCONF Session

```
Device# enable
Device# configure terminal
Device(config)# ipv6 access-list ipv6-acl1_permit
Device(config-ipv6-acl)# permit ipv6 2001:db8::1/32 any
Device(config-ipv6-acl)# deny ipv6 any any
Device(config-ipv6-acl)# exit
Device(config)# restconf ipv6 access-list name ipv6-acl1_permit
Device(config)# end
```

Additional References for NETCONF and RESTCONF Service-Level ACLs

Related Documents

Related Topic	Document Title
NETCONF-YANG	NETCONF Protocol
RESTCONF	RESTCONF Protocol
Programmability commands	*Programmability Command Reference*

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/support

Feature Information for NETCONF and RESTCONF Service-Level ACLs

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 NETCONF and RESTCONF Service-Level ACLs

Feature Name	Releases	Feature Information
NETCONF and RESTCONF Service-Level ACLs	Cisco IOS XE Everest 16.11.1	You can configure an access control list (ACL) for NETCONF and RESTCONF sessions. Clients that do not conform to the configured ACL are not allowed to access the NETCONF or RESTCONF subsystems. The following commands were introduced or modified: **netconf-yang ssh access-list** and **restconf access-list** • Cisco ASR 900 Series Aggregation Services Routers • Cisco ASR 920 Series Aggregated Services Routers (RSP2) • Cisco Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches • Cisco Catalyst 9200 Series Switches • Cisco Catalyst 9300 Series Switches • Cisco Catalyst 9400 Series Switches • Cisco Catalyst 9500 Series Switches • Cisco Catalyst IE 3200, 3300, 3400 Rugged Series • Cisco Embedded Services 3300 Series Switches • Cisco IR1101 Integrated Services Router Rugged • Cisco Network Convergence System 4200 Series • Cisco Network Convergence System 520 Series