Configuring Template ACLs

When user profiles are configured using RADIUS Attribute 242 or vendor-specific attribute (VSA) Cisco-AVPairs, similar per-user access control lists (ACLs) may be replaced by a single template ACL. That is, one ACL represents many similar ACLs. By using template ACLs, you can increase the total number of per-user ACLs while minimizing the memory and Ternary Content Addressable Memory (TCAM) resources needed to support the ACLs.

In networks where each subscriber has its own ACL, it is common for the ACL to be the same for each user except for the user's IP address. The Template ACLs feature groups ACLs with many common access control elements (ACEs) into a single ACL that saves system resources.

- Finding Feature Information, on page 1
- Prerequisites for Template ACLs, on page 1
- Restrictions for Template ACLs, on page 2
- Information About Configuring Template ACLs, on page 2
- How to Configure Template ACLs, on page 5
- Configuration Examples for Template ACLs, on page 7
- Additional References, on page 8
- Feature Information for ACL Template, on page 8

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 Template ACLs

- Cisco ASR 1000 series routers
- Cisco IOS XE Release 2.4 or a later release

Restrictions for Template ACLs

Template ACLs are activated only for per-user ACLs configured through RADIUS Attribute 242 or VSA Cisco-AVPairs (ip:inacl/outacl). No other ACL types are processed by the Template ACL feature.

Template ACL functionality is available only for IPv4 ACLs.

Template ACL functionality is not available for the following types of per-user ACLs:

- Time-based ACLs
- Dynamic ACLs
- Evaluate ACLs
- Reflexive ACLs
- ACLs configured on ISG IP sessions
- IPv6 ACLs

Disabling the Template ACL Feature

When the Template ACL feature is disabled, the system replaces all existing template ACL instances with ACLs. If the system does not have enough resources (in particular TCAM resources) to setup the required number of ACLs, the system generates an error message, and the request to disable the Template ACLs feature fails.

Information About Configuring Template ACLs

Template ACL Feature Design

When the service provider uses AAA servers to configure individual ACLs for each authorized session using with RADIUS attribute 242 or VSA Cisco-AVPairs, the number of sessions can easily exceed the maximum ACL number allowed by the system.

In networks where each subscriber has an ACL, it is common for the ACL to be the same for each user except for the user's IP address. Template ACLs alleviate this problem by grouping ACLs with many common ACEs into a single ACL that compiles faster and saves system resources.

The Template ACL feature is enabled by default, and ACLs set up using the RADIUS attribute 242 or VSA Cisco-AVPairs are considered for template status.

When the Template ACL feature is enabled, the system scans and evaluates all configured per-session ACLs and then creates all required template ACLs.

Disabling Template ACLs

When the Template ACL feature is disabled, the system replaces all existing template ACL instances with ACLs. If the system does not have enough resources (in particular TCAM resources) to setup the required number of ACLs, the system generates an error message, and the request to disable the Template ACL feature fails.

Therefore, before you disable the Template ACL feature, use the **show access-list template summary** command to view the number of template ACLs in the system and ascertain if this number exceeds the system limitations.

When the template ACL feature is disabled, no new ACLS are considered for templating.

Multiple ACLs

When the Template ACL feature is enabled, the system can identify when two per-user ACLS are similar, and the system consolidates the two per-user ACLs into one template ACL.

For example, the following example shows two ACLs for two separate users:

```
ip access-list extended Virtual-Access1.1#1 (PeerIP: 10.1.1.1)
permit igmp any host 10.1.1.1
permit icmp host 10.1.1.1 any
deny ip host 10.31.66.36 host 10.1.1.1
deny tcp host 10.1.1.1 host 10.31.66.36
permit udp any host 10.1.1.1
permit udp host 10.1.1.1 any
permit udp any host 192.168.2.1
permit udp any host 192.168.222.1
permit icmp host 10.55.15.4 host 192.168.2.1
permit udp 10.22.11.0 0.0.0.255 host 192.168.211.2
permit tcp any host 192.168.222.1
permit ip host 10.55.15.4 host 192.168.2.1
permit tcp 10.22.11.0 0.0.0.255 host 192.168.211.2
ip access-list extended Virtual-Access1.1#2 (PeerIP: 10.13.11.2)
permit igmp any host 10.13.11.2
permit icmp host 10.13.11.2 any
deny ip host 10.31.66.36 host 10.13.11.2
deny tcp host 10.13.11.2 host 10.31.66.36
permit udp any host 10.13.11.2
permit udp host 10.13.11.2 any
permit udp any host 192.168.2.1
permit udp any host 192.168.222.1
permit icmp host 10.55.15.4 host 192.168.2.1
permit udp 10.22.11.0 0.0.0.255 host 192.168.211.2
permit tcp any host 192.168.222.1
permit ip host 10.55.15.4 host 192.168.2.1
permit tcp 10.22.11.0 0.0.0.255 host 192.168.211.2
```

With the Template ACL feature is enabled, the system recognizes that these two ACLs are similar, and creates a template ACL as follows:

```
ip access-list extended Template_1
permit igmp any host <PeerIP>
permit icmp host <PeerIP> any
deny ip host 10.31.66.36 host <PeerIP>
deny tcp host <PeerIP> 10.31.66.36
permit udp any host <PeerIP>
permit udp host <PeerIP> any
permit udp any host 192.168.2.1
permit udp any host 192.168.222.1
permit icmp host 10.55.15.4 host 192.168.2.1
permit udp 10.22.11.0 0.0.0.255 host 192.168.211.2
permit tcp any host 192.168.222.1
permit ip host 10.55.15.4 host 192.168.2.1
permit tcp 10.22.11.0 0.0.0.255 host 192.168.211.2
```

In this example, the peer IP address is associated as follows:

- Virtual-Access1.1#1 10.1.1.1
- Virtual-Access1.1#2 10.13.11.2

The two ACLs are consolidated into one template ACL and are referenced as follows:

Virtual-Access1.1#1 maps to Template_1(10.1.1.1)

Virtual-Access1.1#2 maps to Template_1(10.13.11.2)

VSA Cisco-AVPairs

Template ACL processing occurs for ACLs that are configured using Cisco-AVPairs. Only AVPairs that are defined using the ACL number are considered for the templating process.

To be considered for templating, AVPairs for incoming ACLs must conform to the following format:

ip:inacl#number={standard-access-control-list | extended-access-control-list}

For example: ip:inacl#10=deny ip any 10.13.16.0 0.0.0.255

To be considered for templating, AVPairs for outgoing ACLs must conform to the following format:

ip:outacl#number={standard-access-control-list | extended-access-control-list}

For example: ip:outacl#200=permit ip any any

For more information on Cisco-AVPairs, see the Cisco Vendor-Specific AVPair Attributes section of the *Cisco IOS ISG RADIUS CoA Interface Guide*.

RADIUS Attribute 242

Template ACL processing occurs for ACLs that are configured using RADIUS attribute 242. Attribute 242 has the following format for an IP data filter:

Ascend-Data-Filter = “ip <dir> <action> [dstip <dest_ipaddr\subnet_mask>] [srcp <src_ipaddr\subnet_mask>] [<proto> [dstport <cmp> <value>] [srcport <cmp> <value>] [<est>]]”

The table below describes the elements in an attribute 242 entry for an IP data filter.

Table 1: IP Data Filter Syntax Elements

Element	Description
ip	Specifies an IP filter.
<dir>	Specifies the filter direction. Possible values are **in** (filtering packets coming into the router) or **out** (filtering packets going out of the router).
<action>	Specifies the action the router should take with a packet that matches the filter. Possible values are **forward** or **drop**.
dstip <dest_ipaddr\subnet_mask>	Enables destination-IP-address filtering. Applies to packets whose destination address matches the value of **<dest_ipaddr>**. If a subnet mask portion of the address is present, the router compares only the masked bits. If you set **<dest_ipaddr>** to 0.0.0.0, or if this keyword is not present, the filter matches all IP packets.

Element	Description
srcp<src_ipaddr\subnet_mask>	Enables source-IP-address filtering. Applies to packets whose source address matches the value of **<src_ipaddr>**. If a subnet mask portion of the address is present, the router compares only the masked bits. If you set **<src_ipaddr>** to 0.0.0.0, or if this keyword is not present, the filter matches all IP packets.
<proto>	Specifies a protocol specified as a name or a number. Applies to packets whose protocol field matches this value. Possible names and numbers are **icmp** (**1**), **tcp** (**6**), **udp** (**17**), and **ospf** (**89**). If you set this value to zero (0), the filter matches any protocol.
dstport <cmp> <value>	Enables destination-port filtering. This keyword is valid only when **<proto>** is set to **tcp** (**6**) or **udp** (**17**). If you do not specify a destination port, the filter matches any port. **<cmp>** defines how to compare the specified **<value>** to the actual destination port. This value can be <, =, >, or **!**. **<value>** can be a name or a number. Possible names and numbers are **ftp-data (20)**, **ftp (21)**, **telnet (23)**, **nameserver (42)**, **domain (53)**, **tftp (69)**, **gopher (70)**, **finger (79)**, **www (80)**, **kerberos (88)**, **hostname (101)**, **nntp (119)**, **ntp (123)**, **exec (512)**, **login (513)**, **cmd (514)**, and **talk (517)**.
srcport <cmp> <value>	Enables source-port filtering. This keyword is valid only when **<proto>** is set to **tcp**(**6**)or **udp** (**17**). If you do not specify a source port, the filter matches any port. **<cmp>** defines how to compare the specified **<value>** to the actual destination port. This value can be <, =, >, or **!**. **<value>** can be a name or a number. Possible names and numbers are **ftp-data** (**20**), **ftp** (**21**), **telnet**(**23**), **nameserver**(**42**), **domain**(**53**), **tftp**(**69**), **gopher**(**70**), **finger**(**79**), **www**(**80**), **kerberos** (**88**), **hostname** (**101**), **nntp** (**119**), **ntp**(**123**), **exec** (**512**), **login** (**513**), **cmd** (**514**), and **talk** (**517**).
<est>	When set to 1, specifies that the filter matches a packet only if a TCP session is already established. This argument is valid only when **<proto>** is set to **tcp (6)**.

"RADIUS Attribute 242 IP Data Filter Entries" shows four attribute 242 IP data filter entries.

RADIUS Attribute 242 IP Data Filter Entries

```
Ascend-Data-Filter=”ip in drop”
Ascend-Data-Filter=”ip out forward tcp”
Ascend-Data-Filter=”ip out forward tcp dstip 10.0.200.3/16 srcip 10.0.200.25/16
dstport!=telnet”
Ascend-Data-Filter=”ip out forward tcp dstip 10.0.200.3/16 srcip 10.0.200.25/16 icmp”
```

How to Configure Template ACLs

If ACLs are configured using RADIUS Attribute 242 or VSA Cisco-AVPairs, template ACLs are enabled by default.

Configuring the Maximum Size of Template ACLs

By default, template ACL status is limited to ACLs with 100 or fewer rules. However, you can set this limit to a lower number. To set the maximum number of rules that an ACL may have in order to be considered as a template ACL, perform the steps in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list template** *number*
4. **exit**
5. **show access-list template summary**

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	**access-list template** *number* **Example:** `Router(config)# access-list template 50`	Enables template ACL processing. Only ACLs with the specified number of rules (or fewer rules) will be considered for template status.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.
Step 5	**show access-list template summary** **Example:** `Router# show access-list template summary`	(Optional) Displays summary information about template ACLs.

Troubleshooting Tips

The following commands can be used to troubleshoot the Template ACL feature:

- **show access-list template**
- show platform hardware qfp active classification class-group-manager class-group client acl all

- **show platform hardware qfp active feature acl** {**control** | **node** *acl-node-id*}
- show platform software access-list

Configuration Examples for Template ACLs

Example Maximum Size of Template ACLs

The following example shows how to set the maximum number of rules that an ACL may have in order to be considered for template status to 50. Only ACLs whose number of rules is the same as or smaller than 50 are considered for template status.

```
Router> enable

Router# configure terminal

Router(config)# access-list template 50
Router(config)# exit
```

Example Showing ACL Template Summary Information

The following example shows how to view summary information for all ACLs in the system. The output from the command includes the following information:

- Maximum number of rules per template ACL
- Number of discovered active templates
- Number of ACLs replaced by those templates
- Number of elements in the Red-Black tree

```
Router# show access-list template summary
Maximum rules per template ACL = 100
Templates active = 9
Number of ACLs those templates represent = 14769
Number of tree elements = 13
```

Red-Black Tree Elements

The number of tree elements is the number of elements in the Red-Black tree. Each template has 1 unique entry in the Red-Black tree. The system calculates a cyclic redundancy check (CRC) over each ACL masking out the peer IP address and puts the CRC into the Red-Black tree. For example:

Your system has 9 templates (representing 14769 ACLs), and 13 tree elements. If each template has only 1 unique entry in the Red-Black tree, then the additional 4 tree elements means that your system contains 4 per-user ACLs that are not templated.

Example Showing ACL Template Tree Information

The following example shows how to view Red-Black tree information for all ACLs in the system.

The output from the command includes the following information:

- Name of the ACL on the Red-Black tree
- The original CRC32 value
- Number of users of the ACL
- Calculated CRC32 value

```
Router# show access-list template tree
ACL name       OrigCRC    Count   CalcCRC
4Temp_1073741891108       59DAB725    98   59DAB725
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
IP access list commands	*Cisco IOS Security Command Reference*
Configuring IP access lists	"Creating an IP Access List and Applying It to an Interface"

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ACL Template

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 2: Feature Information for ACL Template

Feature Name	Releases	Feature Information
Template ACLs	12.2(28)SB 12.2(31)SB2 Cisco IOS XE Release 2.4	In 12.2(28)SB, this feature was introduced on the Cisco 10000 series router. In 12.2(31)SB2, support was added for the PRE3. In Cisco IOS XE Release 2.4, this feature was implemented on the Cisco ASR 1000 series routers. The following commands were introduced or modified:**access-list template, show access-list template**