



# Sun RPC ALG Support for Firewalls and NAT

The Sun RPC ALG Support for Firewalls and NAT feature adds support for the Sun Microsystems remote-procedure call (RPC) application-level gateway (ALG) on the firewall and Network Address Translation (NAT). Sun RPC is an application layer protocol that enables client programs to call functions in a remote server program. This module describes how to configure the Sun RPC ALG.

- [Finding Feature Information, on page 1](#)
- [Restrictions for Sun RPC ALG Support for Firewalls and NAT, on page 1](#)
- [Information About Sun RPC ALG Support for Firewalls and NAT, on page 2](#)
- [How to Configure Sun RPC ALG Support for Firewalls and NAT, on page 3](#)
- [Configuration Examples for Sun RPC ALG Support for Firewall and NAT, on page 10](#)
- [Additional References for Sun RPC ALG Support for Firewall and NAT, on page 12](#)
- [Feature Information for Sun RPC ALG Support for Firewalls and NAT, on page 13](#)

## 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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

## Restrictions for Sun RPC ALG Support for Firewalls and NAT

- Depending on your release, the following configuration will not work on Cisco ASR 1000 Aggregation Services Routers. If you configure the inspect action for Layer 4 or Layer 7 class maps, packets that match the Port Mapper Protocol well-known port (111) pass through the firewall without the Layer 7 inspection. Without the Layer 7 inspection, firewall pinholes are not open for traffic flow, and the Sun remote-procedure call (RPC) is blocked by the firewall. As a workaround, configure the **match program-number** command for Sun RPC program numbers.
- Only Port Mapper Protocol Version 2 is supported; none of the other versions are supported.
- Only RPC Version 2 is supported.

# Information About Sun RPC ALG Support for Firewalls and NAT

## Application-Level Gateways

An application-level gateway (ALG), also known as an application-layer gateway, is an application that translates the IP address information inside the payload of an application packet. An ALG is used to interpret the application-layer protocol and perform firewall and Network Address Translation (NAT) actions. These actions can be one or more of the following depending on your configuration of the firewall and NAT:

- Allow client applications to use dynamic TCP or UDP ports to communicate with the server application.
- Recognize application-specific commands and offer granular security control over them.
- Synchronize multiple streams or sessions of data between two hosts that are exchanging data.
- Translate the network-layer address information that is available in the application payload.

The firewall opens a pinhole, and NAT performs translation service on any TCP or UDP traffic that does not carry the source and destination IP addresses in the application-layer data stream. Specific protocols or applications that embed IP address information require the support of an ALG.

## Sun RPC

The Sun remote-procedure call (RPC) application-level gateway (ALG) performs a deep packet inspection of the Sun RPC protocol. The Sun RPC ALG works with a provisioning system that allows network administrators to configure match filters. Each match filter defines a match criterion that is searched in a Sun RPC packet, thereby permitting only packets that match the criterion.

In an RPC, a client program calls procedures in a server program. The RPC library packages the procedure arguments into a network message and sends the message to the server. The server, in turn, uses the RPC library and takes the procedure arguments from the network message and calls the specified server procedure. When the server procedure returns to the RPC, return values are packaged into a network message and sent back to the client.

For a detailed description of the Sun RPC protocol, see RFC 1057, *RPC: Remote Procedure Call Protocol Specification Version 2*.

### Sun RPC ALG Support for Firewalls

You can configure the Sun RPC ALG by using the zone-based firewall that is created by using policies and class maps. A Layer 7 class map allows network administrators to configure match filters. The filters specify the program numbers to be searched for in Sun RPC packets. The Sun RPC Layer 7 policy map is configured as a child policy of the Layer 4 policy map with the **service-policy** command.

When you configure a Sun RPC Layer 4 class map without configuring a Layer 7 firewall policy, the traffic returned by the Sun RPC passes through the firewall, but sessions are not inspected at Layer 7. Because sessions are not inspected, the subsequent RPC call is blocked by the firewall. Configuring a Sun RPC Layer 4 class map and a Layer 7 policy allows Layer 7 inspection. You can configure an empty Layer 7 firewall policy, that is, a policy without any match filters.

## Sun RPC ALG Support for NAT

By default, the Sun RPC ALG is automatically enabled when Network Address Translation (NAT) is enabled. You can use the **no ip nat service alg** command to disable the Sun RPC ALG on NAT.

# How to Configure Sun RPC ALG Support for Firewalls and NAT

For Sun RPC to work when the firewall and NAT are enabled, the ALG must inspect Sun RPC packets. The ALG also handles Sun RPC-specific issues such as establishing dynamic firewall sessions and fixing the packet content after NAT translation.

## Configuring the Firewall for the Sun RPC ALG

You must configure a Layer 7 Sun remote-procedure call (RPC) policy map if you have configured the inspect action for the Sun RPC protocol (that is, if you have specified the **match protocol sunrpc** command in a Layer 4 class map).

We recommend that you do not configure both security zones and inspect rules on the same interface because this configuration may not work.

Perform the following tasks to configure a firewall for the Sun RPC ALG:

### Configuring a Layer 4 Class Map for a Firewall Policy

Perform this task to configure a Layer 4 class map for classifying network traffic. When you specify the **match-all** keyword with the **class-map type inspect** command, the Sun RPC traffic matches all Sun remote-procedure call (RPC) Layer 7 filters (specified as program numbers) in the class map. When you specify the **match-any** keyword with the **class-map type inspect**, the Sun RPC traffic must match at least one of the Sun RPC Layer 7 filters (specified as program numbers) in the class map.

To configure a Layer 4 class map, use the **class-map type inspect {match-any | match-all} class-map-name** command.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type inspect {match-any | match-all} class-map-name**
4. **match protocol protocol-name**
5. **end**

#### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>

	Command or Action	Purpose
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>class-map type inspect</b> { <b>match-any</b>   <b>match-all</b> } <i>class-map-name</i> <b>Example:</b> Device(config)# class-map type inspect match-any sunrpc-l4-cmap	Creates a Layer 4 inspect type class map and enters QoS class-map configuration mode.
<b>Step 4</b>	<b>match protocol</b> <i>protocol-name</i> <b>Example:</b> Device(config-cmap)# match protocol sunrpc	Configures a match criterion for a class map on the basis of the specified protocol.
<b>Step 5</b>	<b>end</b> <b>Example:</b> Device(config-cmap)# end	Exits QoS class-map configuration mode and enters privileged EXEC mode.

## Configuring a Layer 7 Class Map for a Firewall Policy

Perform this task to configure a Layer 7 class map for classifying network traffic. This configuration enables programs such as mount (100005) and Network File System (NFS) (100003) that use Sun RPC. 100005 and 100003 are Sun RPC program numbers. By default, the Sun RPC ALG blocks all programs.

For more information about Sun RPC programs and program numbers, see RFC 1057, *RPC: Remote Procedure Call Protocol Specification Version 2*.

Use the **class-map type inspect** *protocol-name* command to configure a Layer 7 class map.

### SUMMARY STEPS

1. enable
2. configure terminal
3. class-map type inspect *protocol-name* {**match-any** | **match-all**} *class-map-name*
4. match program-number *program-number*
5. end

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b>	Enters global configuration mode.

	Command or Action	Purpose
	Device# configure terminal	
<b>Step 3</b>	<b>class-map type inspect</b> <i>protocol-name</i> { <b>match-any</b>   <b>match-all</b> } <i>class-map-name</i> <b>Example:</b> Device(config)# class-map type inspect sunrpc match-any sunrpc-l7-cmap	Creates a Layer 7 (application-specific) inspect type class map and enters QoS class-map configuration mode.
<b>Step 4</b>	<b>match program-number</b> <i>program-number</i> <b>Example:</b> Device(config-cmap)# match program-number 100005	Specifies the allowed RPC protocol program number as a match criterion.
<b>Step 5</b>	<b>end</b> <b>Example:</b> Device(config-cmap)# end	Exits QoS class-map configuration mode and enters privileged EXEC mode.

## Configuring a Sun RPC Firewall Policy Map

Perform this task to configure a Sun remote-procedure call (RPC) firewall policy map. Use a policy map to allow packet transfer for each Sun RPC Layer 7 class that is defined in a class map for a Layer 7 firewall policy.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type inspect** *protocol-name* *policy-map-name*
4. **class type inspect** *protocol-name* *class-map-name*
5. **allow**
6. **end**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>policy-map type inspect</b> <i>protocol-name</i> <i>policy-map-name</i> <b>Example:</b>	Creates a Layer 7 (protocol-specific) inspect type policy map and enters QoS policy-map configuration mode.

## Attaching a Layer 7 Policy Map to a Layer 4 Policy Map

	Command or Action	Purpose
	Device(config)# policy-map type inspect sunrpc sunrpc-l7-pmap	
<b>Step 4</b>	<b>class type inspect</b> <i>protocol-name class-map-name</i>  <b>Example:</b> Device(config-pmap)# class type inspect sunrpc sunrpc-l7-cmap	Specifies the traffic class on which an action is to be performed and enters QoS policy-map class configuration mode.
<b>Step 5</b>	<b>allow</b>  <b>Example:</b> Device(config-pmap-c)# allow	Allows packet transfer.
<b>Step 6</b>	<b>end</b>  <b>Example:</b> Device(config-pmap-c)# end	Exits QoS policy-map class configuration mode and returns to privileged EXEC mode.

## Attaching a Layer 7 Policy Map to a Layer 4 Policy Map

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type inspect** *policy-map-name*
4. **class** {*class-map-name* | **class-default**}
5. **inspect** [*parameter-map-name*]
6. **service-policy** *protocol-name policy-map-name*
7. **exit**
8. **class** **class-default**
9. **drop**
10. **end**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>policy-map type inspect</b> <i>policy-map-name</i>  <b>Example:</b>	Creates a Layer 4 inspect type policy map and enters QoS policy-map configuration mode.

	Command or Action	Purpose
	<code>Device(config)# policy-map type inspect sunrpc-l4-pmap</code>	
<b>Step 4</b>	<b>class</b> { <i>class-map-name</i>   <b>class-default</b> } <b>Example:</b> <code>Device(config-pmap)# class sunrpc-l4-cmap</code>	Associates (class) on which an action is to be performed and enters QoS policy-map class configuration mode.
<b>Step 5</b>	<b>inspect</b> [ <i>parameter-map-name</i> ] <b>Example:</b> <code>Device(config-pmap-c)# inspect</code>	Enables stateful packet inspection.
<b>Step 6</b>	<b>service-policy</b> <i>protocol-name policy-map-name</i> <b>Example:</b> <code>Device(config-pmap-c)# service-policy sunrpc sunrpc-l7-pmap</code>	Attaches the Layer 7 policy map to a top-level Layer 4 policy map.
<b>Step 7</b>	<b>exit</b> <b>Example:</b> <code>Device(config-pmap-c)# exit</code>	Exits QoS policy-map class configuration mode and returns to QoS policy-map configuration mode.
<b>Step 8</b>	<b>class class-default</b> <b>Example:</b> <code>Device(config-pmap)# class class-default</code>	Specifies the default class (commonly known as the class-default class) before you configure its policy and enters QoS policy-map class configuration mode.
<b>Step 9</b>	<b>drop</b> <b>Example:</b> <code>Device(config-pmap-c)# drop</code>	Configures a traffic class to discard packets belonging to a specific class.
<b>Step 10</b>	<b>end</b> <b>Example:</b> <code>Device(config-pmap-c)# end</code>	Exits QoS policy-map class configuration mode and returns to privileged EXEC mode.

## Creating Security Zones and Zone Pairs and Attaching a Policy Map to a Zone Pair

You need two security zones to create a zone pair. However, you can create only one security zone and the second one can be the system-defined security zone. To create the system-defined security zone or self zone, configure the **zone-pair security** command with the **self** keyword.



**Note** If you select a self zone, you cannot configure the inspect action.

In this task, you will do the following:

- Create security zones.
- Define zone pairs.

- Assign interfaces to security zones.
- Attach a policy map to a zone pair.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **zone security** {*zone-name* | **default**}
4. **exit**
5. **zone security** {*zone-name* | **default**}
6. **exit**
7. **zone-pair security** *zone-pair-name* **source** *source-zone-name* **destination** *destination-zone-name*
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **ip address** *ip-address mask* [**secondary** [*vrf vrf-name*]]
12. **zone-member security** *zone-name*
13. **exit**
14. **interface** *type number*
15. **ip address** *ip-address mask* [**secondary** [*vrf vrf-name*]]
16. **zone-member security** *zone-name*
17. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b> <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 3	<b>zone security</b> { <i>zone-name</i>   <b>default</b> }	Creates a security zone and enters security zone configuration mode. <ul style="list-style-type: none"><li>• Your configuration must have two security zones to create a zone pair: a source zone and a destination zone.</li><li>• In a zone pair, you can use the default zone or self zone as either the source or destination zone.</li></ul>
Step 4	<b>exit</b> <b>Example:</b>	Exits security zone configuration mode and returns to global configuration mode.



	Command or Action	Purpose
	<code>Device(config-sec-zone)# exit</code>	
<b>Step 5</b>	<p><b>zone security</b> <i>{zone-name   default}</i></p> <p><b>Example:</b></p> <pre>Device(config)# zone security z-server</pre>	<p>Creates a security zone and enters security zone configuration mode.</p> <ul style="list-style-type: none"> <li>Your configuration must have two security zones to create a zone pair: a source zone and a destination zone.</li> <li>In a zone pair, you can use the default zone as either the source or destination zone.</li> </ul>
<b>Step 6</b>	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>Device(config-sec-zone)# exit</pre>	Exits security zone configuration mode and returns to global configuration mode.
<b>Step 7</b>	<p><b>zone-pair security</b> <i>zone-pair-name source source-zone-name destination destination-zone-name</i></p> <p><b>Example:</b></p> <pre>Device(config)# zone-pair security clt2srv source z-client destination z-server</pre>	Creates a zone pair and enters security zone-pair configuration mode.
<b>Step 8</b>	<p><b>service-policy type inspect</b> <i>policy-map-name</i></p> <p><b>Example:</b></p> <pre>Device(config-sec-zone-pair)# service-policy type inspect sunrpc-l4-pmap</pre>	Attaches a firewall policy map to a zone pair.
<b>Step 9</b>	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>Device(config-sec-zone-pair)# exit</pre>	Exits security zone-pair configuration mode and returns to global configuration mode.
<b>Step 10</b>	<p><b>interface</b> <i>type number</i></p> <p><b>Example:</b></p> <pre>Device(config)# interface gigabitethernet 2/0/0</pre>	Configures an interface type and enters interface configuration mode.
<b>Step 11</b>	<p><b>ip address</b> <i>ip-address mask [secondary [vrf vrf-name]]</i></p> <p><b>Example:</b></p> <pre>Device(config-if)# ip address 192.168.6.5 255.255.255.0</pre>	Sets a primary or secondary IP address for an interface.
<b>Step 12</b>	<p><b>zone-member security</b> <i>zone-name</i></p> <p><b>Example:</b></p> <pre>Device(config-if)# zone-member security z-client</pre>	Attaches an interface to a security zone.
<b>Step 13</b>	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>Device(config-if)# exit</pre>	Exits interface configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 14	<b>interface</b> <i>type number</i> <b>Example:</b> Device(config)# interface gigabitethernet 2/1/1	Configures an interface type and enters interface configuration mode.
Step 15	<b>ip address</b> <i>ip-address mask [secondary [vrf vrf-name]]</i> <b>Example:</b> Device(config-if)# ip address 192.168.6.1 255.255.255.0	Sets a primary or secondary IP address for an interface.
Step 16	<b>zone-member security</b> <i>zone-name</i> <b>Example:</b> Device(config-if)# zone-member security z-server	Attaches an interface to a security zone.
Step 17	<b>end</b> <b>Example:</b> Device(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

## Configuration Examples for Sun RPC ALG Support for Firewall and NAT

### Example: Configuring a Layer 4 Class Map for a Firewall Policy

```
Device# configure terminal
Device(config)# class-map type inspect match-any sunrpc-14-cmap
Device(config-cmap)# match protocol sunrpc
Device(config-cmap)# end
```

### Example: Configuring a Layer 7 Class Map for a Firewall Policy

```
Device# configure terminal
Device(config)# class-map type inspect sunrpc match-any sunrpc-17-cmap
Device(config-cmap)# match program-number 100005
Device(config-cmap)# end
```

### Example: Configuring a Sun RPC Firewall Policy Map

```
Device# configure terminal
Device(config)# policy-map type inspect sunrpc sunrpc-17-pmap
Device(config-pmap)# class type inspect sunrpc sunrpc-17-cmap
Device(config-pmap-c)# allow
Device(config-pmap-c)# end
```

## Example: Attaching a Layer 7 Policy Map to a Layer 4 Policy Map

```
Device# configure terminal
Device(config)# policy-map type inspect sunrpc14-pmap
Device(config-pmap)# class sunrpc14-cmap
Device(config-pmap-c)# inspect
Device(config-pmap-c)# service-policy sunrpc sunrpc-l7-pmap
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap-c)# drop
Device(config-pmap-c)# end
```

## Example: Creating Security Zones and Zone Pairs and Attaching a Policy Map to a Zone Pair

```
Device# configure terminal
Device(config)# zone security z-client
Device(config-sec-zone)# exit
Device(config)# zone security z-server
Device(config-sec-zone)# exit
Device(config)# zone-pair security clt2srv source z-client destination z-server
Device(config-sec-zone-pair)# service-policy type inspect sunrpc-l4-pmap
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 2/0/0
Device(config-if)# ip address 192.168.6.5 255.255.255.0
Device(config-if)# zone-member security z-client
Device(config-if)# exit
Device(config)# interface gigabitethernet 2/1/1
Device(config-if)# ip address 192.168.6.1 255.255.255.0
Device(config-if)# zone-member security z-server
Device(config-if)# end
```

## Example: Configuring the Firewall for the Sun RPC ALG

The following is a sample firewall configuration for the Sun remote-procedure call (RPC) application-level gateway (ALG) support:

```
class-map type inspect sunrpc match-any sunrpc-l7-cmap
  match program-number 100005
!
class-map type inspect match-any sunrpc-l4-cmap
  match protocol sunrpc
!
!
policy-map type inspect sunrpc sunrpc-l7-pmap
  class type inspect sunrpc sunrpc-l7-cmap
  allow
!
!
policy-map type inspect sunrpc-l4-pmap
  class type inspect sunrpc-l4-cmap
  inspect
  service-policy sunrpc sunrpc-l7-pmap
!
class class-default
```

```

    drop
    !
    !
    zone security z-client
    !
    zone security z-server
    !
    zone-pair security clt2srv source z-client destination z-server
    service-policy type inspect sunrpc-l4-pmap
    !
    interface GigabitEthernet 2/0/0
    ip address 192.168.10.1 255.255.255.0
    zone-member security z-client
    !
    interface GigabitEthernet 2/1/1
    ip address 192.168.23.1 255.255.255.0
    zone-member security z-server
    !

```

## Additional References for Sun RPC ALG Support for Firewall and NAT

### Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Master Command List, All Releases</a>
IP Addressing commands	<a href="#">IP Addressing Services Command Reference</a>
Security commands	<ul style="list-style-type: none"> <li>• <a href="#">Security Command Reference: Commands A to C</a></li> <li>• <a href="#">Security Command Reference: Commands D to L</a></li> <li>• <a href="#">Security Command Reference: Commands M to R</a></li> <li>• <a href="#">Security Command Reference: Commands S to Z</a></li> </ul>

### Standards and RFCs

Standard/RFC	Title
RFC 1057	<i>RPC: Remote Procedure Call Protocol Specification Version 2</i>

**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.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

# Feature Information for Sun RPC ALG Support for Firewalls and NAT

*Table 1: Feature Information for Sun RPC ALG Support for Firewalls and NAT*

Feature Name	Releases	Feature Information
Sun RPC ALG Support for Firewalls and NAT	Cisco IOS XE Release 3.2S	<p>The Sun RPC ALG Support for Firewalls and NAT feature adds support for the Sun RPC ALG on the firewall and NAT.</p> <p>The following command was introduced or modified: <b>match protocol</b>.</p>

