Sun RPC ALG Support for Firewall and NAT

Last Updated: December 18, 2011

The Sun RPC ALG Support for Firewall and NAT feature adds support for the Sun Microsystems (Sun) Remote Procedure Call (RPC) Application Layer 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.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 at the end of this document.

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.

Restrictions for Sun RPC ALG Support for Firewall and NAT

- Only port-mapper version 2 is supported.
- Only RPC version 2 is supported.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Information About Sun RPC ALG Support for Firewall and NAT

Sun RPC

Sun RPC ALG provides a deep packet inspection of the Sun RPC protocol. It works with a provisioning system that allows the administrator to configure match filters. The match filters define a match criterion used for search in a Sun RPC packet, thereby permitting only the packets that match the criterion.

In RPC, a client program calls the functions in a server program. The RPC library packages the procedure arguments into a network message and sends it to the server. The server in turn, using the RPC library, takes the arguments from the network message, and calls the specified server procedure. When the server function returns, the 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* .

How to Configure Sun RPC ALG Support for Firewall and NAT

For Sun RPC to work when the firewall and NAT are enabled, ALG has to inspect the Sun RPC packets. ALG also has to handle Sun RPC-specific issues like establishing dynamic firewall sessions and fixing the packet content after NAT translation.

Configuring the Firewall for Sun RPC ALG

Sun RPC is configured using the zone-based firewall that is created using policies and class maps. The Layer 7 class map allows the administrator to configure match filters. The filters specify the program numbers to be searched in the Sun RPC packet. The Sun RPC Layer 7 policy map is configured as a child policy of the Layer 4 policy map using the **service-policy** command.

When a Sun RPC Layer 4 class map is configured but no Layer 7 firewall policy is configured, the traffic returned by Sun RPC can pass through the firewall, but the sessions are not inspected at the Layer 7 level. As a result, 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, with no match filters configured.

Configuring a firewall consists of the following tasks:

Restrictions

- Cisco does not recommend configuring both security zones and inspect rules on the same interfaces.
- If you are inspecting the Sun RPC protocol (that is, you have specified the **match protocol sunrpc** command in the Layer 4 class map), a Layer 7 Sun RPC policy map is required.

For more information about the zone-based firewall policy, see the “Zone-Based Firewall Policy” module in the *Cisco IOS Security Configuration Guide: Securing the Data Plane*.

Configuring a Class Map for a Layer 7 Firewall Policy

Perform this task to configure a class map for classifying network traffic. This configuration enables programs like mount (100005) and Network File System (NFS) (100003) using Sun RPC. 100005 and 100003 are Sun RPC program numbers. By default, 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* .

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. **exit**

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	**class-map type inspect** *protocol-name* {**match-any**	**match-all**} *class-map-name* **Example:** `Router(config)# class-map type inspect sunrpc match-any sunrpc-l7-cmap`	Creates a Layer 7 (application-specific) inspect type class map and enters class-map configuration mode.

	Command or Action	Purpose
Step 4	**match program-number** *program-number* **Example:** `Router(config-cmap)# match program-number 100005`	Specifies the allowed RPC protocol program number as a match criterion.
Step 5	**exit** **Example:** `Router(config-cmap)# exit`	Exits class-map configuration mode and enters global configuration mode.

Configuring a Class Map for a Layer 3 and Layer 4 Firewall Policy

Perform this task to configure a class map for classifying network traffic. When you specify the match-all criterion, the Sun RPC traffic obeys all the Sun RPC Layer 7 filters (specified as program numbers) in the class. When you specify the match-any criterion, the Sun RPC traffic follows at least one of the Sun RPC Layer 7 filters (specified as program numbers) in the class.

SUMMARY STEPS

1. **class-map type inspect** {**match-any** | **match-all**} *class-map-name*
2. **match protocol** *protocol-name*
3. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**class-map type inspect** {**match-any**	**match-all**} *class-map-name* **Example:** `Router(config)# class-map type inspect match-any sunrpc-l4-cmap`	Creates a Layer 3 and Layer 4 inspect type class map and enters class-map type configuration mode.
Step 2	**match protocol** *protocol-name* **Example:** `Router(config-cmap)# match protocol sunrpc`	Configures the match criterion for a class map on the basis of a specified protocol.

	Command or Action	Purpose
Step 3	**exit** **Example:** `Router(config-cmap)# exit`	Exits class-map configuration mode and enters global configuration mode.

Configuring a Sun RPC Firewall Policy Map

Perform this task to configure a Sun 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. **policy-map type inspect** *protocol-name policy-map-name*
2. **class type inspect** *protocol-name class-map-name*
3. **allow**
4. **exit**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**policy-map type inspect** *protocol-name policy-map-name* **Example:** `Router(config)# policy-map type inspect sunrpc sunrpc-l7-pmap`	Creates a Layer 7 (protocol-specific) inspect type policy map and enters policy-map configuration mode.
Step 2	**class type inspect** *protocol-name class-map-name* **Example:** `Router(config-pmap)# class type inspect sunrpc sunrpc-l7-cmap`	Specifies the traffic (class) on which an action is to be performed and enters policy-map class configuration.
Step 3	**allow** **Example:** `Router(config-pmap-c)# allow`	Allows packet transfer.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Router(config-pmap-c)# exit`	Exits policy-map class configuration mode and returns to policy-map configuration mode.
Step 5	**exit** **Example:** `Router(config-pmap)# exit`	Exits policy-map configuration mode and returns to global configuration mode.

Associating a Layer 4 Class and Layer 7 Policy Map

Perform this task to assign a Layer 4 class and a Layer 7 policy map.

SUMMARY STEPS

1. **policy-map type inspect** *policy-map-name*
2. **class type inspect** *class-map-name*
3. **inspect** [*parameter-map-name*]
4. **service-policy** *protocol-name policy-map-name*
5. **exit**
6. **class class-default**
7. **drop**
8. **exit**
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**policy-map type inspect** *policy-map-name* **Example:** `Router(config)# policy-map type inspect sunrpc-l4-pmap`	Creates a Layer 3 and Layer 4 inspect type policy map and enters policy-map configuration.
Step 2	**class type inspect** *class-map-name* **Example:** `Router(config-pmap)# class type inspect sunrpc-l4-cmap`	Specifies the traffic (class) on which an action is to be performed and enters policy-map class configuration.

	Command or Action	Purpose
Step 3	**inspect** [*parameter-map-name*] **Example:** `Router(config-pmap-c)# inspect`	Enables Cisco IOS stateful packet inspection.
Step 4	**service-policy** *protocol-name policy-map-name* **Example:** `Router(config-pmap-c)# service-policy sunrpc sunrpc-l7-pmap`	Attaches the Layer 7 policy map to the top-level Layer 3 or Layer 4 policy map.
Step 5	**exit** **Example:** `Router(config-pmap-c)# exit`	Exits policy-map class configuration mode and returns to policy-map configuration mode.
Step 6	**class class-default** **Example:** `Router(config-pmap)# class class-default`	Specifies the default class (commonly known as the class-default class) before you configure its policy and enters policy-map class configuration mode.
Step 7	**drop** **Example:** `Router(config-pmap-c)# drop`	Configures a traffic class to discard packets belonging to a specific class.
Step 8	**exit** **Example:** `Router(config-pmap-c)# exit`	Exits policy-map class configuration mode and returns to policy-map configuration mode.
Step 9	**exit** **Example:** `Router(config-pmap)# exit`	Exits policy-map configuration mode and returns to global configuration 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, configure the **zone-pair security**command with the **self** keyword.

Note If you select a self zone, you cannot configure inspect policing.

Use this process to complete the following tasks:

- Create at least one security zone
- Define zone pairs
- Assign interfaces to security zones
- Attach a policy map to a zone pair

Note

- An interface cannot be a part of a zone and a legacy inspect policy at the same time.
- An interface can be a member of only one security zone.
- When an interface is a member of a security zone, all traffic to and from that interface is blocked, unless you configure an explicit interzone policy on a zone pair involving that zone.
- Traffic cannot flow between an interface that is a member of a security zone and an interface that is not a member of a security zone because a policy can be applied only between two zones.
- For traffic to flow among all interfaces in a router, the interfaces must be members of at least one security zone. This is particularly important because after you make an interface a member of a security zone, a policy action (such as inspect or pass) must explicitly allow packet transfer. Otherwise, packets are dropped.
- If an interface on a router cannot be part of a security zone or firewall policy, you have to add that interface in a security zone and configure a pass all policy (that is, a dummy policy) between that zone and the other zones to which a traffic flow is desired.
- An access control list (ACL) cannot be applied between security zones and zone pairs. Include the ACL configuration in a class map, and use policy maps to drop traffic.
- All interfaces in a security zone must belong to the same virtual routing and forwarding (VRF) instance.
- You can configure policies between security zones whose member interfaces are in separate VRFs. However, traffic may not flow between these VRFs if the configuration does not allow it. If traffic does not flow between VRFs (because route-leaking between VRFs is not configured), the policy across the VRFs is not executed. This is a configuration issue on the routing side, not on the policy side.
- Traffic between interfaces in the same security zone is not subject to any policy; traffic passes freely.
- The source and destination zones in a zone pair must be of the type security.
- The same zone cannot be defined as both the source and the destination.

>

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**zone security** {*zone-name* | **default**} **Example:** `Router(config)# zone security z-client`	Creates a security zone and enters security zone configuration mode.
Step 2	**exit** **Example:** `Router(config-sec-zone)# exit`	Exits security zone configuration mode and returns to global configuration mode.
Step 3	**zone security** {*zone-name* | **default**} **Example:** `Router(config)# zone security z-server`	Creates a security zone and enters security zone configuration mode.
Step 4	**exit** **Example:** `Router(config-sec-zone)# exit`	Exits security zone configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 5	**zone-pair security** *zone-pair-name* **source** {*source-zone-name* | **self** | **default**} **destination** {*destination-zone-name* | **self** | **default**} **Example:** `Router(config)# zone-pair security clt2srv source z-client destination z-server`	Creates a zone pair and enters zone-pair configuration mode.
Step 6	**service-policy type inspect** *policy-map-name* **Example:** `Router(config-sec-zone-pair)# service-policy type inspect sunrpc-l4-pmap`	Attaches a firewall policy map to a zone pair.
Step 7	**exit** **Example:** `Router(config-sec-zone-pair)# exit`	Exits zone-pair configuration mode and returns to global configuration mode.
Step 8	**interface** *type number* **Example:** `Router(config)# interface Serial2/0`	Configures an interface type and enters interface configuration mode.
Step 9	**ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]] **Example:** `Router(config-if)# ip address 192.168.6.5 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 10	**zone-member security** *zone-name* **Example:** `Router(config-if)# zone-member security z-client`	Attaches an interface to a security zone.
Step 11	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 12	**interface** *type number* **Example:** `Router(config)# interface Serial2/1`	Configures an interface type and enters interface configuration mode.
Step 13	**ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]] **Example:** `Router(config-if)# ip address 192.168.6.5 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 14	**zone-member security** *zone-name* **Example:** `Router(config-if)# zone-member security z-server`	Attaches an interface to a security zone.
Step 15	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring NAT for Sun RPC ALG

By default, Sun RPC ALG is automatically enabled when NAT is enabled. There is no need to explicitly enable Sun RPC ALG in the NAT-only configuration. You can use the **no ip nat service alg** command to disable Sun RPC ALG on NAT.

Configuration Examples for Sun RPC ALG Support for Firewall and NAT

Example Configuring the Firewall for Sun RPC ALG

The following is a sample firewall configuration for Sun RPC 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 GigabitEthernet0/1
 ip address 192.168.10.1 255.255.255.0
 zone-member security z-client
!
interface GigabitEthernet0/2
 ip address 192.168.23.1 255.255.255.0
 zone-member security z-server
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IP Addressing commands	*Cisco IOS IP Addressing Command Reference*
Security commands	*Cisco IOS Security Command Reference*
Firewall	"Zone-Based Firewall Policy" module in the *Cisco IOS Security Configuration Guide: Securing the Data Plane*
NAT	"Configuring NAT" module in the *Cisco IOS IP Addressing Configuration Guide*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1057	*RPC: Remote Procedure Call Protocol Specification Version 2*

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 Sun RPC ALG Support for Firewall and NAT

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 Sun RPC ALG Support for Firewall and NAT

Feature Name	Releases	Feature Information
Sun RPC ALG Support for Firewall and NAT	15.1(1)S	The Sun RPC ALG Support for Firewall and NAT feature adds support for the Sun RPC ALG on the firewall and NAT.