MSRPC ALG Support for Firewall and NAT

The MSRPC ALG Support for Firewall and NAT feature provides support for the Microsoft (MS) Remote Procedure Call (RPC) application-level gateway (ALG) on the firewall and Network Address Translation (NAT). The MSRPC ALG provides deep packet inspection (DPI) of the MSRPC protocol. The MSRPC ALG works in conjunction with a provisioning system to allow the network administrator to configure match filters to define match criteria that can be searched in an MSRPC packet.

The MSRPC ALG additionally supports the Virtual Transport Control Protocol (vTCP) functionality which provides a framework for various ALG protocols to appropriately handle the TCP segmentation and parse the segments in the Cisco IOS zone-based firewall, Network Address Translation (NAT) and other applications.

• Prerequisites for MSRPC ALG Support for Firewall and NAT, on page 1
• Restrictions for MSRPC ALG Support for Firewall and NAT, on page 1
• Information About MSRPC ALG Support for Firewall and NAT, on page 2
• How to Configure MSRPC ALG Support for Firewall and NAT, on page 4
• Configuration Examples for MSRPC ALG Support for Firewall and NAT, on page 8
• Additional References for MSRPC ALG Support for Firewall and NAT, on page 9
• Feature Information for MSRPC ALG Support for Firewall and NAT, on page 11

Prerequisites for MSRPC ALG Support for Firewall and NAT

• You must enable the Cisco IOS XE firewall and Network Address Translation (NAT) before applying the Microsoft (MS) Remote Procedure Call (RPC) application-level gateway (ALG) on packets.

Note

MSRPC ALG is automatically enabled if traffic is sent to TCP port 135 by either Cisco IOS XE firewall or NAT, or both.

Restrictions for MSRPC ALG Support for Firewall and NAT

• Only TCP-based MSRPC is supported.

• You cannot configure the allow and reset commands together.

• You must configure the match protocol msrpc command for DPI.
Only traffic that reaches destination port 135 is supported. This setting can be changed by configuration.

Information About MSRPC ALG Support for Firewall 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.

MSRPC

MSRPC is a framework that developers use to publish a set of applications and services for servers and enterprises. RPC is an interprocess communication technique that allows the client and server software to communicate over the network. MSRPC is an application-layer protocol that is used by a wide array of Microsoft applications. MSRPC supports both connection-oriented (CO) and connectionless (CL) Distributed Computing Environment (DCE) RPC modes over a wide variety of transport protocols. All services of MSRPC establish an initial session that is referred to as the primary connection. A secondary session over a port range between 1024 to 65535 as the destination port is established by some services of MSRPC.

For MSRPC to work when firewall and NAT are enabled, in addition to inspecting MSRPC packets, the ALG is required to handle MSRPC specific issues like establishing dynamic firewall sessions and fixing the packet content after the NAT.

By applying MSRPC protocol inspection, most MSRPC services are supported, eliminating the need for Layer 7 policy filters.

MSRPC ALG on Firewall

After you configure the firewall to inspect the MSRPC protocol, the MSRPC ALG starts parsing MSRPC messages. The following table describes the types of Protocol Data Units (PDU) supported by the MSRPC ALG Support on Firewall and NAT feature:
Table 1: Supported PDU Types

<table>
<thead>
<tr>
<th>PDU</th>
<th>Number</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>REQUEST</td>
<td>0</td>
<td>call</td>
<td>Initiates a call request.</td>
</tr>
<tr>
<td>RESPONSE</td>
<td>2</td>
<td>call</td>
<td>Responds to a call request.</td>
</tr>
<tr>
<td>FAULT</td>
<td>3</td>
<td>call</td>
<td>Indicates an RPC runtime, RPC stub, or RPC-specific exception.</td>
</tr>
<tr>
<td>BIND</td>
<td>11</td>
<td>association</td>
<td>Initiates the presentation negotiation for the body data.</td>
</tr>
<tr>
<td>BIND_ACK</td>
<td>12</td>
<td>association</td>
<td>Accepts a bind request.</td>
</tr>
<tr>
<td>BIND_NAK</td>
<td>13</td>
<td>association</td>
<td>Rejects an association request.</td>
</tr>
<tr>
<td>ALTER_CONTEXT</td>
<td>14</td>
<td>association</td>
<td>Requests additional presentation negotiation for another interface and/or version, or to negotiate a new security context, or both.</td>
</tr>
<tr>
<td>ALTER_CONTEXT_RESP</td>
<td>15</td>
<td>association</td>
<td>Responds to the ALTER_CONTEXT PDU. Valid values are accept or deny.</td>
</tr>
<tr>
<td>SHUTDOWN</td>
<td>17</td>
<td>call</td>
<td>Requests a client to terminate the connection and free the related resources.</td>
</tr>
<tr>
<td>CO_CANCEL</td>
<td>18</td>
<td>call</td>
<td>Cancels or orphans a connection. This message is sent when a client encounters a cancel fault.</td>
</tr>
<tr>
<td>ORPHANED</td>
<td>19</td>
<td>call</td>
<td>Aborts a request that in progress and that has not been entirely transmitted yet, or aborts a (possibly lengthy) response that is in progress.</td>
</tr>
</tbody>
</table>

**MSRPC ALG on NAT**

When NAT receives an MSRPC packet, it invokes the MSRPC ALG that parses the packet payload and forms a token to translate any embedded IP addresses. This token is passed to NAT, which translates addresses or ports as per your NAT configuration. The translated addresses are then written back into the packet payload by the MSRPC ALG.

If you have configured both the firewall and NAT, NAT calls the ALG first.

**MSRPC Stateful Parser**

The MSRPC state machine or the parser is the brain of the MSRPC ALG. The MSRPC stateful parser keeps all stateful information within the firewall or NAT depending on which feature invokes the parser first. The parser provides DPI of MSRPC protocol packets. It checks for protocol conformance and detects
out-of-sequence commands and malformed packets. As the packet is parsed, the state machine records various data and fills in the correct token information for NAT and firewall inspection.

How to Configure MSRPC ALG Support for Firewall and NAT

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

Configuring a Layer 4 MSRPC Class Map and Policy Map

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `class-map type inspect match-any class-map-name`
4. `match protocol protocol-name`
5. `exit`
6. `policy-map type inspect policy-map-name`
7. `class type inspect class-map-name`
8. `inspect`
9. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable&lt;br&gt;Example:&lt;br&gt;&lt;code&gt;Router&gt; enable&lt;/code&gt;</td>
<td>Enables privileged EXEC mode.&lt;br&gt;• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal&lt;br&gt;Example:&lt;br&gt;&lt;code&gt;Router# configure terminal&lt;/code&gt;</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>class-map type inspect match-any class-map-name&lt;br&gt;Example:&lt;br&gt;&lt;code&gt;Router(config)# class-map type inspect match-any msrpc-cmap&lt;/code&gt;</td>
<td>Creates an inspect type class map for the traffic class and enters QoS class-map configuration mode.</td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

**Step 4**  
**match protocol** `protocol-name`  
**Example:**  
Router(config-cmap)# match protocol msrpc

**Purpose**

Configures the match criteria for a class map on the basis of a specified protocol.  
- Only Cisco IOS XE stateful packet inspection-supported protocols can be used as match criteria in inspect type class maps.

**Step 5**  
**exit**  
**Example:**  
Router(config-cmap)# exit

**Purpose**

Exits QoS class-map configuration mode and enters global configuration mode.

**Step 6**  
**policy-map type inspect** `policy-map-name`  
**Example:**  
Router(config)# policy-map type inspect msrpc-pmap

**Purpose**

Creates a Layer 3 or Layer 4 inspect type policy map and enters QoS policy-map configuration mode.

**Step 7**  
**class type inspect** `class-map-name`  
**Example:**  
Router(config-pmap)# class type inspect msrpc-class-map

**Purpose**

Specifies the traffic (class) on which an action is to be performed and enters QoS policy-map class configuration mode.

**Step 8**  
**inspect**  
**Example:**  
Router(config-pmap-c)# inspect

**Purpose**

Enables Cisco IOS XE stateful packet inspection.

**Step 9**  
**end**  
**Example:**  
Router(config-pmap-c)# end

**Purpose**

Exits QoS policy-map class configuration mode and enters privileged EXEC mode.

---

### Configuring a Zone Pair and Attaching an MSRPC Policy Map

**SUMMARY STEPS**

1. `enable`  
2. `configure terminal`  
3. `zone security` `security-zone-name`  
4. `exit`  
5. `zone security` `security-zone-name`  
6. `exit`  
7. `zone-pair security` `zone-pair-name` [source `source-zone` destination `[destination-zone]`]  
8. `service-policy type inspect` `policy-map-name`

---

**MSRPC ALG Support for Firewall and NAT**
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><em>enable</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><em>configure terminal</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Creates a security zone to which interfaces can be assigned and enters security zone configuration mode.</td>
</tr>
<tr>
<td><em>zone security security-zone-name</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# zone security in-zone</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Exits security zone configuration mode and enters global configuration mode.</td>
</tr>
<tr>
<td><em>exit</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-sec-zone)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Creates a security zone to which interfaces can be assigned and enters security zone configuration mode.</td>
</tr>
<tr>
<td><em>zone security security-zone-name</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# zone security out-zone</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Exits security zone configuration mode and enters global configuration mode.</td>
</tr>
<tr>
<td><em>exit</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-sec-zone)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Creates a zone pair and enters security zone pair configuration mode.</td>
</tr>
<tr>
<td><em>zone-pair security zone-pair-name [source source-zone destination [destination-zone]]</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# zone-pair security in-out source in-zone destination out-zone</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Attaches a firewall policy map to the destination zone pair.</td>
</tr>
<tr>
<td><em>service-policy type inspect policy-map-name</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-sec-zone-pair)# service-policy type inspect msrpc-pmap</td>
<td></td>
</tr>
</tbody>
</table>

**Note**

To apply a policy, you must configure a zone pair.

If a policy is not configured between a pair of zones, traffic is dropped by default.
### Purpose

#### Command or Action | Purpose
---|---
**Step 9** | **end**
*Example:* Router(config-sec-zone-pair)# end
| Exits security zone pair configuration mode and enters privileged EXEC mode.

### Enabling vTCP Support for MSRPC ALG

#### SUMMARY STEPS

1. enable
2. configure terminal
3. alg vtcp service msrpc
4. exit
5. set platform hardware qfp active feature alg msrpc tolerance on

#### 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** | **alg vtcp service msrpc**
*Example:* Router(config)# alg vtcp service msrpc
| Enables vTCP functionality for MSRPC ALG.
*Note* By default, MSRPC ALG supports vTCP. |
**Step 4** | **exit**
*Example:* Router(config)# exit
| Exits global configuration mode and returns to privileged EXEC mode. |
**Step 5** | **set platform hardware qfp active feature alg msrpc tolerance on**
*Example:* Router# set platform hardware qfp active feature alg msrpc tolerance on
| Enables MSRPC unknown message tolerance.
*Note* By default, the tolerance is switched off. |
Disabling vTCP Support for MSRPC ALG

SUMMARY STEPS

1. enable
2. configure terminal
3. no alg vtcp service msrpc
4. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 no alg vtcp service msrpc</td>
<td>Disables vTCP functionality for MSRPC ALG.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# no alg vtcp service msrpc</td>
<td></td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Exits global configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

Configuration Examples for MSRPC ALG Support for Firewall and NAT

Example: Configuring a Layer 4 MSRPC Class Map and Policy Map

```
Router# configure terminal
Router(config)# class-map type inspect match-any msrpc-cmap
Router(config-cmap)# match protocol msrpc
Router(config-cmap)# exit
Router(config)# policy-map type inspect msrpc-pmap
Router(config-pmap)# class type inspect msrpc-cmap
Router(config-pmap-c)# inspect
```
Example: Configuring a Zone Pair and Attaching an MSRPC Policy Map

Router# configure terminal
Router(config)# zone security in-zone
Router(config)# zone security out-zone
Router(config)# zone-pair security in-out source in-zone destination out-zone
Router(config)# service-policy type inspect msrpc-pmap
Router(config)# end

Example: Enabling vTCP Support for MSRPC ALG

Router# configure terminal
Router(config)# alg vtcp service msrpc
Router(config)# end

Example: Disabling vTCP Support for MSRPC ALG

Router# configure terminal
Router(config)# no alg vtcp service msrpc
Router(config)# end

Additional References for MSRPC ALG Support for Firewall and NAT

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
<tr>
<td>NAT commands</td>
<td>Cisco IOS IP Addressing Services Command Reference</td>
</tr>
</tbody>
</table>
### Related Topic | Document Title
---|---
Security commands | • Cisco IOS Security Command Reference: Commands A to C  
• Cisco IOS Security Command Reference: Commands D to L  
• Cisco IOS Security Command Reference: Commands M to R  
• Cisco IOS Security Command Reference: Commands S to Z  
NAT ALGs | “Using Application-Level Gateways with NAT” module  
ALG support | NAT and Firewall ALG Support on Cisco ASR 1000 Series Routers  

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
## Feature Information for MSRPC ALG Support for Firewall and NAT

### Table 2: Feature Information for MSRPC ALG Support for Firewall and NAT

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSRPC ALG Support for Firewall and NAT</td>
<td>Cisco IOS XE Release 3.5S</td>
<td>The MSRPC ALG Support for Firewall and NAT feature provides support for the MSRPC ALG on the firewall and NAT. The MSRPC ALG provides deep packet inspection of the MSRPC protocol. The MSRPC ALG works in conjunction with a provisioning system to allow the network administrator to configure match filters that define match criteria that can be searched in an MSRPC packet. The following commands were introduced or modified: <code>ip nat service msrpc</code>, <code>match protocol msrpc</code>.</td>
</tr>
<tr>
<td>MSRPC ALG Inspection Improvements for Zone-based Firewall and NAT</td>
<td>Cisco IOS XE Release 3.14S</td>
<td>The MSRPC ALG Inspection Improvements for Zone-based Firewall and NAT feature supports Virtual Transport Control Protocol (vTCP) functionality which provides a framework for various ALG protocols to appropriately handle the TCP segmentation and parse the segments in the Cisco firewall, Network Address Translation (NAT) and other applications. The following command was introduced: <code>alg vtcp service msrpc</code>.</td>
</tr>
</tbody>
</table>