53-1003816-02
14 September 2015

Brocade 5600 vRouter ALG

Reference Guide

Supporting Brocade 5600 vRouter 3.5R6

BROCADE

Contents

Preface

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Brocade technical documentation.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used in the flow of the text to highlight specific words or phrases.

Format	Description
bold text	Identifies command names
	Identifies keywords and operands
	Identifies the names of user-manipulated GUI elements
	Identifies text to enter at the GUI
italic text	Identifies emphasis
	Identifies variables
	Identifies document titles
`Courier font`	Identifies CLI output
	Identifies command syntax examples

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
value	In Fibre Channel products, a fixed value provided as input to a command option is printed in plain text, for example, **--show** WWN.

Convention	Description
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options. In Fibre Channel products, square brackets may be used instead for this purpose.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

CAUTION
A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Brocade resources

Visit the Brocade website to locate related documentation for your product and additional Brocade resources.

You can download additional publications supporting your product at www.brocade.com. Select the Brocade Products tab to locate your product, then click the Brocade product name or image to open the individual product page. The user manuals are available in the resources module at the bottom of the page under the Documentation category.

To get up-to-the-minute information on Brocade products and resources, go to MyBrocade. You can register at no cost to obtain a user ID and password.

Release notes are available on MyBrocade under Product Downloads.

White papers, online demonstrations, and data sheets are available through the Brocade website.

Contacting Brocade Technical Support

As a Brocade customer, you can contact Brocade Technical Support 24x7 online, by telephone, or by e-mail. Brocade OEM customers contact their OEM/Solutions provider.

Brocade customers

For product support information and the latest information on contacting the Technical Assistance Center, go to http://www.brocade.com/services-support/index.html.

If you have purchased Brocade product support directly from Brocade, use one of the following methods to contact the Brocade Technical Assistance Center 24x7.

Online	Telephone	E-mail
Preferred method of contact for non-urgent issues: • My Cases through MyBrocade • Software downloads and licensing tools • Knowledge Base	Required for Sev 1-Critical and Sev 2-High issues: • Continental US: 1-800-752-8061 • Europe, Middle East, Africa, and Asia Pacific: +800-AT FIBREE (+800 28 34 27 33) • For areas unable to access toll free number: +1-408-333-6061 • Toll-free numbers are available in many countries.	support@brocade.com Please include: • Problem summary • Serial number • Installation details • Environment description

Brocade OEM customers

If you have purchased Brocade product support from a Brocade OEM/Solution Provider, contact your OEM/Solution Provider for all of your product support needs.

- OEM/Solution Providers are trained and certified by Brocade to support Brocade® products.
- Brocade provides backline support for issues that cannot be resolved by the OEM/Solution Provider.

- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information, contact Brocade or your OEM.
- For questions regarding service levels and response times, contact your OEM/Solution Provider.

Document feedback

To send feedback and report errors in the documentation you can use the feedback form posted with the document or you can e-mail the documentation team.

Quality is our first concern at Brocade and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. You can provide feedback in two ways:

- Through the online feedback form in the HTML documents posted on www.brocade.com.
- By sending your feedback to documentation@brocade.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

About This Guide

This guide describes the ALGs available on the Brocade 5600 vRouter (referred to as a virtual router, vRouter, or router in the guide).

ALG Overview

Brocade vRouter Application Layer Gateway (ALG) is a software protocol that provides network address and port translations in the IP packet payloads for the supported applications. The packet payloads allow supported applications to work as expected across a Network Address Translation (NAT) boundary.

When you configure NAT, the ALG protocol detects that an application-specific packet flow originates within the private area of the NAT boundary. If the packet matches with an IP protocol or with the configured destination port, the packet is forwarded to a specific ALG for deep packet inspection. If required, the ALG rewrites the packet payload that uses an appropriate translation network address and a port address. It also rewrites the checksums, TCP sequence, or acknowledgment numbers, and the packet is forwarded to its destination address. You may see different packet lengths on packets that are delivered to the public side of a NAT configuration because certain application protocols are text based.

Several common application protocols consist of multiple packet flows. For example, when a packet contains various protocol commands, an application may consist of a control flow. These command packets may result in one of more secondary packet flows that are related to the control flow. The ALG protocol identifies these applications and creates connections between the sessions that are established for these flows.

When an ALG inspects a control flow, it recognizes that a secondary flow may begin at some point in the future. In that case, the ALG protocol creates an entry in the ALG flow table. When the secondary flow begins, the ALG is notified, and it creates a session that is appropriate for the secondary flow. The established session allows secondary flows to be established regardless of whether they originate from the private or public side of a NAT boundary.

The ALG protocol also creates a firewall pinhole to enable these ALG secondary flows through which these ALG secondary flows can pass. These firewall pinholes are valid only for the duration of the secondary flow, and after the flow is completed, the pinholes are removed.

Supported ALG protocols

The following ALG protocols are included in the current release:

- File Transfer Protocol (FTP)
- Point-to-Point Tunneling Protocol (PPTP)
- Internet Control Management Protocol (ICMP) and Internet Control Management Protocol version 6 (ICMPv6)
- Remote Procedure Call (RPC)
- Session Initiation Protocol (SIP)
- Trivial File Transfer Protocol (TFTP)

ALG Types

The following sections provide specific information about each of the Brocade vRouter ALGs.

FTP

File Transfer Protocol (FTP) is a file transfer protocol that allows FTP clients from inside the private side of a NAT boundary to operate as expected with an FTP server located on the public side.

The FTP protocol includes both active and passive data transfers. An *active* data transfer means that the transfer is initiated from the FTP server back to the FTP client. A *passive* data transfer means that the FTP client initiates the transfer to the FTP server. The Brocade vRouter ALG protocol automatically supports both the FTP transfer modes.

The FTP data sessions are automatically linked to the FTP control session.

TFTP

Trivial File Transfer Protocol (TFTP) is a file transfer protocol that allows a client to either get or put a file onto a remote host. The Brocade vRouter TFTP ALG protocol allows a TFTP client on the private side of NAT to access a TFTP server on the public side.

The TFTP data sessions are automatically linked to the TFTP control session.

SIP

Session Initiation Protocol (SIP) provides signaling capabilities for multimedia communication sessions. Common SIP applications include Internet telephony (both audio and video calls) and instant messaging.

The Brocade vRouter SIP ALG protocol provides network address and port translation for both SIP request and response messages that are originating from the private side of NAT to the public side.

SIP media packet flows generally use the Realtime Transport Protocol (RTP) over the UDP IP protocol for multimedia sessions. The SIP ALG automatically detects these multimedia sessions and links them to the SIP control session.

The SIP ALG correctly manages up to eight media sessions in a single SIP invitation request. A limit of 400 outstanding invitation requests exists at any given time.

PPTP

Point-to-Point Tunneling Protocol (PPTP) is a method for providing virtual private networks. The Brocade vRouter PPTP ALG protocol provides a mechanism for establishing sessions that are associated with PPTP.

ICMP

Internet Control Management Protocol (ICMP) is an error-reporting and message-control protocol that network devices use to report problems in IP packet delivery. The ICMP ALG protocol allows ICMP and ICMP6 packets to traverse from the public side of NAT back to the private side.

RPC

Remote Procedure Call (RPC) is a protocol that enables various RPC services to establish session relationships between related packet flows of applications.

The RPC ALG protocol is automatically configured with several NFS program numbers to enable an NFS client from the private side of a NAT to access a NFS server on the public side. The following table lists the default RPC programs.

TABLE 1 Default RPC Program

Number	Program
100000	portmap
100003	nfsprog
100005	mount
100021	nlockmgr
100227	nfs_acl

You can enable additional RPC programs by adding those program numbers to the RPC ALG configuration. A complete listing of RPC program numbers can be found in `/etc/rpc`.

ALG Configurations

Several Brocade vRouter ALGs share common configuration concepts. This section describes the shared concepts and their behaviors.

In the Brocade vRouter, all ALGs are enabled by default and automatically start detecting their respective packet flows if NAT is configured. You can control which ALGs are enabled or disabled by using the configuration system. You can dynamically enable or disable ALGs during run time.

For PPTP and ICMP, ICMP6 protocol detection takes place on the IP protocol of the packets. For all other ALGs, the detection takes place on the basis of UDP and TCP or the TCP destination port that matches configured control ports. When a packet is received with a destination port that matches a control port, the packet is forwarded to the correct ALG for processing.

ALG control ports

For port-based ALGs, the default configuration includes application ports as specified by the Internet Assigned Numbers Authority (IANA). The following table lists the default ports for port-based ALGs.

TABLE 2 ALG control ports

ALG	IP Protocol	Control Port
FTP	TCP	21
TFTP	UDP	69
SIP	UDP/TCP	5060
RPC	UDP/TCP	111

Additional control ports can be added or removed by using the configuration system with the commands that are listed in the ALG commands section.

You can configure up to 32 additional control ports per port-based ALG. Each added control port must be unique throughout all configured ports for all port-based ALGs. For example, you cannot add port 4242 to both SIP and FTP protocols.

If you add additional control ports to a port-based ALG, the default port for that ALG will be replaced with the list of configured ports. If you wish to have both configured port and default control port, include the default port in your configuration.

When you remove all ports from the ALG configuration, the default port is enabled automatically.

Enabling and disabling ALG protocols

All Brocade vRouter ALG protocols are enabled by default. You can disable an ALG by setting the `disable` parameter in the configuration. For example, to disable the FTP ALG, use the following commands:

- `# set system alg ftp disabled`
- `# commit`

You can re-enable an ALG by deleting the `disable` parameter from the configuration. If the FTP ALG is in a disabled state, the following commands will re-enable the ALG:

- `# delete system alg ftp disable`
- `# commit`

When an ALG is disabled, the new packet flows are not forwarded to the ALG for processing. This means that the packet payloads are not translated and session connections are not established.

NOTE
The existing sessions continue to reference the ALG until the packet flow terminates.

Monitoring and Logging

You can use the `show session-table` command to see the relationships between ALG control packet flows and any secondary packet flows. The session handles are created if the control packet flows match either a stateful firewall rule or a NAT rule for the interface.

An example of a `show session-table` output for a SIP packet flow follows.

```
vyatta@vyatta:~$ show session-table
TCP state codes: SS - SYN SENT, SR - SYN RECEIVED, ES - ESTABLISHED,
                 FW - FIN WAIT, CW - CLOSE WAIT, LA - LAST ACK,
                 TW - TIME WAIT, CL - CLOSE, LI - LISTEN

CONN ID         Source                          Destination
Protocol        TIMEOUT Intf            Parent
19              192.168.11.111:54984            192.168.22.22:5060
udp [17] ES     58      dp0s12  0
20              192.168.11.111:4242             192.168.22.22:23000
udp [17] ES     58      dp0s12  19
```

The session handle represents a control packet flow if the value of the last column of the output is '0' (zero). Otherwise, the number in the last column is the Connection ID of the parent control flow for this secondary flow.

Certain ALGs may have nested relationships between various session handles, which means that a secondary flow may also be a parent to a tertiary packet flow. The nested relationships are captured in the parent column of the session table output. There is no implied order to the output of show session-table output. If multiple packet flows generate session handles, related session handles may be intermixed with other session handles in the command output.

The error messages from the ALG system is recorded in the system log file `/var/log/messages` and `/var/log/dataplane/vplane.log`.

ALG Commands

system alg ftp disable

Disables the FTP ALG.

Syntax **set system alg ftp disable**

delete system alg ftp disable

Parameters None

Modes Configuration mode.

Configuration Statement

```
system {
    alg {
        ftp {
            disable
        }
    }
}
```

Usage Guidelines Use the **set** form of this command to disable FTP ALG.

Use the **delete** form of this command to enable FTP ALG.

system alg ftp port <port-number>

Adds an FTP control port to use for tracking initial connections.

Syntax **set system alg ftp port** *port-number*

delete system alg ftp port *port-number*

Parameters None

Modes Configuration mode.

Configuration Statement

```
system {
    alg {
        ftp {
            port port-number
        }
    }
}
```

Usage Guidelines Use the **set** form of this command to add a FTP control port to use for tracking initial connections.

Use the **delete** form of this command to delete a FTP control port that is used for tracking initial connections.

You can specify up to 32 additional ports for this ALG.

system alg sip disable

Disables the SIP ALG.

Syntax **set system alg sip disable**

delete system alg sip disable

Parameters None

Modes Configuration mode.

Configuration Statement

```
system {
    alg {
        ftp {
            disable
        }
    }
}
```

Usage Guidelines Use the **set** form of this command to disable SIP ALG.

Use the **delete** form of this command to enable SIP ALG.

system alg sip port <port-number>

Adds a SIP control port to use for tracking initial connections.

Syntax **set system alg sip port** *port-number*

delete system alg sip port *port-number*

Parameters None

Modes Configuration mode.

Configuration Statement

```
system {
    alg {
        sip {
            port port-number
        }
    }
}
```

Usage Guidelines Use the **set** form of this command to add a SIP control port to use for tracking initial connections.

Use the **delete** form of this command to delete a SIP control port that is used for tracking initial connections.

You can specify up to 32 additional ports for this ALG.

system alg tftp disable

Disables the TFTP ALG.

Syntax **set system alg tftp disable**

delete system alg tftp disable

Parameters None

Modes Configuration mode.

Configuration Statement

```
system {
    alg {
        tftp {
            disable
        }
    }
}
```

Usage Guidelines Use the **set** form of this command to disable TFTP ALG.

Use the **delete** form of this command to enable TFTP ALG.

system alg tftp port <port-number>

Adds a TFTP control port to use for tracking initial connections.

Syntax **set system alg tftp port** *port-number*

delete system tftp port *port-number*

Parameters None

Modes Configuration mode.

Configuration Statement

```
system {
    alg {
        tftp {
            port port-number
        }
    }
}
```

Usage Guidelines Use the **set** form of this command to add a TFTP control port to use for tracking initial connections.

Use the **delete** form of this command to delete a TFTP control port that is used for tracking initial connections.

You can specify up to 32 additional ports for this ALG.

system alg pptp disable

Disables the PPTP ALG.

Syntax **set system alg pptp disable**

delete system alg pptp disable

Parameters None

Modes Configuration mode.

Configuration Statement

```
system {
    alg {
        pptp {
            disable
        }
    }
}
```

Usage Guidelines Use the **set** form of this command to disable PPTP ALG.

Use the **delete** form of this command to enable PPTP ALG.

system alg icmp disable

Disables the ICMP ALG.

Syntax **set system alg icmp disable**

delete system alg icmp disable

Parameters None

Modes Configuration mode.

Configuration Statement

```
system {
    alg {
        icmp {
            disable
        }
    }
}
```

Usage Guidelines Use the **set** form of this command to disable ICMP ALG.

Use the **delete** form of this command to enable ICMP ALG.

system alg rpc program number

Allows you to set program numbers.

Syntax **set system alg rpc program** *number*

delete system alg rpc program *number*

Parameters None

Modes Configuration mode.

Configuration Statement

```
system {
    alg {
        rpc {
            program number
        }
    }
}
```

Usage Guidelines Use the **set** form of this command to add a program number.

Use the **delete** form of this command to delete a program number.