



DANOS-Vyatta edition

Disaggregated Network Operating System Version 2009a

Application Layer Gateway Configuration Guide
October 2020

Contents

Chapter 1. Copyright Statement.....	1
Chapter 2. Preface.....	2
Document conventions.....	2
Chapter 3. About This Guide.....	4
Chapter 4. ALG Overview.....	5
Supported ALG protocols.....	5
ALG Types.....	6
Chapter 5. ALG Configurations.....	8
ALG control ports.....	8
Enabling and disabling ALG protocols.....	8
Recommended additional RSH configuration.....	9
Chapter 6. Monitoring and Logging.....	11
Chapter 7. ALG Commands.....	12
system alg ftp disable.....	12
system alg ftp port.....	12
system alg pptp disable.....	13
system alg icmp disable.....	13
system alg rpc program number.....	14
system alg rsh disable.....	14
system alg sip disable.....	15
system alg sip port.....	15
system alg tftp disable.....	16
system alg tftp port.....	16
show alg state.....	17

Chapter 1. Copyright Statement

© 2020 IP Infusion Inc. All Rights Reserved.

This documentation is subject to change without notice. The software described in this document and this documentation are furnished under a license agreement or nondisclosure agreement. The software and documentation may be used or copied only in accordance with the terms of the applicable agreement. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's internal use without the written permission of IP Infusion Inc.

IP Infusion Inc.
3965 Freedom Circle, Suite 200
Santa Clara, CA 95054
+1 408-400-1900

<http://www.ipinfusion.com/>.

For support, questions, or comments via E-mail, contact:

support@ipinfusion.com.

Trademarks:

IP Infusion is a trademark of IP Infusion. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Use of certain software included in this equipment is subject to the IP Infusion, Inc. End User License Agreement at <http://www.ipinfusion.com/license>. By using the equipment, you accept the terms of the End User License Agreement.

Chapter 2. Preface

Document conventions

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

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.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font are used to highlight specific words or phrases.

Format	Description
bold text	Identifies command names. Identifies keywords and operands.
<i>italic text</i>	Identifies emphasis. Identifies variables. Identifies document titles.
<code>Courier font</code>	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.
<i>italic text</i>	Identifies a variable.
[]	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.
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, <i>member</i> [<i>member</i> ...].
\	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.

Chapter 3. About This Guide

This guide describes how to configure Application Layer Gateways (ALGs) on DANOS-Vyatta edition.

Chapter 4. ALG Overview

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 or 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 supported:

- File Transfer Protocol (FTP)
- Point-to-Point Tunneling Protocol (PPTP)
- Remote Procedure Call (RPC)
- Remote Shell (RSH)
- Session Initiation Protocol (SIP)
- Trivial File Transfer Protocol (TFTP)

ALG Types

The following sections provide specific information about each of the router 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 router ALG protocol automatically supports both the FTP transfer modes.

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

PPTP

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

RPC

Remote Procedure Call (RPC) protocol 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 programs

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`.

To enable RPC programs that are not included in the default list, use the following command:

```
set system alg rpc program
```

Note:

If you explicitly configure an additional ALG RPC program, the configuration automatically deletes the default programs. Therefore, if you require the default programs as well as additional programs, you must explicitly configure those programs as well as the desired additional programs by using the `set system alg rpc program` command.

No `show` command exists to display the active RPC programs.

The RPC ALG runs on port 111. You cannot change this port number.

The full list of RPC programs that can run on port 111 are at <https://www.iana.org/assignments/rpc-program-numbers/rpc-program-numbers.xhtml>.

RSH

Remote Shell (RSH) is a highly insecure and aged protocol that enables a remote user to run shell-level commands on a computer system. Because the protocol includes a port string that is used for stderr output, the RSH protocol does not work correctly in a NAT environment unless this string is properly recognized and translated. The RSH ALG protocol correctly recognizes RSH streams and performs the appropriate operations on the packets to enable RSH to work in both SNAT and DNAT configurations.

On some operating systems, the RSH services make use of the IDENT (RFC-1413) identification protocol. IDENT uses text-based messages to determine the identity of the user of a particular TCP connection. RSH ALG also includes support for correctly translating these messages.

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 router 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.

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 router 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.

Chapter 5. ALG Configurations

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

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, 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
RPC	UDP/TCP	111
RSH	TCP	514
SIP	UDP/TCP	5060
TFTP	UDP	69

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 router 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.

Recommended additional RSH configuration

The RSH server imposes strict requirements on client connections, which is why IP Infusion Inc. recommends that administrators create distinct SNAT rules to match expected RSH usage from the private side of the NAT gateway. The RSH protocol requires that client connections for the control and stderr connections use ports in a range from 512 through 1023. This range means that in an SNAT scenario, you can concurrently establish as many as 256 RSH connections for each translation address (each RSH connection consists of two connections to the same address: a control-port connection and a stderr-port connection).

Because of this limitation, IP Infusion Inc. recommends that administrators create an RSH-specific SNAT rule that contains an address and a port range to handle the expected number of concurrent connections. This rule must have a higher rule index than any other matching SNAT rule for the private side of the NAT gateway. This SNAT source rule must include the following configurations:

- A matching TCP destination port of 514
- A translation address range
- A transport port range of 513 through 1023 for TCP

The size of the address range depends on the number of concurrent connections.

 **Note:** There are no special requirements for DNAT rules.

The following example shows how to configure an SNAT rule that can be used for RSH traffic. This rule matches TCP packets that are destined for port 514 and modifies them to use the 192.66.66.6 translation address and a port range of 512 through 1023.

Step	Command
Create an SNAT rule.	<pre>vyatta@R1# set service nat source rule 22 description rsh</pre>
Configure the rule to match TCP packets destined for port 514.	<pre>vyatta@R1# set service nat source rule 22 destination port 514</pre>
Specify the outbound interface for the rule.	<pre>vyatta@R1# set service nat source rule 22 outbound-interface dp0s5</pre>
Configure the rule to handle TCP packets.	<pre>vyatta@R1# set service nat source rule 22 protocol tcp</pre>
Configure the rule to modify the packets to use the 192.66.66.6 translation address and 512-through-1023 port range.	<pre>vyatta@R1# set service nat source rule 22 translation address 192.66.66.6 vyatta@R1# set service nat source rule 22 translation port 513-1023</pre>
Commit and view the configuration.	<pre>vyatta@R1# commit [edit] vyatta@R1# show service nat source source { rule 22 { description rsh destination { port 514 } outbound-interface dp0s5 protocol tcp translation { address 192.66.66.6 port 513-1023 } } }</pre>

Chapter 6. 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 are recorded in the dataplane log. To display the error messages, use the `show dataplane log` command

Chapter 7. ALG Commands

system alg ftp disable

Disables the FTP ALG.

```
set system alg ftp disable
```

```
delete system alg ftp disable
```

None

Configuration mode.

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

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

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

```
set system alg ftp port port-number
```

```
delete system alg ftp port port-number
```

None

Configuration mode.

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

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 pptp disable

Disables the PPTP ALG.

```
set system alg pptp disable
```

```
delete system alg pptp disable
```

None

Configuration mode.

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

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.

```
set system alg icmp disable
```

```
delete system alg icmp disable
```

None

Configuration mode.

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

}

 **Note:** This command is deprecated. ICMP error messages are now handled internally without the requirement for an ALG.

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.

```
set system alg rpc program number
```

```
delete system alg rpc program number
```

None

Configuration mode.

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

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

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

system alg rsh disable

Disables RSH ALG.

```
set system alg rsh disable
```

```
delete system alg rsh disable
```

None

Configuration mode.

```
system {
  alg {
    rsh {
      disable
    }
  }
}
```

```

}
}
}

```

Use the **set** form of this command to disable RSH ALG.

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

system alg sip disable

Disables the SIP ALG.

```
set system alg sip disable
```

```
delete system alg sip disable
```

None

Configuration mode.

```

system {
  alg {
    sip {
      disable
    }
  }
}

```

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

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

```
set system alg sip port port-number
```

```
delete system alg sip port port-number
```

None

Configuration mode.

```

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

```

```
}
}
```

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.

```
set system alg tftp disable
```

```
delete system alg tftp disable
```

None

Configuration mode.

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

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

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

```
set system alg tftp port port-number
```

```
delete system tftp port port-number
```

None

Configuration mode.

```
system {
  alg {
```

```
tftp {
  port port-number
}
}
```

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.

show alg state

Displays the ALGs that are enabled and the ports they are configured on.

```
show alg state
```

Operational mode

Use this command to view the ALGs that are enabled and the ports they are configured on.

 **Note:** Ports are not displayed for disabled ALGs.

The `show alg state` command displays the following information:

Output field	Description
VRF	The VRF name
Name	The ALG name
Protocol	The protocol name
Port	The port on which the ALG is configured

The following example shows information of all the ALGs that are enabled and the ports they are configured on.

```
vyatta@vyatta:~$ show alg state
```

```
VRF: default
```

```

Name      Protocol      Port
----      -
ftp       tcp           21
rpc       tcp           111
rsh       tcp           514
sip       tcp           5060
tftp     udp           69
rpc       udp           111
```

sip	udp	5060
pptp	n/a	n/a