

NAT and Firewall ALG and AIC Support on Cisco ASR 1000 Series Aggregation Services Routers

First Published: February 6, 2009

Last Updated: January 25, 2012

The following tables summarize Cisco ASR1000 Series Aggregation Services Routers support of:

- Application Layer Gateways (ALGs) also called Application-level gateways, support for Network Address Translation (NAT) and Firewall Services
- Application Inspection Controls (AICs) support for Firewall Services

This document lists all of the ALGs and AICs that have been introduced since Cisco IOS XE Release 2.1 to Cisco IOS XE Release 3.5S.

Each table maps the IOS-XE Release and the introduced ALG and/or AIC features. NAT ALG, Firewall ALG and AIC support are cumulative; that is ALGs and AICs supported in earlier releases continue to be supported in later releases.

This document contains the following tables:

- ***NAT and Firewall ALG Support on Cisco ASR 1000 Series Routers in Cisco IOS XE Release 3.5S***
- ***NAT and Firewall ALG Support on Cisco ASR 1000 Series Routers in Cisco IOS XE Release 3.4S***
- ***NAT and Firewall ALG Support on Cisco ASR 1000 Series Routers in Cisco IOS XE Release 3.2S***
- ***NAT and Firewall ALG Support on Cisco ASR 1000 Series Routers in Cisco IOS XE Release 3.1S***
- ***NAT and Firewall ALG Support on Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.5***
- ***NAT and Firewall ALG Support on Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.4***
- ***NAT and Firewall ALG Support on Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.2***
- ***NAT and Firewall ALG Support on Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.1***

The following table summarizes the NAT ALG, Firewall ALG and AIC support on Cisco ASR1000 Series Aggregation Services Routers that was introduced in Cisco IOS XE Release 3.5S:

NAT and Firewall ALG Support on Cisco ASR1000 Series Aggregation Services Routers in Cisco IOS XE Release 3.5S

Application Layer Gateway	Features Supported
Microsoft Remote Procedure Call (MSRPC)	<ul style="list-style-type: none"> ▪ Firewall (FW) Layer 7 policy inspection of TCP communication between the EPM (Endpoint Mapper) on the Server side to the Client on the well-known TCP port 135. ▪ A client will call the endpoint mapper at the server to ask for a "well known" service. The server will answer the client at the addresses this service is available (or if this service is not available at all). ▪ Apply NAT if needed and rewrite the message. ▪ Allow multiple use of the imprecise FW session, since a client may attempt multiple connections to the server port returned by the EPM. ▪ A FW session is based on 5-tuples: source or destination IP addresses source or destination ports and the protocol. When the source port is unknown, an imprecise FW session will be created. When traffic "hits" the other 4-tuples, a FW session will be created. ▪ Provide validity of the MSRPC protocol (messages and protocol): binding – bind request and response tracking, call, request and response message tracking. ▪ No TCP segmentation (vTCP) support in this release.
FTP64	<ul style="list-style-type: none"> ▪ Intra-Chassis High Availability Support.
Skinny Call Control Protocol (SCCP)	<ul style="list-style-type: none"> ▪ Support SCCP Version 17 to interwork with Cisco Unified Communications Manager (CUCM) 8.x. ▪ No High Availability is supported for SCCP ALG.
Session Initiation Protocol (SIP) IP ALG- vTCP Enhancements	<ul style="list-style-type: none"> ▪ Multiple SIP messages per TCP segment. ▪ No High Availability is supported for SIP ALG.

The following tables summarize the NAT ALG, Firewall ALG and AIC support on Cisco ASR1000 Series Aggregation Services Routers that was introduced in Cisco IOS XE Release 3.4S:

NAT and Firewall ALG support on Cisco ASR1000 Series Aggregation Services Routers in Cisco IOS XE Release 3.4S

Application Layer Gateway	Features Supported
FTP64	<ul style="list-style-type: none"> ▪ Support draft-ietf-behave-ftp64-06. ▪ Support stateful NAT64 only; stateless NAT64 is not supported. ▪ Support Virtual Fragmentation Reassembly (VFR)/IP Reassembly. ▪ No FW support. ▪ No virtual routing and forwarding (VRF) support. ▪ No IPv4-embedded IPv6 address support.

Firewall AIC support on Cisco ASR1000 Series Aggregation Services Routers in Cisco IOS XE Release 3.4S

Application Inspection Control	Features Supported
GPRS Tunneling Protocol (GTP) v0, v1	<ul style="list-style-type: none"> ▪ FW Layer 7 policy inspection. ▪ Verify protocol integrity. ▪ Support GTPv0 and GTPv1 control packets inspection (APN regular expression, MCC/MNC, packet type, length). ▪ Data packets are not inspected. ▪ Provides partial parity to Adaptive Security Appliance (ASA) functionality.

The following tables summarize the NAT ALG, Firewall ALG and AIC support on Cisco ASR1000 Series Aggregation Services Routers that was introduced in Cisco IOS XE Release 3.2S:

NAT and Firewall ALG Support on Cisco ASR1000 Series Aggregation Services Routers in Cisco IOS XE Release 3.2S

Application Layer Gateway	Features Supported
Session Initiation Protocol (SIP) Enhancements	<ul style="list-style-type: none"> ▪ Support TCP segmentation (vTCP) under NAT and/or FW configuration. ▪ Support SIP Trunk. ▪ Support REFER Method. ▪ Support Multiple M-Lines in Session Description Protocol (SDP) (up to 5 m-lines).
SunRPC	<ul style="list-style-type: none"> • Support NAT and FW. • Portmapper Version 2 will be inspected while Version 3 & 4 will be passed through. <p>The following is NOT supported:</p> <ul style="list-style-type: none"> • TCP segmentation.

Firewall AIC Support on Cisco ASR1000 Series Aggregation Services Routers in Cisco IOS XE Release 3.2S

Application Inspection Control	Features Supported
Simple Mail Transfer Protocol (SMTP)	<ul style="list-style-type: none"> ▪ FW Layer 7 policy inspection. ▪ Support SMTP and Extended SMTP (ESMTP), only regular extensions. ▪ Data inspection.
Post Office Protocol 3 (POP3)	<ul style="list-style-type: none"> ▪ FW Layer 7 policy inspection. ▪ Inspection of session establishment only. ▪ Encrypted packets are passed through.
Internet Message Access Protocol (IMAP)	<ul style="list-style-type: none"> ▪ FW Layer 7 policy inspection. ▪ Inspection of session establishment only. ▪ Encrypted packets are passed through.
SunRPC	<ul style="list-style-type: none"> ▪ Layer 7 policy inspection based on SUNRPC program number.

The following table summarizes NAT ALG, Firewall ALG and AIC support on Cisco ASR1000 Series Aggregation Services Routers that was introduced in Cisco IOS XE Release 3.1S:

NAT and Firewall ALG Support on Cisco ASR1000 Series Aggregation Services Routers in Cisco IOS XE Release 3.1S

Application Layer Gateway	Features Supported
Real Time Streaming Protocol (RTSP) Enhancement	<ul style="list-style-type: none"> ▪ Support NAT (in RTP, RDT and Interleave mode.) ▪ Support TCP segmentation under NAT and/or FW configuration.
Domain Name System (DNS) Enhancement	<ul style="list-style-type: none"> ▪ Support TCP segmentation under NAT and/or FW configuration.
RCMD	<ul style="list-style-type: none"> • Support NAT and FW. • Support rlogin, rsh and rexec. • TCP-only. • Support VRF. • External authentication mechanisms on behaves of peers involved.
NETBIOS	<ul style="list-style-type: none"> • Support RFC 1002 under NAT and Firewall configurations. • Support NetBIOS over IP only. • Support the following services: <ul style="list-style-type: none"> - Naming Service - Session Service - Datagram Service • Support protocol conformance under NAT and FW. • Support VRF. <p>The following are not supported:</p> <ul style="list-style-type: none"> • Enforcing user authentication via Active Directory and Lightweight Directory Access Protocol (LDAP) to access NetBIOS Name Service. • Server Message Block Protocol (SMB) messages under NetBIOS Session Service. These messages have TCP port 445. • TCP segmentation.

The following table summarizes NAT ALG, Firewall ALG and AIC support on Cisco ASR1000 Series Aggregation Services Routers that was introduced in Cisco IOS XE Release 2.5:

NAT and Firewall ALG Support on Cisco ASR1000 Series Aggregation Services Routers in Cisco IOS XE Release 2.5

Application Layer Gateway	Features Supported
FTP, TFTP, DNS, LDAP, SIP, H323, SCCP, RTSP	▪ VRF Support

The following table summarizes NAT ALG, Firewall ALG and AIC support on Cisco ASR1000 Series Aggregation Services Routers that was introduced in Cisco IOS XE Release 2.4:

NAT and Firewall ALG Support on Cisco ASR1000 Series Aggregation Services Routers in Cisco IOS XE Release 2.4

Application Layer Gateway	Features Supported
H.323 RAS	<ul style="list-style-type: none"> ▪ All Gatekeeper-related messages are supported. ▪ The following features are not supported: <ul style="list-style-type: none"> - Discovering Gatekeeper network element using multicast mechanism. - Discovering Gatekeeper network element using a fully qualified domain name (FQDN). - Discovering Gatekeeper network element using URL. - TCP segmentation.
LDAP	<ul style="list-style-type: none"> • Support NAT only (not applicable to Firewall.) • Support LDAP Version 2 and Version 3 messages. • NAT fixup will be done on the following LDAP messages: <ul style="list-style-type: none"> - ADDREQUEST - SEARCHREQUEST - SEARCHRESPONSE
SIP Extension	<ul style="list-style-type: none"> ▪ Support RFC 2976 – INFO. ▪ Support RFC 3262 – PRACK. ▪ Support RFC 3265 - SUBSCRIBE/NOTIFY. ▪ Support RFC 3311 – UPDATE. ▪ Support RFC 3428 – MESSAGE. ▪ Support RFC 3515, 3892 – REFER. ▪ Support SIP over TCP. ▪ TCP segmentation is not supported. ▪ FQDN is not supported.
Skinny Video	<ul style="list-style-type: none"> ▪ Support IP phones with video capability. ▪ The following two new messages are supported for NAT and Firewall: <ul style="list-style-type: none"> - OpenMultiMediaReceiveChannelAck - StartMultiMediaTransmission ▪ Support Cisco Unified Communications Manager (through Release 6.1). ▪ TCP segmentation is not supported.

The following table summarizes NAT ALG, Firewall ALG and AIC support on Cisco ASR1000 Series Aggregation Services Routers that was introduced in Cisco IOS XE Release 2.2:

NAT and Firewall ALG Support on Cisco ASR1000 Series Aggregation Services Routers in Cisco IOS XE Release 2.2

Application Layer Gateway	Features Supported
RTSP	<ul style="list-style-type: none">▪ RFC 2326, Real Time Streaming Protocol (RTSP) as follows:<ul style="list-style-type: none">- TCP only.- No content-type will be examined by RTSP ALG.- No fully qualified domain name (FQDN) support.▪ Support Firewall only.▪ Support RTSP as a pass-thru protocol as follows:<ul style="list-style-type: none">- No RTSP request/response sources/terminates on the platform.- No RTSP configuration.▪ No RTSP-specific statistics will be sent.▪ No multicast support.

The following table summarizes NAT and Firewall ALG support on Cisco ASR1000 Series Aggregation Services Routers that was introduced in Cisco IOS XE Release 2.1:

NAT and Firewall ALG Support on Cisco ASR1000 Series Aggregation Services Routers in Cisco IOS XE Release 2.1

Application Layer Gateway	Features Supported
Domain Name System (DNS)	<ul style="list-style-type: none"> ▪ Support RFC 1035, both TCP and UDP, for NAT and Firewall. DNS ALG will parse all DNS packets, including the following: <ul style="list-style-type: none"> - TYPE_A query/response - TYPE_CNAME - TYPE_MX - TYPE_NS - TYPE_PTR query/response - TYPE_SOA
File Transfer Protocol (FTP)	<ul style="list-style-type: none"> ▪ Support RFC765 for NAT and Firewall. Supported modes include the following: <ul style="list-style-type: none"> - Active mode - Passive mode
H.323	<ul style="list-style-type: none"> ▪ H.323v4 with H.225v4 and H.245v7. Support for GW-Terminal is available. Gatekeeper-related messages will be ignored. ▪ Backward compatibility support only until H.323v2. H.323v1 messages will be ignored. ▪ FastConnect and Tunneling are supported. (Tunneling specifically refers to sending H.245 messages within H.225.0 messages.) ▪ Support both NAT and Firewall. ▪ H.323 RAS is not supported. ▪ Multipoint is not supported. ▪ T.120 is not supported.
Internet Control Message Protocol (ICMP)	<ul style="list-style-type: none"> ▪ Supported ICMP types for Firewall include the following: <ul style="list-style-type: none"> - ECHO - ECHO REPLY - TIME EXCEEDED - TIMESTAMP - TIMESTAMP REPLY - UNREACHABLE ▪ Supported ICMP types for NAT include the following: <ul style="list-style-type: none"> - ECHO - ECHO REPLY - SOURCE QUENCH - TIME EXCEEDED

Application Layer Gateway	Features Supported
	<ul style="list-style-type: none"> - TIMESTAMP - TIMESTAMP REPLY - UNREACHABLE
Session Initiation Protocol (SIP)	<ul style="list-style-type: none"> ▪ Support RFC3261 for NAT and Firewall. Supported methods include the following: <ul style="list-style-type: none"> - ACK - BYE - CANCEL - INVITE - OPTIONS - REGISTER - RE-INVITE ▪ Only User Datagram Protocol (UDP) SIP is supported; Transmission Control Protocol (TCP) SIP is not supported.
Skinny Call Control Protocol (SCCP)	<ul style="list-style-type: none"> ▪ Supported messages for NAT and Firewall include the following: <ul style="list-style-type: none"> - CloseReceiveChannel - OpenReceiveChannelAck - Register ack - Register message - Register reject - StartMediaTransmission - StopMediaTransmission
Trivial File Transfer Protocol (TFTP)	<ul style="list-style-type: none"> ▪ Support for NAT and Firewall. ▪ Support opcode RRQ (read request) and WRQ (write request) in RFC-1350.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Copyright © 2009-2012
Cisco Systems, Inc.
All rights reserved