

Ports and Protocols

Clearswift SECURE ICAP Gateway v4.10

Version 2.4

April 2019

Copyright

Version 2.4, April 2019

Published by Clearswift Ltd.

© 1995–2019 Clearswift Ltd.

All rights reserved.

The materials contained herein are the sole property of Clearswift Ltd unless otherwise stated. The property of Clearswift may not be reproduced or disseminated or transmitted in any form or by any means electronic, mechanical, photocopying, recording, or otherwise stored in any retrievable system or otherwise used in any manner whatsoever, in part or in whole, without the express permission of Clearswift Ltd.

Information in this document may contain references to fictional persons, companies, products and events for illustrative purposes. Any similarities to real persons, companies, products and events are coincidental and Clearswift shall not be liable for any loss suffered as a result of such similarities.

The Clearswift Logo and Clearswift product names are trademarks of Clearswift Ltd. All other trademarks are the property of their respective owners. Clearswift Ltd. (registered number 3367495) is registered in Britain with registered offices at 1310 Waterside, Arlington Business Park, Theale, Reading, Berkshire RG7 4SA, England. Users should ensure that they comply with all national legislation regarding the export, import, and use of cryptography.

Clearswift reserves the right to change any part of this document at any time.

Contents

1	Connection Ports and Protocols.....	4
1.1	External Connections	5
1.2	Internal Connections.....	6
1.3	Change History	7

1 Connection Ports and Protocols

The Clearswift SECURE ICAP Gateway requires connectivity to external services over a number of different ports and protocols.

Clients should be aware that these entries may be liable to change with limited notice as Clearswift extends its infrastructure to exceed demands.

Wherever possible, clients should configure their firewalls to utilize the hostname of the service and only use IP addresses if defining access by hostname is not possible.

When using Clearswift SECURE ICAP Gateway with other third-party solutions, it need check the ports and protocols requirement of the other solution to allow a smooth integration between both products.

1.1 HTTP/S Proxy support restrictions

Customers using HTTP/S proxies will suffer from 2 issues

1. If customers are using Avira or Kaspersky AV with Cloud Lookup enabled will not be able to decrypt the 443 traffic due to it being a proprietary protocol, therefore it is advisable to bypass any form of scanning.
2. Customers performing license validation can either bypass content inspection on the proxy or deploy a client certificate to enable the SSL content to be processed and validate the license key correctly.

1.2 External Connections

The following table summarizes the required connections from the Gateway to or from servers outside the organization.

Description	Protocol	Port	Direction	Hostname/URL	Current IP Address
DNS requests to Internet servers	UDP	53	Out/In		
Avira AV Updates	TCP	80	Out	aav-update-1.clearswift.net aav-update-2.clearswift.net aav-update-3.clearswift.net aav-update-4.clearswift.net	185.155.104.24 70.33.161.213 185.155.104.25 70.33.161.214
Kaspersky AV updates	TCP	80	Out	kav-update-8-1.clearswift.net kav-update-8-2.clearswift.net kav-update-8-3.clearswift.net kav-update-8-4.clearswift.net	185.155.104.24 70.33.161.213 185.155.104.25 70.33.161.214
Sophos AV updates	TCP	80	Out	sav-update-1.clearswift.net sav-update-2.clearswift.net sav-update-3.clearswift.net sav-update-4.clearswift.net	185.155.104.24 70.33.161.213 185.155.104.25 70.33.161.214
Clearswift Update Server	TCP	80	Out	repo.clearswift.net rh.repo.clearswift.net	46.51.174.180 176.34.178.169 54.216.128.43
Avira APC Cloud lookup	TCP	443	Out	query-api.eu1.apc.avira.com	See https://ip-ranges.amazonaws.com/ip-ranges.json
Sophos Cloud Lookups	TCP	443	Out	cls.sophosxl.net	Multiple servers exist and are subject to change
Kaspersky KSN lookup	TCP	443	Out	ksn1.kaspersky-labs.com ksn2.kaspersky-labs.com ksn3.kaspersky-labs.com ksn4.kaspersky-labs.com ksn-url.geoksn.kaspersky.com	Multiple servers exist and are subject to change
RSS Feed	TCP	80	Out	www.clearswift.com	185.181.126.115
Gateway online help	TCP	80	Out	apphelpweb.clearswift.com	75.125.18.99
Service Availability List	TCP	80	Out	services1.clearswift.net services2.clearswift.net	See https://ip-ranges.amazonaws.com/ip-ranges.json

Description	Protocol	Port	Direction	Hostname/URL	Current IP Address
URL Database Updates	TCP	80	Out	url1.clearswift.net url2.clearswift.net url3.clearswift.net url4.clearswift.net	185.155.104.24 70.33.161.213 185.155.104.25 70.33.161.214
NTP server	UDP	123	Out/In	time.clearswift.net	Forms part of the NTP Pool project (http://www.pool.ntp.org)
Clearswift license key validation	TCP	443	Out	applianceupdate.clearswift.com	86.188.240.24 213.106.99.208 46.236.38.70

1.3 Internal Connections

The following table summarizes the required connections from the Gateway to or from servers inside the organization.

Description	Protocol	Port	Direction	Comment
FTP/S Backup/Restore	TCP	20/21	Out	
SSH access to the Gateway Console	TCP	22	In	Disabled by default
SFTP Lexical data import	TCP	22	Out	To the server containing the lexical data
SFTP Backup & Restore	TCP	22	Out	To the backup server
SFTP Transaction Log Export	TCP	22	Out	To the log repository server
Outbound SMTP for alerts	TCP	25	Out	
DNS requests to internal servers	UDP	53	Out	
NTP to internal server	UDP	123	Out/in	By default it is configured to connect to Clearswift NTP server
SNMP monitoring	UDP	161	In	From SNMP management servers
SNMP alerts	UDP	162	Out	
LDAP Directory access	TCP	389	Out	The port is configurable
Secure LDAP Directory access	TCP	636	Out	The port is configurable

Description	Protocol	Port	Direction	Comment
HTTPS access to the Gateway's Web Interface	TCP	443	In	
HTTPS Lexical data import	TCP	443	Out	To the server containing the lexical data
SYSLOG export	TCP	514	Out	To the central SYSLOG server
FTPS Lexical data import	TCP	990/21	Out	To the server containing the lexical data
FTPS Backup & Restore	TCP	990/21	Out	To the backup server
FTPS Transaction Log Export	TCP	990/21	Out	To the log repository server
SCOM Monitoring	TCP	1270	In	From the SCOM server
ICAP Service	TCP	1344	In	This port is configurable
LDAP connection to an active directory global catalogue	TCP	3268	Out	
	TCP	3269	Out	
Distribution of information to peer appliances	UDP	9000	In/Out	

1.4 Change History

Date	Vers	Description
Oct-2018	2.2	Add additional IPs for new AV mirrors (old addresses will be retired) URL database downloads from new servers. Change to Clearswift Website The following addresses used for AV updates will be retired on 22/11/18 184.72.245.1, 79.125.8.252, 175.41.136.7, 174.129.26.118, 176.34.251.142 and 54.254.98.96 The URL database servers on 79.125.3.206, 184.72.241.7, 174.129.200.98 and 46.137.169.34 will be retired on 22/11/18
Nov-2018	2.3	Added aav-update[1-4] update servers
April-2019	2.4	Add more details to Cloud lookups