

Ports and Protocols

Clearswift SECURE ICAP Gateway v4.7

Version 2.0

January 2018

Copyright

Version 2.0, January, 2018

Published by Clearswift Ltd.

© 1995–2018 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	4
1.2	Internal Connections.....	5

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.

1.1 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		
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 kav-update-8-5.clearswift.net kav-update-8-6.clearswift.net	184.72.245.1 79.125.8.252 175.41.136.7 174.129.26.118 176.34.251.142 54.254.98.96
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 sav-update-5.clearswift.net sav-update-6.clearswift.net	184.72.245.1 79.125.8.252 175.41.136.7 174.129.26.118 176.34.251.142 54.254.98.96
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
RSS Feed	TCP	80	Out	www.clearswift.com	162.13.22.202
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	79.125.3.206 184.72.241.7 174.129.200.98 46.137.169.34
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	213.146.158.142 46.227.51.215

1.2 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	