clearswift
RUAG Cyber Security

Ports and Protocols

Clearswift SECURE Web Gateway v4.11

Version 2.6

August 2019

Copyright

Version 2.6, August 2019

Published by Clearswift Ltd.

Contents

1 Connection Ports and Protocols 4
1.1 External Connections 5
1.2 Internal Connections 7
1.3 HTTP/S Proxy support restrictions 8
1.4 Change History 9

1 Connection Ports and Protocols

The Clearswift SECURE Web 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
FTP Over HTTP	TCP	20/21	Out		
DNS requests to Internet servers	UDP/TCP	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
OneCRL	TCP	443	Out	One-crl.clearswift.net	185.155.104.24 70.33.161.213 185.155.104.25 70.33.161.214
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
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
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	185.181.126.115

Description	Protocol	Port	Direction	Hostname/URL	Current IP Address
Appliance online help	TCP	80	Out	apphelpweb.clearswift.com	79.125.18.99
Service Availability List	TCP	80	Out	services1.clearswift.net services2.clearswift.net services3.clearswift.net	See https://ip-ranges.amazonaws.com/ip-ranges.json
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	0.rhel.pool.ntp.org 1.rhel.pool.ntp.org 2.rhel.pool.ntp.org 3.rhel.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
General HTTPS web access	TCP	443	Out		
HTTP/S block page (images)	TCP	8444	In		<ip address of Gateway>
WCCPv2	GRE (47) TCP TCP	 8444 9102	In In In		
PBR	TCP TCP	8444 9102	In In		

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	
User Authentication using Kerberos	TCP UDP	88 88	Out Out	
NTP to internal server	UDP	123	Out/in	By default it is configured to connect to Clearswift NTP server
User Authentication using NTLM	TCP UDP TCP TCP	135 137 139 445	Out Out Out Out	To directory servers
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
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

Description	Protocol	Port	Direction	Comment
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
LDAP connection to an active directory global catalogue	TCP TCP	3268 3269	Out Out	
Master/Slave HTTPS configuration	TCP TCP TCP	8071 8070 8090	In (Master) In (Slave) In (Slave)	Communications are always between Master and Slaves. So "In" for Master means "Out" from Slaves to Master
Distribution of information to peer appliances	UDP	9000	In/Out	This port is configurable through the Web UI

1.3 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.

1.4 Change History

Date	Vers	Description
Oct-2018	2.2	Add additional IPs for new AV mirrors (old addresses will be retired) Add OneCRL entries for certificate revocation feature in 4.9 release URL database downloads from new servers. Change 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
May-2019	2.5	Add 8444 for HTTP/S block page images
Aug-19	2.6	Updated for 2.6