clearswift
RUAG Cyber Security

Ports and Protocols

Clearswift SECURE Exchange Gateway V4.11

Issue 2.6

August 2019

Copyright

Contents

Connection Ports and Protocols

The Clearswift SECURE Exchange Gateway Version 4 requires connectivity to both internal and external services over several different ports and protocols.

Clearswift recommends that Exchange Gateways have unrestricted outbound access to HTTP, HTTP/S and DNS services to permit connections to the various cloud based services used for detection of spam and malware.

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

However, Clearswift appreciates that some customers may wish to restrict access to HTTP, HTTP/S and DNS services using external firewall rules. Clearswift recommends customers configure their firewalls to utilise the Hostname of the service and only use IP addresses if defining access by hostname is not possible.

DNS configuration

The performance of the DNS servers in use will have an effect on overall message processing rates, therefore choose the fastest most reliable servers.

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, they 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.

External Connections

Item	UDP/ TCP	Port	Details
DNS	UDP/ TCP	53 (in/out)	If the Gateway will use an **internal DNS** then the local DNS servers have full access then no changes are required (which is the norm) If the Gateway is using an **external DNS** server then the Gateway needs to have unrestricted access to DNS for resolution

Item	UDP/ TCP	Port	URL/Hostname	IP Address
Appliance online help	TCP	80	apphelp.clearswift.com	79.125.18.99
Product and OS updates	TCP	80	Repo.clearswift.net rh.repo.clearswift.net	46.51.174.180 176.34.178.169 54.216.128.43
Avira AV updates	TCP	80	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	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	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
RSS Feed	TCP	80	www.clearswift.com	185.181.126.115
Service availability list	TCP	80	services1.clearswift.net services2.clearswift.net services3.clearswift.net	See https://ip-ranges.amazonaws.com/ip-ranges.json
NTP server	UDP	123	0.rhel.pool.ntp.org 1.rhel.pool.ntp.org 2.rhel.pool.ntp.org 3.rhel.pool.ntp.org	
Avira APC Cloud lookup	TCP	443	query-api.eu1.apc.avira.com	See https://ip-ranges.amazonaws.com/ip-ranges.json
Kaspersky KSN lookup	TCP	443	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
Sophos Cloud Lookups	TCP	443	cls.sophosxl.net	Multiple servers exist and are subject to change
License key validation	TCP	443	applianceupdate.clearswift.com	86.188.240.24 213.106.99.208 46.236.38.70

Internal Connections

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
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
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

Description	Protocol	Port	Direction	Comment
LDAP connection to an active directory global catalogue	TCP TCP	3268 3269	Out Out	
Distribution of information to peer appliances	UDP	9000	In/Out	This port is configurable through the Web UI

Change History

Date	Vers	Description
Oct-2018	2.3	Add additional IPs for new AV mirrors (old addresses will be retired) 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
Nov-2018	2.4	Added aav-update[1-4] update servers
April-2019	2.5	Add more details to Cloud lookups
Aug-19	2.6	Updates for 4.11