clearswift
RUAG Cyber Security

Ports and Protocols

Clearswift SECURE Email Gateway V4.11

Issue 2.6

August 2019

Copyright

Contents

Connection Ports and Protocols

The Clearswift SECURE Email Gateway Version 4 requires connectivity to both internal and external services over a number of different ports and protocols.

Clearswift recommends that Email 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. It is advisable not to use large public DNS servers such as Google's 8.8.8.8 service as the behaviour of RBL servers will be impaired.

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.

External Connections

Item	UDP/ TCP	Port	Details	
TRUSTmanager LiveFeed checks	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**	**Hostname**	**IP Address**
SMTP	TCP	25	Any	Any
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
SpamLogic Rule/Engine updates	TCP	80	If the customer is using a HTTP Proxy then the HTTP proxy must be able to access the servers listed in Section 4 – Spam Rule updates If the customer is *NOT* using a HTTP Proxy then the Gateway must be able to access the servers listed in Section 4 – Spam Rule updates	
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
Spam Detection Stats	TCP	80	Clearswiftstat.mailshell.net	45.79.132.16
SwissSign mpki interface	TCP	443	ra.swisssign.net	
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	
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
Accessing keyservers over LDAP and LDAP/S	TCP	389 636	Out	
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
Accessing keyservers over HTTP and HTTP/S	TCP	443 11371	Out	
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	
Distribution of information to peer appliances	UDP	9000	In/Out	This port is configurable through the Web UI
Greylisting synchronisation between peers	UDP	19200	In/Out	Greylist sync

Spam Rule Updates

The following servers are accessed by the product to gather update information and to perform real-time checks

- sn12.mailshell.net
- sn60.mailshell.net
- db11.spamcatcher.net
- verio.mailshell.net
- ruledownloads.mailshell.net
- tisdk.mailshell.net

178.79.188.10
82.165.143.243
104.131.131.132
173.255.209.236
173.255.232.151
176.58.112.126
176.58.117.75
212.71.251.168
80.85.85.200
162.216.18.163
173.230.152.57
213.171.205.141
50.21.180.126

50.116.4.68
80.85.85.58
88.208.248.146
178.79.182.43
87.106.141.10
88.80.190.155
104.200.24.34
192.155.86.92
209.157.64.163
209.157.64.164
209.157.64.166
209.157.64.175
209.157.64.177

198.74.58.243

TRUSTmanager Connections

The following name servers are accessed by the product to verify information about the senders IP and its reputation.

- dnsbl7.mailshell.net
- lbl7.mailshell.net
- lbl8.sn12.mailshell.net
- rules.mailshell.net
- lbl8.mailshell.net

173.255.254.232
198.58.97.43
88.80.184.106
139.162.166.52
209.157.64.166
74.208.79.224
74.208.99.25
74.208.79.219
87.106.214.177
87.106.240.160
176.58.99.196
176.58.99.197
178.79.190.135
178.79.163.250
178.79.164.196
176.58.117.5
178.79.190.174
178.79.138.31
176.58.111.163
178.79.152.167
176.58.112.160
176.58.115.138
50.116.50.102
50.116.50.105
50.116.50.109
173.255.234.85
50.116.2.121

173.255.243.160
198.74.57.188
74.207.240.108
50.116.63.215
50.116.63.216
50.116.62.242
50.116.61.111
50.116.14.27
173.255.245.232
192.155.84.126
66.175.223.13
50.116.11.250
176.58.119.151
176.58.101.140
85.159.211.160
178.79.143.222
178.79.183.81
50.116.50.197
50.116.50.202
66.175.214.89
173.255.218.51
192.155.87.170
192.81.134.251
176.58.111.122
176.58.111.124
176.58.115.39
178.79.128.94
178.79.150.32

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 2019	2.6	Update for 4.11