clearswift

Clearswift SECURE Email Gateway V4.x

Ports and Protocols

Issue 1.5

November 2016

Copyright

Version 1.5, November, 2016

Published by Clearswift Ltd.

Contents

1 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. The requirements of Version 4 differs from V3.X.

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

Where possible, customers should configure their firewalls to utilise the Hostname of the service and only use IP addresses if defining access by hostname is not possible.

2 External Connections

Item	Protocol	Port	URL/Hostname
TRUSTmanager LiveFeed checks	UDP/TCP	53 (in/out)	dnsbl7.mailshell.net lbl7.mailshell.net lbl8.sn12.mailshell.net rules.mailshell.net lbl8.mailshell.net
EMEA/APAC IP addresses			
176.58.111.122, 176.58.111.124, 176.58.115.39, 178.79.128.94, 178.79.150.32, 87.106.214.177, 87.106.240.160, 176.58.99.196,176.58.99.197, 176.58.111.163, 176.58.112.160, 176.58.115.138, 176.58.117.5, 178.79.138.31, 178.79.152.167, 178.79.163.250, 178.79.164.196, 178.79.190.135, 178.79.190.174, 178.79.143.222, 176.58.119.151, 176.58.101.140, 85.159.211.160, 178.79.183.81, 173.255.254.232, 198.58.97.43, 88.80.184.106			
US IP Addresses			
192.155.87.170, 192.81.134.251, 50.116.50.197, 50.116.50.202, 66.175.214.89, 173.255.218.51, 209.157.64.166, 74.208.79.224, 74.208.99.25, 74.208.79.219, 173.255.234.85, 173.255.243.160, 173.255.245.232, 192.155.84.126, 198.74.57.188, 50.116.2.121, 50.116.11.250, 50.116.14.27, 50.116.50.102, 50.116.50.105, 50.116.50.109, 50.116.63.215, 50.116.63.216, 50.116.62.242, 50.116.61.111, 66.175.223.13, 74.207.240.108			

Item	Protocol	Port	URL/Hostname	IP Address
DNS	UDP	53		
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
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 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	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

SpamLogic Rule/Engine updates	TCP	80	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 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
RSS Feed	TCP	80	www.clearswift.com	162.13.22.202
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	time.clearswift.net (default)	Forms part of the NTP Pool project
License key validation TRUSTmanager stats collection	TCP	443	applianceupdate.clearswift.com	86.188.240.24 213.106.99.208 46.236.38.70

3 Internal Connections

Item	Protocol	Port
For backing up and restoring the system	TCP	FTP 21 FTP/S 21 or 990 SFTP 22
Secure console access	TCP	SSH 22
Browser access to the management UI Peer communications	TCP	443
Browser access to the PMM UI	TCP	80
Connecting to directory servers for user authentication (PMM)	TCP	135 139 445
Connecting to directory servers for user authentication (PMM)	UDP	137
For accessing directory servers Accessing Global Catalogue server (normal and secure)	TCP	389 3268 3269 LDAP/S 636
Accessing keyservers over LDAP and LDAP/S	TCP	LDAP 389 LDAP/S 636
Accessing keyservers over HTTP and HTTP/S	TCP	HTTP 11371 HTTP/S 443
Greylisting synchronisation between peers	UDP	19200
SNMP alerts from the system	UDP	162
To the server containing the lexical data HTTP/S, SFTP, FTP/S	TCP	HTTP/S 443 SFTP 22 FTPS 990
To the central SYSLOG server	TCP	514

4 Subnet handling

Some of the addresses entered are in the format of 72.21.192.0/19, which implies that they use a special 19 bit subnet mask and when applied to IP address ranges can extend or reduce the maximum permissible number of addresses available for usage.

In this example 72.21.192.0/19, provides for a range of addresses from 72.21.192.1 to 72.21.223.254.