clearswift

Clearswift SECURE Email Gateway V3.*

Ports and Protocols

Issue 3.14

October 2016

Copyright

Version 1.1, October, 2016

Published by Clearswift Ltd.

Contents

1 Connection Ports and Protocols

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

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

The following table summarizes the required connections from the Gateway to or from servers outside the organization.

Description	Protocol	Port	Hostname/URL	Current IP Address
Appliance online help	TCP	80	apphelp.clearswift.com	79.125.18.99
Product updates	TCP	80	app-patches.clearswift.net	54.231.0.0./17 72.21.192.0/19 207.171.160.0/19 87.238.86.0/23 178.236.4.0/19
License key validation	TCP	443	applianceupdate.clearswift.com	86.188.240.24 213.106.99.208 46.236.38.70
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
TRUSTmanager stats collection	TCP	443	applianceupdate.clearswift.com	213.106.99.208 86.188.240.24
TRUSTmanager host checking	UDP	8007	Reputations1.clearswift.net Reputations2.clearswift.net reputations3.clearswift.net reputations4.clearswift.net	175.41.129.251 46.51.189.37 79.125.11.244 75.101.139.128

Description	Protocol	Port	Hostname/URL	Current IP Address
Spam Signatures cloud **(Also see section 1.3 of this document)**	TCP	80	bulkmail1.clearswift.net bulkmail2.clearswift.net bulkmail3.clearswift.net bulkmail4.clearswift.net bulkmail5.clearswift.net	84.39.153.31 64.191.223.35 38.113.116.210 216.163.188.45 84.39.152.31
Spam Signatures download (pre 3.1)	TCP	80	spamupdate-appliance.clearswift.com	204.236.225.214 75.101.147.224
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	72.21.192.0/19 207.171.160.0/19 87.238.86.0/23 178.236.4.0/19 89.21.228.84
DNS	UDP	53		
NTP server	UDP	123	time.clearswift.net	Forms part of the NTP Pool project

3 Internal Connections

Description	Protocol	Port	Comment
FTP	TCP	20,21	For backing up and restoring the system
SSH	TCP	22	Secure console access
HTTP/S	TCP	443	Browser access to the management UI Peer communications
HTTP	TCP	80	Browser access to the PMM UI
NTLM (PMM)	TCP	135 139 445	Connecting to directory servers for user authentication
NTLM (PMM)	UDP	137	Connecting to directory servers for user authentication
LDAP (Address lists & PMM)	TCP	389 3268 3269	For accessing directory servers Accessing Global Catalogue server (normal and secure)
LDAP Key server (Encryption)	TCP	389	Accessing keyservers over LDAP
HTTP Key server (Encryption)	TCP	11371	Accessing keyservers over HTTP
Greylisting (Anti-spam)	UDP	19200	Greylisting synchronisation between peers
SNMP alerts	UDP	162	SNMP alerts from the system
SFTP Lexical data import	TCP	22	To the server containing the lexical data
SYSLOG export	TCP	514	To the central SYSLOG server
FTPS Lexical data import	TCP	990	To the server containing the lexical data

4 Spam Signatures (Cloud)

This service uses global load balancers to distribute traffic to the most appropriate servers in your region. The entries in the table are effective for EMEA, but customers in APAC, US, Latin America and Japan should determine their local resolvers by using NSLOOKUP as follows:

```
C:\>nslookup
Default Server:  XXXXX.clearswift.org
Address:  10.XX.XX.XXX
> set type=a
> bulkmail1.clearswift.net
Server:  XXXXX.clearswift.org
Address:  10.XX.XX.XXX

Name:    resolver.1.geo.ctmail.com
Address:  84.39.153.31
Aliases:  bulkmail1.clearswift.net
```

For each of the 5 designated servers (bulkmail1 to bulkmail5) and setting their firewalls accordingly.

5 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.