Clearswift ARgon Gateway V1.8

Ports and Protocols

Issue 2.2

September 2018

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 Kaspersky AV with Cloud Lookup enabled will not be able to decrypt the 443 connection due to it being a proprietary protocol

2. Customers performing license validation can either bypass content inspection on the proxy or deploy a client certificate to enable the SSL content to processed and validate the license key correctly.

External Connections

Item	Protocol	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	
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
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	time.clearswift.net (default)	Forms part of the NTP Pool project
License key validation	TCP	443	applianceupdate.clearswift.com	86.188.240.24 213.106.99.208 46.236.38.70

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