Libraesva ESG Firewall Ports Requirements

Libraesva ESG needs to open and receive connections from and to some ports. You must completely exclude the firewall and all Layer-7 inspections from it on the listed ports.

Note: you can easily test your firewall configuration using the on-board Check Firewall Ports tool.

Mandatory ports

Below are the ports Libraesva ESG needs open.

- **TCP/UDP 53**: DNS (outbound) without Layer-7 firewall inspection
- **TCP 25**: SMTP (bi-directional) without Layer-7 firewall inspection
- **TCP 80**: HTTP (outbound) without Layer-7 firewall inspection
- **TCP 443**: HTTPS (outbound) without Layer-7 firewall inspection
- **TCP 2703**: Razor2 (outbound)
- **UDP 24441**: Pyzor (outbound)
- **UDP 6277**: DCC (outbound)

Optional ports

Below are the ports Libraesva ESG needs open if using the related service.

- **TCP 465**: SMTPS (inbound)
- **TCP 578**: SMTPS (inbound)
- **TCP 389**: LDAP (from Libraesva ESG to LDAP Server)
- **TCP 636**: LDAPS (from Libraesva ESG to LDAP Server)

More details

DNS **(port 53)**

ESG performs a very high volume of DNS requests during email analysis, for this reason it has a high performance recursive DNS onboard.
DNS is crucial both for being able to deliver email and to perform reputation checks of email relays, contents and links.
Using an external DNS may lead to delays in email delivery and in a degradation of the quality of the analysis.
The onboard DSN requires outbound traffic to port 53 (both UDP and TCP) to be allowed without any inspection or rate-limiting.

SMTP (port 25)

ESG must be able to receive email and to send outbound email (this includes NDR messages for inbound traffic), so traffic to TCP port 25 inbound and outbound must be unrestricted.
Content inspection on SMTP can interfere and impair ESG's ability to perform its task, it is advised to disable any content inspection for this traffic, ESG is a perimeter protection appliance designed to handle malicious content safely.

HTTP (port 80)

ESG analyses links in emails and also discovers the real link behind a shortener (or a chain of shorteners). Some of these links are in plain HTTP.
There are hundreds of shortening services and new services pop-up every day, so the list of IP addresses cannot be pre-determined and ESG must be able to access any host on TCP port 80 (outbound only).
If the firewall blocks this outbound traffic to port 80, ESG will not be able to resolve some of the shortened links and it will not be able to perform reputation checks on the real links hidden behind the shortening services (a very common technique to try to avoid reputation checks).
Inbound HTTP traffic is required for certificate renewal.
Let's Encrypt servers need to connect to Libraesva ESG on port 80 when issuing or renewing the certificate. The list of servers is not static and cannot be pre-authorised. If inbound traffic to port 80 is not allowed, Let's Encrypt certificates cannot be used.
Content inspection on HTTP can interfere and impair ESG ability to perform its task, it is advised to disable any content inspection for this traffic, ESG is a perimeter protection

appliance designed to handle malicious content safely.

HTTPS (port 443)

This protocol is used to download system updates, security updates, virus definition updates, engine updates and reputation data updates. Such updates happen continuously with a frequency of about five minutes.
This data is distributed through content delivery networks like Cloudflare’s and others. It is not possible to define a list of IP addresses to be pre-authorised therefore outbound traffic to TCP port 443 must be unrestricted for ESG.
If this traffic is restricted, ESG will not be able to perform it’s tasks.
Inbound HTTPS traffic must be allowed if the web interface of Libraesva ESG must be accessed from the Internet, this includes outlook plugins and mobile applications. Network restrictions can be configured on Libraesva ESG itself.

Razor2 (port 2703)

It is a distributed network of servers that share hashes of email features along with a reputation index. The system is used to quickly discover and block spam campaigns that hit multiple servers.
The protocol automatically discovers the list of IP addresses to connect to, the network is dynamic and a fixed list of IP addresses cannot be pre-approved.
The firewall configuration requires outbound TCP traffic to port 2703, this enables ESG to connect to any host but only on this port.
If the firewall blocks this traffic, ESG will not use razor2 for the email analysis, all other checks will be performed.

Pyzor (port 24441)

It is a distributed network of servers that share sanitised hashes of email contents. It is used to discover email campaigns that hit multiple email servers and multiple recipients with the same email content, which is one of the characteristics of spam campaigns.
The protocol automatically discovers the list of IP addresses to connect to, the network is dynamic and a fixed list of IP addresses cannot be pre-approved.
The firewall configuration requires outbound UDP traffic to port 24441, this enables ESG to connect to any host but only on this port.
If the firewall blocks this traffic, ESG will not use Pyzor for the email analysis, all other checks will be performed.

DCC (port 6277)

It is a distributed network of servers that share sanitised checksums of email contents It is used to discover email campaigns that hit multiple email servers and multiple recipients with the same email content, which is one of the characteristics of spam campaigns.
The protocol connects to Libraesva's DCC servers dcc1.esvacloud.com and dcc2.esvacloud.com.
The firewall configuration requires outbound UDP traffic to port 6277 of the servers above.
If the firewall blocks this traffic, ESG will not use DCC for the email analysis, all other checks will be performed.

OpenPGP (port 11371)

By convention and history, HKP uses HTTP on TCP port 11371, and HTTPS on TCP port 443. These are often distinguished from generic use of HTTP(S) by using the URI schemes "hkp" and "hkps". For reasons of maximum compatibility with firewalls and filtering HTTP proxies, HKP is also often served over the standard HTTP port (TCP port 80)

reference https://www.ietf.org/archive/id/draft-gallagher-openpgp-hkp-04.html