Control Center Syslog Service

https://campus.barracuda.com/doc/96026470/

The CC Syslog service collects log messages from CloudGen Firewalls that are managed by the Barracuda Firewall Control Center and streams those log messages to an external log host or sends them to the HA partner. Syslog streaming consists of three major steps:

- Log Reception
- Log Processing
- Log Delivery

Log Reception

Log reception via port 5144 and/or 5143:
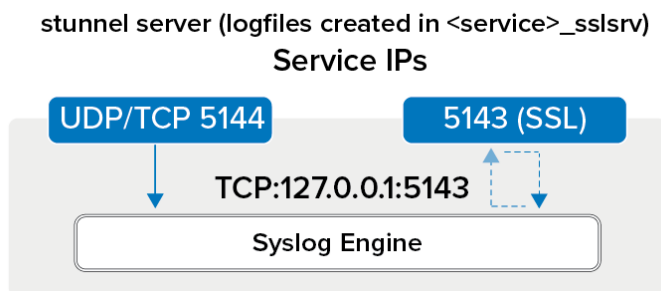
SSL-encrypted connections on port 5143 are used for log reception of managed boxes that do not use management tunnels. Using SSL allows for both encryption and authentication.
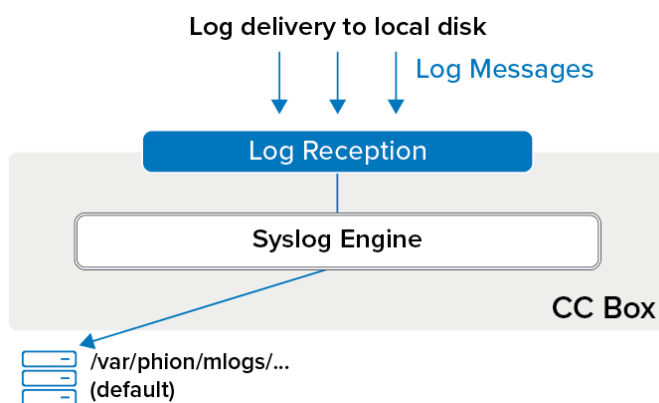
Managed firewalls using a remote management tunnel connect to the syslog engine on port 5144. These connections are unencrypted and unauthenticated, so the default firewall rules restrict access managed boxes and access via VPN tunnel.
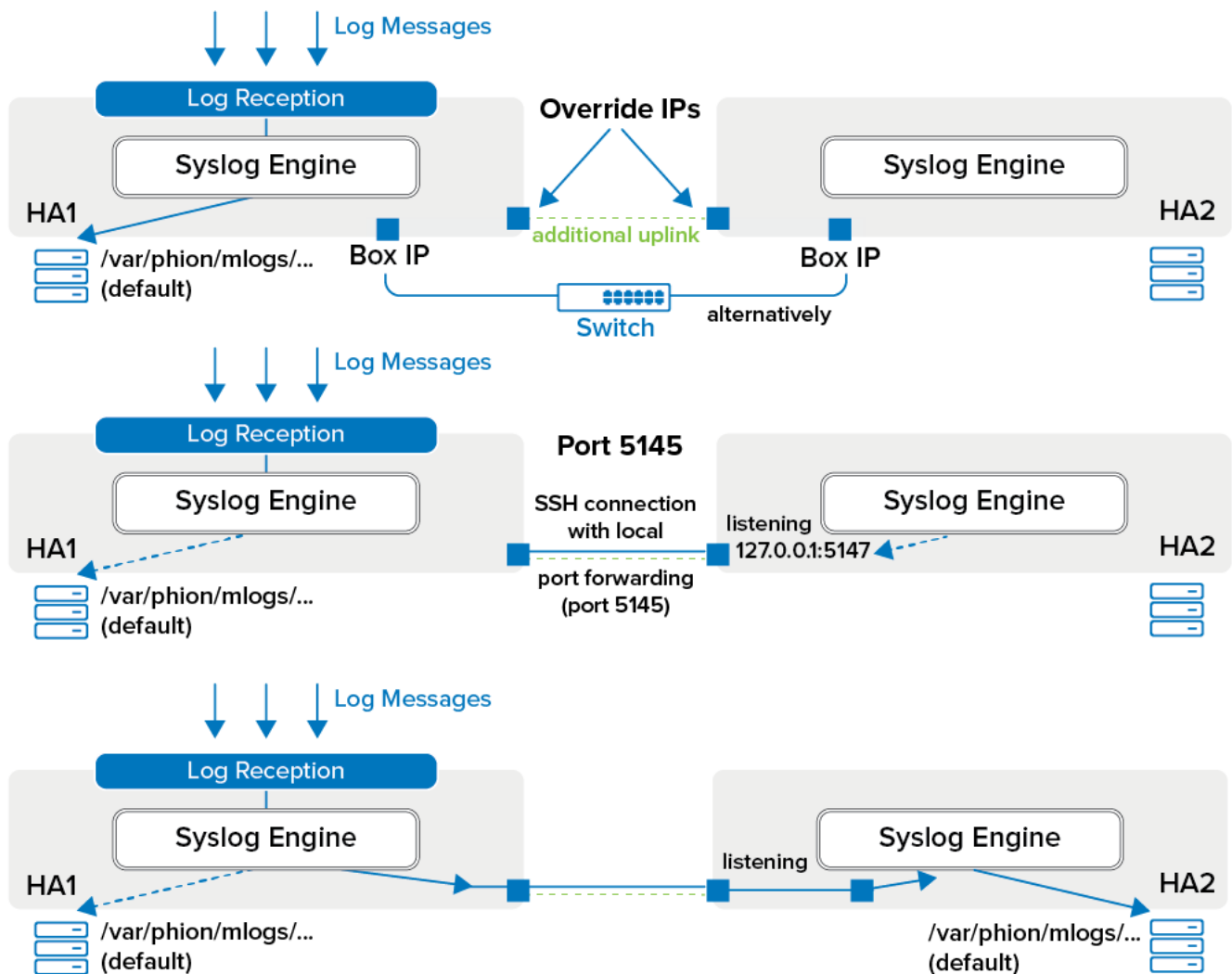
Log Processing
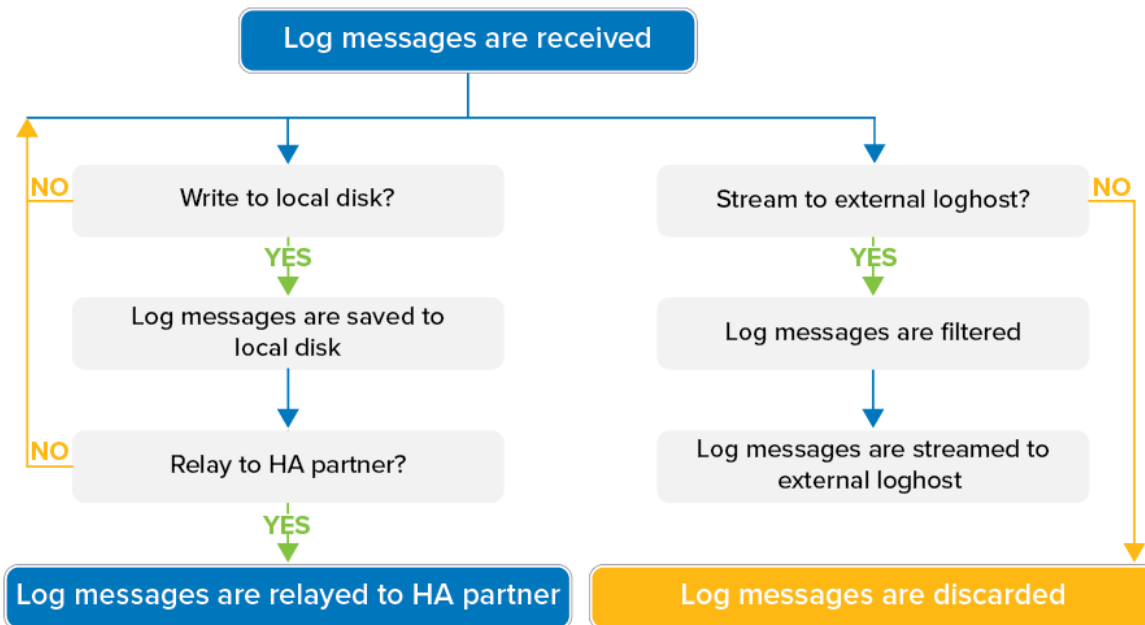
Log Delivery

Log Delivery to Local Disk

Log Delivery via Private Uplink (HA Sync)

Using override IP addresses is mandatory in this scenario:

Log Delivery by Relaying

The CloudGen Firewall supports active querying and passive receiving via SSL-encrypted connection or passive receiving without encryption.

Active SSL Querying

If read access is not possible (for example, because log host is down), transferring log messages is not possible. This method of transferring is not recommended for use in an HA Control Center cluster.
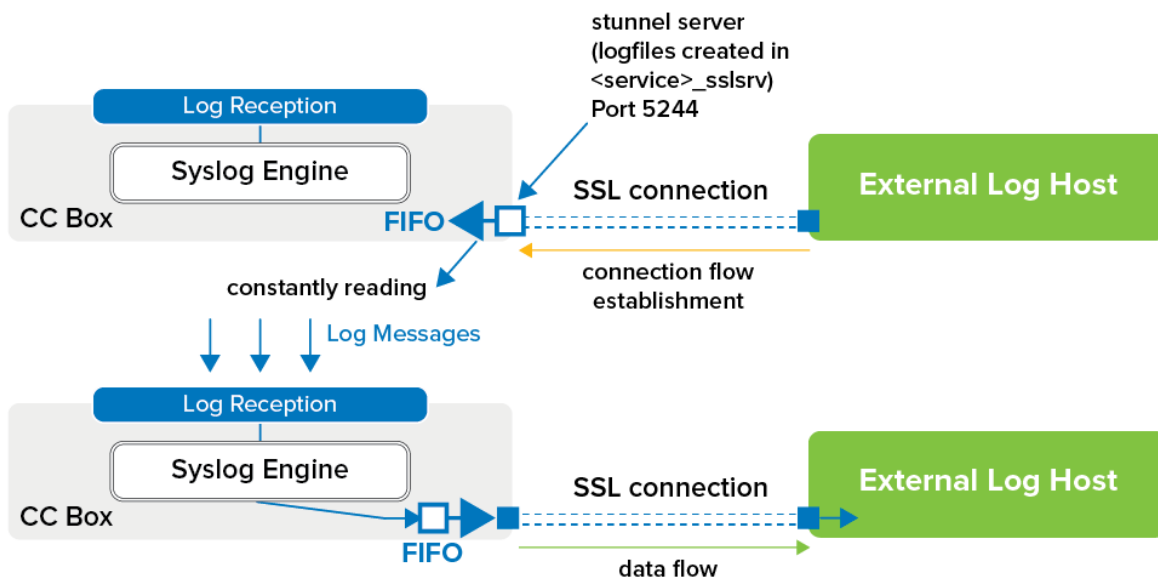
SSL Passive Receiving

Used for an HA Control Center cluster because the external log host does not need to know which partner is currently active for syslog streaming to work.
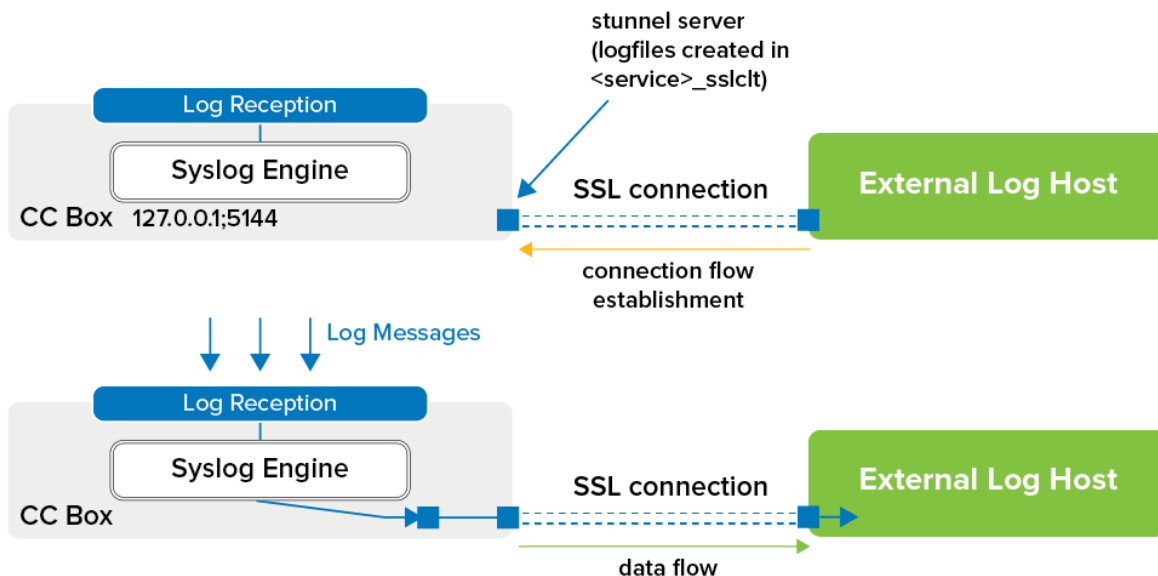
Plain Passive

You can also do standGard syslog streaming without an SSL connection if needed.

Figures

1. cc_syslog01.png
2. cc_syslog02.png
3. cc_syslog03.png
4. cc_syslog04.png
5. cc_syslog05.png
6. cc_syslog06.png