Prerequisites for Impex systems

SYSCTL AB

Contents

Definitions

Word	Definition
Impex	The family name of USB Protect, ICC, Repo and DataLock
ICC	The server which control the Stations
USB Protect	The kiosk computer used to scan mass storage devices
Repo	The server that has the updates and definitions
DataLock	Server used for network flows that will scan files before transferring them onwards
Network flows	This is the description of data being scanned and transferred through the DataLock to a remote destination. A DataLock can have multiple remote destinations configured
Operators	The users who will use the administrative interface on the ICC server

Installation preparation

This document explains the preparations that are needed before the installation and configuration of an Impex system can be done. These steps and the information collected should be documented and kept ready at the time of the installation to ensure proper configuration.

USB Protect

USB Protect needs the following documented: 1. IP-address 2. Netmask 3. Default gateway 4. DNS servers 5. Proxy configuration, optional 6. Fully qualified domain name 7. Fully qualified domain name for the ICC and REPO server 8. IP-address of the ICC

USB Protect needs the following configuration prepared:

1. Outbound firewall opening to the ICC server

DataLock need the following configuration prepared:

1. Inbound firewall opening from the sending part
2. Outbound firewall opening to the destination server

USB Protect needs port TCP/443 to be open outwards to be able to communicate with the ICC server and Repo server. USB Protect will synchronize time and obtain software updates over this port. It also uses this connection to upload scanning reports and system logs. All traffic between the Station USB to the ICC server is encrypted with TLS. If USB Protect cannot validate the server certificate, this is likely with a self signed certificate or a certificate from an internal CA, the Trust On First Use(TOFU) method will be used. If USB Protect uses a proxy the proxy must allow connections from the USB Protect to the ICC and the Repo server.

DataLock

The server can be a virtual appliance or a physical server. The server should have the following minimum specification:

1. 16 GB memory
2. 2 GHz CPU, 2 core or more depending on usage
3. 1 TB of disk storage or more depending on data usage in network flows

The DataLock server needs the following information before installation can be completed:

1. IP-address
2. Netmask
3. Default gateway
4. Proxy configuration, optional
5. Resolver
6. Fully qualified domain name
7. Fully qualified domain name for the ICC and REPO server

If firewall openings are required the following should be allowed:

1. Outbound firewall opening to the resolver
2. Outbound firewall opening to proxy, optional
3. Outbound firewall to the ICC server
4. Outbound firewall to the Repo server

DataLock needs port TCP/443 to be open outwards to be able to communicate with the ICC server and Repo server. DataLock will synchronize time and obtain software updates over this port. It also uses this connection to upload scanning reports and system logs. All traffic between the DataLock to the ICC server is encrypted with TLS. If DataLock cannot validate the server certificate, this is likely with a self signed certificate or a certificate from an internal CA, the Trust On First Use(TOFU) method will be used. If the DataLock uses a proxy the proxy must allow connections from the DataLock to the ICC and the Repo server.

The DataLock needs TCP/22 to be open for incoming and outgoing SFTP connections.

Repo server

The server can be a virtual appliance or a physical server. It is also possible to have the Repo services installed in the ICC server. The server should have the following minimum specification:

1. 16 GB memory
2. 2 GHz CPU, 4 cores
3. 500 GB of disk storage

The Repo server needs the following information before installation can be completed:

1. IP-address
2. Netmask
3. Default gateway
4. Proxy configuration, optional
5. Time server
6. Resolver
7. Fully qualified domain name

If firewall openings are required the following should be allowed:

1. Outbound firewall opening to updates.sysctl.se
2. Outbound firewall opening to time service (NTP)
3. Outbound firewall opening to proxy, optional
4. Outbound firewall opening to Active Directory, if used
5. Inbound firewall from Impex stations
6. Inbound firewall from ICC server
7. Inbound firewall from remote access solution, if used

ICC server

The server can be a virtual appliance or a physical server. The server should have the following minimum specification:

1. 16 GB MiB memory
2. 2 GHz CPU, 4 cores
3. 500 GB of disk storage

The ICC server needs the following information before installation can be completed:

1. IP-address
2. Netmask
3. Default gateway
4. Proxy configuration, optional
5. Time server
6. Resolver
7. Mail relay
8. Fully qualified domain name

If firewall openings are required the following must be allowed:

1. Outbound firewall opening to time service (NTP)
2. Outbound firewall opening to letsencrypt, if used
3. Outbound firewall opening to mail relay(SMTP), if used
4. Outbound firewall opening to proxy, if used
5. Outbound firewall opening to Active Directory, if used
6. Outbound firewall opening to Repo server
7. Inbound firewall from Impex stations
8. Inbound firewall from operators network
9. Inbound firewall from remote access solution, if used

Virtualization requirements

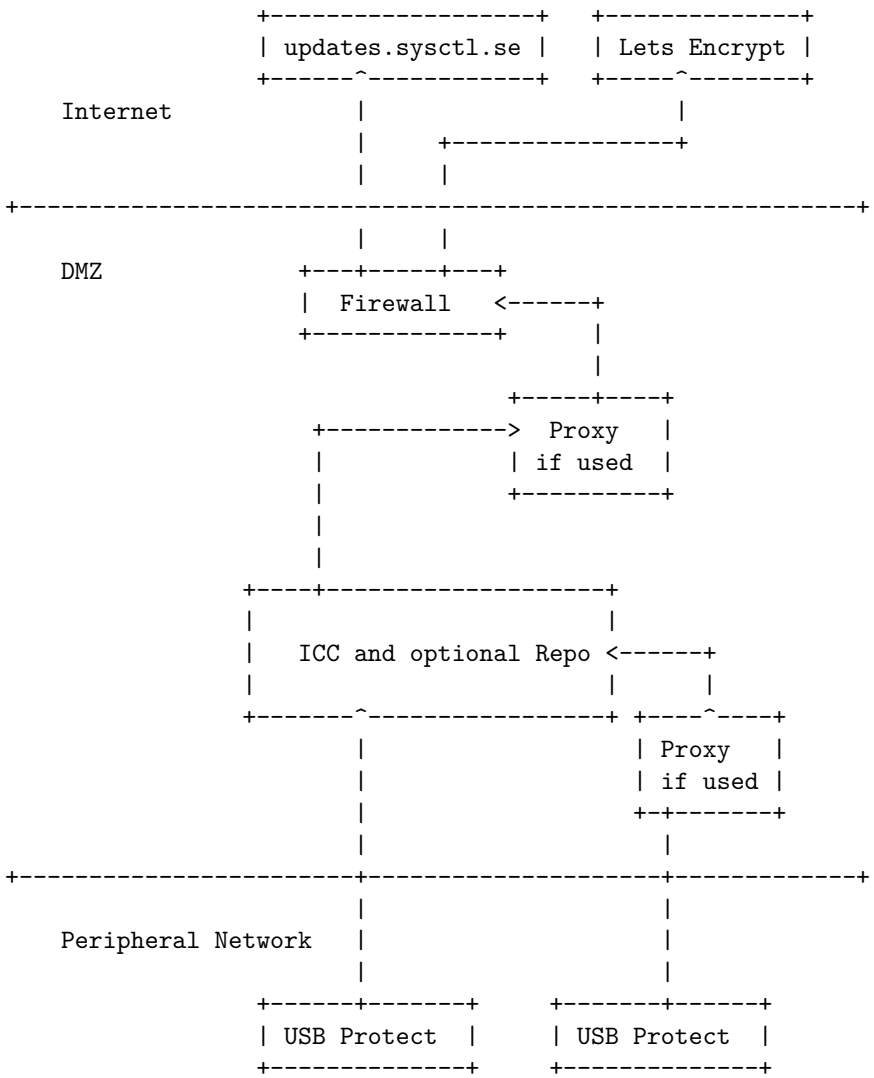
If the Repo server, DataLock or the ICC server is installed as a virtual server we recommend the options below. Other options might be possible but would require additional testing.

1. Boot options
    a. EFI boot is mandatory
    b. Secure boot when possible, mandatory for DataLock
2. One of the following disk devices
    a. SATA
    b. PV SCSI
3. Network options
    a. VMXNET3
4. Hardware options
    a. TPM when possible

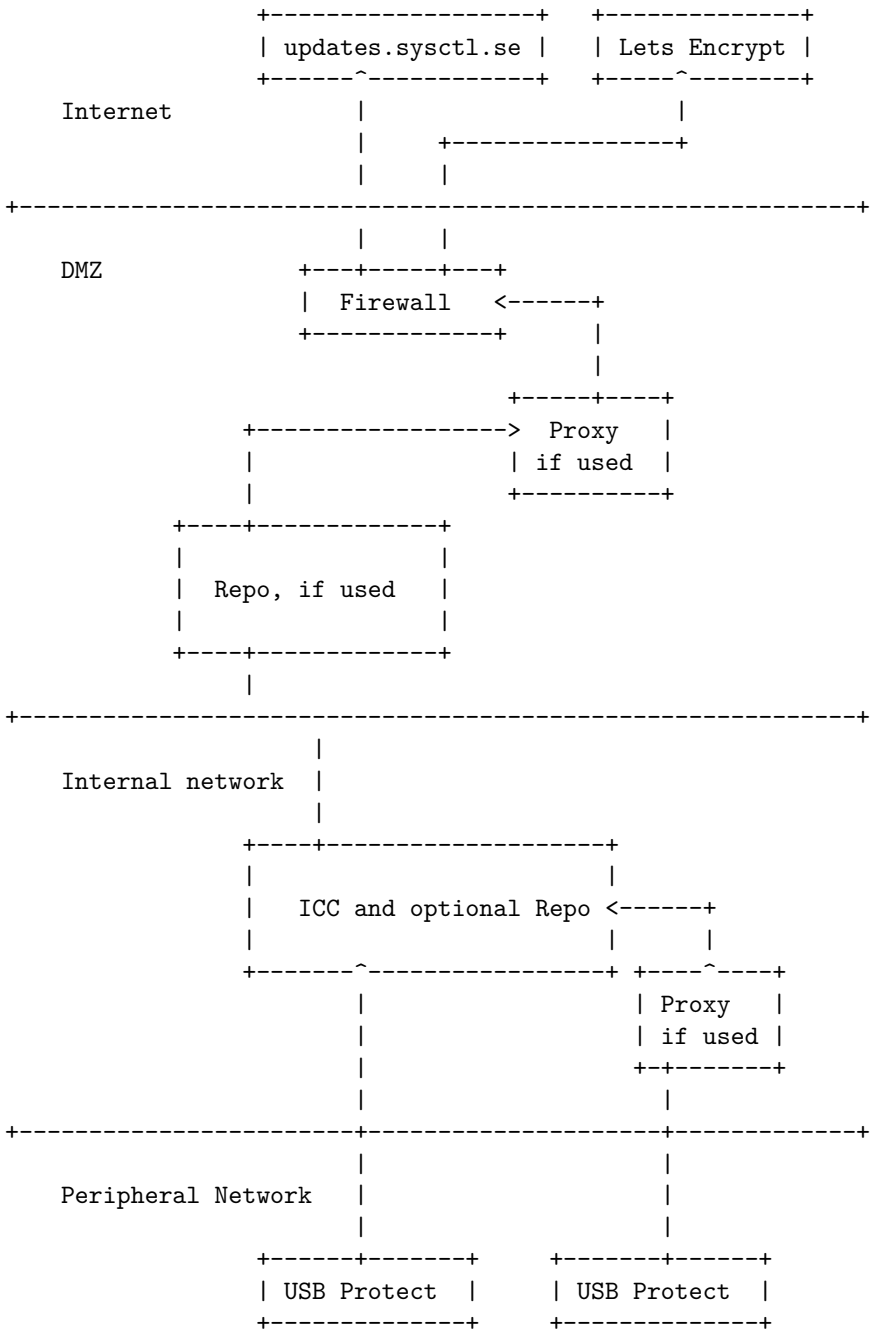
Network

The impex solution is built to be in architecures based on IEC62443 and simular zone concept solution as well as other network designs. This is two example of how Impex can fit in a network. The ICC and the Repo can be on the same machine and does not need to be separated servers. The solution supports a proxy but a proxy is not required.

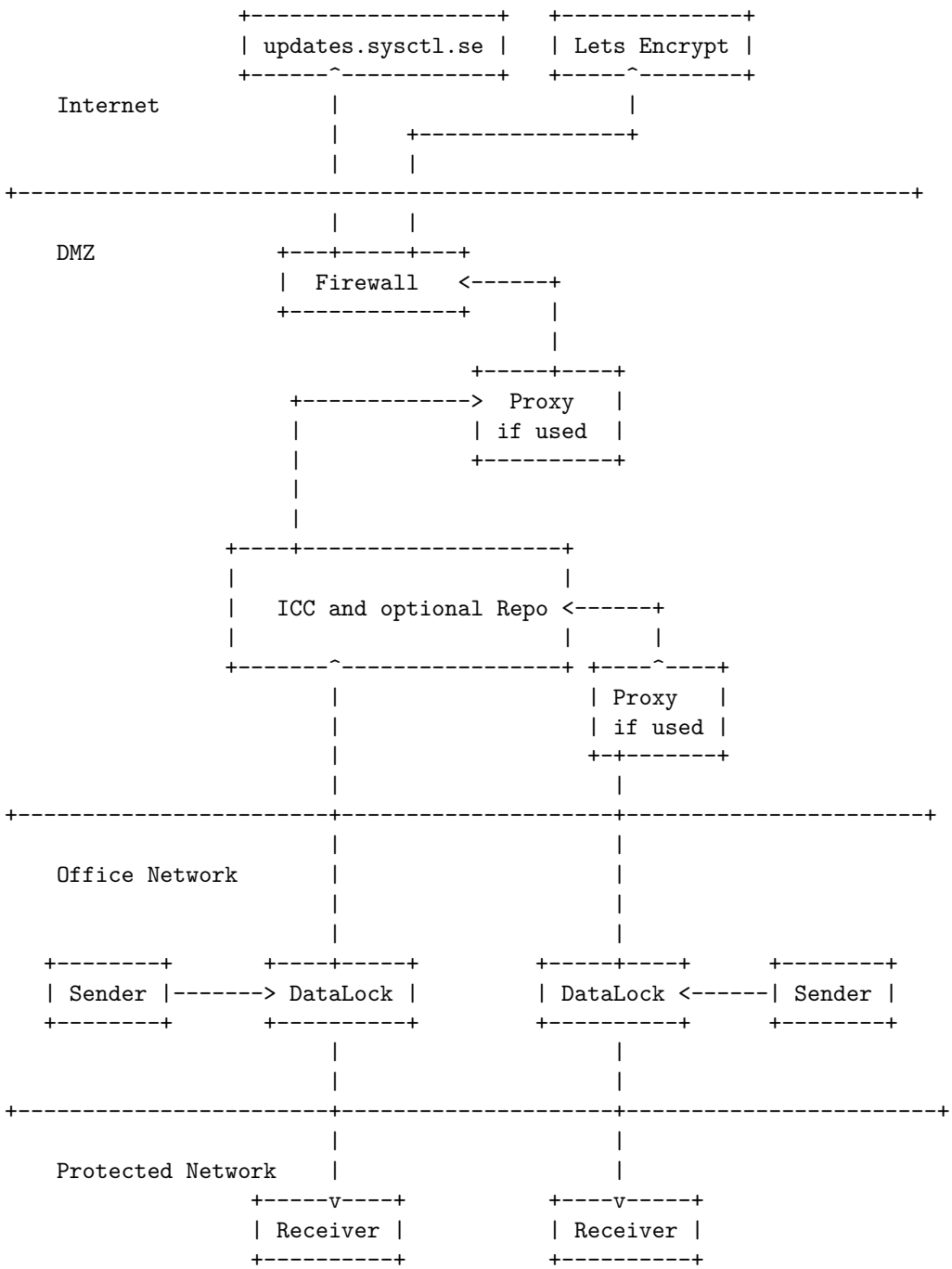
Network with ICC and Repo installed on the same server in a basic network



Network with ICC and Repo installed on seperate servers in a zone based network



Network for the DataLock



Internet dependencies

The Repo server requires internet connectivity to be able to access updates.sysctl.se for updates. All updates for Operating System, ICC-server, USB Protect, DataLock and AV-signatures are downloaded from updates.sysctl.se over a TLS-connection.

The ICC server supports the use of letsencrypt[1] to get a trusted certificate. Letsencrypt is not required and certificates can be installed manually to the ICC and Repo. Using the letsencrypt feature ensures that certificates are updated automatically. This greatly reduces administrative overhead, but as with all public CA:s, the certificate will be published in the CT log.

The Repo server is the only device that requires internet connection and it is only used to a clearly defined destination.

DMZ

The Repo server could be placed in a DMZ network segment. The Repo needs outbound connection to the internet and specifically updates.sysctl.se, this could be through a proxy.

Internal Network

The ICC server can as a suggestion be placed in an internal network and access to the ICC should be restricted by an external firewall. The ICC needs outbound connection to the Internet and specifically to Lets Encrypt when the module is used, this can be through a proxy.

The ICC server needs access to a time-server to get the correct time and a DNS server to resolv DNS names. If email notifications are enabled the ICC-server must have access to a mail relay.

The ICC server requires inbound connections from the Impex stations to be able to receive scanning reports. It should also allow inbound access from administrators and operators so that they can access the web interface.

It should also allow inbound access from administrators to the SSH console.

Peripheral Network

In the peripheral network or where the USB Protect are placed, the only network access needed is from the USB Protect is to the ICC server over TCP/443.

USB Protect are not listening on any port so it is not possible to connect to a station. It is possible to ping the devices, they allow ICMP echo and can send ICMP echo replies.

Protected Network

The protected network where the only way to transferer in files are through the DataLock.

[1] https://letsencrypt.org/

Firewalls and proxies

Firewall

The firewalls should limit access to the Stations and the ICC server and only allow the defined ports and protocols that are needed by the service.

Network ports with ICC and Repo on separate servers

Source	Destination	Port	Protocol	Optional
Repo server	updates.sysctl.se	TCP/443	SSL/TLS	No
ICC server	Repo server	TCP/443	SSL/TLS	No
ICC server	acme-v02.api.letsencrypt.org	TCP/80	HTTP or Acme protocol	Yes
ICC server	acme-v02.api.letsencrypt.org	TCP/443	SSL/TLS or Acme protocol	Yes
ICC server	Mail relay	TCP/25	STMP	Yes
ICC server	DNS servers	TCP/53	DNS	No
ICC server	DNS servers	UDP/53	DNS	No
ICC server	NTP server	UDP/123	NTP	No
ICC server	Proxy server	TCP/XXX	HTTP/HTTPS/SOCKS	Yes
Repo server	Proxy server	TCP/XXX	HTTP/HTTPS/SOCKS	Yes
USB Protect	Repo server	TCP/443	SSL/TLS	No
USB Protect	Proxy server	TCP/XXX	HTTP/HTTPS/SOCKS	Yes
USB Protect	ICC server	TCP/443	SSL/TLS	No
DataLock	Repo server	TCP/443	SSL/TLS	No
DataLock	Proxy server	TCP/XXX	HTTP/HTTPS/SOCKS	Yes
DataLock	ICC server	TCP/443	SSL/TLS	No
DataLock	Receiver server	TCP/22	SFTP	No
Sender server	DataLock	TCP/22	SFTP	No
Remote Access	ICC server	TCP/22	SSH	Yes
Operators	ICC server	TCP/443	SSL/TLS	Yes
.letsencrypt.org	ICC server	TCP/80	SSL/TLS or Acme protocol	Yes
.letsencrypt.org	ICC server	TCP/443	SSL/TLS or Acme protocol	Yes

Network ports with ICC and Repo on the same server

Source	Destination	Port	Protocol	Optional
ICC server	updates.sysctl.se	TCP/443	SSL/TLS	No
ICC server	acme-v02.api.letsencrypt.org	TCP/80	HTTP or Acme protocol	Yes

Source	Destination	Port	Protocol	Optional
ICC server	acme-v02.api.letsencrypt.org	TCP/443	SSL/TLS or Acme protocol	Yes
ICC server	Mail relay	TCP/25	STMP	Yes
ICC server	DNS servers	TCP/53	DNS	No
ICC server	DNS servers	UDP/53	DNS	No
ICC server	NTP server	UDP/123	NTP	No
ICC server	Proxy server	TCP/XXXHTTP/HTTPS/SOCKS		Yes
USB Protect	Proxy server	TCP/XXXHTTP/HTTPS/SOCKS		Yes
USB Protect	ICC server	TCP/443	SSL/TLS	No
DataLock	Proxy server	TCP/XXXHTTP/HTTPS/SOCKS		Yes
DataLock	ICC server	TCP/443	SSL/TLS	No
DataLock	Receiver server	TCP/22	SFTP	No
Remote Access	ICC server	TCP/22	SSH	Yes
Operators	ICC server	TCP/443	SSL/TLS	Yes
.letsencrypt.org	ICC server	TCP/80	SSL/TLS or Acme protocol	Yes
.letsencrypt.org	ICC server	TCP/443	SSL/TLS or Acme protocol	Yes

Proxy

The ICC server, Repo server, DataLock and USB Protectcan use a proxy but it is optional and if no proxy should be used is it still possible to use the services.

Proxy configuration

The ICC server, Repo server, DataLock and the USB Protect have support for the most common proxies and the proxy should be configured to limit the server to only access the required domains.

Transparent proxy

If there are any transparent proxies who try to inspect the traffic, the connection will fail due to strong encryption and certificate validation enforcements. It is recommended to use syslog to get audit logs from the systems.

Checklist

The information below should be filled in before the installation date.

Signature:

_____

Name:

_____

Contacts

Sysctl would like to have email and optional mobile numbers to contact persons.

Email address to receivers of new release information emails:

Email and number to system owner:

Servers

The ICC and Repo server could be either on the same machine or on separate servers.

ICC server

☐ Virtual machine is created

☐ Physical machine exist

- IP address:

  _____

- Netmask:

  _____

- Default gateway:

  _____

- Fully qualified domain name:

  _____

- Proxy configuration:

  _____

- NTP servers:

  _____

- DNS servers:

  _____

- SMTP server:

  _____

Repo server

☐ Virtual machine is created

☐ Physical machine exist

- IP address:

  _____

- Netmask:

  _____

- Default gateway:

  _____

- Fully qualified domain name:

  _____

- Proxy configuration:

  _____

- NTP servers:

  _____

- DNS servers:

  _____

Network

- ☐ Routing exists between ICC server and USB Protect
- ☐ Routing exists between ICC server and DataLock
- ☐ Routing exists between Repo server and ICC
- ☐ Routing exists between Repo server and updates.sysctl.se

Firewall rules

- ☐ USB Protect have access to ICC server
- ☐ DataLock have access to ICC server
- ☐ Operators have access to ICC server
- ☐ Repo server has access to updates.sysctl.se
- ☐ ICC server has access to Repo server
- ☐ USB Protect have access to Repo server
- ☐ DataLock have access to Repo server
- ☐ ICC has access to letsencrypt
- ☐ ICC has access to proxy
- ☐ ICC has access to NTP server
- ☐ ICC has access to DNS servers
- ☐ ICC has access to mail relay

Stations

USB Protect

- IP address:

  _____

- Netmask:

  _____

- Default gateway:

  _____

- Fully qualified domain name:

  _____

- Proxy:

  _____

- DNS resolver:

  _____

DataLock

- IP address:

  _____

- Netmask:

  _____

- Default gateway:

  _____

- Fully qualified domain name:

  _____

- Proxy:

  _____

- DNS resolver:

  _____

