TCP AND UDP PORTS USED BY RCDEVS SOLUTIONS

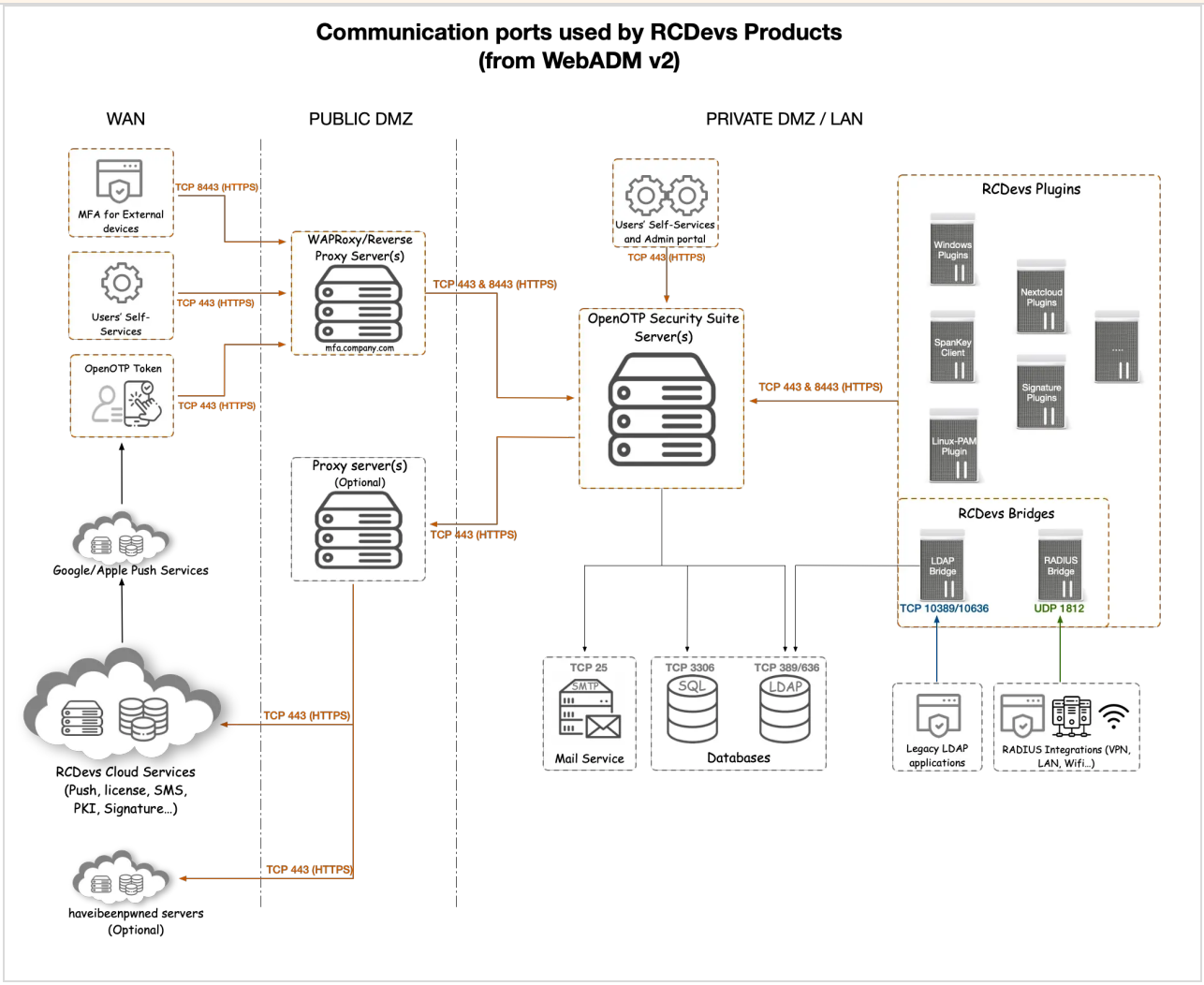
TCP and UDP Ports used by RCDevs solutions

TCP UDP Traffic Ports Firewall PROTOCOLS

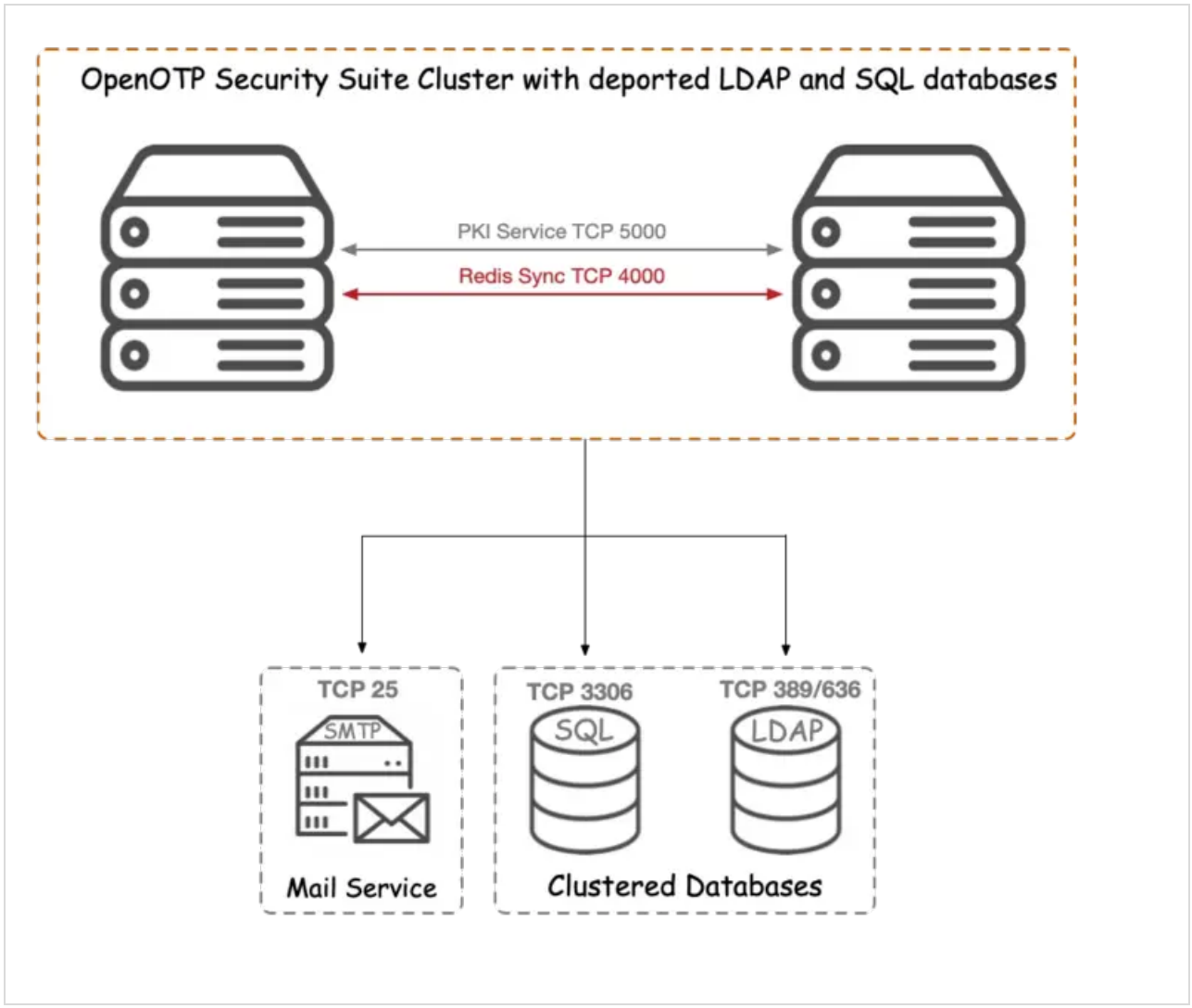
1. Overview

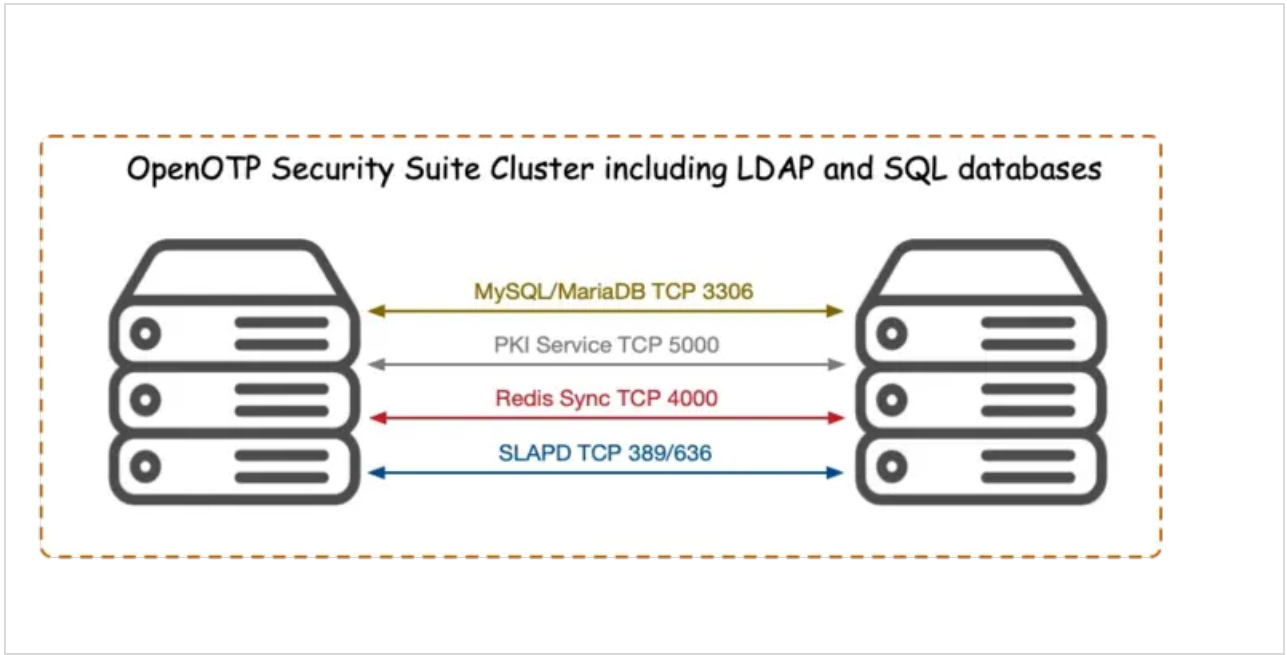
This documentation demonstrates ports and protocols used by RCDevs products between different components.

2. Communication Ports used by RCDevs Products



3. WebADM Cluster Ports





At RCDevs Hardening Guide - 5.5 HA Cluster Firewall Rules is an example of the iptables firewall rules for a high availability cluster with 4 nodes.

4. Incoming and Outgoing Traffic per Product

Product	Incoming	Outgoing
WebADM primary node & Web Services	SSH **TCP 22**, Session Server **TCP 4000**, SOAP **TCP 8443**, HTTPS **443**, HTTP **80**, PKI **TCP 5000**	Session Server **TCP 4000** to WebADM secondary nodes, LDAPS **389** or **636**, SQL **3306**, **before v2**: Licenses service **TCP 7001** to license.rcdevs.com, **before v2**: Push service **TCP 7000** to push.rcdevs.com, **from v2**: Cloud services **TCP 443** to cloud.rcdevs.com, **SMTP** port to your mail server, TCP **5000** to WebADM secondary nodes
WebADM secondary nodes & Web Services	SSH **TCP 22**, Session Server **TCP 4000** SOAP **TCP 8443**, HTTPS **443** , HTTP **80**, PKI **TCP 5000**	Session Server **TCP 4000** to WebADM Primary node, HTTPS **443** to WebADM primary node, LDAPS **389** or **636**, SQL **3306**, PKI **TCP 5000** to WebADM primary node, **before v2**: Licenses service **TCP 7001** to license.rcdevs.com, **before v2**: Push service **TCP 7000** to push.rcdevs.com, **from v2**: Cloud services **TCP 443** to cloud.rcdevs.com, **SMTP** port to your mail server, TCP **5000** to WebADM primary node
Radius Bridge	**UDP 1812**	**TCP 8443** to WebADM, HTTPS **443** to WebADM primary node, HTTPS **443** to WebADM secondary nodes
LDAP Bridge	LDAPS **389** or **636**	**TCP 8443** to WebADM(s) **389** or **636** to LDAP server(s), HTTPS **443** to WebADM primary node, HTTPS **443** to WebADM secondary nodes
WAProxy	HTTPS **443**, HTTPS **8443** (only if publish_websrvs is enabled), HTTP **80** (OCSP)	HTTPS **443** to WebADM, SOAP **TCP 8443** to WebADM web services (only if publish_websrvs is enabled), HTTP **80** to all WebADM nodes
SpanKey Client	SSH **TCP 22**	SOAP **TCP 8443** to SpanKey Web Service, HTTPS **443** to WebADM primary node, HTTPS **443** to WebADM secondary nodes
Windows Plugins	X	SOAP **TCP 8443** to OpenOTP Web service,

		HTTPS **443** to WebADM primary node, HTTPS **443** to WebADM secondary nodes
PAM OpenOTP plugin	UNIX SOCKET	SOAP **TCP 8443** to OpenOTP Web service, HTTPS **443** to WebADM primary node, HTTPS **443** to WebADM secondary nodes
SQL Replication	**TCP 3306**	**TCP 3306**
OpenLDAP Replication	LDAPS **389 or 636**	LDAPS **389 or 636**
Web Applications	**TCP 443**	HTTPS **443** to https://haveibeenpwned.com/API/v3 URL if Prevent Known Passwords setting is activated on Secure Password Reset. Other web applications do not have external communications.

5. Change default WebADM listening Ports

The proper way to change a WebADM listening port is by creating the `/opt/webadm/conf/webadm.env` file. In that file, you can configure the following settings:

```
# Interface used
INTERFACE=1.2.3.4

# Apache standard port
HTTP_PORT_STD=1080

# Apache SSL port
HTTP_PORT_SSL=1443

# Web Service standard port
SOAP_PORT_STD=2080

# Web Service SSL port
SOAP_PORT_SSL=2443
```

To take into account these changes, you have to restart your WebADM services.

If you need to change the PKI Server Port then follow this documentation RCDevs Hardening Guide - 7.2 Change Port.