Shipping & Mailing
Postage Meters

Connect+®/SendPro® P Series

US Networking Technical Specification

User Guide
SV62440 Rev R
March 6, 2018

Introduction

This document details the networking technical considerations for the Connect+/SendPro™ P Series.

Network Requirements

- The Connect+/SendPro system will require a high-speed network connection.
- The Connect+/SendPro system will initiate all communication.
- The Connect+/SendPro system will initiate all communication (via HTTP or HTTPS), so it can safely sit behind most corporate firewalls.
- The Connect+/SendPro system will communicate to external Web Services via HTTP over Port 80.
- The Connect+/SendPro system will communicate to PB secure server(s) via HTTPS over port 443.
- The Connect+/SendPro system will use Port 53 for DNS lookup.
- Pitney Bowes requires a minimum network bandwidth of 384 kbps (upstream and downstream) to operate, but we recommend 1 Mbit/sec for best performance.
- It is recommended that DSL or 3G modem devices are not shared across multiple Connect+/SendPro systems.
- Customer owned web filtering devices or software, as well as SSL packet inspection should be disabled for these ports as they can affect performance.

Port/Communication Requirements

All communication is initiated from the Connect+/SendPro system via ports 80 (HTTP) and 443 (HTTPS). All communication from the Connect+/SendPro system to the back end system is in the form of XML messages.

Port 80 (HTTP)

- OS Update
- AV Updates
- Web Services
- TeamViewer

Port 443 (HTTPS)

- Connect+ will send requests to refill or audit its PSD (Postal Security Device) based on a low funds or inspection date. Refills currently occur when the PSD funds drop below $xx.xx). Audits occur if the PSD inspection date has expired.
- During initial install, the system will automatically request an Operational Block, from the infrastructure, for the PSD.
- On PSD replacement the System will automatically request the configuration data for the replacement PSD.
- Transaction Records from the Connect+/SendPro system are automatically uploaded when:
  - The System goes into Sleep Mode.
  - While powering down the system.
  - Activating Web Accounting Services.
  - Uploading Postal Information.
- On power up the System freshens the Web Service (checks for Download Services, Software, Rates and Graphic Updates. It will also contact Supplies, My Account, Tracking etc.) configuration data.

Port 53

- DNS lookup
  - IT departments that use a "rules based" method for allowing specific ports to pass traffic on their network for port 53 and make sure to allow BOTH UDP and TCP traffic for this port. Port 53 listens for DNS requests and may respond on either protocol, based on the type of request it receives. Short responses should come in over UDP. Longer, more detailed responses on TCP.

URL Information

The following URLs must be accessible from the Connect+/SendPro system, without any obstructions. It is strongly recommended that the firewall reference the URL rather than IP address, which can change over time. If IP addresses must be referenced, it is suggested to keep open the block of IP addresses 199.231.32.0 to 199.231.47.255, 152.144.128.0 to 152.144.128.255, 209.85.128.000 to 209.85.255.255.

Teamviewer

TeamViewer is used by service and sales for remote diagnostics and training. A TeamViewer session can only be initiated by someone on the customer end and therefore the system cannot be accessed without the customers knowledge. All communication is initiated from the Connect+/SendPro system via ports 80 (HTTP) and 443 (HTTPS). All communication from the Connect+/SendPro system to the back end system is in the form of XML messages.

There are two options to unblock Teamviewer:

1. General unlocking of Port 5938 TCP for outgoing connections (recommended). Port 5938 is only used by a few programs and therefore is no security risk. This traffic should then neither be filtered or cached.

2. Unlocking of URLs of the following formats (to any Server)

    - **GET /din.aspx?s=…&client=DynGate…**
    - **GET /dout.aspx?s=…&client=DynGate…**
    - **POST /dout.aspx?s=…&client=DynGate…**

Regardless of which method is chosen to unblock TeamViewer, also check that no content filter or similar is blocking one of the following URLs:

- *.teamviewer.com
- *.dyngate.com.

Required firewall exceptions

- **Connect+®/SendPro® P Series Network Linux Proxy Test**

  Description: Built in tools that pings select PB servers for connectivity testing. Used by PB Service (Resides on Linux Desktop).

  Network Test:

  - http://www.google.com
    (Domain www.google.com; IP=72.14.253.104)
  - http:// www.l.google.com
    (Domain www.google.com; IP=74.125.230.81, 74.125.230.82, 74.125.230.83, 74.125.230.84, 74.125.230.80)
  - http://www.novell.com

  SUSE Linux Proxy Test

  - Domain ftp.novell.com IP = 130.57.1.88
  - http:// www.l.google.com
    (Domain www.google.com; IP=74.125.230.81, 74.125.230.82, 74.125.230.83, 74.125.230.84, 74.125.230.80)

- **Distributor**

  Description: Main PB Server that authenticates machine for access to other PB web service.

  - Distributor: http://distservp1.pb.com/dstproduct.asp

    https://distservp1.pb.com/dstproduct.asp
    (Domain distservp1.pb.com; IP=152.144.128.244, 152.144.128.230, 199.231.44.31, 199.231.43.31, 199.231.45.46)

- **Comet (Funds Management & Refills)**

  Description: Funds are managed through a separate Funds Server system.

  - http://cometservc1.pb.com/T3cometserver_03.asp
  - https://cometservc1.pb.com/T3cometserver_03.asp
    (Domain cometservp1.pb.com; IP=152.144.128.230, 152.144.128.236, 199.231.45.37, 199.231.43.215)

- **Rates and Updates (Download Services)**

  Description: Downloads, new software, graphics, rate price data etc.

  - Misc. Data Upload:

    https://pbgdspp1.pb.com/MS1ConfigurationUpload/MS1ProductConfigurationUpload.svc (Domain pbgdspp1.pb.com; IP= 199.231.44.222, 199.231.44.148 and 199.231.45.41,199.231.45.35)

  - ClamAV: http://clamserver.pb.com

    (Domain clamserver.pb.com; IP=199.231.45.165; 199.231.44.54, 199.231.33.54,199.231.35.165)

  - Error log uploads:

    (Domain pbdlsp1.pb.com; IP=199.231.44.30; 199.231.45.38)

  - Configuration web page:

    https://MyMS1Configuration.pb.com
    (Domain MyMS1Configuration.pb.com; IP=199.231.44.166)

  - OS Updates: https://SMT.pb.com

    (Domain SMT.pb.com; IP=199.231.44.54; 199.231.35.165)

  - File Updates:

    https://pbgdspp1.pb.com/MS1/DlaService.svc
    (Domain pbgdspp1.pb.com; IP=199.231.44.222)

  - Orders (CCD):

    https://pbgdspp1.pb.com/MS1CCD/DlaCCDService.svc (Domain pbgdspp1.pb.com; IP=199.231.44.222)

- **Manage Accounts (Accounting Web App):**

  Description: Separate PB Server that manages Accounting including Account Creation, Reports etc.

  - Accounting Web Application:

    https://ms1app.pb.com/
    (Domain ms1app.pb.com; IP=199.231.32.67)

  - Accounting Web Services:

    https://ms1app.pb.com/ms1atweb/services/
    (Domain ms1app.pb.com; IP=199.231.32.47)

- **On Line Help**

  Description: This is the on line website.

  - http://support.pb.com/help_videos/SV62370-help/default.htm

    (Domain support.pb.com, IP=152.144.192.210, IP=152.144.192.211)

- **Buy Ink Express**

  Description: Allows direct access to Ink Ordering page

  - http://www.pitneybowes.us/shop/ink-and-supplies/postage-meter-ink-supplies/connect-series--1/en-us/storeus

    (Domain: www.pitneybowes.com; IP Address 199.231.33.6, 199.231.44.12)

- **Health and Ink Upload**

  Description: Machine Health Information upload

  - https://cplus-logs-fusion.pb.com/api/v1/uploads

    (Domain: www.pb.com ; IP Address = 199.231.33.6, 199.231.44.12)

Optional firewall exceptions (enabled by default)

- **Verify Address (address cleansing)**

  Description: Utility website to validate addresses against USPS database

  - http://www.pb.com/ms1av/checkaddress.jsp

    (Domain www.pb.com; IP=199.231.44.12)

- **Your Account (PB.com)**

  Description: Utility website to access your account on PB.com.

  - https://www.pb.com/cgi-bin/pb.dll/jsp/Login.do?lang=en&country=US&ga1=MS1

    (Domain www.pb.com; IP=199.231.44.12)

    (Domain http://www.google.com/analytics; IP=209.85.128.000, 209.85.227.101, 209.85.227.113)

- **Presort Savings and Services**

  Description: Utility website to manage Discounts & Presorting.

  - http://www.pb.com/mailstream/mailing-services

    (Domain www.pb.com; IP=199.231.44.12)

- **Buy Supplies**

  Description: Utility website to order Connect+®/SendPro® P Series supplies

  - http://www.pb.com/mailstream/supplies/ms1

    (Domain www.pb.com; IP=199.231.44.12)

- **Track a Package**

  Description: Carrier independent web tracking site for packages.

  - http://pb.boxoh.com/

    (Domain pb.boxoh.com; IP=72.47.250.186)

- **Apps & Tools**

  Description: Utility website for additional applications and tools.

  - http://www.pb.com/connectplus/apps/

    (Domain www.pb.com; IP=199.231.44.12)

Optional firewall exceptions (disabled by default)

- **Ship a Package**

  Description: Package shipping application.

  - http://shipapackage.us.pitneybowes.com

    (Domain www.pb.com; IP address = 199.231.44.12)

    Ship A Package is a legacy Shipping Application that is being replaced by SendPro. If this is a new installation, you do not need to open up the firewall for Ship A Package.

- **SendPro**

  Description: Newest package shipping application.

  - https://sending.us.pitneybowes.com/

    (Domain www.pitneybowes.com; IP address 199.231.33.6, 199.231.44.12)

- **SendSuite Tracking**

  Description: SendSuite Tracking application.

  - http://sendsuitetracking/pitneybowes.com/

    (Domain: www.pitneybowes.com; IP Address 199.231.33.6, 199.231.44.12)

FAQs

Question	Answer
What OS does this device run?	SUSE Linux Sled 11
What controls are in place to protect this device against network-based malware (viruses/worms) threats?	Controls include: • White list of URL's • HTTPS • Anti Virus Software • Only executes services needed to perform activities • OS distribution has been optimized and locked down
Does it have a firewall?	Yes
Who controls the firewall rules?	Pre-configured and not modifiable
How are the firewall rules configured?	Allow only the ports Http, Https and DNS
What is the security patch process?	Connect+ security patches are applied by emergency updates via PB only, and on a regular schedule through PB services.
What anti-virus controls does Connect+ use?	ClamAv is installed on every system. AV signature updates regularly updated
What is the software update process, and how often does this occur?	As required, in some cases monthly
What is the network traffic flow to and from the Connect+/SendPro system? What firewall rules need to be in place to allow the necessary communication?	• Outgoing contact initiated (no push) utilizing HTTPS, URLs provided by PB services • Outgoing - transactional data • Incoming is both transactional data and files and Web Services
Can you identify suspicious activity affecting Connect+?	Yes. An audit process exists to validate the financial integrity of the system. Error logs are available and can be uploaded to the PB data center. • Regularly scheduled physical visits from PB Service

Question	Answer
What are the access controls in place to secure Connect+?	The application access is managed by the customer using User IDs and passwords. Unique, cryptographically strong passwords for each machine restricts access to the operating system.
How do you authenticate an individual? A service?	The application access is managed by the customer using User IDs and passwords. The Connect+ Series does not provide services over a network so authentication not required.
Are there audit trails in place?	Yes. PSD transactional audits, extensive logs all financial transactions are audited by the PB infrastructure. The Connect+ Series logs all error conditions, and maintains ink usage logs, print usage logs, etc.
Is data stored on the device?	Yes. The Connect+ Series stores transactional data, graphic images, customer profiles and settings, files (rates, etc.).
What controls protect the data?	All files and data interface utilizing HTTPS. Incoming data and files are signed and verified prior to use. If consumed by the printer, it is verified on each use. If used by the application, it is verified on load.
Does the Connect+ Series allow remote administration?	Pitney Bowes will use TeamViewer to troubleshoot system problems remotely. The end user will initiate the session using a special code.