Networking Technical Specification
Connect+ Series

Introduction

This document details the networking technical considerations for the Connect+ Series.

Network Requirements

- The Connect+ system will require a high-speed network connection.
- The Connect+ system will initiate all communication.
- The Connect+ system will initiate all communication (via HTTP or HTTPS), so it can safely sit behind most corporate firewalls.
- The Connect+ system will communicate to external Web Services via HTTP over Port 80.
- The Connect+ system will communicate to PB secure server(s) via HTTPS over port 443.
- The Connect+ system will use Port 53 for DNS lookup.

Port/Communication Requirements

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

Port 80 (HTTP)

- OS Update
- AV Updates
- Web Browsing (Help)
- 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 $xxx.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+ system are automatically uploaded when:
- The System has been idle for a period of 10 minutes
- While powering down the system.
- Web Accounting Services.
- On power up the System freshens the Web Service (Supplies, My Account, Tracking etc.) configuration data.
- Software, Rates and Graphic updates.

Port 53

DNS lookup

IT departments that use a "rules based" method for allowing specific ports to pass traffic on their network need to enable BI-directional communication 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.

URLs

The following URLs must be accessible from the Connect+ 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, 172.28.106.0 to 172.28.107.255, 172.31.224.0 to 172.31.224.255 and 209.85.128.000 to 209.85.255.255.

If the PB infrastructure IP ranges are used, the following third-party addresses cited below must also be open: google.com, novell.com, http://pb.boxoh.com/.

At a minimum, these URLs must be accessible:

- Connect+ 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)
- 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, 199.231.32.31, 199.231.34.46)
- Comet Server:
    - http://cometservm1.pb.com/T3cometserver_03.asp
    - https://cometservm1.pb.com/T3cometserver_03.asp
      (Domain cometservp1.pb.com; IP=152.144.128.230, 152.144.128.236, 199.231.44.215, 199.231.45.37, 199.231.43.215, 199.231.44.36, 199.231.32.215, 199.231.34.37)
- PB Infrastructure Services
  (IP=199.231.44.15)

Download Services

- Misc. Data Upload:
  https://pbgdspp1.pb.com/MS1ConfigurationUpload/MS1ProductConfigurationUpload.svc
  (Domain pbgdspp1.pb.com; IP=199.231.44.28, 199.231.44.222, 199.231.44.148 and
  199.231.45.41, 199.231.43.222, 152.144.128.232, 152.144.128.167, 199.231.45.35,
  199.231.43.148)
- 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: https://pbdlsp1.pb.com/UploadService/service.svc
  (Domain pbdlsp1.pb.com; IP=199.231.44.30; 152.144.128.226, 199.231.45.38, 199.231.43.30,
  199.231.34.38, 199.231.32.30)
- Configuration web page: https://MyMS1Configuration.pb.com
  (Domain MyMS1Configuration.pb.com; IP=152.144.128.48, 199.231.44.166)
- OS updates: https://SMT.pb.com
  (Domain SMT.pb.com; IP=199.231.44.54; 199.231.45.165, 199.231.33.54, 199.231.35.165)
- File Updates: https://pbgdspp1.pb.com/MS1/DlaService.svc
  (Domain pbgdspp1.pb.com; IP=199.231.44.222, 199.231.32.148, 199.231.34.35)
- Orders (CCD): https://pbgdspp1.pb.com/MS1CCD/DlaCCDService.svc
  (Domain pbgdspp1.pb.com; IP=199.231.44.222, 199.231.32.222, 199.231.34.41)

Accounting

- Accounting Web Application: https://ms1app.pb.com/
  (Domain ms1app.pb.com; IP=199.231.44.149, 199.231.32.22, 199.231.34.34)
- Accounting Web Services: https://ms1app.pb.com/services/
  (Domain ms1app.pb.com; IP=199.231.44.149)

More than a Mailing Machine

- Verify Address (Address cleansing):
  http://www.pb.com/ms1av/checkaddress.jsp
  (Domain www.pb.com; IP=199.231.44.12, 172.28.106.14 , 172.28.107.18, 172.28.107.19,
  172.28.107.183)
- My Account at 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, 172.28.106.14 , 172.28.107.18, 172.28.107.19,
  172.28.107.183)
  (Domain http://www.google.com/analytics; IP=209.85.128.000, 209.85.227.101, 209.85.227.113,
  172.28.106.14 , 172.28.107.18, 172.28.107.19, 172.28.107.183)
- Discounts & Presort Services: http://www.pb.com/mailstream/mailing-services
  (Domain www.pb.com; IP=199.231.44.12, 172.28.106.14 , 172.28.107.18, 172.28.107.19,
  172.28.107.183)
- Buy Supplies:
  http://www.pb.com/mailstream/supplies/ms1
  (Domain www.pb.com; IP=199.231.44.12, 172.28.106.14 , 172.28.107.18, 172.28.107.19,
  172.28.107.183)
- Track a Package (Web tracking – Boxo Generic package tracking service): http://pb.boxoh.com/
  (Domain pb.boxoh.com; IP=72.47.250.186)
- Postal Tools: http://www.pb.com/connectplus/apps/.
  (Domain www.pb.com; IP=199.231.44.12, 172.28.106.14 , 172.28.107.18, 172.28.107.19,
  172.28.107.183)
- On Line Help: www.pitneyworks.com/ms1
  (Domain www.pitneyworks.com, IP= 199.231.33.16, 172.31.224.16)

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.

There are 2 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 nor 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

FAQs

Q: What OS does this device run?

A: SUSE Linux Sled 11

Q: What controls are in place to protect this device against network-based malware (viruses/worms) threats?

A: 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

Q: Does it have a firewall?

A: Yes

Q: Who controls the firewall rules?

A: Pre-configured and not modifiable

Q: How are the firewall rules configured?

A: Allow only the ports Http, Https and DNS

Q: What is the security patch process?

A: Connect+ security patches are applied by emergency updates via PB only, and on a regular schedule through PB services.

Q: What anti-virus controls does Connect+ use?

A: ClamAv is installed on every system. AV signature updates regularly updated

Q: What is the software update process, and how often does this occur?

A: As required, in some cases monthly

Q: What is the network traffic flow to and from the Connect+ 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

Q: Can you identify suspicious activity affecting Connect+?

A: 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

Q: What are the access controls in place to secure Connect+?

A: 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.

Q: How do you authenticate an individual? A service?

A: 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

Q: Are there audit trails in place?

A: 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.

Q: Is data stored on the device?

A: Yes. The Connect+ Series stores transactional data, graphic images, customer profiles and settings, files (rates, etc.).

Q: What controls protect the data?

A: 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.

Q: Does the Connect+ Series allow remote administration?

A: Pitney Bowes will use TeamViewer to troubleshoot system problems remotely. The end user will initiate the session using a special code.