



Expédition et envoi
Compteurs postaux

Connect + ^{MD} / SendPro ^{MC} P

Spécifications techniques de mise en réseau

Introduction.....	2
Exigences du réseau.....	2
Exigences des ports et des communications.....	2
Information URL.....	3
FAQ.....	10

Introduction

Ce document explique en détail les aspects techniques de mise en réseau pour la Connect + / SendPro P.

Exigences requises pour le

- Le système Connect + / SendPro P nécessitera une connexion de réseau à grande vitesse
- Le système Connect + / SendPro P initiera toutes les communications.
- Le système Connect + / SendPro P initiera toutes les communications (via HTTP ou HTTPS), afin de rester en sécurité derrière la plupart des pare-feux d'entreprise.
- Le système Connect + / SendPro P communiquera aux services Web externes via HTTP sur le port 80.
- Le système Connect + / SendPro P communiquera avec les serveurs sécurisés PB via HTTPS sur le port 443.
- Le système Connect + / SendPro P utilisera le port 53 pour la recherche DNS.
- Pitney Bowes nécessite une bande passante de réseau minimale de 384 kbps (en émission et en réception) pour fonctionner, mais nous recommandons 1 Mbit/sec pour des performances optimales.
- Il est recommandé que les périphériques de modem DSL ou 3G ne soient pas partagés entre plusieurs systèmes Connect + / SendPro P.
- Les périphériques ou logiciels de filtrage Web appartenant au client, ainsi que l'inspection des paquets SSL doivent être désactivés pour ces ports car ils peuvent affecter les performances.

Exigences des ports et des communications

Toutes les communications sont initiées à partir du système Connect + / SendPro P via les ports 80 (HTTP) et 443 (HTTPS). Toutes les communications du système Connect + / SendPro P au système dorsal se font sous la forme de messages XML.

Port 80 (HTTP)

- Mises à jour du système d'exploitation
- Mises à jour AV
- Service Web
- TeamViewer

Port 443 (HTTPS)

- Le Connect + / SendPro P enverra des demandes de recharge ou de vérification du DSP (dispositif de sécurité postale) sur la base d'un niveau de fonds bas ou d'une date d'inspection. Les recharges se produisent lorsque les fonds du DSP sont en-dessous de (xx,xx \$). Les vérifications se produisent si la date d'inspection du DSP a expirée.
- Lors de l'installation initiale, le système demandera automatiquement un bloc opérationnel à l'infrastructure pour le DSP.
- Lors du remplacement du DSP, le système demandera automatiquement les données de configuration pour le remplacement du DSP.
- Les enregistrements de transactions du système Connect + /SendPro P sont automatiquement téléchargés lorsque :
 - Le système passe en mode veille.
 - Pendant la mise hors tension du système.
 - L'activation des services de comptabilité Web.
 - Le téléchargement d'informations postales.
- Lors de la mise sous tension, le système rafraîchit les données de configuration du service Web (vérifie les services de téléchargements, les mises à jour de logiciels, des tarifs et graphiques. Il communiquera également avec les fournitures, My Account, les suivis, etc.).

Port 53

- Recherche DNS
 - Les services informatiques qui utilisent une méthode "basée sur des règles" pour autoriser des ports spécifiques à transmettre le trafic sur leur réseau pour le port 53 doivent autoriser le trafic UDP et TCP pour ce port. Le port 53 reçoit les demandes DNS et peut répondre par l'un ou l'autre des deux protocoles, en fonction du type de demandes qu'il reçoit. Les réponses courtes devraient venir du UDP. Les réponses plus longues et plus détaillées du TCP.

Informations URL

Les URL suivants doivent être accessibles à partir du système Connect + /SendPro P, sans aucune obstruction. Il est fortement recommandé que le pare-feu référence l'URL plutôt que l'adresse IP, qui peut changer avec le temps. Si les adresses IP doivent être référencées, il est suggéré de garder ouvert le bloc d'adresses IP 199.231.32.0 à 199.231.47.255, 152.144.128.0 à 152.144.128.255, 209.85.128.000 à 209.85.255.255.

TeamViewer

Le service et les ventes utilisent TeamViewer à des fins de diagnostic et de formation à distance. Seule une personne à l'établissement du client peut ouvrir une session dans TeamViewer; par conséquent, il est impossible d'accéder au système sans son aide. Toutes les communications sont initiées à partir du système Connect + / SendPro P via les ports 80 (HTTP) et 443 (HTTPS). Toutes les communications du système Connect + / SendPro P au système dorsal se font sous la forme de messages XML.

Il y a deux options de débloquent TeamViewer :

1. Déverrouillage général du port 5938 TCP pour les connexions sortantes (recommandé). Le port 5938 n'est utilisé que par quelques programmes et ne présente donc aucun risque pour la sécurité. Ce trafic ne doit alors être ni filtré ni masqué.
2. Déverrouillage des URL des formats suivants : (vers n'importe quel serveur)
 - **OBTENIR** /din.aspx?s=...&client=DynGate...
 - **OBTENIR** /dout.aspx?s=...&client=DynGate...
 - **POSTER** /dout.aspx?s=...&client=DynGate...

Quelle que soit la méthode choisie pour débloquent TeamViewer, vérifiez également qu'aucun filtre de contenu ou similaire ne bloque l'un des URL suivants :

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

Exceptions requises pour le pare-feu

- **Test du réseau Proxy Linux du Connect + / SendPro P**

Description : Outils intégrés qui sélectionnent les serveurs PB par pings pour les tests de connectivité. Utilisé par le service de Pitney Bowes (réside sur le bureau de Linux).

Test du réseau :

- <http://www.google.com>
(Domaine : www.google.com; IP = 72.14.253.104)
- <http://www.l.google.com>
(Domaine : 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>

Test du proxy SUSE Linux

- Domaine : [ftp.novell.com](ftp://ftp.novell.com) IP = 130.57.1.88
- <http://www.l.google.com>
(Domaine : www.google.com; IP = 74.125.230.81, 74.125.230.82, 74.125.230.83, 74.125.230.84, 74.125.230.80)

- **Distributeur**

Description: Serveur principal de Pitney Bowes qui authentifie la machine pour l'accès à d'autres services Web de Pitney Bowes.

- Distributeur :

<https://distservp1.pb.com/dstproduct.asp>
(Domaine 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 (gestion de fonds et recharges)**

Description : Les fonds sont gérés par un système de serveur distinct.

- http://cometservc1.pb.com/T3cometsserver_03.asp
- https://cometservc1.pb.com/T3cometsserver_03.asp
(Domaine : cometservc1.pb.com; IP = 152.144.128.230, 152.144.128.236, 199.231.45.37, 199.231.43.215)

- **Tarifs et mises à jour (Services de téléchargement)**

Description : Téléchargements, nouvelle version de logiciels, graphiques, données tarifaires, etc.

- Téléchargement de données diverses :

<https://pbgdspp1.pb.com/MS1ConfigurationUpload/MS1ProductConfigurationUpload.svc>
(Domaine pbgdspp1.pb.com; IP = 199.231.44.222, 199.231.44.148 et 199.231.45.41, 199.231.45.35)

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

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

- Téléchargement du journal des erreurs :

(Domaine : pbdlspp1.pb.com; IP = 199.231.44.30; 199.231.45.38)

- Page web de configuration :

<https://MyMS1Configuration.pb.com>
(Domaine : MyMS1Configuration.pb.com; IP = 199.231.44.166)

- Mises à jour du système d'exploitation : <https://SMT.pb.com>

(Domaine : SMT.pb.com; IP = 199.231.44.54; 199.231.35.165)

- Mises à jour de fichiers :

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

- Commandes (CCD):

<https://pbgdspp1.pb.com/MS1CCD/DlaCCDSvc.svc>
(Domaine : pbgdspp1.pb.com; IP = 199.231.44.222)

- **Gérer les comptes (Application Web de comptabilité) :**

Description : Serveur distinct de Pitney Bowes qui gère la comptabilité, incluant la création de comptes, de rapports etc.

- Application Web de comptabilité :

<https://ms1app.pb.com/>

(Domaine : ms1app.pb.com; IP = 199.231.32.67)

- Services Web de comptabilité :

<https://ms1app.pb.com/ms1atweb/services/>

(Domaine : ms1app.pb.com; IP = 199.231.32.47)

- **Aide en ligne**

Description : C'est le site Web en ligne.

- <http://eureka.pitneybowes.com/sendpro-p-series/fr-ca/SV62565-help-fr-ca/Default.htm>

(Domaine : support.pb.com, IP = 152.144.192.210, IP = 152.144.192.211)

- **Téléchargement de la santé de la machine et de l'encre**

Description : Téléchargement des informations sur la santé des machines

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

(Domaine : www.pb.com; IP Adresse = 199.231.33.6, 199.231.44.12)

Exceptions de pare-feu facultatives (activées par défaut)

- **Vérification de l'adresse (nettoyage des adresses)**

Description : Site Web de l'utilitaire pour valider les adresses par rapport à la base de données de Postes Canada.

- <https://www.pitneybowes.com/ca/fr/connect-plus/address-verification.html>

(Domaine : www.pb.com; IP = 199.231.44.12)

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

Description : Site Web de l'utilitaire pour accéder à votre compte sur PB.com.

- <http://fr.pitneybowes.ca/signin>

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

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

- **Acheter des fournitures**

Description : Site Web de l'utilitaire pour commander des fournitures pour le Connect + / SendPro P.

- <https://fr.pitneybowes.ca/shop/encre-et-fournitures/encre-et-fournitures-pour-compteurs-postaux/encre-et-fournitures-pour-compteurs-postaux/fr-ca/storecafr>

(Domaine : www.pb.com; IP = 199.231.44.12)

- **Suivre un envoi**

Description : Site WEB indépendant pour le suivi de colis selon le transporteur.

- <https://www.pitneybowes.com/ca/fr/connect-plus/track-a-package.html>

(Domaine : pb.boxoh.com; IP = 72.47.250.186)

- **DM Works**

Description : Accès aux solutions et soutien de Pitney Bowes

- <http://www.pitneybowes.com/ca/fr>

(Domaine : www.pb.com; IP = 199.231.44.12)

- **Outils postaux Outils de messagerie Web**

Description : Un lien vers les pages Web de Postes Canada offrant des informations sur les règlements postaux et le soutien.

- <https://www.pitneybowes.com/ca/fr/connect-plus/postal-tools.html>

(Domaine : www.pb.com; IP = 199.231.44.12)

Exceptions de pare-feu facultatives (désactivées par défaut)

- **SendPro**

Description : Nouvelle application d'expédition de colis.

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

(Domaine : www.pitneybowes.com; IP adresse 199.231.33.6, 199.231.44.12)

- **SendSuite Tracking Online – Suivi en ligne**

Description : L'application de suivi en ligne de SendSuite Tracking Online

- <http://sendsuitetracking.pitneybowes.com/>

(Domaine : www.pitneybowes.com; IP Adresse 199.231.33.6, 199.231.44.12)

FAQ

Question

Quel système d'exploitation cet appareil utilise-t-il?

Quels sont les contrôles en place pour protéger cet appareil contre les menaces de logiciels malveillants (virus / vers) provenant du réseau?

A-t-il un pare-feu?

Qui contrôle les règles du pare-feu?

Comment les règles du pare-feu sont-elles configurées?

Quel est le processus correctif de sécurité?

Quels sont les contrôles antivirus utilisés par Connect + / SendPro P?

Quel est le processus des mise à jour de logiciels, et à quelle fréquence cela se produit?

Quel est le flux de trafic réseau vers et en provenance du Système Connect + / SendPro P? Quelles règles de pare-feu doivent être en place pour permettre la communication nécessaire?

Réponse

SUSE Linux Sled 11

Les mesures de contrôles comprennent :

- Liste blanche d'URL
- HTTPS
- Logiciel anti virus
- N'exécute que les services nécessaires à l'exécution des activités
- Le système d'exploitation de distribution a été optimisé et verrouillé

Oui

Préconfiguré et non modifiable

Autorise uniquement les ports Http, Https et DNS

Les correctifs de sécurité Connect + / SendPro P sont appliqués par les mises à jour d'urgence via Pitney Bowes seulement, et sur une base régulière via les services de Pitney Bowes.

ClamAv est installé sur chaque système. La signature AV est régulièrement actualisée.

Au besoin, dans certains cas mensuellement

- Contact sortant initié (pas poussé) utilisant les ports HTTPS et URL fournies par les services PB
- Données transactionnelles sortantes
- L'entrée est à la fois des données et des fichiers transactionnels et des services Web

Question

Pouvez-vous identifier une activité suspecte affectant le Connect + / SendPro P?

Quels sont les contrôles d'accès en place pour sécuriser le Connect + / SendPro P?

Comment authentifiez-vous un individu? Un service?

Existe-t-il des pistes d'audit?

Les données sont-elles enregistrées sur l'appareil?

Quels contrôles protègent les données?

Est-ce que le Connect + / SendPro P autorise la gestion à distance?

Réponse

Oui. Un processus d'audit existe pour valider l'intégrité financière du système. Des journaux d'erreurs sont disponibles et peuvent être téléchargés au le centre de données de Pitney Bowes.

- Visites physiques régulières du service de Pitney Bowes

L'accès à l'application est géré par le client à l'aide de comptes d'utilisateurs et de mots de passe. Des mots de passe uniques et cryptographiquement forts pour chaque machine limitent l'accès au système d'exploitation.

L'accès à l'application est géré par le client à l'aide de comptes d'utilisateurs et de mots de passe.

L'authentification n'est pas exigée car le Connect + / SendPro P ne fournit pas de services sur un réseau.

Oui. L'infrastructure de PB vérifie les audits transactionnels du PSD, les journaux complets et toutes les transactions financières. Le Connect + / SendPro P enregistre toutes les conditions d'erreur, et maintient des journaux sur la consommation d'encre, la fréquence d'impression, etc.

Oui. Le Connect + / SendPro P garde en mémoire des données transactionnelles, des images graphiques, des profils et des paramètres de clients, des fichiers (tarifs, etc.)

Tous les fichiers et l'interface de données utilisent HTTPS. Les données et les fichiers entrants sont signés et vérifiés avant l'utilisation. S'ils sont acheminés à l'imprimante, ils sont vérifiés à chaque utilisation. Si l'application les utilise, ils sont vérifiés au chargement.

Pitney Bowes utilisera TeamViewer pour résoudre les problèmes du système à distance. L'utilisateur de la machine lancera la session à l'aide d'un code spécial.