



Exigences réseau, optimisation et sécurité dans Paxton10

Présentation

Paxton10 est un système de contrôle d'accès et de gestion vidéo basé sur le réseau, qui est contrôlé et configuré par le serveur Paxton10 via son interface utilisateur web. Paxton10 peut fonctionner sur presque n'importe quel réseau, mais nécessite certaines fonctionnalités réseau pour fonctionner correctement.

Ce document traite des exigences réseau et des meilleures pratiques pour le déploiement de périphériques Paxton10 sur votre réseau IP, afin d'obtenir des performances réseau optimales et une sécurité réseau.

Les informations et suggestions contenues dans ce guide ont été recueillies grâce à des tests approfondis de nos produits dans une variété de topologies et d'environnements de mise en réseau.

En suivant ce guide, les sites peuvent bénéficier des avantages suivants :

- Découverte de périphériques Plug-and-Play
- Amélioration de la réactivité des périphériques Paxton en réduisant la latence dans votre réseau IP
- Réduction de la consommation de bande passante par les appareils Paxton
- Moins de latence réseau/perte de paquets pendant la communication entre les périphériques
- Disponibilité garantie des appareils Paxton10
- Temps de téléchargement/chargement réduits pour les mises à jour du firmware
- Un réseau sécurisé, empêchant les pirates informatiques, les outils de reniflage et les violations de sécurité des données

Public cible

Ce document s'adresse à tous les installateurs Paxton10 et aux professionnels de l'informatique du site, y compris ceux qui disposent de réseaux segmentés complexes utilisant plusieurs sous-réseaux et/ou emplacements physiques.

Exigences réseau

Paxton10 ne nécessite aucune configuration réseau spécialisée, cependant, pour obtenir une fonctionnalité et une simplicité complètes, nous recommandons ce qui suit :

- 1) Connexion Internet : Paxton10 ne nécessite pas d'Internet pour le quotidien. Cependant, certaines fonctionnalités dépendent d'une connexion Internet :
 - Accès à distance : L'accès à distance à l'interface utilisateur et l'utilisation de l'application mobile Paxton Connect nécessitent une connexion Internet au serveur Paxton10.
 - Multi-site : la fonction multi-site intégrée de Paxton10 nécessite une connexion Internet au serveur Paxton10 et à tous les contrôleurs Paxton10.

- Mise à niveau du système : Paxton10 offre des mises à jour gratuites à vie. Les mises à jour sont détectées et transmises via la connexion Internet au serveur Paxton10. Les mises à niveau hors ligne ne sont actuellement pas disponibles.
 - Identifiants intelligents : l'émission des identifiants intelligents Paxton10 nécessite une connexion Internet au serveur Paxton10. Les identifiants intelligents peuvent être rayés et supprimés en mode hors connexion.
- 2) DHCP : Le réseau doit exécuter un serveur DHCP compatible avec DNS, IPv4 et IPv6. Un serveur DHCP dédié peut être utilisé, sinon de nombreux routeurs fournissent une prise en charge DHCP sans avoir besoin de matériel supplémentaire. Connectez un routeur ou un serveur DHCP au réseau.
 - 3) DNS : Paxton10 nécessite l'exécution d'un serveur DNS afin qu'il puisse traduire le nom du serveur Paxton10 (paxton10-xxxxx) en son adresse IP associée. Sans DNS, la navigation vers le serveur Paxton10 devra se faire à l'aide de son adresse IP.
 - 4) Protocole réseau : Paxton10 utilise à la fois IPv4 et IPv6 pour communiquer. Cela signifie que tout réseau utilisé par Paxton10 doit être compatible avec IPv4 et IPv6.

Optimisation réseau

Voici les étapes qui peuvent être effectuées pour améliorer les performances et la fiabilité du réseau :

- 1) Évaluez et testez votre réseau pour comprendre les performances/capacités actuelles du réseau
 - Il est préférable d'évaluer votre capacité réseau existante et de vérifier si elle peut gérer la charge réseau attendue à partir du nombre et du type de périphériques Paxton10 que vous envisagez de déployer.
 - Si vous envisagez de déployer des périphériques Paxton10 sur différents sous-réseaux répartis dans différentes régions géographiques, il est recommandé d'effectuer d'abord des tests entre deux périphériques de ces sous-réseaux afin de recueillir des statistiques telles que la latence, la perte de paquets, la gigue et la bande passante.
 - Testez la connectivité ICMP de tous les emplacements réseau/sous-réseaux vers le serveur Paxton10.
 - Testez les mesures de fiabilité UDP/TCP de tous les sous-réseaux vers le serveur Paxton10 pour vous assurer que tous les périphériques Paxton10 peuvent établir et maintenir une connexion fiable au serveur.
 - Créez un inventaire de tous les emplacements physiques, emplacements réseau, sous-réseaux et espaces d'adressage dans lesquels vous prévoyez de déployer les produits Paxton10.

Sécurité du réseau

Nous recommandons à nos clients de mettre en oeuvre des mécanismes de sécurité à chacune des 7 couches du modèle d'interconnexion des systèmes ouverts de réseau (OSI). Voici quelques approches qui devraient être suivies pour assurer la sécurité du réseau.

- 1) Mettre en oeuvre une sécurité physique forte dans les locaux de l'entreprise en utilisant un badge, un code PIN ou une authentification biométrique, de sorte qu'un étranger puisse être arrêté avant qu'il puisse entrer dans les bâtiments de l'entreprise.
- 2) Mettre en oeuvre des normes de contrôle d'accès réseau telles que l'authentification IEEE 802.1X pour sécuriser le LAN (réseau local) et le WLAN (réseau local sans fil).

Cette norme applique la sécurité en accordant uniquement aux périphériques conformes aux règles de sécurité l'accès aux ressources réseau lorsque ces périphériques sont branchés à un port LAN physique ou sont connectés à un SSID WLAN. Cette norme gère non seulement les fonctions d'authentification et d'autorisation d'accès, mais contrôle également les données auxquelles ces utilisateurs peuvent accéder en reconnaissant les utilisateurs, leurs appareils et leurs rôles réseau. IEEE 802.1X est pris en charge nativement par toutes les machines Windows, Mac et Linux.

- 3) Mettre en oeuvre des pare-feu de nouvelle génération pour prévenir les attaques externes et internes. Un pare-feu de nouvelle génération, en plus de l'inspection dynamique traditionnelle basée sur les paquets, devrait également exécuter des fonctions telles que l'inspection de la couche d'application, la prévention et la détection des intrusions, la sécurisation du trafic Web, et plus encore.

En outre, étirez tous les VLAN de couche interne 2 potentiellement non sécurisés (réseaux locaux virtuels) vers le pare-feu et protégez l'accès de ces VLAN à d'autres VLAN sécurisés à l'aide de stratégies de sécurité.

- 4) Mettre en oeuvre des VLAN pour la sécurité et la ségrégation du réseau. Les VLAN nous permettent de séparer les paquets de données provenant de plusieurs réseaux (tels que les réseaux départementaux, les réseaux de serveurs critiques, etc.). La segmentation du réseau avec des VLAN crée un ensemble de réseaux isolés au sein d'un réseau d'entreprise et réduit les surfaces d'attaque ; même si un étranger accède à un petit réseau logique, il ne sera pas en mesure de visualiser ou d'attaquer directement les périphériques sur d'autres VLAN.
- 5) Implémentez des mots de passe forts pour vous connecter à l'application Paxton10 et à toutes les bases de données associées. »

Certificats SSL Paxton10

Paxton10 utilise HTTPS entre les clients, le serveur et les contrôleurs Paxton10. Chaque serveur Paxton10 est délivré avec un certificat auto-signé unique, délivré par l'autorité de certification racine Paxton10.

Pour éviter les messages d'avertissement de sécurité du navigateur, le certificat Paxton10 doit être installé sur chaque ordinateur client.

Le certificat d'un site peut se trouver en suffixant l'URL de votre site avec '/setup'. La page de configuration fonctionnera également sur HTTP. Par exemple, <http://paxton10-xxxxxx/setup>.

Sur la page de configuration, 2 options sont disponibles : « Installation automatique » télécharge un exécutable pour installer automatiquement le certificat sur l'ordinateur actuel pour l'utilisateur connecté — un autre exécutable est disponible pour Windows et Mac. « Installation manuelle » télécharge le certificat dans le dossier de téléchargements par défaut. Le certificat peut être installé sur l'ordinateur actuel ou transmis à un administrateur informatique pour l'installer sur tous les ordinateurs du réseau.

FAQ

Quelles sont les exigences en matière de bande passante lors de l'utilisation de Paxton10 sur un accès multisite ou distant?

- Il est recommandé que toute connexion Internet impliquée avec Paxton10 soit de 20 Mbps en téléchargement et de 10 Mbps en transfert.
- Pour chaque flux principal de la caméra visualisé, il est recommandé d'avoir 6 Mbps supplémentaires en téléchargement et 2 Mbps en transfert pour chaque connexion réseau impliquée.
- Pour chaque flux secondaire de la caméra visualisé, il est recommandé que chaque réseau dispose d'un débit supplémentaire de 3 Mbps en téléchargement et de 1 Mbps en transfert.

Si les exigences de bande passante recommandées ne sont pas respectées, vous pouvez rencontrer des problèmes de performances lors de l'utilisation de Paxton10, notamment un temps de mise en mémoire tampon plus long lors de la visualisation de séquences vidéo en direct ou d'archives et des temps de chargement plus longs lors de la navigation dans le système.

Comment le Paxton10 détecte-t-il les appareils?

Paxton10 utilise le DNS de multidiffusion sur IPv6 pour détecter les contrôleurs de porte P10 sur le réseau.

Il existe un problème connu avec un programme qui peut être intégré aux commutateurs réseau et qui s'appelle MLD (Multicast Listener Discovery).

Le MLD est une méthode efficace pour gérer les communications IPv6 sur le réseau, mais elle empêche la détection des contrôleurs de porte P10.

Le MLD doit être désactivé par un ingénieur réseau ou un service informatique pour que le P10 détecte les portes.