Net2 - Recommandations de sécurité réseau

Résumé

Pour maximiser la sécurité de votre système Paxton Net2 sur votre site, Paxton recommande que l'installateur (ou le département informatique) implémente les meilleures pratiques des mécanises de sécurité informatique dans chacune des 7 couches du modèle OSI (Network Open Systems Interconnection).

Implémentez une sécurité physique rigoureuse

Implémentez une sécurité physique rigoureuse aux locaux de la société en utilisant par exemple l'identification biométrique, l'authentification basée sur les badges et d'autres moyens. Ainsi, toute personne étrangère pourrait être interceptée avant qu'elle ne puisse s'introduire dans un bâtiment abritant un réseau d'entreprise.

Implémentez les standards de contrôle d'accès au réseau tels que l'authentification IEEE 802.1X pour la sécurisation des LAN et WLAN

Ce standard impose une politique de sécurité en n'octroyant qu'aux dispositifs conformes à la politique de sécurité un accès aux ressources réseau lorsque ces dispositifs sont branchés à un port LAN physique ou connectés à un SSID de WLAN. Ce standard gère non seulement les fonctions d'authentification et d'autorisation des accès, mais peut également contrôler les données consultées par ces utilisateurs spécifiques en reconnaissant les utilisateurs, leurs dispositifs et leurs rôles au sein du réseau. IEE 802.1X est pris en charge de manière native par toutes les machines Windows, Mac et Linux.

Implémentez des pare-feux de nouvelle génération pour empêcher les attaques externes et internes

Implémentez un pare-feu de nouvelle génération, qui en plus d'une inspection d'état traditionnelle basée sur les paquets, effectue aussi une inspection de couche applicative, une prévention et une détection des intrusions et sécurise le trafic web, en plus d'autres fonctionnalités.

En plus, étendez tout VLAN interne de couche 2 potentiellement non sécurisé vers le pare-feu et protégez l'accès émanant de ces VLAN vers les autres VLAN sécurisés/de confiance en utilisant des politiques de sécurité configurables.

Implémentez des VLAN (Virtual Local Area Networks) pour la sécurité et la ségrégation des réseaux

Les VLAN nous permettent de séparer les paquets de données de plusieurs réseaux (tels que les réseaux départementaux, les réseaux de serveur critiques, etc.). La segmentation du réseau par le biais des VLAN crée une collection de réseaux isolés au sein d'un réseau d'entreprise et réduit les surfaces d'attaque, car même au cas où un intrus accéderait à un petit réseau logique, il ne serait pas en mesure de voir ni d'attaquer directement les dispositifs sur les autres VLAN.

Implémentez des mots de passe robustes pour l'authentification des applications du serveur Net2 et les bases de données associées. Veuillez voir la note d'application APN-1162 pour découvrir comment y parvenir.

Ayez une machine dédiée au serveur Net2

Ayez une machine dédiée à l'exécution du serveur Net2 et n'installez dessus aucun autre logiciel à l'exception des outils de surveillance réseau (le cas échéant).

La machine du serveur Net2 physique ne devrait être accessible qu'au personnel autorisé seulement.

Sécurité de la machine

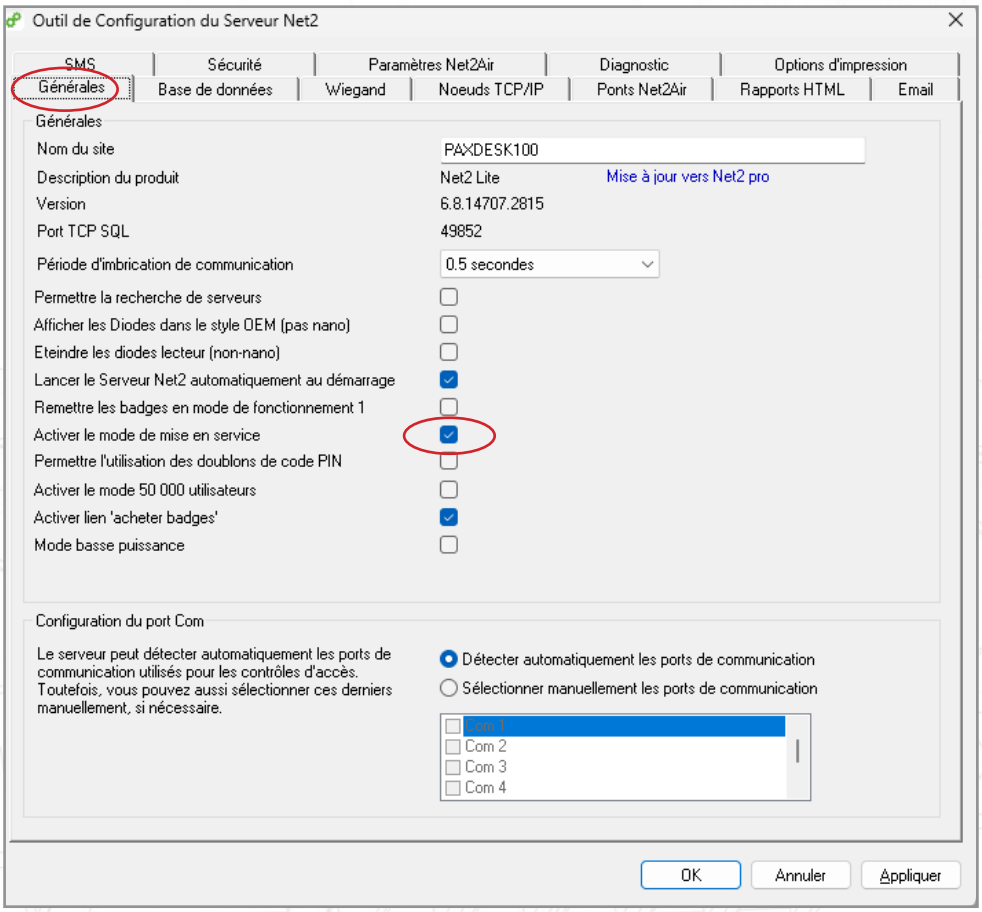
Tenez les machines de serveur et clientes à jour avec les dernières mises à jour critiques du système d'exploitation et veillez à la présence d'une protection par analyse antivirus sur les machines clientes.

Les clients Net2 devraient être installés sur des machines sans des clients e-mail ou de messagerie instantanée afin d'éviter l'exécution non intentionnelle de code malicieux à partir des pièces jointes.

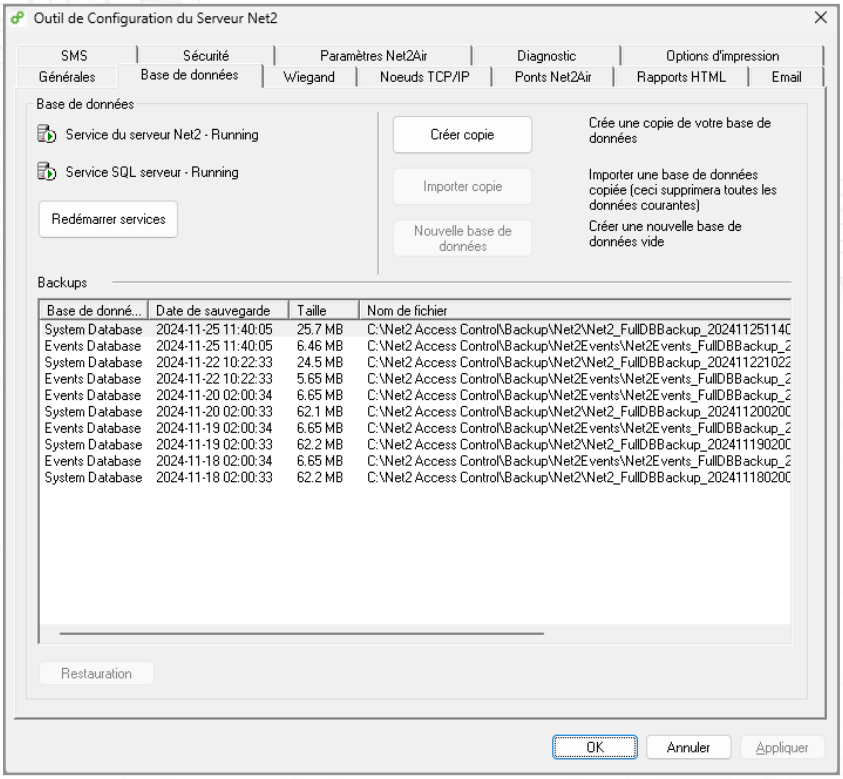
Mode de mise en service

Une fois que vous avez mis en service votre système, il peut être verrouillé en décochant la case « **Activer le mode de mise en service** », sous l'onglet « **Général** » de l'utilitaire de configuration Net2.

Veuillez noter :
Avec le mode de mise en service désactivé, il n'est plus possible d'ajouter ou de supprimer des ACU et elles seront verrouillées sur ce serveur.

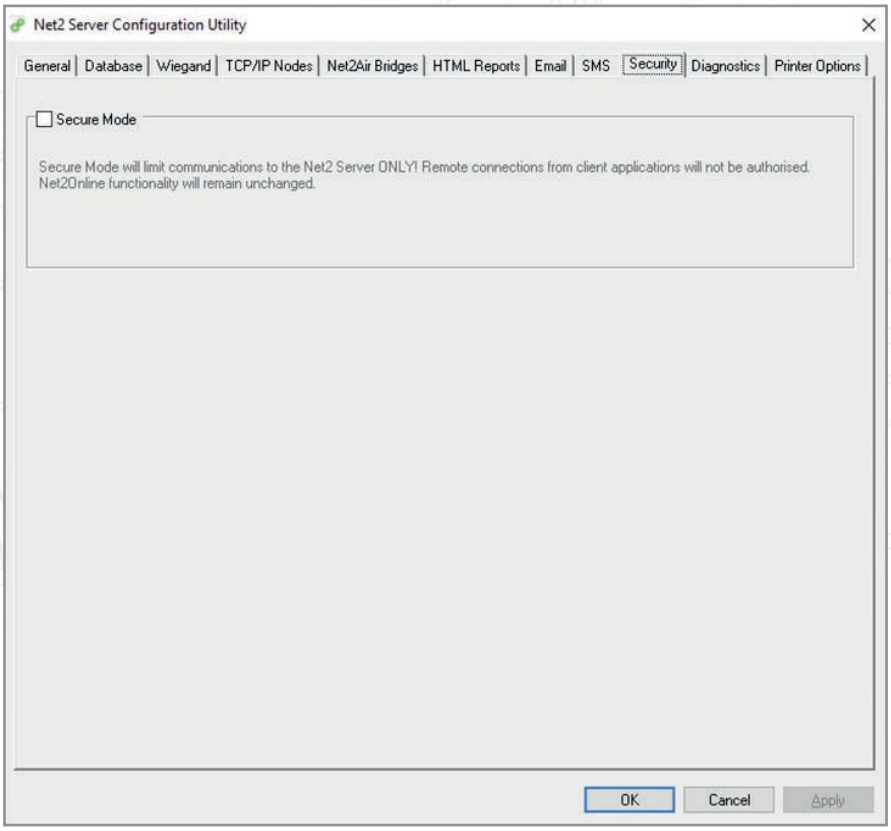


Avec le mode de mise en service désactivé, les options de l'onglet « **Base de données** » seront également grisées dans l'utilitaire de configuration Net2.



Mode sécurisé de Net2

Pour garantir une sécurité maximale, songez à exécuter à la fois le logiciel serveur et le logiciel client depuis la même machine en bloquant le port du serveur TCP SQL 1433 pour les connexions entrantes. Pour y parvenir, activez le « mode sécurisé » en utilisant l'onglet de sécurité de Net2.



Sinon, pour profiter pleinement de toutes les fonctionnalités du client, utilisez un logiciel d'application virtualisée tel que VMware horizon pour distribuer les applications clientes Net2 restreintes et connectées à un serveur Net2 sur un LAN ou un VLAN séparé.

Pour faciliter l'inscription des badges, utilisez un lecteur existant ou un lecteur connecté à un Net2 Nano sans-fi si le câblage réseau n'est pas une solution viable. Cette solution permettra aussi aux SDK (Software Development Kit) et aux applications vidéo d'être isolés dans le bureau virtualisé et déployés avec aisance, tout en étant intégralement administrés dans le centre de données.

Qu'est-ce que VMware Horizon ? | VDI Software | VMware | UK

Remarque : VMware horizon propose l'USB passthrough, mais les performances sont dictées par la vitesse du réseau et nécessitent des tests. Cela pourrait autoriser l'utilisation d'un lecteur de bureau et d'une webcam standards.

Étapes de sécurité supplémentaires

1. Implémentez le filtrage des adresses MAC sur le switch

Implémentez le filtrage des adresses MAC sur le port d'entrée. Lorsqu'un dispositif non reconnu se connecte à un port, le port en question sera désactivé et une alerte sera envoyée.

2. Isolez le VLAN

Placez tous les dispositifs Paxton dotés de capacités IP sur un VLAN dédié. Isolez ce VLAN du réseau de l'entreprise pour restreindre l'accès aux zones autres que les dispositifs de contrôle d'accès.