KDFM eXplorer

ACCES WEB AU PERIPHERIQUE (DEVICE WEB ACCESS)

La description du processus d'**Accès Web au Périphérique** (DWA) avec le DCA 4 permet à un utilisateur disposant des autorisations adéquates de se connecter au serveur Web interne des imprimantes à l'aide de la fonctionnalité appelée « **Accès Web au Périphérique** », qui présente les spécifications techniques et les fonctions de sécurité suivantes :

1. DCA4 reçoit une commande de connexion Device Web Access du portail KDFM eXplorer et vérifie que la demande concerne une imprimante gérée, puis crée un tunnel SSH inversé.

2. Le tunnel SSH inversé est basé sur le protocole SSH et il est créé à partir du port d'imprimante du service Web (généralement 80 ou 443, ou autre qui peut être configuré) vers un serveur SSH distant (port 22 / SSH) accessible via différentes URL de domaine appartenant au domaine racine https://*.mpsmonitor.com.

3. À l'aide du protocole SSH, le système implémente une authentification basée sur une clé publique et crypte les connexions entre l'imprimante et les terminaux du serveur KDFM eXplorer SSH.

4. La connexion côté serveur est créée en tant que nouveau tunnel à chaque demande de connexion, et terminée après chaque session, avec une durée maximale de 10 minutes. Les clés de sécurité sont uniques pour chaque installation et chaque nouveau tunnel utilise un ID de session différent pour éviter la réutilisation de session.

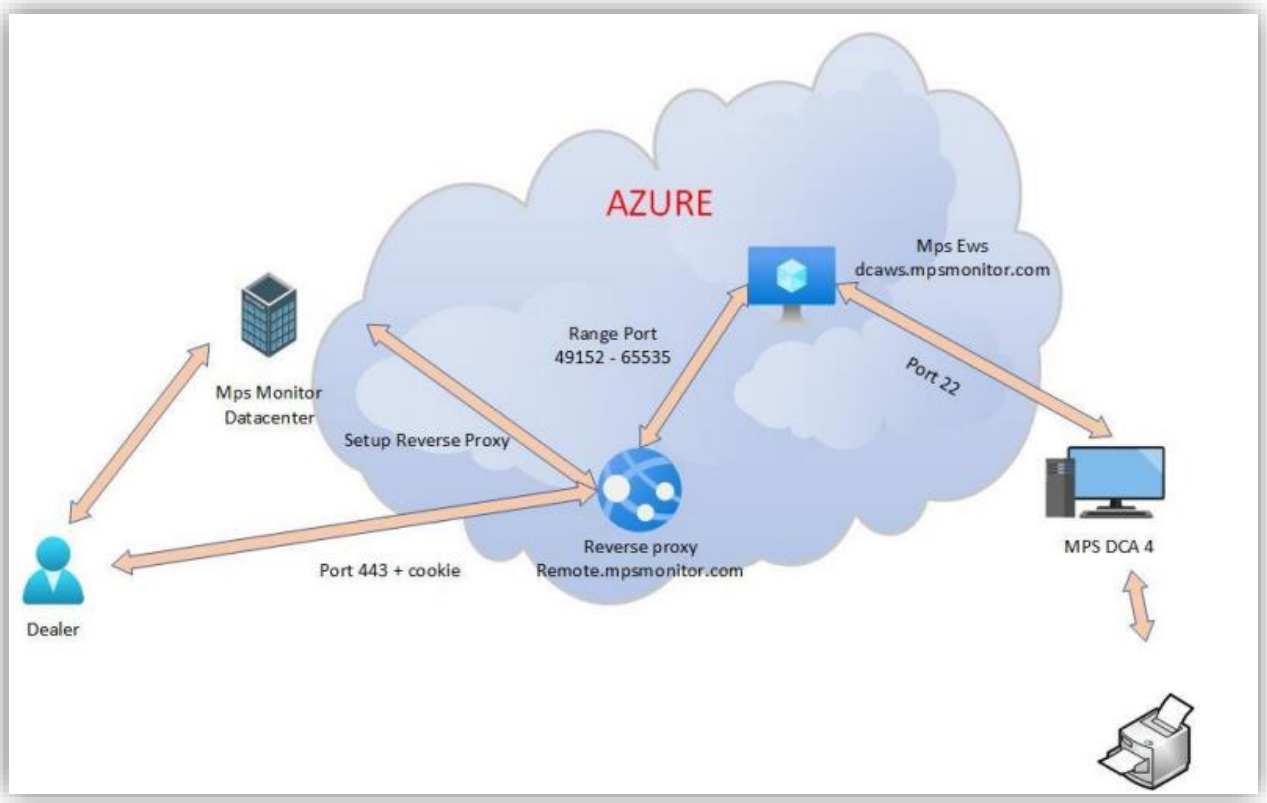
5. Une méthodologie d'authentification complexe est mise en œuvre pour garantir que toutes les parties impliquées dans chaque tunnel SSH sont légitimes et ont l'autorité d'ouvrir et de maintenir la connexion.

6. Un certain nombre de vérifications sur l'équipement sont effectuées avant l'ouverture du tunnel pour s'assurer que l'équipement cible correspond à celui sur lequel la connexion a été demandée. Si l'une de ces vérifications échoue, le tunnel n'est pas ouvert.

7. La connexion Device Web Access est limitée uniquement aux profils utilisateur sélectionnés et ne peut être activée que par les utilisateurs disposant d'une authentification forte au portail KDFM eXplorer (authentification à deux facteurs ou authentification unique via Active Directory). Cela empêche l'utilisation non autorisée ou malveillante de la fonctionnalité Device Web Access en cas de vol d'informations d'identification.

8. Toutes les activités Web effectuées dans Device Web Access sont enregistrées sur le serveur SSH. Les clients peuvent accéder aux journaux pour vérifier l'utilisation de cette fonction par d'autres utilisateurs.

9. L'accès Web au périphérique peut être désactivé sur chaque client par l'utilisateur dans le portail KDFM eXplorer, ou directement à partir de l'interface utilisateur locale DCA 4, par le client lui-même. Si la fonction est désactivée dans l'interface utilisateur DCA, elle ne peut pas être réactivée à partir du portail, garantissant ainsi que chaque client a la possibilité de désactiver cette fonction localement à partir du système sur lequel le DCA 4 est installé.



Description du Process

ÉTAPE 1
Le revendeur connecté sur kdfmportal.katun.com clique sur l'imprimante souhaitée et demande le DWA à un périphérique particulier.

ÉTAPE 2
Le portail génère un "Session id" qui sera utilisé entre les différents composants pour reconnaître
la connexion.

ÉTAPE 3
Le portail envoie une commande au DCA pour ouvrir la connexion en transmettant les paramètres suivants :
• Adresse IP et adresse Mac de l'imprimante
• Le port d'interface Web de l'imprimante (80 ou 443) de l'imprimante qui doit être redirigé
• L'identifiant de session pour se connecter
• Les paramètres SSH
• Autres détails de l'imprimante comme le numéro de série, la marque et le modèle

ÉTAPE 4

Le DCA a reçu la commande :

1. Vérifiez que les données de l'imprimante sont égales aux données dans sa base de données locale et vérifiez qu'il s'agit bien d'une imprimante.

2. Utilisez la commande Windows ssh.exe et ouvrez un tunnel SSH sur dcaws.mpsmonitor.com sortant sur le port 22

3. Notifiez le portail que le tunnel est actif

ÉTAPE 5

Le portail se connecte à remote.mpsmonitor.com à l'aide d'un cookie qui contient l'identifiant de session afin que le proxy inverse puisse transférer les demandes vers le bon port transféré sur le serveur SSH.

L'utilisateur peut maintenant travailler sur l'imprimante