Cible de sécurité CSPN – DZ-NETWORK 1.0			
Auteurs :	Benoit BADRIGNANS (SECLAB), Pierre NGUYEN (EDF R&D)	***Date :***	09/04/2014
Référence :	**CR-I2D-2013-029**	***Version***	1.2

Révisions :

09/04/14 : Pierre Nguyen : précision sur longueur des noms de fichier et fichiers image tiff

18/11/13 : Benoît Badrignans : modification entête et mise en page

12/11/13 : Benoît Badrignans : Intégration commentaires, relecture et finalisation version 1.0

08/11/13 : Pierre Nguyen : Relecture et ajout de compléments

06/11/13 : Benoît Badrignans : Première version de travail diffusable

1. OBJECTIF DU DOCUMENT

Ce document présente la cible de sécurité CSPN du dispositif DZ-NETWOK. Il respecte le formalisme et les rubriques classiques des cibles.

2. IDENTIFICATION DU PRODUIT

Organisation éditrice	SECLAB
Lien vers l'organisation	http://www.seclab-solutions.com
Nom commercial du produit	DZ-NETWORK
Numéro de la version évaluée	1.0
Catégorie de produit	Pare-feu

3. ARGUMENTAIRE (DESCRIPTION) DU PRODUIT

3.1. DESCRIPTION GENERALE DU PRODUIT

Le produit est un dispositif permettant l'échange bidirectionnel d'information entre deux réseaux de niveaux de confiance différents, sans interconnexion réseau. Il réalise également un filtrage et une restriction des informations échangées lors du transfert. Le réseau correspondant au niveau de confiance le plus haut est nommé **zone haute** ; l'autre réseau est nommé **zone basse** et est potentiellement exposé à des malveillances.

Le produit se présente sous la forme d'une appliance rackable, composé de deux PC embarqués l'un situé en zone basse, l'autre en zone haute ; reliés via une carte de filtrage et de rupture protocolaire.

On considère que le dispositif DZ-NETWORK est le seul point d'entrée entre la zone basse et la zone haute. Son objectif est de protéger la zone haute des attaques pouvant provenir de la zone basse.

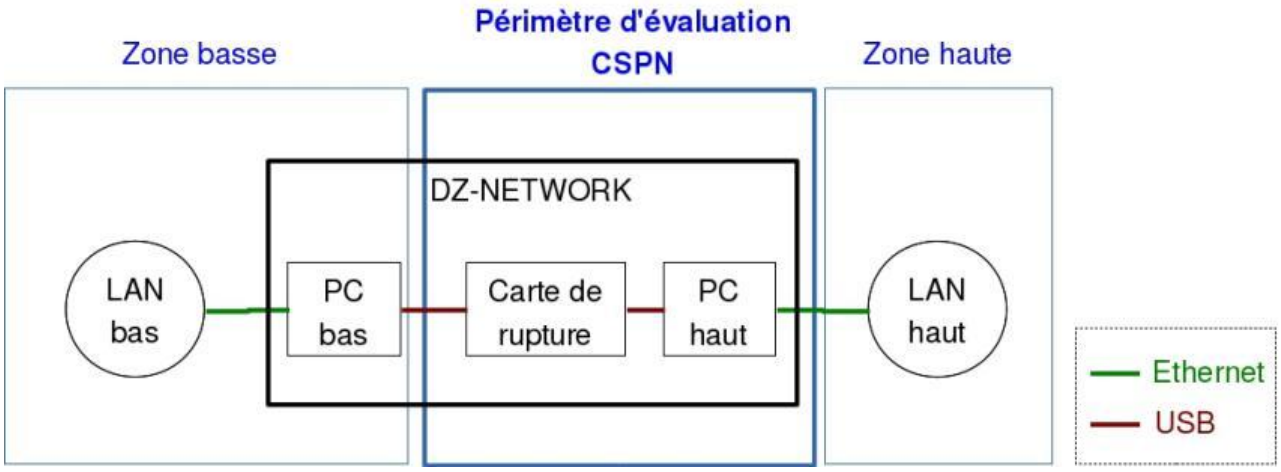

Figure 1. Fonctionnement général du produit et périmètre d'évaluation CSPN

3.2. DESCRIPTION DE LA MANIERE D'UTILISER LE PRODUIT

Le produit fonctionne comme un proxy filtrant. La version 1.0 du produit supporte les protocoles réseaux FTP et Modbus-TCP.

Dans le cas du protocole FTP (transfert de fichiers), l'utilisateur ou un programme présent sur le réseau bas dépose un fichier sur le serveur FTP disponible sur le PC bas. Le fichier est transféré automatiquement au PC haut via la carte de rupture, si celle-ci valide sa politique de sécurité le fichier est alors disponible sur le serveur FTP haut. Une entrée dans un fichier de log distinct pour chacun des serveurs FTP indique si le fichier a été transféré ou bloqué. L'utilisateur ou un programme présent sur le réseau haut peut récupérer les fichiers transférés. Le dispositif fonctionne de manière similaire pour les transferts de fichiers du réseau haut vers le réseau bas.

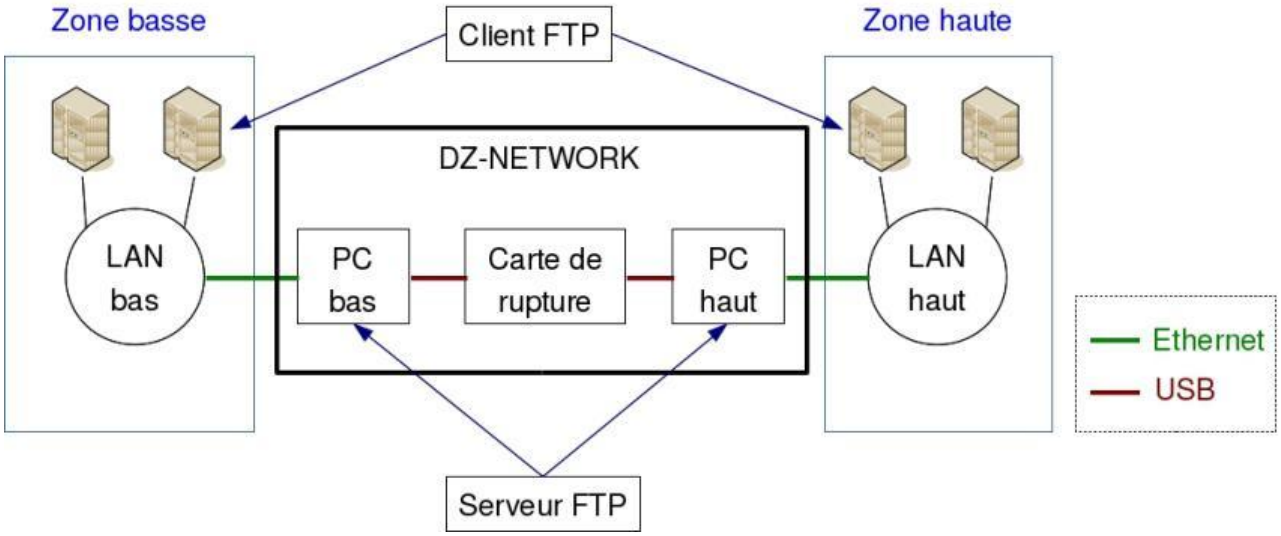

Figure 2. Description générale du fonctionnement serveur FTP du produit

Dans le cas du protocole Modbus-TCP (fonctionnement type client/serveur), le client Modbus-TCP présent sur le réseau haut peut émettre des trames vers le serveur Modbus-TCP présent sur le PC haut. Le contenu Modbus de la trame TCP/IP est transféré au PC bas à travers la carte de rupture. Un client Modbus-TCP présent sur le PC bas émet une trame Modbus-TCP à destination du véritable serveur Modbus-TCP présent sur le réseau bas. La réponse du véritable serveur Modbus-TCP suit le même chemin en sens inverse.

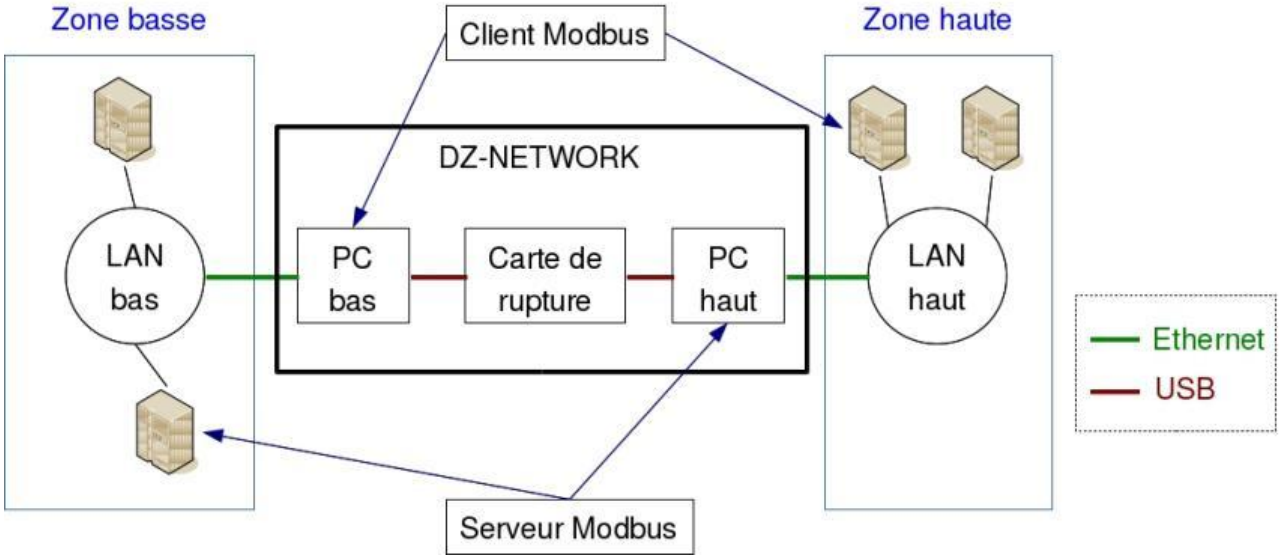

Figure 3. Description générale du fonctionnement Modbus du produit

3.3. DESCRIPTION DE L'ENVIRONNEMENT PREVU POUR SON UTILISATION

L'environnement est considéré comme physiquement sûr au niveau du produit et de la zone haute. Ainsi, le produit ne prend pas en compte des mesures de sécurité particulières au niveau de la malveillance matérielle et/ou utilisant un accès physique au produit.

L'utilisation concerne des transferts :

- De fichiers via des serveurs FTP présents sur chacun des PC haut et bas. Ces fichiers peuvent être :
    - Au format texte, ne comportant que des caractères ayant un code UTF-8 défini dans des intervalles déterminés (décrits dans la documentation utilisateur).
    - Des fichiers de type images au format tiff (les fichiers tiff de plusieurs pages ne sont pas supportés), bitmap, jpeg ou png.
    - Des fichiers au format PDF.

Un contrôle des caractères utilisés pour nommer le fichier est effectué avec des règles similaires. De la même façon, ils ont une taille limitée et ne peuvent pas porter n'importe quelle extension (liste des extensions dans la documentation utilisateur) ; la longueur du nom de fichier est également contrôlée (longueur maximale de 127 caractères, extension et dernier caractère '.' non compris).

Les images et les fichiers PDF peuvent perdre en qualité après transmission.

- De trames conformes au protocole Modbus. La documentation utilisateur décrit les commandes Modbus autorisées ainsi que les formats valides.

Le contenu de ces échanges n'est pas confidentiel.

3.4. DESCRIPTION DES HYPOTHESES SUR L'ENVIRONNEMENT

Les attaques nécessitant un accès physique au produit ne sont pas prises en compte par hypothèse (cf. §3.3).

[H.SEC_PHYSIQUE] Le dispositif DZ-NETWORK doit être utilisé dans un environnement considéré comme physiquement sûr au niveau du produit (le dispositif est physiquement installé dans la zone haute). Ainsi, le produit ne prend pas en compte des mesures de sécurité particulières au niveau de malveillances matérielles et/ou utilisant un accès physique au produit.

[H.INIT] Le dispositif DZ-NETWORK est entièrement configuré lors de sa fabrication, donc avant sa livraison. Les fonctions du produit sont figées et ne sont plus modifiables par la suite. La seule action de l'administrateur est la configuration réseau, FTP et Modbus de chaque PC embarqué (ex: adresse IP, comptes FTP, adresses serveur modbus) via une interface série. Les rôles distincts existants sont donc :

- le rôle utilisateur côté zone basse ;
- le rôle utilisateur côté zone haute ;
- le rôle administrateur côté zone haute pouvant définir la configuration réseau des PC embarqués avant mise en service.

[H.PRECAUTIONS_EMPLOI] Les utilisateurs respectent les précautions d'emploi définies dans la documentation utilisateur.

[H.NON_COLLUSION] L'utilisateur, l'administrateur et les programmes situés en zone haute sont considérés de confiance. De ce fait :

- Si l'utilisateur situé côté zone basse est un attaquant, il ne peut pas disposer de complice ayant accès à la zone haute.
- Un utilisateur situé côté zone haute ne peut faire des attaques volontaires et conscientes visant le PC embarqué haut ou les systèmes présents sur le réseau haut. Par exemple un programme malveillant inséré dans une image via des techniques de stéganographie ne peut pas être reconstitué côté haut.
- Les programmes situés côté zone haute (ex : client Modbus-TCP, client FTP) sont considérés de confiance. Par exemple ils ne peuvent pas attaquer le PC embarqué haut, ou tenter d'ex-filtrer des données via des canaux cachés.

3.5. DESCRIPTION DES DEPENDANCES PAR RAPPORT A DES MATERIELS, DES LOGICIELS ET/OU DES MICROPROGRAMMES DU SYSTEME QUI NE SONT PAS FOURNIS AVEC LE PRODUIT

Il n'existe pas de dépendance particulière. La version du protocole Modbus autorisé est décrite dans la documentation utilisateur. Les serveurs FTP utilisés sur les PC embarqués sont décrits dans la documentation utilisateur (version utilisée, procédure de configuration).

La configuration par l'administrateur se fait via un port USB « device » présentant un port série virtuel. Ce port série virtuel nécessite l'installation de driver via « Windows update » pour les systèmes Windows, il est supporté par les systèmes Linux disposant des drivers « usb_serial » et « ftdi_sio » en plus des drivers USB standards, ces deux modules sont généralement présent sur les distributions récentes. Une fois le port série reconnu par le système, il peut être utilisé avec des outils standards comme par exemple « putty / HyperTerminal » sous Windows ou « minicom » sous Linux comme décrit dans la documentation utilisateur.

3.6. DESCRIPTION DES UTILISATEURS TYPIQUES CONCERNES (UTILISATEURS FINAUX, ADMINISTRATEURS, EXPERTS…) ET DE LEUR ROLE PARTICULIER DANS L'UTILISATION DU PRODUIT

Lors de la fabrication, les fonctions du produit sont figées et ne sont plus modifiables par la suite.

Les rôles standards existants sont les rôles utilisateur côté zone basse et utilisateur côté zone haute.

L'administrateur côté zone haute peut uniquement définir la configuration réseau, FTP et Modbus de chacun des PC embarqués avant mise en service.

3.7. DEFINITION DU PERIMETRE DE L'EVALUATION, A SAVOIR LES CARACTERISTIQUES DE SECURITE DU PRODUIT CONCERNEES PAR L'EVALUATION

Le périmètre de l'évaluation couvre le PC embarqué haut et la carte de rupture, tous deux inclus dans le dispositif DZ-NETWORK ; ces éléments sont considérés en « boîte noire » (cf. Figure 1).

Le PC embarqué bas est considéré en dehors du périmètre.

En effet, le point fort de DZ-NETWORK en termes de sécurité est de garantir la sécurité de la zone haute même si un attaquant à pris le contrôle de la zone basse. En d'autres termes, quelles que soient les exactions effectuées au niveau bas, même en ayant pris le contrôle du PC embarqué bas, la sécurité de la zone haute est conservée.

L'objectif de sécurité principal du dispositif DZ-NETWORK consiste à protéger la zone haute de tout fichier malveillant ou de toute trame réseau malveillante provenant de la zone basse, notamment grâce à une rupture protocolaire et un filtrage restrictif sur les données transférées.

4. DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE D'EVALUATION

4.1. MATERIEL COMPATIBLE OU DEDIE

Chaque PC embarqué est accessible via une interface RJ45 et supporte les clients FTP et les logiciels Modbus décrits dans la documentation utilisateur.

Le poste de configuration de l'administrateur situé côté zone haute dispose d'un port USB hôte et d'un système d'exploitation disposant du driver nécessaire pour le port série virtuel (voir documentation utilisateur).

4.2. SYSTEME D'EXPLOITATION COMPATIBLE : TYPE, VERSION, CORRECTIFS

Les systèmes côté zone haute ou basse sont du type Windows (XP SP3, 7 ou version supérieure) ou Linux noyau 2.6 à partir du 2.6.31, gérant une interface réseau RJ45.

Les PC embarqués haut et bas supportent uniquement le protocole IPV4 et non pas IPV6.

5. DESCRIPTION DES BIENS SENSIBLES QUE LE PRODUIT DOIT PROTEGER

Le produit est conçu pour protéger les biens sensibles suivants :

- **[D.MHAUTE]** Données présentes sur la zone haute.
- **[D.RESEAU_HAUT]** Toutes les machines accessibles par rebond du côté de la zone haute.
- **[D.CONFIG_FILTRAGE]** Paramètres de configuration et de filtrage du dispositif de rupture entre les PC embarqués.

- **[D.TRANSFERT]** Données mises à disposition de la machine haute par le dispositif DZ-NETWORK.

On considère (cf. §3.3) que les données transférées entre les zones basse et haute ne sont pas des biens sensibles, e.g. non confidentiels.

6. DESCRIPTION DES MENACES

L'agent menaçant est tout utilisateur ou programme pouvant se connecter sur le réseau bas. Les menaces contre lesquelles protège le dispositif DZ-NETWORK sont les suivantes :

- **[M. INTRUSION_BAS>HAUT]** Tentative de prise de contrôle des machines situées côté zone haute depuis la zone basse via le dispositif DZ-NETWORK. Ou tentative de découverte de l'architecture du réseau haut depuis le réseau bas.
- **[M. TRANSFERT_DONNEES_ILLICITES]** Transfert de données non autorisées (cf. §5, F.FILTRAGE_FORMAT) depuis la zone basse vers la zone haute ou inversement.
- **[M. MODIF_CONFIG]** Modification de la configuration du dispositif via les seules interfaces accessibles du dispositif.

7. DESCRIPTION DES FONCTIONS DE SECURITE DU PRODUIT

Les fonctions de sécurité du produit sont les suivantes :

- **[F.FILTRAGE_FORMAT]** Filtrage du format des données transférées (ex : transfert de fichiers au format texte, ne comportant que des caractères ayant un code UTF8 défini dans des intervalles déterminés, décrits dans la documentation utilisateur).
- **[F.RUPTURE_RESEAU]** Protection contre l'accès direct au réseau haut depuis le réseau bas (ex : « ping » d'une machine du niveau haut depuis le réseau bas, scan du réseau haut depuis le réseau bas, attaque des piles TCP/IP présentes sur les systèmes du niveau haut depuis le réseau bas).
- **[F.PROTECTION_CONFIG_FILTRAGE]** Protection contre les tentatives de modification / altération de la configuration de filtrage du dispositif via les seules interfaces accessibles du dispositif.

8. VULNERABILITES IDENTIFIEES A CE JOUR

Aucune vulnérabilité connue.