Routeur Chiffrant Navista
Version 2.8.0

Et le protocole de chiffrement du Réseau Privé Virtuel
Navista Tunneling System - NTS
Version 3.1.0

Cibles de sécurité C.S.P.N

Référence : **NTS-310-CSPN-CIBLES-1.05**

Diffusion

Document	
Référence de ce document	NTS-310-CSPN-CIBLES-1.05
Version du document	1.05
Date de dernière mise à jour	15 Mai 2012
Confidentialité	Reproduction et utilisation interdites sauf autorisation préalable de Navista.

Mises à jour

N° de version	Date	Auteur	Objet
1.00	05 juill 2011	JN.LECLERCQ	Création du document
1.01	09 Août 2011	JN.LECLERCQ	restructuration du document
1.02	16 Août 2011	JN.LECLERCQ	Ajout des remarques ANSSI
1.03	29 Août 2011	JN.LECLERCQ	Intégration de l'accès maintenance
1.04	02 Février 2012	JN LECLERCQ	Modification du titre
1.05	15 Mai 2012	JN LECLERCQ	Restriction de la cible

navista®

Sommaire

1. Synthèse

1.1. Identification de la cible de sécurité

Cette cible de sécurité a été élaborée dans le cadre d'une évaluation de premier niveau CSPN [1]

1.2. Identification du logiciel VPN

Catégorie	Identification
Organisation éditrice	*navista*®
Lien vers l'organisation	www.navista.fr
Nom commercial du produit	Navista Tunneling System (NTS)
Numéro de version évaluée	3.1.0
Catégorie de produit	Communications sécurisées

1.3. Identification du produit

Catégorie	Identification
Organisation éditrice	*navista*®
Lien vers l'organisation	www.navista.fr
Nom commercial du produit	Routeur chiffrant Navista
Numéro de version évaluée	2.8.0
Catégorie de produit	Equipement réseau

2. Argumentaire (description) du produit

2.1. Description générale du produit

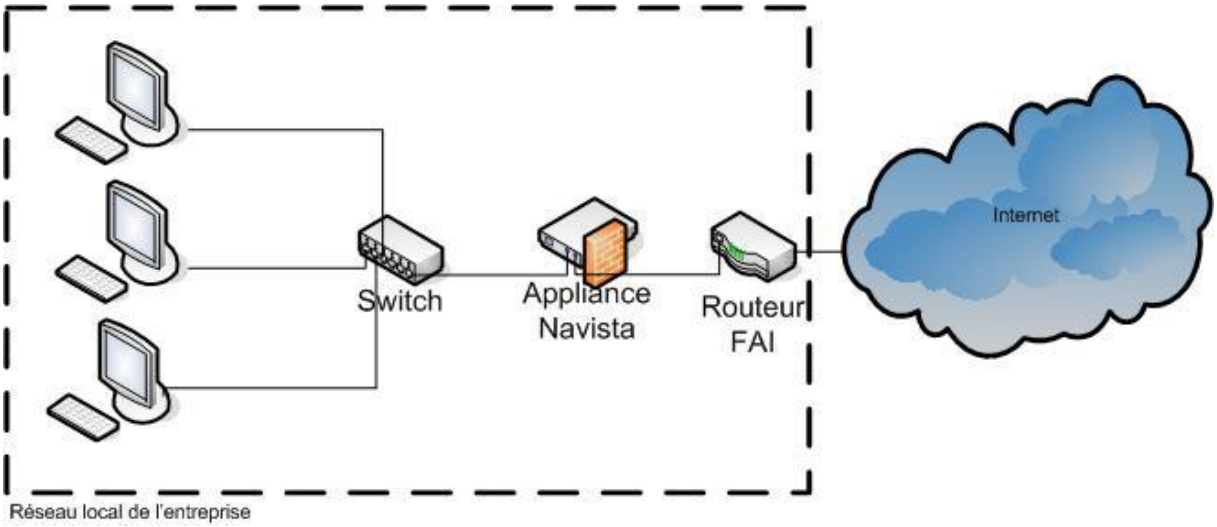
Le produit évalué concerne le routeur chiffrant Navista en version 2.8.0, son interface web de configuration HTTPS, le système de mises à jour et plus particulièrement sa fonction de réseau privé virtuel mis en œuvre par le protocole NTS en version 3.1.0. L'authentification et le chiffrement des flux de ses connexions garantissant l'intégrité et la confidentialité des données transitant par ce biais.
Le protocole NTS 3.1.0 a été développé par NAVISTA et est intégré dans la « Solution Réseau Privé Virtuel *navista*® ».
La solution de réseau privé NAVISTA permet de créer une infrastructure globale au sein de laquelle la confidentialité et l'intégrité des échanges sont assurées par des mécanismes cryptographiques. Une fois en place, seuls les réseaux locaux interconnectés à ce réseau virtuel peuvent s'échanger des informations. Cette solution comprend une multitude d'autres services tels que le Filtrage des contenus web, la Gestion de la Qualité de Services, la Résilience des liens Internet, ne faisant pas l'objet de cette certification.

L'ensemble des composants logiciels est embarqué dans des équipements d'accès communément nommés "appliances". Ces appliances peuvent être plus ou moins puissantes selon le nombre de postes présents sur le réseau local concerné. Certaines appliances, de type concentrateur, permettent à tout ou partie des réseaux locaux d'accéder à des ressources partagées (serveur de mails, serveurs de données, application en mode Saas, etc…). Ces concentrateurs sont appelés "frontaux". Ces frontaux sont des serveurs classiques, dimensionnés selon le nombre de tunnels à gérer. Ces matériels sont spécifiés, et les différents logiciels qu'ils embarquent (système d'exploitation, les logiciels NAVISTA dont le protocole NTS) sont installés par NAVISTA. Leur conformité aux spécifications est donc testée et garantie par NAVISTA.
L'appliance NAVISTA, au travers du protocole NTS 3.1.0 permet donc de créer des réseaux privés virtuels permettant l'interconnexion de réseaux locaux au travers des réseaux non sûrs (exemple Internet public).
Le routeur chiffrant Navista est décliné en plusieurs offres commerciales sous les noms NXP, NBX, RSA ou SAS en fonction du réseau qu'il protège.

Communément, pour un réseau local de 30 postes au maximum, les appliances installées sur les réseaux locaux ont les spécifications suivantes :

- carte mère de type industrielle (mtbf : 100.000 heures), - châssis aluminium massif, - aucune pièce mécanique en mouvement (mémoire flash, CPU "fanless", sans ventilation), - processeur Intel-Atom (N270), - mémoire flash 512 Mo, mémoire RAM 512 Mo, - 2 interfaces réseau 1Gbts, - alimentation externe. - OS : Linux 2.6.37	

Exemple d'une appliance NAVISTA.

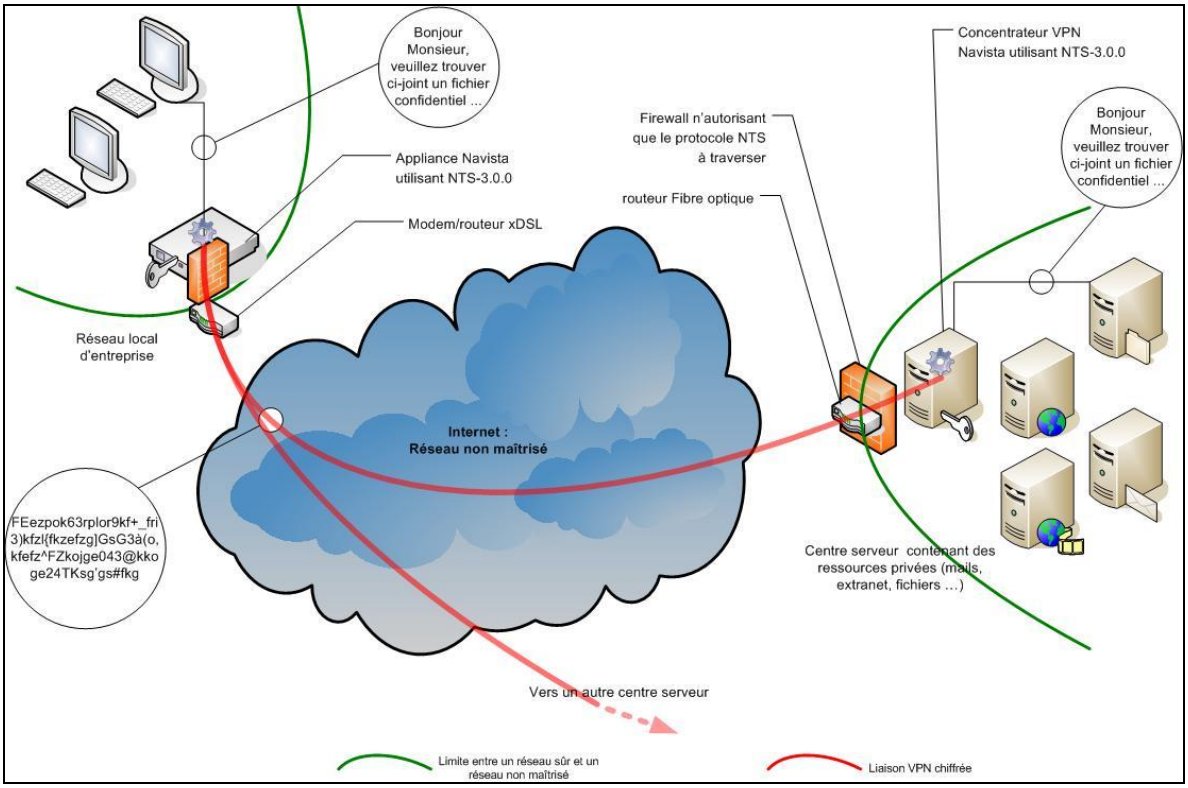


Exemple d'une installation dans un réseau local.

Le schéma ci-dessus illustre un mode d'installation standard d'une appliance NAVISTA-VPN. L'ensemble du trafic émis par les postes du réseau et à destination d'un autre réseau, va traverser l'appliance Navista. Les fonctions de routage de l'appliance envoient sur Internet le flux à destination des réseaux intégrés au réseau privés virtuel via le protocole NTS, les autres flux sont routés sur Internet sans chiffrement. De ce fait la présence sur le réseau local de l'appliance embarquant le protocole NTS est parfaitement transparente pour l'utilisateur.

Le schéma suivant représente la mise en œuvre du protocole NTS entre un réseau local équipé d'une appliance NAVISTA, et un centre d'hébergement équipé d'un frontal mettant à disposition diverses ressources.

Le protocole NTS a pour but de garantir la confidentialité et l'intégrité des données transitant par ce système. La connexion ne s'établie qu'après une authentification forte négociée entre le client et le serveur.



Exemple de mise en œuvre de la solution NAVISTA-VPN.

2.2. Description de la manière d'utiliser le produit

Deux grands types d'utilisateurs sont impliqués :

- les utilisateurs finaux. Ce sont les utilisateurs des postes présents sur les réseaux locaux intégrant le réseau virtuel privé. Pour ces utilisateurs, l'utilisation du produit est totalement transparente. Les tunnels "montés" vers les autres appliances ou les concentrateurs, les droits et les priorités afférents sont définis par l'administrateur du réseau et les utilisateurs des postes de travail n'ont aucune action à effectuer.

- les administrateurs du réseau. Ils peuvent avoir des niveaux d'intervention et des droits différents sur l'administration, la maintenance et la télé-administration des appliances et des concentrateurs. Les outils logiciels intégrants la solution NAVISTA-VPN, et utilisés par ces administrateurs, se situent en dehors du périmètre de la présente cible et ne seront donc pas décrits. Cependant la modification des configurations de l'appliance est faite à distance. L'outil de configuration est un concentrateur VPN destiné à la télé-maintenance et télé-administration de toutes les appliances.

2.3. Description de l'environnement prévu pour l'utilisation du produit.

L'environnement système dans lequel évolue le logiciel est sûr car maîtrisé par l'intégrateur NAVISTA. De ce fait seul l'environnement physique nécessite quelques pré-requis.
L'appliance NAVISTA doit être installée au sein des locaux d'une entreprise, il est considéré par défaut que l'accès au site et au local où se trouve précisément l'appliance est réservé aux personnels connus de l'entreprise et pour lesquels ce local est accessible. L'appliance ne peut donc pas être attaquée physiquement. L'administrateur du réseau d'entreprise a la possibilité de configurer l'appliance, configuration réseau, ajout/suppression de services, ajout/suppression de VPN. En aucun cas l'utilisateur et l'administrateur n'ont accès aux clés et certificats utilisés par NTS 3.1. Pour les réseaux « grand comptes », l'administration est faite par le support NAVISTA qui est exclusivement composé de personnes qualifiées internes à la société.

Concernant les concentrateurs, l'installation est généralement faite dans un centre serveurs. Ce type d'activité est réputé comme mettant en œuvre toutes les procédures d'accès et de sécurité généralement pratiqués dans ce domaine d'activité.

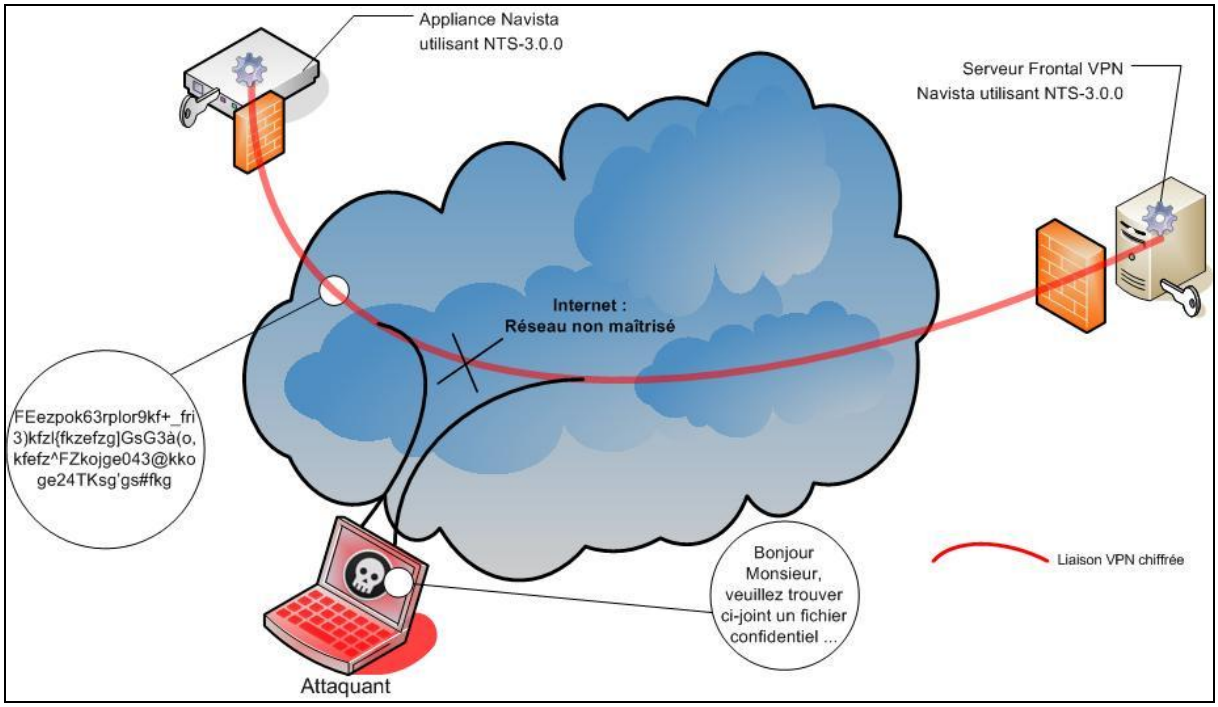
Génération et partage des clés RSA

Pour fonctionner, le protocole NTS, en mode client, nécessite une clé privée de 4096 bits et la clé publique du serveur. En mode serveur, le protocole NTS nécessite sa propre clé privée de taille 4096 bits, la clé publique du client et une clef Diffie-Hellman.
Pour chaque appliance produite, les clés privées, uniques et propres à chaque matériel sont générées lors de la production en usine dans les locaux de NAVISTA, les clés publiques en sont déduites.
Lors de la mise au rebus d'une appliance, les supports de stockages sont formatés, les clés sont détruites.
L'échange des clés RSA publiques entre les deux environnements devant communiquer ainsi que le stockage de celles-ci ne font pas l'objet de cette certification et sont donc hors du périmètre d'évaluation.

2.4. Exemple de menaces sur l'exploitation du produit.

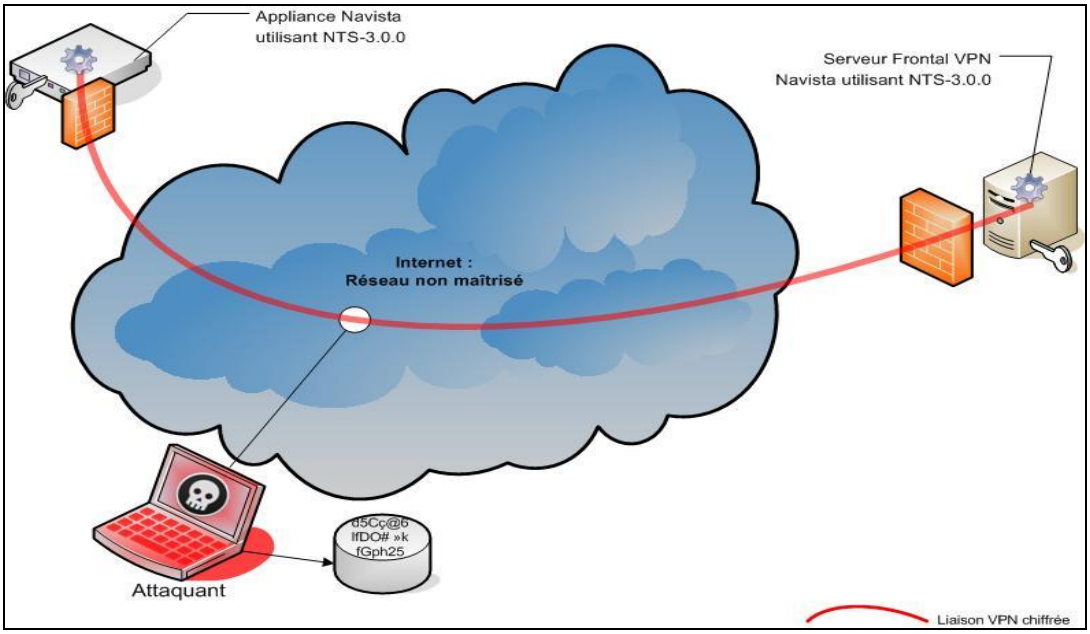
2.4.1. Attaque de type Man in the middle

Un attaquant dispose de plusieurs méthodes connues pour s'interfacer entre deux éléments d'un réseau, comme par exemple le spoofing arp ou encore le DNS poisoning. L'attaquant peut se faire passer pour le serveur VPN vis à vis du client et se faire passer pour le client VPN vis à vis du serveur. Son but étant de tracer l'authentification des VPN afin de récupérer les clés de session et de déchiffrer les données échangées.



2.4.2. Attaque de type Sniffing

Un attaquant peut éventuellement enregistrer les données chiffrées par NTS, afin de tenter d'en déduire les clés de session et de pouvoir ainsi déchiffrer les flux ou communiquer avec NTS en utilisant cette même clé de session.

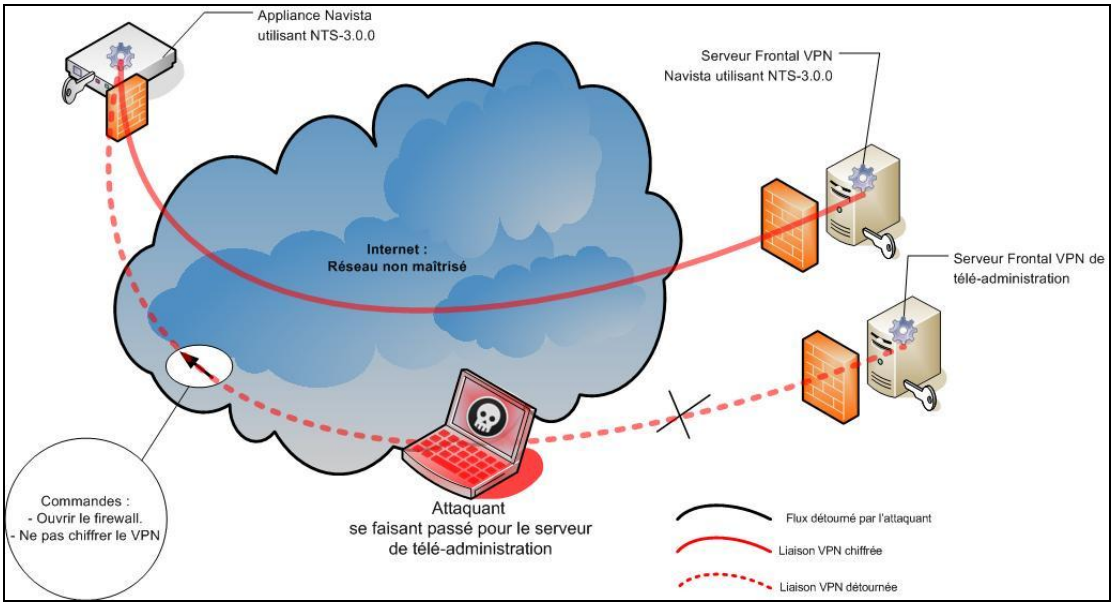


2.4.3. Attaque par rejeu

Un attaquant peut simplement "sniffer" le réseau comme dans l'attaque vue précédemment et, après que le dialogue entre les deux parties soit terminé, réémettre les paquets capturés vers le serveur afin de se faire passer pour le client sans pour autant connaître les clés de session. Cela lui permet de rejouer une ancienne transaction et de s'authentifier auprès du serveur comme s'il était le client NTS.

2.4.4. Attaque par usurpation d'identité.

Un attaquant a la possibilité de se faire passer pour le concentrateur VPN destiné à la télé administration des appliances. Si l'attaquant s'interpose entre l'appliance et le serveur de télé administration, il a la possibilité de prendre la main sur la configuration de l'appliance en question et donc de modifier le fonctionnement de celle-ci. Les données en transit vers les services métiers pourraient êtres détournées et corrompues. Dans le cas d'une attaque de ce type réussie, l'attaquant peut très bien ouvrir le firewall de l'appliance, changer le mode de chiffrement d'un autre VPN NTS… Cette méthode d'attaque n'est ni plus ni moins qu'une attaque de type man-in-the-middle mais faite sur le VPN NTS servant à la télé-administration. Contrairement à l'attaque décrite dans le chapitre 2.4.2, l'attaquant n'a pas la nécessité de laisser la connexion établie entre l'appliance et le concentrateur VPN. Il n'a pas à se soucier de la connexion vers le concentrateur. Il lui suffit d'établir la connexion qui lui permettra de communiquer avec l'appliance
Le schéma ci-après illustre ce type d'attaque.



2.5. Mesures de sécurité mises en œuvre pour contrer les menaces.

2.5.1. Prévention du man in the middle

Afin de prévenir les attaques de type man in the middle, NTS utilise une authentification mutuelle en utilisant la cryptographie asymétrique. Chaque paquet envoyé par NTS est signé par le protocole **RSA-PSS** avec une clé permettant d'authentifier l'autre partie. De ce fait un attaquant ne connaissant pas les clés de signature ne peut émettre des paquets signés. Les paquets non signés ou signés avec une mauvaise clé sont détruit et comptabilisés. A partir d'un nombre défini de paquets dont la signature n'est pas valide, le VPN se déconnecte et une nouvelle authentification à lieu.

2.5.2. Prévention des attaques par Sniffing

NTS renouvelle régulièrement les clés de session qui servent à chiffrer et déchiffrer les paquets. Le but étant de renouveler les clés avant qu'un attaquant ait le temps d'identifier les clés de session utilisées lors de son analyse.
Plusieurs paramètres définissent le renouvellement des clés. Le temps, la quantité de données qui ont été chiffrés avec cette clé et le nombre de paquets qui ont été chiffrés à l'aide de la clé de session sont les principaux paramètres pris en compte par NTS.

2.5.3. Prévention des attaques par rejeu

Pour empêcher un attaquant de rejouer une transaction chiffrée et de s'authentifier auprès du serveur comme s'il connaissait la clef privé du client, le protocole NTS génère, lors du processus d'authentification, des aléas qui seront échangés entre les deux parties. Ces aléas seront utilisés pour construire les clés de session et de hachage. Le client et le serveur vont donc chiffrer et déchiffrer les messages avec des clefs différentes à chaque nouvelle connexion. Du fait de l'utilisation de ces aléas, si un attaquant veut rejouer une session, les clés de chiffrement et de hachage du serveur seront différente par rapport à la session précédente et tous les paquets envoyés par celui-ci seront refusés car indéchiffrables. De plus lorsqu'un nombre défini de paquet reçu par une des partie n'a pas réussi à être déchiffré, la connexion est interrompue et une nouvelle authentification à lieu.

2.5.4. Prévention des attaques d'usurpation d'identité.

La seule protection mise en œuvre pour ce type d'attaque reste dans l'inviolabilité du protocole NTS-3.1.0. Le VPN de maintenance est établi avec les mêmes spécificités que pour un VPN métier.
L'authentification mutuelle et les signatures sont gages de l'identité participant à la connexion VPN.

2.6. Dépendance du logiciel

NTS v3.1.0 fonctionne sur une plateforme LINUX 32 ou 64bits, pour fonctionner il nécessite les librairies et composantes suivantes :

Programme	Version	Description
kernel	>= 2.6.0	Noyau linux
Glibc	>= 2.3.4	Librairie standard linux
OpenSSL	>= 0.9.8r	Librairie cryptographique
FIPS	>= 1.2.3	Librairie cryptographique certifiée
Confuse	>= 2.5	Librairie de lecture de fichier de configuration

Plus de détails sont fournis dans le manuel d'installation et d'utilisation de NTS joint à ce document : *NTS-300-CSPN-MANUEL-1.01*

3. Définition du périmètre d'évaluation

Le périmètre d'évaluation concerne exclusivement l'application logicielle NTS en version 3.1.0. Des extensions sont disponibles pour le logiciel, comme des GUI, qui ne font pas partie de cette évaluation. Le logiciel est aussi décliné en version compatible Windows et MacOS qui n'entrent pas dans le champ de cette évaluation.

4. Description des biens sensibles que le produit doit transmettre

4.1. Protocoles supportés

Une multitude de protocoles peuvent être chiffrés par NTS. Les plus couramment utilisés sont les protocoles standards relatifs à la navigation comme HTTP, au transfert de fichiers comme FTP, ou encore à l'envoi et la réception d'email (SMTP, POP, IMAP), les protocoles de prise en main à distance comme RDP, VNC, …
Il est aussi capable de chiffrer les flux audio et vidéo comme le RTP, SIP, H323.
Les protocoles qui utilisent déjà un chiffrement (par exemple, HTTPS, SSH, SMTPS) sont sur-chiffrés. Tous les protocoles IP qu'ils utilisent ou non un chiffrement peuvent être encapsulés et de ce fait sécurisés par le VPN NTS.

Le protocole NTS encapsule et chiffre tous les types de flux sans distinction. Il est ainsi transparent aux données.

4.2. Type de biens

Toutes les données échangées au sein du réseau privé virtuel mettant en œuvre le protocole NTS sont chiffrées. On retrouve le plus fréquemment :

- des accès web vers un intranet ou extranet partagé par plusieurs réseaux.
- des connexions au bureau à distance (TSE, VNC, Console AS400), souvent utilisés dans la télémaintenance ou le télétravail.
- de l'échange de document, que ce soit en utilisant des partages réseaux distants ou en pièce jointe d'email, au bien dans les systèmes de télésauvegarde.
- des communications audio ou vidéo, de plus en plus utilisés par la visioconférence ou la téléphonie IP.

Dans tous ces cas et bien d'autres, le protocole NTS a pour seul but de garantir l'intégrité et la confidentialité des échanges de données à caractère confidentiel qui transitent via le réseau Internet public.