Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2012/05

Routeur chiffrant Navista
Version 2.8.0

Paris, le 16 mai 2012

Le directeur général de l'agence nationale de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié. C'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CSPN-2012/05**
Nom du produit **Routeur chiffrant Navista**
Référence/version du produit **2.8.0**
Catégorie de produit **Communication sécurisée**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)***
Développeur **NAVISTA** **567, rue Félix Trombe** **66100 Perpignan** **France**
Commanditaire **NAVISTA** **567, rue Félix Trombe** **66100 Perpignan** **France**
Centre d'évaluation **Oppida** **4-6, avenue du Vieil Etang - Bât B** **78180 Montigny Le Bretonneux**

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est le « Routeur chiffrant Navista**,** version 2.8.0 **»** développé par la société NAVISTA.

Ce produit est utilisé pour créer un réseau privé virtuel (*virtual private network*, ci-après dénommé VPN) permettant de garantir la confidentialité et l'intégrité des échanges de flux entre des réseaux locaux qui sont interconnectés à travers un réseau considéré comme « non sûr », typiquement Internet.

Il est livré sous la forme d'une *appliance* de puissance variable en fonction de la taille du réseau local auquel il est connecté. Le routeur chiffrant Navista s'appuie sur le protocole propriétaire NTS version 3.1.0 qui gère les mécanismes cryptographiques permettant la création du VPN. Ce sont principalement ces mécanismes qui ont été la cible de cette évaluation.

1.2. Description du produit évalué

La cible de sécurité [CDS] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1. Catégorie du produit

☐ 1 - détection d'intrusions
☐ 2 - anti-virus, protection contre les codes malicieux
☐ 3 – firewall
☐ 4 - effacement de données
☐ 5 - administration et supervision de la sécurité
☐ 6 - identification, authentification et contrôle d'accès
☒ **7 - communication sécurisée**
☐ 8 - messagerie sécurisée
☐ 9 – stockage sécurisé
☐ 10 - matériel et logiciel embarqué
☐ 99- Autres

1.2.2. Identification du produit

Le produit évalué est le routeur chiffrant en version 2.8.0 basé sur le protocole NTS en version 3.1.0.
La version certifiée du produit est identifiable dans l'interface d'administration du produit dans l'onglet « Informations générales ».

1.2.3. Services de sécurité

Le principal service de sécurité fourni par le produit est la création d'un réseau privé virtuel.

1.2.4. Configuration évaluée

La configuration évaluée est celle utilisée dans les petits réseaux, dans laquelle au maximum 30 machines peuvent être connectées au produit.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau. Les références des documents se trouvent en annexe 2.

2.2. Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation a été conforme à la charge de travail prévue lors de la demande de certification, elle-même conforme à la charge de travail préconisée dans [CSPN] pour un produit comportant des mécanismes cryptographiques, soit 35 hommes x jours.

2.3. Travaux d'évaluation

Ce paragraphe apporte des précisions sur la cible de sécurité [CDS] fournie en entrée de l'évaluation. Ces précisions sont issues du [RTE] élaboré par l'évaluateur suite à ses travaux.

2.3.1. Fonctionnalités, environnement d'utilisation et de sécurité

2.3.1.1. Spécification de besoin du produit

Conforme à la cible de sécurité [CDS] (chapitre 2 « Argumentaire (description) du produit »).

2.3.1.2. Biens sensibles manipulés par le produit

Conforme à la cible de sécurité [CDS] (chapitre 4 « Description des biens sensibles que le produit doit transmettre »).

2.3.1.3. Description des menaces contre lesquelles le produit apporte une protection

Conforme à la cible de sécurité [CDS] (chapitre 2.4 « Exemple de menaces sur l'exploitation du produit »).

2.3.1.4. Fonctions de sécurité

Conforme à la cible de sécurité [CDS] (chapitre 2.5 « Mesures de sécurité mises en œuvre pour contrer les menaces »).

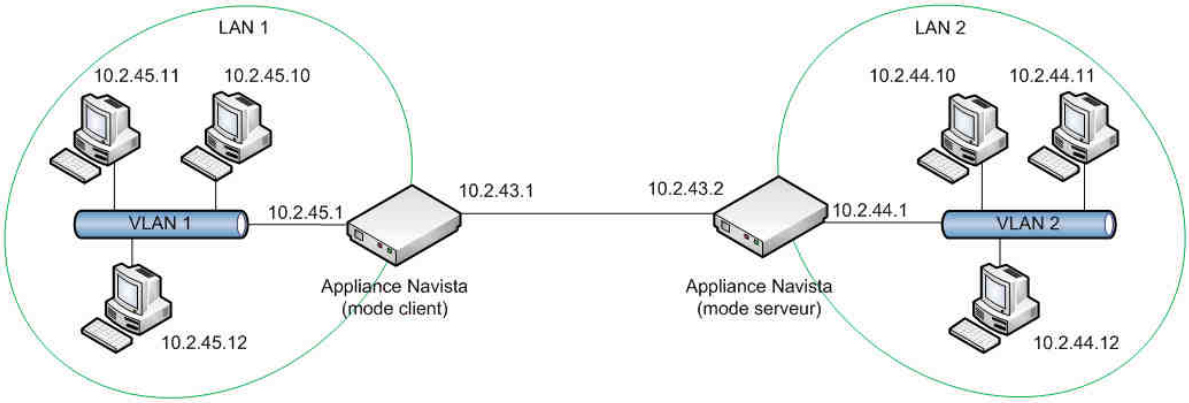
2.3.1.5. Utilisateurs typiques

Conforme à la cible de sécurité [CDS] (chapitre 2.2 « Description de la manière d'utiliser le produit »).

2.3.2. Installation du produit

2.3.2.1. Plate-forme de test

Lors de l'évaluation du produit, deux sous-réseaux ont été créés. Ils communiquaient sur un réseau local en utilisant les routeurs chiffrant Navista.



Des machines virtuelles VMWare Workstation 7.0 ont été utilisées pour simuler les sous-réseaux LAN1 et LAN2.

2.3.2.2. Particularités de paramétrage de l'environnement

Le produit est une *appliance* qui bascule automatiquement entre le mode client et le mode serveur en fonction du sous-réseau appelant. Les boitiers sont initialisés (configuration ou mise à jour logicielle) par l'intermédiaire du serveur *Navista Control Center* (Ncc) hébergé par Navista et hors du périmètre de la présente évaluation. Les clés maîtres privées (uniques et propres à chaque boitier) sont générées et chargées en usine dans les locaux de Navista, également en dehors du périmètre de la présente évaluation.

Aucun paramétrage n'est donc nécessaire si ce n'est la configuration des sous-réseaux.

2.3.2.3. Options d'installation retenues pour le produit

Sans objet.

2.3.2.4. Description de l'installation et des non-conformités éventuelles

Malgré une erreur de dénomination des interfaces dans le guide d'installation [GUIDES], l'évaluation n'a pas soulevé de difficulté ou de non-conformité lors de l'installation du produit.

2.3.2.5. Durée de l'installation

L'installation du produit se déroule en 30 minutes. La configuration du produit et des réseaux locaux peut prendre plus de temps en fonction de la taille des réseaux ciblés.

2.3.2.6. Notes et remarques diverses

L'installation est simple et ne requiert aucune configuration de la part de l'utilisateur.

2.3.3. Analyse de la documentation

L'évaluateur a eu accès à la documentation technique du produit [GUIDES]. La documentation est claire et aucune non-conformité n'a été relevée.

2.3.4. Revue du code source (facultative)

Les évaluateurs n'ont eu accès qu'à certaines parties du code source. Le code est bien documenté, il est lisible et facilement compréhensible.

L'audit du code disponible n'a pas permis de mettre en évidence l'utilisation de pratiques dangereuses.

2.3.5. Fonctionnalités testées

Fonctionnalité	Résultat
Authentification mutuelle	**Réussite**
Renouvellement de l'authentification	**Réussite**
Chiffrement et déchiffrement des communications	**Réussite**
Prévention anti-rejeu	**Réussite**
Mise à jour sécurisée	**Réussite**

2.3.6. Fonctionnalités non testées

L'évaluation du produit a été axée sur la création d'un réseau privée virtuel. Certaines fonctions de l'*appliance* (notamment le pare-feu) n'ont pas été testées en profondeur.

2.3.7. Synthèse des fonctionnalités testées / non testées et des non-conformités

Sans objet.

2.3.8. Avis d'expert sur le produit

Le produit est fonctionnellement conforme à sa cible de sécurité [CDS].

2.3.9. Analyse de la résistance des mécanismes et des fonctions

2.3.9.1. Liste des fonctions et des mécanismes testés

Fonction et mécanisme
Authentification
Gestion des sessions
Gestion des autorisations d'accès
Validation des données d'entrée

2.3.9.2. Avis d'expert sur la résistance des mécanismes

L'analyse de résistance des fonctions et mécanismes mis en œuvre par le routeur chiffrant Navista est positive. Le protocole NTS s'appuie sur des mécanismes cryptographiques décrits dans le §2.4 du présent rapport. Leur implémentation est jugée robuste par l'évaluateur.

2.3.10. Analyse des vulnérabilités (conception, construction…)

2.3.10.1. Liste des vulnérabilités connues

Il n'a pas été identifié de vulnérabilités connues sur ce produit particulier.

2.3.10.2. Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Aucune.

2.3.11. Accès aux développeurs

Au cours de l'évaluation, les évaluateurs ont eu accès au développeur du produit. Au cours des échanges techniques qui ont eu lieu, le développeur a fait preuve d'une bonne maîtrise de son produit et a été en mesure de répondre aux questions posées.

2.3.12. Analyse de la facilité d'emploi et préconisations

2.3.12.1. Cas où la sécurité est remise en cause

Néant.

2.3.12.2. Recommandations pour une utilisation sûre du produit

Les postes présents sur les sous-réseaux connectés au produit doivent héberger un système d'exploitation à jour concernant les correctifs de sécurité et correctement configuré (mise en place d'une politique de gestion de supports, authentification robuste), administré et supervisé. Ils doivent être par ailleurs au minimum, à défaut de l'emploi de technologies plus robustes, protégés par un produit anti-virus (avec bases d'informations à jour et proposant des fonctions de détection des infections informatiques furtives - anti-*spyware*, anti-*rootkit*, etc.) et un pare-feu correctement configuré.

L'accès physique à la cible de l'évaluation doit être restreint à des personnes de confiance.

Les recommandations présentent dans [GUIDES] doivent être appliquées.

2.3.12.3. Avis d'expert sur la facilité d'emploi

Moyennant le respect des recommandations évoquées précédemment, l'évaluateur n'a pas identifié de cas où le produit serait configuré ou utilisé de façon non sûre mais qu'un utilisateur pourrait raisonnablement croire sûre.

2.3.12.4. Notes et remarques diverses

Néant.

2.4. Analyse de la résistance des mécanismes cryptographiques

La liste des mécanismes cryptographiques analysés est fournie par la cible de sécurité [CDS] et les spécifications cryptographiques [SPEC_CRY].

La résistance de ces mécanismes a été analysée par l'évaluateur. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] et concluent que, si les recommandations présentes dans [GUIDES] sont appliquées, les mécanismes analysés atteignent le niveau standard défini dans le référentiel cryptographique de l'ANSSI (Cf. [REF-CRY]).

2.5. Analyse du générateur d'aléas

Les moyens mis en œuvre pour la génération et le retraitement des nombres aléatoires qui sont utilisés dans le routeur chiffrant Navista permettent d'atteindre le niveau de résistance aux attaques visé par la CSPN.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé.

Ce certificat atteste que le produit « Routeur chiffrant Navista**,** 2.8.0 **»** soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation spécifiés dans la cible de sécurité [CDS] et suivre les recommandations énoncées dans le présent rapport et dans l'ensemble des guides [GUIDES].

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CSPN ;* Référence : *NTS-310-CSPN-CIBLES-1.05* ; Date : *15/05/2012.*
[RTE]	*Rapport Technique d'Evaluation (RTE) - CSPN NTS-2.8.0 ;* Référence : *OPPIDA/CESTI/NTS/RTE/2.0* ; Date : *27/03/2012.*
[SPEC-CRY]	*Spécifications cryptographiques - Routeur Chiffrant Navista (version 2.8.0) et le protocole NTS (version 3.1.0) ;* Date : *02/02/2012.*
[ANA-CRY]	*Rapport d'évaluation des mécanismes cryptographiques ;* Référence : *OPPIDA/CESTI/NTS/CRYPTO/2.0* ; Date : *26/03/2012.*
[GUIDES]	Guide d'installation : *Navista Box - Manuel d'installation ;* Référence : *NBX v2.7.0* ; Date : *Juillet 2011.*

Annexe 2. Références à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CSPN]	Certification de sécurité de premier niveau (CSPN) des technologies de l'information, version 1, n° 1414/ANSSI/SR du 30 mai 2011. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1417/ANSSI/SR du 30 mai 2011. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1416/ANSSI/SR du 30 mai 2011. Documents disponibles sur www.ssi.gouv.fr.
[REF-CRY]	Référentiel général de sécurité, version 1.0, annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20. Documents disponibles sur www.ssi.gouv.fr.