PREMIER MINISTRE

Liberté
Égalité
Fraternité

Agence nationale de la sécurité
des systèmes d'information

Secrétariat général de la défense et de la sécurité nationale

Rapport de certification ANSSI-CSPN-2024/04

Logiciel passerelle IPSec virtualisée Mistral VS9

Version 9.1.0.13

Paris, le 22 Août 2024

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

Vincent STRUBEL

[ORIGINAL SIGNE]

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@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CSPN-2024/04**
Nom du produit **Logiciel passerelle IPSec virtualisée Mistral VS9**
Référence/version du produit **Version 9.1.0.13**
Catégorie de produit **Communication sécurisée**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **Thales SIX GTS France** 4 avenue des Louvresses 92622 Gennevilliers, France
Développeur **Thales SIX GTS France** 110 avenue Maréchal Leclerc 49300, Cholet
Centre d'évaluation **THALES / CNES** 290, allée du Lac 31670 Labège, France
Accord de reconnaissance applicable fixed time certification Ce certificat est reconnu dans le cadre du [BSZ_CSPN]
Fonctions de sécurité évaluées Audit et journalisation des évènements Gestion des clefs et certificats de trafic Contrôle d'accès Mise à jour logicielle Protection des flux de données Etat de défaillance Auto-test
Fonctions de sécurité non évaluées Sans objet
Restriction(s) d'usage Non

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 directeur général de l'Agence nationale de la sécurité des systèmes d'information 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 CSPN sont disponibles sur le site Internet cyber.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « Logiciel passerelle IPSec virtualisée Mistral VS9, Version 9.1.0.13 » développé par Thales SIX GTS France.

Ce produit est une passerelle IPSec virtualisée proposant le profil IPSec-DR, destinée à protéger les données échangées entre plusieurs *endpoints* dans un réseau complexe avec accès multisites, par l'instanciation de tunnels IPSec.

Ce produit fait partie plus largement du système Mistral, qui est composé d'une ou plusieurs passerelles IPSec Mistral VS9, d'un centre de gestion (Mistral Management Center - MMC) et d'une infrastructure à gestion de clefs (PKI).

La figure ci-dessous explicite l'architecture du système Mistral.

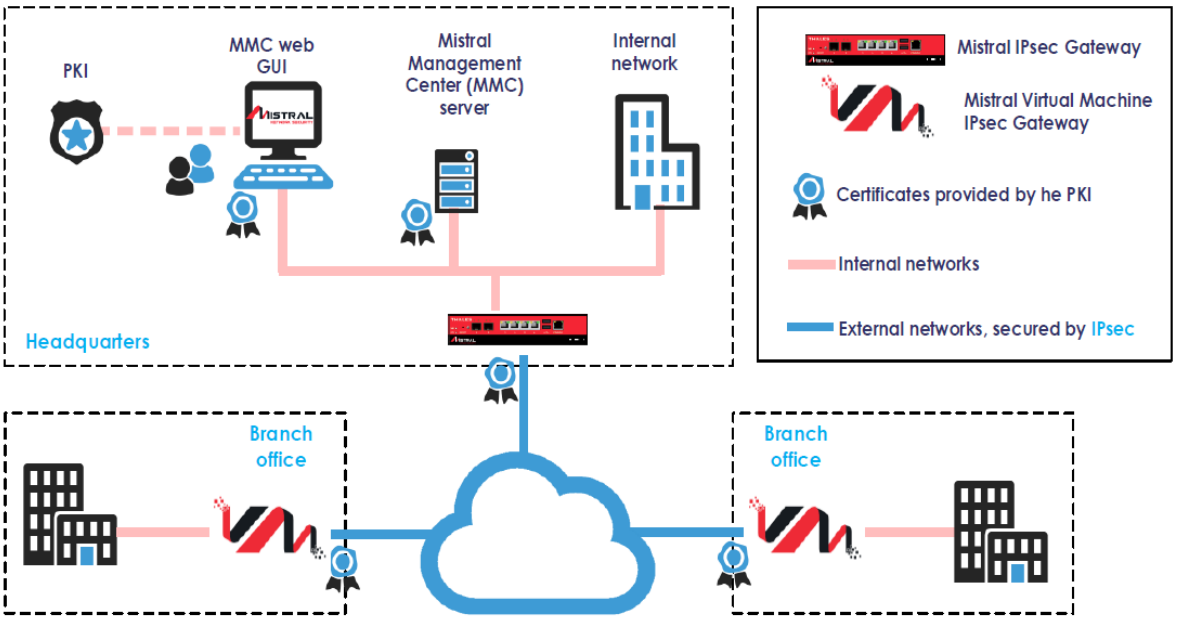


Figure 1 - Architecture du système Mistral.

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*

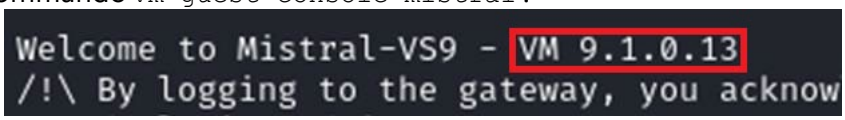
☐	1	détection d'intrusions
☐	2	anti-virus, protection contre les codes malicieux
☐	3	pare-feu
☐	4	effacement de données
☐	5	administration et supervision de la sécurité
☐	6	identification, authentification et contrôle d'accès
☒	**7**	**communication sécurisée**
☐	8	messagerie sécurisée
☐	9	stockage sécurisé
☐	10	environnement d'exécution sécurisé
☐	11	terminal de réception numérique (*Set top box*, STB)
☐	12	matériel et logiciel embarqué
☐	13	automate programmable industriel
☐	99	autre

1.2.2 *Identification du produit*

Produit	
Nom du produit	Logiciel passerelle IPSec virtualisée Mistral VS9
Numéro de la version évaluée	Version 9.1.0.13

La version certifiée du produit peut être identifiée :

- en se connectant à la console série de l'hyperviseur NEXIUM SafeCore puis au 'Mistral CLI' via la commande `vm-guest-console mistral` :



;

- et/ou en exécutant la commande `show system` dans le 'Mistral CLI' :

```
Mistral-VM / Mistral-VS9
OS release: 9.1.0.13
```

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- l'audit et journalisation des évènements ;
- la gestion des clefs et des certificats de trafic ;
- le contrôle d'accès ;
- la mise à jour logicielle ;
- la protection des flux de données ;
- l'état de défaillance ;
- l'auto-test.

1.2.4 *Configuration évaluée*

La configuration évaluée est le logiciel Mistral VS9, exécuté dans une machine virtuelle sur l'hyperviseur NEXIUM SafeCore, et comprenant un système d'exploitation Linux durci et des applications Mistral.

Tous les autres éléments du système Mistral (l'équipement matériel, l'environnement de virtualisation, le centre de gestion MMC, la PKI) font partie de l'environnement opérationnel du produit et sont en dehors du périmètre d'évaluation.

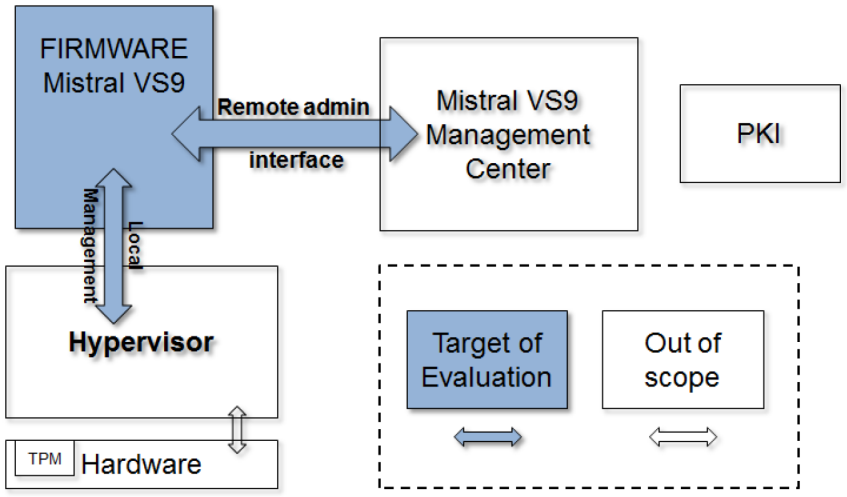


Figure 2 – Périmètre d'évaluation.

La plateforme de test est constituée des éléments suivants :

- une version de production de la machine virtuelle Mistral ;
- une version de *debug* (avec serveur SSH) de la machine virtuelle Mistral ;
- un banc de tests réseau comprenant un ordinateur de test avec plusieurs interfaces réseau et un commutateur (*switch*) virtuel ;
- un câble de connexion série connecté aux versions de production et de *debug* des machines virtuelles ;
- une PKI indépendante pour contrôler la génération des certificats.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN].

2.2 Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, des menaces, des utilisateurs et des fonctions de sécurité définis dans la cible de sécurité [CDS].

2.2.1 *Installation du produit*

2.2.1.1 Particularités de paramétrage de l'environnement et options d'installation

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

2.2.1.2 Description de l'installation et des non-conformités éventuelles

Le produit doit être installé par le service de support du développeur.

Le manuel d'utilisation inclut une section décrivant l'installation d'une machine virtuelle sur l'hyperviseur NEXIUM SafeCore.

Deux solutions sont possibles pour l'installation d'une machine virtuelle :

- Solution 1 : Installation connectée (au réseau) via un boot PXE :
    - connexion d'un équipement à un réseau d'installation ;
    - démarrage en boot PXE de l'équipement ;
    - réception des paramètres réseau du serveur DHCP dont les paramètres TFTP ;
    - récupération de l'installeur auprès du serveur TFTP et démarrage en local ;
    - récupération de la liste des profils d'installation auprès du serveur d'artefacts ;
    - installation suivant les instructions décrites dans le profil puis redémarrage
- Solution 2 : Installation déconnectée via un boot sur un périphérique local :
    - boot sur un périphérique local (clef USB, CD, etc.) sur lequel les artefacts sont présents. Si les artefacts sont chiffrés, les clefs de déchiffrement sont également nécessaires.

La deuxième solution a été choisie pour l'installation de la plateforme de test pour l'évaluation.

2.2.1.3 Notes et remarques diverses

Sans objet.

2.2.2 *Analyse de la documentation*

Les guides du produit permettent d'installer et d'utiliser le produit sans causer de dégradation accidentelle de la sécurité.

L'évaluateur a eu accès à des documents internes de conception dans le cadre de cette évaluation.

2.2.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source de l'intégralité du produit.

Cette analyse a contribué à l'analyse de conformité et de résistance des fonctions de sécurité du produit.

2.2.4 *Analyse de la conformité des fonctions de sécurité*

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

2.2.5 *Analyse de la résistance des mécanismes des fonctions de sécurité*

Toutes les fonctions de sécurité ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

2.2.6 *Analyse des vulnérabilités (conception, construction, etc.)*

2.2.6.1 Liste des vulnérabilités connues

Des vulnérabilités publiques existent sur le produit ou sur ses briques logicielles tierces, mais se sont révélées inexploitables pour le niveau d'attaquant considéré et dans le contexte défini par la cible de sécurité [CDS].

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

Des vulnérabilités potentielles ont été identifiées, mais se sont révélées inexploitables pour le niveau d'attaquant considéré et dans le contexte défini par la cible de sécurité [CDS].

2.2.7 *Analyse de la facilité d'emploi*

2.2.7.1 Cas où la sécurité est remise en cause

L'évaluateur n'a pas identifié de cas où la sécurité de la TOE est remise en cause.

2.2.7.2 Avis d'expert sur la facilité d'emploi

Aucun avis d'expert du CESTI n'a été donné quant à la facilité d'emploi du produit.

2.2.7.3 Notes et remarques diverses

Aucune note, ni remarque n'a été formulée dans le [RTE].

2.3 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [CDS]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [RTE].

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

2.4 Analyse du générateur d'aléa

Le produit comporte un générateur d'aléa qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto].

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

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 « Logiciel passerelle IPSec virtualisée Mistral VS9, Version 9.1.0.13 » 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 Recommandations et 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 spécifiés dans la cible de sécurité [CDS], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

3.3 Reconnaissance du certificat

Ce certificat est émis dans les conditions de l'accord du [BSZ_CSPN].

Cet accord permet la reconnaissance mutuelle des certificats de sécurité pour les schémas CSPN (Certification de Sécurité de Premier Niveau) et BSZ (Beschleunigte Sicherheitszertifizierung ou Certification de sécurité accélérée).

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : - *CSPN SECURITY TARGET - MISTRAL VS9 VIRTUAL IPSEC GATEWAY SOFTWARE*, référence 68922788-306-D, version D, 30 mai 2024.
[RTE]	Rapport technique d'évaluation : - *CSPN Evaluation Technical Report*, référence *BRQ_CSPN revision 1.5*, version 1.5, 2 juillet 2024.
[GUIDES]	Guide d'utilisation, administration ou installation du produit : - Manuel d'Utilisation - Gateway IPsec MISTRAL Virtualisée, référence 67691343-108-A - *Technical Note - Mistral VS9 system - guide to certificates, system version 9.1*, référence 68911167-612-B - *Technical Note Mistral VS9 system - creation of VPN tunnels*, référence 68916522-612-- - Manuel d'Utilisation MISTRAL Management Center, référence 67147242-108

ANNEXE B. Références liées 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 des produits des technologies de l'information, référence ANSSI-CSPN-CER-P-01, version 4.0, 3 mars 2022. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02, version 4.0, 28 mars 2020. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 3.0, 6 septembre 2018.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1, 26 janvier 2021.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.
[BSZ_CSPN]	*Mutual Recognition Agreement of cybersecurity evaluation certificates issued under fixed time certification process, BSI/ANSSI,* référence *bsz_cspn_mutual_recognition_agreement,*version 2.0, mai 2024.