Tableaux des exigences et des recommandations du référentiel IPsec DR

Version 1.0.3 – Février 2023

Ce document présente deux tableaux : un tableau d'exigences et un tableau de recommandations. Le tableau d'exigences liste les critères qu'un équipement doit satisfaire pour être éligible à l'obtention d'un agrément DR. Le tableau des recommandations, quant à lui, précise des critères additionnels permettant à l'équipement d'atteindre un niveau de sécurité plus élevé. En fonction de l'évolution de la menace ou de la réglementation, l'ANSSI sera susceptible de faire évoluer le contenu de ces tableaux.

Référence exigence	Description
E1	Un élément de configuration (e.g. case à cocher, commande unique spécifique, etc) permet de mettre la ToE dans un état de configuration compatible avec celui imposé par le référentiel (activation des fonctionnalités requises, désactivation des fonctionnalités interdites, désactivation des éléments crypto interdits, etc).
E2	L'ensemble des valeurs par défaut des options de la ToE favorisent la sécurité, i.e. tout mécanisme augmentant la surface d'attaque ou réduisant la sécurité de la ToE est désactivé.
E3	Le démon IKEv2 de la ToE implémente et négocie AES-GCM avec une clé de 256 bits et un ICV de 16 octets pour la protection des IKE_SA et des SA IPsec.
E4	Le démon IKEv2 et la pile IPsec de la ToE utilisent tous les deux des IV incrémentaux pour leurs implémentations d'AES_GCM.
E5	Le démon IKEv2 de la ToE implémente et négocie AES-CTR avec une clé de 256 bits et AUTH_HMAC_SHA2_256_128 pour la protection des IKE_SA et des SA IPsec.
E6	Le démon IKEv2 et la pile IPsec de la ToE utilisent tous les deux des IV incrémentaux pour leurs implémentations d'AES_CTR.
E7	Seuls les mécanismes cryptographiques AES-GCM, AES-CTR et AUTH_HMAC_SHA2_256_128 sont activés pour assurer la confidentialité et l'intégrité des données du démon IKEv2 et de la pile IPsec de la ToE.
E8	L'unique PRF négociée et utilisée dans le démon IKEv2 de la ToE est PRF_HMAC_SHA2_256.

E9	Le démon IKEv2 de la ToE implémente ECDSA sur secp256r1 avec SHA256 comme mécanisme d'authentification asymétrique (Auth Method 9, comme indiqué dans [NOTE-CRYPTO]).
E10	L'implémentation ECDSA du démon IKEv2 de la ToE inclut les vérifications complémentaires indiquées en section 3.4.3 de la note crypto du référentiel IPsec DR.
E11	Le démon IKEv2 de la ToE ne met en œuvre aucun autre mécanisme d'authentification que ceux listés en E9, R1, R2, R4, R5 et R6.
E12	Le démon IKEv2 de la ToE négocie et impose le support de l'anti-rejeu via ESN en émission et réception.
E13	Le démon IKEv2 de la ToE implémente, négocie et impose le support des *Childless* SA défini dans [RFC6023].
E14	Le démon IKEv2 n'émet aucun *payload* SA ou TS lors de l'échange IKE_AUTH.
E15	Le démon IKEv2 refuse tout échange IKE_AUTH contenant un *payload* SA ou TS.
E16	Le démon IKEv2 de la ToE implémente et négocie secp256r1 comme groupe ECDH.
E17	Le démon IKEv2 de la ToE implémente et négocie BrainpoolP256r1 comme groupe ECDH.
E18	Le démon IKEv2 de la ToE implémente et négocie les Diffie-Hellman Group Transform IDs 19 (256-bit random ECP group basé sur secp256r1) et 28 (brainpoolP256r1).
E19	Le démon IKEv2 de la ToE ne négocie et n'utilise aucun autre Diffie-Hellman Group Transform IDs que ceux listés ci-dessus. Soit les IDs 19 (256-bit random ECP group basé sur secp256r1) et 28 (brainpoolP256r1).
E20	Les *payloads* ID émit par le démon IKEv2 de la ToE n'incluent pas de données topologiques.
E21	Le démon IKEv2 de la ToE ne produit et n'accepte que des *payloads* SA dont les *proposal* ne contiennent chacune qu'au plus une seule instance de chaque type de *transform*. Se référer à l'annexe A de la [NOTE-CRYPTO].
E22	Le démon IKEv2 ne propose pas et refuse le support d'IPcomp.
E23	Le démon IKEv2 ne permet que la mise en œuvre de SA IPsec utilisant ESP en mode tunnel (pas de mode transport, pas d'AH, etc).
E24	Lors d'une authentification asymétrique, le démon

	IKEv2 de la ToE vérifie la validité des certificats présentés par l'homologue (remontée à une racine de confiance locale, validité temporelle, validité du *keyUsage*, validation de l'identité, etc).
E25	Le démon IKEv2 de la ToE supporte et utilise la prise en compte de CRL comme mécanisme de révocation lors de l'utilisation de la validation de certificat.
E26	Le démon IKEv2 de la ToE supporte et utilise OCSP comme mécanisme de révocation lors de l'utilisation de la validation de certificat. Pour cela, le démon IKEv2 doit supporter l'agrafage OCSP transmis au sein du tunnel IKEv2 [RFC4806] ainsi que la vérification directe auprès d'un serveur OCSP. Le choix entre ces deux méthodes doit être possible via des paramètres de configuration. Pour cela, la valeur OCSP Content (14), définie dans [RFC4806], pour le champ Certificate Encoding des payloads IKEv2 CERT et CERTREQ est autorisée en plus des valeurs listées dans la section 3.6 de [RFC7296_modifiée_ANSSI].
E27	Les paquets IKEv2 et ESP reçus par la ToE avec une intégrité cryptographique invalide sont rejetés silencieusement par la ToE. Il en est de même des paquets rejoués.
E28	Le démon IKEv2 de la ToE émet et attend des *payload* KE (et NONCE) lors de chaque échange CREATE_CHILD_SA, i.e. chaque négociation de SA IPsec utilise un secret frais basé sur un échange ECDH utilisant l'un des deux groupes définis précédemment.
E29	Lors des générations de points aléatoires sur une courbe par tirage d'une valeur secrète k dans]0,q[(q étant l'ordre de la courbe), la méthode de génération de k est associée à un générateur d'aléa cryptographique conforme au RGS et est implémentée sous la forme de l'une des deux méthodes présentées en section 7.1 de [NOTE-CRYPTO].
E30	Le démon IKEv2 de la ToE réalise les vérifications d'usage en matière de format et de valeur attendus sur les paramètres ECDH reçus dans les *payloads* KE, comme précisé en section 4.4. de [NOTE-CRYPTO].
E31	Les nonces produits par le démon IKEv2 ont exactement une taille de 16 octets.
E32	Tout nonce reçu d'un homologue qui a une taille

	strictement différente à 16 octets résulte en un arrêt de l'échange.
E33	Chaque production d'un secret partagé via un échange de *payload* KE met en œuvre une valeur secrète éphémère générée spécifiquement pour l'occasion et d'une manière sûre. Cette valeur est effacée de manière sûre après calcul du secret partagé. Ce dernier point est validé spécifiquement dans le binaire produit pour la ToE.
E34	Le démon IKEv2 de la ToE utilise par défaut le mécanisme de COOKIE défini dans [RFC7296_modifiée_ANSSI].
E35	Le démon IKEv2 de la ToE est développé de manière défensive et met en œuvre des mécanismes de défense en profondeur.
E36	Les *toolchains* utilisés pour compiler la ToE sont à l'état de l'art et tirent parti de l'ensemble des mécanismes de durcissement disponibles. Les mécanismes de durcissement non activés sont listés et des justifications sérieuses sont apportées.
E37	La pile IPsec de la ToE implémente AES-GCM avec une clé de 256 bits et un ICV de 16 octets.
E38	La pile IPsec de la ToE implémente AES-CTR avec une clé de 256 bits et AUTH_HMAC_SHA2_256_128.
E39	La ToE implémente dans ses mécanismes d'auto-test les différents vecteurs de test fournis dans la note crypto [NOTE-CRYPTO].
E40	La ToE implémente les formats d'encodage de données fournis dans la note crypto [NOTE-CRYPTO].
E41	Si la ToE met en œuvre des coprocesseurs cryptographiques, celle-ci respecte [ANSSI-CC-CRY-P-01].
E42	Le démon IKEv2 de la ToE supporte une *window size* de 1 non configurable, i.e. n'émet, ni n'accepte de notification SET_WINDOW_SIZE permettant de changer cette valeur. Toute notification SET_WINDOW_SIZE est ignorée.
E43	La pile IPsec de la ToE ne produit pas pour une SA donnée de déséquencement de paquet avec une distance supérieure à 64, quelle que soit la taille ou le débit considéré.
E44	La pile IPsec de la ToE supporte une fenêtre anti-rejeu d'au moins 1024 paquets par SA.
E45	La pile IPsec de la ToE ne permet pas la désactivation des mécanismes d'anti-rejeu.

E46	La pile IPsec de la ToE implémente bien après déchiffrement une vérification des paquets contre la SP associée à la SA ayant permis le déchiffrement.
E47	La ToE permet l'export des clés d'authentification symétriques (Auth Method 2) et des clés publiques d'authentification asymétriques (Auth Method 9, 214, 225 et 228) dans un format documenté permettant la mise en place d'interopérabilité avec un autre équipement compatible du référentiel.
E48	L'ensemble des composants logiciels de la ToE traitant des données extérieures est programmé de manière défensive.
E49	L'ensemble des composants logiciels de la ToE traitant des données extérieures est compilé avec les différentes options de durcissement de la *toolchain* utilisée.
E50	L'ensemble des composants logiciels de la ToE traitant des données extérieures est compilé avec un niveau de *warning* élevé.
E51	L'ensemble des composants logiciels de la ToE traitant des données extérieures compile sans *warning*.
E52	L'ensemble des composants logiciels de la ToE traitant des données extérieures est compilé sans option de *debug*.
E53	La *toolchain* utilisée pour la compilation des composants logiciels de la ToE est récente et à jour.
E54	La ToE utilise les fonctionnalités de durcissement applicatifs fournis par l'*OS support* (e.g. ASLR, diminution de privilège, *sandboxings*, etc).
E55	La ToE fait un usage par défaut nul des mécanismes de *bypass*, garantissant ainsi par défaut l'absence de fuite de données claires vers l'extérieur.

Référence recommandation	**Description**
R1	Le démon IKEv2 de la ToE implémente ECSDSA sur BrainpoolP256r1 avec SHA256 comme mécanisme d'authentification asymétrique (Auth Method 228, comme indiqué dans [NOTE-CRYPTO]).
R2	Le démon IKEv2 de la ToE implémente ECSDSA sur secp256r1 avec SHA256 comme mécanisme d'authentification asymétrique (Auth Method 225,

	comme indiqué dans [NOTE-CRYPTO]).
R3	L'implémentation ECSDSA du démon IKEv2 de la ToE inclut les vérifications complémentaires indiquées en section 3.3.3 de la note crypto du référentiel IPsec DR.
R4	Le démon IKEv2 de la ToE implémente ECDSA sur BrainpoolP256r1 avec SHA256 comme mécanisme d'authentification asymétrique (Auth Method 214, comme indiqué dans [NOTE-CRYPTO]).
R5	Le démon IKEv2 de la ToE utilise PRF_HMAC_SHA2_256 comme mécanisme d'authentification symétrique (dans le cadre de l'Auth Method 2 et de la négociation de la PRF PRF_HMAC_SHA2_256).
R6	Le démon IKEv2 de la ToE implémente RSA avec des clés de taille supérieure ou égale à 2048 bits comme mécanisme d'authentification asymétrique (Auth Method 1) et est conforme à la partie relative à RSA dans la section 3.8 de [RFC7296]. Cette option ne doit être mise en place qu'à des fins de rétrocompatibilité avec l'IGC du système. Cette dernière devant être migrée vers ECDSA ou ECSDSA. La ToE permet l'export de ces clés RSA.
R7	Le démon IKEv2 n'utilise que le port 4500 UDP et met toujours en œuvre les mécanismes de NAT-Traversal sans négociation.
R8	L'ensemble des paquets ESP sont transportés encapsulés sur UDP port 4500.

Ressources :

[NOTE-CRYPTO] https://www.ssi.gouv.fr/ipsec-dr
[ANSSI-CC-CRY-P-01] https://www.ssi.gouv.fr/uploads/2015/01/anssi-cc-cry-p-01-modalites-pour-la-realisation-des-analyses-cryptographiques_v4.1.pdf
[RFC6023] https://www.rfc-editor.org/rfc/rfc6023.html
[RFC7296] https://www.rfc-editor.org/rfc/rfc7296.html
[RFC4806] https://www.rfc-editor.org/rfc/rfc4806.html
[RFC7296_modifiée_ANSSI] https://ssi.gouv.fr/guide/ipsec-dr/