AMOSSYS

CIBLE DE SECURITE CSPN

PROVE IT

version 4.0-4

Catégorie

« Identification, authentification, contrôle d'accès »

Référence : CSPN-ST-PROVE IT-1.01-version-publique

Date : le 26/07/2018

Code interne : RUB001

Siège : 4 bis allée du Bâtiment ● 35000 Rennes ● France ● www.amossys.fr

SIRET : 493 348 890 00036 ● **NAF** : 6202 A ● RCS Rennes B 493 348 890 ● SAS au capital de 38.000 Euros

FICHE D'EVOLUTIONS

Révision	Date	Description	Rédacteur(s)
1.00	05/12/2017	Création du document	K. RESCHE
1.01	26/07/2018	Modifications suite à la première évaluation CSPN	E. GOUSSET

Ce document a été validé par RUBYCAT-Labs.

SOMMAIRE

1. INTRODUCTION

1.1. OBJET DU DOCUMENT

Ce document est réalisé dans le cadre de l'évaluation, selon le schéma CSPN[1] promu par l'ANSSI[2], du produit « **PROVE IT** » développé par la société **RUBYCAT-Labs**.

La TOE[3] considérée comprend les modules :

Contrôle d'accès RDP
Traçabilité RDP
Administration et audit

de la solution **PROVE IT en version 4.0**.

Ce document est soumis au contrôle technique et qualité d'**AMOSSYS** ainsi qu'à la validation de **RUBYCAT-Labs**. Les mises à jour de ce document sont effectuées par l'équipe projet d'**AMOSSYS**.

1.2. IDENTIFICATION DU PRODUIT

Éditeur	**RUBYCAT-Labs** 1137 A Avenue des Champs Blancs 35510 Cesson-Sévigné
Lien vers l'organisation	https://www.rubycat-labs.com
Nom commercial du produit	PROVE IT
Numéro de la version évaluée	4.0-4
Catégorie du produit	Identification, authentification et contrôle d'accès

1.3. REFERENCES

L'analyse d'impact entre la première et la présente évaluation est présentée dans le document CSPN-IAR-ProveIT2-1.00.docx.

Pour l'établissement de la présente cible de sécurité, les documents suivants ont été consultés par le rédacteur :

- Brochure « Renforcez la sécurité des accès sensibles au SI » ;
- Brochure « Contrôle des accès critiques – Maîtrise des actions sensibles » ;
- Document RUBYCAT_Labs_PROVEIT_CSPN_doc_preliminaire_20171120.pdf, « CSPN – Document préliminaire » ;
- Document RUBYCAT_Labs_PROVEIT_CSPN_environnement_test_20171128.pdf, « CSPN - Complément informations - Environnement de test ».

[1] Certification de Sécurité de Premier Niveau
[2] Agence nationale de la sécurité des systèmes d'information
[3] *Target Of Evaluation*

2. DESCRIPTION DU PRODUIT

2.1. DESCRIPTION GENERALE

PROVE IT est une appliance logicielle qui vise à renforcer le contrôle des accès sensibles aux ressources d'un système d'information ainsi qu'à apporter une traçabilité avancée en proposant des pistes d'audit pour l'ensemble de ces accès.

Cette appliance offre ainsi un point d'entrée fédérateur pour les différents accès au Système d'Information (SI). **PROVE IT** permet notamment à l'administrateur de déclarer différentes populations d'utilisateurs et de leur donner accès à des serveurs via les protocoles RDP et SSH. Les utilisateurs doivent s'authentifier et accèdent ensuite uniquement aux ressources qui sont éligibles par rapport à leur profil.

La plateforme dispose également d'un module de gestion des identités permettant de protéger les identifiants des comptes d'accès aux ressources critiques.

Seul le mode RDP de PROVE IT entre dans le cadre de l'évaluation CSPN. Le mode SSH est considéré hors périmètre.

2.2. PRINCIPE DE FONCTIONNEMENT

La solution se positionne en coupure des accès internes et externes du SI. Elle se place sur le réseau interne pour assurer sa fonction de portail d'accès centralisé aux ressources. La solution ne nécessite pas l'installation d'agents sur les serveurs cibles ni sur les clients.

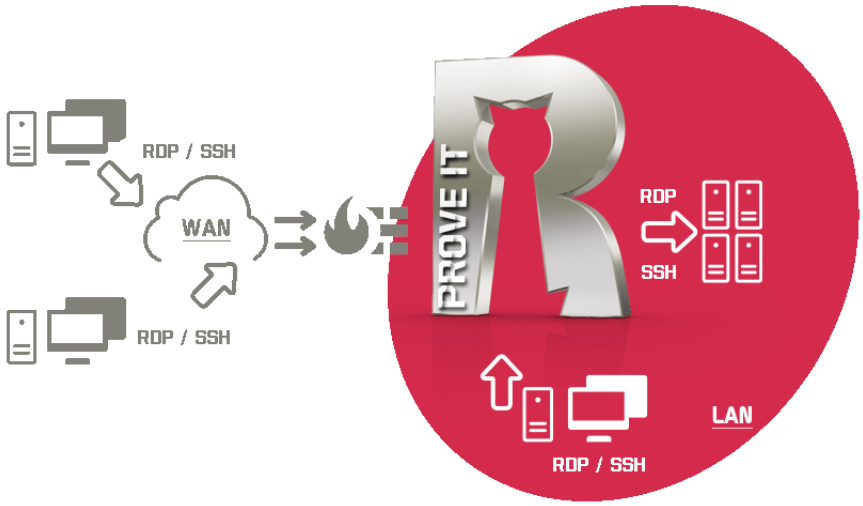

Figure 1 - Schéma de fonctionnement de PROVE IT

L'administration de la solution passe par une interface web accessible de façon sécurisée (HTTPS) qui met à disposition un tableau de bord avec une vue générale sur :

- l'activité des utilisateurs « à privilèges » connectés au portail ;
- l'espace de stockage utilisé pour l'archivage ;
- la charge de la plateforme.

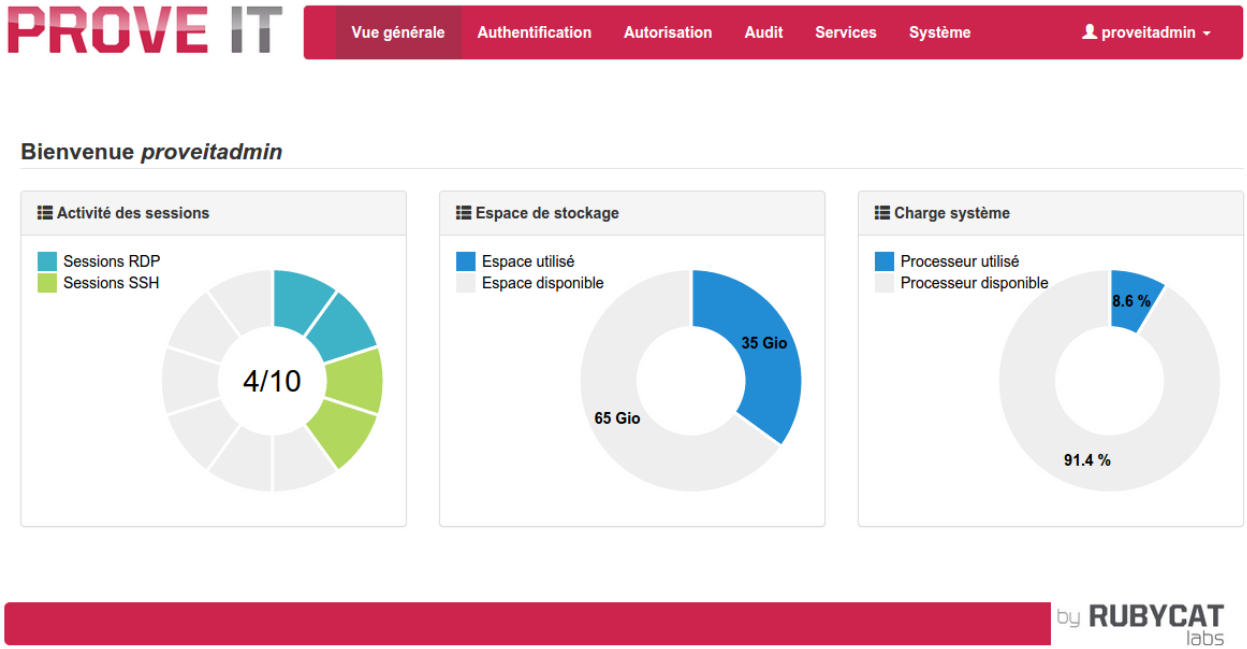

Figure 2 - Tableau de bord

En outre, à travers cette interface, un administrateur à la possibilité de :

- visualiser les sessions RDP en cours ;
- accéder aux connexions RDP archivées ;
- visualiser un enregistrement RDP ;
- etc.

2.3. DESCRIPTION DES DEPENDANCES

PROVE IT est distribué en tant qu'image ISO à installer sur un serveur dédié. Les systèmes de virtualisation compatibles sont VMware ESX 5+, Microsoft Hyper-V 2008+ et QEMU/KVM. Le système d'exploitation est Ubuntu 16.04 LTS.

2.4. DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT

2.4.1. Matériel compatible ou dédié

Les systèmes de virtualisation compatibles avec la solution **PROVE IT** sont VMware ESX 5+, Microsoft Hyper-V 2008+ et QEMU/KVM.

En ce qui concerne l'environnement RDP, la solution est compatible avec les éléments suivants (versions actuellement supportées i.e. officiellement testées) :

- Clients RDP :
  - MSTSC – MS Windows 7 (6.2.9200) ;
  - MSTSC – MS Windows 8 (6.3.9600) ;
  - MSTSC – MS Windows 10 (10.0.15063) ;
  - XFREERDP (≥ 1.0.2) – Linux ;

- Serveurs RDP :
  - Windows Server 2008 R2 ;
  - Windows Server 2012 ;
  - Windows Server 2016 ;

2.4.2. Système d'exploitation retenu

Pour l'évaluation, le produit **PROVE IT** (image ISO) sera installé au sein d'un environnement VMware ESXi. Le système d'exploitation sous-jacent est Ubuntu 16.04 LTS (64 bits).

Les ressources cibles seront hébergées sur des postes Windows Server 2016 (RDP). Les postes utilisateurs seront des postes Windows 10 sur lesquels le client RDP sera installé.

2.5. PERIMETRE DE L'EVALUATION

2.5.1. Périmètre

L'évaluation porte sur :

- les modules de contrôle d'accès et de traçabilité des flux utilisateurs sur le protocole RDP ;
- le module d'administration web.

Sont considérés hors périmètre :

- Les systèmes d'exploitation et logiciels RDP des ressources cibles et postes utilisateurs ;
- Les modules de « Filtrage », « Gestion des Identités secondaires », « Accès Admin maintenance » et « Gestion DB & Storage », de la solution **PROVE IT** ;
- Les modules de contrôle d'accès et de traçabilité des flux utilisateurs sur le protocole SSH.

2.5.2. Plateforme d'évaluation

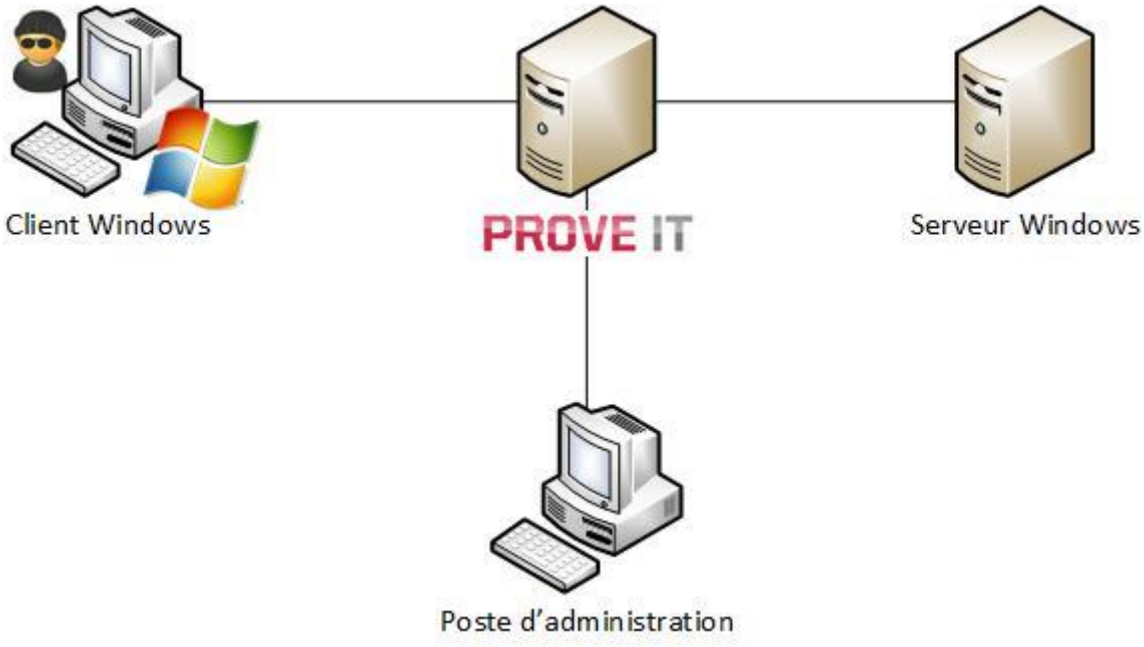

Figure 3 - Plateforme d'évaluation

3. PROBLEMATIQUE DE SECURITE

3.1. DESCRIPTION DES UTILISATEURS TYPIQUES

Par définition, les utilisateurs concernent les personnes et services applicatifs qui interagissent avec **PROVE IT**.

Les rôles suivants doivent être pris en considération dans le cadre de l'évaluation de sécurité :

- les **administrateurs** sont les personnes en charge de l'administration de **PROVE IT** et pouvant se connecter à l'interface web (l'accès maintenance n'étant pas considéré pour l'évaluation). Ils réalisent les opérations d'administration suivantes :
  - gérer les comptes utilisateurs et les moyens d'authentification ;
  - définir la politique de sécurité ;
  - gérer les ressources cibles ;
  - modifier certains paramètres techniques de la plate-forme.
- les **utilisateurs** sont des personnes utilisant les ressources du système d'information sous le contrôle de **PROVE IT**. Ces personnes peuvent être en charge de l'administration de ces ressources mais ne disposent normalement pas des droits d'administration sur **PROVE IT**.

3.2. DESCRIPTION DES BIENS SENSIBLES

Par définition, un bien sensible est une donnée (ou fonction) jugée comme ayant de la valeur par la TOE. Sa valeur est estimée selon des critères de sécurité (aussi appelés besoins de sécurité) : disponibilité, intégrité et confidentialité.

Les biens à protéger sont les suivants :

- B1.FLUX UTILISATEURS

Les flux applicatifs transitant par **PROVE IT** doivent être protégés en intégrité et confidentialité. **PROVE IT** ne doit pas altérer de manière illicite ces flux et ne doit pas permettre à une personne non explicitement autorisée de les consulter.

- B2.PISTES D'AUDIT

Les données d'activité concernant les utilisateurs, sauvegardées à des fins d'audit ultérieur, doivent être protégées en intégrité et confidentialité. **PROVE IT** ne doit pas permettre à une personne de supprimer, modifier ou même de consulter des pistes d'audit s'il n'en a pas explicitement les droits.

- B3.DONNEES UTILISATEURS

Il s'agit des identifiants et moyen d'assurer l'authentification des utilisateurs du SI sur la plateforme **PROVE IT**. Une personne non explicitement autorisée ne doit pas pouvoir consulter, modifier ou supprimer ces données.

- B4.DONNEES RESSOURCES CIBLES

Il s'agit des données permettant de se connecter aux serveurs cibles (informations réseaux, *credentials*…), ainsi que les règles d'accès à ces équipements (associations autorisées entre les clients et les serveurs cibles). Une personne non explicitement autorisée ne doit pas pouvoir consulter, modifier ou supprimer ces données.

- B5.JOURNAUX

Les données journalisées par la TOE (outre les pistes d'audit) ne doivent pas pouvoir être modifiées, supprimées ou consultées par une personne non explicitement autorisée à réaliser ces actions.

Les besoins de sécurité de chacun des biens à protéger sont donnés ci-dessous :

Biens sensibles	Disponibilité	Intégrité	Confidentialité
Flux utilisateurs		√	√
Pistes d'audit		√	√
Données utilisateurs		√	√
Données ressources cibles		√	√
Journaux		√	√

Tableau 1 - Besoins de sécurité des biens sensibles

3.3. DESCRIPTION DES HYPOTHESES SUR L'ENVIRONNEMENT

Par définition, les hypothèses sont des déclarations portant sur le contexte d'emploi de la TOE ou de son environnement.

Les hypothèses sur l'environnement de la TOE suivantes doivent être considérées :

- H1.ADMINISTRATEURS

Les administrateurs sont compétents, formés pour l'utilisation et l'administration de la TOE, et non hostiles.

- H2.INTEGRATION SI

La solution sera déployée sur une plateforme virtuelle (VM basée sur VMware ESX) positionnée sur un réseau interne IPv4 (nommé « LAN ») qui est isolé des réseaux extérieurs par un équipement de type pare-feu.

PROVE IT doit être le seul point d'entrée pour les utilisateurs, c'est à dire qu'il faut appliquer un cloisonnement réseau de sorte que les utilisateurs ne puissent pas se connecter en direct sur les serveurs.

Pour les accès utilisateurs et administrateurs initiés à partir du réseau « LAN », la connexion sera établie directement sur la plateforme **PROVE IT**. Pour les accès externes au réseau « LAN », la connexion sera établie au travers d'un équipement tiers de type VPN.

En outre, l'environnement virtuel de déploiement (ESX) est considéré comme sécurisé et de confiance.

- H3.ACCES PHYSIQUE

L'accès physique sur le serveur **PROVE IT** (et à sa console web) est restreint aux seuls administrateurs du produit. En outre, l'accès de maintenance (en SSH) au système est désactivé.

3.4. DESCRIPTION DES MENACES

Par définition, une menace est une action ou un événement susceptible de porter préjudice à la sécurité de la TOE.

Les agents menaçants à considérer pour l'évaluation de sécurité doivent être les suivants :

- **Entités non autorisées** : un attaquant humain ou entité qui interagit avec la TOE mais ne dispose pas d'accès légitime à la TOE ;
- **Entités autorisées**, à savoir les utilisateurs qui ont un accès à la ressource contrôlée par la TOE.

Les administrateurs ne sont pas considérés comme des attaquants.

Les menaces qui portent sur les biens sensibles de la TOE sont les suivantes :

- M1.ALTERATION DES FLUX UTILISATEURS

Un attaquant parvient à intercepter, lire et modifier les flux applicatifs transitant par la TOE.

- M2.ACCES ILLICITE A UNE RESSOURCE ADMINISTREE

Un attaquant parvient à accéder de manière illicite à un équipement administré par la TOE (usurpation d'un client, contournement de règles de filtrage…).

- M3.ACCES ILLICITE A LA TOE

Un attaquant parvient à accéder de manière illicite à la plateforme **PROVE IT** et/ou modifier illicitement des données sensibles telles que les données d'authentification, pistes d'audit, journaux, etc. (usurpation d'identité d'un administrateur…).

- M4.ABUS DE DROITS UTILISATEUR

Un utilisateur (client) malveillant abuse de ses privilèges pour commettre des actions illicites sur une ressource cible.

- M5.REPUDIATION D'UNE OPERATION

Un utilisateur malveillant nie avoir réalisé une opération sur un équipement contrôlé par la TOE.

3.5. DESCRIPTION DES FONCTIONS DE SECURITE

Par définition, les fonctions de sécurité sont l'ensemble des mesures techniques et mécanismes mis en œuvre dans la TOE pour protéger de façon proportionnée les biens sensibles de la TOE contre les menaces identifiées.

Les fonctions de sécurité essentielles de la TOE sont les suivantes :

- F1.COMMUNICATIONS SECURISEES

Les communications avec **PROVE IT** sont protégées en confidentialité et en intégrité (TLS pour l'encapsulation des flux RDP et l'accès à l'interface d'administration).

- F2.AUTHENTIFICATION

Un mécanisme d'authentification est mis en place pour :

- accéder à l'interface d'administration de la TOE ;
- accéder aux équipements contrôlés par la TOE.

La solution dispose d'un annuaire LDAP intégré. L'usage d'un serveur LDAP externe ne sera pas considéré pour la présente évaluation.

- F3.CONTROLE D'ACCES

Les utilisateurs authentifiés n'ont le droit d'accéder qu'aux ressources cibles RDP pour lesquelles ils ont été explicitement habilités.

En outre, seuls les administrateurs peuvent accéder à la plateforme **PROVE IT** elle-même à travers l'interface web dédiée (accès aux pistes d'audit…).

- F4.TRAÇABILITE

Placée en coupure entre l'utilisateur et une ressource cible, la TOE permet d'enregistrer toutes les opérations réalisées sur des services RDP.

La TOE journalise les opérations sur les équipements administrés en RDP ainsi que sur le serveur **PROVE IT** et garantit l'intégrité des journaux. La confidentialité de ces traces est assurée par un contrôle d'accès réalisé sur la console d'administration Web qui n'autorise que les administrateurs de la solution à y accéder.

3.6. MATRICES DE COUVERTURES

3.6.1. Menaces et biens sensibles

La matrice suivante présente la couverture des menaces sur les biens sensibles (les lettres "**D**", "**I**", "**C**" et "**A**" représentent respectivement les besoins de **D**isponibilité, **I**ntégrité, **C**onfidentialité et **A**uthenticité) :

	Flux utilisateurs	Pistes d'audit	Données utilisateurs	Données ressources cibles	Journaux
Altération des flux utilisateurs	**IC**				
Accès illicite à une ressource administrée			**IC**	**IC**	
Accès illicite à la TOE		**IC**	**IC**	**IC**	**IC**
Abus de droits utilisateur		**IC**			
Répudiation d'une opération		**IC**			

Tableau 2 - Couverture des biens sensibles par les menaces

3.6.2. Menaces et fonctions de sécurité

La matrice suivante présente la couverture des menaces par les fonctions de sécurité :

	Communications sécurisées	Authentification	Contrôle d'accès	Traçabilité
Altération des flux utilisateurs	√			
Accès illicite à une ressource administrée	√	√	√	
Accès illicite à la TOE	√	√	√	

	Communications sécurisées	Authentification	Contrôle d'accès	Traçabilité
Abus de droits utilisateur				√
Répudiation d'une opération				√

Tableau 3 - Couverture des menaces par les fonctions de sécurité

Fin du document