acceis

rubycat

PROVE IT 5.0-12 Standard

Cible de sécurité CSPN

Maîtrise du document

Réf. document	RUB-001-CDS-PROVEIT
Version	1.1
Validé le	13/09/2022
Validé par	Vincent DUCOT

Historique des modifications

Version	Date	Modifications apportées
1.0	01/06/2022	Rédaction initiale du document
1.1	13/09/2022	Mise à jour suite revue ANSSI

Diffusion

Niveau de classification	Liste de diffusion
C2-Document confidentiel	RUBYCAT, ACCEIS, ANSSI

Définition des niveaux de classification utilisés :

- **C0 – Public :** les informations contenues dans ce document peuvent être diffusées sans aucune restriction
- **C1 – Accès limité :** les informations contenues dans ce document ne peuvent être communiquées qu'à des personnels d'ACCEIS ou de ses partenaires.
- **C2 – Document confidentiel :** les informations contenues dans ce document ne peuvent être communiquées qu'à des personnels d'ACCEIS ou des tiers explicitement nommés dans la liste de diffusion.
- **C3 – Document secret :** les informations contenues dans ce document ne peuvent être communiquées qu'aux personnes physiques identifiées dans la liste de diffusion.
- **DR – Diffusion restreinte :** les informations contenues dans ce document bénéficient des mesures de sécurité spécifiques en lien avec la réglementation en vigueur et les politiques de sécurité dédiées d'ACCEIS.

Sommaire

1. Introduction

Ce document décrit la cible de sécurité du produit PROVE IT version 5.0-12 édition Standard, dans le cadre de l'évaluation selon le schéma Certification de Sécurité de Premier Niveau (CSPN) promu par l'ANSSI.

Identification du produit	
Nom de l'éditeur	**Rubycat** 1137 A Av. des Champs Blancs 35510 Cesson-Sévigné
Lien vers l'organisation	https://www.rubycat.eu/
Nom commercial du produit	PROVE IT édition Standard
N° de la version analysée	5.0-12 (5.0 LTS)
Catégorie du produit	Identification, authentification et contrôle d'accès

Documents de références	
CSPN	Certification de sécurité de premier niveau des produits des technologies de l'information, référence ANSSI-CSPN-CER-P-01, version en vigueur.
ST-2018	Cible de sécurité CSPN PROVE IT version 4.0-4, référence CSPN-ST-PROVE IT-1.01-version-publique, version 1.01 https://www.ssi.gouv.fr/uploads/2019/01/anssi-cible-cspn-2018_24fr.pdf

2. Description du produit

2.1. Description générale

PROVE IT est une solution logicielle de PAM[1]/Bastion 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 solution 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 coffre-fort d'identités intégré qui renforce la sécurité des accès effectués par les comptes à privilèges grâce à la non-divulgation des identifiants des comptes sensibles.

La solution se décline en trois gammes :

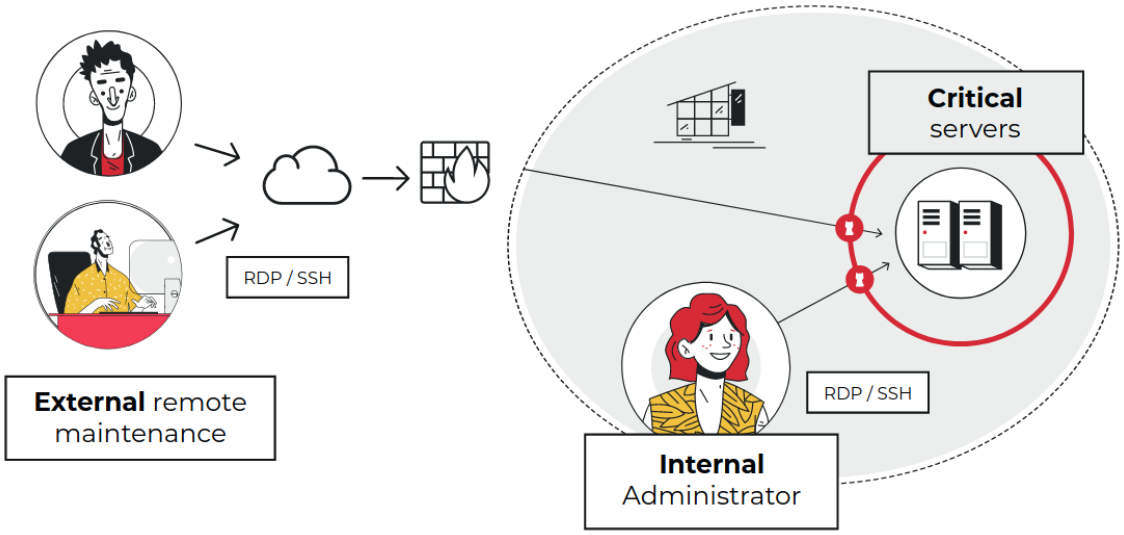
- L'édition *Standard* inclut les fonctionnalités principales de la solution PROVE IT ;
- L'édition *Advanced* permet de segmenter des droits d'administration par profil (auditeur, opérateur, administrateur). Il est ainsi possible de définir une délégation d'administration par population utilisatrice ainsi que par serveurs cibles. Cette gamme dispose d'une API REST pour les opérations d'administration les plus courantes tels que le provisioning automatique des serveurs cibles, etc.
- L'édition Advanced Cluster permet la gestion d'une volumétrie de sessions simultanées plus importante et assurant une haute disponibilité.

Seul le mode RDP de PROVE IT en édition Standard entre dans le cadre de l'évaluation CSPN. Le mode SSH, et les fonctionnalités supplémentaires offertes par les gammes avancées sont considérés hors périmètre.

[1] Privileged Access Management

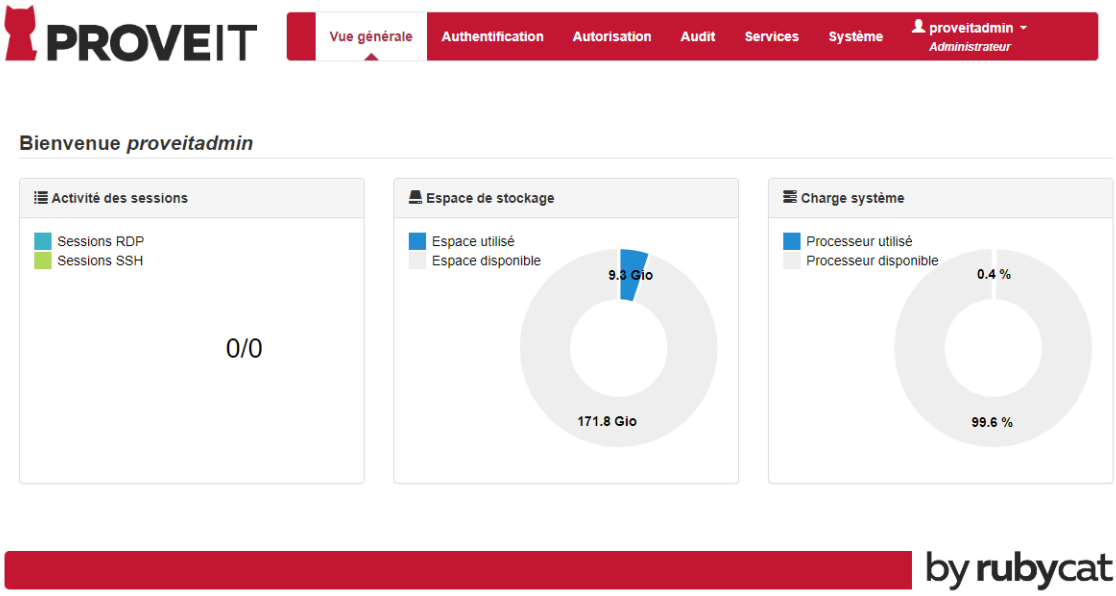
2.2. Description fonctionnelle

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.

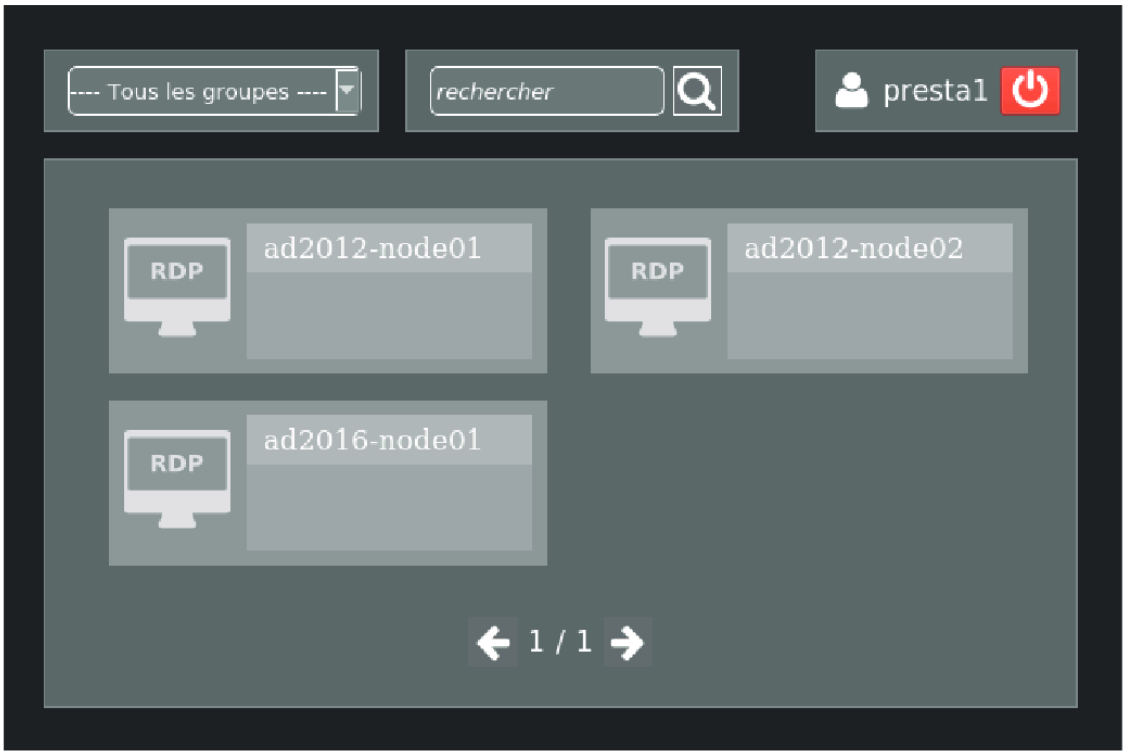


La solution comprend une interface web mettant à disposition des administrateurs un tableau de bord avec une vue générale sur les accès sensibles et des indicateurs tels que :

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



Du côté utilisateur « à privilèges », la connexion est transparente. En effet, l'utilisateur se connecte au portail PROVE IT en utilisant son client natif (RDP ou SSH) et s'authentifie. Un kiosque personnalisé lui propose les serveurs autorisés pour son profil. Après sélection d'un serveur, il est averti de l'enregistrement de sa session, il peut alors accepter ou refuser la connexion à la ressource autorisée. La connexion s'effectue alors de manière transparente sur le serveur cible.



2.3. Architecture

PROVE IT s'articule autour de différents modules :

- **Gestion Accès SSH utilisateurs**

  Ce module (désactivable) est chargé de gérer les accès SSH utilisateur et notamment d'appliquer un contrôle d'accès sur les serveurs SSH contrôlés par la plateforme PROVE IT. Les sous-modules intégrés sont :

  - Contrôle d'accès
  - Traçabilité
  - Filtrage

  Ce module est désactivable et ne fait pas partie du périmètre de l'évaluation.

- **Gestion Accès RDP utilisateurs**

  Ce module est chargé de gérer les accès RDP utilisateur et notamment d'appliquer un contrôle d'accès sur les serveurs RDP publiés par la plateforme PROVE IT. Les sous-modules intégrés sont :

  - Contrôle d'accès
  - Traçabilité
  - Filtrage

  Le sous-module Filtrage est considéré comme un mécanisme métier.

- **Administration et audit**

  Ce module permet d'administrer la plateforme PROVE IT pour les opérations les plus courantes via une interface web (création des politiques d'habilitation, définition des serveurs accessibles, interfaçage avec un serveur d'authentification). Il permet aussi d'accéder à l'ensemble des traces d'audit associées aux accès réalisés par les utilisateurs de la plateforme sur les services RDP.

- **Accès API REST d'administration**

  Ce module (désactivé par défaut à l'installation) met à disposition une API REST permettant d'administrer la plateforme PROVE IT via des requêtes HTTP. Cette API permet de d'effectuer les opérations courantes d'administration réalisables par ailleurs via l'interface web. L'accès se fait via le protocole HTTPS sur un port spécifique (14443) en utilisant des comptes préalablement autorisés.

  Ce module, désactivé par défaut, ne fait pas partie du périmètre de l'évaluation.

- **Accès administration maintenance**

  Ce module (désactivable) permet d'effectuer un accès de maintenance sur la plateforme PROVE IT et notamment d'accéder au système d'exploitation sous-jacent. L'accès se fait via le protocole SSH (sur le port 48991).

  Ce module est désactivable et ne fait pas partie du périmètre de l'évaluation.

- **Gestion identités secondaires (SIMM)**

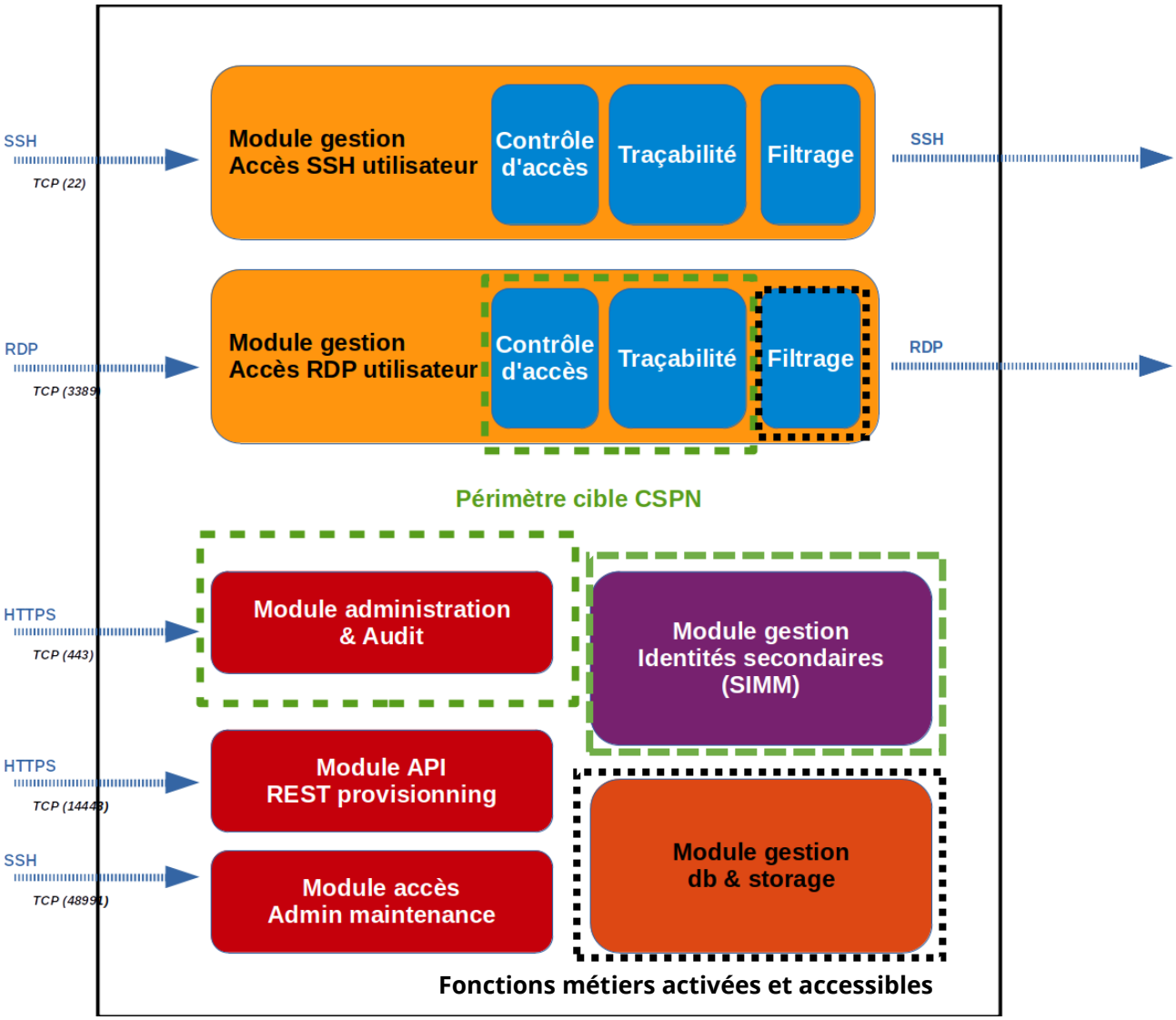
  Ce module permet de provisionner les identifiants des comptes sensibles dans une base sécurisée pour utilisation ultérieure lors des accès. Les identifiants sont stockés sous forme chiffrée en base avec

les paramètres cryptographiques suivants : SHA-512, Scrypt et Chacha20-Poly1305.

- **Gestion DB et storage**

  Ce module gère les accès aux bases de données contenant la configuration de la plateforme et les traces d'audit. Il permet également de gérer l'espace de stockage pour les enregistrements associés aux accès.

  Ce module est une fonctionnalité métier transverse.



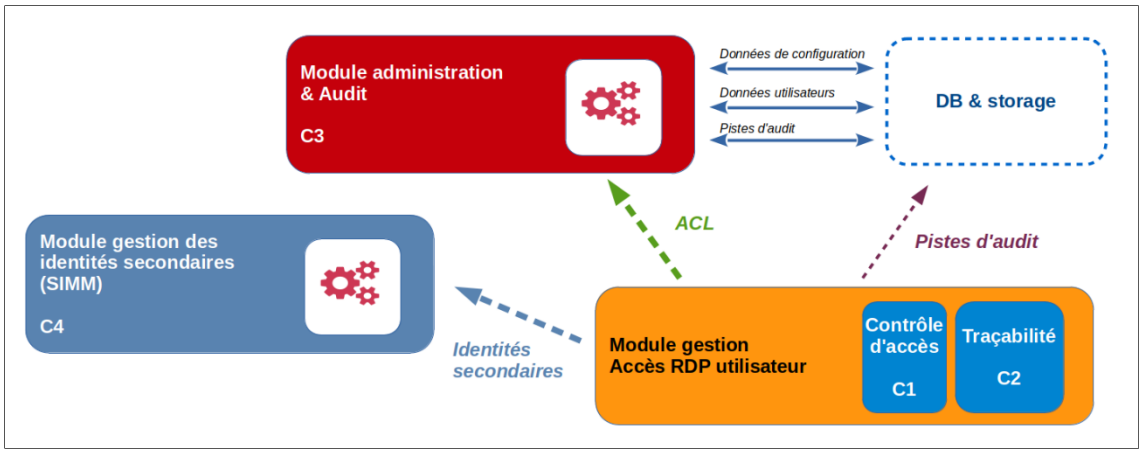
La figure ci-dessus présente l'architecture logicielle de la solution PROVE IT. Les modules inclus dans le périmètre d'évaluation sont encadrés en [vert pointillé] (Périmètre cible CSPN). Les fonctions métiers activées et accessibles

par un adversaire sont encadrées en [noir pointillé] (Analyse efficacité uniquement).

Pour résumer, les modules évalués en conformité et efficacité seront :

- Sous-module de contrôle d'accès RDP utilisateur (C1) ;
- Sous-module de traçabilité d'accès RDP utilisateur (C2) ;
- Module d'administration et d'audit (C3) ;
- Module gestion des identités secondaires (C4).

La figure ci-dessous illustre les interactions entre les modules de la TOE :



2.4. Description de l'environnement prévu pour son utilisation

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 18.04 LTS.

2.5. Description des dépendances

Outre les hyperviseurs et système d'exploitation mentionnés précédemment, aucune autre dépendance externe à des matériels, logiciels et/ou microgrammes du système n'est requise.

2.6. Description de l'environnement technique de fonctionnement

2.6.1. 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.

Les prérequis pour la machine virtuelle PROVE IT sont :

- Nombres de CPUs : 4
- RAM : 3 Go
- Espace disque (OS) : 200 Go
- Carte réseau : 1x Gb/s

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 10 (10.0.15063) ;
  - XFREERDP (≥ 2.1.1) – Linux ;
- Serveurs RDP :
  - Windows Server 2008 R2 ;
  - Windows Server 2012 ;
  - Windows Server 2016 ;
  - Windows Server 2019.

2.6.2. Système d'exploitation retenu

Pour l'évaluation, le produit PROVE IT (image ISO) sera installé au sein d'un environnement QEMU/KVM. Le système d'exploitation sous-jacent est Ubuntu 18.04 LTS (64 bits).

Les ressources cibles seront hébergées sur des postes Windows Server 2019 (RDP). Les postes utilisateurs seront des postes Windows 10 sur lesquels le client RDP sera installé.

3. Périmètre de l'évaluation

L'évaluation porte principalement sur :

- Les modules de contrôle d'accès et de traçabilité des flux utilisateurs sur le protocole RDP ;
- Le module d'administration web ;
- Le module de gestion des identités secondaires.

Seront également analysés au titre de l'efficacité :

- Le module de filtrage sur le protocole RDP ;
- Le module « Gestion DB & Storage » de la solution PROVE IT.

Sont considérés hors périmètre :

- Les systèmes d'exploitation et logiciels RDP des ressources cibles et postes utilisateurs ;
- Les fonctionnalités désactivées par défaut ou désactivables :
    - Le module « Accès Admin maintenance » de la solution PROVE IT ;
    - Les modules de contrôle d'accès, de traçabilité et de filtrage des flux utilisateurs sur le protocole SSH ;
    - Les fonctionnalités d'administration avancée (API REST).

4. Utilisateurs typiques du produit

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 de PROVE IT édition Standard :

- 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.

5. Hypothèses 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 :

1. Administrateurs

Les administrateurs sont compétents, formés pour l'utilisation et l'administration de la TOE, et non hostiles. Ils suivent les guides de la solution et respectent les bonnes pratiques de sécurité, notamment en ce qui concerne la définition des mots de passe.

2. Intégration SI

La solution sera déployée sur une plateforme virtuelle positionnée sur un réseau interne IPv4 (nommé « LAN ») qui est isolé des réseaux extérieurs par un équipement de type pare-feu. En outre, la solution est configurée pour permettre l'administration depuis une interface réseau dédiée, distincte donc de l'interface des accès utilisateurs.

PROVE IT doit être le seul point d'entrée pour les utilisateurs à privilèges, 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 est considéré comme sécurisé et de confiance.

3. Accès 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.

6. 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, confidentialité et authenticité.

Les biens à protéger sont les suivants :

1. 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.

2. 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.

3. Données 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.

4. Données 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.

5. 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	Authenticité
Flux utilisateurs		X	X	
Pistes d'audit		X	X	
Données utilisateurs		X	X	
Données ressources cibles		X	X	
Journaux		X	X	

7. 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 :

1. Altération des flux utilisateurs

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

2. Accès illicite à une ressource administrée

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

3. Accès illicite à 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…).

4. Abus de droits utilisateur

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

5. Répudiation d'une opération

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

La correspondance entre les menaces et les biens sensibles impactés par ces dernières en termes de confidentialité (C), d'intégrité (I), de disponibilité (D) et d'authenticité (A) est représentée par la matrice ci-dessous :

	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 utilisateurs		IC			
Répudiation d'une opération		IC			

8. Fonctions de sécurité

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 :

1. Communications sécurisées

Les communications avec PROVE IT sont protégées en confidentialité et en intégrité.

2. 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.

3. Authentification unique

Les utilisateurs des équipements contrôlés n'ont plus besoin de présenter des secrets d'authentification sur chacun des équipements. Ils s'authentifient uniquement auprès de PROVE IT, qui après s'être assuré que les accès sont autorisés, ouvre l'accès aux équipements autorisés.

3. Contrôle d'accès

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…).

4. Traçabilité

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.

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

	Communications sécurisées	Authentification	Authentification unique	Contrôle d' accès	Traçabilité
Altération des flux utilisateurs	X				
Accès illicite à une ressource administrée	X	X	X	X	
Accès illicite à la TOE	X	X	X	X	
Abus de droits utilisateurs					X
Répudiation d'une opération					X