Cible de sécurité CSPN - Bastion 6.0.102

Document : Cible de sécurité CSPN - WALLIX Bastion 6.0

Version : 3.2

Référence : CSPN-Bastion-6.0

Date : 2019-01-30

Révisions

VERSION	DATE	DESCRIPTION	REDACTEURS
0.1	2013-03-05	Version initiale pour Bastion 3.1.9	EFA
0.2	2013-03-28	Prise en compte des commentaires Oppida	EFA
1.0	2013-04-05	Ajout de précisions sur les interfaces Ethernet	EFA
1.1	2013-04-23	Précisions sur les domaines réseau et les utilisateurs	EFA
2.0	2015-02-13	Mise à jour pour la version 5.0.1 : • Proxy HTTPS sorti de la cible • Ajout du port HA & Domaine d'administration	SDD
2.1	2015-04-10	Prise en compte des retours de l'ANSSI	SDD
2.2	2015-06-24	Prise en compte des commentaires ST Bastion ANSSI v2	SDD
2.3	2016-06-14	Description des procédés d'authentification primaire et des protocoles de changement de mot de passe	SDD
2.4	2016-06-23	Ajout de la version du protocole Kerberos et du mode d'authentification sur la console le port SSH 2242.	SDD
2.5	2016-06-24	SSH sur port 2242 permet l'authentification par clé SSH.	SDD
2.6	2017-02-15	Modifications demandées par le CESTI : • UTILISATEURS TYPIQUES DU PRODUIT : Description du croisement par port réseau • HYPOTHESES SUR L'ENVIRONNEMENT : Suppression de l'hypothèse sur l'accès physique.	SSD

WALLIX
TRACE. AUDIT & TRUST

3.0	2018-07-06	Modification du Bastion cible (v6.0.100)	CMU
3.1	2018-11-02	Modification suite à analyse CESTI	CMU
3.2	2019-01-10	Suppression de l'administrateur malveillant Réorganisation des Fonctions de sécurité Ajout du SIEM externe comme entrepôt de log	CMU

Contents

1 IDENTIFICATION DU PRODUIT

Organisation éditrice	WALLIX
Lien vers l'organisation	http://www.wallix.fr/
Nom commercial du produit	WALLIX Bastion
Numéro de la version évaluée	6.0.102.100
Catégorie de produit	Identification, authentification et contrôle d'accès

2 ARGUMENTAIRE (DESCRIPTION) DU PRODUIT

2.1 DESCRIPTION GENERALE DU PRODUIT

Le principal objectif du WALLIX Bastion (appelé Bastion dans le reste du document) est de jouer le rôle de passerelle d'administration entre un domaine Utilisateurs potentiellement hostile et un domaine protégé Ressources, comme le montre la Figure 1.

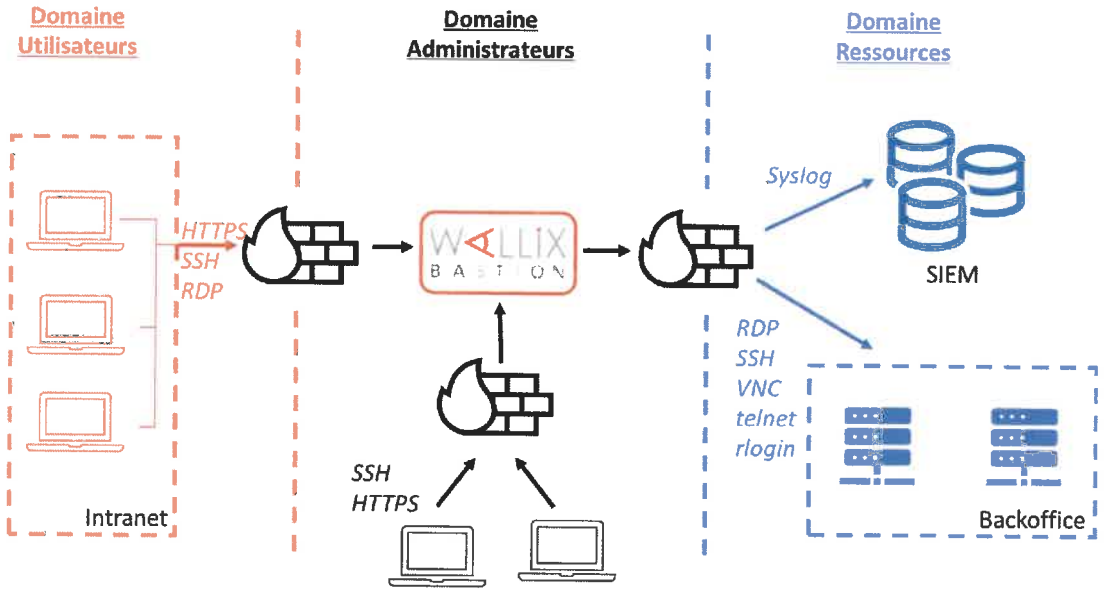

Figure 1. Environnement du Bastion

Du côté du domaine Utilisateurs, les protocoles supportés pour l'accès aux ressources sont les suivants :

- SSH v2 (remote command, remote shell, SFTP, SCP),
- RDP en TLS.

Du côté du domaine Ressources, les protocoles supportés sont les suivants :

- SSH (remote command, remote shell, SFTP, SCP),
- RDP, VNC,
- Telnet,
- Rlogin,
- Microsoft RPC[1] (UserInfo) pour changer les mots de passe des systèmes Windows.

[1] https://msdn.microsoft.com/en-us/library/cc243560.aspx

Les protocoles HTTPS et SSH sont également utilisés pour l'administration du produit depuis le domaine d'Administration. Ce domaine est géré selon les pratiques de la « Note technique - Recommandations relatives à l'administration sécurisée des systèmes d'information »[2].

Le protocole HTTPS est également disponible pour interroger l'API REST du Bastion, à partir des différents domaines.

Le lien de haute-disponibilité (High-Availability ou HA en anglais) permet de faire travailler deux Bastions en mode actif/passif. Si le Bastion actif n'est plus disponible, le deuxième Bastion passe alors en mode actif.

2.2 UTILISATION DU PRODUIT

Le Bastion possède quatre ports Ethernet. La configuration recommandée est la suivante :

- Port Ethernet 0 : Port dédié à l'administration du Bastion (Domaine d'administration), aussi nommé « Port Ethernet d'Administration »
- Port Ethernet 1 : Port dédié à la HA, aussi nommé « Port Ethernet HA »
- Port Ethernet 2 : Port dédié à la connexion des utilisateurs et des auditeurs (Domaine Utilisateurs), aussi nommé « Port Ethernet Utilisateurs »
- Port Ethernet 3 : Port dédié à l'accès aux ressources (Domaine Ressources), aussi nommé « Port Ethernet Ressources ».

Le Bastion s'administre grâce à une interface WEB qui est accessible en HTTPS sur le port TCP 443 du port Ethernet d'administration. Pour certaines actions, le Bastion peut s'administrer via le shell accessible depuis la console locale de l'équipement ou en SSH v2 sur le port TCP 2242 du Port Ethernet d'Administration. La console locale est accessible par un port d'affichage VGA et un port clavier USB, ainsi que par l'iDrac[3]. Les administrateurs du Bastion ne peuvent s'identifier sur la console que par mot de passe. Ils peuvent cependant s'authentifier sur le port TCP 2242 au moyen d'une clé SSH en plus d'un mot de passe.

Les utilisateurs se connectent aux ressources via des composants Bastion appelés proxys. Il existe un proxy pour chaque protocole supporté : RDP et SSH. L'utilisation des proxys se fait en utilisant les clients standards SSH et RDP respectivement sur les ports 22, et 3389 du Port Ethernet Utilisateurs.

---

[2] DAT-NT-22/ANSSI/SDE/NP du 20 février 2015 dans la cible de sécurité, http://www.ssi.gouv.fr/guide/securiserladministration-des-systemes-dinformation/

[3] L'iDrac est un composant des serveurs DELL qui permet une gestion et une surveillance d'un serveur grâce aux fonctionnalités suivantes :

- Aide au diagnostic : capture automatique de l'écran et des logs à la détection du crash
- Gestion de l'alimentation : Extinction, allumage et redémarrage du serveur à distance
- KVM sur IP dédié déport complet à distance de l'écran / clavier / souris du serveur
- Possibilité de monter des images ISO à distance

2.3 ENVIRONNEMENT D'UTILISATION

Le Bastion est prévu pour fonctionner en appliance matérielle. Il est livré installé sur des serveurs Dell R340, R440 ou R640 avec carte de supervision à distance iDrac et alimentation redondante.

Le Bastion peut être déployé selon l'un de ces deux modes de fonctionnement :

1. Standalone : le système tourne sur un seul Bastion;
2. HA : le système est composé de deux Bastions en mode actif-passif. Les Ports Ethernet HA de chaque machine doivent être reliés avec un câble physique.

2.4 DEPENDANCES DU PRODUIT

Aucune dépendance externe à des matériels, logiciels et/ou des microprogrammes du système n'est requise pour la version matérielle.

2.5 UTILISATEURS TYPIQUES DU PRODUIT

Il y a cinq rôles possibles sur l'interface utilisateur du Bastion :

1. Utilisateurs,
2. Auditeurs,
3. Administrateurs applicatif Bastion,
4. Administrateurs système Bastion,
5. Super administrateur du Bastion.

Le Bastion est accessible au travers de différents ports réseaux. Les fonctionnalités d'un rôle sont restreintes par port. Par exemple, les fonctionnalités nécessaires aux rôles Administrateurs applicatif et Administrateurs système Bastion ne sont disponibles qu'au travers du *Port Ethernet Administrateurs*. Il y a donc un cloisonnement des rôles par port réseau.

Les personnes accédant au Bastion depuis le domaine Utilisateurs peuvent endosser les rôles décrits ci-dessous. Ils interagissent avec le Bastion uniquement au travers du *Port Ethernet Utilisateurs* et accèdent aux ressources uniquement au travers du *Port Ethernet Ressources*. Ces personnes doivent être connues de l'entreprise soit par un contrat de travail soit par un contrat de prestation par exemple. Leurs rôles sont :

- Les Utilisateurs sont des personnes utilisant les ressources du système d'information sous le contrôle du Bastion. Ces personnes peuvent être en charge de l'administration de ces ressources mais ne disposent pas des droits d'administration sur le Bastion.
  Un utilisateur doit s'authentifier auprès du Bastion pour accéder aux services suivants offerts par le Bastion :
  - Se connecter à une ressource cible,
  - Changer ses secrets d'authentification sur le Bastion.
- Les Auditeurs du Bastion peuvent consulter les informations suivantes :
  - Historiques des connexions,
  - Enregistrements des sessions,

- L'historique des comptes,
- L'historique des approbations,
- L'historique des authentifications primaires,
- Les statistiques sur les connexions.

Les personnes accédant au Bastion depuis le domaine d'Administration peuvent endosser les rôles décrits ci-dessous. Ils interagissent avec le Bastion uniquement au travers du *Port Ethernet d'Administration*. Ces personnes sont, le plus souvent, des employés de l'entreprise et appartiennent à une des équipes dédiées à la sécurité des systèmes d'information :

- Les Administrateurs applicatif Bastion sont les personnes en charge de l'administration de l'application Bastion. Ils réalisent les opérations d'administration suivantes :
  - Gérer les comptes utilisateurs et les moyens d'authentification,
  - Définir la politique de sécurité sur les comptes utilisateurs,
  - Définir la politique de changement des mots de passe des comptes des ressources cibles,
  - Gérer les ressources cibles,
  - Gérer les habilitations (i.e. les droits d'accès des utilisateurs aux services offerts par le Bastion),
- Un Administrateur système Bastion est une personne en charge de l'administration système du Bastion, que ce soit au travers de la GUI ou de l'accès à la console SSH d'administration .
- Le Super Administrateur du Bastion est un Administrateur système Bastion en possession du Mot de passe maître pour déverrouiller la clé de chiffrement au démarrage du système.

2.6 HYPOTHESES SUR L'ENVIRONNEMENT

2.6.1 Utilisateurs

- Le Super Administrateur est compétent, formé et non hostile,
- Les Administrateurs Système Bastion sont compétents, formés et non hostiles,
- Les administrateurs applicatif sont compétents, formés et non hostiles,
- Les utilisateurs du Bastion sont potentiellement malveillants
- Les personnes ayant un accès physique au Bastion en production (en fonctionnement) et/ou lors de son installation sont bienveillants.
- Les personnes ayant un accès physique au Bastion hors production (stockage, transport, ...) sont malveillantes.

2.6.2 Postes utilisateurs et serveurs cibles

- Les postes des utilisateurs sont durcis, mis à jour régulièrement, et leur accès physique est protégé.
- Les postes des Utilisateurs possèdent les certificats ou les clés publiques permettant d'authentifier le Bastion.
- Les postes des Administrateurs possèdent les certificats ou les clés publiques permettant d'authentifier le Bastion.

2.6.3 Cloisonnement réseau

- Le Bastion doit être protégé par des pare-feu du domaine Utilisateurs, du domaine d'Administration et de la partie du domaine Ressources accessibles depuis Internet. Seuls les flux autorisés doivent être ouverts (cf. matrice de flux - Tableau 1 page 9),
- En mode HA, le Bastion actif et le Bastion passif sont reliés directement par un câble physique Ethernet via leur Ports Ethernet HA. En aucun cas, les données échangées entre les Bastion actif et passif via leurs Ports Ethernet HA ne transitent au travers des réseaux.

2.6.3.1 Domaine Utilisateurs

- Le Bastion est accessible par le Port Ethernet Utilisateurs depuis le réseau du domaine Utilisateurs.
- Le domaine Utilisateurs est une zone interne du système d'information comme un intranet par exemple. Il ne doit en aucun cas être accessible, directement ou indirectement, depuis Internet.

2.6.3.2 Domaine Ressources

- Le réseau du domaine Ressources est accessible depuis le Bastion à partir du Port Ethernet Ressource.
- L'accès à distance aux équipements du domaine Ressources directement depuis le domaine Utilisateurs est restreint de manière à obliger le passage par le Bastion.
- On considère également que l'accès au domaine Ressources depuis un autre domaine est impossible.

2.6.3.3 Domaine Administration

- Le Bastion est accessible par le Port Ethernet d'Administration depuis le réseau du domaine d'Administration.
- Le domaine d'Administration est un réseau composé de systèmes dédiées à l'administration (non bureautique) connectés par un réseau physiquement dédié à l'administration ou cloisonné par des moyens de filtrages, de chiffrement et d'authentification de réseau, et d'authentification au réseau. Ce réseau n'a pas d'accès à Internet.

Tableau 1 - Matrice des flux ouvert

		Destination			
		Bastion	Domaine Utilisateur	Domaine Administrateur	Domaine Ressource
Source	Bastion			AD (636) DNS (53) NTP (123) Syslog (514)	SSH (22) RDP (3389)
	Domaine Utilisateur	SSH (22) RDP (3389) HTTPS (443)			
	Domaine Administrateur	SSH (2242) HTTPS (443)			
	Domaine Ressource				

2.6.4 Stockage - Sauvegarde

- Toutes les traces vidéo générées par le Bastion sont stockées sur le produit, pas de stockage externe actif.
- Tous les journaux générés par le Bastion sont envoyés à un SIEM.
- Les données de configuration du Bastion, une fois chiffrées et exportées, sont stockées à l'aide d'une solution agréée au niveau adéquat.
- Le Bastion peut être volé (stockage, maintenance, transport).

2.7 PERIMETRE DE L'EVALUATION

Le périmètre d'évaluation inclut :

- Le logiciel Bastion
- La plateforme matérielle Dell

Le périmètre d'évaluation couvre les fonctionnalités suivantes du Bastion :

- La fonction d'enregistrement des actions des Utilisateurs,
- La fonction d'enregistrement des actions des Auditeurs,
- La fonction d'enregistrement des actions des Administrateurs applicatif Bastion,
- Confidentialité et en intégrité des traces stockées sur le Bastion par les utilisateurs (vidéo de session)
- Intégrité des journaux envoyés au SIEM, concernant les traces des utilisateurs, des auditeurs et des Administrateurs applicatif Bastion,
- Accès aux interfaces d'administration applicative (HTTPS port TCP 443),
- Accès aux proxys (SSH v2 port TCP 22, RDP TLS port TCP 3389),
- Accès aux interfaces utilisateurs du Bastion (HTTPS port TCP 443),
- L'authentification via Active Directory des utilisateurs et administrateurs sur le bastion,
- L'authentification secondaire avec des comptes locaux, sur les cibles via SSH v2 et RDP TLS,
- Les fonctions de création de compte à scénario,
- L'utilisation de comptes à scénario,
- Changement des mots de passe des ressources cibles,
- La protection en confidentialité et en intégrité des données stockées sur le Bastion,
- Le vol de bastion

Le périmètre d'évaluation ne couvre pas :

- Les accès administrateurs et super administrateur du Bastion (SSH v2 port TCP 2242),
- Les accès administrateurs système de l'interface web (profil « *WAB_administrator* »)
- Les accès administrateurs applicatif de l'interface web (profil « *operation_administrator* »)
- Les authentifications primaires ne reposant pas sur Active Directory (ex : comptes locaux, clé SSH, ...),
- Les accès sur les cibles ne reposant pas sur SSH v2 ou RDP (protocoles VNC, Telnet et RLogin),
- Les authentifications secondaires ne reposant pas sur des comptes locaux (ex : comptes interactif, account mapping ...),
- L'interface d'API REST exposée par le Bastion,

- Le mode HA du Bastion,
- Le remplacement d'un Bastion par un serveur frauduleux.

3 ENVIRONNEMENT TECHNIQUE DANS LEQUEL LE BASTION DOIT FONCTIONNER

3.1 ENVIRONNEMENT STANDARD

Le Bastion s'intègre dans un réseau IPv4 et ne nécessite aucune modification sur les postes clients ou sur les équipements à protéger. Les clients standards pour accéder aux équipements du domaine Ressources restent identiques à ceux utilisés avant la mise en place du Bastion :

- Clients SSH : OpenSSH, PuTTY. Il est également possible d'utiliser BastionPutty (version modifiée de PuTTY pour prendre la cible en paramètre sur la ligne de commande),
- Clients RDP : mstsc (Microsoft Remote Desktop Client).

3.2 CONDITIONS D'EVALUATION

La configuration retenue pour l'évaluation est une configuration matérielle en mode standalone.

Dans cette configuration, les ports Utilisateurs et Administrateur sont mutualisés physiquement, chaque réseau est cloisonné par un VLAN distinct, sans routage inter-VLAN. La configuration réseau est la suivante :

- Port Ethernet 0 :
  - VLAN 100 : Port dédié à l'administration du Bastion (Domaine d'administration), aussi nommé « Port Ethernet d'Administration ».
  - VLAN natif : Port dédié à la connexion des utilisateurs et des auditeurs (Domaine Utilisateurs), aussi nommé « Port Ethernet Utilisateurs ».
- Port Ethernet 1 : Port dédié à la HA, aussi nommé « Port Ethernet HA ». Non utilisé
- Port Ethernet 2 : Port dédié à l'accès aux ressources (Domaine Ressources), aussi nommé « Port Ethernet Ressources ».

Les utilisateurs s'identifient auprès du Bastion grâce à un mot de passe, validé auprès d'un Active Directory.

Les données d'authentification auprès des cibles sont stockées dans le coffre interne du Bastion.

Les journaux d'activités générés par le Bastion sont envoyés à un SIEM externe (guide d'administration, « paragraphe Intégration SIEM »). Le SIEM est considéré comme la source intègre pour récupérer les journaux.

Une configuration spécifique est appliquée dans le cadre de cette évaluation :

- Un mot de passe maître de chiffrement est défini, la clé Apache est protégée (Guide d'installation – Security Level).
- Le chiffrement des traces est activé (Guide d'Administration, paragraphe « options des enregistrements de sessions »).
- L'enregistrement des touches claviers SSH est activé (Guide d'Administration, paragraphe « Configuration du log de toutes les entrées clavier pour les protocoles RLOGIN, SSH et TELNET»)

- Le chiffrement est configuré pour utiliser uniquement les algorithmes compatibles avec le Référentiel Général de Sécurité (RGS)[4] . Les paramètres suivants sont définis :
  - RDP : HIGH:!ADH:!3DES:!SHA (Guide d'Administration, paragraphe « Configurer le niveau de sécurité pour permettre la compatibilité du protocole RDP »)
  - Proxy SSH : (Guide d'Administration, paragraphe « Configurer le niveau de sécurité pour permettre la compatibilité du protocole SSH »)
    - Hostkeys : rsa,ecdsa
    - Client kex algos : ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha256
    - Client cipher algos : aes256-ctr, aes192-ctr, aes128-ctr
    - Client integrity algos : hmac-sha2-256, hmac-sha2-512

[4] Le Référentiel Général de Sécurité définit un ensemble de règles de sécurité qui s'imposent aux autorités administratives dans la sécurisation de leurs systèmes d'information. Il propose également des bonnes pratiques en matière de sécurité des systèmes d'information que les autorités administratives sont libres d'appliquer (http://www.ssi.gouv.fr/administration/reglementation/administration-electronique/le-referentiel-general-de-securitergs/)

4 BIENS SENSIBLES QUE LE BASTION DOIT PROTEGER

En supplément des services offerts par le Bastion qui doivent être disponibles et intègres, le Bastion doit protéger les données suivantes :

4.1 DONNEES UTILISATEURS

4.1.1 B1. Flux Utilisateurs

Les flux transitant par le Bastion doivent être protégés en Disponibilité, Intégrité et Confidentialité. Le Bastion ne doit pas altérer de manière illicite (c.à.d. autre que ses fonctions nominales de proxy) ces flux et ne doit pas permettre à une personne non explicitement autorisée de les consulter.

4.1.2 B2. Flux Administrateurs

Les flux d'administration transitant par le Bastion doivent être protégés en Intégrité et Confidentialité. Il ne doit pas être possible pour une personne malveillante de modifier ou consulter ces flux.

4.1.3 B3. Enregistrements

Les enregistrements des flux utilisateurs doivent être protégés en Intégrité et Confidentialité. Le Bastion ne doit pas permettre à une personne de supprimer, modifier ou même consulter des traces s'il n'en a pas explicitement les droits.

La suppression des enregistrements (purge) ne doit pouvoir être effectuée que par un administrateur système du Bastion. Celle-ci doit être journalisée et la modification des enregistrements ne doit pas pouvoir être possible.

4.2 DONNEES INTERNES

4.2.1 B4. Base des utilisateurs

Cette base contient les identifiants et les moyens d'assurer l'authentification des utilisateurs du SI sur le Bastion (généralement un condensat d'un secret d'authentification ou une clé publique). Une personne non explicitement autorisée ne doit pas pouvoir consulter, modifier ou supprimer des données dans cette base. Le condensat du mot de passe ne doit pas pouvoir être accessible à une personne malveillante.

4.2.2 B5. Base de ressources cibles

Cette base contient des informations réseaux sur les ressources cibles (par exemple adresse IP, port destination), les identifiants et les secrets d'authentification des comptes accessibles sur les ressources cibles. Une personne non explicitement autorisée ne doit pas pouvoir modifier, supprimer ou même simplement consulter les données de cette base.

4.2.3 B6. Contrôle d'accès (ACL)

Cette base contient les associations autorisées entre les Utilisateurs et les Ressources cibles. Une personne non explicitement autorisée ne doit pas pouvoir modifier ou supprimer des données dans cette base.

4.2.4 B7. Journaux

Outre générer des traces des flux utilisateurs, le Bastion génère des journaux des opérations effectuées par lui-même. Une personne non explicitement autorisée à le faire ne doit pas pouvoir modifier, supprimer ou même simplement consulter les données de cette base.

4.2.5 B8. Fichiers de configuration sensible

Des services externes peuvent être configurés sur le Bastion (serveur SMTP, serveur LDAP, ...). Les identifiants nécessaires à ces comptes applicatifs, et tout autre fichier contenant des informations sensibles (clés privées, keytab Kerberos) ne doivent être accessibles qu'aux personnes explicitement autorisées.

4.3 DONNEES EXTERNES

4.3.1 B9. Ressources cibles

Le Bastion peut être considéré comme un reverse proxy Applicatif. Il ne doit pas permettre à une personne malveillante de porter atteinte en confidentialité, disponibilité ou intégrité vis-à-vis des ressources protégées.

5 DESCRIPTION DES MENACES

5.1 AGENTS DE MENACE

Les agents de menace considérés pour l'évaluation sont :

- Les personnes malveillantes ayant un accès logique ou physique à des équipements du domaine Utilisateurs hormis les postes de travail des Utilisateurs : ci-après les « **attaquants utilisateurs externes** » ;
- Les Utilisateurs et Auditeurs du Bastion malveillants : ci-après les « **attaquants utilisateurs internes** ». Il est rappelé que ceux-ci sont localisés également dans le domaine Utilisateurs ; tout attaquant interne peut aussi être considéré comme attaquant externe ;
- Les personnes malveillantes ayant un accès logique ou physique à des équipements du domaine d'Administration hormis les postes de travail des Administrateurs : ci-après les « **attaquants administrateurs externes** »
- Les personnes malveillantes ayant un accès logique ou physique à des équipements du domaine Ressources : ci-après les « **attaquants à privilèges** » ;
- Les personnes malveillantes ayant un accès physique à des équipements Bastion : ci-après les « **dérobeurs** ».

5.2 LISTE DES MENACES RETENUES

5.2.1 Menaces sur les flux Utilisateurs

5.2.1.1 M1. Écoute des flux Utilisateurs

Un attaquant utilisateur externe écoute les flux utilisateurs sur le domaine Utilisateurs pour compromettre la Confidentialité des données transmises.

5.2.1.2 M2. Altération des flux Utilisateurs

Un attaquant utilisateur externe intercepte et modifie les flux utilisateurs sur le domaine Utilisateurs. Menaces liées aux opérations réalisées par les Utilisateurs.

5.2.1.3 M3. Abus des droits Utilisateurs

Un attaquant utilisateur interne abuse de ses privilèges pour commettre une action illicite sur une ressource cible.

5.2.1.4 M4. Répudiation des actions Utilisateurs

Un attaquant utilisateur interne nie avoir réalisé une opération (ou a contrario certifie avoir réalisé une opération).

5.2.1.5 M5. Elévation de privilèges Utilisateurs

Un attaquant utilisateur interne utilise une vulnérabilité présente sur l'interface WEB pour accéder à des ressources ou données auxquelles il n'aurait pas accès, ou pour disposer d'un accès administrateur applicatif ou système.

5.2.2 Menaces sur les flux Administrateurs

5.2.2.1 M6. Écoute des flux Administrateur

Un attaquant administrateur externe écoute les flux administrateurs sur le domaine d'Administration pour compromettre la Confidentialité des données transmises.

5.2.2.2 *M7. Altération des flux Administrateur*

Un attaquant administrateur externe intercepte et modifie les flux utilisateurs sur le domaine d'Administration.

5.2.3 Menaces sur le Bastion

5.2.3.1 *M8. Usurpation d'identité Utilisateurs*

Un attaquant utilisateur externe tente d'usurper l'identité d'un utilisateur légitime pour utiliser ses privilèges (accès aux ressources cibles).

5.2.3.2 *M9. Usurpation d'identité Administrateurs Applicatif*

Un attaquant administrateur externe tente d'usurper l'identité d'un administrateur applicatif pour utiliser ses privilèges (accès à l'interface d'administration du Bastion).

5.2.3.3 *M10. Accès illicite par le Port Ethernet Utilisateurs*

Un attaquant utilisateur externe réussit, par une attaque sur le Port Ethernet Utilisateurs, à s'introduire dans le système et à accéder et/ou modifier illicitement les données sensibles stockées dans le Bastion (données d'authentification, traces).

5.2.3.4 *M11. Accès illicite Port Ethernet d'Administration*

Un attaquant administrateur externe réussit, par une attaque sur le Port Ethernet d'Administration, à s'introduire dans le système et à accéder et/ou modifier illicitement les données sensibles stockées dans le Bastion (données d'authentification, traces) ou à élever ses privilèges pour devenir Administrateur système Bastion.

5.2.3.5 *M12. Accès illicite Port Ethernet Ressources*

Un attaquant à privilèges réussit, par une attaque sur le Port Ethernet Ressources, à utiliser le Bastion comme machine de rebond pour accéder à d'autres ressources du domaine Ressources, aux postes des administrateurs du domaine d'Administration, aux postes des utilisateurs du domaine Utilisateurs.

5.2.4 Menaces liées à un attaquant ayant un accès physique au Bastion

5.2.4.1 *M13. Vol d'un Bastion*

Un dérobeur vole un Bastion puis tente de porter atteinte à la confidentialité des biens sensibles à protéger en confidentialité et identifiés au Chapitre 4.

5.2.5 Matrice de couverture des biens sensibles vis-à-vis des menaces

Le tableau ci-dessous décrit l'impact des menaces en Disponibilité (D), Confidentialité (C), Intégrité (I) et Authenticité (A) sur les biens sensibles.

	B1. Flux Utilisateurs	B2. Flux Administrateurs	B3. Enregistrements	B4. Base des utilisateurs	B5. Base des ressources cibles	B6. Contrôle d'accès (ACL)	B7. Journaux	B8. Ressources cible	B9. Fichiers configuration sensible
M1. Écoute des flux utilisateurs	**C**								
M2. Altération des flux utilisateurs	**DIA**							**DCI**	
M3. Abus des droits utilisateurs	**I**							**DCI**	
M4. Répudiation des actions utilisateurs			**IA**				**IA**		
M5. Élévation de privilèges utilisateurs			**CIA**	**I**	**CI**	**I**	**CIA**	**DCI**	**CI**
M6. Écoute des flux administrateurs		**C**							
M7. Altération des flux administrateurs		**DIA**				**I**		**DCI**	
M8. Usurpation d'identité utilisateurs	**I**		**C**		**C**		**IA**	**DCI**	
M9. Usurpation d'identité Administrateur Applicatif		**I**	**CIA**	**CIA**	**CI**	**I**	**IA**	**DCI**	**CI**
M10. Accès illicite par le port Ethernet Utilisateur			**CIA**	**CI**	**CIA**	**I**	**CIA**	**DCI**	**CI**
M11. Accès illicite par le port Ethernet d'Administration			**CIA**	**CI**	**CIA**	**I**	**CIA**		**CI**
M12. Accès illicite par le port Ethernet Ressources			**CIA**	**CI**	**CIA**	**I**	**CIA**		**CI**
M13. Vol d'un Bastion			**C**	**C**	**C**		**C**		**C**

Tableau 2 - Couverture des biens sensibles vis-à-vis des menaces

5.3 POLITIQUE DE SECURITE DE L'ORGANISATION

5.3.1 Authentification des utilisateurs

Les utilisateurs doivent être authentifiés pour pouvoir accéder aux ressources cibles.

5.3.2 Contrôle d'Accès aux ressources cibles

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

5.3.3 Traçabilité

Toutes les opérations sur les ressources cibles doivent être enregistrées.

Toutes les opérations d'administration effectuées sur le bastion doivent être enregistrées et exportées sur un serveur de gestion de log externe.

6 DESCRIPTION DES FONCTIONS DE SECURITE DU BASTION

6.1 F1. Communications sécurisées

Le Bastion permet de mettre en œuvre une protection des communications en Confidentialité et en Intégrité entre les utilisateurs et administrateur et le Bastion, ainsi qu'entre le Bastion et les ressources.

6.2 F2. Authentification et contrôle des accès aux ressources

Le Bastion permet de mettre en œuvre une politique d'accès aux ressources cibles.

6.3 F3. Authentification et contrôle d'accès GUI

Le Bastion permet de mettre en œuvre une politique d'accès à l'interface web, avec une gestion de profils et de rôles (utilisateur, auditeur, administrateur, ...).

6.4 F4. Authentification unique

Les utilisateurs des ressources cibles n'ont plus besoin de présenter des secrets d'authentification sur chacune des ressources cibles. Ils s'authentifient auprès du Bastion, qui après s'être assuré que les accès sont autorisés, ouvre l'accès aux ressources cibles autorisées.

6.5 F5. Traçabilité des connexions aux ressources

Placé en coupure entre l'utilisateur et la ressource cible, le Bastion permet d'enregistrer toutes les opérations réalisées, et ceci pour tous les protocoles supportés.

6.6 F6. Traçabilité des actions GUI

Les actions d'administration et d'audit réalisées dans l'interface web sont tracées. Ces actions peuvent être la création d'un compte, la visualisation d'une session enregistrée, la suppression d'un groupe utilisateur, ...

6.7 F7. Stockage sécurisé

Les données sensibles du Bastion (mot de passe des cibles, traces, ...) sont protégées en Confidentialité et Intégrité.

6.8 F8. Durcissement du Bastion

Seuls les services nécessaires sont installés et configurés. Les bonnes pratiques de développement sécurisés sont respectées, le noyau est durci (patch GRSecurity entre autres).

6.9 F9. Changement automatique de mot de passe

Les types de cibles dans le périmètre de la TOE sont les serveurs Linux et les serveurs Windows. Il est possible de créer des politiques de génération de mots de passe afin de s'adapter aux contraintes des ressources.

Une politique est définie par les paramètres suivants :

- Le nombre de caractères formant le mot de passe (i.e. sa longueur).
- Le nombre de caractères ASCII non alphanumériques qui doivent être présents.
- Le nombre de caractères minuscules qui doivent être présents.
- Le nombre de caractères majuscules qui doivent être présents.
- Le nombre de chiffres qui doivent être présents.
- Une liste de caractères à exclure.

6.10 Matrice de couverture des menaces vis-à-vis des fonctions de sécurité offertes par le Bastion

	F1. Communications sécurisées	F2. Authentification et contrôle accès ressource	F3. Authentification et contrôle d'accès GUI.	F4. Authentification unique	F5. Traçabilité des connexions aux ressources	F6. Traçabilité des actions GUI.	F7. Stockage sécurisé	FF8. Durcissement du Bastion	F9. Changement automatique de mot de passe
M1. Écoute des flux utilisateurs	√								
M2. Altération des flux utilisateurs	√								
M3. Abus des droits utilisateurs					√	√		√	√
M4. Répudiation des actions utilisateurs					√	√		√	√
M5. Élévation de privilèges utilisateurs								√	
M6. Écoute des flux administrateurs	√								
M7. Altération des flux administrateurs	√								
M8. Usurpation d'identité utilisateurs		√	√	√					
M9. Usurpation d'identité Administrateur Applicatif			√						
M10. Accès illicite par le port Ethernet Utilisateur								√	
M11. Accès illicite par le port Ethernet d'Administration								√	
M12. Accès illicite par le port Ethernet Ressources								√	
M13. Vol d'un Bastion							√		

Tableau 3 - Couverture des menaces offertes par le Bastion

7 GLOSSAIRE

- ACL (Access Control List) : Gestion des droits d'accès des utilisateurs aux ressources du Bastion dans l'interface web d'administration, les services WEB et les proxys.
- Administrateurs applicatif Bastion : personnes du domaine d'Administration possédant les droits d'accès et d'administration applicatif dans l'interface web du Bastion. Cet administrateur applicatif ne dispose pas des droits de modifications des paramètres systèmes et des capacités de sauvegarde / restauration du système.
- Administrateurs système Bastion : personnes du domaine d'Administration possédant les droits d'accès et d'administration sur le shell via la console locale et le SSH 2242. Ce sont des personnes de confiance.
- Attaquants utilisateurs externes : personnes malveillantes du domaine Utilisateurs ne possédant aucun accès valide sur le Bastion.
- Attaquants administrateurs externes : personnes malveillantes du domaine d'Administration ne possédant aucun accès valide sur le Bastion.
- Attaquants Utilisateurs internes : personnes malveillantes du domaine Utilisateurs possédant des accès valides sur l'interface web du Bastion et les proxys, avec le rôle Utilisateur du Bastion ou Auditeur du Bastion mais essayant d'outrepasser leurs habilitations.
- Attaquants Administrateurs internes : personnes malveillantes du domaine d'Administration possédant des accès valides sur l'interface web du Bastion, avec le rôle Administratif applicatif Bastion mais essayant d'outrepasser leurs habilitations.
- Auditeurs du Bastion : personnes du domaine Utilisateurs possédant des droits d'accès et d'audit des traces dans l'interface web du Bastion. Ces personnes peuvent être des attaquants internes.
- Console Locale : La console locale est accessible par un port d'affichage VGA et un port clavier USB, ainsi que par l'iDrac2. Elle permet, après authentification, d'avoir accès à un shell du système d'exploitation.
- Domaine d'Administration : domaine des postes de travail des Administrateurs applicatif Bastion, des Administrateurs système Bastion et des Super Administrateurs du Bastion
- Domaine Ressources : domaine des machines cibles des connexions aux proxys.
- Domaine Utilisateurs : domaine des utilisateurs du Bastion (rôles Utilisateurs du Bastion, Auditeurs du Bastion, et attaquants utilisateurs internes). Ce domaine peut aussi servir d'accès pour les Attaquants externes.
- Mot de passe maître de chiffrement : lors de la première connexion au Bastion, le super administrateur doit indiquer s'il désire protéger les données sensibles chiffrées du Bastion par un mot de passe. Le mot de passe doit être fourni après chaque redémarrage pour rendre le Bastion pleinement opérationnel.
- Super Administrateur du Bastion : personnes du domaine d'Administration possédant à la fois les droits d'accès et d'administration dans l'interface WEB du Bastion et le shell (console locale et SSH 2242) et en possession du mot de passe maître de chiffrement. Ce sont des personnes de confiance.
- Enregistrements : enregistrements des sessions utilisateur par les proxys.
- Utilisateurs du Bastion : personne du domaine Utilisateurs possédant de simples droits d'accès utilisateurs à l'interface web du Bastion et aux proxys. Ces personnes peuvent être des attaquants internes.