Cible de sécurité CSPN - WAB 3.1.9

Document:	Cible de sécurité CSPN - Wallix AdminBastion 3.1.9
Version:	1.1
Référence:	CSPN-WAB-3.1.9
Date:	2013-04-23

WALLIX
TRACE, AUDIT & TRUST

Révisions

Version	Date	Description	Rédacteurs
0.1	2013-03-05	Version initiale pour WAB 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

Sommaire

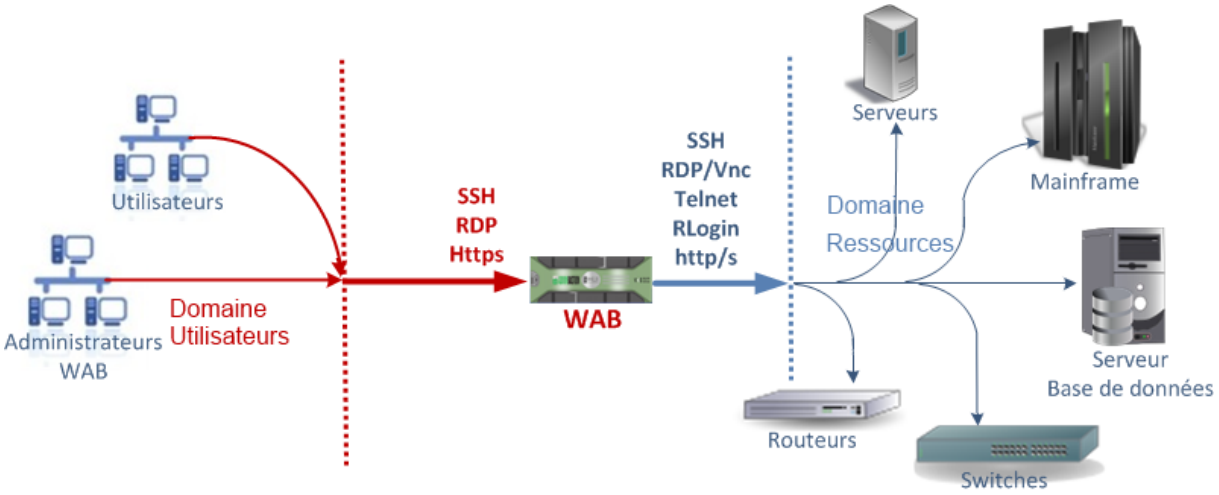
1. Identification du produit

Organisation éditrice	Wallix
Lien vers l'organisation	http://www.wallix.fr/
Nom commercial du produit	Wallix AdminBastion
Numéro de la version évaluée	3.1.9
Catégorie de produit	Identification, authentification et contrôle d'accès

2. Argumentaire (description) du produit

2.1. Description générale du produit

Le principal objectif du Wallix AdminBastion (appelé WAB dans le reste du document) est de jouer le rôle de relais applicatif (proxy) entre un domaine Utilisateurs potentiellement hostile et un domaine protégé Ressources.



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

- SSH v2 (remote command, remote shell, sftp, scp),
- RDP en TLS,
- HTTPS.

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

- SSH (remote command, remote shell, sftp, scp),
- RDP, VNC,
- HTTP, HTTPS,
- Telnet,
- commandes Berkeley rsh, rlogin, rcp.

Les protocoles HTTPS et SSH sont également utilisés pour l'administration du produit depuis n'importe lequel des deux domaines.

2.2. Utilisation du produit

Le WAB s'administre grâce à une interface HTML qui est accessible en HTTPS sur le port 443, et pour certaines actions via le shell accessible en console et en SSH v2 sur le port 2242.

L'utilisation des proxys se fait en utilisant les clients standard SSH, RDP ou HTTPS respectivement sur les ports 22, 3389 et 8080.

La HA fonctionne à travers une connexion entre les ports Ethernet 1 des deux machines du cluster. Les autres services sont disponibles sur tous les ports ethernet configurés.

2.3. Environnement d'utilisation

Le WAB est prévu pour fonctionner en appliance matérielle. Il est livré installé sur des serveurs Dell R320 ou R520 avec carte de supervision à distance iDrac et alimentation redondante.

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

1. standalone: le système tourne sur une seule appliance;
2. HA: le système tourne sur deux appliances en mode actif-passif. Une liaison doit être établie entre les ports Ethernet 1 de chaque machine.

2.4. Dépendances du produit à des matériels, logiciels et/ou des microprogrammes du système

Aucune dépendance externe n'est requise pour la version matérielle.

2.5. Utilisateurs typiques du produit

Il y a trois rôles possibles sur l'interface utilisateur du WAB :

1. Utilisateurs ;
2. Auditeurs ;
3. Administrateurs du WAB.

À cela s'ajoute les rôles possibles sur la console et l'interface SSH 2242 :

4. Administrateurs système WAB.

Les personnes qui accèdent au WAB doivent le faire depuis le domaine « Utilisateur » et endosser l'un de ces rôles. Ces personnes doivent être connues de l'entreprise soit par un contrat de travail soit par un contrat de prestation par exemple.

Les rôles sont décrits ci-dessous :

- Les **Utilisateurs** sont des personnes utilisant les ressources du système d'information sous le contrôle du WAB. Ces personnes peuvent être en charge de l'administration de ces ressources mais ne disposent normalement pas des droits d'administration sur le WAB. Il est à noter que le serveur WAB peut lui-même être considéré comme une ressource ; de ce fait, les opérations réalisées sur le serveur peuvent être surveillées.

  Un utilisateur doit s'authentifier auprès du WAB pour accéder aux services suivants offerts par le WAB :

  - Se connecter à une ressource cible,
  - Changer ses secrets d'authentification sur le serveur WAB.

- Les **Auditeurs** du WAB peuvent consulter les informations suivantes :

  - Historiques des connexions;
  - Enregistrements des sessions.

- Les **Administrateurs du WAB** sont les personnes en charge de l'administration de l'application WAB. 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 WAB).
  - Modifier certains paramètres techniques de la plate-forme.

  Un ou plusieurs administrateurs du WAB doivent également être possession du **Mot de passe maître** de la crypto pour la déverrouiller au démarrage du système. Le **Mot de passe maître** de la crypto permet de protéger les données sensibles encryptées du WAB par un mot de passe. Il s'agit d'une protection supplémentaire empêchant un utilisateur malveillant de décrypter les données.
- Un **Administrateur système WAB** est une personne en charge de l'administration du système Linux au cœur du WAB. Cette personne est généralement également un Administrateur du WAB en possession du mot de passe maître de la Crypto. Nous appellerons « **Super Administrateur du WAB** » une personne en charge de ce triple rôle.

2.6. Hypothèses sur l'environnement

- les administrateurs du produit (WAB et système WAB) sont compétents, formés et non hostiles
- les domaines « Utilisateur » et « Ressources » sont des réseaux internes à l'entreprise, non accessible depuis internet.
- les administrateurs de l'infrastructure réseau des domaines « Utilisateur » et « Ressources » sont compétents, formés et non hostiles
- l'accès physique au serveur WAB et à sa console est restreint aux seuls administrateurs du produit (WAB et système WAB)
- le produit est installé et configuré par des personnes compétentes, formées et non hostiles
- l'accès à distance aux équipements du domaine « Ressources » directement depuis le domaine « Utilisateur » est restreint de manière à obliger le passage par le WAB. On considère également que l'accès depuis un autre domaine est impossible.
- toutes les traces générées par le WAB sont stockées sur le produit, pas de stockage externe actif.
- le réseau du domaine « Ressources » est relié au port Ethernet 1 et le réseau du domaine « Utilisateur » au port Ethernet 2. Les interfaces eth0 et eth1 sont configurées respectivement pour chacun de ces réseaux.

2.7. Périmètre de l'évaluation

Le périmètre d'évaluation inclut:

- le logiciel WAB
- l'OS (Linux) sur lequel s'exécute le logiciel WAB

- les packages (dont les principaux sont : Apache2, MySQL 5.1, python 2.6). La liste exhaustive est disponible dans la documentation du produit.
- l'appliance matérielle Dell

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

- Accès aux interfaces d'administration (SSH v2 port 2242 et HTTPS SSLv3 TLSv1 port 80)
- Accès aux proxys (SSH v2 port 22, RDP TLSv1 port 3389 et HTTPS SSLv3 TLSv1 port 8080)
- Confidentialité des traces stockées sur le WAB
- Le changement des mots de passe des ressources cibles.

3. Environnement technique dans lequel le produit doit fonctionner

Le WAB 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 restent identiques à ceux utiliser avant la mise en place du WAB:

- clients SSH: openssh, putty
- clients RDP: mstsc (Microsoft Remote Desktop Client)
- clients HTTPS: Firefox, Google Chrome, Internet Explorer

3.1. Conditions d'évaluation

La configuration retenue pour l'évaluation est une configuration matérielle en mode haute disponibilité (HA): deux serveurs Dell en mode actif-passif. Le nœud actif est accessible via une adresse IP virtuelle et les deux serveurs sont connectés au même commutateur réseau (switch). C'est la configuration la plus utilisée par les clients de Wallix.

4. Biens sensibles que le produit doit protéger

Outre les services offerts par le WAB qui doivent être disponibles et intègres, le WAB doit protéger les données suivantes :

4.1. Données utilisateur

4.1.1. Flux Utilisateurs

Les flux transitant par le WAB doivent être protégés en Disponibilité, Intégrité et Confidentialité. Le WAB 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. Traces

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

4.2. Données internes

4.2.1. Base des utilisateurs

Cette base contient les identifiants et les moyens d'assurer l'authentification des utilisateurs du SI sur le WAB (généralement un hash d'un secret d'authentification ou une clé publique). Une personne non explicitement autorisée à le faire ne doit pas pouvoir modifier ou supprimer des données dans cette base. Si la base ne contient a priori pas de données confidentielles, il est toutefois préférable également d'éviter qu'une personne non autorisée puisse consulter la liste complète des utilisateurs.

4.2.2. Base de ressources cibles

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

4.2.2.1. Contrôle d'accès (ACL)

Cette base contient les associations autorisées entre les Utilisateurs et les Ressources cibles. Rappel : le WAB étant considéré comme une ressource cible, cette base permet donc aussi de gérer l'accès à l'interface d'administration du WAB. Une personne non explicitement autorisée à le faire ne doit pas pouvoir modifier ou supprimer des données dans cette base. Si la base ne contient a priori pas de données confidentielles, il est toutefois préférable également d'éviter qu'une personne non autorisée puisse consulter la liste complète des utilisateurs et des ressources cibles.

4.2.2.2. Journaux

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

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 « Utilisateur » : ci-après les « **attaquants externes** » ;
- les Utilisateurs et Auditeurs du WAB malveillants : ci-après les « **attaquants internes** ». Il est rappelé que ceux-ci sont localisés également dans le domaine « Utilisateurs ».

5.2 Liste des menaces retenues

5.2.1. Menaces sur les flux Utilisateurs

5.2.1.1. Écoute des flux

Un attaquant externe écoute les flux utilisateurs sur le domaine « Utilisateurs » pour compromettre la confidentialité des données transmises.

Données impactées : Confidentialité des flux Utilisateurs

5.2.1.2. Altération des flux

Un attaquant externe intercepte et modifie les flux utilisateurs sur le domaine « Utilisateurs ».

Données impactées : Intégrité des flux Utilisateurs

5.2.2. Menaces liées aux opérations réalisées par les Utilisateurs

5.2.2.1. Abus des droits utilisateurs

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

Données impactées : Intégrité des flux Utilisateurs

5.2.2.2. Répudiation

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

Données impactées : Intégrité des flux Utilisateurs

5.2.3. Menaces sur le WAB

5.2.3.1. Usurpation d'identité

Un attaquant externe tente d'usurper l'identité d'un utilisateur légitime ou d'un administrateur du WAB pour utiliser ses privilèges (accès aux ressources cibles ou accès à l'interface d'administration du WAB).

Données impactées : Intégrité et confidentialité des biens sensibles accessibles avec le compte usurpé.

5.2.3.2. Accès illicite

Un attaquant externe ou interne réussit par une attaque à s'introduire dans le système et à accéder et/ou modifier illicitement les données sensibles stockées dans le WAB (données d'authentification, traces).

Données impactées : Intégrité et confidentialité des biens sensibles stockés (traces, secrets d'authentification, ACL, ...).

5.3. Politique de sécurité 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, y compris le serveur WAB puisque l'interface d'administration est une ressource cible, doivent être enregistrées.

6. Description des fonctions de sécurité du produit

Outre fournir des fonctionnalités de proxy, le WAB offre les fonctionnalités de sécurité suivantes:

- Contrôle des accès aux ressources cibles : le WAB permet de mettre en oeuvre une politique d'accès aux ressources cibles ;
- 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 WAB qui, après s'être assuré que les accès sont autorisés, ouvre l'accès à la ressource cible demandée.

- Traçabilité : placé en coupure entre l'utilisateur et la ressource cible, le WAB permet d'enregistrer toutes les opérations réalisées, et ceci pour tous les protocoles supportés;
- Changement des mots de passe des ressources cibles (Windows et UNIX) périodiquement ou à la demande.

7. Glossaire

- ACL : Gestion des droits d'accès des utilisateurs aux ressources du WAB dans l'interface web d'administration, les webservices et les proxys.
- Administrateurs du WAB: personnes possédant les droits d'accès et d'administration dans l'interface web du WAB. Ce sont des personnes de confiance.
- Administrateurs système WAB: personnes possédant les droits d'accès et d'administration sur le shell via la console et le SSH 2242. Ce sont des personnes de confiance.
- Attaquants externes: personnes malveillantes ne possédant aucun accès valide sur le WAB.
- Attaquants internes: personnes malveillantes possédant des accès valides sur l'interface web du WAB et les proxys, avec le rôle Utilisateur du WAB ou Auditeur du WAB mais essayant d'outrepasser leurs habilitations.
- Auditeurs du WAB: personnes possédant des droits d'accès et d'audit des traces dans l'interface web du WAB. Ces personnes peuvent être des Attaquants internes.
- Domaine Ressources: domaine des machines cibles des connexions aux proxys. Ce domaine est sûr.
- Domaine Utilisateurs: domaine des utilisateurs du WAB (rôles Utilisateurs du WAB, Auditeurs du WAB, Administrateurs du WAB, Administrateurs système WAB, Super Administrateur du WAB et Attaquants internes). Ce domaine peut aussi servir d'accès pour les Attaquants externes.
- Journaux: fichiers logs du système linux et des services WAB.
- Mot de passe maître de la crypto : lors de la première connexion au WAB, le super-administrateur doit indiquer s’il désire protéger les données sensibles encryptées du WAB par un mot de passe. Il s’agit d’une protection supplémentaire empêchant un utilisateur malveillant de décrypter les données, mais qui nécessite de rentrer le mot de passe après chaque redémarrage pour rendre le WAB pleinement opérationnel.
- Traces: enregistrements des sessions utilisateurs par les proxys.
- Super Administrateur du WAB: personnes possédant à la fois les droits d'accès et d'administration dans l'interface web du WAB et le shell (console et SSH 2242) et en possession du mot de passe maître de la crypto. Ce sont des personnes de confiance.
- Utilisateurs du WAB: personne possédant de simples droits d'accès utilisateurs à l'interface web du WAB et aux proxys. Ces personnes peuvent être des Attaquants internes.