DÉPLOIEMENT D'UNE SOLUTION DE BASTION POUR L'ADMINISTRATION DES SERVEURS AVEC GUACAMOLE OU WALLIX

DESCRIPTION DU THÈME

Propriétés	Description
Intitulé long	Déploiement d'une solution de BASTION pour l'administration des serveurs et des éléments d'interconnexion avec guacamole ou wallix
Formation(s) concernée(s)	BTS Services Informatiques aux Organisations
Matière(s)	Bloc 3 SISR – Cybersécurité des services informatiques
Présentation	L'objectif de ce « Labo » est de comprendre l'intérêt d'un Bastion et d'en tester les principaux usages (intermédiaire des connexions pour l'administration des éléments sensibles d'une infrastructure réseau : serveurs et éléments d'interconnexion, journalisation des accès). Deux solutions seront étudiées Guacamole et Wallix mais les fonctionnalités présentées sont disponibles dans d'autres solutions de bastions. Ce « Labo » comporte 3 activités qui peuvent être réalisées en bloc3 SISR : • Activité 1 : Réflexions préalables à l'installation d'un bastion • Activité 2 : Installation du bastion, gestion des utilisateurs et des connexions (ssh / rdp) • Activité 3 : Audit et authentification renforcée
Savoirs	Savoirs-associés : • rupture protocolaire, bastion, périmètre de sécurité, authentification MFA, moindre privilège, audit.
Compétences	Compétences : • Déployer les moyens appropriés de preuve électronique • Gérer les accès et les privilèges appropriés • Vérifier l'efficacité de la protection • Organiser la collecte et la conservation des preuves numériques
Prolongements	D'autres activités (comme la gestion plus fine des autorisations) seront intégrées ultérieurement.

Prérequis	Commandes de base d'administration d'un système Linux. Administration de l'Active Directory. Notions de réseau (périmètre de sécurité, filtrage, etc.).
Outils	Un serveur physique ou virtuel sous une distribution Linux 64 bits (ici Debian 12 ou Ubuntu serveur ou Debian 13 avec l'utilisation de Docker) sur lequel le bastion Guacamole sera installé. Un serveur physique ou virtuel sous Linux avec le service DHCP. Un serveur physique ou virtuel sous un environnement Windows Serveur avec Active Directory installé. Une machine physique ou virtuelle pour le poste client « Administrateur ». Documentation Guacamole et Wallix.
Mots-clés	Bastion, RDP, SSH, journalisation
Durée	8 heures
Auteur·e·s	David BALNY avec la relecture et les tests d'Apollonie Raffalli (Guacamole), Valérie Martinez et Zakari BERREMILI (Wallix).
Version	v1
Date de publication	30/10/26

DERNIÈRES RÉVISIONS

Ce tableau contient les modifications apportées au document après sa publication uniquement.

Date	Auteur·e	Description

CONTEXTE

Née en décembre 2010, la société CUB est une entreprise spécialisée dans l'incubation de startups partageant les mêmes valeurs de solidarité et de développement durable. Au travers de sa plate-forme web, CUB permet à des professionnels d'accéder à des espaces de travail dédiés : salles de réunion, de formation ou de séminaire.

Le concept novateur de CUB repose sur une démarche collaborative de type « BtoB », en effet CUB propose aux entreprises qui disposent d'espaces inoccupés de les louer à l'heure ou à la journée.

À la différence d'une pépinière d'entreprises classique, CUB s'adresse à des sociétés très jeunes, ou encore en création, pour leur apporter un appui lors des premières étapes de la vie de l'entreprise. Elle met à disposition de ses clients un ensemble de solutions techniques d'accès dans un millier de salles de réunion situées dans une quarantaine de villes différentes. Les ressources et outils du Web 2.0 qui permettent aux entreprises de gérer leurs contenus et leurs connaissances de manière sécurisée sont accessibles indépendamment via des prestataires de type informatique dans les nuages (cloud computing) : partage de fichiers, gestion de projet, réseau social d'entreprise, wiki d'entreprise, etc.

La direction des systèmes d'information (DSI), située au siège à Paris, participe étroitement aux choix stratégiques de CUB, elle a pour mission de définir et mettre en œuvre la politique informatique en accord avec la stratégie générale et ses objectifs de performance.

CUB héberge, dans un Vlan « production » des services réseaux essentiels :

- un Active Directory paramétré sur un **serveur Windows** (RDP activé) ;
- un service DHCP paramétré sur un **serveur debian** (SSH activé).

Deux autres Vlan sont utilisés dans l'infrastructure :

- le Vlan « Bastion » pour héberger l'installation du **serveur Bastion** (solution au choix entre le bastion Guacamole et le bastion Wallix) ;
- le Vlan « Administrateurs » pour les postes des collaborateurs de la société.

À la demande de la DSI de la société CUB, souhaitant renforcer la sécurité de l'administration de ses serveurs et mieux maîtriser les accès à privilèges, la mise en place d'un bastion d'administration est envisagée.

Ce projet s'articule autour de trois activités complémentaires :

- **l'activité 1,** consacrée aux réflexions préalables à l'installation du bastion (analyse des risques, définition du périmètre, architecture réseau et règles d'accès) ;
- **l'activité 2,** portant sur l'installation de la solution, la gestion des utilisateurs et la configuration des connexions sécurisées aux serveurs via SSH et RDP ;
- **l'activité 3,** dédiée à l'audit des sessions et à la mise en place d'une authentification renforcée afin d'assurer la traçabilité des actions et de réduire le risque de compromission des comptes administrateurs. Ce déploiement répond ainsi aux exigences de sécurité, de contrôle et de conformité fixées par la DSI.

Voici le schéma de cette architecture :

