Mise en œuvre d'un équipement de gestion unifiée des menaces informatiques

Description du thème

Propriétés	Description
Intitulé long	Cette activité a pour but de mettre en place un équipement de gestion unifiée des menaces répondant aux besoins en matière de sécurité informatique de l'entreprise CUB.
Formation(s) concernée(s)	BTS Services Informatiques aux Organisations
Matière(s)	Bloc 3 SISR – Cybersécurité des services informatiques
Présentation	Cet ensemble d'activités lié au bloc 3 Cybersécurité spécialité SISR a pour but d'immerger les étudiants dans un contexte spécifique nommé CUB. Ils devront dans un premier temps remobiliser des compétences techniques acquises dans le bloc 2 afin de déployer la maquette qui leur est proposée : Segmentation réseau, VLAN, 802.1q, routage, routage inter-VLAN, DHCP, DNS, HTTP, HTTPS, Contrôleur de domaine Windows. Puis dans un second temps, acquérir des compétences spécifiques au bloc 3 à travers la mise en place d'un équipement de gestion unifiée des menaces informatiques.
Compétences	• Appliquer la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel • Appliquer les procédures garantissant le respect des obligations légales • Identifier les menaces et mettre en œuvre les défenses appropriées • Gérer les accès et les privilèges appropriés • Vérifier l'efficacité de la protection • Participer à la vérification des éléments contribuant à la sûreté d'une infrastructure informatique • Prendre en compte la sécurité dans un projet de mise en œuvre d'une solution d'infrastructure • Mettre en œuvre et vérifier la conformité d'une infrastructure à un référentiel, une norme ou un standard de sécurité • Prévenir les attaques • Détecter les actions malveillantes
Prérequis	Cette activité est à proposer en deuxième année SISR. L'idée centrale est de remobiliser des compétences déjà acquises dans un nouveau contexte utilisant un matériel professionnel spécifique à savoir un pare-feu UTM Stormshield physique ou virtuel (les VM de Stormshield sont disponibles dès lors que l'on a suivi la formation CSNA). **Nous recommandons l'utilisation de la version 4.3.x du firmware SNS (future version LTS) lors de la réalisation de ces activités.**
Mots-clés	Bonnes pratiques, protocoles DNS, HTTP, HTTPS, LDAP, VPN IPsec, VPN SSL, routage, NAT, filtrage, IPS/IDS, portail captif, proxy web.
Durée	Entre 32 et 40 heures
Auteur.e(s)	Quentin Demoulière et Apollonie Raffalli avec les précieuses relectures de David Balny, Ludovic Mery et Valérie Martinez
Version	v 1.1
Date de publication	Octobre 2023

I. Préambule

L'activité proposée est uniquement à visée pédagogique. Son objectif est l'amélioration de la sécurité informatique d'un système d'information. Il permet également l'acquisition de compétences associées au bloc 3 Cybersécurité SISR du BTS SIO.

⚠ Les outils abordés dans ce support sont uniquement utilisés à des fins éthiques (Ethical Hacking) et pédagogiques. Leur usage est formellement interdit en dehors de ce cadre sur un réseau tiers sans autorisation explicite.

Pour rappel, l'article 323-1 du code pénal stipule que le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

⚠ **Attention !** Les versions de firmware évoluant très régulièrement, il est possible que les captures d'écran présentées dans les documents puissent différer parfois de ce que vous obtiendrez lors de la mise en œuvre des situations.

II. Présentation du 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.

Armand Zaks, Michèle Ribez et Quentin Reynaud, les trois fondateurs, sont partis d'un double constat :

- en Île-de-France, 6 millions de m² de bureaux sont vacants ;
- en France, plus de 100 000 personnes travaillent ou ont déjà travaillé en espace de coworking. La France se classe au 6e rang mondial pour ce qui est du nombre d'espaces, et la pratique du coworking devrait continuer à progresser.

Forte d'une croissance très rapide, CUB fait une levée de fonds de 1,2 millions d'euros en 2016 et développe son activité pour atteindre sa dimension actuelle d'incubateur.

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. Outre un parc de près de 200 m² mis à disposition des jeunes entrepreneurs, l'incubateur offre des services logistiques et d'infrastructures mutualisés, un accompagnement professionnel de conseil et de financement personnalisé aux porteurs de projets liés au digital, aux applications mobiles et au e-commerce.

Chaque agence disposera d'une adresse IPv4 publique propre et nominative. Pour cela, l'entreprise CUB a demandé auprès du RIPE NCC l'obtention d'un numéro d'AS et d'un préfixe IPv4 : 192.36.253.0/24. Elle est donc considérée comme un LIR (Local Internet Registry).

CUB 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.

Le siège social de CUB est situé à Paris, des agences sont implantées dans plusieurs grandes villes internationales : Anvers, Barcelone, Hong-Kong, Los Angeles et en Corse.

La direction des systèmes d'information (DSI), située 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.

Le siège social est le cœur du système d'information interne de CUB, mais un service informatique de proximité (SIP) est présent sur chaque agence. Le SIP est responsable de l'assistance aux utilisateurs locaux et de la maintenance des ressources locales (infrastructure réseau et serveurs). Le SIP prend également en charge des projets qui concernent ponctuellement leur site.

III. Définition du projet auquel vous allez participer

Le malware Emotet est un cheval de Troie qui se diffuse par mail (capacité à récupérer des listes de contacts et envoi de mail d'hameçonnage avancé) et par des failles de sécurité liées au protocole de partage de fichiers SMB de Microsoft. Il permet de récupérer des mots de passe, des listes de contact. Il sert actuellement à installer d'autres outils malveillants spécialisés dans la récupération d'informations bancaires.

Emotet a touché un nombre important d'entreprises françaises en 2020 ce qui a conduit l'Agence nationale de la sécurité des systèmes d'information (ANSSI) à publier un bulletin d'alerte[1]. Ainsi, le service RSSI de l'entreprise CUB envisage le remplacement des pare-feu stateful vieillisants PFSense par une solution de sécurité unifiée (UTM) de l'entreprise Stormshield afin d'améliorer la gestion des menaces informatiques au sein de la société.

Aujourd'hui, vous travaillez dans l'équipe SIP de l'entreprise en tant que technicien systèmes et réseaux. Vous serez notamment en charge de la mise en œuvre d'un nouveau dispositif de sécurité, dans chacune des agences, nommé UTM (Unified Thread Management). Ces équipements émanent de la société Stormshield spécialisée en sécurité des réseaux et des systèmes d'information.

Stormshield est une entreprise française, sous-filiale d'Airbus, dont le siège social se situe à Issy-les-Moulineaux. Ainsi, elle est soumise à la loi française et à la loi européenne (loi informatique et libertés, RGPD, etc).

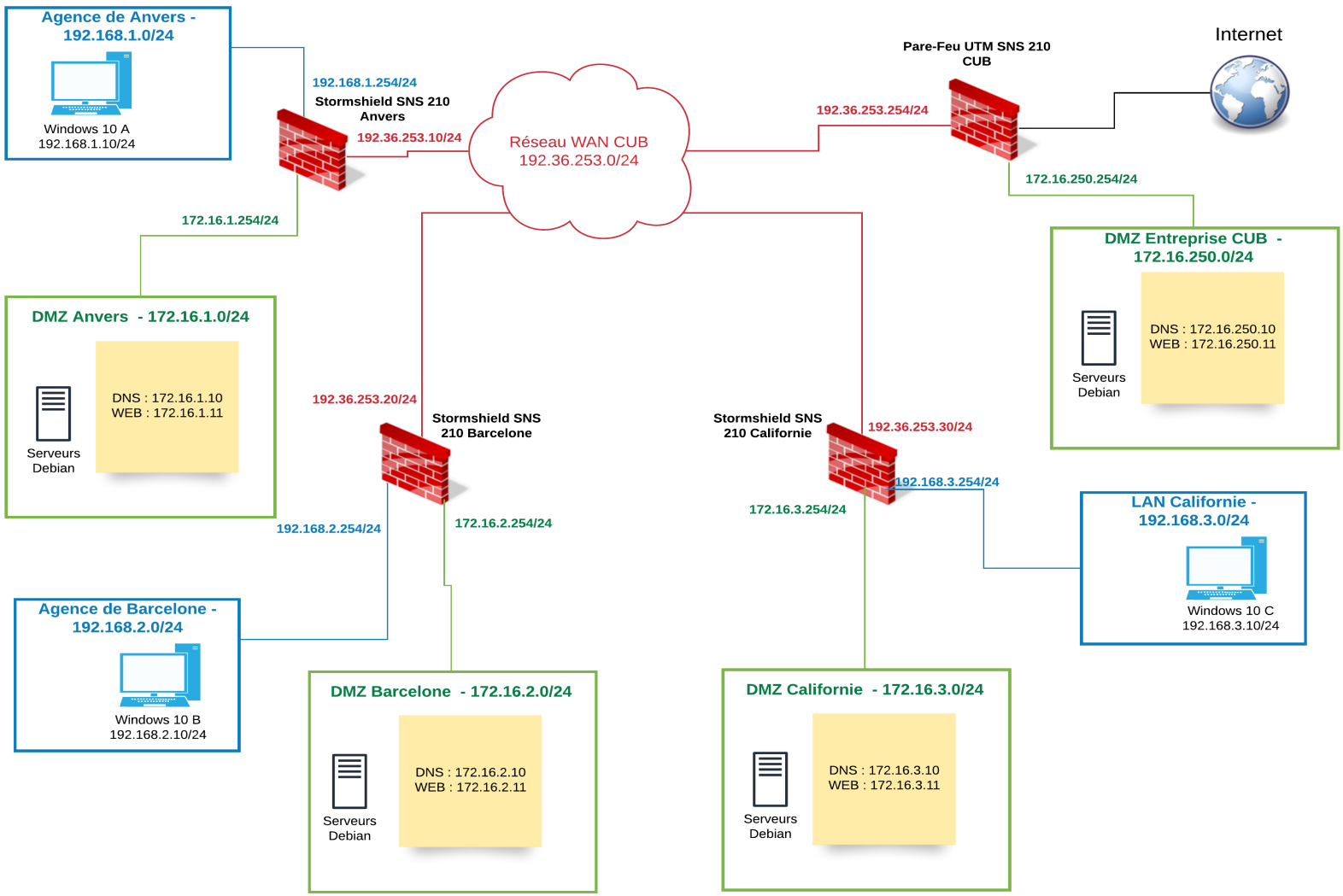
L'outil de protection réseau Stormshield SNS a obtenu la certification ANSSI EAL4+ et une qualification de niveau standard.
L'administration de l'outil en question se fera exclusivement par le biais du réseau local de l'agence où vous avez été affecté.

L'architecture du réseau CUB est fournie dans la documentation ci-après :

- Document 1 : Schéma logique simplifié du réseau CUB

1 https://www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-019/

Document 1 – Schéma logique simplifié du réseau CUB



IV. Plan d'organisation de l'activité

Groupes	Adresses de sous-réseaux	Adresses IP de votre firewall
Agence Anvers	LAN 1 – 192.168.1.0/24 DMZ 1 – 172.16.1.0/24 WAN – 192.36.253.0/24	In : 192.168.1.254 DMZ : 172.16.1.254 Out : 192.36.253.10
Agence Barcelone	LAN 2 – 192.168.2.0/24 DMZ 2 – 172.16.2.0/24 WAN – 192.36.253.0/24	In : 192.168.2.254 DMZ : 172.16.2.254 Out : 192.36.253.20
Agence Californie	LAN 3 – 192.168.3.0/24 DMZ 3 – 172.16.3.0/24 WAN – 192.36.253.0/24	In : 192.168.3.254 DMZ : 172.16.3.254 Out : 192.36.253.30
Agence Dortmund	LAN 7 – 192.168.4.0/24 DMZ 7 – 172.16.4.0/24 WAN – 192.36.253.0/24	In : 192.168.4.254 DMZ : 172.16.4.254 Out : 192.36.253.40
Agence Edimbourg	LAN 5 – 192.168.5.0/24 DMZ 5 – 172.16.5.0/24 WAN – 192.36.253.0/24	In : 192.168.5.254 DMZ : 172.16.5.254 Out : 192.36.253.50
Agence Frankfurt	LAN 6 – 192.168.6.0/24 DMZ 6 – 172.16.6.0/24 WAN – 192.36.253.0/24	In : 192.168.6.254 DMZ : 172.16.6.254 Out : 192.36.253.60
Agence Galway	LAN 4 – 192.168.7.0/24 DMZ 4 – 172.16.7.0/24 WAN – 192.36.253.0/24	In : 192.168.7.254 DMZ : 172.16.7.254 Out : 192.36.253.70
Agence Hong-Kong	LAN 8 – 192.168.8.0/24 DMZ 8 – 172.16.8.0/24 WAN – 192.36.253.0/24	In : 192.168.8.254 DMZ : 172.16.8.254 Out : 192.36.253.80

Vous trouverez, ci-dessous, un tableau présentant les différents serveurs présents en DMZ avec leur configuration respective pour les trois agences dont vous allez vous occuper.

Intitulé serveurs	Adresse IP interne	Adresse IP publique	Nom de domaine
Anvers Serveur DNS A Serveur Web A	 172.16.1.10 172.16.1.11	 192.36.253.10	 ns0.anvers.cub.fr www.anvers.cub.fr
Barcelone Serveur DNS B Serveur Web B	 172.16.2.10 172.16.2.11	 192.36.253.20	 ns0.barcelone.cub.fr www.barcelone.cub.fr
Californie Serveur DNS C Serveur Web C	 172.16.3.10 172.16.3.11	 192.36.253.30	 ns0.californie.cub.fr www.californie.cub.fr

NB : L'enregistrement ns0.xxxx.cub.fr correspondra dans le fichier de zone à l'adresse IP publique de l'interface OUT du firewall SN210.