

CONTEXTE CUB

BLOC 2 – ADMINISTRATION DES SYSTÈMES

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 formations ou de séminaires.

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 6ème 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.

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.

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.

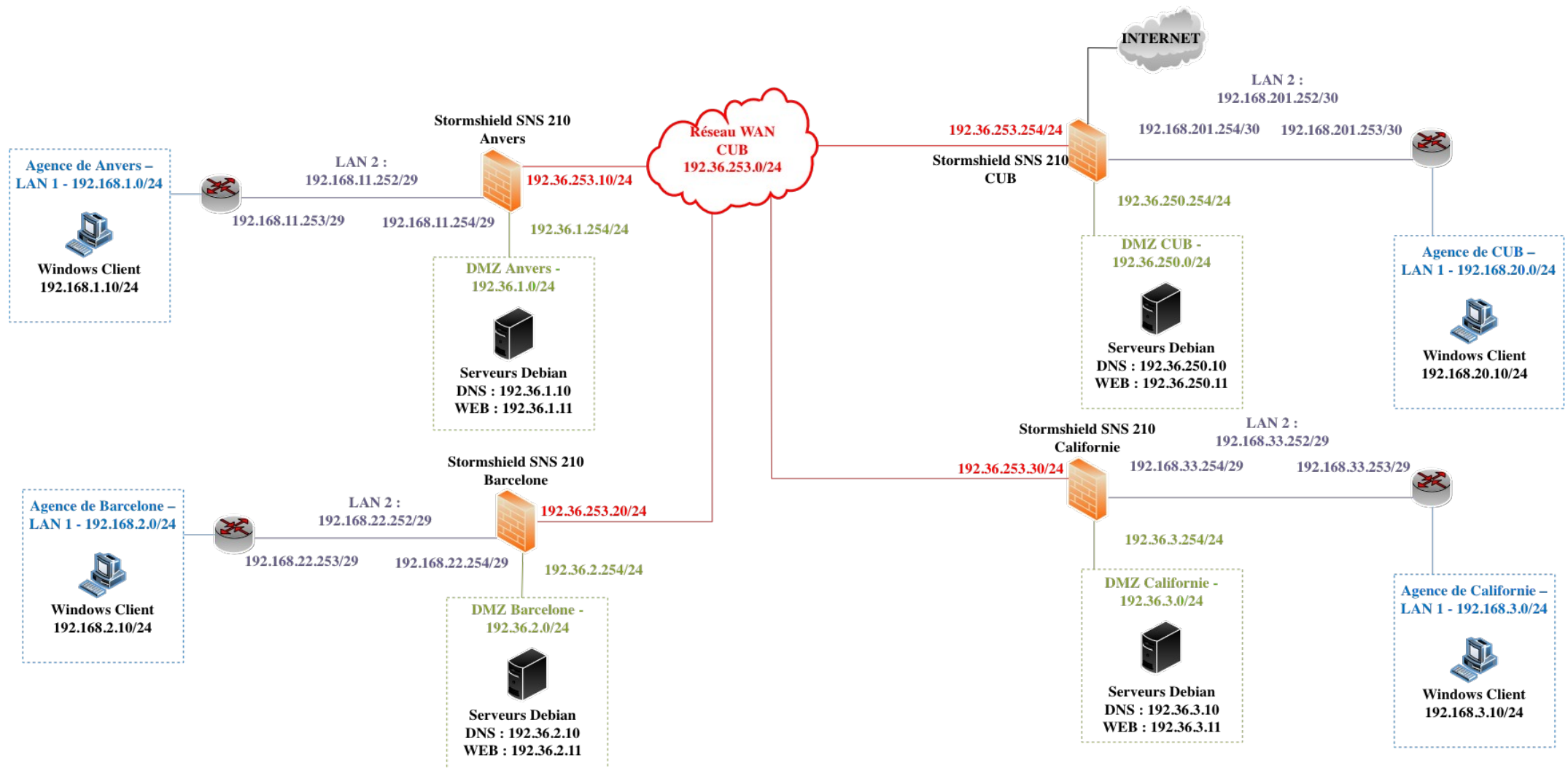
Emotet a touché un nombre important d'entreprises françaises en 2020 ce qui a conduit l'ANSSI à publier un bulletin d'alerte¹. Ainsi, le service RSSI de l'entreprise CUB envisage le remplacement des pare-feu stateful vieillissants PFSense par une solution de sécurité unifiée (UTM) de l'entreprise Stormshield afin d'améliorer la gestion des menaces informatiques au sein de la société.

Aujourd'hui, vous travaillez dans l'équipe SIP des différentes agences 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) émanant de la société française Stormshield spécialisée en sécurité des réseaux et des systèmes d'information. L'administration de cet équipement 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 A – Architecture simplifiée du réseau CUB
- Document B – Plan d'adressage du réseau CUB
- Document C – Schéma réseau physique du réseau CUB
- Document D – Liste des serveurs présents sur le site du siège

Document A – Architecture simplifiée du réseau CUB



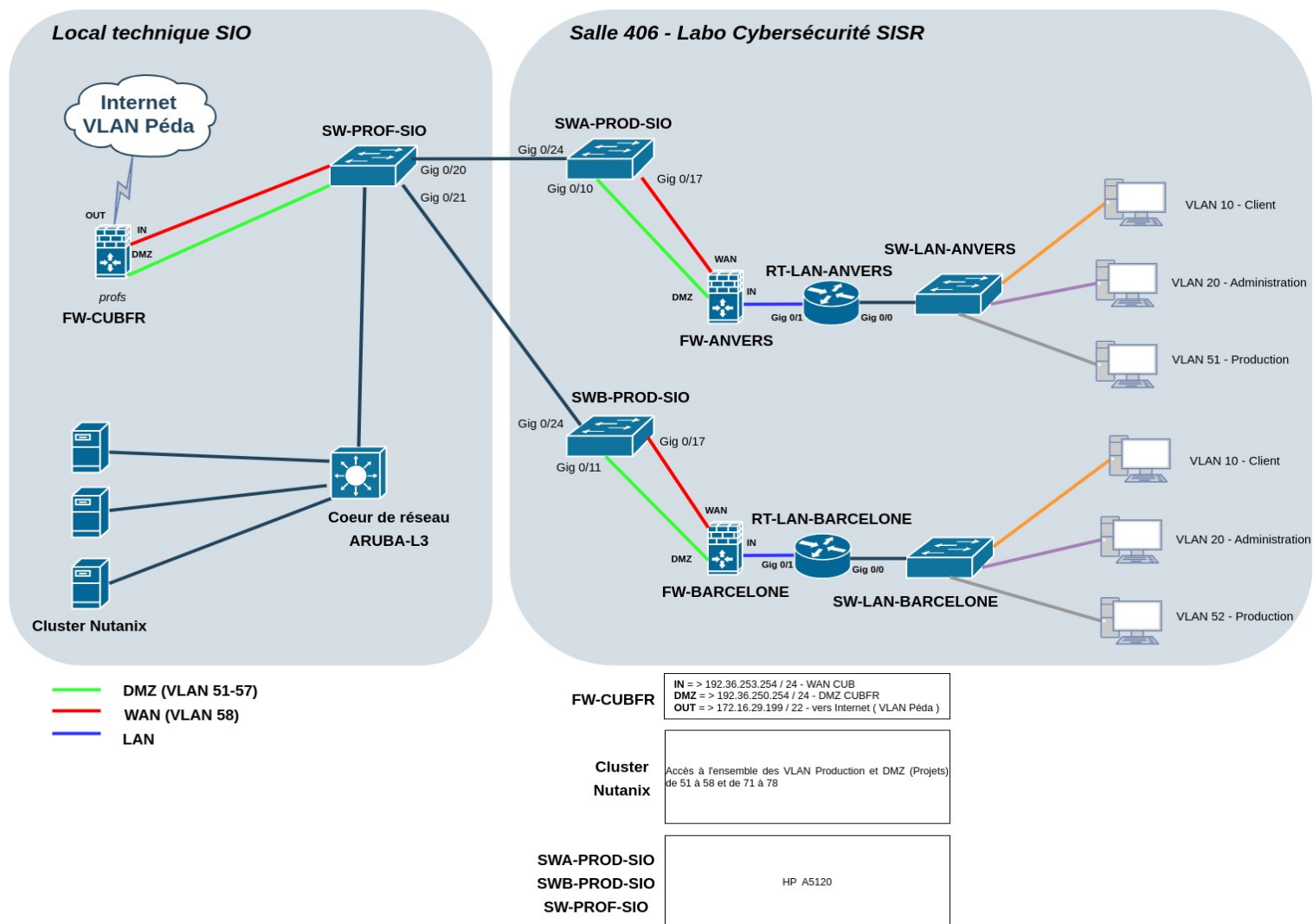
Document B – Plan d’adressage du réseau CUB

Groupes	Adresses de sous-réseaux	Adresses IP de votre firewall
Agence Anvers	LAN 1 – 192.168.1.0/24 LAN 2 – 192.168.11.252/30 DMZ – 192.36.1.0/24 WAN – 192.36.253.0/24	In : 192.168.11.254 DMZ : 192.36.1.254 Out : 192.36.253.10
Agence Barcelone	LAN 1 – 192.168.2.0/24 LAN 2 – 192.168.22.252/30 DMZ – 192.36.2.0/24 WAN – 192.36.253.0/24	In : 192.168.22.254 DMZ : 192.36.2.254 Out : 192.36.253.20
Agence Californie	LAN 1 – 192.168.3.0/24 LAN 2 – 192.168.33.252/30 DMZ – 192.36.3.0/24 WAN – 192.36.253.0/24	In : 192.168.33.254 DMZ : 192.36.3.254 Out : 192.36.253.30
Agence Dortmund	LAN 1 – 192.168.4.0/24 LAN 2 – 192.168.44.252/30 DMZ – 192.36.4.0/24 WAN – 192.36.253.0/24	In : 192.168.44.254 DMZ : 192.36.4.254 Out : 192.36.253.40
Agence Edimbourg	LAN 1 – 192.168.5.0/24 LAN 2 – 192.168.55.252/30 DMZ – 192.36.5.0/24 WAN – 192.36.253.0/24	In : 192.168.55.254 DMZ : 192.36.5.254 Out : 192.36.253.50
Agence Frankfurt	LAN 1 – 192.168.6.0/24 LAN 2 – 192.168.66.252/30 DMZ – 192.36.6.0/24 WAN – 192.36.253.0/24	In : 192.168.66.254 DMZ : 192.36.6.254 Out : 192.36.253.60
Agence Galway	LAN 1 – 192.168.7.0/24 LAN 2 – 192.168.77.252/30 DMZ – 192.36.7.0/24 WAN – 192.36.253.0/24	In : 192.168.77.254 DMZ : 192.36.7.254 Out : 192.36.253.70
Agence Hong-Kong (Agence mise en place par les enseignants)	LAN 1 – 192.168.8.0/24 LAN 2 – 192.168.88.252/30 DMZ – 192.36.8.0/24 WAN – 192.36.253.0/24	In : 192.168.88.254 DMZ : 192.36.8.254 Out : 192.36.253.80
Agence Bangkok	LAN 1 – 192.168.9.0/24 LAN 2 – 192.168.99.252/30 DMZ 8 – 192.36.9.0/24 WAN – 192.36.253.0/24	In : 192.168.99.254 DMZ : 192.36.9.254 Out : 192.36.253.90
Agence Tokyo	LAN 1 – 192.168.10.0/24 LAN 2 – 192.168.101.252/30 DMZ – 192.36.10.0/24 WAN – 192.36.253.0/24	In : 192.168.101.254 DMZ : 192.36.10.254 Out : 192.36.253.100
Société mère CUB	LAN 1 – 192.168.20.0/24 LAN 2 – 192.168.201.252/30 DMZ – 192.36.20.0/24 WAN – 192.36.253.0/24	In : 192.168.201.254 DMZ : 192.36.20.254 Out : 192.36.253.254

Vous trouverez enfin ci-dessous, un tableau vous présentant les différents serveurs présents en DMZ avec leur configuration respective.

Intitulé serveurs	Adresses IP publiques dans la DMZ	Adresse IP publique	Nom de domaine
<u>Anvers</u> Serveur DNS A Serveur Web A	192.36.1.10 192.36.1.20	192.36.253.10	ns0.anvers.cub.sioplcl.fr www.anvers.cub.sioplcl.fr
<u>Barcelone</u> Serveur DNS B Serveur Web B	192.36.2.10 192.36.2.20	192.36.253.20	ns0.barcelone.cub.sioplcl.fr www.barcelone.cub.sioplcl.fr
<u>Californie</u> Serveur DNS C Serveur Web C	192.36.3.10 192.36.3.20	192.36.253.30	ns0.californie.cub.sioplcl.fr www.californie.cub,sioplcl.fr
<u>Dortmund</u> Serveur DNS D Serveur Web D	192.36.4.10 192.36.4.20	192.36.253.40	ns0.dortmund.cub.sioplcl.fr www.dortmund.cub.sioplcl.fr
<u>Edimbourg</u> Serveur DNS E Serveur Web E	192.36.5.10 192.36.5.20	192.36.253.50	ns0.edimbourg.cub.sioplcl.fr www.edimbourg.cub.sioplcl.fr
<u>Frankfurt</u> Serveur DNS F Serveur Web F	192.36.6.10 192.36.6.20	192.36.253.60	ns0.frankfurt.cub.sioplcl.fr www.frankfurt.cub.sioplcl.fr
<u>Galway</u> Serveur DNS G Serveur Web G	192.36.7.10 192.36.7.20	192.36.253.70	ns0.galway.cub.sioplcl.fr www.galway.cub.sioplcl.fr
<u>Hong-Kong</u> Serveur DNS H Serveur Web H	192.36.8.10 192.36.8.20	192.36.253.80	ns0.hongkong.cub.sioplcl.fr www.hongkong.cub.sioplcl.fr
<u>Bangkok</u> Serveur DNS Ba Serveur Web Ba	192.36.9.10 192.36.9.20	192.36.253.90	ns0.bangkok.cub.sioplcl.fr www.bangkok.cub.sioplcl.fr
<u>Tokyo</u> Serveur DNS T Serveur Web T	192.36.10.10 192.36.10.20	192.36.253.100	ns0.tokyo.cub.sioplcl.fr www.tokyo.cub.sioplcl.fr
<u>Cub</u> Serveur DNS Prof Serveur Web Prof	192.36.250.10 192.36.250.20	192.36.253.254 192.36.253.254	ns0.cub.sioplcl.fr www.cub.sioplcl.fr

Document C – Schéma réseau physique du réseau CUB



Document D – Liste des serveurs présents sur le site du siège

Serveur	Configuration réseau	Description
ns0.cub.sio plc.fr	IP : 192.36.250.10/24 Passerelle : 192.36.250.254 DNS : 172.16.20.11, 9.9.9.9	Serveur DNS maître faisant autorité sur le domaine cub.sio plc.fr.
ns1.cub.sio plc.fr	IP : 192.36.250.11/24 Passerelle : 192.36.250.254 DNS : 172.16.20.11, 9.9.9.9	Serveur DNS esclave faisant autorité sur le domaine cub.sio plc.fr.
www.cub.sio plc.fr	IP : 192.36.250.20/24 Passerelle : 192.36.250.254 DNS : 172.16.20.11, 9.9.9.9	Serveur web vitrine de l'entreprise CUB