

Hamza BOURAKADI

@ : bourakadihamza@gmail.com

Tél : 07 51 04 28 34

115 rue du Point du Jour, Boulogne-Billancourt, 92100



Ingénieur Réseaux et Sécurité

FORMATION

- **Ecole Mohammedia d'Ingénieurs** - Maroc, Cycle d'ingénieur – Génie Réseaux et Télécommunications, année d'obtention : 2017

EXPERIENCES PROFESSIONNELLES

Ingénieur sécurité réseaux
BNP Paribas

02/2023–Aujourd'hui

Lead - Infrastructure Firewall pour un DataBunker (DC double backup)

Mise en place d'une infrastructure dormante et totalement isolée, synchronisée avec les environnements de production, afin de garantir la continuité des services essentiels de la banque en cas de perte totale des datacenters principaux.

- Conception de l'architecture sécurisée :
 - Étude et design d'une infrastructure Firewall isolée pour un DataBunker garantissant une séparation complète des environnements de production, tout en permettant une synchronisation sécurisée des données critiques.
 - Analyse des besoins en sécurité avec les équipes SOC et identification des risques potentiels liés à l'isolation du DC.
 - Définition des flux réseau nécessaires pour garantir une synchronisation périodique avec les datacenters principaux et les systèmes métiers prioritaires.
- Mise en œuvre technique :
 - Configuration et déploiement des Firewalls (Fortinet et Palo alto selon les zones de sécurité : Bastion, presBastion, Databunker et AirGaps).
 - Mise en place des consoles de managements : FMG/FAZ et Panorama.
 - Création des règles Firewall spécifiques pour assurer :
 - La synchronisation sécurisée des applications entre les environnements prod et backup.
 - La segmentation stricte des zones pour éviter tout risque de contamination en cas d'attaque.
 - Mise en place d'un « Red Button » pour tout bloquer avec l'environnement de production en cas de contamination.
 - Mise en place d'une politique globale par zone héritée.
 - Mise en place de deux zone AirGaps :
 - Une zone temporaire pour la construction des applications et qui est coupé post migration.
 - Une deuxième zone qui permet la synchronisation et qui porte le Red Button.
 - Mise en place d'un IPS sur le firewall de PresBastion.
- Collaboration inter-équipes :
 - Travail étroit avec les équipes d'architectes réseaux et applications pour définir les prérequis techniques pour la réplication des applications critiques.
 - Coordination avec les équipes Cloud pour mettre en place une politique d'accès au Databunker différente des accès production afin d'éviter la contamination.
 - Collaboration avec les équipes Réseaux pour l'intégration des équipements et la configuration des liens de communication avec les datacenters principaux.
 - Debug des problèmes avec les équipes applications lors des créations ou bien des synchronisations.

- Gestion de projet et alignement stratégique :
 - Participation aux comités de pilotage avec les chefs de projet pour aligner les livrables.
 - Contribution à la planification des phases du projet, à la gestion des risques, et à l'élaboration de la roadmap technique.
 - Rédaction de la documentation technique (HLD, LLD) et des procédures pour assurer une montée en compétence des équipes Run.
 - Préparation des comptes rendus d'avancement à destination des parties prenantes (chefs de projet et direction technique).

Build firewalls :

- Integration firewalls (Palo alto et Fortigate) :
 - Préparation des schémas réseaux et câblage.
 - Application de la configuration de base (Licence, HA, Tacacs, DNS, DHCP, SNMP et NTP)
 - Ajout dans les consoles de managements FMG/FAZ et Panorama.
 - Création de la politique de sécurité de base et push les firewalls.
 - Migration ou embarquement des nouveaux équipements en production dans le cadre de change HNO.
 - Configuration des VPN IPsec partenaires sur (Checkpoint, Fortigate et Palo Alto).
 - Mise en place de l'IPS pour les Flux SRA.
- Migration firewalls :
 - Intra technologie pour les Checkpoints ; migrer des VS vers des applicances physique ou bien l'inverse.
 - Inter technologies ; faire des opérations de transformations de firewalls d'une technologie à une autre sur Palo alto, Checkpoint et Fortigate.

Run firewalls :

- Assurer le bon fonctionnement des firewalls (RUN).
- Analyser et corriger les incidents en niveaux 2 et 3.
- Réaliser des diagnostics pour identifier les causes de dysfonctionnement et proposer des corrections et des solutions de contournement.
- Maintien en condition opérationnelle les infrastructures dans un objectif de qualité, de productivité et de sécurité.

Architecte réseaux et sécurité – Equipe Intégration SD-WAN

Bouygues Telecom

10/2021–02/2023

Déploiement SD-WAN Fortinet

Afin d'assurer le bon déroulement de la phase de BUILD, la procédure de déploiement est la suivante :

- Audit technique :
- Réception et analyse des documents fournis :
 - Schémas d'architecture des Sites
 - Détail des équipements LAN/WAN
 - Liste des ports disponibles sur les équipements LAN et WAN
 - Détail des liens : typologies, débits, protocoles
 - Plans d'adressage IP
 - Liste des priorisations applicatives (QoS)
 - Règles de sécurité
- Définition des UseCases et de l'architecture cible
- Identification des contraintes et points de vigilance
- Identification des sites pilotes (1 Template / UseCase par site)
- Livrable :
 - Compte rendu d'audit (à valider par le client)
 - Document d'architecture (incluant les schémas de câblage)
 - Dossier de conception
- Dossier d'exploitation

➤ Pilote :

- Paramétrage technique/Configuration :
 - Configuration du contrôleur
 - Création des templates (1 par UseCase)
 - Implémentation des règles SDWAN
 - Implémentation des règles QoS
 - Implémentation des règles QoE (SLA applicatifs)
 - Implémentation des règles de sécurité
 - Provisionning des CPE des sites Pilotes dans le contrôleur
 - Rédaction du cahier de recette
- Installation et migration des sites pilotes :
 - Installation du ou des CPE sur le site principal
 - Installation des CPE des autres sites pilotes
 - Recette technique des fonctionnalités relatives au socle
 - Rédaction du PV de recette
- Période d'observation :
 - Surveillance du site du pilote passé en production
 - Intervention en cas d'incidents et assister le Run
 - Vérification des indicateurs client (Saturation, dégradation de service, coupures...)
- Passation et accompagnement du client afin de monter en compétence

➤ Déploiement généralisé :

A la suite de la validation du pilote par le client, nous procédons au déploiement généralisé des autres sites du client.

Le déploiement massive se fait en se basant sur l'automatisation par le biais de script CLI ou bien Jinja en parallèle avec le ZTP.

Environnement technique FortiManager, FortiAnalyzer, Fortigate (gamme de série de 40F - 60F - 80F - 100F – 200F – 300F – 400E)

**Ingénieur réseaux et sécurité – Equipe Build SD-WAN
SANOFI**

09/2020–10/2021

• **La migration de tout le parc WAN Sanofi des zone APAC, EMEA et Chine (270 sites) vers SD-WAN CloudGenix Palo Alto**

• Planning :

- Etude de l'architecture actuelle de chaque site et design de l'architecture SD-WAN cible (Branch, DC ou Hybrid)
- Rédaction des documents/livrables techniques (HLD, LLD)
- Etablissement de la liste de contrôles du déploiement / Runbooks (mise en œuvre et tests)
- Logistiques et coordinations spécifique aux sites pour la livraison des circuits, du rack/pile d'équipements et du câblage
- Planification et alignement du projet avec les dates cibles de migrations

• Implémentation :

- Finalisation le document technique de mise en œuvre
- Configuration des équipements CloudGenix SD-WAN sur les sites (eBGP, Filtrage réseau, Règles Firewall et Règles VPN)
- Configuration CloudGenix SD-WAN Path et politiques QoS
- Configuration CloudGenix ZScaler CloudBlade
- Mise à jour des outils de Monitoring
- Configuration et préparation des équipements LAN du site selon la taille (switch cœur et Nexus9K) ainsi que les routeurs de l'opérateur pour la migration
- Configuration des préfixes locaux/globaux et assurer l'accessibilité des sites Branch aux DCs

- Livraison de bout en bout des circuits tout en coordonnant avec les fournisseurs sur les sites concernés (Sanofi, OBS, Colt et PaloAlto)
- Tests et Validation :
 - Révision et modification de la configuration à l'aide de scripts Python
 - Examen des données de l'onglet Analytics du PRISMA Palo Alto et les flux Flow Browser
 - Tests d'applications et validations des utilisateurs finaux sur les sites
 - Assurer l'accessibilité des Branch CloudGenix SD-WAN, des bases de données et des applications principales par les utilisateurs
 - Nettoyage du matériel hérité après basculement du site
- Développement de scripts Python pour automatiser le processus de migrations et de tests
- Environnement 100% en Anglais

Environnement technique : PaloAlto CloudGenix IONs 9K, 2K et 3K, Cisco Nexus 9K, Zscaler, Efficient IP, Entuity, Prisma PaloAlto CloudGenix

**Ingénieur réseaux – Equipe Run Télécom
CARREFOUR**

03/2019–08/2020

-
- **La gestion de tout le réseau LAN, WAN et DATACENTER du Groupe Carrefour à travers un centre de service dédié (4 équipes de 32 personnes en total)**
 - Maintien en condition opérationnelle du WAN (France, Taiwan, Argentine, Espagne, Roumanie, Pologne, Brésil, Belgique, Chine et Italie) et des LAN des principaux sites (3440 magasins, 216 hypermarchés, entrepôts et datacenters)
 - Maintien en condition opérationnelle du Datacenter (4 Datacenters en total)
 - Traitement des incidents et changements N2 et N3 (LAN DC, WAN, WiFi)
 - Maintenance matérielle (RMA, pilotage d'interventions sur site) et logicielle (upgrades IOS sur Switch, Access point, Contrôleur Wifi Cisco et Aruba)
 - Participation à des conférences de crise dans le cas d'incidents impactant sur tout le périmètre Carrefour en 24/7
 - Modification des topologies et configuration de matériel à risque sur la production (migrations du parc WiFi de 216 Hypermarchés Carrefour depuis Cisco Vers Aruba)
 - Coordinations avec les intervenants des différents chantiers (opérateurs OBS, SFR et Intégrateurs Axians, OCWS)
 - Utilisation d'outils de supervision et de reporting (Alaloop, Skylight Accedian, Splunk, Ipanema, Observer, 5-View et Wireshark)
 - Participation aux différentes réunions Agile (Daily Stand Up, Story Time, Spring Planning, Retrospective)
 - Rédaction de la documentation et transfert de connaissance auprès des autres collaborateurs (SecOps, Réseau, UCS, DCP)
 - Formation des nouveaux arrivants dans l'équipe

Environnement technique : WAN MPLS Juniper, Cisco Nexus 9K – Cisco Fabric Path, Nexus 7K, Switch d'accès Nexus (2K, 4K, 5K), Catalyst (3650, 4500, 6500), Wifi Cisco (WLC, AP 1230, 1240, 29600), Wifi Aruba, DATACENTER (technologie VXLAN), Fortigate 401 E, Fortigate 201 E, Fortigate 61F CheckPointSG5600

**Ingénieur réseaux – Equipe Build SD-WAN
VEOLIA**

09/2018–02/2019

-
- **Migration du WAN Veolia VeoBridge vers SD-WAN Cisco Meraki**
 - Rédaction des documents/livrables techniques (HLD, LLD)
 - Animation des comités de pilotage du déploiement des sites SD-WAN sur le périmètre National
 - Logistiques et coordinations spécifiques aux sites pour la livraison des circuits, du rack/pile d'équipements et du câblage
 - Planification et alignement du projet avec les dates cibles de migrations

- Animation des comités de pilotage du déploiement des sites SD-WAN sur le périmètre National
- Développement de scripts pour automatiser tout le process de Build et de migration SD-WAN à l'aide de Google Apps Script et Meraki API :
 - Claim des nouveaux Meraki MX,
 - Configuration du LAN sur les MX (Vlans, Ports, adressage IP),
 - Configuration des règles de routages selon les BU de Veolia,
 - Configuration des règles VPN et des tunnels vers les ZEN Zscaler,
 - Etablissement de la communication avec le Hub central,
 - Assigner les licences,
- Utilisation d'outils de supervision et de reporting (ServiceNow, Alaloop et Centreon)
- Assurer la gestion des situations de crises en 24/7
- Rédaction de procédure et documentation de support pour le N1 et N2 sur la partie SD-WAN

Environnement technique Cisco Merak, Infoblox (DHCP et DNS), Zscaler, ServiceNow, Centreon, Alaloop

**Ingénieur réseaux et sécurité – Equipe Run Télécom
VEOLIA**

09/2017–08/2018

- **La gestion de tout le réseau LAN et WAN du Groupe Veolia à travers une équipe NOC dédiée**
 - Maintien en condition opérationnelle du WAN (France et international) et des LAN des principaux sites
 - Traitement des incidents et changements N2 et N3 (LAN, WAN, DC, Firewalls, WiFi, Proxy)
 - Animation des comités de pilotage du déploiement des liens WAN sur le périmètre international
 - Automatisation du traitement WAN et SD-WAN à l'aide de Google Apps Script, API et Python (traitement de plus que 400 opérations par semaine)
 - Pilotage des mises en production des sites WAN et SD-WAN (suivi et validation des services, Facturation et Pénalités)
 - Modification des topologies et configuration de matériel à risque sur la production (migration de tout le parc WAN Cisco vers SD-WAN Meraki).
 - Maintenance matérielle (RMA, pilotage d'interventions sur site) et logicielle (upgrades IOS/NX-OS)
 - Déploiement de liens IPSec avec les différents partenaires Veolia
 - Coordinations avec les intervenants des différents chantiers (opérateurs OBS, SFR et Intégrateurs Axians, NXO et gestionnaire de DC IBM, Equinix)
 - Utilisation d'outils de supervision et de reporting (ServiceNow, Alaloop, Centreon, Zabbix et Wireshark)
 - Assurer la gestion des situations de crises en 24/7
 - Rédaction de procédure et documentation de support pour le N1 et N2
 - Rédaction de document d'exploitation pour les équipes internes Veolia sur la partie SD-WAN
 - Formation des nouveaux arrivant dans l'équipe

Environnement technique : WAN MPLS, Cisco Nexus 7K, Nexus 5K, Catalyst 3650, Fortinet 1500D, Checkpoint 13500, Palo Alto PA-3060, Infoblox (DHCP et DNS), Zscaler, Meraki, ServiceNow, Zabbix

**Ingénieur stagiaire réseaux et sécurité
Centre National pour la Recherche Scientifique et Technique**

01/2017–06/2017

- **La mise en place d'un SIEM pour le NOC Maroc**
 - Conception de l'architecture cible de la maquette
 - Intégration et mise en œuvre de l'infrastructure (Routeurs, serveurs SIEM, Firewalls et IPS/IDS)
 - Collecte et agrégation des fichiers de journalisations sur un serveur central hébergeant le SIEM
 - Conduite des tests d'intrusion à l'aide de Kali Linux
 - Vérification du bon fonctionnement du SIEM par la génération d'alertes (Warning et envoi de mails) vers les groupes de contacts
 - Mise en place de tableaux de bord et de rapports d'activités pour améliorer la visibilité sur le SI

Environnement technique : ELK stack avec module Xpack (SIEM), Cisco 3800, Cisco ME 3400, Cisco ASR1001-X, Cisco ISR 4431, Cisco ASA, serveur Ubuntu et CentOS

COMPETENCES & CERTIFICATIONS

Certifications

- Certifié Cisco CCNP ENARSI 300-410
- Certifié Cisco CCNP and CCIE Entreprise Core ENCOR 350-401
- Certifié Cisco CCNA Routing and Switching 200-125
- Certifié Fortinet NSE4 Network Security Professional
- Certifié Palo Alto PCNSA Network Security Administrator
- Certifié Microsoft Azure Fundamentals AZ-900
- Certifié Zscaler ZCCA-IA

Compétences techniques

- Infrastructures et services LAN, WAN , SD-WAN , SD-Access, VXLAN, LISP
- Routage: BGP, RIP, OSPF, EIGRP, NAT, routage IPv6
- Switching: VLAN, STP, MST, Etherchannel, vPC
- Services IP: HSRP, VRRP, DNS, NAT, DHCP, SNMP
- Outils: Wireshark, Zabbix, Centreon, Infoblox, Alaloop, Service now, Kibana
- Firewalls: Fortinet, CheckPoint, Palo Alto
- IPS / IDS: Snort, Palo alto.
- Proxy: Zscaler
- Protocoles d'authentification: RADIUS, 802.11X, TACACS
- Sécurité des échanges: VPN IPSec, SSH

Cloud

- Connaissance générale des services Cloud AWS et de l'environnement Microsoft AzureCloud.

Programmation

- Python, API, JavaScript, Ansible

COMPETENCES Fonctionnels

Méthodologies

- Collecte et synthèse de besoins fonctionnels et techniques
- Pilotage de projets de déploiement d'infrastructures
- Formalisation de livrables : compte-rendu de réunion, schéma et dossier d'architecture, note de synthèse, document d'exploitation ...
- Encadrement
- Mise en place de procédures

LANGUES

- Anglais : courant
- Français : courant
- Arabe : maternel

