

*Ingénieur Sécurité Réseau Confirmé – Palo Alto / Fortinet / NSX
6 ans d'expérience
Certifié PCNSA et NSE4*

Consultant disposant d'une expertise solide sur les environnements firewalling, SD-WAN, VPN, load balancing, proxy et supervision, avec une forte pratique des solutions Fortinet, Palo Alto, F5 et Zscaler. Son parcours couvre des missions de Run et Build en contexte grand compte : BNPParibas, incluant le maintien en conditions opérationnelles, la gestion des incidents N2/N3, les ouvertures de flux, les audits de règles firewall, l'optimisation de règles de filtrage.

FORMATIONS & CERTIFICATIONS

2016 : Bac +4 en Technologie des Informations, Ghana Technology University College, Accra
2018 : Stage de formation CCNA R&S, CCNP R&S et CCIE R&S, Networkershomes
2021 : CCNA (Cisco Certified Network Associate)
2022 : PCNSA (Palo Alto Networks Certified Network Security Administrator)
2022 : NSE4 (Network Security Professional)

COMPETENCES FONCTIONNELLES & TECHNIQUES

Compétences principales :

- Troubleshooting
- Optimisation de l'infrastructures firewall
- Matrice de flux
- Rédaction de la documentation technique détaillée
- Suivi de plan d'upgrade sécurité

Réseau & sécurité : conception, exploitation et optimisation d'infrastructures réseau sécurisées : TCP/IP, LAN/WAN, VLAN, DHCP, NAT, DNAT, SNAT, routage BGP/OSPF, VPN IPsec, SSL VPN et segmentation réseau.

Optimisation d'infrastructures : amélioration de la performance, de la disponibilité et de la résilience des environnements réseau et sécurité, rationalisation des règles firewall, fiabilisation des flux critiques et réduction des points de blocage.

Firewalling & sécurité périmétrique : administration, audit, revue de conformité et optimisation des politiques de sécurité sur Fortinet, Palo Alto et Stormshield.

SD-WAN & accès sécurisés : déploiement, migration et optimisation d'architectures SD-WAN Fortinet, tunnels GRE, accès Internet sécurisés et intégration Zscaler ZIA.

Load balancing & publication applicative : exploitation et optimisation des services applicatifs via F5 BIG-IP LTM/ASM, gestion des VIP, Pools, Nodes et certificats SSL/TLS.

Run / Build & MCO : maintien en conditions opérationnelles, gestion d'incidents N2/N3, upgrades de sécurité, traitement des vulnérabilités, supervision et amélioration continue des infrastructures.

Outils & environnements : FortiManager, FortiAnalyzer, Panorama, Wallix Bastion, Centreon, GitLab, AWX, CMDB, Azure, VMware ESXi.

Virtualisation : NSX Firewall, NX Load Balancer, VMware vSphere, Sécurité virtualisée

Gouvernance technique : animation de comités techniques, recommandations d'évolution, coordination avec les équipes métiers, sécurité, systèmes et supports constructeurs.

Administration & supervision : FortiManager, FortiAnalyzer, Panorama, Centreon, CMDB, ABT, Azure, Azure AD, VMware ESXi, Hyper-V

Outils & méthodes : GitLab, AWX, ITIL, MCO, SOC, gestion des changements, suivi des vulnérabilités, comités techniques, rédaction de guides et de procédures

Langues : Anglais courant

EXPERIENCES PROFESSIONNELLES

ORANGE CYBERDEFENSE, 2025 / 2026

Ingénieur sécurité réseaux N3 – Run & Build

Contexte du projet :

Intervention au sein d'un NSOC mutualisé en environnement critique, comme référent technique sécurité firewalls sur un portefeuille multi-clients grands comptes.

Missions réalisées :

- Administration d'environnements Fortinet et Palo Alto multi-VDOM / VSYS pour les accès distants sécurisés, GlobalProtect SSL VPN et IPsec VPN
- Exploitation N3 (MCO) et contribution Build sur des infrastructures sécurité à forte criticité.
- Audits, conformité, rédaction de standards, gestion RUN/BUILD
- Participation au déploiement et à la migration d'une infrastructure SD-WAN Fortinet internationale, avec plus de 330 sites migrés sur un objectif de 800 sites.
- Optimisation des configurations Fortinet via FortiManager, AWX et GitLab dans le cadre des déploiements ZTP.
- Configuration des accès Internet sécurisés via Zscaler : tunnels GRE, static IP et locations.
- Validation post-migration des tunnels Overlay, Underlay et GRE, puis intégration dans les outils de supervision, CMDB et sauvegarde.
- Gestion des changements complexes
- Gestion des ouvertures de flux et des incidents critiques en coordination avec les supports constructeurs Fortinet et Zscaler.
- Administration F5 BIG-IP LTM : création de VIP, Pools et Nodes, publication applicative et renouvellement des certificats SSL/TLS.
- Production de rapports mensuels de vulnérabilités, animation de comités techniques et suivi des plans d'upgrade sécurité.
- Mise en place de règles Palo Alto App-ID et de règles DNAT à travers des tunnels IPsec pour répondre aux besoins métiers.

Impact : MCO des environnements firewalls Palo Alto, Fortinet, environnement virtualisé NSX, sécurisation des accès, fiabilisation des migrations SD-WAN et amélioration du maintien en conditions opérationnelles d'infrastructures critiques multi-clients.

Environnement technique : FortiGate 40F, 60F, 80F, 100F, 200F, 400F, 400E, 600F, FortiGate 401F, FortiManager VM Azure, FortiAnalyzer VM Azure / Hyper-V, FortiAuthenticator, VMware NSX, SD-WAN, GRE, BGP, Zscaler ZIA, Zscaler Client Connector, Azure, Azure AD, SAML, GitLab, AWX, Centreon, CMDB, ABT, Palo Alto PA-5410 / PA-3250 / PA-3420 / PA-440 / PA-5250 / PA-220, Panorama, Cisco Catalyst C9300, SSL VPN, VDOM, VSYS, F5 BIG-IP LTM/ASM, Stormshield SNS-520, Wallix Bastion

SNCF, 2022 / 2025

Ingénieur sécurité réseaux

Contexte du projet :

Mission en environnement grand compte, centrée sur le pilotage des ouvertures de flux, l'analyse des risques sécurité et le MCO (maintien en conditions opérationnelles) des infrastructures réseau et sécurité.

Missions réalisées :

- MCO, administration, troubleshooting et revue des règles de firewalling Fortinet, Palo Alto, F5, Vmware NSX en cohérence avec les exigences sécurité et performance.
- Réalisation d'audits de règles et de revues de conformité afin de réduire les risques et d'améliorer la posture de sécurité.
- Rédaction de standards, gestion BUILD / RUN
- Pilotage des demandes d'ouverture de flux réseau avec analyse des besoins, qualification technique et évaluation des risques sécurité.
- Validation des règles de sécurité en coordination avec le RSSI, sur la base des dossiers d'architecture et des politiques internes.
- Analyse avancée des flux réseau et troubleshooting pour identifier les points de blocage et proposer des solutions adaptées.
- Gestion des incidents réseau et sécurité en environnement client avec engagement sur la qualité de service et les délais de résolution.
- Conseil et accompagnement des équipes métiers et techniques sur les bonnes pratiques de sécurisation des accès.
- Contribution à l'amélioration continue des processus et standards de sécurité.

Impact : optimisation de l'infrastructures firewall, réduction des risques liés aux ouvertures de flux, rédaction des standards et des règles, amélioration de la conformité des règles de sécurité et renforcement de la qualité de service.

Environnement technique : Fortinet, Palo Alto, F5, Vmware NSX, firewalling, audit de règles, DAT, politiques de sécurité, analyse de flux, troubleshooting réseau, MCO, gestion des incidents, accompagnement RSSI.

BNP PARIBAS BP2I, 2019 / 2022

Ingénieur sécurité réseaux

Contexte du projet :

Première expérience en environnement grand compte, au sein d'une équipe de support Réseau & Sécurité de niveau 2 chargée de l'exploitation d'infrastructures critiques.

Missions réalisées :

- Gestion des incidents réseau et sécurité avec analyse, diagnostic et résolution de bout en bout.
- Exploitation et configuration d'équipements réseau, routeurs et switches, dans des environnements critiques.
- Réalisation d'opérations courantes : ajout de routes, upgrades d'équipements et gestion des remplacements matériels RMA.
- Intervention sur des infrastructures Cisco Nexus 2K et 7K.
- Support des technologies réseau Spanning Tree, vPC, OSPF et BGP.
- Analyse des flux réseau et support au troubleshooting sur firewalls, avec identification de règles bloquantes et vérification des flux.
- Participation aux opérations de maintenance sécurité, notamment le renouvellement de certificats.
- Collaboration avec les équipes techniques pour assurer la disponibilité, la performance et la sécurité du réseau.

Impact : fiabilisation du support réseau et sécurité, réduction des interruptions de service et amélioration de la prise en charge des incidents.

Environnement technique : Routeurs, switches, Cisco Nexus 2K / 7K, Spanning Tree, vPC, OSPF, BGP, firewalls, certificats, RMA, support N2, exploitation réseau et sécurité.