RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CNPF

Rapport écrit par :

Alexandre ERNANDEZ

Sujet :

Rapport de stage, mission infrastructure réseau CNPF

Date :

Du 8 Janvier au 23 Février 2024

Table des matières

Remerciements

Je souhaite exprimer ma sincère gratitude envers M. Alain Posty, mon tuteur de stage, pour sa confiance inébranlable tout au long de mon parcours. Son accueil chaleureux, sa disponibilité, ses conseils avisés et ses expériences précieuses partagées ont été une source d'inspiration pour moi.

Je tiens également à adresser mes remerciements à M. Sylvain Guichard, qui m'a encadré avec rigueur et bienveillance tout au long de ce second stage. Ses conseils éclairés et sa motivation constante m'ont permis de progresser efficacement dans l'accomplissement de ma mission.

Je souhaite exprimer ma profonde reconnaissance envers le CNPF et toute son équipe informatique. Cette expérience au sein du CNPF a largement dépassé mes attentes initiales et a renforcé ma confiance en mes capacités à atteindre mes objectifs professionnels futurs.

Glossaire

FAI : Le sigle FAI défini les organismes étant des fournisseurs d'accès à Internet.

Firewall / Pare-feu : Un pare-feu est un logiciel et/ou matériel permettant de faire respecter la politique de sécurité de réseaux, celle-ci définissant quels sont les types de communications autorisés sur un réseau informatique. Il surveille et contrôle les applications et les flux de données. (Source : Wikipédia)

VPN MPLS : C'est une technologie qui permet à plusieurs sites de s'interconnecter de façon transparente et chiffré par l'intermédiaire du FAI.

Introduction

Pendant ma formation BTS SIO (Services informatiques aux organisations) avec une spécialisation en SISR (Solution d'Infrastructure Système et Réseau) lors de mes années au lycée Benjamin Franklin à Orléans, j'ai été tenu d'accomplir deux stages obligatoires, chacun d'une durée comprise entre six et sept semaines, en vue de l'obtention de mon diplôme.

Ma quête d'un lieu de stage m'a dirigé vers le CNPF. Lors d'un entretien, j'ai eu l'occasion de rencontrer M. Alain Posty et M. Sylvain Guichard, qui m'ont exposé les différents projets cruciaux pour l'évolution et la maintenance de l'infrastructure réseau du CNPF. Dans ce rapport, je me concentrerai particulièrement sur le projet de mon deuxième stage au sein du CNPF.

La mission consistait à élaborer une approche réfléchie pour mettre en place un système de filtrage sur les pare-feu Stormshield dans une centaine de sites en France, en les adaptant à leurs utilisations respectives. En effet, depuis la transition des CRPF (Centre Régional de la Propriété Forestière) au CNPF (Centre National de la Propriété Forestière), le service informatique et réseau du CNPF fait face à des défis de centralisation, d'homogénéisation des infrastructures réseau et de gestion de la sécurité.

Ce rapport va donc présenter la structure des différentes approches mises en place pour comprendre et élaborer un système sécurisé adapté aux besoins et aux utilisations des divers acteurs de la CNPF sur leurs 100 sites à travers la France, ainsi que leur réseau associé. Plusieurs technologies ont été utilisées tout au long de ce stage, ce qui m'a permis d'acquérir un ensemble important de compétences.

Pour conclure cette introduction, cette expérience fût riche et ma permit d’aborder des perspectives très intéressantes sur mes envies professionnelles.

Présentation générale

Au cours de cette présentation, je vais aborder plusieurs points essentiels. Tout d'abord, je vais vous présenter l'entreprise dans laquelle j'ai effectué mon stage. Ensuite, je vais vous exposer en détail la mission qui m'a été confiée. Enfin, je vais aborder le cadre de travail qui a favorisé l'avancement ainsi que la concrétisation, ou non, de cette mission.

Présentation de l'entreprise

CNPF (Centre National de la Propriété Forestière)

Le CNPF est l'établissement public chargé du développement de la gestion durable des forêts privées : quelque 3,5 millions de propriétaires forestiers pour 12,6 millions d'hectares soit environ 23% du territoire. Placé sous la tutelle du Ministère de l'Agriculture et de la Souveraineté alimentaire.

Missions du CNPF

Je vous présente les missions principales du CNPF :

- Orienter la gestion des forêts privées : il agrée les documents de gestion durable, qui prévoient la gestion d'une propriété sur 10 à 20 ans. Tout propriétaire de plus de 20 ha doit avoir un plan simple de gestion agréé ;

- Conseiller et former : il réalise des études et des expérimentations sur la forêt, puis vulgarise les méthodes de sylviculture auprès des propriétaires en les formant et les informant ;

- Regrouper la propriété privée : la forêt privée étant très morcelée, le CNPF regroupe les propriétaires pour réaliser des projets de desserte, mobiliser les bois, regrouper les chantiers d'exploitation, mutualiser les coûts de travaux forestiers…

Organisation structurelle et emplacement géographique

La CNPF est répartie en une centaine de sites à travers la France (voir annexe), cette organisation se fait à travers 11 centres régionaux appelés (CRPF).

Un service de Recherche et Développement est également disponible au sein du CNPF, l'Institut pour le développement forestier (IDF).

Pour soutenir ses activités, le CNPF bénéficie d'un service général essentiel qui assure le soutien administratif, coordonne les activités internes et gère les ressources humaines, les finances et les systèmes d'information.

Le CNPF compte pour plus de 500 agents, des ingénieurs forestiers, des techniciens forestiers, des formateurs, des chercheurs, ainsi que du personnel administratif et des informaticiens.

SDN (Service du Développement Numérique)

Au sein du CNPF, il existe un service informatique, celui-ci porte le nom de Service du Développement Numérique (SDN). Il est sous la supervision et la direction de M. Alain Posty qui occupe le poste de Directeur des Systèmes d'Information (DSI). Le rôle du SDN est d'organiser, développer et sécuriser l'infrastructure, les données ainsi que le bon fonctionnement des systèmes d'information. Ce service permet l'évolution et la maintenance du l'informatique pour améliorer la compétitivité du CNPF.

Le département informatique du CNPF, principalement situé à l'antenne d'Orléans, est constitué d'une diversité de profils, comprenant des administrateurs systèmes, des développeurs, des techniciens support et des chefs de projet. Bien que l'équipe soit de taille modeste, elle se démarque par sa vitalité et sa croissance constante, attirant régulièrement de nouveaux talents et compétences.

Présentation de la mission

Dans le cadre de mon stage en entreprise pour l'obtention de mon BTS au sein de la CNPF, je fus chargé de la conception et la mise en place de règles de filtrage sur infrastructure des différents pare-feu présents sur chaque site de la CNPF à travers la France. De plus, je devais imager et catégoriser les différents outils qui pourraient être mis en place pour la gestion de la sécurité sur l'infrastructure Cloud AWS de la CNPF.

Toutes ses tâches avaient pour but de maximiser et fortifier les aspects cyber sécurité au sein du CNPF. Avec la croissance de la numérisation des entreprises, elles sont devenues des proies aux yeux des cybercriminels, il est donc important pour une entreprises comme la CNPF avec une forte empreinte numérique de prendre les précautions nécessaires.

Mission : Planification et configuration des pare-feu

Contexte

Depuis la centralisation de la gestion des réseaux de la CNPF, les pare-feu Stormshield présents sur chaque site ne possédaient que des configurations permettant une interconnexion due à leur présence via un VNP dans un MPLS grâce au FAI de la CNPF. Aucune règle de filtrage n'était présente sur les pare-feu.

Objectifs et enjeux du projet

Aujourd'hui, l'objectif pour le SDN est de limiter les flux et de contrôler efficacement l'accès des utilisateurs au réseau local ainsi qu'à Internet. Cette approche vise à mieux répondre aux habitudes de travail des utilisateurs et aux impératifs de sécurité pour le SDN. Un premier aspect crucial dans la réflexion sur le SDN est d'éviter la possibilité d'une découverte totale du réseau en cas d'infiltration par une personne malveillante. Il est également essentiel de limiter la propagation d'une telle infiltration à travers le réseau du CNPF, afin de préserver la sécurité globale de l'infrastructure.

Mise en œuvre

Outils utilisées

Streamcore : Logiciel rattaché à des sondes physique présent sur chaque site de la CNPF qui analyse en temps réel chaque requête qui passe sur le réseau.

Stormshield (SNS210) : C'est un pare-feu physique mis à ma disposition afin de créer mes règles de filtrage sur l'appareil type présent sur tous les sites de la CNPF afin de prévoir le déploiement de celle-ci.

Stormshield (SMC) : Agent de déploiement et de gestion des pare-feu Stormshield, il permet la gestion globale de manière centralisée des pare-feu de la CNPF (voir annexe).

Nmap (Windows) : Il s'agit d'un outil pour analyser les adresses IP et les ports d'un réseau et pour détecter les applications installées. Nmap permet aux administrateurs réseau de trouver quels appareils s'exécutent sur leur réseau, de découvrir les ports et services ouverts et de détecter les vulnérabilités.

AWS : Plateforme de service Cloud utilisée par la CNPF pour l'hébergement de leur serveur application.

Théorie

La manière que j'ai utilisée pour résoudre la problématique de gestion des flux et accès par le pare-feu est la suivante. Il est important de prendre en compte qu'une règle qui bloque la totalité des

flux se situera à la fin du tableau des règles de filtrage. Cela signifie qu'il faut en premier lieu autoriser les flux de manière précise puis plus on descend dans les priorités et les règles d'autorisations seront globales.

J'ai eu pour idée de me positionner et de me concentrer uniquement sur les requêtes sortantes et non entrantes. En effet, les sites de la CNPF n'ont pas pour but d'être atteignable par l'extérieur, il convient donc de se concentrer d'avantage sur ce que les utilisateurs en interne ont le droit ou non d'accéder.

J'ai eu comme première idée d'analyser les protocoles les plus utilisés par les utilisateurs sur une dizaine de sites en France sur des plages horaires qui diffèrent dans la journée. Afin d'extraire un modèle d'utilisation type d'un utilisateur de la CNPF durant sa journée de travail. Cette analyse aurait pour but de m'aider à comprendre la méthodologie de travail et l'organisation des divers outils et applications utilisés par les utilisateurs de la CNPF.

Une fois qu'un schéma d'utilisation moyenne de l'utilisateur est établi, il est nécessaire de se pencher sur la destination des flux. Cela permettra d'empêcher les utilisateurs d'accéder à des sites internet ou des applications qui ne sont pas reconnus comme essentiels à l'accomplissement de leurs tâches et obligations professionnelles.

Pratique

Après avoir effectué une première analyse via l'outil Streamcore (voir annexe) présent sur tous les sites de la CNPF, celle-ci m'a permis de tirer la théorie suivante qui est qu'un utilisateur de la CNPF sur site à une utilisation classique des outils de travail mis à sa disposition. En effet, seulement des connexions de navigation Web Internet, des échanges de mail, et les outils de vidéoconférence sont les plus ressortis.

Dans un deuxième temps, j'ai entrepris une analyse approfondie de la destination des flux sur le réseau. Il m'a semblé crucial de garantir aux utilisateurs la liberté de naviguer sans entraves sur Internet, tout en préservant la sécurité de l'infrastructure réseau de la CNPF. Cette démarche était nécessaire afin de concilier l'accessibilité du réseau avec la protection contre les menaces potentielles.

Il était impératif de trouver un équilibre entre l'ouverture nécessaire à la productivité et à la recherche d'informations, et la nécessité de protéger les ressources sensibles de la CNPF contre les cybers menaces. Par conséquent, il était essentiel de mettre en place des mesures visant à restreindre l'accès des utilisateurs aux autres sites de la CNPF.

En effet, en cas d'infiltration du réseau d'un site de la CNPF par un cybercriminel, les risques de propagation à l'ensemble du réseau sont considérables. Limiter l'accès aux autres sites réduit la surface d'attaque potentielle et renforce la capacité de la CNPF à contenir et à neutraliser les menaces éventuelles.

Cette approche permet non seulement de prévenir les attaques externes, mais aussi de limiter les dommages en cas de compromission d'un point spécifique du réseau. En restreignant l'accès aux ressources internes, nous renforçons la résilience du système global de la CNPF face aux cybers menaces, tout en préservant la liberté d'utilisation d'Internet pour les utilisateurs autorisés.

En premier lieu, j'ai créé un tableau de règles de filtrage de manière conventionnelle (voir annexe), sans utiliser les options proposées par la SMC Stormshield. Cette approche simpliste présentait de nombreux inconvénients, notamment en ce qui concerne l'évolutivité potentielle du projet dans le temps. De plus, une problématique liée au regroupement des protocoles selon les destinations limitait la capacité d'évolution et les détails potentiels pour un meilleur suivi avec un agent de gestion des logs.

Proposition

Selon moi, pour renforcer et optimiser la sécurité lors de la navigation sur le Web, il est essentiel de mettre en place un proxy afin de filtrer et limiter l'accès aux sites Internet jugés potentiellement dangereux ou inappropriés, notamment dans un environnement professionnel.

Un proxy agit comme un intermédiaire entre l'utilisateur et les ressources en ligne qu'il souhaite consulter. En établissant un tel système, le SDN peut exercer un contrôle accru sur les sites auxquels les utilisateurs ont accès tout en protégeant l'infrastructure informatique et en réduisant les risques liés à la sécurité.

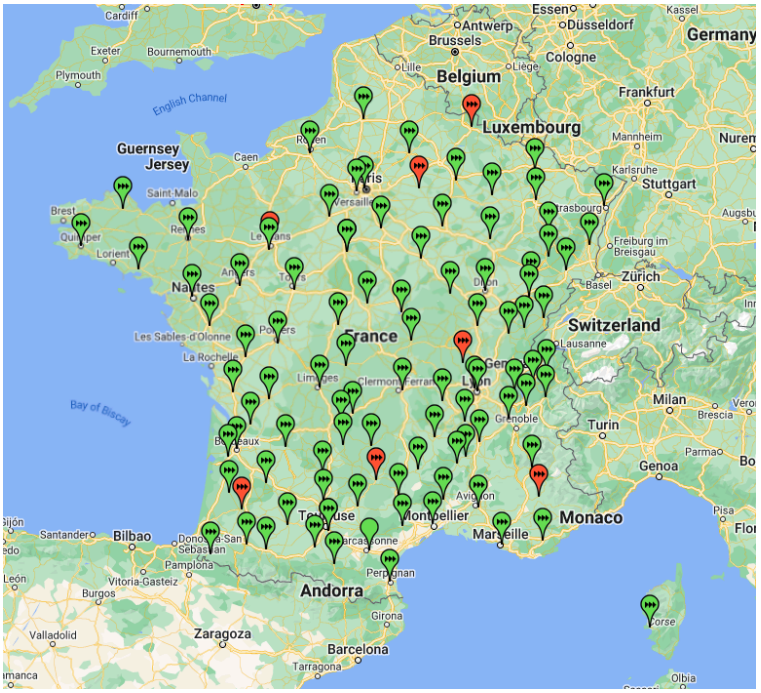
En restreignant l'accès aux sites potentiellement dangereux, tels que ceux associés à des logiciels malveillants, des contenus inappropriés, ou des activités frauduleuses, les entreprises peuvent limiter les risques d'attaques informatiques, de fuites de données confidentielles.

De plus, la mise en place d'un tel système permet de promouvoir une culture de sécurité auprès des utilisateurs du CNPF en les sensibilisant aux risques liés à la navigation sur Internet et en encourageant des pratiques responsables en ligne pour assurer leur sécurité et celle du CNPF.

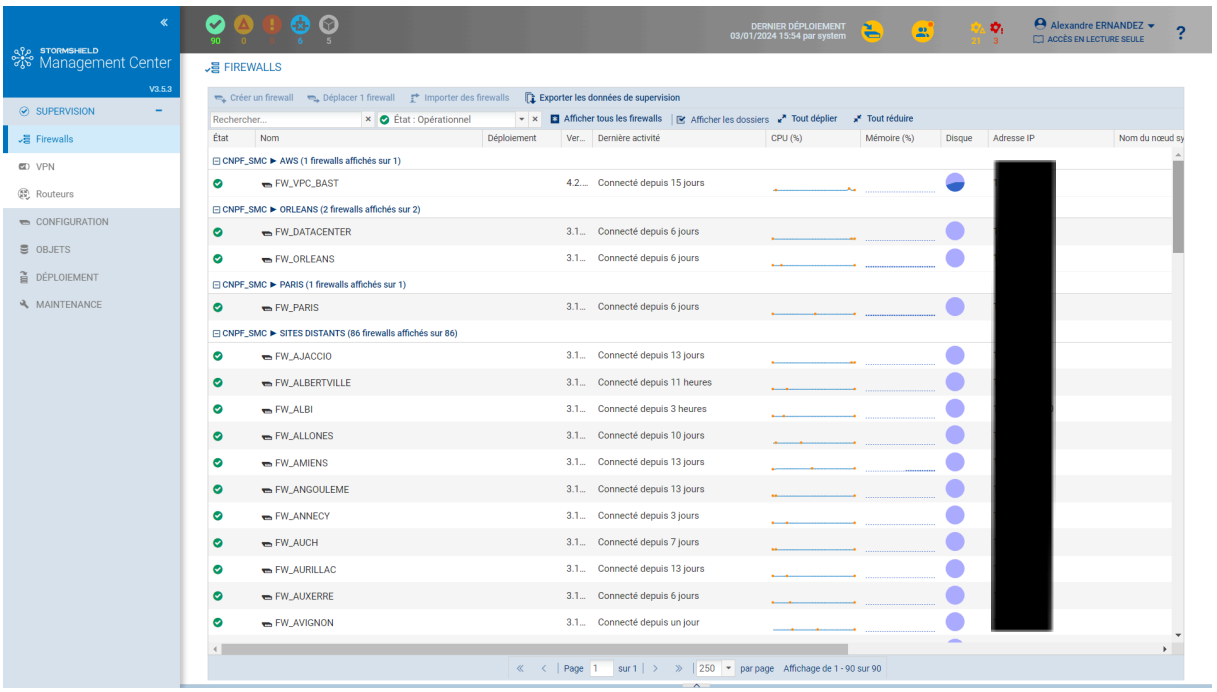
Toutefois, il est également important de trouver un équilibre entre la sécurité, la liberté et la productivité. Il convient donc de mettre en place des politiques claires et des critères de filtrage bien définis, tout en laissant aux utilisateurs un accès raisonnable aux ressources nécessaires à l'exécution de leurs tâches professionnelles.

Annexe

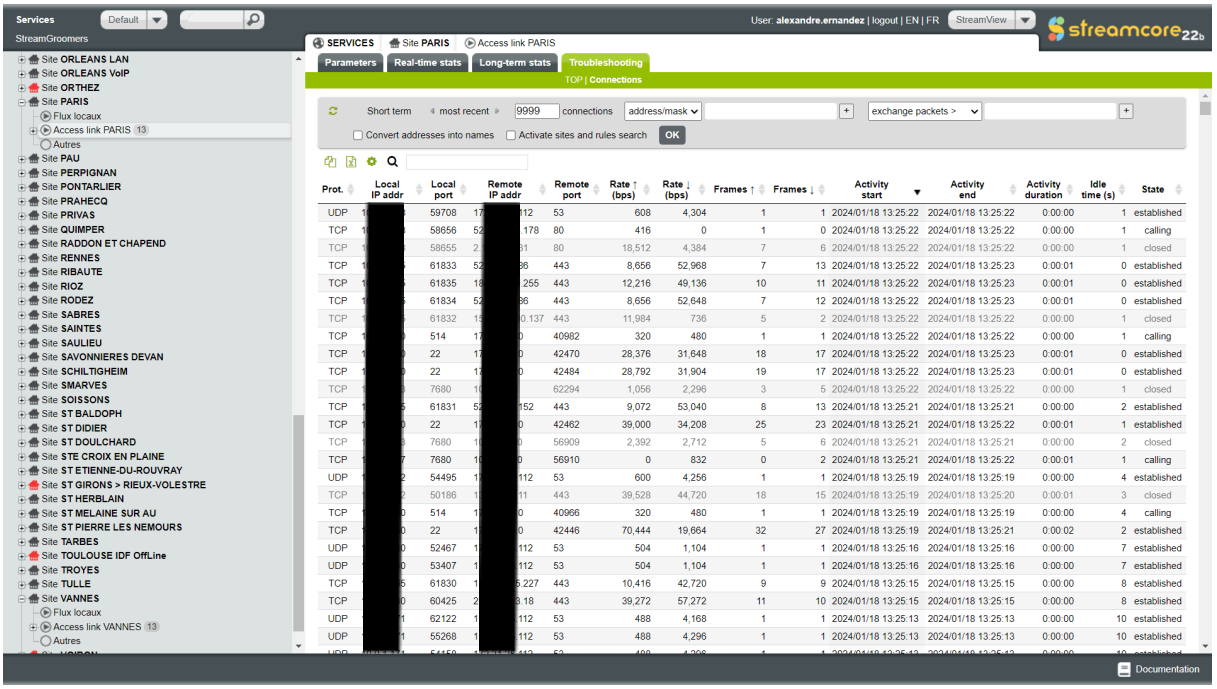
Carte des sites de la CNPF en France :



Interface SMC Stormshield :



Interface analyse Streamcore :



Extrait de la première version du tableau des règles de filtrage :

	Source		Destination				
Action	Interface	Source	Interface	Destination	Port	Protocol	Inspection
ZOOM							
Autoriser	LAN	Network_internals	ANY	Internet	zoom	Any	IPS
TEAMVIEWER							
Autoriser	LAN	Network_internals	ANY	Internet	teamviewer		IPS
NETWORK_APPLIANCE_TRAFIC							
Autoriser	LAN	Network_internals	WAN	Any	ssh		IPS
Autoriser	LAN	Network_internals	LAN	Any	netbios-ns		IPS
Autoriser	LAN	Network_internals	LAN	Any	netbios-dgm		IPS
Autoriser	LAN	Network_internals	LAN	Any	netbios-ssn		IPS
Autoriser	LAN	Network_internals	ANY	Any		ICMP	IPS
Autoriser	LAN	Network_internals	WAN	LOCAL-SERVER_CHAILLOT	microsoft-ds		IPS
Autoriser	LAN	Network_internals	LAN	Network_internals	snmp		IPS
Autoriser	LAN	Network_internals	LAN	Network_internals	ipp		IPS
Autoriser	LAN	Network_internals	LAN	Network_internals	printer		IPS
AWS							
Autoriser	LAN	Network_internals	WAN	AWS-STREAMCORE	http, https		IPS
Autoriser	LAN	Network_internals	WAN	AWS-AUTH_SERVER	http, https		IPS
Autoriser	LAN	Network_internals	WAN	AWS-SECOIA_SERVER	http, https		IPS
Autoriser	LAN	Network_internals	WAN	AWS-SUADEO	http, https		IPS
Autoriser	LAN	Network_internals	WAN	AWS-PHOTOTHEQUE	http, https		IPS
Autoriser	LAN	Network_internals	WAN	AWS-GFIpep	any		IPS
Autoriser	LAN	Network_internals	WAN	AWS-RDP_SECURE	any		IPS
Autoriser	LAN	Network_internals	WAN	AWS_VIRTUALIA	any		IPS
Autoriser	LAN	Network_internals	WAN	AWS-FILE_SERVER	microsoft-ds		IPS
Autoriser	LAN	Network_internals	WAN	AWS-POCERT	ssh, microsoft-ds		IPS
Autoriser	LAN	Network_internals	WAN	AWS-ZIMBRA_SERVER_PROD	imaps, pop3s, smtp, smtps		IPS
Autoriser	LAN	Network_internals	WAN	LOCAL-DNS	dns, DoT		IPS
WEB							
Autoriser	LAN	Network_internals	ANY	Internet	http		IPS
Autoriser	LAN	Network_internals	ANY	Internet	https		IPS
NTP							
Autoriser	LAN	Network_internals	WAN	LOCAL-NTP	ntp		IPS