Veille technologique - Implémentation d'une infrastructure réseau (Pack-a-Node)

420-1SH-SW

13 Juin 2025

Par Ariane Courcy

Remise à M. Nicolas Bourré

Table des matières

Introduction

Dans un monde où les cyberattaques sont de plus en plus fréquentes, la cybersécurité est devenue une priorité absolue pour les entreprises et organisations. Selon une enquête menée, en 2024, par l'Autorité canadienne pour les enregistrements Internet (CIRA) on dit que 43% des gestionnaires en cybersécurité ont changé leur façon de répondre aux cyberattaques de grande envergure[^1].

Just over 4-in-10 (43%) say their organization has made changes to its cybersecurity approaches in response to news about major cyber attacks.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2024	2024	2024	2024	2023	2024
	500	368	99	58	500	500
	%	%	%	%	%	%
Yes	43	39	51	45	38	43
No	50	55	37	43	53	50
Prefer not to answer	1	1	2	3	2	1
Don't know	5	4	10	9	7	5

Cette enquête met en lumière l'importance des mesures de sécurité robustes pour protéger le réseau et les données. L'un des éléments clés de ces mesures est la mise en place d'un pare-feu, qui est un système de

sécurité qui contrôle le trafic réseau. La segmentation réseau, qui consiste à diviser un réseau en segments isolés, est aussi essentielle pour limiter la propagation des attaques. La combinaison de ces deux mesures renforce la sécurité et les actifs numériques des organisations.

> Sur un plan personnel, j'ai choisi ce projet pour sa capacité à effectuer des tests sur le long terme. En effet, il est essentiel d'avoir une bonne structure réseau pour protéger l'établissement. Mon objectif est donc de créer une infrastructure réseau simplifiée et efficace, capable de répondre aux besoins de l'établissement et de garantir la sécurité des données. Je souhaite ainsi évaluer les performances et la sécurité de cette infrastructure et identifier les domaines d'amélioration. Je reproduirai la structure du département de Techniques de l'informatique pour faciliter la structure du projet. Aussi, j'aurais aimé pousser plus loin lors du cours de réseau, j'aime apprendre en profondeur ce qui n'était pas le but du cours de réseau. Donc, j'ai l'occasion de m'épanouir dans ce projet.

Explication du projet

Glossaire [^2]

VLANs: les VLAN (Virtual Local Area Networks) sont des réseaux locaux virtuels qui permettent de diviser un réseau physique en plusieurs réseaux logiques indépendants. Cela permet d'améliorer la sécurité, la gestion et la flexibilité du réseau.

Switch: une switch est un appareil réseau qui connecte plusieurs ordinateurs ou périphériques dans un réseau local. Il reçoit les paquets de données provenant d'un périphérique et les transmet à la destination appropriée.

WAN: un WAN (Wide Area Network) est un réseau étendu qui couvre une grande zone géographique, telle qu'une ville, un pays ou même le monde entier. Les WAN sont souvent utilisés pour relier plusieurs réseaux locaux entre eux.

Pare-feu: un pare-feu est un système de sécurité qui contrôle et filtre les communications entre un réseau et l'extérieur. Il bloque les accès non autorisés et protège le réseau contre les attaques et les menaces, telles que les virus, les chevaux de Troie et les hackers.

Objectif

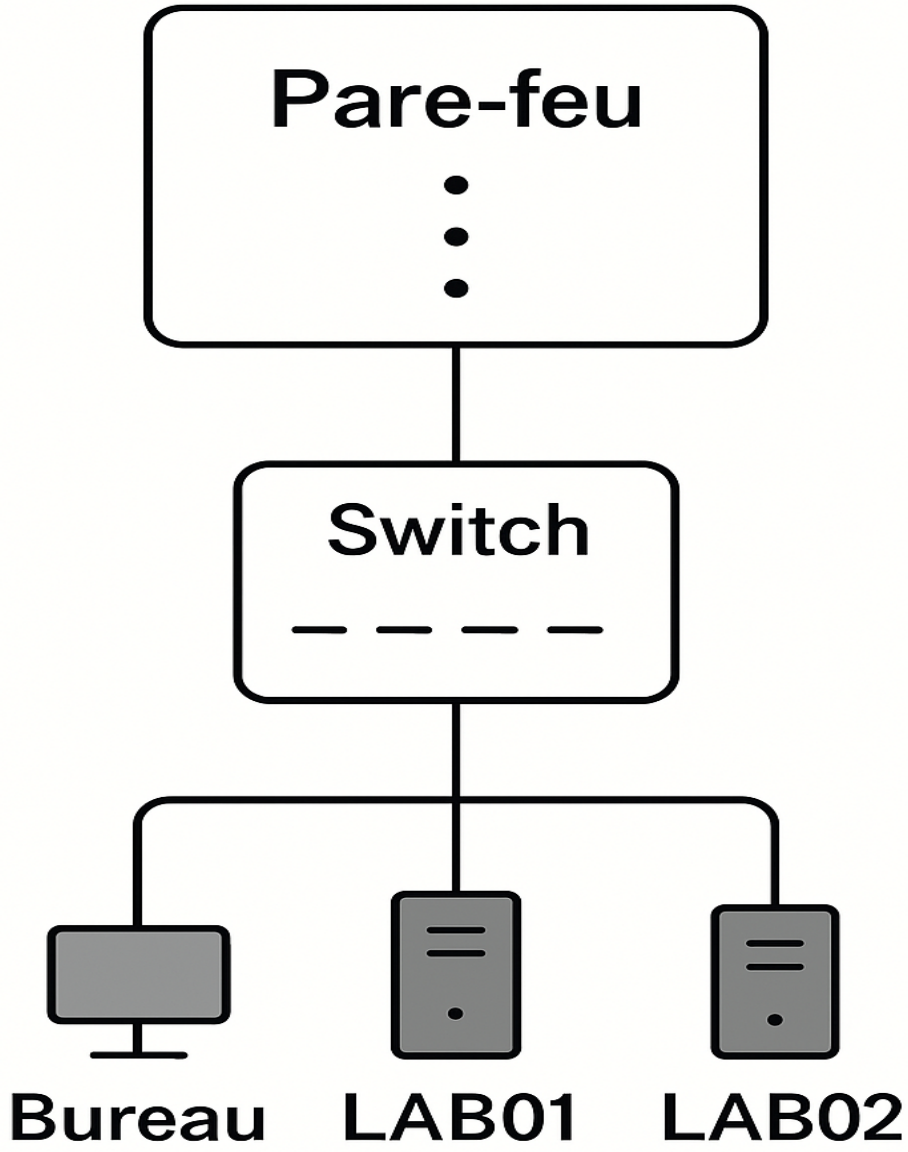
L'objectif de ce projet est de mettre en place une infrastructure réseau simplifiée pour expérimenter. Pour y parvenir, nous utiliserons un pare-feu qui offre une sécurité avancée et une gestion du trafic réseau efficace, et une *switch* configurable qui est connue pour sa fiabilité et sa facilité de configuration. Nous allons avoir une connectivité Internet sur le pare-feu, puis nous allons mettre en place une segmentation réseau de base pour isoler les différents segments de réseau. Les interfaces seront configurées pour recréer l'infrastructure du département de Techniques de l'informatique et garantir la sécurité et la fiabilité des communications.

Planification

La configuration du pare-feu impliquera la définition des paramètres de connexion WAN et la configuration des interfaces réseau. Ensuite, nous configurerons la *switch* pour connecter les différents segments de réseau et définir les paramètres de commutation. La dernière étape sera d'ajouter les règles sur le pare-feu pour segmenter les différents segments de réseau. À la fin de ce projet, nous aurons mis en place une infrastructure réseau simple et sécurisée qui nous permettra de tester et d'évaluer les performances de nos

équipements et de nos configurations réseau, et de garantir la sécurité et la fiabilité de nos réseaux informatiques.

Notre infrastructure réseau comportera un pare-feu qui sera connecté à une *switch* pour étendre les réseaux virtuels (vlans) et garantir la sécurité des communications. Les vlans seront configurés pour séparer les différents locaux, la switch sera utilisée pour tester la communication entre les interfaces. Nous aurons trois interfaces réseau : un bureau qui servira d'interface de gestion, une pour le laboratoire un et une pour le laboratoire deux [^3].



Explication des fonctionnalités

Choix des technologies

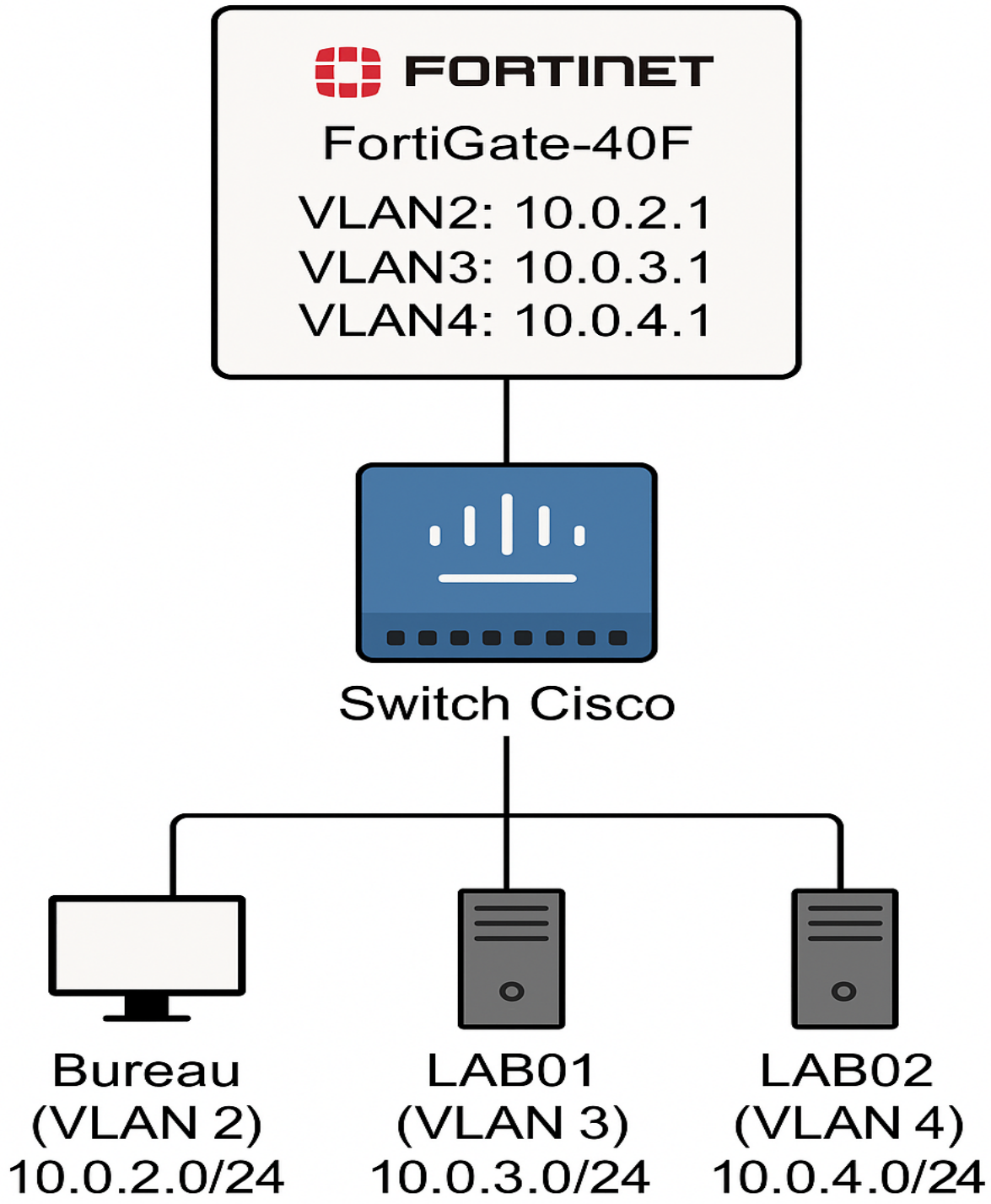
Notre infrastructure réseau sera équipée d'un pare-feu Fortigate-40F, qui offre une sécurité réseau robuste et une grande flexibilité de configuration. Nous avons choisi ce modèle pour sa disponibilité et son adaptabilité aux besoins de petites entreprises, qui nécessitent une sécurité réseau efficace sans les coûts et la complexité associés aux solutions plus grandes. Nous n'aurons malheureusement pas les ressources et le temps de tout configurer dans ce projet.

Notre infrastructure réseau sera également équipée d'une *switch* Cisco 8 ports, qui offre une grande flexibilité et une facilité de configuration. Nous avons choisi ce modèle pour sa simplicité de mise en œuvre et sa capacité à gérer les communications entre les différents équipements de notre réseau. De plus, sa facilité de configuration nous permettra de mettre en place rapidement et facilement les paramêtres de gestion de réseau nécessaires pour protéger notre infrastructure.

Au lieu d'utiliser des zones de sécurité sur le Fortigate, nous avons choisi de configurer des VLANs (Virtual Local Area Networks) pour séparer les différents réseaux et améliorer la sécurité de notre infrastructure. Les VLANs nous permettent de créer des réseaux virtuels isolés les uns des autres, ce qui réduit les risques de propagation des attaques et des menaces. De plus, la configuration des VLANs est plus simple et plus intuitive que la configuration des zones, ce qui nous permet de gérer plus facilement les paramètres de sécurité et de réseau.

Notre infrastructure réseau comportera trois VLANs : un pour le bureau et deux pour les laboratoires[^4].

- VLAN2: Bureau - 10.0.2.0/24
- VLAN3: LAB01 - 10.0.3.0/24
- VLAN4: LAB02 - 10.0.4.0/24



Le bureau sera en mesure de surveiller et de gérer les laboratoires, mais les laboratoires seront isolés les uns des autres et ne pourront pas se voir. De même, les laboratoires ne pourront pas accéder au bureau, ce qui permettra de maintenir une séparation stricte entre les différents environnements de travail.

Implémentation

Pour toute l'implémentation, la documentation existante était incomplète, ce qui a nécessité une exploration approfondie pour comprendre les configurations requises. Une exploration a donc été menée pour combler les lacunes de la documentation et découvrir les meilleures pratiques pour l'infrastructure. Cette exploration a

permis de créer des documentations détaillées et précises pour les futures configurations, ce qui facilitera la mise en œuvre et la gestion de l'infrastructure.

Voici une liste des documentations qui ont été créées:

- Activation du WAN
- Création d'un VLAN
- Configuration de la *switch* Cisco
- Implémentation des règles de pare-feu

Cette règle de trafic est un exemple de la façon dont la segmentation réseau peut être utilisée pour contrôler les communications entre les différents réseaux virtuels et garantir la sécurité de l'infrastructure. En créant des règles de trafic personnalisées, il est possible de contrôler les communications entre les VLANs et de garantir que les utilisateurs n'accèdent qu'aux ressources nécessaires pour leur travail.

Malgré tout, les documentations officielles[^5] [^6] ont été explorées pour faciliter la compréhension de l'environnement.

Autres technologies

À la place de Fortigate, des solutions telles que Juniper SRX, Check Point Next Generation Firewall ou Palo Alto Networks Firewall pourraient être utilisées pour offrir des fonctionnalités de sécurité réseau avancées. Ces solutions proposent des capacités de détection et de prévention des menaces, ainsi que des fonctionnalités de gestion de réseau et de sécurité.

Pour la commutation, des *switchs* de marque HP, Dell ou Netgear pourraient être utilisées à la place de Cisco. Ces switchs offrent des fonctionnalités de commutation Gigabit Ethernet, des capacités de gestion de réseau et des fonctionnalités de sécurité, telles que la gestion des accès et la détection des intrusions.

D'autres alternatives pourraient également être considérées, telles que les solutions de sécurité réseau de Sophos, de WatchGuard ou de SonicWall, qui offrent des fonctionnalités de sécurité avancées et des capacités de gestion de réseau. Les choix de ces alternatives dépendraient des besoins spécifiques de l'infrastructure et des exigences de sécurité de l'organisation.

Difficultés

Malheureusement, le manque de documentation sur le projet a entraîné une quantité importante de recherches non prévues, ce qui a considérablement allongé le temps de réalisation. En conséquence, le temps a manqué pour expérimenter davantage et pour approfondir certaines aspects du projet, ce qui a limité la portée des résultats obtenus.

De plus, les caractéristiques physiques des appareils utilisés pour le projet ont également posé des problèmes, car elle a empêché de travailler à certains moments, notamment lorsqu'il était nécessaire de déplacer ou de reconfigurer les équipements. Cela a entraîné des retards et des interruptions dans le travail, ce qui a encore réduit le temps disponible pour expérimenter et pour améliorer les résultats.

Ces difficultés ont mis en évidence l'importance de disposer d'une documentation complète et à jour, ainsi que de la flexibilité et de la mobilité des équipements physiques, pour garantir la réussite d'un projet de ce type.

Conclusion

En conclusion, ce projet a démontré l'importance d'une bonne infratructure réseau pour garantir la sécurité et la fiabilité des communications. Le pare-feu et la *switch* Cisco ont été configurés pour créer une infrastructure réseau sécurisée et flexible, capable de gérer les communications entre les différents réseaux virtuels.

Il est important de noter que les possibilités de configuration du pare-feu et de la *switch* Cisco sont quasi infinies, et que nous n'avons expérimenté ici que quelques-unes des nombreuses fonctionnalités disponibles. Le pare-feu permet de nombreuses choses, telles que la détection et la prévention des intrusions, la gestion des accès, la mise en place de règles de trafic, etc.

L'importance d'une bonne infrastructure réseau ne doit pas être négligée, car elle est essentielle pour garantir la sécurité et la fiabilité des communications. Une infrastructure réseau bien conçue et bien configurée peut aider à prévenir les attaques et les pertes de données, et à garantir que les utilisateurs ont accès aux ressources nécessaires pour leur travail.

En résumé, ce projet a démontré l'importance de la planification et de la configuration d'une infrastructure réseau pour garantir la sécurité et la fiabilité des communications. Il est essentiel de prendre en compte les besoins et les exigences de l'organisation pour concevoir et configurer une infrastructure réseau qui répond à ces besoins et qui est capable de garantir la sécurité et la fiabilité des communications.

Ce projet servira de test pour notre Cégep afin d'avoir un environnement pour expérimenter.

Médiagraphie

[^1]: CIRA. (2024). CIRA 2024 Cybersecurity Report. Récupéré de https://www.cira.ca/uploads/2024/09/CIRA-2024-Cybersecurity-Report.pdf, Consulté le 8 juin 2025

[^2]: DuckGo, Prompt: duck.ai/prompt, Duck.ai, Llama 3.3 70B Model, https://duckduckgo.com, Généré le 12 juin 2025

[^3]: Microsoft, Prompt: https://copilot.microsoft.com/shares/4TRTwPKWooDKMSSNtdHiA, Copilot, Version Web (aucune version précise), https://copilot.microsoft.com/, Généré le 12 juin 2025

[^4]: OpenAI, Prompt: https://chatgpt.com/share/68487cf6-bfc0-8008-b970-63f259c72cd0, ChatGPT, Version GPT-4o mini, https://chatgpt.com/, Généré le 10 juin 2025

[^5]: Fortinet. (2022). FortiGate Administration Guide (Chapitre 5 : Configuration du pare-feu), Récupéré de https://docs.fortinet.com/, Consulté le 26 mai 2025

[^6]: Cisco Systems, Inc. (2022). CCNA Routing and Switching. Récupéré de https://www.netacad.com/, Consulé le 26 mai 2025