Centre de la sécurité des télécommunications Canada
Communications Security Establishment Canada

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Considérations de sécurité pour le protocole Internet version 6

Gestionnaires

TLP:CLEAR

Canada

Avant-propos

La présente publication est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Pour de plus amples renseignements, veuillez communiquer avec le Centre pour la cybersécurité :

- Courriel : contact@cyber.gc.ca
- Téléphone : 613-949-7048 ou 1-833-CYBER-88

Date d'entrée en vigueur

Le présent document entre en vigueur le 10 octobre 2025.

Historique des révisions

Révision	Modifications	Date
1	Première version.	10 octobre 2025

D97-4/80-003-2025F-PDF
ISBN 978-0-660-78182-2

Vue d'ensemble

La croissance exponentielle de l'utilisation des technologies Internet pour offrir des services et des applications modernes est liée à l'épuisement de la disponibilité mondiale des adresses du protocole Internet version 4 (IPv4 pour Internet Protocol version 4). Le système d'adressage du protocole Internet version 6 (IPv6) a été conçu par l'Internet Engineering Task Force (IETF) afin de remplacer le protocole IPv4, tout en offrant un nombre considérablement plus élevé de blocs d'adresses privées et publiques pour appuyer les besoins des entreprises et d'autres entités modernes. Le déploiement de terminaux IPv6 en parallèle à une infrastructure IPv4 existante est devenu une stratégie courante dans les réseaux d'entreprise. Bien que le protocole IPv6 offre plusieurs améliorations de sécurité par rapport à IPv4, l'exécution d'architectures à double pile introduit de nouveaux risques qui doivent être gérés de manière appropriée.

Pour assurer l'évolution continue de l'architecture liée à ses services, le gouvernement du Canada (GC) devra concevoir de nouvelles architectures réseau et migrer son infrastructure numérique existante pour prendre en charge IPv6. Dans le cadre de cette stratégie, les services intégrant IPv6 devront être conçus pour coexister de manière sécurisée avec l'infrastructure IPv4 jusqu'à ce qu'une architecture d'entreprise entièrement IPv6 soit déployée. L'introduction d'IPv6 au sein de l'infrastructure du GC ne devrait pas toucher directement les utilisatrices et utilisateurs ni les services frontaux, ou très peu. Toutefois, les ministères du GC se doivent d'examiner et d'évaluer les implications de l'utilisation d'IPv6 sur leurs services et leurs objectifs de sécurité.

La présente publication souligne les considérations de sécurité essentielles pour les déploiements d'IPv6 dans les réseaux du GC. Les ministères du GC devront ainsi concevoir des plans de transition afin de prendre en charge IPv6 tout en atténuant les risques liés aux opérations et à la sécurité qui en découlent.

Table des matières

1 Introduction 6
1.1 Protocole Internet version 6 7
1.2 Améliorations apportées au protocole Internet version 6 8
1.2.1 Prise en charge du protocole IPsec 8
1.2.2 Configuration automatique 8
1.2.3 Découverte de voisin 8
1.2.4 Sécurité du protocole DHCP 8
1.2.5 En- têtes d'extension 8
1.2.6 Absence d'adresses de diffusion 8
1.3 Enouncé du problème 8
1.4 Contexte de menace 9
1.4.1 Tunnellisation de protocole 9
1.4.2 Attaques par déni de service distribué 9
1.4.3 Commande et contrôle 9
1.4.4 Mauvaises configurations de périphérique réseau 9
1.4.5 Découverte de service réseau 10
2 Considérations liées à la sécurité 11
2.1 Risques relatifs à la migration 11
2.2 Approvisionnement et tests 11
2.3 Architecture cible 12
2.4 Applications patrimoniales 12
2.5 Tunnels non autorisés 12
2.6 Configurations par défault 13
2.7 Flux de trafic IPV6 non autorisés 13
2.8 Outils de surveillance et de gestion 13
2.9 Système d'adressage 14
2.10 Prise en charge d'adressage multiple 14
2.11 Protocole DHCP pour IPv6 14
2.12 Protections concernant la configuration automatique d'adresse 15
2.13 Environnements à double pile 15
2.14 Protection du plan de données et du plan de gestion 16
2.15 Messages de découverte de voisin 16
2.16 Risques liés à la traduction d'adresse 16

2.17 Architecture à vérification systématique 17
2.18 Connaissances techniques et opérationnelles 17
3 Conclusion 18

Liste des tableaux

Tableau 1 : Comparaison entre le protocole Internet version 6 et le protocole Internet version 4 7

1 Introduction

Le GC s'appuie sur des systèmes numériques en réseau pour la prestation de services essentiels aux Canadiennes et Canadiens. Les technologies de mise en réseau continuent d'évoluer en raison des exigences en matière d'infrastructure numérique nécessaires pour appuyer la connectivité des services modernes. Bien que l'utilisatrice canadienne ou utilisateur canadien typique n'ait pas besoin de savoir quelle pile IP appuie les services, on s'attend à ce que l'infrastructure des services numériques du GC soit en mesure de traiter les demandes de service à partir d'appareils intégrant IPv6 ou IPv4. Puisque les réseaux et les services du GC sont développés pour traiter la pile technologique IPv6, les principales parties prenantes doivent évaluer les risques et les répercussions de l'adoption du protocole IPv6 dans leur réseau d'entreprise, notamment les risques de sécurité associés à la mise en œuvre d'une architecture à double pile (IPv4 et IPv6).

Les systèmes et les applications modernes présentent une prise en charge variable du protocole IPv6. Parfois, le protocole est disponible par défaut; d'autres fois, des personnalisations uniques à un fournisseur sont mises en œuvre, ce qui peut mener à des défis en matière d'interopérabilité. Un tel contexte peut ainsi exposer les réseaux d'entreprise à des risques de sécurité importants, augmenter les possibilités de mauvaise configuration et mener à des contrôles de sécurité incomplets.

En 2013, le Secrétariat du Conseil du Trésor du Canada (SCT) a également publié la Ligne directrice sur l'achat d'équipement pour le réseau de la version 6 du protocole Internet (IPv6) à titre de document complémentaire à sa stratégie d'adoption. La ligne directrice visait à aider les ministères du GC à mieux comprendre les exigences techniques pour l'achat d'équipement réseau (par exemple, les routeurs, les dispositifs de surveillance de réseau, les serveurs mandataires et les pare-feu) afin de s'assurer que les capacités IPv6 sont évaluées dans le cadre des processus d'approvisionnement des systèmes. Toutefois, ni la stratégie ni la ligne directrice sur l'achat d'équipement ne sont parvenues à traiter convenablement les questions de sécurité associées à IPv6.

Bien que certaines sections de l'architecture numérique ministérielle existante soient en mesure de prendre en charge le protocole IPv6, sans un cadre sécurisé pour la mise en œuvre, des risques de sécurité pourraient être introduits par inadvertance dans l'environnement d'entreprise. Les ministères ne doivent pas présumer que l'activation de la prise en charge du protocole IPv6 peut s'effectuer simplement au moyen d'un bouton.

Selon les spécifications du protocole IPv6, l'adressage IPv6 doit par défaut avoir la priorité sur l'adressage IPv4. Bien que les applications d'entreprise n'utilisent pas forcément le protocole IPv6, il se peut que les normes définies relatives aux spécifications et les configurations par défaut mises en œuvre permettent les communications avec des adresses locales IPv6. Par exemple, Microsoft1 ne recommande pas de désactiver la prise en charge du protocole IPv6 dans les environnements d'exploitation Windows, même si l'adressage IPv6 n'est pas utilisé. Pour évaluer ce cas, et d'autres problèmes du genre, le Centre pour la cybersécurité recommande aux ministères du GC d'examiner les flux réseau IPv6 au sein de leur environnement et de corriger les lacunes dans leurs outils de surveillance de la sécurité des réseaux avant de procéder à la mise en œuvre. L'activation des flux de trafic IPv6 sans une surveillance adéquate de la visibilité du réseau et sans mesures de protection appropriées liées au filtrage réseau peut augmenter la surface d'attaque des entreprises et exposer le réseau à des risques de sécurité supplémentaires.

[1] Instructions relatives à la configuration d'IPv6 dans Windows pour les utilisateurs avancés : https://learn.microsoft.com/fr-ca/troubleshoot/windows-server/networking/configure-ipv6-in-windows.

1.1 Protocole Internet version 6

Le protocole IP est le principal protocole de communication d'Internet; il précise comment les paquets réseau doivent être transportés entre les frontières réseau. Il s'agit d'un composant de la couche réseau dans le modèle de référence d'interconnexion de systèmes ouverts, un cadre servant à organiser les protocoles de communication et à partager de l'information sur l'Internet public.

L'adressage IPv6 vise à remplacer l'adressage IPv4 et comprend certaines améliorations aux fonctions opérationnelles et de sécurité. Il existe des différences entre IPv6 et IPv4, qui ont des conséquences sur les conceptions d'architecture réseau. La norme IPv6 est un système d'adressage réseau de 128 bits qui fournit un espace d'adressage considérablement plus grand comparativement à IPv4 (qui utilise un système d'adressage de 32 bits). Par défaut, IPv6 n'est pas rétrocompatible avec IPv4. Ainsi, les administratrices et administrateurs réseau devront peut-être mettre en œuvre des changements dans leurs architectures réseau existantes.

Le tableau 1 ci-dessous présente quelques différences entre les protocoles IPv4 et IPv6.

Tableau 1 : Comparaison entre le protocole Internet version 6 et le protocole Internet version 4

Composants du protocole	Protocole Internet version 4	Protocole Internet version 6
Espace adresse et notation	• Espace adresse de 32 bits, donc offre un espace d'adressage limité pour les cas d'utilisation privés et publics • Notation d'adresse constituée de chiffres séparés par un point, par exemple 192.168.0.1	• Espace adresse de 128 bits, donc permet jusqu'à 2^128 adresses réseau uniques (environ 340 billions) • Notation d'adresse constituée de huit valeurs hexadécimales séparées par les deux points, par exemple 2001:0DB8:0000:0000:0000:000A:09C0:00B4
Fonctions de sécurité	Protocole ne prenant pas en charge nativement l'authentification et les fonctions de sécurité	Prise en charge native de l'authentification, de l'intégrité des données et de la confidentialité des données (par exemple, prise en charge d'IPsec [protocole de sécurité pour IP])
Types	Prise en charge de l'adressage statique public et privé pour la gestion des réseaux; toutefois l'espace adresse est limité	• Prise en charge de l'adressage statique privé et le routage public pour la gestion des périphériques réseau • Adresse réseau typique composée de sections et d'identificateurs (préfixe de routage mondial, identificateur de sous-réseau local et identificateur d'interface)
Distribution d'adresse	Configuration automatique non prise en charge; nécessiterait une affectation statique des adresses IP ou au moyen du protocole de configuration d'hôte dynamique (DHCP)	Configuration automatique permise (configuration d'adresse sans état), allégeant le besoin d'affectation d'adresse par un serveur DHCP. La configuration automatique repose sur

		l'information du routeur pour les adresses réseau afin d'accéder aux services réseau

1.2 Améliorations apportées au protocole Internet version 6

La norme de spécification IPv6 propose certaines améliorations par rapport à IPv4. Les sous-sections suivantes fournissent de l'information supplémentaire sur les améliorations de sécurité.

1.2.1 Prise en charge du protocole IPsec

IPsec est une suite de protocoles pouvant servir à l'authentification, au chiffrement et aux mesures de protection de l'intégrité. Bien qu'il soit possible d'utiliser le protocole IPsec à titre d'extension rétroactive dans IPv4, IPv6 prend en charge IPsec, qui est intégré à la norme. Il convient de noter que le protocole IPsec n'est plus obligatoire en IPv6, tel qu'il est énoncé dans le document RFC 8504[2].

1.2.2 Configuration automatique

La configuration automatique permet à un nœud de s'attribuer automatiquement une adresse réseau IPv6 en fonction de l'information de préfixe réseau présentée par le routeur. Pour ce faire, le mécanisme de configuration automatique d'adresse sans état (SLAAC pour Stateless Address Autoconfiguration) est utilisé.

1.2.3 Découverte de voisin

Le protocole de découverte de voisin remplace le protocole de résolution d'adresse utilisé par les réseaux IPv4 afin de fournir des options de chiffrement pour des messages de découverte sécurisés.

1.2.4 Sécurité du protocole DHCP

Le protocole de configuration d'hôte dynamique de IPv6 (DHCPv6) prend en charge l'authentification et le chiffrement des messages DHCP au moyen du protocole IPsec dans le but de prévenir les possibilités d'écoute clandestine et d'attaque par interception de message.

1.2.5 En- têtes d'extension

Les en-têtes d'extension IPv6 peuvent servir à améliorer la sécurité, au débogage et aux fonctions de gestion.

1.2.6 Absence d'adresses de diffusion

La norme IPv6 a aboli l'utilisation des adresses de diffusion et a adopté des adresses multidiffusion à titre de mécanisme principal pour les communications de groupe.

1.3 Enouncé du problème

À mesure que les réseaux d'entreprise évoluent, IPv6 devra inévitablement être pris en charge et géré. Les nouveaux périphériques réseau seront assurément compatibles avec IPv6, qui sera activé par défaut. La priorité sera donc accordée à

[2] IPv6 Node Requirements : https://datatracker.ietf.org/doc/html/rfc8504 (en anglais seulement)

son flux de trafic conformément à la norme de spécification. Le déploiement d'appareils IPv6 sans une bonne compréhension, une surveillance adéquate, un renforcement de la sécurité et un déploiement de contrôles d'atténuation mènera à une augmentation de la surface d'attaque de l'entreprise et exposera l'organisme à des risques considérables.

1.4 Contexte de menace

Le présent document est destiné aux systèmes NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B. En général, le Centre pour la cybersécurité recommande aux ministères et organismes du GC de mener une évaluation des menaces et des risques dans le contexte de leurs besoins opérationnels avant l'adoption partielle ou complète d'IPv6. Les organismes doivent tenir compte des sources de menace qui peuvent exploiter les vulnérabilités associées à IPv6. Le Centre pour la cybersécurité évalue que des auteurs de menace dotés de moyens peu sophistiqués (Td3) pourraient cibler les erreurs liées aux mauvaises configurations d'appareil et les appareils exposés par inadvertance afin de s'infiltrer dans les réseaux et maximiser leurs activités criminelles. Les groupes cybercriminels et les auteurs de cybermenace motivés par des gains financiers (Td4 et Td5) pourraient cibler les faiblesses de mise en œuvre de conception et les vulnérabilités d'appareil liées à IPv6[3]. Les auteurs de menace parrainés par un État (Td6 et niveaux supérieurs), en plus de leurs tactiques de faible niveau, peuvent cibler les faiblesses des spécifications du protocole IPv6 et les vulnérabilités d'intégration de système afin d'atteindre des objectifs stratégiques plus vastes. Les mesures d'atténuation des menaces avancées parrainées par des États sont considérées comme ne faisant pas partie de la portée de la présente publication.

La section suivante présente certaines menaces informatiques (attaques) identifiées qui pourraient s'appliquer aux environnements IPv6 :

1.4.1 Tunnellisation de protocole

Les auteurs de menace peuvent encapsuler des paquets réseau dans un autre protocole ou encore créer plusieurs tunnels au moyen d'un périphérique réseau afin d'éviter les mesures de détection. Par exemple, un périphérique réseau peut permettre à un auteur de menace d'intégrer des paquets IPv6 non autorisés à des tunnels IPv4 afin d'éviter ou de contourner les contrôles de filtrage réseau. De plus, les auteurs de menace peuvent lancer des attaques par mystification à l'aide de techniques d'injection de tunnel, où un paquet encapsulé valide est falsifié (en fonction des connaissances partielles des points d'extrémité du tunnel et du protocole d'encapsulation)[4].

1.4.2 Attaques par déni de service distribué

Les auteurs de menace peuvent utiliser les capacités du protocole IPv6, comme les messages multidiffusion ou les en-têtes d'extension, afin de lancer des attaques par déni de service distribué (DDoS) dans le but de surcharger les systèmes de défense réseau. Par exemple, un auteur de menace peut utiliser les messages multidiffusion de la couche liaison en IPv6 qui ont été trafiqués pour lancer une attaque par déni de service sur une adresse source ciblée.

1.4.3 Commande et contrôle

Les auteurs de menace peuvent exploiter les améliorations apportées à IPv6 (en-têtes d'extension ou autres améliorations) en intégrant et en communiquant des signaux de contrôle ou des balises malveillantes par l'intermédiaire d'un réseau compromis. Les blocs d'espace d'adressage de plus grande portée du protocole IPv6, accessibles mondialement, sont des cibles attrayantes du point de vue des auteurs de menace pour déployer des canaux de commande et de contrôle.

1.4.4 Mauvaises configurations de périphérique réseau

Les auteurs de menace peuvent exploiter les mauvaises configurations de périphérique réseau ou encore les incohérences de configuration lorsque les filtres de contrôle de l'accès à la passerelle de périmètre ne sont pas mis en œuvre

[3] Évaluation des cybermenaces nationales 2025-2026 https://www.cyber.gc.ca/fr/orientation/evaluation-cybermenaces-nationales-2025-2026
[4] RFC 9099: Operational Security Considerations for IPv6 Networks : https://www.rfc-editor.org/rfc/rfc9099.html (en anglais seulement)

correctement. En particulier, les auteurs de menace peuvent exploiter les périphériques réseau qui exposent des interfaces IPv6 non configurées par défaut afin de contourner les contrôles de sécurité réseau.

1.4.5 Découverte de service réseau

Les messages de découverte de service multidiffusion en IPv6 (par exemple, le protocole DNS multidiffusion [mDNS pour Multicast *DNS*][5] ou le protocole de résolution de nom multidiffusion de liaison locale [LLMNR pour *Link-Local Multicast Name Resolution*][6]) peuvent être mystifiés ou créés de manière à rediriger les points d'extrémité vers une infrastructure contrôlée par l'attaquant. En outre, les auteurs de menace peuvent exploiter les capacités par défaut du protocole IPv6 (par exemple, la découverte de voisin) pour appuyer les activités de reconnaissance (comme l'extraction de données sensibles de périphérique réseau), ce qui peut servir à cibler les vulnérabilités.

[5] Multicast DNS - https://datatracker.ietf.org/doc/html/rfc6762 (en anglais seulement)
[6] Link-Local Multicast Name Resolution (LLMNR) – https://www.rfc-editor.org/rfc/rfc4795.html (en anglais seulement)

2 Considérations liées à la sécurité

Le modèle de sécurité nécessaire aux architectures réseau d'entreprise pour appuyer les appareils IPv6 est différent des mises en œuvre traditionnelles du protocole IPv4. Cette section porte sur les considérations en matière de cybersécurité et les mesures recommandées afin d'atténuer les risques associés à l'utilisation du protocole IPv6 dans un réseau d'entreprise. Les plans de transition vers IPv6 doivent tenir compte des répercussions sur les services opérationnels et la posture de sécurité de l'organisme.

2.1 Risques relatifs à la migration

L'activation du protocole IPv6 modifie les communications réseau et les exigences de surveillance de la sécurité d'un organisme. Par conséquent, une approche systématique tenant compte des plans de transition, des risques d'interopérabilité et des exigences opérationnelles à venir est fortement recommandée. Il se peut que les protocoles IPv4 et IPv6 soient déployés en même temps au cours de la période de transition des organismes. Il est donc essentiel d'évaluer si les infrastructures de sécurité réseau existantes peuvent prendre en charge le protocole IPv6. L'équipe de direction doit s'assurer que les plans de transition vers IPv6 respectent les processus de gestion du changement. Les politiques et procédures du programme de sécurité de niveau organisationnel pourraient devoir être mises à jour, au besoin.

Par ailleurs, l'équipe de direction doit déterminer l'objectif, les échéanciers pour la transition et les voies de migration. Il pourrait s'avérer nécessaire de mettre à jour les politiques de contrôle de sécurité qui gèrent les audits et la surveillance, les exigences d'interconnexion, les mécanismes d'identification et d'authentification des appareils, la protection du périmètre et les interfaces gérées. En général, le Centre pour la cybersécurité recommande d'utiliser le cadre de gestion des risques présenté dans le document La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33) afin d'établir et de gérer les risques de sécurité pour les systèmes d'information.

2.2 Approvisionnement et tests

Les plans de transition vers IPv6 et de mise en œuvre doivent être alignés sur la stratégie d'approvisionnement de l'organisme. L'approvisionnement d'actifs comprenant des fonctions de réseautique doit être évalué en tenant compte de la prise en charge du protocole IPv6. Le National Institute of Standards and Technology (NIST) et le laboratoire sur l'interopérabilité de l'université du New Hampshire (UNH) ont mis au point un programme d'évaluation et de test pouvant faciliter l'évaluation fonctionnelle de produits IPv6. Ce programme tient un registre des appareils et des applications IPv6 qui ont été testés en fonction des exigences techniques du profil de norme IPv6 du gouvernement des États-Unis (profil USGv6-r1)[7] à des fins de performance et de conformité. Le Centre pour la cybersécurité recommande que les organismes adoptent des produits figurant dans le registre du programme USGv6 dans le cadre de leur stratégie d'approvisionnement. Les organismes doivent consulter la déclaration de conformité du fournisseur pour le produit, qui documente les énoncés de capacités IPv6. De plus, ils doivent tester les capacités de l'infrastructure réseau pour appuyer les scénarios de déploiement IPv6 exclusif.

[7] United States Government (USGv6-r1) Profile : https://www.nist.gov/programs-projects/usgv6-program/usgv6-revision-1 (en anglais seulement)

2.3 Architecture cible

L'architecture cible pour l'adoption du protocole IPv6 doit présenter un niveau de risque résiduel acceptable (tolérance au risque) pour l'organisme. Le Centre pour la cybersécurité recommande un plan d'architecture cible menant ultimement à une infrastructure réseau entièrement IPv6 à l'état final. Bien qu'une architecture à double pile (IPv4 et IPv6) puisse être un choix transitoire évident, le Centre pour la cybersécurité recommande de concevoir le plan de transition avec l'objectif d'obtenir une architecture entièrement IPv6 à l'état final. Une architecture à une seule pile (IPv6 exclusivement) à l'état final simplifie la gestion réseau et la surveillance de la sécurité et réduit également les coûts opérationnels globaux.

2.4 Applications patrimoniales

Il se peut que les applications patrimoniales ne prennent pas en charge nativement le protocole IPv6, ce qui les rend incapables de traiter les données de paquets IPv6. La situation peut être particulièrement complexe pour les applications opérationnelles essentielles qui n'offrent pas de mécanismes pour prendre en charge IPv6. Lorsque le protocole IPv6 est activé, les applications patrimoniales ou les contrôles de sécurité qui reposent sur des adresses IPv4 figées dans le code comme noms d'hôte peuvent être touchés. En l'absence de mécanismes adéquats de traduction de trafic, les points d'extrémité exclusivement IPv6 risquent de ne pas être en mesure de se connecter aux services uniquement compatibles avec IPv4 (et vice versa). Le Centre pour la cybersécurité recommande aux organismes d'évaluer l'incidence des plans de transition sur leurs applications logicielles.

Le document Happy Eyeballs[8] Version 2: Better Connectivity Using Concurrency algorithm (en anglais seulement) est une norme proposée par l'IEFT pour la gestion des lancements et des traitements des requêtes DNS asynchrones sur des hôtes à double pile par les applications système. L'algorithme permet aux applications Web de passer de manière transparente entre des réseaux IPv4 et IPv6. Les administratrices et administrateurs réseau devraient donc tester les applications opérationnelles afin de déterminer leurs capacités IPv6. Bien que l'algorithme Happy Eyeballs offre l'avantage de pouvoir gérer les passages entre IPv4 et IPv6, il peut toutefois masquer quelques problèmes réseau. Par conséquent, le fait de pouvoir établir avec succès une connexion sur une application n'est pas nécessairement un indicateur d'un état adéquat pour les réseaux IPv4 ou IPv6 dans un environnement à double pile.

2.5 Tunnels non autorisés

Les organismes doivent mettre en œuvre des contrôles de sécurité réseau pour détecter et bloquer l'utilisation de tunnels de transition IPv6 non autorisés. Les tunnels de transition sont des techniques servant au transport de paquets IPv6 sur une infrastructure réseau IPv4. Les tunnels IPv6 peuvent correspondre à des tunnels manuels ou automatiques, comme ceux fournis par les protocoles Teredo, 6to4[9] ou ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*)[10]. Teredo est un protocole de tunnellisation automatique créé par Microsoft qui utilise la technologie UDP (User Datagram Protocol) pour mettre en tunnel des paquets IPv6 sur des réseaux IPv4. L'IETF a créé le protocole 6to4 afin de fournir une tunnellisation automatique IPv6 sur IPv4 pour interconnecter des réseaux Ipv6, tandis que le protocole ISATAP sert à transmettre des paquets IPv6 entre des nœuds à double pile sur un réseau IPv4. Bien que ces techniques et ces protocoles puissant offrir certains avantages, en particulier lors de la phase de transition, le transport de paquets IPv6 sur une infrastructure IPv4 a toutefois des conséquences sur la sécurité. Par exemple, ces applications de tunnellisation peuvent servir à contourner les stratégies de filtrage réseau. Les organismes doivent ainsi mettre en œuvre des mécanismes afin de bloquer l'utilisation des tunnels automatiques par défaut sur les appareils des utilisatrices et utilisateurs finaux ainsi que sur les dispositifs périphériques (pare-feu et routeurs de bordure). Le Centre pour la cybersécurité recommande l'utilisation de solutions de sécurité qui tiennent compte de la présence de tunnels. Sur les dispositifs périphériques, comme les pare-feu, les

[8] Happy Eyeballs, version 2 : Better Connectivity Using Concurrency : https://datatracker.ietf.org/doc/html/rfc8305 (en anglais seulement)
[9] RFC 6343 Advisory Guidelines for 6to4 Deployment : https://datatracker.ietf.org/doc/html/rfc6343 (en anglais seulement)
[10] Wikipedia : RFC 5214 Intra-site Automatic Tunnel Addressing Protocol (ISATAP) : https://en.wikipedia.org/wiki/ISATAP (en anglais seulement)

organismes doivent refuser par défaut tout le trafic sortant UDP et mettre en œuvre des exceptions pour les services autorisés seulement[11].

2.6 Configurations par défault

Les systèmes d'exploitation et les périphériques réseau modernes prendront vraisemblablement en charge le protocole IPv6 et, en raison des exigences de la norme, celui-ci pourrait être activé par défaut. Par ailleurs, les fonctions de système critiques peuvent également exiger que le protocole IPv6 soit activé. Par exemple, Microsoft ne recommande pas de désactiver la prise en charge du protocole IPv6 sur les appareils utilisant le système d'exploitation Windows, même lorsqu'il n'est pas utilisé [5]. Pour comprendre et évaluer les risques connexes, les organismes doivent évaluer proactivement l'état par défaut du protocole IPv6 sur leurs appareils. Il faut être conscient des risques associés aux configurations par défaut et concevoir des mécanismes de surveillance et de contrôle préventifs afin d'atténuer ces risques. Par exemple, le protocole de tunnellisation 6to4 est activé par défaut sur les serveurs Windows lorsqu'une adresse IPv4 publique est affectée à une interface. Le tunnel affecte et enregistre dynamiquement une adresse IPv6 sur un réseau[12]. Si ce type d'activité n'est pas surveillé, le réseau est exposé à d'importants risques. Les organismes doivent mettre en œuvre des mécanismes visant à retirer les flux de trafic IPv6 non autorisés. Pour atténuer les menaces associées au trafic IPv6 en transit sur le réseau sans qu'il ne soit détecté, le Centre pour la cybersécurité recommande une surveillance proactive basée sur l'hôte pour les communications réseau IPv6, même lorsque l'interface réseau est désactivée. La détection du trafic réseau non autorisé doit être analysée.

2.7 Flux de trafic IPV6 non autorisés

Un manque de visibilité des flux de trafic IPv6 représente des risques importants pour le réseau. Les organismes sans utilisation approuvée du trafic IPv6 doivent s'assurer que les flux de trafic IPv6 sont filtrés sur les coupe-feu et les routeurs de bordure conformément à leurs stratégies de réseau. Un réseau ayant déployé le protocole IPv6 ne devrait permettre que le trafic IPv6 qui est autorisé par la stratégie. De plus, il sera nécessaire d'utiliser une liste de contrôle d'accès (LCA) afin de ne permettre que les flux de trafic et les protocoles autorisés et de bloquer tous les autres éléments par défaut. Lors du déploiement du protocole IPv6, selon le cas d'utilisation opérationnel, il pourrait être nécessaire de mener une évaluation des menaces et des risques (EMR) dans le but de déterminer et d'atténuer les risques connexes. Dans certaines situations, il pourrait s'avérer impossible de désactiver entièrement la fonctionnalité IPv6, même sans cas d'utilisation opérationnel. Par exemple, Microsoft ne recommande pas de désactiver IPv6 sur Windows, car certains composants ont besoin du protocole pour fonctionner convenablement. Le Centre pour la cybersécurité recommande de mener une évaluation des risques afin de cerner les mesures de protection opérationnelles et de sécurité qui pourraient atténuer les risques connexes. En général, désactiver IPv6 est recommandé, sauf s'il existe un besoin opérationnel approuvé de l'utiliser sur le réseau d'entreprise [5].

2.8 Outils de surveillance et de gestion

Les outils de gestion et de surveillance réseau exigent une mise à niveau importante pour le traitement et la prise en charge du trafic réseau IPv6. Les outils de surveillance de la sécurité réseau et de production de rapports, comme les systèmes de détection et de prévention d'intrusion, l'agrégation des journaux (au moyen d'un système de gestion des informations et des événements de sécurité [GIES]), les scanneurs de vulnérabilité et les outils de gestion de correctifs, doivent prendre en charge le protocole IPv6 afin d'assurer une conformité continue aux politiques de sécurité organisationnelles. Le Centre pour la cybersécurité recommande aux organismes, en priorité, de tester différents scénarios de surveillance réseau (double pile, IPv6 exclusivement) dans le cadre de leur stratégie de transition vers le protocole IPv6. De plus, des scénarios de test personnalisés devraient être développés dans le but de valider la prise en charge du protocole IPv6 pour les activités liées au développement de logiciel et de service d'entreprise.

[11] RFC 9099: Operational Security Considerations for IPv6 Networks : https://www.rfc-editor.org/rfc/rfc9099.html (en anglais seulement)
[12] Instructions relatives à la configuration d'IPv6 dans Windows pour les utilisateurs avancés :https://learn.microsoft.com/fr-ca/troubleshoot/windows-server/networking/configure-ipv6-in-windows.

2.9 Système d'adressage

Un système d'adressage IPv6 robuste améliore la sécurité du réseau tout en fournissant la flexibilité de prendre en charge les services opérationnels et d'atténuer les menaces de fuite d'information. Les organismes devraient prendre en compte l'architecture actuelle de leur réseau ainsi que leurs besoins à venir lors de la sélection d'un plan d'adressage IPv6. En fonction de la complexité et des interdépendances des réseaux et des applications modernes, nous recommandons un plan d'adressage qui adopte une approche par phases et incrémentielle pour la transition vers IPv6. Un système de gestion des adresses IP est essentiel pour une gestion efficace du plan d'adressage. Les organismes devraient prendre en considération les applications opérationnelles et les stratégies de sécurité lors de la sélection d'un système d'adressage. Le plan d'adressage peut également servir à améliorer la posture de sécurité d'un organisme, à titre de moyen de base pour séparer les réseaux, tout en appliquant les principes de vérification systématique pour la segmentation et la ségrégation réseau. Si vous envisagez des adresses locales uniques (ULA), celles-ci doivent être générées au moyen d'algorithmes pseudo-aléatoires approuvés et être filtrées aux frontières du réseau. De plus, ces adresses ne doivent pas être exposées au-delà du réseau interne. Bien que les adresses locales uniques offrent certains avantages pour les déploiements IPv6, nous ne les recommandons pas pour les environnements à double pile. Pour que les adresses locales uniques soient efficaces dans un déploiement à double pile, il pourrait être nécessaire de mettre à jour les valeurs d'étiquettes et de priorité de la table des politiques de sélection d'adresse sur tous les appareils sur le réseau, ce qui introduit des complications opérationnelles supplémentaires et complexifie les processus de sécurité et de gestion réseau.

2.10 Prise en charge d'adressage multiple

Une seule interface IPv6 peut détenir plusieurs adresses[13], telles qu'une adresse de bouclage d'interface, une adresse locale de liaison, une adresse locale unique ou encore une adresse pouvant être acheminée partout dans le monde. Par défaut, une adresse locale de liaison est affectée à une interface réseau avec IPv6. L'adressage multiple offre des avantages à la fois sur le plan de la sécurité et sur le plan opérationnel. Toutefois, une telle prise en charge peut complexifier l'application des stratégies de surveillance et de filtrage réseau, en particulier si les stratégies de filtrage ne sont pas suffisamment robustes. Elle augmente donc l'exposition aux menaces et pourrait permettre à des auteurs de menace d'éviter les règles de détection de trafic réseau. Le Centre pour la cybersécurité recommande aux administratrices et administrateurs de système de mettre en œuvre des restrictions pour les changements non autorisés aux adresses IPv6 et de s'assurer de mettre en place des contrôles de surveillance afin de prévenir et de détecter les modifications. Dans le but d'atténuer les menaces associées au contournement des stratégies de sécurité réseau, il est nécessaire de mettre en œuvre une stratégie de type « refus par défaut » pour s'assurer que le trafic entrant et sortant d'une interface est bloqué aux frontières du réseau, à l'exception du trafic qui est explicitement autorisé par les stratégies de sécurité réseau de l'organisme.

2.11 Protocole DHCP pour IPv6

La plupart des réseaux d'entreprise utilisent le protocole DHCP pour la distribution de l'information d'adressage IP sur le réseau. En IPv6, DHCP version 6 (DHCPv6)[14] prend en charge l'adressage avec et sans état pour les périphériques réseau. Comme le protocole DHCP traditionnel, DHCPv6 est exposé à une variété d'attaques, comme les attaques par interception malveillante de message, par mystification et par déni de service distribué. Pour les réseaux d'entreprise utilisant DHCPv6, le Centre pour la cybersécurité recommande de protéger les messages réseau DHCP en utilisant le protocole IPsec et le chiffrement [6]. En outre, le Centre pour la cybersécurité recommande d'établir des mécanismes d'authentification entre les serveurs HCP, les hôtes de relais et les points d'extrémité client. Les organismes doivent également mettre en œuvre des mesures de protection supplémentaires, comme DHCPv6 Guard[15], afin de bloquer les réponses DHCP malveillantes et les messages d'annonce de la part de périphériques réseau non autorisés. Les organismes devraient également envisager

[13] RFC 7934 Host Address Availability Recommendations : https://datatracker.ietf.org/doc/html/rfc7934.txt (en anglais seulement)
[14] RFC 8415: Dynamic Host Configuration Protocol for IPv6 (DHCPv6): https://www.rfc-editor.org/rfc/rfc8415 (en anglais seulement)
[15] Cisco : DHCP – DHCPv6 Guard : https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-sy/dhcp-15-sy-book/ip6-dhcpv6-guard.pdf (en anglais seulement)

d'utiliser des capacités de basculement DHCPv6[16] afin d'offrir une meilleure disponibilité et une protection contre les attaques par déni de service.

2.12 Protections concernant la configuration automatique d'adresse

La spécification du protocole IPv6 permet aux appareils de s'attribuer automatiquement une adresse réseau (identifiants d'interface [IID]) en utilisant le protocole SLAAC. Tel qu'il est énoncé dans le document NIST SP 800-119 Guidelines for the secure deployment of IPv6 (PDF) (en anglais seulement), SLAAC utilise les données réseau reçues du routeur et l'adresse MAC de l'appareil, ce qui peut permettre à des auteurs de menace de localiser les points d'extrémité IPv6. Le Centre pour la cybersécurité recommande de désactiver l'utilisation du protocole SLAAC, en particulier lors de la mise en œuvre d'un modèle d'adressage public. Toutefois, dans les cas d'utilisation approuvés pour SLAAC, le Centre pour la cybersécurité recommande d'activer les extensions de confidentialité SLAAC (qui génèrent des adresses IPv6 temporaires) pour les communications externes à l'extérieur du réseau d'entreprise (par exemple, sur Internet ou des réseaux de tierce partie). L'activation d'un adressage temporaire DHCPv6 peut également fournir les mêmes protections que les extensions de confidentialité SLAAC. Il est important de noter que certains points d'extrémité ne prennent pas en charge DHCPv6, par exemple les appareils exécutant le système d'exploitation Android, et peuvent nécessiter l'adressage SLAAC auto-configuré à titre d'option unique pour la configuration automatique. Dans ces scénarios, les organismes doivent activer l'enregistrement d'adresses DHCPv6 à titre de mécanisme pour les appareils SLAAC pour informer le serveur DHCPv6[17] de l'utilisation d'une adresse générée automatiquement. Cependant, cela risque de ne pas fournir une visibilité suffisante des appareils auto-configurés qui ne prennent pas en charge l'enregistrement d'adresses ou qui choisissent (de manière malveillante) de ne pas informer le serveur DHCPv6. Les organismes devraient donc mettre en œuvre des contrôles de sécurité réseau dans le but d'identifier, de gérer et d'autoriser les liaisons réseau avec des adresses auto-configurées.

2.13 Environnements à double pile

Les environnements à double pile sont attrayants pour les organismes souhaitant réaliser des économies, car ils permettent d'utiliser l'infrastructure IPv4 existante, parallèlement au protocole IPv6. Toutefois, la nécessité de maintenir l'infrastructure IPv4 tout en intégrant de nouveaux réseaux IPv6 peut augmenter le fardeau de gestion, ainsi que la surface d'attaque. Les réseaux à double pile soulèvent d'autres préoccupations de sécurité en raison de l'utilisation de multiples piles IP, qui augmente la surface d'attaque et qui exige des contrôles de sécurité additionnels pour atténuer les risques connexes. Les points d'extrémité hôtes d'une infrastructure à double pile, en particulier, présentent des défis de sécurité supplémentaires. Les contrôles de point d'extrémité doivent disposer de contrôles d'adressage à la fois pour les systèmes d'adressage IPv4 et IPv6, ce qui introduit une complexité supplémentaire. Le Centre pour la cybersécurité recommande aux organismes de limiter les points d'extrémité hôtes aux solutions à pile IP simple (IPv4 uniquement ou IPv6 uniquement). Limiter les architectures à double pile aux mécanismes de transition, aux commutateurs, aux routeurs ou aux passerelles réseau permettra de réduire la surface d'attaque. Les organismes doivent s'assurer que les pare-feu réseau et d'application sont configurés pour le filtrage des paquets réseau IPv4 et IPv6 et sont capables de le faire.

La norme de spécification Ipv6 établit des règles de priorité pour gérer les interfaces à double pile. Selon le document RFC 6724 de l'IETF, Default address selection for Internet Protocol Version 6 (en anglais seulement), les stratégies par défaut configurées peuvent accorder la priorité à des groupes d'adresses particuliers par rapport à d'autres adresses, ce qui peut complexifier les opérations réseau. Ces stratégies peuvent également avoir des répercussions sur la sécurité et les opérations au sein des réseaux à double pile. Les administratrices et administrateurs de réseau et de la sécurité doivent savoir quelles valeurs de priorité sont déployées pour la sélection d'adresses dans leur environnement réseau. De plus, ils doivent examiner et approuver les stratégies de sélection d'adresses et s'assurer qu'elles sont alignées sur leurs objectifs de sécurité réseau. Les dispositifs de sécurité réseau, y compris les pare-feu, les routeurs de bordure et les passerelles, doivent mettre en œuvre des stratégies de filtrage afin de prévenir le trafic IPv4 et IPv6 entrant ou sortant non autorisé.

[16] RFC 8156: DHCPv6 Failover Protocol : https://www.rfc-editor.org/rfc/rfc8156 (en anglais seulement)
[17] Registering Self-Generated IPv6 Addresses Using DHCPv6 : https://datatracker.ietf.org/doc/rfc9686/ (en anglais seulement)

Dans les environnements DNS à double pile, les enregistrements A (servant à mapper les noms de domaine aux adresses IPv4) et les enregistrements AAAA (servant à mapper les noms de domaine aux adresses IPv6) sont cruciaux pour le maintien des services. En ce qui concerne les réseaux exposés à Internet, le Centre pour la cybersécurité recommande aux organismes d'utiliser une infrastructure DNS séparée pour les réseaux IPv4 et IPv6 internes et externes (aussi connue sous le nom d'architecture DNS fractionnée), ce qui permet d'assurer la stabilité des applications système, d'augmenter la sécurité et de préserver la confidentialité des données réseau. Pour en savoir plus sur l'architecture DNS fractionnée, veuillez consulter le document de la NSA intitulé Internet Protocol Version 6 Security Guidance (en anglais seulement).

2.14 Protection du plan de données et du plan de gestion

Les communications administratives réseau pour les environnements IPv6 doivent être protégées contre l'écoute clandestine, le reniflage de données et d'autres menaces semblables. Le Centre pour la cybersécurité recommande de séparer le plan de gestion du plan de données en utilisant des mécanismes tels que la séparation du réseau local virtuel (VLAN) ou le filtrage au moyen d'un pare-feu. Les listes de contrôle d'accès (LCA), les systèmes de prévention d'intrusion (SPI) et les mécanismes de filtrage de niveau 2 devraient également être utilisés afin de protéger les appareils au niveau du plan de gestion réseau. Dans le cas des réseaux plus sensibles, la séparation physique et cryptographique est hautement recommandée (par exemple, la séparation du plan de gestion et du plan de données). Le Centre pour la cybersécurité recommande par ailleurs que les organismes utilisent le protocole IPsec pour protéger les communications IPv6. Seuls les algorithmes de chiffrement approuvés par le CST doivent être utilisés, tel qu'il est indiqué dans la publication du Centre pour la cybersécurité intitulée Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111). Les protocoles du plan de contrôle pour les réseaux IPv6 incluent la découverte de voisin, DHCP, le protocole BGP (Border Gateway Protocol) et le protocole NTP (Network Time Protocol). Les organismes doivent envisager de mettre en œuvre des contrôles de sécurité liés au filtrage réseau. Ces contrôles empêcheront des messages du plan de contrôle de fuiter par inadvertance de l'information et bloqueront ou désactiveront les protocoles du plan de contrôle qui ne sont pas autorisés.

2.15 Messages de découverte de voisin

La fonctionnalité de découverte de voisin[18] dans la spécification IPv6 est semblable au protocole de résolution d'adresse utilisé par IPv4. Elle sert à gérer des capacités essentielles du protocole IPv6, comme la configuration automatique d'adresse, la résolution d'adresse, la détection d'adresse en double, etc. Toutefois, le protocole de découverte de voisin est exposé à plusieurs attaques[19] et peut également être exploité par des auteurs de menace pour mener des attaques par usurpation d'adresse ou par empoisonnement. Le Centre pour la cybersécurité recommande de mettre en œuvre des produits réseau qui prennent en charge les protections cryptographiques pour la découverte de voisin, comme SEND (*Secure Neighbor Discovery*)[19]. Les signatures cryptographiques générées au moyen de SEND servent à valider et à vérifier les messages de découverte de voisin afin d'offrir une protection contre les attaques par usurpation d'adresse. L'activation du protocole IPsec peut améliorer la protection des messages de découverte de voisin. Il est également conseillé de filtrer les messages de découverte de voisin (par exemple, ICMPv6 [Internet Control Message Protocol version 6]) sur les passerelles aux frontières du réseau externe, sauf ceux nécessaires pour la connectivité réseau IPv6. Veuillez consulter le document RFC 4890[20] pour des conseils sur le filtrage des messages ICMPv6 pour les pare-feu.

2.16 Risques liés à la traduction d'adresse

La traduction d'adresse et la tunnellisation de paquets IPv4 sur un réseau IPv6 (et vice versa) peuvent introduire des préoccupations additionnelles en matière de sécurité. Les dispositifs de traduction peuvent représenter un point de défaillance unique. Par conséquent, des mesures de protection visant à assurer une haute disponibilité et la redondance doivent être incluses dans l'infrastructure lors de tout déploiement. Les interfaces de traduction forcent également l'arrêt de

[18] RFC 4861 Neighbor Discovery for IP version 6 (IPv6) : https://datatracker.ietf.org/doc/html/rfc4861 (en anglais seulement)
[19] RFC 3971 SEcure Neighbor Discovery (SEND) : https://datatracker.ietf.org/doc/html/rfc3971 (en anglais seulement)
[20] RFC 4890 Recommendations for Filtering ICMPv6 Messages in Firewalls : https://datatracker.ietf.org/doc/html/rfc4890 (en anglais seulement)

mécanismes de sécurité, comme les protocoles IPsec et DNSSEC (extensions de sécurité du système des noms de domaine).

NAT-PT (*Network Address Translation-Protocol Translation*)[21] est un mécanisme courant de traduction qui permet aux appareils IPv4 exclusivement de communiquer à des appareils IPv6 exclusivement. Le Centre pour la cybersécurité ne recommande pas d'utiliser NAT-PT pour communiquer entre des réseaux entièrement IPv6 au moyen d'une infrastructure dorsale IPv4 (ou vice versa) en raison des préoccupations concernant la disponibilité et la sécurité de bout en bout. Les organismes peuvent considérer NAT64 (traduction d'adresse réseau avec état[22] pour les clients utilisant exclusivement IPv6 afin de communiquer avec des serveurs IPv4) combiné à DNS64 (mécanisme permettant de synthétiser des enregistrements DNS AAAA à partir d'enregistrements A)[23] ou 464XLAT (combinaison de la traduction avec état[22] et sans état[24] pour une connectivité IPv4 de réseaux entièrement IPv6)[25].

2.17 Architecture à vérification systématique

L'architecture à vérification systématique repose sur le principe de sécurité de base visant à éliminer la confiance explicite au sein d'un réseau d'entreprise. Cette architecture ne suppose aucune confiance inhérente pour les ressources (applications, périphériques, utilisatrices et utilisateurs et interfaces réseau) et exige que chaque ressource soit identifiée de manière unique, authentifiée et autorisée.

La norme IPv6 offre des capacités de base pour la mise en œuvre d'une architecture à vérification systématique. Ces capacités incluent un espace d'adressage plus vaste, plusieurs adresses par interface et des extensions d'en-tête IPsec pour l'authentification de la source, l'intégrité des données et la confidentialité des données.

Une stratégie d'adressage multiple peut servir à identifier les appareils, les interfaces ou les applications sur le réseau et fournit un soutien fondamental pour la microsegmentation. Elle facilite la microsegmentation en permettant une gestion des flux de trafic au moyen de listes de contrôle d'accès réseau à granularité fine.

De plus, les organismes peuvent utiliser les en-têtes d'extension IPv6 en activant le protocole IPsec afin d'offrir des communications IP sécurisées de bout en bout. L'activation du protocole IPsec permet d'authentifier les interfaces et d'assurer la protection de bout en bout de la confidentialité et de l'intégrité des données et des messages de contrôle sur le réseau.

2.18 Connaissances techniques et opérationnelles

Une compréhension technique insuffisante et une expertise opérationnelle déficiente en matière d'IPv6 représentent un défi important pour de nombreux organismes. Très peu d'ingénieures et ingénieurs de réseau possèdent des connaissances approfondies des normes de spécification IPv6. Afin d'obtenir les compétences techniques nécessaires à l'avenir, les organismes doivent investir dans la formation de professionnelles et professionnels de la sécurité et de la réseautique en ce qui a trait au protocole IPv6 et à ses capacités. Les organisations doivent également développer une expertise en réalisant de la recherche sur les capacités IPv6 dans leur laboratoire réseau dédié ou des déploiements pilotes limités. Nous encourageons les organismes à renforcer leurs compétences et leurs capacités techniques pour assurer un bon rendement réseau, corriger les problèmes opérationnels et de conception réseau, et concevoir les exigences de sécurité.

[21] RFC 4966 Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status : https://datatracker.ietf.org/doc/rfc4966/ (en anglais seulement)
[22] RFC 6146 Stateful NAT64 : Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers : https://datatracker.ietf.org/doc/html/rfc6146 (en anglais seulement)
[23] DNS64 : DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers : https://datatracker.ietf.org/doc/html/rfc6147 (en anglais seulement)
[24] RFC 7915 Stateless IP/ICMP Translation Algorithm : https://datatracker.ietf.org/doc/html/rfc7915 (en anglais seulement)
[25] 464XLAT : Combination of Stateful and Stateless Translation : https://datatracker.ietf.org/doc/html/rfc6877 (en anglais seulement)

3 Conclusion

Les défis associés au nombre limité d'adresses IPv4 vont probablement augmenter. Le protocole IPv6 a été conçu pour répondre à ces défis et offrir des avantages supplémentaires sur le plan de la sécurité. Les piles réseau modernes accordent la priorité à IPv6 et se conforment à la norme de spécification de l'IETF. Les stratégies organisationnelles de réseau d'entreprise doivent être mises à jour afin de gérer les risques qui en découlent. Les contrôles de sécurité traditionnels établis en fonction de l'adressage IPv4, comme les capacités de surveillance, devront ainsi être mis à jour et réalignés. Le Centre pour la cybersécurité recommande fortement aux organismes du GC de prendre des mesures proactives et informées afin d'adopter des pratiques de conception sécurisée et d'établir la portée de leur plan de transition vers IPv6, tout en suivant les recommandations du Centre pour la cybersécurité.