Sujet élaboré par une cellule pédagogique nationale

CONCOURS INTERNE D'INGÉNIEUR TERRITORIAL

SESSION 2025

ÉPREUVE DE PROJET OU ÉTUDE

ÉPREUVE D'ADMISSIBILITÉ :

L'établissement d'un projet ou étude portant sur l'une des options, choisie par le candidat lors de son inscription, au sein de la spécialité dans laquelle il concourt.

Durée : 8 heures
Coefficient : 7

SPÉCIALITÉ : INFORMATIQUE ET SYSTÈMES D'INFORMATION

OPTION : RÉSEAUX ET TÉLÉCOMMUNICATIONS

À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET :

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni initiales, ni votre numéro de convocation, ni le nom de votre collectivité employeur, de la commune où vous résidez ou du lieu de la salle d'examen où vous composez, ni nom de collectivité fictif non indiqué dans le sujet, ni signature ou paraphe.
- Sauf consignes particulières figurant dans le sujet, vous devez impérativement utiliser une seule et même couleur non effaçable pour écrire et/ou souligner. Seule l'encre noire ou l'encre bleue est autorisée. L'utilisation de plus d'une couleur, d'une couleur non autorisée, d'un surligneur pourra être considérée comme un signe distinctif.
- Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.
- Les feuilles de brouillon ne seront en aucun cas prises en compte.

Ce sujet comprend 66 pages.

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué.
S'il est incomplet, en avertir le surveillant.

- Vous répondrez aux questions suivantes dans l'ordre qui vous convient, en indiquant impérativement leur numéro.
- Vous répondrez aux questions à l'aide des documents et de vos connaissances.
- Des réponses rédigées sont attendues et peuvent être accompagnées si besoin de tableaux, graphiques, schémas…

Vous êtes ingénieur territorial, chargé de mission au conseil départemental d'Ingédep (150 000 habitants et 1300 agents) à la direction des services de l'information et du numérique (DSIN). La DSIN regroupe 25 agents dans plusieurs services (réseaux/télécommunication, infrastructures, postes de travail, applications).

Situé en zone de montagne, le département se doit d'intervenir dans le cadre de la viabilité hivernale. Les 4 000 km de routes départementales sont entretenus par 4 Unités territoriales routières (UTR). Pour des raisons historiques, les 4 UTR sont reliées par faisceaux hertziens. Les conditions climatiques nécessitent une forte implication des services de viabilité des routes et une communication fiable entre les services (liaison informatique et téléphonique).

Le président du conseil départemental ayant été sensibilisé à la directive « Sécurité des réseaux et des systèmes d'information (NIS2) », il souhaite que la DSIN propose un plan d'action pour répondre à ces obligations réglementaires.

Question 1 (4 points)

Le déploiement du très haut débit sur le département a permis de relier 2 des UTRs vers le site central d'Ingédep.

Vous ferez des propositions d'évolution d'architecture réseau pour renforcer la continuité des activités de viabilité des routes.

Question 2 (5 points)

Afin de répondre aux exigences de la directive NIS2, vous proposerez, dans une note à l'attention du DSI, des préconisations techniques et organisationnelles pour la sécurisation de l'administration du système d'information d'Ingédep. Cette note devra aussi prendre en compte l'administration à distance par les agents de la DSIN (télétravail) ou par des prestataires extérieurs.

Question 3 (7 points)

L'article 21 de la directive NIS2 attache une grande importance à la détection des incidents, à leur gestion et à leur remédiation.

Vous proposerez des solutions techniques et organisationnelles afin d'assurer une détection et une réponse proactive face aux nouvelles menaces pour la cybersécurité ainsi que la démarche projet permettant de les mettre en œuvre.

Question 4 (4 points)

En matière de responsabilité et de gouvernance face aux cybermenaces (article 20), la directive NIS2 oblige entre autres les organes de direction à acquérir des connaissances et des compétences pour évaluer les risques en matière de cybersécurité.

a) Vous proposerez des actions envers les organes de direction du conseil départemental et envers les responsables élus. (2 points)

b) Vous proposerez des actions envers le personnel et les usagers du conseil départemental. (2 points)

Liste des documents :

Document 1 : « Directive (UE) 2022/2555 du parlement européen et du conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (extrait) - *Journal officiel de l'Union européenne* - 14 décembre 2022 - 5 pages

Document 2 : « Faisceau hertzien (FH) : comment ça marche ? points positifs / négatifs » - *entreprises.selectra.info* - 28 avril 2022 - 6 pages

Document 3 : « Tout ce que vous devez savoir sur le SOC : Guide complet » - *exodata.fr* - 5 avril 2024 - 5 pages

Document 4 : « Cybersécurité : comment concevoir des programmes de formation efficaces » - *LinkedIn Learning* - consulté le 28 novembre 2024 - 3 pages

Document 5 : « Recommandations relatives à l'administration sécurisée des systèmes d'information » (extraits) - *ANSSI* - 11 mai 2021 - 11 pages

Document 6 : « EIGRP ou OSPF : quel protocole de routage répond le mieux aux besoins de votre réseau ? » - *ascentoptics.com* - 5 janvier 2024 - 10 pages

Document 7 : « Comment Orange Cyberdéfense aide les entreprises à se protéger grâce à ses campus » - *usine-digitale.fr* - 8 juillet 2024 - 2 pages

Document 8 : « Privileged Access Management & Bastion informatique pour protéger et contrôler vos comptes à privilèges » - *rubycat.eu* - consulté le 28 novembre 2024 - 4 pages

Document 9 : « Le rôle de l'IA dans la gestion de réseau » - *dlink.com* - consulté le 28 novembre 2024 - 3 pages

Document 10 : « XDR versus EDR : quelles différences et comment choisir la meilleure solution pour votre entreprise ? » - *cybersecurite-management.fr* - 26 avril 2024 - 3 pages

Document 11 : « Le CERT-FR décortique la cyberattaque contre le CHRU de Brest » - *lemondeinformatique.fr* - 18 septembre 2023 - 2 pages

Document 12 : « Fibre, satellite, 4G fixe : quelle technologie d'accès à Internet choisir ? » - *pro.orange.fr* - 24 janvier 2024 - 4 pages

Document 13 : « PRI vs PCI : pour la stabilité informatique » - *groupecapinfo.fr* - 1er novembre 2024 - 2 pages

Liste des annexes :

Annexe A : « Descriptif de la Direction des travaux et des routes » - *Conseil départemental d'Ingédep* - 2025 - 2 pages

L 333/126 FR Journal officiel de l'Union européenne 27.12.2022

(...)

« Directive (UE) 2022/2555 du parlement européen et du conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2)

(extrait)

CHAPITRE IV

MESURES DE GESTION DES RISQUES EN MATIÈRE DE CYBERSÉCURITÉ ET OBLIGATIONS D'INFORMATION

Article 20

Gouvernance

1. Les États membres veillent à ce que les organes de direction des entités essentielles et importantes approuvent les mesures de gestion des risques en matière de cybersécurité prises par ces entités afin de se conformer à l'article 21, supervisent sa mise en œuvre et puissent être tenus responsables de la violation dudit article par ces entités.

L'application du présent paragraphe est sans préjudice du droit national en ce qui concerne les règles en matière de responsabilité applicables aux institutions publiques, ainsi que de responsabilité des agents de la fonction publique et des responsables élus ou nommés.

2. Les États membres veillent à ce que les membres des organes de direction des entités essentielles et importantes soienttenus de suivre une formation et ils encouragent les entités essentielles et importantes à offrir régulièrement une formation similaire aux membres de leur personnel afin que ceux-ci acquièrent des connaissances et des compétences suffisantes pour déterminer les risques et évaluer les pratiques de gestion des risques en matière de cybersécurité et leur impact sur les services fournis par l'entité.

Article 21

Mesures de gestion des risques en matière de cybersécurité

1. Les États membres veillent à ce que les entités essentielles et importantes prennent les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information que ces entités utilisent dans le cadre de leurs activités ou de la fourniture de leurs services, ainsi que pour éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services et sur d'autres services.

Les mesures visées au premier alinéa garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité adapté au risque existant, en tenant compte de l'état des connaissances et, s'il y a lieu, des normes européennes et internationales applicables, ainsi que du coût de mise en œuvre. Lors de l'évaluation de la proportionnalité de ces mesures, il convient de tenir dûment compte du degré d'exposition de l'entité aux risques, de la taille de l'entité et de la probabilité de survenance d'incidents et de leur gravité, y compris leurs conséquences sociétales et économiques.

2. Les mesures visées au paragraphe 1 sont fondées sur une approche «tous risques» qui vise à protéger les réseaux et les systèmes d'information ainsi que leur environnement physique contre les incidents, et elles comprennent au moins:

a) les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information;

b) la gestion des incidents;

c) la continuité des activités, par exemple la gestion des sauvegardes et la reprise des activités, et la gestion des crises;

d) la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs;

e) la sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités;

f) des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité;

g) les pratiques de base en matière de cyberhygiène et la formation à la cybersécurité;

h) des politiques et des procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement;

i) la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs;

j) l'utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence au sein de l'entité, selon les besoins.

3. Les États membres veillent à ce que, lorsqu'elles examinent lesquelles des mesures visées au paragraphe 2, point d), du présent article sont appropriées, les entités tiennent compte des vulnérabilités propres à chaque fournisseur et prestataire de services direct et de la qualité globale des produits et des pratiques de cybersécurité de leurs fournisseurs et prestataires de services, y compris de leurs procédures de développement sécurisé. Les États membres veillent également à ce que, lorsqu'elles examinent lesquelles des mesures visées audit point sont appropriées, les entités soient tenues de prendre en compte les résultats des évaluations coordonnées des risques pour la sécurité des chaînes d'approvisionnement critiques, effectuées conformément à l'article 22, paragraphe 1.

4. Les États membres veillent à ce que, lorsqu'une entité constate qu'elle ne se conforme pas aux mesures prévues au paragraphe 2, elle prenne, sans retard injustifié, toutes les mesures correctives nécessaires appropriées et proportionnées.

5. Au plus tard le 17 octobre 2024, la Commission adopte des actes d'exécution établissant les exigences techniques et méthodologiques liées aux mesures visées au paragraphe 2 en ce qui concerne les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux, et les prestataires de services de confiance.

La Commission peut adopter des actes d'exécution établissant les exigences techniques et méthodologiques ainsi que les exigences sectorielles, si nécessaire, liées aux mesures visées au paragraphe 2 concernant les entités essentielles et importantes autres que celles visées au premier alinéa du présent paragraphe.

Lorsqu'elle prépare les actes d'exécution visés aux premier et deuxième alinéas du présent paragraphe, la Commission suit, dans la mesure du possible, les normes européennes et internationales ainsi que les spécifications techniques pertinentes. La Commission échange des conseils et coopère avec le groupe de coopération et l'ENISA sur les projets d'actes d'exécution conformément à l'article 14, paragraphe 4, point e).

Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 39, paragraphe 2.

Article 22

Évaluations coordonnées au niveau de l'Union des risques pour la sécurité des chaînes d'approvisionnement critiques

1. Le groupe de coopération, en coopération avec la Commission et l'ENISA, peut procéder à des évaluations coordonnées des risques pour la sécurité des chaînes d'approvisionnement de services TIC, de systèmes TIC ou de produits TIC critiques spécifiques, en tenant compte des facteurs de risque techniques et, le cas échéant, non techniques.

2. La Commission, après avoir consulté le groupe de coopération et l'ENISA et, selon le cas, les acteurs concernés, détermine les services TIC, systèmes TIC ou produits TIC critiques spécifiques qui peuvent faire l'objet de l'évaluation coordonnée des risques de sécurité visée au paragraphe 1.

Article 23

Obligations d'information

1. Chaque État membre veille à ce que les entités essentielles et importantes notifient, sans retard injustifié, à son CSIRT ou, selon le cas, à son autorité compétente, conformément au paragraphe 4, tout incident ayant un impact important sur leur fourniture des services visés au paragraphe 3 (ci-après dénommé «incident important»). Le cas échéant, les entités concernées notifient, sans retard injustifié, aux destinataires de leurs services les incidents importants susceptibles de nuire à la fourniture de ces services. Chaque État membre veille à ce que ces entités signalent, entre autres, toute information permettant au CSIRT ou, le cas échéant, à l'autorité compétente de déterminer si l'incident a un impact transfrontière. Le simple fait de notifier un incident n'accroît pas la responsabilité de l'entité qui est à l'origine de la notification.

Lorsque les entités concernées notifient un incident important à l'autorité compétente en application du premier alinéa, l'État membre veille à ce que cette autorité compétente transmette la notification au CSIRT dès qu'elle la reçoit.

En cas d'incident important transfrontière ou transsectoriel, les États membres veillent à ce que leurs points de contact uniques reçoivent en temps utile les informations notifiées conformément au paragraphe 4.

2. Le cas échéant, les États membres veillent à ce que les entités essentielles et importantes communiquent, sans retard injustifié, aux destinataires de leurs services qui sont potentiellement affectés par une cybermenace importante toutes les mesures ou corrections que ces destinataires peuvent appliquer en réponse à cette menace. Le cas échéant, les entités informent également ces destinataires de la cybermenace importante elle-même.

3. Un incident est considéré comme important si:

a) il a causé ou est susceptible de causer une perturbation opérationnelle grave des services ou des pertes financières pour l'entité concernée;

b) il a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables.

4. Les États membres veillent à ce que, aux fins de la notification visée au paragraphe 1, les entités concernées soumettent au CSIRT ou, selon le cas, à l'autorité compétente:

a) sans retard injustifié et en tout état de cause dans les 24 heures après avoir eu connaissance de l'incident important, une alerte précoce qui, le cas échéant, indique si l'on suspecte l'incident important d'avoir été causé par des actes illicites ou malveillants ou s'il pourrait avoir un impact transfrontière;

b) sans retard injustifié et en tout état de cause dans les 72 heures après avoir eu connaissance de l'incident important, une notification d'incident qui, le cas échéant, met à jour les informations visées au point a) et fournit une évaluation initiale de l'incident important, y compris de sa gravité et de son impact, ainsi que des indicateurs de compromission, lorsqu'ils sont disponibles;

c) à la demande d'un CSIRT ou, selon le cas, de l'autorité compétente, un rapport intermédiaire sur les mises à jour pertinentes de la situation;

d) un rapport final au plus tard un mois après la présentation de la notification d'incident visée au point b), comprenant les éléments suivants:

   i) une description détaillée de l'incident, y compris de sa gravité et de son impact;

   ii) le type de menace ou la cause profonde qui a probablement déclenché l'incident;

   iii) les mesures d'atténuation appliquées et en cours;

   iv) le cas échéant, l'impact transfrontière de l'incident;

e) en cas d'incident en cours au moment de la présentation du rapport final visé au point d), les États membres veillent à ce que les entités concernées fournissent à ce moment-là un rapport d'avancement puis un rapport final dans un délai d'un mois à compter du traitement de l'incident.

Par dérogation au premier alinéa, point b), un prestataire de services de confiance notifie au CSIRT ou, selon le cas, à l'autorité compétente les incidents importants qui ont un impact sur la fourniture de ses services de confiance, sans retard injustifié et en tout état de cause dans les 24 heures après avoir eu connaissance de l'incident important.

5. Le CSIRT ou l'autorité compétente fournissent, sans retard injustifié et si possible dans les 24 heures suivant la réception de l'alerte précoce visée au paragraphe 4, point a), une réponse à l'entité émettrice de la notification, y compris un retour d'information initial sur l'incident important et, à la demande de l'entité, des orientations ou des conseils opérationnels sur la mise en œuvre d'éventuelles mesures d'atténuation. Lorsque le CSIRT n'est pas le premier destinataire de la notification visée au paragraphe 1, l'orientation est émise par l'autorité compétente en coopération avec le CSIRT. Le CSIRT fournit un soutien technique supplémentaire si l'entité concernée le demande. Lorsqu'il y a lieu de suspecter que l'incident est de nature criminelle, le CSIRT ou l'autorité compétente fournit également des orientations sur les modalités de notification de l'incident important aux autorités répressives.

6. Lorsque c'est approprié, et notamment si l'incident important concerne deux États membres ou plus, le CSIRT, l'autorité compétente ou le point de contact unique informent sans retard injustifié les autres États membres touchés et l'ENISA de l'incident important. Sont alors partagées des informations du type de celles reçues conformément au paragraphe 4. Ce faisant, le CSIRT, l'autorité compétente ou le point de contact unique doivent, dans le respect du droit de l'Union ou du droit national, préserver la sécurité et les intérêts commerciaux de l'entité ainsi que la confidentialité des informations communiquées.

7. Lorsque la sensibilisation du public est nécessaire pour prévenir un incident important ou pour faire face à un incident important en cours, ou lorsque la divulgation de l'incident important est par ailleurs dans l'intérêt public, le CSIRT d'un État membre ou, selon le cas, son autorité compétente et, le cas échéant, les CSIRT ou les autorités compétentes des autres États membres concernés peuvent, après avoir consulté l'entité concernée, informer le public de l'incident important ou exiger de l'entité qu'elle le fasse.

8. À la demande du CSIRT ou de l'autorité compétente, le point de contact unique transmet les notifications reçues en vertu du paragraphe 1 aux points de contact uniques des autres États membres touchés.

9. Le point de contact unique soumet tous les trois mois à l'ENISA un rapport de synthèse comprenant des données anonymisées et agrégées sur les incidents importants, les incidents, les cybermenaces et les incidents évités notifiés conformément au paragraphe 1 du présent article et à l'article 30. Afin de contribuer à la fourniture d'informations comparables, l'ENISA peut adopter des orientations techniques sur les paramètres des informations à inclure dans le rapport de synthèse. L'ENISA informe le groupe de coopération et le réseau des CSIRT de ses conclusions concernant les notifications reçues tous les six mois.

10. Les CSIRT ou, selon le cas, les autorités compétentes fournissent aux autorités compétentes en vertu de la directive (UE) 2022/2557 des informations sur les incidents importants, les incidents, les cybermenaces et les incidents évités notifiés conformément au paragraphe 1 du présent article et à l'article 30 par les entités identifiées comme des entités critiques en vertu de la directive (UE) 2022/2557.

11. La Commission peut adopter des actes d'exécution précisant plus en détail le type d'informations, le format et la procédure des notifications présentées en vertu du paragraphe 1 du présent article et de l'article 30 ainsi que des communications présentées en vertu du paragraphe 2 du présent article.

Au plus tard le 17 octobre 2024, la Commission adopte, en ce qui concerne les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux, des actes d'exécution précisant plus en détail les cas dans lesquels un incident est considéré comme important au sens du paragraphe 3. La Commission peut adopter de tels actes d'exécution pour d'autres entités essentielles et importantes.

La Commission échange des conseils et coopère avec le groupe de coopération sur les projets d'actes d'exécution visés aux premier et deuxième alinéas du présent paragraphe conformément à l'article 14, paragraphe 4, point e).

Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 39, paragraphe 2.

(...)

Faisceau hertzien (FH) : comment ça marche ? points positifs / négatifs

L'ADSL et la fibre sont les moyens de connexions les plus connus. Parfois coûteux, inaccessibles en zone rurale ou montagneuse, non fiables ou au débit ralenti, il peut être intéressant de porter sa réflexion vers une autre technologie. La technologie du Faisceau Hertzien (FH) est une bonne solution lorsque les besoins du professionnel en matière de connectivité doivent être plus puissants, en zones géographiques à risques ou "blanches". On détaillera ici, son mode de fonctionnement, les facteurs perturbateurs, ses avantages et ses inconvénients, son utilité pour les professionnels ou encore son histoire. Le faisceau hertzien (FH) est proposé par des fournisseurs au sein de leurs offres et services.

Faisceau hertzien (FH) : qu'est-ce que c'est ?

- L'accès au réseau peut se faire de différentes manières :
- **Le sol** : fibre optique, ADSL, VDSL ;
- **Les airs** : par satellite ou par **faisceau hertzien**, qui utilise des ondes radio.

L'**accès à internet** est une question cruciale sur les territoires, en France, et bien entendu à l'étranger.

Le faisceau hertzien est une technologie permettant la transmission d'informations et de données d'un point A à un point B par l'intermédiaire d'ondes radioélectriques, dont les fréquences sont comprises entre **1 et 86 GHz**. Ce dispositif "sans fil" peut être rapproché du wifi domestique et dispose de nombreux avantages. Cette technologie s'améliore continuellement, stimulée par de nombreuses recherches scientifiques.

Le Plan national du très haut débit **En février 2013**, le gouvernement a partagé son ambition de croissance, notamment au travers du développement du numérique sur le territoire.
Pour cela, le président de la République a alloué un budget annoncé de **20 milliards d'euros** sur les 10 ans à venir afin d'accroître l'accès au très haut débit. L'objectif du gouvernement est de proposer, à **horizon 2022**, un accès à une connexion internet d'au moins **30 Mb/s à toute la population française**, surtout en zones rurales et difficiles d'un point de vue topographique.
Pour ce faire, l'**état souhaite notamment s'appuyer sur le faisceau hertzien (FH)**.
Afin de préciser les besoins et les enjeux deux cahiers des charges ont été conçus. Un datant de 2013 et l'autre de 2015.

Le faisceau hertzien semble être le moyen de communication parfait pour les **connexions avec les objets mobiles** : les automobiles, les trains, les bateaux, les avions, les satellites, les piétons, etc. Cette technologie est intéressante notamment dans le cadre de la **diffusion d'un émetteur à plusieurs récepteurs**.

Par exemple, à l'échelle d'une ville, il paraît plus intéressant et moins coûteux de mettre en place un seul émetteur et une antenne chez chaque particulier, plutôt que de les relier les uns aux autres avec un câble.

Faisceau hertzien (FH) : comment ça marche ?

Une onde radioélectrique moins coûteuse

Ces ondes radioélectriques sont focalisées et concentrées grâce à des **antennes directives**. Afin que les ondes arrivent à bon port lors de longues distances géographiques, le trajet hertzien entre deux équipements d'extrémité est la plupart du temps sectionné en plusieurs **tronçons ou "bonds"**, grâce à des stations relais. On peut **opposer le faisceau hertzien à la fibre optique** qui demande d'importants travaux de génie civil et nécessite un support physique entre l'émetteur et le récepteur.

Une technologie "sans fil"

Le faisceau hertzien, par sa technologie "sans fil", ne requiert pas d'acceptation des propriétaires des terrains traversés. En effet, dès lors que l'**ARCEP a validé l'installation de la connexion entre deux antennes relais** aucune autre demande n'est requise.

Le faisceau hertzien semble être une des meilleures solutions pour développer l'installation d'internet au sein de secteurs topographies difficiles tels que les zones de montages, rurales, etc.

Un pont radio en bande réservée

Le faisceau hertzien peut être considéré comme un pont radio en bande réservée, soit une **fréquence radio privée et certifiée par l'ARCEP**. Des antennes directives converties au numérique peuvent effectuer le relai. A contrario, la fibre utilise une bande passante, plusieurs usagers peuvent la partager. Aussi, les "points" intermédiaires dans les réseaux de fibre sont plus nombreux. Ces deux éléments apportant plus de latence.

Faisceau hertzien (FH) : comment l'installer ?

L'installation d'un faisceau hertzien est proposée par des **opérateurs de réseaux**. Une **étude de terrain et de faisabilité** est alors nécessaire :

1. En fonction de l'**adresse de l'entreprise** concernée, un premier **pronostique de faisabilité** peut être prononcé ainsi qu'un **budget prévisionnel** ;
2. Suite à un premier accord de principe, l'opérateur se rend sur le terrain afin d'effectuer une **étude approfondie** ;
3. Une fois la faisabilité du projet confirmée, la **commande est alors déployée dans un délai de 8 à 20 semaines**, en fonction de l'opérateur.

Faisceau hertzien (FH) : Quel tarif ?

Le tarif de l'installation du faisceau hertzien est bien entendu calibré en fonction du projet, il inclut :

- **Les frais d'accès aux services** : les frais du déploiement et du raccordement de l'antenne ;
- **Un abonnement mensuel** : variable en fonction du débit, du réseau de l'opérateur et de la zone géographique de l'entreprise.

Qui sont les fournisseurs ?

Les fournisseurs sont nombreux, et vous proposent un **accompagnement expert afin de déployer cette offre**. En plus d'apporter un diagnostic, un conseil, l'installation du matériel et de sa mise en place, les fournisseurs se proposent en général de gérer la partie administrative avec l'ARCEP.

Par exemple :

- Bouygues Telecom Entreprises
- Orange
- Iris64
- Triad
- ADW Network
- Alcatel-Lucent

Quelles sont les conditions d'utilisation des faisceaux hertziens (FH) ?

La station émettrice rayonne, traversant le territoire afin d'atteindre **le récepteur**. L'énergie que la station déploie décroit au fur et à mesure qu'elle avance vers le récepteur. Il est donc important d'**étudier le trajet parcouru** et de veiller à adapter les éléments qui l'entourent et qui peuvent affecter son déploiement.

Premier ellipsoïde de Fresnel. Il s'agit d'un volume présent dans l'espace qui permet de mesurer l'atténuation que peut apporter un obstacle (colline, immeuble ou encore montagne) lors de la propagation d'une onde.

Toutes les conditions d'utilisation des réseaux sont recommandées et définies par l'UIT-R.

1. Pour que les ondes puissent correctement se propager de la station émettrice au récepteur, il est important de veiller au **dégagement de la zone de liaison**. Le relief, la végétation ou encore le bâti peuvent causer des pertes d'émission. L'énergie la plus importante est contenue dans la zone appelée **"premier ellipsoïde de Fresnel"**. À cet effet, l'étendue de cette zone - concentrée sur quelques dizaines de mètres - doit être dégagée.
2. Il est aussi primordial d'étudier les **conditions climatiques et atmosphériques** de la zone traversée par l'onde. Les rayons ne se déploient pas en ligne droite, mais se calent aux zones disposant d'un fort indice électromagnétique, soit les couches de

l'atmosphère les plus denses. Ce que l'on appelle aussi la **réfraction atmosphérique**. Les fortes précipitations peuvent aussi perturber la propagation de l'onde. À cet effet, lors des études de terrain préalables, il est important de mener des **études statistiques afin d'anticiper le déplacement de l'onde en fonction de la courbure de la terre et des changements climatologiques**.

La réfraction atmosphérique Ce phénomène optique se produit lorsque la trajectoire d'une lumière est non rectiligne du fait de la variation de la densité de l'air avec l'altitude.

Faisceau hertzien (FH) : quels facteurs peuvent perturber leur propagation ?

Les facteurs pouvant perturber la propagation des faisceaux hertziens sont liés à celles des ondes radios.

Lors de la propagation de l'onde hertzienne, **trois types d'éléments peuvent la perturber** :

1. **Son rayonnement en espace libre**, impliquant la difficulté parfois à palier à la présence d'obstacles sur son chemin ;
2. **Les variations aléatoires climatologiques**, les hautes précipitations pouvant perturber son parcours ;
3. **Les interférences**, les perturbations électromagnétiques, les brouillages ou encore la réflexion principale ou de multi-trajets.

Faisceau hertzien (FH) : quelle est son utilité pour les professionnels et les entreprises ?

De nombreux opérateurs proposent un service de mise en place de faisceau hertzien, notamment **Bouygues Telecom Entreprises**, **ADW Network** ou encore **Orange**.

Les professionnels et entreprises ayant recours à ce type de technologies sont motivés par un **accès Internet Très Haut Débit**, dont les locaux sont situés en **"zone blanche"**, soit un lieu qui n'est pas éligible à la fibre optique et où l'ADSL ne suffirait pas.

La technologie du faisceau hertzien (FH) permet aussi de **limiter l'enveloppe budgétaire** allouée à la construction d'un réseau de communication relié à Internet, contrairement à la fibre optique. Le **faisceau hertzien semble être une technologie économique et facile de mise en place**. Le faisceau hertzien ne demande pas de travaux de grande ampleur, les coûts d'installation d'un faisceau hertzien sont en moyenne dix fois moins élevés que ceux utilisés dans le cadre de l'installation de la fibre optique.

Avantage et inconvénient d'un faisceau hertzien (FH)

Les avantages

- **Sans fil et robuste** ;
- Très haut débit - **jusqu'à 2 Gbits/s** ;
- La transmission de **tous les types de flux** (voix, data, vidéo) ;
- Travaux **moins coûteux** - meilleur rapport qualité/prix par rapport à la fibre ;
- Installation **facile, rapide et évolutif** : 4 à 5 jours pour installer la liaison hertzienne ;
- Une connexion **pour tous** - au sein de zones topographiques difficiles et éloignées.

Les inconvénients

Les inconvénients d'un faisceau hertzien, ceux des **moyens radio** :

- Les ondes sont **sensibles aux masquages et obstacles** tels que le relief, la végétation et les bâtiments ;
- Liaison perturbée en cas de **fortes intempéries**, comme la pluie, la réfractivité de l'atmosphère et aux phénomènes de réflexion ;
- Les paraboles doivent avoir **une vue directe** ;
- La **confidentialité et sa traçabilité** - il est possible de pouvoir intercepter une communication, car l'information est transmise en "espace libre".
  Dans ce cas, **un système de cryptage peut être mis en place** entre l'émetteur et le récepteur.

L'histoire des faisceaux hertziens (FH)

1931 : après de multiples recherches, **une première liaison entre Calais et la ville Douvres** est effectuée.

1942 : **l'ANTRC, fabrication du premier faisceau hertzien (FH)** aux États-Unis, anciennement appelé VHF, puis "câble hertzien".

1944 : cette **technologie fut transmise aux Français** en dotation à l'époque du débarquement.

1944 - fin des années 80 : mise en service pour les **transmissions des forces, pour ensuite servir à la D.O.T**.

Pendant les années 60 : la technologie se développe pour donner vie à **3 nouvelles gammes de faisceaux hertziens**. Chacun de ces appareils répond à des besoins spécifiques, les faisceaux hertziens de l'Avant (QR-MH-8), de descente de site (QR-TH-3) ou bien de franchissement de coupures ou encore des grandes unités (ARIANE ou GR-MH-11). Afin de pouvoir respecter les besoins de confidentialité nécessaires à l'époque de la guerre froide, le RITA a été mis en place. Cet appareil a permis par le chiffrement de jonction, de respecter un degré de discrétion acceptable.

Pendant les années 70 : **France Télécom fait l'usage des faisceaux hertziens** pour des besoins régionaux.

2006 - 2010 - 2012 et 2014 : les conditions de l'utilisation sont **réglementées et revues** par les autorités.

Février 2013 : **le Plan France Très Haut Débit** a été initié par le président de la République.

2018 : **l'Institut Fraunhofer a permis d'atteindre un débit de 40 Gbit/s pour 1 km de distance**, ce qui en fait une avancée scientifique car quasiment équivalente à la puissance de la fibre optique.
Par exemple, l'ADSL en France propose un débit de 6 Mbit/s, soit un total de 6 000 fois moins.

Ces recherches menées par l'Institut Fraunhofer a aussi mis en valeur la **haute résistance du faisceau hertzien (FH)** face aux conditions climatiques extrêmes qui peuvent parfois dégrader et perturber la qualité du signal entre l'émetteur et le récepteur.

Tout ce que vous devez savoir sur le SOC : guide complet

Dans le domaine de la cybersécurité, la mise en place d'un SOC (Security Operations Center) revêt une importance cruciale pour protéger les systèmes d'information des entreprises contre les menaces en constante évolution. Cet article vise à fournir un **guide complet sur le SOC**, depuis sa définition et son fonctionnement jusqu'à son rôle essentiel dans la sécurité des entreprises et les étapes pour sa mise en place.

01. Qu'est-ce qu'un SOC ? Définition

La définition du SOC

Le SOC, ou centre des opérations de sécurité (Security Operations Center en anglais), est le cœur névralgique de la cybersécurité d'une entreprise. Il s'agit d'une entité chargée de surveiller en permanence les activités informatiques, de détecter les menaces potentielles et de répondre aux incidents de sécurité en temps réel.

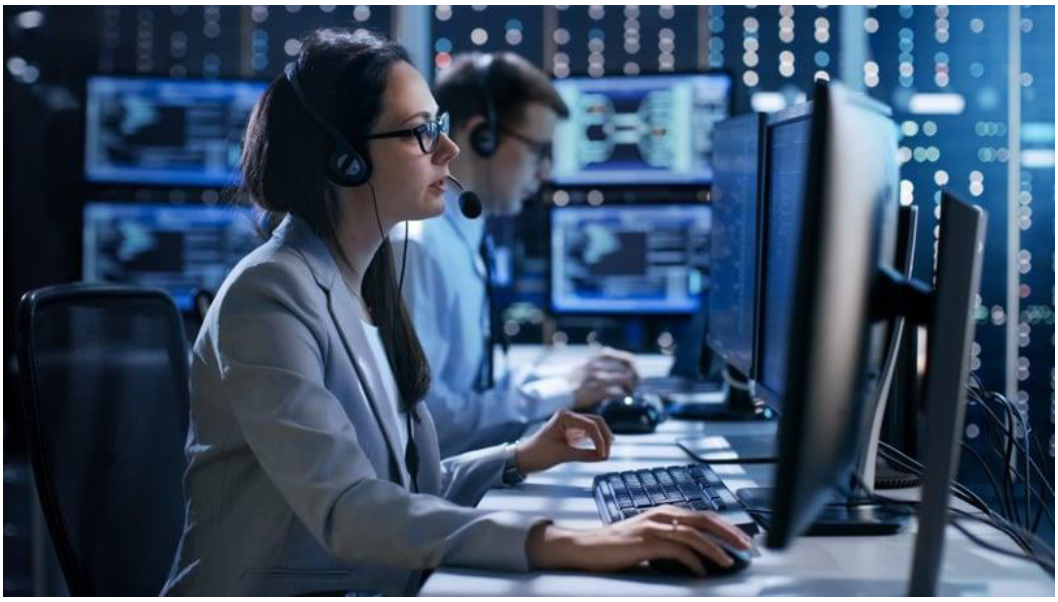
Pour assurer ses fonctions, un SOC se compose de plusieurs éléments essentiels, y compris les outils de gestion des événements et des incidents, les systèmes de détection d'intrusion, ainsi que les équipes d'analystes de sécurité. La définition du SOC informatique est donc centrale pour comprendre son rôle et son fonctionnement dans la protection des systèmes d'information d'une entreprise.

Fonctionnement général d'un SOC

Le fonctionnement d'un SOC repose sur une série d'étapes bien définies. Tout d'abord, il collecte et analyse les données provenant de diverses sources telles que les journaux système, les alertes de sécurité, et les systèmes de détection d'intrusion.

Ensuite, il utilise des outils avancés tels que les SIEM (Security Information and Event Management) pour corréler et contextualiser ces données, afin de détecter les activités suspectes et les menaces potentielles.

Enfin, il répond aux incidents de sécurité en prenant des mesures correctives et en coordonnant les efforts de remédiation.



Les différents composants d'un SOC

Un SOC comprend généralement plusieurs composants clés, notamment :

- La salle de surveillance, où les analystes de sécurité surveillent en temps réel les activités suspectes ;
- Les outils de détection d'intrusion, qui identifient les tentatives d'accès non autorisées ;
- Les systèmes de gestion des événements et des incidents, qui collectent, corréler et analysent les données de sécurité ;
- Les équipes d'intervention, chargées de répondre aux incidents de sécurité et de coordonner les mesures de remédiation.

02. Quel est le rôle d'un SOC ?

Le rôle principal d'un Security Operation Center est de garantir la sécurité des systèmes d'information de l'entreprise. Pour ce faire, il remplit plusieurs fonctions essentielles :

Identification des menaces et des cyberattaques

Le Centre des Opérations de sécurité surveille en permanence les réseaux et les systèmes de l'entreprise pour identifier les activités suspectes et les indicateurs de compromission. Il utilise des techniques avancées telles que l'analyse comportementale et la détection d'anomalies pour repérer les menaces potentielles.

Surveillance en temps réel des systèmes et des réseaux

En surveillant activement les activités informatiques, le Security Operations Center peut détecter les intrusions et les attaques en cours, et intervenir rapidement pour limiter les dommages potentiels.

Réponse aux incidents de sécurité

En cas d'incident de sécurité, le Security Operations Center prend des mesures immédiates pour contenir la menace, investiguer l'incident, et restaurer la sécurité des systèmes affectés. Il travaille en étroite collaboration avec les équipes informatiques et de gestion des risques pour coordonner les efforts de remédiation.

03. Pourquoi le Security Operation Center est un élément essentiel pour les entreprises ?

Les entreprises sont de plus en plus exposées à une multitude de risques liés aux cyberattaques, allant des logiciels malveillants aux attaques de phishing en passant par les violations de données. Sans un centre opérationnel de sécurité efficace, elles sont vulnérables aux attaques et risquent de subir des dommages financiers et réputationnels considérables.

Risques liés aux cyberattaques pour les entreprises

Les cyberattaques peuvent avoir des conséquences dévastatrices pour les entreprises, allant de la perte de données sensibles à la perturbation des opérations commerciales, en passant par les amendes réglementaires et les litiges judiciaires. Les entreprises doivent donc être proactives dans leur approche de la cybersécurité (grâce notamment au SOC) pour se protéger contre ces menaces.

Avantages de l’utilisation d’un SOC pour la sécurité des entreprises

En utilisant un SOC, les entreprises peuvent détecter et prévenir les incidents de sécurité avant qu'ils ne causent des dommages importants. Un SOC bien conçu permet une réponse rapide et efficace aux cyberattaques, réduisant ainsi les risques et les coûts associés aux incidents de sécurité.

Conséquences d’une absence de SOC pour la sécurité des entreprises

Sans un SOC, les entreprises risquent de passer à côté des signaux d'alerte précoce indiquant des activités malveillantes, ce qui peut entraîner des retards dans la détection et la réponse aux incidents de sécurité. Cela peut également compromettre la capacité de l'entreprise à se conformer aux réglementations en matière de protection des données et à protéger la confidentialité et l'intégrité des données sensibles.

04. Comment fonctionne un SOC et quels en sont les différents types ?

Fonctionnement opérationnel d'un SOC

Un SOC fonctionne 24 heures sur 24, 7 jours sur 7, pour assurer une surveillance continue des systèmes et des réseaux de l'entreprise. Il utilise une combinaison de technologies avancées, de processus opérationnels et de personnel qualifié pour détecter, analyser et répondre aux incidents de sécurité.

Différents types de SOC : interne et externe

Il existe deux principaux types de Security Operations Center : interne et externe. Un SOC interne est géré en interne par l'entreprise, tandis qu'un SOC externe est géré par un fournisseur de services spécialisé. Le choix entre un SOC interne et un SOC externe dépend des besoins spécifiques de l'entreprise, de ses ressources disponibles et de son niveau de maturité en matière de cybersécurité.

Critères de choix entre un SOC interne et externe

Lors du choix entre un SOC interne et externe, les entreprises doivent prendre en compte plusieurs facteurs, notamment leur niveau d'expertise en matière de cybersécurité, leurs ressources disponibles, leur tolérance au risque, et leurs objectifs stratégiques à long terme. Le temps et les ressources nécessaires pour construire un SOC en interne ajoutent des coûts importants et souvent inattendus au projet.

05. Qui sont les principaux membres de l’équipe du centre des opérations de sécurité ?

Les équipes SOC comprennent généralement une variété de membres spécialisés, chacun jouant un rôle crucial dans la protection des systèmes d'information de l'entreprise :

- Les analystes de sécurité sont responsables de la surveillance des systèmes et des réseaux, de l'analyse des alertes de sécurité et de la détection des activités suspectes.
- Les ingénieurs en sécurité sont chargés de la mise en œuvre et de la gestion des outils de sécurité, tels que les pare-feu, les systèmes de détection d'intrusion et les solutions de protection des points d'accès.

- Les experts en gestion des incidents coordonnent la réponse aux incidents de sécurité, en identifiant les priorités, en mobilisant les ressources nécessaires et en suivant les procédures opérationnelles.
- Les responsables de la conformité veillent à ce que l'entreprise respecte les normes et les réglementations en matière de cybersécurité, telles que le PCI DSS, le RGPD et d'autres réglementations sectorielles.
- Les membres du personnel de soutien fournissent un support administratif et logistique aux équipes de sécurité, en assurant le bon fonctionnement du SOC et en facilitant la communication entre les différentes parties prenantes.

06. Comment mettre en place un SOC dans son entreprise ?

La mise en place d'un SOC dans son entreprise nécessite une approche méthodique et planifiée, comprenant les étapes de déploiement suivantes :

- **Évaluation des besoins en matière de sécurité :** Identifiez les actifs critiques de l'entreprise, les menaces potentielles et les lacunes en matière de sécurité pour définir les objectifs et les exigences du Security Operations Center.
- **Sélection des outils et des technologies :** Choisissez les outils de sécurité et les solutions technologiques les mieux adaptés aux besoins de l'entreprise, en tenant compte des contraintes budgétaires et des ressources disponibles.
- **Recrutement et formation du personnel :** Engagez du personnel qualifié et formez-le aux outils et aux processus spécifiques du SOC, en veillant à ce qu'il dispose des compétences nécessaires pour identifier, analyser et répondre aux incidents de sécurité.
- **Mise en place de processus et de procédures opérationnels :** Élaborez des procédures opérationnelles standardisées pour la surveillance, la détection et la réponse aux incidents de sécurité, en définissant clairement les rôles et les responsabilités de chaque membre de l'équipe.
- **Évaluation continue et amélioration :** Évaluez régulièrement les performances du Security Operations Center, en identifiant les lacunes et en mettant en œuvre des mesures correctives pour renforcer la posture de sécurité de l'entreprise. Le Security Configuration Assessment, en auditant vos systèmes existants, peut vous aider à renforcer vos systèmes, serveurs et applications.

En conclusion, le SOC est un élément essentiel de la stratégie de cybersécurité de toute entreprise. En surveillant en permanence les activités informatiques, en détectant les menaces potentielles et en répondant aux incidents de cybersécurité, il aide les entreprises à protéger leurs systèmes d'information contre les cyberattaques et à préserver leur réputation et leur compétitivité sur le marché. En suivant les meilleures pratiques et en mettant en place un SOC efficace, les entreprises peuvent renforcer leur posture de sécurité et réduire les risques liés aux cyberattaques.

DOCUMENT 4

LinkedIn Learning - consulté le 28 novembre 2024

Cybersécurité : comment concevoir des programmes de formation efficaces ?

Phishing, ransomwares, attaques en déni de service… Aujourd'hui, la cybercriminalité est considérée comme un risque majeur pour la survie des organisations car elle peut avoir des conséquences désastreuses qui mettent en péril leur fonctionnement, leurs finances et leur image. Avec l'essor et la complexification des cybermenaces dans le paysage numérique actuel, la cybersécurité s'est imposée comme un enjeu stratégique majeur dans la résilience organisationnelle. La formation et la sensibilisation proactives des équipes à la cybersécurité (à tous les niveaux) sont indispensables à la mise en œuvre d'une stratégie efficace de gestion des cyber-risques.

Dans cet article, vous comprendrez pourquoi et comment mettre en œuvre un programme de sensibilisation et de formation en sécurité informatique au sein de votre entreprise tout en instaurant une culture de la cybersécurité.

Comprendre les cybermenaces

Les organisations doivent faire face à un nombre croissant de cybermenaces de plus en plus sophistiquées. Parmi les cybermalveillances les plus courantes, on trouve les suivantes :

- Le **phishing** est une technique qui consiste à envoyer des messages frauduleux par e-mail ou sms en usurpant l'identité d'un tiers pour amener quelqu'un à divulguer des informations sensibles (personnelles, professionnelles ou bancaires).
- Les **ransomwares** désignent des cyberattaques qui bloquent l'accès de l'utilisateur à son appareil ou à ses fichiers en les chiffrant et demandent le paiement d'une rançon pour lever le blocage.
- **Les attaques en déni de service** ont pour but de rendre un service indisponible, notamment en le saturant de demandes de connexion.

Ces cyberattaques peuvent être anticipées et traitées dans le cadre d'une approche proactive de la gestion des risques informatiques.

Former les employés à la cybersécurité : pourquoi c'est important

Si la mise en place d'un arsenal technique est nécessaire pour créer un environnement résilient aux cybermenaces, l'humain joue assurément un rôle crucial dans leur prévention et leur traitement. Si le Chief Information Security Officer occupe une place importante, ce sont tous vos collaborateurs qui sont en première ligne de défense. Et des collaborateurs bien formés et sensibilisés aux cyber-risques ont une fonction déterminante dans la préservation des actifs de votre organisation.

Des employés vigilants, conscients des risques, qui savent les identifier seront en mesure de les reconnaître, de les signaler à un stade précoce et de réduire le nombre de cyberattaques. Instaurer une culture de la cybersécurité au sein de l'entreprise grâce à des programmes de cours en cybersécurité et des modules de sensibilisation permettra à vos équipes de comprendre les menaces et d'être proactives dans leur prévention.

Comment concevoir un programme de formation efficace en cybersécurité ?

Concevoir et mettre en œuvre des programmes de formation en cybersécurité sur mesure pour les équipes est devenu impératif pour les préparer efficacement à faire face aux cybermenaces.

Voici quelques étapes clés pour élaborer des programmes de formation en cybersécurité adaptés :

- **Quels sont les objectifs spécifiques de votre organisation ?** Identifiez les besoins, les lacunes et les risques au sein de votre entreprise au regard de la diversité des profils de vos talents.

- **Créer du contenu sur mesure** adapté aux besoins et aux responsabilités de chacun(e). Par exemple, un(e) responsable marketing n'aura sans doute pas besoin du même type de formation en cybersécurité qu'un(e) CFO.

- **Des programmes évolutifs de formation continue :** l'évolution du domaine de la cybersécurité suit l'évolution des cybermenaces. Votre programme doit régulièrement être mis à jour en fonction des dernières tendances et doit être suivi de manière régulière.

- **Des exercices pratiques :** les exercices de simulation et d'apprentissage basés sur des scénarios permettent aux participants de faire usage de leurs connaissances théoriques dans des situations réalistes.

- Utilisez des **indicateurs de performance** pour mesurer l'impact de votre programme de formation !

Comment réussir à créer une culture de la cybersécurité ?

Avec l'essor du numérique, la question de la cybersécurité n'est plus uniquement du ressort des experts en informatique. Elle concerne chacun(e) des membres de l'organisation, à tous les échelons. Il est crucial de créer une culture organisationnelle inclusive de la cybersécurité et d'établir une défense à plusieurs niveaux.

L'impulsion et le soutien de la direction jouent un rôle clé. C'est "par le haut" qu'il faudra commencer et proposer des programmes de formation personnalisés en cybersécurité, encourager une communication ouverte et bienveillante sur les cyber-risques, tout en valorisant les employés engagés dans la prévention et les signalements des cybermenaces.

La cybersécurité doit devenir un élément clé de la culture d'entreprise dans le but de construire une résilience numérique collective et faire face de manière efficace aux cybermenaces.

Comment répondre efficacement aux menaces émergentes ?

La complexification, l'explosion et l'évolution rapide des cybermenaces nécessitent une adaptation constante des organisations, et des formations solides de leurs équipes en cybersécurité. Les cours en cybersécurité doivent être réguliers, spécialisés, intégrés à l'emploi du temps des équipes pour garantir une mise à jour constante de leurs compétences en cybersécurité.

L'agilité des organisations et leur adaptabilité jouent en outre un rôle important dans le renforcement de la cyber-résilience et favorisent une vigilance, une prévention et un traitement efficaces des cybermenaces.

Il est aussi primordial de prendre en compte les considérations éthiques dans les formations en sécurité informatique afin d'inculquer aux employés des pratiques numériques à la fois éthiques, responsables et efficaces.

Des organismes comme l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ou la Cybersecurity and Infrastructure Security Agency (CISA) proposent des (in)formations en matière de cybersécurité.

La formation et la sensibilisation du personnel à la cybersécurité jouent un rôle clé dans la gestion efficace des cyber-risques. Des employés dotés de compétences en cybersécurité à jour pourront contribuer efficacement à la prévention, au signalement et à l'atténuation des cybermenaces sous toutes leurs formes. Il est nécessaire d'investir dans des programmes de formation collectifs continus qui tiennent compte de considérations éthiques et du caractère volatile des cybermenaces.

Chez LinkedIn, nous comprenons l'impératif de développer une culture de la cybersécurité de l'entreprise où chaque employé(e) a un rôle de défenseur(se) à jouer dans la gestion des cyberattaques. Grâce à nos programmes de formation en cybersécurité, vous avez le pouvoir de faire de vos talents des personnes numériquement responsables et de contribuer à renforcer la cyber-résilience de votre organisation.

DOCUMENT 5

(...)

RECOMMANDATIONS RELATIVES À L'ADMINISTRATION SÉCURISÉE DES SYSTÈMES D'INFORMATION

GUIDE ANSSI

(extraits)

ANSSI-PA-022
11/05/2021

PUBLIC VISÉ :

Développeur | **Administrateur** | **RSSI** | **DSI** | Utilisateur

(...)

(...)

5
Réseau d'administration

Le réseau d'administration se définit comme le réseau de communication sur lequel transitent les flux internes au SI d'administration et les flux d'administration à destination des ressources administrées. Ce réseau doit faire l'objet de mesures de sécurisation spécifiques en phase avec l'analyse de risque et les objectifs de sécurité décrits dans la section 3.1.

5.1 Protection des ressources d'administration

À l'instar de la recommandation sur les postes d'administration, la mise en œuvre d'un réseau d'administration physiquement dédié aux ressources d'administration offre un niveau de sécurité maximal pour se prémunir d'une compromission du SI d'administration et garantir un cloisonnement fort avec tout autre réseau potentiellement connecté à Internet.

Pour éviter le branchement d'équipements indésirables sur ce réseau d'administration dédié (ex. : postes bureautiques, postes personnels), une authentification réseau est recommandée en complément, par exemple par l'implémentation du protocole 802.1X en suivant les recommandations du guide de l'ANSSI [11].

R15

Connecter les ressources d'administration sur un réseau physique dédié

Les ressources d'administration (ex. : postes d'administration, serveurs outils) doivent être déployées sur un réseau physiquement dédié à cet usage.
Le cas échéant, il est recommandé que les postes d'administration s'authentifient pour accéder au réseau d'administration.

Si l'application stricte de cette recommandation est techniquement impossible (ex. : sur un réseau étendu) ou disproportionnée par rapport aux besoins de sécurité, une alternative d'un niveau de sécurité moindre peut être envisagée sur la base d'un réseau logique dédié.

R15 -

Connecter les ressources d'administration sur un réseau VPN IPsec dédié

À défaut d'un réseau physique dédié, les ressources d'administration doivent être déployées sur un réseau logique dédié à cet usage en mettant en œuvre des mécanismes de chiffrement et d'authentification de réseau, à savoir le protocole IPsec. En complément, des mécanismes de segmentation logique (VLAN) et de filtrage réseau sont recommandés pour limiter l'exposition du concentrateur VPN IPsec aux seuls postes d'administration.
Pour la mise en œuvre du protocole IPsec, les recommandations du guide de l'ANSSI [16] doivent être appliquées.

Un regroupement des ressources d'administration par zone de confiance permet de mettre en place un cloisonnement pertinent et les mesures de filtrage réseau idoines au sein du SI d'administration. En outre, afin de garantir le cloisonnement du SI d'administration vis-à-vis de l'extérieur, un filtrage périmétrique doit également être assuré. Dans le cadre du maintien en condition de sécurité, celui-ci doit faire l'objet d'une procédure régulière de révision. De cette façon, les règles de filtrage obsolètes, inutiles ou trop permissives sont supprimées ou, à défaut, désactivées.

R16

Appliquer un filtrage interne et périmétrique au SI d'administration

Quelle que soit la solution de réseau retenue, un filtrage réseau entre zones de confiance doit être mis en œuvre au sein du SI d'administration. Par ailleurs, toutes les interconnexions avec le SI d'administration doivent être identifiées et filtrées. Une matrice de flux, limitée au juste besoin opérationnel, doit être élaborée et revue régulièrement afin d'assurer la traçabilité et le suivi des règles de filtrage.

Information

L'ANSSI publie des recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu [15] et pour son nettoyage [17].

La figure 5.1 illustre les recommandations R16 et R15 (schéma de gauche), R16 et R15- (schéma de droite). L'illustration de R15-, à droite, ne représente que des postes d'administration connectés en VPN IPsec (cas classique de déploiement d'un client VPN). Cependant il est tout à fait envisageable de connecter d'autres ressources d'administration de la même manière.

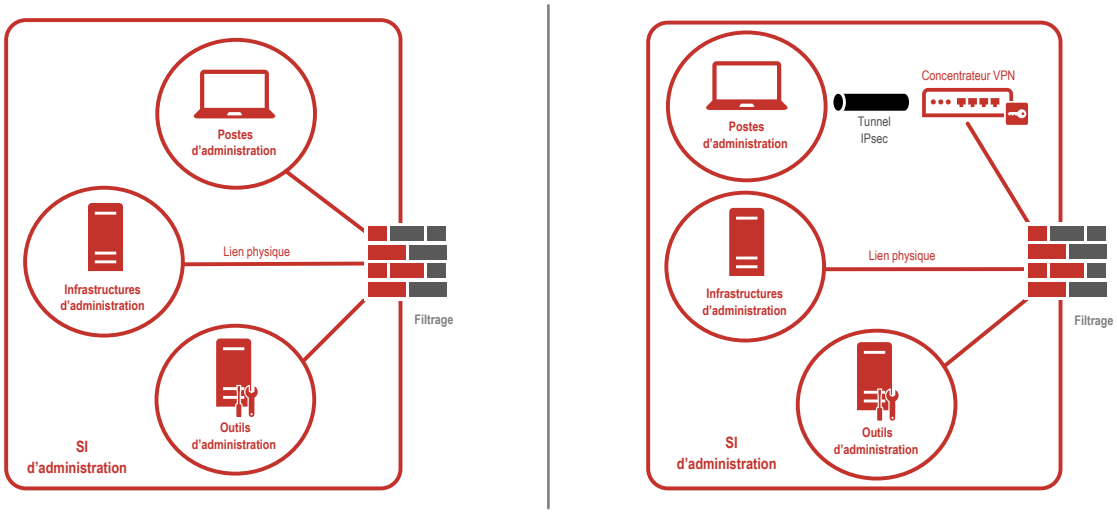


FIGURE 5.1 – Réseaux d'administration avec fonction de filtrage

5.2 Accès aux ressources administrées

L'accès aux ressources administrées doit être maîtrisé, non seulement au niveau local grâce à des configurations applicatives sur ces ressources, mais aussi au niveau réseau par des mesures complémentaires de blocage ou de filtrage réseau dans une démarche de défense en profondeur.

5.2.1 Sécurisation locale de l'accès aux ressources administrées

Afin de filtrer au plus près l'accès à une ressource administrée, il est recommandé de mettre en œuvre un filtrage local, par exemple à l'aide d'un pare-feu applicatif avec une matrice des flux limitée au strict besoin opérationnel. En particulier, seules des ressources d'administration identifiées peuvent accéder aux services d'administration. Par exemple, le service de production d'un serveur Web est accessible sur le port TCP/443 (HTTPS) par l'ensemble de ses clients légitimes et son service d'administration est accessible sur le port TCP/22 (SSH) par les ressources d'administration identifiées pour ce besoin.

R17

Appliquer un filtrage local sur les ressources administrées

Pour maîtriser les accès au plus près des ressources administrées, il est recommandé de leur appliquer un filtrage local correspondant au juste besoin opérationnel.

Information

Certains systèmes, par exemple des systèmes de gestion de contenu ou le service Active Directory de Microsoft, ne distinguent pas le port d'écoute des services de production et d'administration (même port TCP). Dans ce cas de figure, l'application de R17 est toujours nécessaire mais non suffisante. La sécurité de l'administration au niveau de la ressource administrée repose de façon ultime sur la configuration applicative du service (ex : contrôle d'accès, gestion des droits) et sa robustesse ; cela doit être traité avec attention mais n'est pas l'objet de ce guide.

5.2.2 Mise en œuvre d'une interface d'administration dédiée

Dès lors qu'elle est techniquement réalisable au niveau d'une ressource administrée, la séparation des interfaces de production et d'administration est recommandée. Cette mesure garantit non seulement un filtrage local plus spécifique (ex. : un service d'administration n'est autorisé que sur l'interface d'administration) mais aussi une disponibilité accrue de la ressource administrée en cas de déni de service sur l'interface de production.

Une séparation en interfaces réseau physiques offre un niveau de sécurité maximal et permet ainsi de dissocier les équipements de filtrage réseau respectivement sur les réseaux de production et d'administration. À défaut, une séparation en interfaces réseau virtuelles est recommandée.

Si cette séparation n'est techniquement pas réalisable sur un système, alors l'application des mesures locales, dont la recommandation R17, doit être d'autant plus stricte.

R18

Dédier une interface réseau physique d'administration

Il est recommandé de dédier une interface réseau physique d'administration sur les ressources administrées en s'assurant des pré-requis suivants :

- les services logiques permettant l'exécution des actions d'administration doivent être en écoute uniquement sur l'interface réseau d'administration prévue à cet effet ;
- les fonctions internes du système d'exploitation ne doivent pas permettre le routage d'informations entre les interfaces réseau de production et l'interface réseau d'administration d'une même ressource. Elles doivent être désactivées (ex. : désactivation d'*IPForwarding*).

R18 -

Dédier une interface réseau virtuelle d'administration

À défaut d'une interface réseau physique d'administration, il est recommandé de dédier une interface réseau virtuelle d'administration sur les ressources administrées. Les mêmes pré-requis que R18 s'appliquent.

Information

Certains constructeurs proposent des interfaces de gestion à distance (ex. : Cisco IMC, Dell RAC, HP iLO) permettant un accès à la couche basse de l'équipement. Dès lors, si elles sont utilisées, elles doivent être considérées comme des interfaces réseau d'administration spécifiques et raccordées au réseau d'administration. En fonction de l'analyse de risque et de l'organisation des équipes d'administration, ces interfaces peuvent être raccordées dans une zone différente de l'administration des couches plus hautes.

Il est nécessaire de s'assurer qu'il n'est pas possible pour un attaquant, ayant pris le contrôle d'une ressource administrée, d'utiliser l'interface réseau d'administration pour rebondir sur les ressources d'administration. En conséquence, seuls les flux initialisés depuis les postes ou les serveurs d'administration vers les ressources administrées doivent être autorisés par défaut. Les remontées des journaux d'événements depuis les ressources administrées (ex. : client syslog) vers le SI d'administration peuvent constituer une exception.

R19

Appliquer un filtrage entre ressources d'administration et ressources administrées

La recommandation R16 doit être appliquée rigoureusement entre les ressources d'administration et les ressources administrées.

De même, il est nécessaire de s'assurer qu'il n'est pas possible pour un attaquant, ayant pris le contrôle d'une ressource administrée, d'utiliser l'interface réseau d'administration pour rebondir sur les autres ressources administrées. Par conséquence, toute communication entre les ressources administrées doit être interdite à travers le réseau d'administration. Dans ce cadre, il est possible d'avoir recours à :

- un filtrage réseau sur la base d'une « micro-segmentation » (une ressource administrée = un sous-réseau), cette pratique pouvant néanmoins représenter une certaine complexité opérationnelle ;
- l'utilisation de la fonctionnalité de VLAN privé (*Private VLAN* ou PVLAN) au niveau des commutateurs (cf. le guide ANSSI [7]).

R20

Bloquer toute connexion entre ressources administrées à travers le réseau d'administration

Une mesure de blocage ou de filtrage réseau doit être mise en œuvre entre les ressources administrées afin d'interdire toute tentative de compromission par rebond à travers les interfaces réseaux d'administration.

5.2.3 Cas d'un réseau étendu

Dans le cas d'architectures multi-sites ou de réseaux étendus, les ressources d'administration peuvent être éloignées des ressources administrées. Les flux d'administration transitent alors potentiellement par un réseau de transport tiers[7]. Dans ce cas, il est nécessaire de protéger les flux d'administration en confidentialité, en intégrité et en authenticité.

R21

Protéger les flux d'administration transitant sur un réseau tiers

Si les flux d'administration circulent à travers un réseau tiers ou hors de locaux avec un niveau de sécurité physique adéquat (ex. : portion de fibre noire traversant l'espace public), ceux-ci doivent être chiffrés et authentifiés de bout en bout jusqu'à atteindre une autre zone du SI d'administration ou une ressource à administrer. Dans ce cas, un tunnel IPsec doit être établi.
Pour la mise en œuvre du protocole IPsec, les recommandations du guide de l'ANSSI [16] doivent être appliquées.

Les figures 5.2 et 5.3 illustrent respectivement l'accès aux ressources administrées dans le cas d'un réseau local et d'un réseau étendu.

7. Un réseau de transport est dit *tiers* dès lors qu'il n'est pas maîtrisé par l'entité (ex. : Internet ou un réseau d'opérateur de télécommunications).

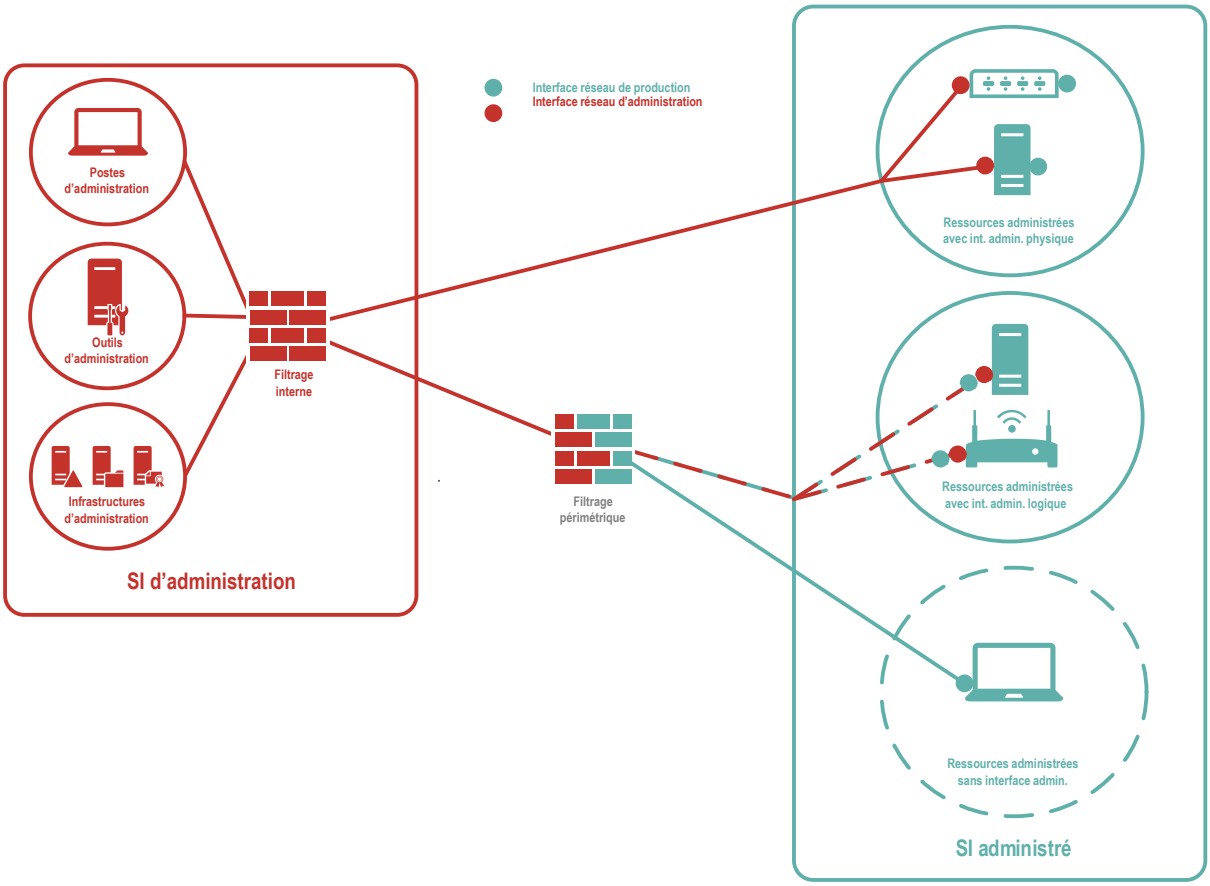


FIGURE 5.2 – Administration, sur un réseau local, à travers des interfaces d'administration dédiées (physiques ou logiques) ou une interface de production

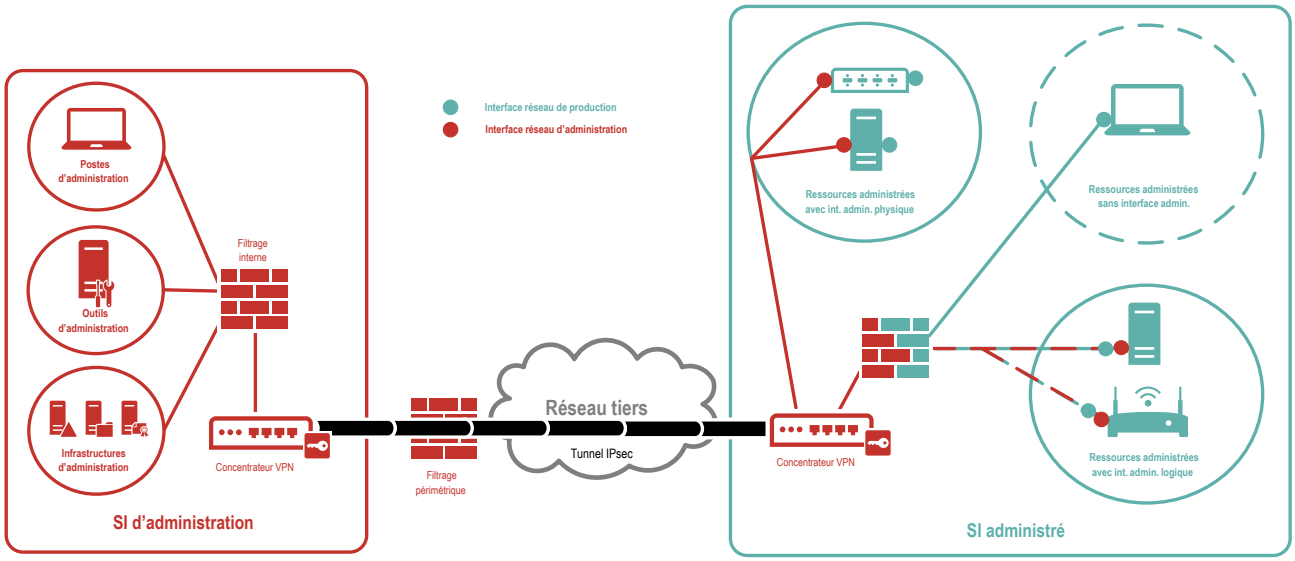


FIGURE 5.3 – Administration, sur un réseau étendu, à travers des interfaces d'administration dédiées (physiques ou logiques) ou une interface de production

6
Outils d'administration

Les outils d'administration, logiciels permettant la réalisation d'actions d'administration, sont mis à disposition des administrateurs, soit localement sur leur poste d'administration soit de façon déportée et centralisée sur des serveurs. Des mesures spécifiques à leur protection contre des tentatives de compromission ou des usages illicites doivent être mises en œuvre. Le cas particulier des outils d'administration d'un *cloud* public est abordé dans la section 13.6.

6.1 Cloisonnement des outils d'administration

Dans la continuité des principes de réduction de surface d'attaque décrits dans la section 3.2, la principale mesure vise à cloisonner les outils d'administration par zone d'administration. Pour rappel, à une zone d'administration du SI d'administration correspond une ou plusieurs zones de confiance du SI administré.

6.1.1 Outils d'administration locaux

Dans le cas d'outils d'administration locaux au poste d'administration, le cloisonnement par zone d'administration est difficilement applicable. Il est rappelé que ces outils doivent être déployés en fonction du strict besoin opérationnel conformément à R13.

6.1.2 Outils d'administration centralisés

Dans le cas d'outils d'administration centralisés, la mise en œuvre de serveurs dédiés par zone d'administration permet la mise en œuvre du cloisonnement recherché et facilite la mise à jour des outils.

R22

Déployer les outils d'administration sur des serveurs dédiés par zone d'administration

Les outils d'administration doivent être déployés par zone d'administration en fonction du juste besoin opérationnel. Cette mesure peut se traduire par la mise en œuvre de serveurs outils dédiés, intégrant par exemple les outils d'administration proposés par des éditeurs ou des équipementiers (ex. : client lourd ou service Web interagissant avec les ressources administrées).
Les recommandations de sécurisation logicielle des postes d'administration (R10, R11, R12, R13, R14) doivent être appliquées, dès que possible, aux serveurs outils d'administration.

En complément, la mise en œuvre de mécanismes de cloisonnement réseau physique ou de segmentation réseau logique (ex. : VLAN) et de filtrage (ex. : pare-feu) doivent garantir les seules

connexions légitimes depuis les postes d'administration vers les serveurs outils d'administration. Cette pratique contribue, en outre, à restreindre les risques de compromission, par rebond, d'une zone vers une autre.

R23

Appliquer un filtrage entre les postes d'administration et les serveurs outils d'administration

La recommandation R16 doit être appliquée rigoureusement entre les postes d'administration et les serveurs outils d'administration en autorisant uniquement les flux à l'initiative des postes d'administration.

6.2 Sécurisation des flux d'administration

Quelles que soient les mesures de cloisonnement retenues, les flux d'administration requièrent des protocoles utilisant des mécanismes de chiffrement et d'authentification (ex. : SSH, HTTPS, SFTP). L'objectif consiste à renforcer la confidentialité, l'intégrité et l'authenticité des flux d'administration.

R24

Utiliser des protocoles sécurisés pour les flux d'administration

Il est recommandé d'utiliser systématiquement, dès lors qu'ils existent, des protocoles et des outils d'administration utilisant des mécanismes de chiffrement et d'authentification robustes (cf. RGS [22]), en privilégiant les protocoles sécurisés standardisés et éprouvés (ex. : TLS ou SSH).
Le cas échéant, les protocoles non sécurisés doivent être explicitement désactivés ou bloqués.

Attention

Certains outils peuvent mettre en avant l'emploi de mécanismes de sécurité mais leur implémentation peut ne pas être conforme à l'état de l'art. Il convient donc de s'assurer par exemple des traces éventuelles générées par ces outils (ex. : condensat de mot de passe) et de vérifier le chiffrement de l'ensemble des informations.

Certains protocoles ou outils d'administration sont obsolètes et ne mettent pas en œuvre ces mécanismes cryptographiques. Dans ce cas, l'emploi de VPN IPsec, depuis le serveur outils ou le poste d'administration jusqu'au plus proche de la ressource administrée, permet de pallier ces carences.

R24 -

Protéger le cas échéant les flux d'administration dans un tunnel VPN IPsec

À défaut d'interfaces d'administration dédiées ou d'outils d'administration permettant le chiffrement et l'authentification de bout en bout, les flux d'administration doivent être protégés par la mise en œuvre d'un tunnel VPN IPsec, avec authentification mutuelle par certificats, depuis le serveur outils ou le poste d'administration vers les ressources administrées. Ce tunnel VPN IPsec doit être établi au plus près de la ressource d'administration et de la ressource administrée.

6.3 Rupture ou continuité des flux d'administration

Les actions d'administration imposent entre autres des exigences de traçabilité et de confidentialité. Suivant l'expression des besoins de sécurité élaborée dans le cadre de l'analyse de risque, il peut être souhaité soit d'assurer une rupture des échanges entre le poste d'administration et la ressource administrée, soit de garantir l'établissement de bout en bout d'une authentification puis d'une session. Les paragraphes suivants illustrent les deux cas d'usage : avec ou sans rupture protocolaire.

La figure 6.1 présente le cas d'usage de la mise en œuvre de rebonds dans une zone d'administration permettant d'appliquer un certain nombre de traitements tels le filtrage des connexions, l'authentification des administrateurs sur un portail frontal, un contrôle d'accès ou encore la journalisation des actions effectuées et des commandes exécutées par les administrateurs. De plus, lorsque le protocole d'administration d'une ressource est peu ou pas sécurisé, le recours à une rupture protocolaire peut être souhaitable en complément de R24-.

R25

Étudier la mise en œuvre d'une rupture protocolaire des flux d'administration

Pour la traçabilité des accès ou des actions d'administration, ou pour pallier des faiblesses de sécurité des protocoles d'administration, il est recommandé d'étudier la mise en œuvre d'une rupture protocolaire des flux d'administration.

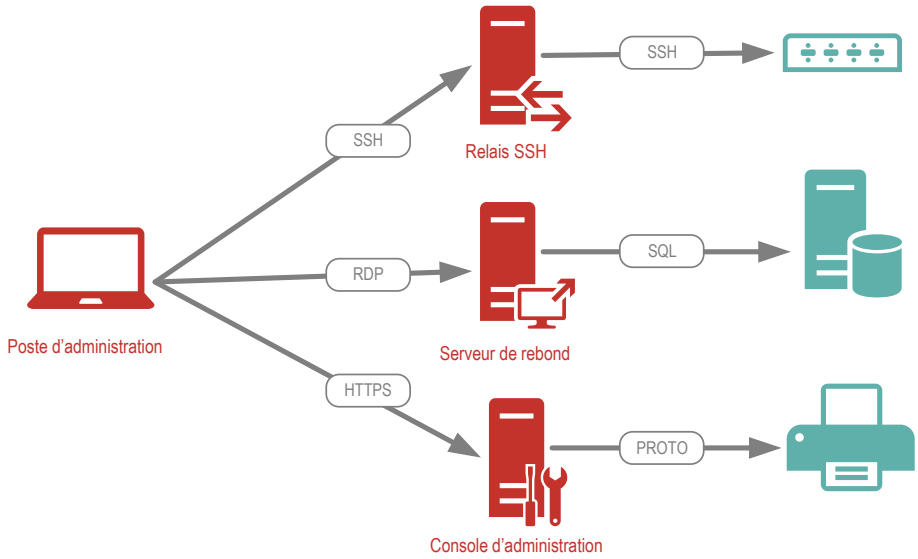


FIGURE 6.1 – Administration avec rupture protocolaire

Information

La section 13.1 traite plus en détails les problématiques d'architecture liées aux bastions d'administration.

Pour l'autre cas d'usage, sans rupture protocolaire, l'objectif consiste à ne pas rompre la session sécurisée, reposant sur des mécanismes cryptographiques de confiance (cf. figure 6.2).

R26

Renoncer à la rupture protocolaire pour les besoins en confidentialité

L'absence de rupture protocolaire doit être privilégiée en cas de besoin fort de confidentialité des flux d'administration et après une analyse de risque complémentaire. Le cas échéant, les protocoles utilisés doivent d'autant plus être sécurisés et configurés à l'état de l'art conformément à R24.

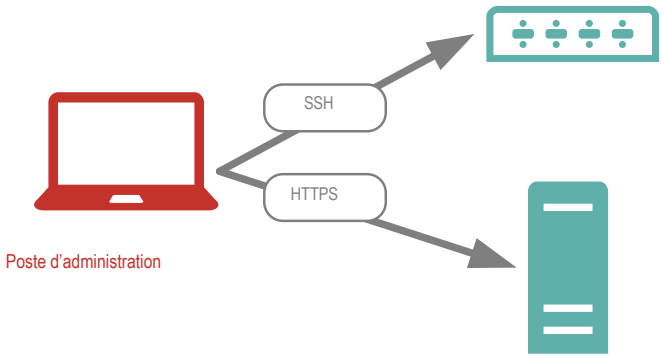


FIGURE 6.2 – Administration sans rupture protocolaire

(...)

EIGRP ou OSPF : quel protocole de routage répond le mieux aux besoins de votre réseau ?

Comprendre le protocole de routage EIGRP

Le protocole EIGRP (Enhanced Interior Gateway Routing Protocol) est un protocole de routage avancé à vecteur de distance, propriétaire de Cisco. Il est principalement utilisé dans les réseaux des grandes entreprises en raison de son évolutivité, de sa flexibilité et de sa robustesse. L'EIGRP utilise un algorithme unique connu sous le nom d'algorithme de mise à jour diffusante (DUAL) pour garantir une convergence rapide et éviter les boucles de routage. De plus, il prend en charge plusieurs protocoles de couche réseau tels qu'IP, AppleTalk et Novell IPX, ce qui le rend polyvalent dans divers environnements réseau.

Principales caractéristiques de l'EIGRP

L'EIGRP apporte plusieurs fonctionnalités distinctives. L'un d'eux est la prise en charge des masques de sous-réseau à longueur variable (VLSM) et du routage inter-domaine sans classe (CIDR), qui optimise l'utilisation des adresses IP au sein d'un réseau. Une autre caractéristique notable est sa capacité à effectuer un équilibrage de charge à coûts égaux et inégaux, en répartissant le trafic de données sur plusieurs chemins en fonction de leurs métriques respectives. De plus, l'EIGRP implémente des mises à jour partielles au lieu de mises à jour périodiques complètes, réduisant ainsi le trafic réseau et améliorant l'efficacité.

Configuration du routeur EIGRP

La configuration d'un routeur EIGRP implique plusieurs étapes. Dans un premier temps, nous activons le processus EIGRP et spécifions un numéro de système autonome (AS). Ensuite, nous définissons les adresses réseau que le processus EIGRP doit annoncer. De plus, nous pouvons configurer des paramètres facultatifs tels que les chemins maximaux pour l'équilibrage de charge, les pondérations métriques et l'authentification. Enfin, nous vérifions la configuration EIGRP à l'aide de diverses commandes show.

EIGRP vs autres protocoles de routage

Passerelle	Métrique	Algorithme	Temps de convergence	Évolutivité
EIGRP	Bande passante, délai, fiabilité, charge	DOUBLE	Rapide	Haute
OSPF	Coût (basé sur la bande passante)	SPF	Moyenne	Haute
RIP	Nombre de sauts	Bellman-Ford	Lent	Faible

Avantages de l'EIGRP

L'EIGRP offre plusieurs avantages par rapport aux autres protocoles de routage. Son temps de convergence rapide et sa prise en charge d'un équilibrage de charge à coûts inégaux le rendent très efficace. Ça aussi offre une qualité supérieure évolutivité, prenant en charge de grands réseaux avec de nombreux routeurs. De plus, sa compatibilité avec plusieurs protocoles de couche réseau ajoute à sa flexibilité. Enfin, l'utilisation de mises à jour partielles par l'EIGRP réduit considérablement le trafic réseau, améliorer les performances globales du réseau.

Qu'est-ce qu'OSPF ?

Le protocole OSPF (Open Shortest Path First) est un protocole de routage à état de liens utilisé dans les réseaux IP (Internet Protocol). Développé par l'Internet Engineering Task Force (IETF), OSPF est largement adopté en raison de sa gestion efficace des informations de routage et de son excellente évolutivité. OSPF calcule le chemin le plus court entre les nœuds à l'aide de l'algorithme de Dijkstra, ce qui en fait un choix très fiable pour les applications complexes.

Présentation du protocole de routage OSPF

OSPF fonctionne au sein d'un seul système autonome (AS) et utilise une conception de réseau hiérarchique. Il divise un AS en zones, toutes les zones étant connectées à une zone de base. Les routeurs OSPF échangent des annonces d'état de lien (LSA) qui contiennent des informations sur les liens, les états et les coûts des autres routeurs. Ces informations sont compilées dans une base de données d'état de liens (LSDB), qui est ensuite utilisée pour calculer l'arborescence des chemins les plus courts.

Configuration du réseau OSPF

La configuration d'OSPF implique plusieurs étapes. Tout d'abord, le processus OSPF est activé sur un routeur, puis les adresses réseau à annoncer sont définies. L'ID du routeur est défini, ce qui identifie de manière unique le routeur dans le processus OSPF. Des zones sont définies et des interfaces sont affectées à ces zones. Des paramètres facultatifs tels que l'authentification et les mesures de coût peuvent être configurés. La configuration est vérifiée à l'aide de diverses commandes show.

Comparaison : EIGRP et OSPF

<table>
<tr><td>RIPv1</td><td>RIPv2</td><td>IGRP</td><td>EIGRP</td><td>OSPF</td></tr>
<tr><td colspan="3">Protocole de routage à vecteur de distance</td><td>Vecteur de distance, protocoles de routage hybrides</td><td>Protocoles de routage à état de lien</td></tr>
<tr><td colspan="2">AD=120</td><td rowspan="2">AD=100</td><td>AD interne = 90</td><td></td></tr>
<tr><td colspan="2"></td><td>AD externe = 170</td><td>AD=110</td></tr>
<tr><td>Le CIDR n'est pas pris en charge</td><td>Prend en charge les réseaux CIDR, VLSM et discontinus</td><td>Le CIDR n'est pas pris en charge</td><td>Prise en charge des réseaux CIDR, VLSM et discontinus</td><td>Prend en charge les réseaux CIDR, VLSM et discontinus</td></tr>
<tr><td colspan="4">Prise en charge du résumé automatique</td><td>Ne prend pas en charge le résumé automatique, peut être résumé manuellement</td></tr>
</table>

houblon		Valeurs cumulées de bande passante et de délai de ligne pour une utilisation principale		lien aérien
Maximum 15 sauts		Maximum 255 sauts		libre
la libéralisation		Propriété de Cisco		la libéralisation
Seule la table de routage IP dans la RAM			La RAM contient la table des voisins, la table de topologie et la table de routage.	Hello crée une base de données voisine (table) – LSA crée une base de données d'état des liens (table de topologie) (routeurs avec le même ID de zone) – SPF calcule une table de routage
			Prend en charge simultanément trois protocoles réseau IP, IPX et APPLETALK.	Prise en charge uniquement des protocoles réseau IP
x		Configurez un numéro de système autonome (AS) pour distinguer les routeurs pouvant partager des informations de routage.		Configurez un ID de processus local et utilisez le numéro de zone pour minimiser les mises à jour sur la même zone, qui doit avoir la zone 0 comme zone de base.
Utilisation de la mise à jour du routage de diffusion UDP	Utilisation de la multidiffusion UDP 224.0.0.9	Utilisez UDP pour diffuser une légère mise à jour depuis le	Utiliser le protocole RTP 224.0.0.10 multicast, si aucune réponse, utiliser la retransmission d'adresse unicast 16	Les informations réseau sont d'abord transmises au DR via la multidiffusion 224.0.0.5, puis le DR utilise la multidiffusion 224.0.0.6 pour mettre à jour les routes vers les voisins.
Mises à jour des tables de routage		Mise à jour de la table de routage AS harmonisée	N'envoyer que les itinéraires avec plus de modifications	Déclencheur pour mettre à jour les itinéraires avec les modifications

Utilisation de l'algorithme Bellman-Ford			Convergence utilisant l'algorithme de diffusion (DUAL)	Convergence utilisant l'algorithme de Dijkstra (SPF)
x	Prise en charge de l'authentification peer-to-peer Texte.	x	Prend en charge l'authentification peer-to-peer MD5	Prend en charge l'authentification peer-to-peer Texte, MD5
X				Une fois configurés, des caractères génériques sont utilisés pour identifier le propriétaire du réseau. Tank L'algorithme de convergence lui-même rend OSPF véritablement sans boucle.
Si la commande Passive-Interface est utilisée sur une interface, l'interface accepte uniquement les mises à jour d'itinéraire et n'envoie pas de mises à jour d'itinéraire, réalisant ainsi une segmentation horizontale et empêchant les boucles d'itinéraire de se produire.			Si vous utilisez la commande Passive-Interfacet sur une interface, l'interface n'accepte ni n'envoie de mises à jour de routage, réalisant une segmentation horizontale et empêchant les boucles de routage.	

Au lieu d'un équilibrage de charge dynamique, les chemins vers la destination ont le même nombre de sauts et les charges sont uniformément réparties sur les lignes. Cela peut provoquer l'effet sténopé	Alloue intelligemment le trafic de paquets avec plus de bande passante, tout en équilibrant la charge à l'aide de liens avec la même métrique sur plusieurs interfaces.	L'équilibrage de charge est faible, différentes priorités sont attribuées aux chemins vers la destination, le paquet de transport ayant la priorité la plus élevée est utilisé et l'équilibrage de charge n'est lancé que s'il a la même priorité.

Avantages d'OSPF

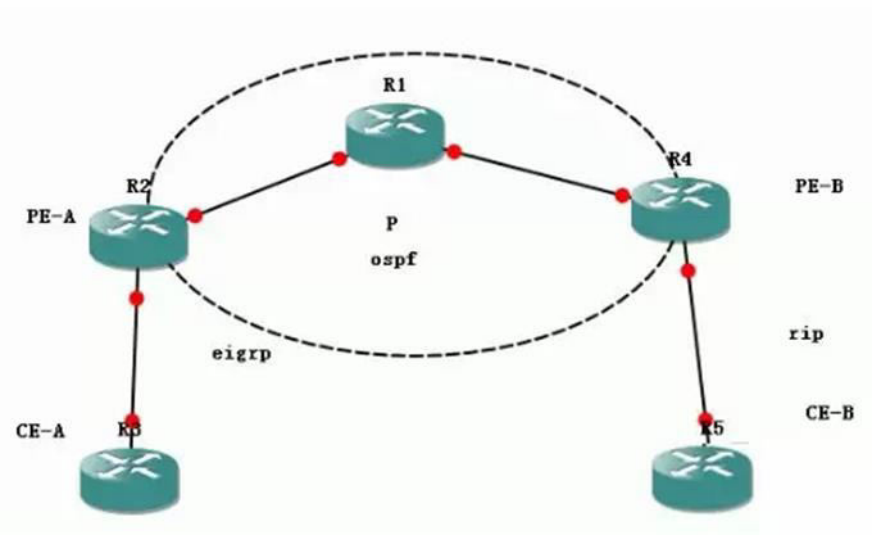
OSPF offre plusieurs avantages. Il n'a pas de limite de nombre de sauts, ce qui le rend adapté aux grands réseaux. Sa conception hiérarchique permet des mises à jour de routage efficaces, réduisant ainsi le trafic réseau. OSPF prend en charge plusieurs chemins à coût égal pour l'équilibrage de charge, et son utilisation de l'adressage multicast pour les mises à jour de routage améliore l'efficacité. Il prend également en charge les liens virtuels, garantissant la connectivité entre les zones non dorsales.

Table de routage OSPF

La table de routage OSPF contient les meilleurs chemins vers tous les réseaux connus. Chaque entrée comprend le réseau de destination, l'adresse du tronçon suivant et la mesure du coût. OSPF gère des tables de routage distinctes pour les routes intra-zone, inter-zone et externes. La table de routage est continuellement mise à jour pour refléter les changements dans la topologie du réseau, garantissant ainsi des informations de routage précises et à jour.

Principales différences entre EIGRP et OSPF

Dans le domaine des protocoles de routage, Enhanced Interior Gateway Routing Protocol (EIGRP) et Open Shortest Path First (OSPF) sont deux noms importants. Ils servent tous deux à déterminer le chemin le plus efficace pour les paquets de données à travers un réseau. Cependant, ils diffèrent sur plusieurs aspects, notamment leurs algorithmes sous-jacents, leur évolutivité, leurs délais de convergence, leurs processus de mise en œuvre, leurs techniques d'équilibrage de charge et leurs mesures de sécurité. Cet article examine ces différences clés et propose une comparaison complète pour aider les administrateurs réseau à prendre des décisions éclairées.



interconnexion d'entreprise mpls eigrp rip

Algorithmes de routage utilisés

L'EIGRP utilise l'algorithme Diffusing Update (DUAL), un algorithme avancé de vecteur de distance qui garantit une convergence rapide et des chemins sans boucle. D'autre part, OSPF est un protocole à état de liens qui utilise l'algorithme de Dijkstra pour calculer l'arbre du chemin le plus court. Alors que DUAL se concentre sur le maintien d'une table de routage équilibrée et optimisée, l'algorithme de Dijkstra se concentre sur le calcul du chemin le moins coûteux entre les nœuds.

Évolutivité et convergence

En termes d'évolutivité, EIGRP et OSPF sont capables de prendre en charge de grands réseaux. Cependant, l'EIGRP présente généralement des temps de convergence plus rapides en raison de son utilisation de successeurs réalisables. À l'inverse, les temps de convergence d'OSPF peuvent être plus lents, en particulier dans les réseaux plus grands, car il doit recalculer l'intégralité de l'arborescence des chemins les plus courts lorsque des modifications du réseau se produisent.

Implémentation dans les réseaux Cisco

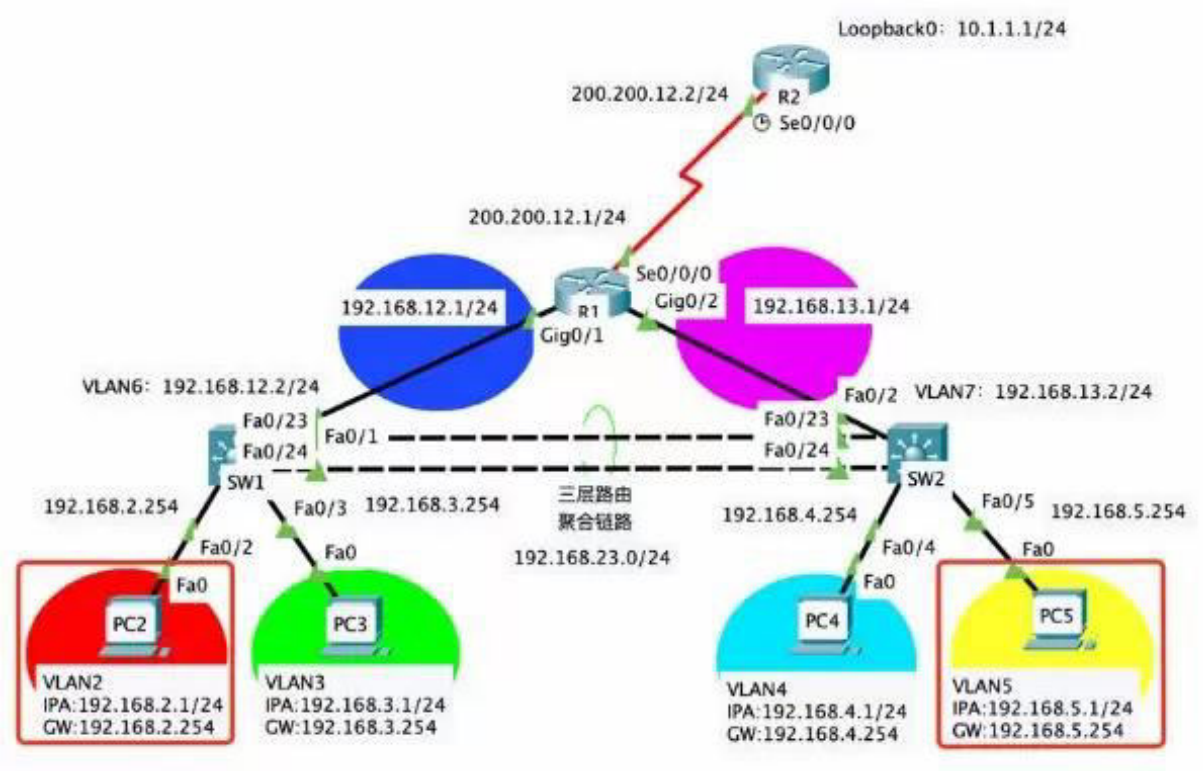
EIGRP est un protocole propriétaire de Cisco, ce qui signifie qu'il est entièrement intégré et pris en charge dans les appareils Cisco. Il offre une interopérabilité transparente entre les différents routeurs et commutateurs Cisco. À l'inverse, OSPF est un protocole standard ouvert développé par l'Internet Engineering Task Force (IETF). Bien qu'il soit pris en charge sur les appareils Cisco, il peut également être implémenté sur des appareils non Cisco, ce qui le rend plus polyvalent dans un environnement multifournisseur.

Techniques d'équilibrage de charge

L'EIGRP prend en charge l'équilibrage de charge à coûts égaux et inégaux, offrant ainsi une flexibilité dans la répartition du trafic sur plusieurs chemins. Cette fonctionnalité peut optimiser l'utilisation des ressources réseau et améliorer les performances globales. En revanche, OSPF ne prend en charge que l'équilibrage de charge à coût égal, ce qui limite sa flexibilité dans certains scénarios de réseau.

Sécurité et authentification

EIGRP et OSPF offrent tous deux des fonctionnalités de sécurité, notamment des mécanismes d'authentification pour sécuriser les mises à jour de routage. EIGRP prend en charge l'authentification en texte brut et MD5, tandis que OSPF prend en charge l'authentification en texte brut, MD5 et SHA. Cependant, il est important de noter que ces méthodes d'authentification ne chiffrent pas le trafic de données : elles authentifient simplement l'identité des routeurs échangeant des informations de routage.



expérience de configuration complète du protocole eigrp nat

Quand choisir l’EIGRP ?

Le protocole EIGRP (Enhanced Interior Gateway Routing Protocol) est un protocole de routage puissant principalement utilisé dans les réseaux d'entreprise à grande échelle. Sa capacité à s'adapter rapidement aux changements du réseau, sa prise en charge de divers protocoles de couche réseau et son évolutivité en font un concurrent sérieux pour de nombreuses conceptions de réseau. Cependant, la décision de choisir l'EIGRP doit être basée sur les exigences spécifiques du réseau, la topologie, la taille et l'infrastructure en place.

Application dans des topologies de réseau spécifiques

L'EIGRP excelle dans plusieurs topologies de réseau. Il est particulièrement efficace dans les topologies hub-and-spoke où un ou plusieurs routeurs centraux (hubs) se connectent à plusieurs routeurs périphériques (spokes). La capacité de l’EIGRP à effectuer un équilibrage de charge à coûts inégaux lui permet de répartir efficacement le trafic sur plusieurs chemins dans cette topologie. Dans les réseaux maillés, où les routeurs disposent de plusieurs connexions à d’autres routeurs, les mécanismes de convergence rapide et de prévention des boucles d’EIGRP garantissent la stabilité et l’efficacité du réseau.

Avantages de l'EIGRP dans les grands réseaux

Dans les grands réseaux, EIGRP offre plusieurs avantages. Son temps de convergence rapide garantit une perturbation minimale lors des modifications du réseau, maintenant ainsi une haute disponibilité. L'utilisation de mises à jour partielles par l'EIGRP réduit le trafic réseau, ce qui est crucial dans les grands réseaux où des mises à jour complètes fréquentes peuvent entraîner une congestion. De plus, sa prise en charge de VLSM et CIDR permet un adressage IP efficace, ce qui constitue souvent un défi dans les environnements à grande échelle.

Limites de la mise en œuvre de l'EIGRP

Malgré ses atouts, l'EIGRP présente certaines limites. En tant que protocole propriétaire de Cisco, il manque d'interopérabilité avec les appareils non Cisco, ce qui limite potentiellement sa mise en œuvre dans des environnements multifournisseurs. De plus, bien que l'EIGRP prenne en charge divers protocoles de couche réseau, il se concentre principalement sur IP, ce qui pourrait limiter son applicabilité dans les réseaux dépendant fortement de protocoles non IP.

Meilleures pratiques de déploiement EIGRP

Un déploiement approprié de l'EIGRP implique de suivre les meilleures pratiques. Il s'agit notamment de limiter le nombre de routeurs dans un système autonome EIGRP pour garantir une complexité gérable et de maintenir une configuration EIGRP cohérente sur tous les routeurs pour plus de stabilité. Il est également recommandé d'utiliser des interfaces passives là où l'EIGRP n'est pas nécessaire et d'implémenter un résumé de route pour réduire la taille des tables de routage.

Prise en charge EIGRP pour l'infrastructure propriétaire

Le statut de l'EIGRP en tant que protocole propriétaire de Cisco signifie qu'il offre une prise en charge robuste de l'infrastructure propriétaire de Cisco. Il s'intègre parfaitement au matériel réseau de Cisco, y compris ses routeurs, commutateurs et pare-feu. Cette intégration garantit des performances optimales, une utilisation efficace des ressources et une gestion facile au sein d'une infrastructure réseau basée sur Cisco.

Quand choisir OSPF ?

OSPF (Open Shortest Path First) est un protocole de routage à état de liens robuste qui est largement utilisé dans de nombreux types d'environnements réseau. Il offre un routage efficace, une évolutivité et une prise en charge des topologies de réseau complexes. Cependant, la décision d'utiliser OSPF doit dépendre de divers facteurs tels que la taille du réseau, la topologie, la diversité des fournisseurs et les cas d'utilisation spécifiques. Cet article approfondira ces considérations, fournissant un guide complet sur le moment de choisir OSPF.

Utilitaire basé sur des scénarios d'OSPF

OSPF montre sa force dans divers scénarios en raison de ses caractéristiques uniques. Par exemple, les temps de convergence rapides d'OSPF minimisent les temps d'arrêt dans les réseaux soumis à de fréquents changements de topologie. Dans les conceptions de réseau hiérarchiques, le concept de zone OSPF permet une gestion efficace des informations de routage, réduisant ainsi la surcharge des routeurs. De plus, la métrique basée sur les coûts d'OSPF facilite un trafic efficace ingénierie en réseaux où l'optimisation de la bande passante est cruciale.

OSPF dans les environnements multifournisseurs

En tant que protocole standard ouvert développé par l'Internet Engineering Task Force (IETF), OSPF offre une large compatibilité entre les appareils de différents fournisseurs. Cette interopérabilité en fait un excellent choix pour les environnements multifournisseurs, offrant une flexibilité dans la sélection du matériel et évitant toute dépendance vis-à-vis d'un fournisseur. L'adoption généralisée d'OSPF garantit également une large base de connaissances et un soutien communautaire, facilitant le dépannage et l'optimisation.

Utilisation optimale d'OSPF dans les petits réseaux

Même si OSPF est évolutif et peut prendre en charge de grands réseaux, il fonctionne également de manière optimale dans les petits réseaux. Sa capacité à calculer le chemin le plus court à l'aide de l'algorithme de Dijkstra garantit un routage efficace, même dans les petites topologies de réseau. De plus, la prise en charge par OSPF de VLSM et CIDR permet un adressage IP flexible et efficace, ce qui profite aux petits réseaux avec des espaces d'adressage IP limités.

Inconvénients de la mise en œuvre d'OSPF

Malgré ses nombreux avantages, OSPF présente certaines limites. Sa complexité peut entraîner une utilisation plus élevée du processeur et de la mémoire sur les routeurs, en particulier dans les grands réseaux comportant de nombreuses entrées de routage. De plus, la mesure des coûts d'OSPF, bien qu'utile pour l'ingénierie du trafic, peut être difficile à configurer correctement. Une mauvaise configuration peut conduire à des chemins de routage sous-optimaux et à une réduction des performances du réseau.

Interconnexion OSPF avec BGP

OSPF peut interagir efficacement avec le Border Gateway Protocol (BGP), un protocole couramment utilisé dans les réseaux fédérateurs Internet. OSPF peut être utilisé pour le routage intra-domaine au sein d'un système autonome (AS), tandis que BGP gère le routage inter-domaine entre les AS. Cette combinaison garantit un routage efficace au sein et entre les grands réseaux, faisant d'OSPF un choix stratégique pour les organisations opérant à l'échelle Internet.

FAQ

Q : Qu'est-ce qui distingue l'EIGRP et l'OSPF ?

R : EIGRP, un protocole de routage à vecteur de distance, forme des tables de routage avec des mesures de bande passante, de délai, de charge et de fiabilité. À l'inverse, OSPF, un protocole de routage à état de liens, utilise une métrique basée sur le coût pour identifier le chemin le plus court.

Q : Dans quelles circonstances l'EIGRP est-il un meilleur choix que l'OSPF ?

R : EIGRP est généralement choisi pour les réseaux plus petits, principalement composés de routeurs Cisco, en raison de son équilibrage de charge à coût inégal et de sa convergence rapide.

Q : Quand OSPF est-il un choix plus approprié que EIGRP ?

R : OSPF est généralement choisi pour les réseaux multifournisseurs plus grands ou pour ceux dotés de nombreuses liaisons multi-accès non diffusées en raison de sa structure hiérarchique et de son utilisation efficace des ressources.

Q : Quels sont les points communs entre l'EIGRP et l'OSPF ?

R : EIGRP et OSPF sont tous deux des protocoles de routage dynamique dans les réseaux IP, visant à fournir des chemins efficaces pour la transmission de données.

Q : Comment fonctionne l'EIGRP en termes de fonctionnement du protocole ?

R : EIGRP partage les informations de routage avec les routeurs voisins via l'algorithme de mise à jour de diffusion (DUAL) et garantit la livraison des paquets avec un protocole de transport fiable.

Q : Quels sont les principaux composants du fonctionnement OSPF ?

R : Les routeurs OSPF échangent des annonces d'état de lien (LSA) pour maintenir une base de données de la topologie du réseau, puis utilisent l'algorithme SPF (Shortest Path First) pour calculer le chemin le plus court vers chaque destination.

Q : Comment les informations de routage sont-elles échangées dans EIGRP et OSPF ?

R : EIGRP échange des informations de routage avec des routeurs directement connectés via un protocole propriétaire, tandis que OSPF diffuse des informations de routage via des publicités d'état de lien.

Q : Quels avantages OSPF offre-t-il par rapport à EIGRP ?

R : OSPF prend en charge l'équilibrage de charge à coûts inégaux et plusieurs chemins vers la même destination, optimisant ainsi les ressources réseau. Il crée également une hiérarchie au sein des grands réseaux pour un échange efficace d'informations de routage.

Q : Quels sont les avantages de l'EIGRP par rapport à OSPF ?

R : EIGRP offre une convergence plus rapide et un routage sans boucle, ce qui le rend idéal pour les réseaux de domaine à routage unique. Ça aussi facilite l'efficacité met à jour et minimise l'utilisation de la bande passante pour la distribution des informations de routage.

Q : EIGRP et OSPF peuvent-ils coexister dans le même réseau ?

R : Bien qu'il soit techniquement réalisable, le déploiement d'EIGRP et d'OSPF sur le même réseau n'est pas standard en raison de la complexité et des conflits potentiels qu'il introduit. Il est conseillé de sélectionner et de mettre en œuvre un seul protocole de routage sur l'ensemble du réseau.

Références

1. **Etude comparative des protocoles EIGRP et OSPF basée sur la convergence des réseaux** – Cet article académique fournit une étude comparative approfondie entre les protocoles EIGRP et OSPF axée sur la convergence des réseaux. Il souligne que l'EIGRP fonctionne mieux dans un réseau plus vaste que l'OSPF.
2. **Analyse des performances des protocoles de routage RIP, OSPF, IGRP et EIGRP dans un réseau** – Une analyse approfondie de plusieurs protocoles de routage, notamment EIGRP et OSPF, discutant du nombre de mises à jour nécessaires, de la réponse aux pannes et de la surcharge sur chaque routeur.
3. **Décision de mise en œuvre du protocole de routage dynamique entre EIGRP, OSPF et RIP basée sur le contexte technique à l'aide du modélisateur OPNET** – Cette source traite des exigences techniques des différents protocoles de routage, y compris la puissance du processeur et la RAM requises par RIP par rapport aux autres.
4. **Évaluation des protocoles de routage OSPF et EIGRP pour ipv6** – Une évaluation ciblée des protocoles de routage OSPF et EIGRP spécifiquement pour IPv6. Le document discute de la nécessité d'exécuter les deux versions d'OSPF simultanément.
5. **Analyse des performances et optimisation des routes : redistribution entre les protocoles de routage EIGRP, OSPF et BGP** – Cet article se concentre sur l'optimisation et la redistribution des routes entre les protocoles EIGRP, OSPF et BGP. Il discute de l'évolution des protocoles propriétaires de Cisco.
6. **Analyse basée sur la simulation de la perspective du routeur du protocole de routage EIGRP et OSPF pour un modèle organisationnel** – Cette source fournit une analyse basée sur la simulation du point de vue du routeur sur les protocoles EIGRP et OSPF pour un modèle organisationnel.

7. **Étude comparative basée sur la simulation sur EIGRP/IS-IS et OSPF/IS-IS** – Cette source présente une étude comparative sur EIGRP/IS-IS et OSPF/IS-IS basée sur des résultats de simulation. Il évalue la robustesse de ces protocoles.
8. **Solutions de conception de réseau EIGRP** – Un livre axé sur les solutions de conception de réseau EIGRP. Il fournit un aperçu des problèmes d'échange de routes avec OSPF et de la manière dont l'EIGRP a été le premier protocole à les résoudre.
9. **Sur la comparaison des performances des protocoles de routage RIP, OSPF, IS-IS et EIGRP** – Cet article compare les performances de plusieurs protocoles de routage, notamment EIGRP et OSPF. Il suggère de créer un réseau et d'utiliser les protocoles pour décider celui qui convient le mieux aux besoins du réseau.
10. **Analyse des performances des protocoles de routage OSPF et EIGRP pour un réseautage Internet plus écologique** – Cette source fournit une analyse des performances d'OSPF et d'EIGRP pour un réseautage Internet plus durable. Cela suggère que l'EIGRP est plus efficace en termes de CPU que l'OSPF pour les applications en temps réel.

DOCUMENT 7

usine-digitale.fr - 8 juillet 2024

Comment Orange Cyberdefense aide les entreprises à se protéger grâce à ses campus

Orange Cyberdefense a déployé un réseau de campus dédiés à la cybersécurité des entreprises. Fin juin, il ouvrait les portes de son entité marseillaise, qui recouvre l'ensemble de son offre.

© Florian Wehde

Nous avons visité le campus d'Orange Cyberdéfense basé à Marseille, qui vient d'ouvrir.

Situé à Marseille (Bouches-du-Rhône), à quelques centaines de mètres du Port, le Campus Orange Cyberdefense joue plutôt la discrétion. Sur 1100 m2, 105 experts en cybersécurité se répartissent les spécialités (hackers éthiques, ingénieurs, analystes, auditeurs…) pour aider les entreprises de Provence-Alpes-Côte d'Azur, Corse et Monaco, quelle que soit leur taille, à prévenir, détecter ou réagir à des attaques sur leurs sites web, leurs serveurs, leurs équipements ou leurs données.

Orange Cyberdefense représente un chiffre d'affaires de 1,07 milliard d'euros en 2023, en croissance de 11%, et emploie 3000 collaborateurs à travers le monde qui interviennent pour 9000 clients. La structure a analysé 129 000 incidents en 2023 et agi sur la fermeture de 40 000 sites internet suspects.

"Nous sommes le leader en Europe des services managés sécurisés, avec 22 centres positionnés dans 12 pays, explique le directeur régional, Alexandre Gazzola. *Plus de 500 sources différentes approvisionnent en continu l'intelligence de notre système de données. En France, Marseille a la particularité de réunir une équipe multi-expertises. C'est une vraie flexibilité puisque la valeur ajoutée en cybersécurité vient du partage de connaissances et de compétences. Quand nous avons démarré ici en 2016, nous n'étions que cinq personnes."*

Le lieu délivre des formations, procède à des démonstrations, sensibilise aux techniques ou à la gestion des incidents de cybersécurité dans des administrations publiques, des industries, des établissements de santé, des communes… *"Nous avons peu à peu étendu nos cibles jusqu'à la TPE ou la profession libérale. Aujourd'hui, de plus en plus de dirigeants d'entreprises nous sollicitent pour discuter des meilleures manières de gérer les crises",* poursuit Alexandre Gazzola.

Une intuition humaine indispensable

Orange Cyberdefense recouvre trois domaines d'activités. D'abord, la prévention qui permet d'explorer toutes les vulnérabilités du système d'information d'une entreprise, en simulant des attaques et la réactivité des barrières qui leur sont opposées. Ensuite, la détection, lorsqu'une menace apparaît pour en cerner l'étendue et la bloquer. Enfin, la protection avec un accompagnement personnalisé des clients selon l'ampleur des risques cyber auxquels leurs activités les exposent.

Nicolas Bourras, 24 ans, s'est formé tout seul au hacking, passionné par le côté "jeu vidéo" du défi. Chez Orange Cyberdefense, il traque les fragilités des clients qui font appel au Campus dans le cadre d'un périmètre et d'une durée que ces derniers définissent. Il ne mène pas d'attaque surprise. Ses interventions donnent lieu à la transmission d'un rapport détaillé.

"Nous pouvons agir à distance, dans un établissement ou le siège de l'entreprise, explique-t-il. *Grâce à ce rapport, le client retrouve toutes les démarches effectuées, ça participe à sa prise de conscience. Une attaque peut, par exemple, modifier les prix qu'il affiche sur son site web, récupérer des mots de passe via la messagerie de salariés, arrêter la chaîne de production d'une usine, pirater des badges d'accès ou une porte de garage, contrefaire une marque… Mon action démontre l'impact potentiel d'une faille. Le management de la surface d'attaque permet de vérifier l'ensemble des actifs exposés"*.

Pour le jeune homme, *"le contexte du métier change chaque semaine"*. Si, à ses yeux, l'intelligence artificielle automatisera demain certaines de ses tâches, il s'avoue convaincu qu'un tel domaine implique *"une intuition que seul un être humain peut avoir pour explorer un endroit spécifique d'un système"*. Sa vision sert aussi à Orange Cyberdefense. *"En connaissant bien les techniques d'attaque, on favorise leur analyse et l'offre de solutions à proposer,"* dit-il.

Une réactivité fondée sur la criticité

Son collègue Jules Bauchet, analyste cyber, supervise, lui, une équipe « MicroSoc » concentrée sur la détection d'attaques chez des clients disposant de 20 à 3 000 licences. Chaque analyste accompagne 20 à 40 clients. *"Certaines attaques sont plus critiques que d'autres, nous sommes engagés sur une réactivité de traitement par rapport à ce niveau de criticité. Nos outils sont développés en interne. La logique est d'aller vers une industrialisation des modes de détection pour apporter les réponses les plus rapides aux besoins des clients"*.

Lorsque l'attaque s'avère complexe, plusieurs analystes s'y mobilisent dessus. La surveillance s'opère 24h sur 24, 7 jours sur 7. *"Les astreintes seront renforcées pendant les Jeux Olympiques",* confie Jules Bauchet. Son service peut repérer si une tentative d'attaque provient de l'étranger. L'événement peut y être propice. Pour protéger efficacement un système, Orange Cyberdefense va jusqu'à opérer du sur-mesure pour des clients potentiellement soumis à un grand nombre de menaces de sources multiples. A l'image du monde maritime, qu'il concerne un navire de commerce, un paquebot de croisière, un yacht…

Selon la configuration, le danger peut venir de l'architecture du système, pas toujours lisible aux propriétaires successifs compte tenu de la durée de vie de l'embarcation, de l'environnement maritime (stabilité, connectivité…), de passagers mal intentionnés, du personnel navigant qui peut partager un même poste de travail… *"Un bateau est une usine flottante, résume Alexandre Gazzola. Nous réalisons des audits cybersécurité à bord, des détections de menaces, des simulations de crise, nous pouvons installer des bornes de nettoyage de clés USB…".*

Une architecture d'interconnexion de navires a été conçue en réalité virtuelle pour un client qui disposait d'une flotte de plusieurs bateaux qui communiquaient via un ancien système Cisco. *"Aujourd'hui, il dispose d'une vision globale et compréhensible du détail des services que nous lui avons apportés pour se protéger",* assure Frédéric Spenatto, architecte cyber.

Privileged Access Management & Bastion informatique pour protéger et contrôler vos comptes à privilèges

Au sein des systèmes d'information, certains utilisateurs se distinguent par leurs privilèges spéciaux. Il s'agit, par exemple des Directeurs ou Responsables des Services Informatiques (DSI et RSSI), des Administrateurs Systèmes et Réseaux, des Responsables d'infrastructures, mais également des prestataires notamment les télémainteneurs …

Qu'ils soient des membres internes à l'entreprise ou des intervenants externes, ces acteurs jouent un rôle crucial dans l'organisation, la gestion et l'évolution des SI. Mais avec ces privilèges, viennent aussi des responsabilités et des risques significatifs.

Nous vous proposons de voir en quoi le Privileged Access Management et la mise en place d'un bastion informatique peut vous permettre de protéger et de contrôler vos comptes à privilèges (interne et externe).

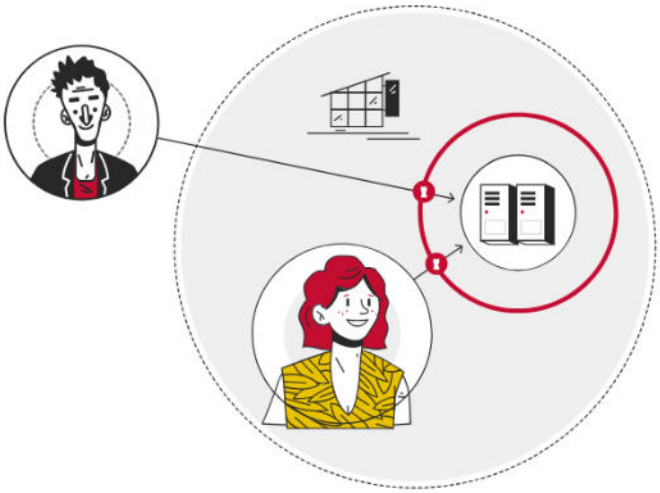
Menaces et enjeux de la gestion des comptes à accès privilégiés

Les menaces

Les menaces qui pèsent sur les comptes à privilèges sont nombreuses et potentiellement dévastatrices pour les organisations en cas de cyberattaques ou de malveillance. Les cybercriminels ciblent souvent ces comptes, sachant qu'ils détiennent des accès pour les parties les plus sensibles d'un système d'information. Les failles de sécurité, les mots de passe faibles ou connus par les utilisateurs, et les attaques ciblées sont autant de risques pour les entreprises.

Les enjeux de la gestion des comptes à accès privilégiés

La gestion des comptes et utilisateurs à accès privilégiés est cruciale pour atténuer ces menaces. Vous déterminez quelles sont les personnes qui auront accès aux différentes ressources de votre SI. Cette gestion vise à contrôler et à surveiller de manière proactive les actions des utilisateurs à privilèges, à garantir la confidentialité des informations sensibles, et à assurer la conformité des organisations avec les réglementations, comme le RGPD.



Nous recommandons alors la mise en place d'un bastion informatique ou d'une solution de PAM :
Privileged Access Management.

Bastion d'administration Vs Privileged Access Management : définissons …

« Bastion informatique » et « Privileged Access Management » (PAM) sont deux concepts liés à la cybersécurité, mais ils ont des fonctions légèrement différentes dans la protection des systèmes d'information. Voici une comparaison entre les deux approches :

Bastion informatique :

1. Point d'entrée sécurisé : Un bastion cybersécurité est un point d'entrée sécurisé permettant aux administrateurs de systèmes d'information d'accéder aux ressources informatiques sensibles. Il s'agit souvent d'un serveur spécialement configuré et renforcé.

2. Contrôle des accès : Un bastion informatique est conçu pour gérer et contrôler strictement les accès des administrateurs aux systèmes et aux données critiques. Il s'assure que seules les personnes autorisées : les utilisateurs à privilèges sélectionnés, peuvent accéder à ces ressources.

3. Traçabilité : Le bastion d'administration enregistre généralement toutes les activités effectuées par les utilisateurs, assurant ainsi une traçabilité complète des actions réalisées.

4. Protection contre les menaces : Ils sont configurés pour prévenir et protéger des tentatives d'intrusion et d'attaques ciblant les comptes à privilèges.

Privileged Access Management PAM :

1. Gestion des privilèges : Le PAM informatique englobe un ensemble de solutions et de bonnes pratiques visant à gérer les comptes à privilèges de manière sécurisée. Cela inclut la gestion des identifiants, la rotation des secrets, la délégation des accès, le coffre-fort numérique etc.

2. Contrôle d'accès : Le Privileged Access Management assure que seuls les utilisateurs autorisés peuvent accéder aux ressources cibles, sur le principe du moindre privilège ou least privilege. Il offre des fonctionnalités de contrôle d'accès granulaire.

3. Audit et conformité : Il génère des rapports ou journaux sur les activités des comptes à privilèges, ce qui est essentiel pour répondre aux exigences de conformité réglementaire et pour détecter toute activité suspecte.

4. Réduction des risques : Le PAM Privileged Access Management vise à réduire les risques liés aux comptes à privilèges. Il protège ces comptes tout en permettant un accès sécurisé lorsque c'est nécessaire.

En résumé, un bastion est généralement **un point d'entrée sécurisé pour les administrateurs**, tandis que le PAM est un **ensemble de pratiques, logiciels et technologies visant à gérer et à sécuriser les comptes à privilèges** dans l'ensemble d'une organisation ou d'un système d'information.

Précisons les fonctionnalités d'une solution de Privileged Access Management

Autoriser et contrôler les accès tiers et utilisateurs à privilèges

Une solution PAM offre une visibilité en temps réel sur les actions entreprises par les utilisateurs à privilèges qu'ils fassent partie de vos collaborateurs ou qu'ils soient prestataires externes, tiers … Ces derniers peuvent être des consultants, des sous-traitants, des partenaires, des entreprises de maintenance…

Elle permet d'autoriser et de contrôler leurs accès aux ressources informatiques, de notifier les connexions et logs, et de suivre leurs activités précisément.

Renforcer la sécurité de vos comptes à privilèges

La non-divulgation des identifiants et secrets *(mots de passe, clés …)* fait partie des outils du PAM et est un levier essentiel pour réduire les risques. En effet, grâce au coffre-fort d'identifiant secondaire les secrets des ressources ne sont plus connus de vos utilisateurs. Il offre une solution performante pour gérer efficacement les rotations d'équipes et sécuriser davantage les ressources cibles.

Traçabilité et conformité avec les réglementations

Comme précédemment évoqué, une solution PAM informatique assure une traçabilité complète des actions effectuées sur le système d'information. Elle facilite l'identification rapide de l'origine d'un incident et assure la conformité avec les normes, les règlementations et les recommandations en vigueur (ANSSI, ISO 27001, RGPD, OSE, TISAX…).

Une réglementation en mouvement !

L'augmentation des cyberattaques

Nous en parlions en début d'article, les cyberattaques sont devenues de plus en plus sophistiquées et fréquentes. Les cybercriminels ciblent délibérément les comptes à accès à privilèges car ces comptes détiennent les droits pour accéder aux parties les plus sensibles des systèmes informatiques d'une organisation. En compromettant ces comptes, les attaquants peuvent causer d'énormes dommages, allant de la perte de données à des perturbations majeures et des pertes financières importantes.

L'action des pouvoirs publics et les réglementations en évolution

Face à cette menace croissante, les gouvernements et les autorités régulatrices ont réagi en mettant en place des réglementations plus strictes en matière de sécurité des données. Le Règlement Général sur la Protection des Données (RGPD) de l'Union européenne et la directive Network and Information Systems (NIS2) en sont de bons exemples. Ces réglementations imposent des exigences strictes aux organisations en matière de protection des données personnelles et de prévention des cyberattaques. Un volet essentiel de la conformité à ces réglementations est la gestion adéquate des comptes à accès privilégiés.

En conclusion, la mise en place d'une solution de PAM est devenue incontournable pour toute organisation souhaitant garantir la sécurité de ses systèmes d'information, se conformer aux réglementations en vigueur et prévenir les risques liés aux comptes à privilèges.

Le rôle de l'IA dans la gestion de réseau

L'intelligence artificielle (IA) fait fureur. Elle est largement présentée comme la panacée pour améliorer les performances de l'entreprise dans un large éventail de domaines différents. Comment, en particulier, l'IA améliore-t-elle la gestion des réseaux informatiques ?

Le terme IA trouve ses origines dans la science-fiction et est souvent lié à des histoires bien connues sur les machines qui tentent de conquérir le monde. Maintenant que l'IA est devenue une réalité, le concept a changé, mais le principe des ordinateurs capables de prendre des décisions en toute indépendance est au cœur de ce concept.
Fondamentalement, dans le contexte des systèmes informatiques, l'intelligence artificielle analyse de grandes quantités de données et fournit des informations basées sur ses découvertes. Associée à l'apprentissage automatique, elle peut être utilisée pour automatiser la prise de décision en réponse à différents événements et effectuer des tâches sans intervention humaine.

L'attrait de l'IA dans la gestion de réseau

Dans les réseaux informatiques, l'IA et l'apprentissage automatique sont désormais utilisés pour analyser en continu de grandes quantités de données à l'aide d'algorithmes sophistiqués afin de déterminer ce qui se passe exactement sur le réseau, de faire des prévisions et de réagir aux événements au fur et à mesure qu'ils se produisent. Cette capacité à analyser intelligemment les données du réseau et à en tirer des informations détaillées sur les performances du réseau sans intervention humaine est au cœur de son attrait.
L'IA suscite autant d'attention dans le monde informatique, car elle permet une automatisation intelligente de nombreuses tâches, un gain de temps considérable et l'amélioration de l'efficacité opérationnelle. Elle s'applique parfaitement à la gestion du réseau où de nombreuses fonctions impliquées dans le fonctionnement efficace d'un réseau peuvent être automatisées, améliorant considérablement les performances, le dépannage et la sécurité du réseau.
Prenons l'exemple simple d'une fonction de commutation réseau qui existe depuis longtemps : la détection de bouclage. Il s'agit d'une fonctionnalité sur les switches smart et administrés qui a permis aux administrateurs réseau de gagner énormément de temps en cas de mauvaise configuration accidentelle ou intentionnelle du réseau. Une boucle réseau se produit lorsqu'un câble d'un port de switch se connecte à un autre port du même switch ou du même réseau. Le bouclage provoque une tempête de diffusion qui met le réseau à rude épreuve car le trafic réseau est continuellement amplifié au lieu de s'arrêter à sa destination prévue. Avec la détection de bouclage, lorsque cela se produit, l'un des ports concernés est automatiquement fermé, ce qui atténue le problème. Sans détection de bouclage, l'administrateur réseau doit localiser et corriger manuellement le défaut qui peut se trouver n'importe où sur l'ensemble du réseau.
L'IA et l'apprentissage machine réduisent les temps d'arrêt et les coûts d'exploitation, facilitent une maintenance préventive tout en faisant gagner du temps aux administrateurs réseau. L'évolution du rôle de l'IA dans ce domaine permet aux entreprises, en particulier les PME, de gérer leur réseau plus efficacement et nous rapproche des réseaux capables d'autorétablissement et de la gestion de réseau sans intervention.

Utilisation des données du journal réseau

Dans n'importe quel réseau informatique, de grandes quantités de données machine sont générées en permanence par les processus internes et via les journaux de serveur, les contrôleurs Wi-Fi, les applications, les appareils connectés et autres équipements de réseau. Dans une configuration de réseau classique, une grande partie de ces données s'accumule dans des journaux et est rarement consultée. L'introduction de l'IA et de l'apprentissage machine permet aux systèmes de gestion de réseau, par le biais de l'automatisation, d'interpréter ces données, de déterminer ce qui se passe dans les moindres détails et d'utiliser ces informations pour améliorer continuellement les performances du réseau et les temps d'arrêt. De plus, ces opérations sont effectuées plus rapidement et plus précisément que ce qu'aucun humain ne pourrait faire.
L'IA et l'apprentissage machine peuvent être utilisés pour détecter les problèmes et appliquer des solutions aux problèmes courants du réseau sans intervention humaine, ce qui en fait un outil puissant pour maintenir et améliorer les opérations réseau. Dans un réseau Wi-Fi, par exemple, cela peut signifier maintenir une couverture complète du réseau en cas de défaillance d'un point d'accès (PA) en augmentant automatiquement la puissance du signal RF des autres points d'accès (PA) afin de reconfigurer le réseau et de couvrir tout point mort potentiel.
Actuellement, l'accent est mis sur l'IA et l'apprentissage automatique, qui prennent en charge les domaines plus administratifs et banals de la gestion de réseau. Fondamentalement, il s'agit d'apprendre au réseau à automatiser les tâches d'administration de base et d'alerter les administrateurs réseau si des problèmes plus complexes nécessitant une intervention humaine sont identifiés.

Hiérarchisation automatique du trafic réseau critique

L'IA intégrée aux switches intelligents est désormais également utilisée pour garantir la fourniture au bon moment du trafic critique lorsqu'il circule sur le réseau. En analysant les paquets Ethernet, ces switches intelligents peuvent automatiquement affecter différents niveaux de service à différents types de trafic réseau et accorder la priorité aux paquets IP vidéo et VoIP sans compromettre la transmission d'autres données réseau. Cela évite d'avoir du matériel séparé et dédié spécifiquement pour la voix et vidéo IP.
En utilisant une technique connue sous le nom d'Auto Surveillance VLAN (ASV), les paquets vidéo IP en temps réel sont prioritaires afin de garantir la qualité de la vidéo en temps réel pour la surveillance et le contrôle. De même, la technologie Auto Voice VLAN garantit la qualité et la sécurité du trafic VoIP et offre des appels VoIP ininterrompus pour les utilisateurs du réseau.

L'IA et les réseaux gérés dans le Cloud

Les architectures de réseau sont de plus en plus souvent gérées dans une structure centralisée avec des fonctions de gestion traitées dans un plan de contrôle distinct du plan de données, comme dans les réseaux gérés dans le Cloud et le Software Defined Networking (SDN). L'IA et l'apprentissage machine sont essentiels pour récolter tous les avantages de ces architectures réseau gérées de manière centralisée.
Des capacités d'analyse et d'apprentissage automatisées sont nécessaires pour profiter des avantages d'une flexibilité accrue du réseau et d'une facilité de gestion offerte par ces infrastructures. La combinaison de l'IA et de la gestion de réseau logicielle centralisée nous pousse à nous tourner vers une mise en réseau entièrement automatisée.

Résumé

Actuellement, l'automatisation est principalement utilisée dans les configurations réseau sans intervention avec des périphériques réseau intelligents qui se connectent automatiquement à un serveur lors de la mise sous tension pour une configuration et des mises à jour automatiques. Ce déploiement « plug and play » basé sur l'IA élimine la nécessité d'une configuration manuelle étendue, ce qui permet de gagner du temps et de déployer les appareils sur des sites distants sans administrateurs réseau sur site.
Les outils d'IA sont également de plus en plus utilisés pour améliorer la surveillance, la gestion et l'analyse du réseau, en raison de leur talent à prédire les problèmes de réseau et à automatiser les correctifs avant que les problèmes ne surviennent. Avec leur capacité à interroger d'énormes quantités de données provenant de sources multiples, l'IA et l'apprentissage machine fournissent une meilleure visibilité sur les performances quotidiennes du réseau et les niveaux d'utilisation actuels. Cette visibilité accrue sur ce qui se passe sur le réseau permet de détecter les changements et les défis à un stade précoce et de prendre des mesures proactives pour garantir l'optimisation continue des performances. L'identification des modèles de trafic et la compréhension des tendances du réseau permettent d'effectuer des prévisions plus précises, améliorant considérablement la précision de la planification de la capacité du réseau.
L'IA et l'apprentissage machine jouent également un rôle de plus en plus important dans l'amélioration de la sécurité du réseau, en fournissant une meilleure visibilité sur le comportement sur le réseau afin que les menaces puissent être automatiquement identifiées et traitées rapidement.
Bien sûr, comme il s'agit d'une approche automatisée, l'IA et l'apprentissage machine fonctionnent en permanence, permettant une gestion et un contrôle continus et constants du réseau sans interruption, ce qui participe à l'amélioration du service.
Alors que la complexité des réseaux ne cesse de croître, qu'ils adoptent des architectures de gestion centralisée et prennent en charge un plus large éventail d'appareils et de systèmes d'exploitation connectés, la gestion de réseau basée sur l'IA est essentielle pour rationaliser, dépanner et améliorer le fonctionnement du réseau. Le moment où l'IA et l'apprentissage machine deviendront essentiels au bon fonctionnement de tout réseau approche à grands pas.

XDR versus EDR : quelles différences et comment choisir la meilleure solution pour votre entreprise ?

La sécurité informatique est un enjeu crucial pour les entreprises, qui doivent faire face à des cybermenaces de plus en plus sophistiquées et ciblées. Parmi les solutions de sécurité disponibles, l'Extended Detection and Response (XDR) et l'Endpoint Detection and Response (EDR) sont deux approches qui suscitent un intérêt grandissant.

Si ces deux technologies partagent des similitudes, elles présentent également des différences notables. Ce contenu vous propose de comprendre les spécificités de l'XDR et de l'EDR, ainsi que leurs avantages respectifs, afin de vous aider à choisir la solution la plus adaptée à vos besoins.

Qu'est-ce que l'XDR ?

L'Extended Detection and Response est une approche de sécurité informatique qui vise à détecter, analyser et neutraliser les menaces en combinant les données provenant de différentes sources au sein d'une entreprise.

L'XDR intègre et corrèle les informations issues des solutions de sécurité existantes, telles que les antivirus, les pare-feux, les systèmes de détection d'intrusion (IDS) et les solutions de protection des terminaux, afin de fournir une visibilité globale et une analyse approfondie des événements de sécurité.

Qu’est-ce que l’EDR ?

L’Endpoint Detection and Response est une solution de sécurité qui se concentre sur la protection des terminaux (ordinateurs, serveurs, appareils mobiles, etc.) en détectant et en répondant aux menaces avancées et ciblées.

L’EDR collecte et analyse les données relatives aux activités sur les terminaux, telles que les processus, les connexions réseau et les modifications de fichiers, afin d’identifier les comportements suspects et de réagir rapidement en cas d’attaque.

Les différences entre XDR et EDR

Si l’XDR et l’EDR partagent l’objectif commun de détecter et de neutraliser les menaces, ils présentent des différences notables en termes de portée et d’approche :

Portée : l’XDR couvre l’ensemble de l’environnement informatique d’une entreprise, en intégrant les données provenant de différentes sources (terminaux, réseau, cloud, etc.), tandis que l’EDR se concentre exclusivement sur la protection des terminaux. **Approche** : l’XDR adopte une approche globale et intégrée de la sécurité, en corrélant les données issues de différentes solutions de sécurité, alors que l’EDR se focalise sur l’analyse des activités au niveau des terminaux.

Les avantages respectifs de l’XDR et de l’EDR

L’XDR et l’EDR présentent chacun des avantages spécifiques en fonction des besoins et des contraintes des entreprises :

XDR

- Visibilité accrue sur l’ensemble du **réseau**
- Détection améliorée des menaces grâce à l’analyse croisée des données
- Réponse plus rapide et plus efficace aux incidents
- Simplification de la gestion de la sécurité

EDR

- Protection renforcée des **terminaux**
- Détection des menaces avancées et ciblées
- Analyse approfondie des activités au niveau des terminaux
- Réponse rapide aux incidents locaux

Comment choisir entre XDR et EDR ?

Pour choisir la solution la plus adaptée à vos besoins, il est important de prendre en compte plusieurs facteurs :

La taille et la complexité de votre environnement informatique : si votre entreprise dispose d'une infrastructure informatique étendue et hétérogène, l'XDR peut être plus adapté pour assurer une visibilité et une protection globale. En revanche, si votre principale préoccupation est la protection des terminaux, l'EDR peut être une solution plus appropriée.

Les menaces auxquelles vous êtes confronté : en fonction des menaces spécifiques qui pèsent sur votre entreprise, l'XDR ou l'EDR peut être plus efficace pour détecter et neutraliser les attaques.

Votre budget et vos ressources : le choix entre XDR et EDR peut également dépendre de vos contraintes budgétaires et de vos ressources humaines et techniques.

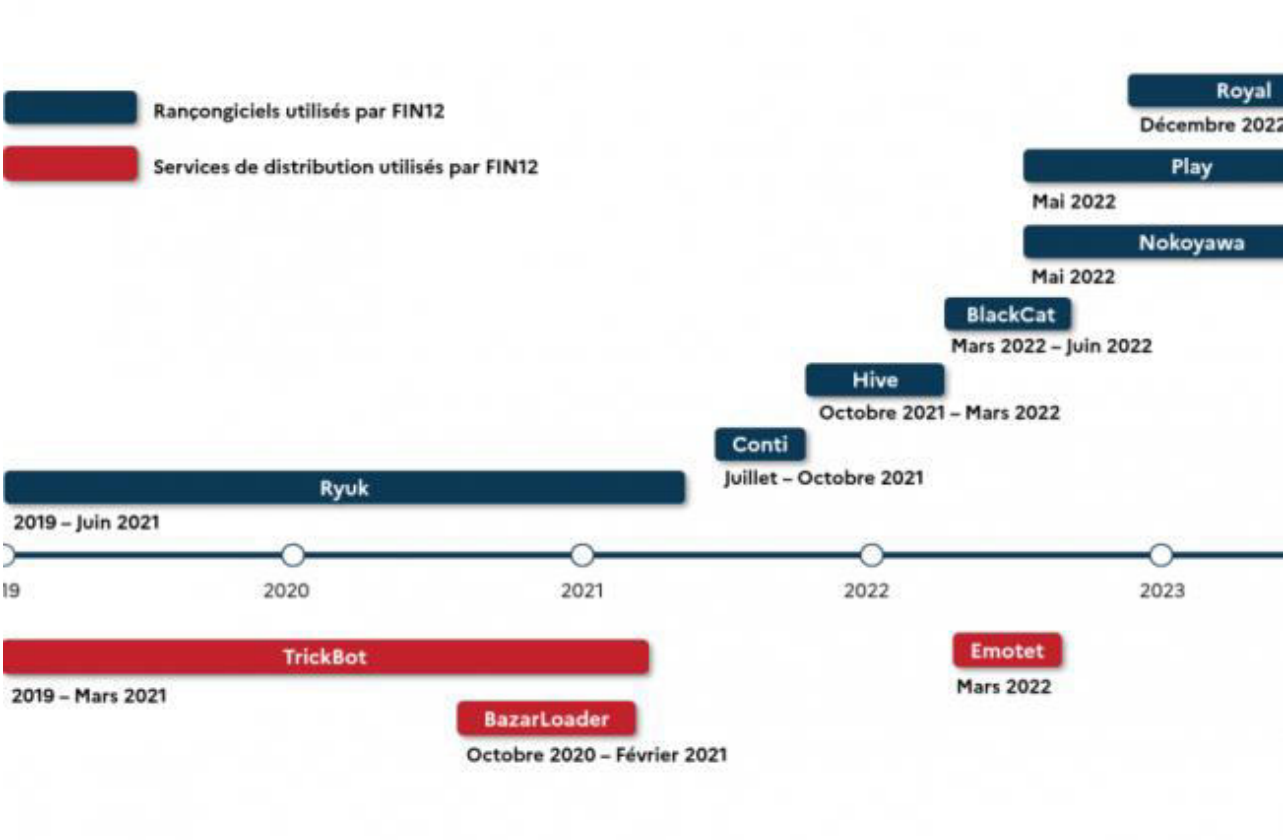
Opter pour une sécurité optimale

Face aux cybermenaces grandissantes, les entreprises doivent renforcer leur sécurité informatique en adoptant des solutions adaptées à leurs besoins et à leur environnement.

L'XDR et l'EDR sont deux approches complémentaires qui présentent des avantages spécifiques en termes de visibilité, de détection et de réponse aux menaces. Pour choisir la solution la plus adaptée à votre entreprise, il est essentiel d'évaluer vos besoins, vos contraintes et les menaces auxquelles vous êtes confronté.

Le CERT-FR décortique la cyberattaque contre le CHRU de Brest

Six mois après la cyberattaque ayant frappé le CHRU de Brest, le CERT-FR est revenu sur le déroulé de l'incident et le mode opératoire d'un groupe de cybercriminels liés à FIN12.



Synthèse chronologique des activités connues du MOA FIN12 (PISTACHE TEMPEST) depuis 2019.
(crédit : CERT-FR / ANSSI)

Le CHRU de Brest se souviendra longtemps du jeudi 9 mars. À 20h33, l'établissement de santé a en effet détecté une cyberattaque ayant impacté ses serveurs. Grâce à la réactivité des équipes en place prévenues par l'Anssi, le CHRU a pu éviter le pire, cette attaque ayant pu être bloquée avant d'aller à son terme. Six mois après cet incident, le CERT-FR - en accord avec le RSSI du CHRU de Brest Jean-Sylvain Chavanne - publie un rapport qui revient sur le déroulé de cet incident et le mode opératoire du cybergang FIN12 qui en est à l'origine. « Ce rapport de CTI démontre notamment l'importance d'avoir une double authentification et une politique de patch des vulnérabilités, surtout les plus classiques, pour éviter les élévations de privilèges », a fait savoir Jean-Sylvain Chavanne. « L'apport de l'EDR aura été important également pour établir ces analyses. Depuis, nous avons mis en œuvre plusieurs

mesures améliorer la cybersécurité de nos établissements, grâce aux analyses de l'ANSSI et de l'ensemble des experts qui ont travaillé avec nous ».

« L'accès initial au système d'information a été effectué depuis un service de bureau à distance exposé et accessible sur Internet. Les opérateurs du MOA ont utilisé des authentifiants valides d'un professionnel de santé pour se connecter. Il est probable que les authentifiants du compte soient issus de la compromission par un information stealer du poste utilisateur, dans le cadre d'une campagne de distribution opportuniste », explique le CERT-FR. « Deux acteurs pourraient donc être impliqués dans l'incident, un fournisseur d'accès initial et l'attaquant chargé de la latéralisation et du déploiement du rançongiciel. Les attaquants ont utilisé leur accès de bureau à distance afin d'exécuter deux portes dérobées : SystemBC et Cobalt Strike. SystemBC a été exécuté dans un intervalle de 20 minutes après Cobalt Strike depuis le même répertoire. Ces deux codes ont donc très probablement été déployés par le même acteur ».

Des affiliés à différentes attaques par ransomware aux manettes

Après avoir tenté d'exploiter les vulnérabilités LocalPotato, trois codes ont été employés pour essayer également de récupérer des données d'authentification : AccountRestore (bruteforce de comptes Active Directory), SharpRoast (attaque par kerberoasting) et Mimikatz (pour de l'extraction d'authentifiants en environnement Windows). Le CERT-FR indique que l'Anssi a permis d'établir les liens entre cet incident et une trentaine de victimes d'attaques par ransomware.

« Ces incidents présentent des caractéristiques techniques dont la plupart sont similaires à celles observées au CHU : accès initial au système d'information par l'utilisation d'authentifiants valides ; utilisation conjointe des codes malveillants SystemBC et Cobalt Strike ; le stockage de charges dans le répertoire C:\Users\Public\Music\ ; nom du chiffreur similaire : xxx.exe, bien que celui-ci n'ait pas pu être observé dans l'incident du CHU. Les attaquants ont employé deux portes dérobées : SystemBC et Cobalt Strike », peut-on lire dans le rapport. « D'après les analyses de l'Anssi, les attaquants responsables de l'incident du CHU de Brest pourraient donc être affiliés à différentes attaques par rançongiciel. Ils auraient utilisé les rançongiciels Ryuk, puis Conti, avant de distribuer Hive, Nokoyawa, Play et Royal. Une analyse historique de leur mode opératoire les lie à FIN12 ainsi qu'à d'autres opérations de rançongiciels ayant succédé à la fin des opérations du groupe Conti (Wizard Spider) ».

Fibre, satellite, 4G fixe : quelle technologie d'accès à Internet choisir ?

Fibre optique, câble, 4G fixe, Internet satellite, réseau radio : il existe de nombreuses technologies d'accès à Internet. Mais comment choisir la plus adaptée aux besoins de son entreprise ? On vous donne les clés.

Plusieurs technologies permettent d'avoir accès à Internet dans son entreprise. On peut citer l'ADSL, bien sûr, mais aussi la fibre optique, le câble, la 4G fixe, l'Internet par satellite ou encore la boucle locale radio. Chaque technologie a ses propres caractéristiques et atouts : on vous explique comment choisir la plus adaptée à vos besoins.

La fibre optique

La fibre optique se présente sous la forme d'un fil de verre conducteur de lumière aussi fin qu'un cheveu (250 micromètres). Elle est utilisée pour transmettre sur de longues distances de très grandes quantités d'informations en un temps record.

Cette technologie, qui devrait être déployée partout sur le territoire d'ici 2030, plonge la France dans l'ère du Très Haut Débit. Avec la fibre optique, on parle en effet de débits minimums de 100 Mbit/s. La plupart des opérateurs promettent même des débits de 200 Mb/s, voire 1 Gb/s, quasiment sans aucune déperdition.

Sauvegarde, envoi et téléchargement de fichiers volumineux, temps de latence très bas, télétravail, visioconférence fluide, utilisation d'un VPN... La fibre optique s'impose actuellement comme la solution d'accès à Internet la plus performante sur le marché et offre plusieurs avantages pour les professionnels :

- une bande passante élevée, ce qui signifie que vous pouvez profiter de la même qualité de connexion même si vous êtes plusieurs à utiliser Internet en même temps ;
- des vitesses de transfert beaucoup plus rapides, environ 100 fois plus élevées que l'ADSL ;
- la possibilité de profiter de débits symétriques, c'est-à-dire de débits identiques en réception (download) qu'en émission (upload) ;

- la fibre est insensible aux perturbations électromagnétiques, ce qui signifie qu'elle est rarement confrontée à une baisse de signal.

Pour bénéficier de la fibre optique, il faut cependant que le logement ou le bâtiment en question soit éligible. Pour connaître son éligibilité, il suffit de se renseigner auprès des différents fournisseurs d'accès à Internet ou directement auprès du syndic de copropriété ou du propriétaire du bien. Si tel est le cas, l'utilisateur peut choisir librement parmi les opérateurs qui proposent des services Très Haut Débit.

Bon à savoir

On entend souvent parler de différentes technologies pour qualifier la fibre optique : FttH, FttO, FttE, etc. Ces différents sigles se réfèrent en réalité à plusieurs techniques de raccordement. Celles-ci présentent des performances différentes et répondent à des besoins bien précis.
L'ADSL, qui couvre environ 99 % du territoire, est toujours disponible. La fibre optique est toutefois en passe de devenir l'infrastructure Internet fixe de référence. Conformément au Plan France Très Haut Débit, elle devrait définitivement remplacer le réseau en cuivre d'ici 2030.

Le câble

Ce que l'on désigne comme étant le "câble" n'est autre que la technologie FTTLA (Fiber to the Last Amplifier), que l'on peut traduire par "fibre jusqu'au dernier amplificateur". Lors de son déploiement dans les années 1980, le câble ne servait qu'à transmettre la télévision en analogique.

Avec l'apparition d'Internet, il fallut adapter ce réseau afin de transporter plus d'informations et, ainsi, développer une réelle offre haut débit. Deux technologies ont alors été mélangées : la fibre optique et le câble.

La FTTLA est donc une technologie hybride. Concrètement, la fibre optique ne vient pas jusqu'au domicile des clients et s'arrête dans un boîtier qui se trouve le plus souvent dans la rue ou dans la cave de l'immeuble. Le raccordement final se fait ensuite au moyen d'un câble coaxial.

Cette technologie se présente comme une excellente alternative à l'ADSL. La connexion est très rapide (jusqu'à 1 Gb/s en téléchargement) et l'installation s'avère simple, rapide et peu coûteuse en comparaison avec la fibre FttH (Fiber To The Home). Toutefois, bien qu'elle propose des débits descendants qui avoisinent ceux de la fibre optique, la FTTLA affiche des débits montants inférieurs, souvent sous les 100 Mb/s.

Cela signifie qu'elle est moins puissante pour certains usages sur Internet comme mettre une vidéo en ligne, partager des fichiers volumineux, ou encore effectuer une visioconférence. Par ailleurs, une connexion câblée est davantage sujette aux interférences. Il se peut donc que vous rencontriez par moments quelques problèmes de stabilité (page qui tourne dans le vide, son saccadé, vidéo qui se fige, etc.)

La 4G fixe

La 4G fixe permet de fournir un service d'accès fixe à Internet via le réseau mobile 4G dans les zones qui ne bénéficient pas d'un réseau haut débit performant. Cette technologie s'avère

être une excellente alternative pour tous ceux qui disposent d'une connexion ADSL trop faible ou inexistante, mais suppose une bonne couverture 4G sur la zone concernée.

En pratique, il s'agit de transformer le réseau mobile 4G en réseau Wi-Fi à l'aide d'un boîtier (routeur) installé sur une prise secteur à l'intérieur du logement ou du bâtiment. Selon votre opérateur, vous disposez soit d'un accès illimité à Internet, soit d'un nombre de gigaoctets mensuels limités.

La 4G fixe permet uniquement la consultation d'Internet. Contrairement à une solution fibre optique, ADSL ou satellite, il n'est pas possible de disposer d'une offre triple play intégrant téléphone, TV et Internet. Les débits, eux, se situent entre 100 Mb/s et 320 Mb/s en download pour une moyenne de 50 Mb/s en upload. Ils varient en fonction de la distance du domicile à l'antenne, ainsi que du nombre d'utilisateurs simultanés sur l'antenne.

Important

Pour être éligible à un abonnement box 4G/5G, il faut remplir plusieurs critères : avoir un débit ADSL inférieur à 10 Mb/s, ne pas être raccordable à la fibre optique et vivre dans une zone de couverture 4G d'un opérateur.

Internet par satellite

La technologie satellitaire se présente comme une alternative pour tous ceux qui vivent en zone blanche (sans connexion ADSL) ou en zone grise (débit ADSL faible). Elle concerne aussi les usagers disposant d'une couverture réseau mobile insuffisante pour souscrire à une box 4G.

Pour être mis en place, l'Internet par satellite a besoin de trois éléments :

1. une station terrestre d'émission/réception raccordée aux réseaux terrestres de télécommunication ;
2. un satellite géostationnaire en orbite (à une distance de 36 000 km de la Terre) ;
3. une parabole installée chez l'abonné et dirigée vers le satellite.

À chaque navigation sur Internet, la parabole envoie les données directement au satellite géostationnaire, qui les renvoie à son tour à la station terrestre appartenant à l'opérateur auquel vous avez souscrit. Une fois la page reçue, la station d'émission/réception renvoie les données au satellite en orbite, qui se charge de la renvoyer jusqu'à votre parabole. En somme : à chaque requête effectuée, ce sont environ 140 000 km qui sont parcourus !

Cette technologie permet de bénéficier d'une connexion Internet convenable en zone blanche mais présente une latence assez élevée, un partage de la bande passante du satellite et suppose que vous disposiez d'une parabole (achat ou location).

Le saviez-vous ?

Une zone blanche c'est un territoire dépourvu de couverture par un certain type de réseau : mobile, internet, TV etc. Alors que la zone grise correspond à un secteur où la couverture est limitée.

Le réseau radio

Plusieurs opérateurs proposent des offres haut ou très haut débit dites RttH (Radio to the Home). Ces offres, comme le WiMAX, ne nécessitent pas de raccordement filaire : le signal arrive par voie hertzienne depuis une antenne émettrice vers une antenne réceptrice généralement située en haut du toit. Celle-ci se charge ensuite de distribuer le signal dans la maison en Wi-Fi.

Le débit WiMAX est d'environ 75 Mb/s mais peut être diminué par d'éventuels obstacles (montagnes, immeubles dans les zones urbaines, etc.) ou lorsque de nombreuses personnes sont connectées simultanément sur la même station de base. Cette technologie permet toutefois de déployer le réseau haut débit dans des lieux isolés où la fibre ne peut pas être installée, ou lorsque le réseau ADSL a un débit trop bas pour une utilisation correcte.

Quelle technologie d'accès à Internet choisir ?

Plusieurs facteurs sont à considérer au moment de choisir sa technologie d'accès à Internet.

Les usages

Avant d’arrêter votre choix, il est indispensable de faire un point sur vos besoins en termes de vitesse de chargement et de téléchargement. En effet, si vous avez une utilisation sommaire d’Internet (consultation de mails, simples recherches sur Internet, etc.), vous n’aurez pas besoin des mêmes débits que si vous diffusez des vidéos sur Internet ou effectuez des visioconférences, par exemple.

L'éligibilité

Que vous habitiez dans une zone rurale ou dans une grande ville, vos options d'accès à Internet ne seront pas les mêmes. À l'heure actuelle, la technologie d'accès à Internet la plus performante est sans aucun doute la fibre optique. Cependant, tout le monde n'y est pas éligible ! Il convient donc de tester votre éligibilité au préalable.

Le coût

Les tarifs constituent évidemment un critère de choix important. En général, il faut compter entre 15 et 55 € par mois pour un accès à Internet en fonction des débits, des performances de la box et des services associés. Afin d'effectuer le meilleur choix possible, il est vivement recommandé de comparer les grilles tarifaires des différents fournisseurs d'accès à Internet. Cela vous permettra de sélectionner la meilleure offre en fonction des services que vous recherchez et du budget dont vous disposez.

PRI vs PCI : Pour la stabilité informatique

Dans le vaste univers de la gestion informatique, deux piliers essentiels se dressent pour assurer la stabilité et la continuité des opérations : le PRI (Plan de Reprise Informatique) et le PCI (Plan de Continuité Informatique).

Sur les deux dernières années, **76% des entreprises déclarent la perte de données informatiques**. Dans cet article, découvrez, comment le PRI et le PCI peut protéger votre entreprise fasse à ces situations.

Le Plan de Reprise Informatique (PRI) : Un Bouclier Contre l'Inattendu

Le PRI fonctionne comme un manuel d'urgence. Imaginez-le comme une trousse de premiers soins pour les systèmes informatiques. En cas de sinistre, il offre une feuille de route détaillée pour la **restauration rapide** des opérations. Son objectif principal est de **minimiser les temps d'arrêt** et de **restaurer les services** aussi rapidement et efficacement que possible.

Objectifs Clés du PRI :

1. Définir les objectifs de reprise : Identifier clairement ce qui doit être rétabli et en quel délai.

2. Inventaire des ressources critiques : Cartographier les actifs essentiels pour les opérations.

3. Stratégies de sauvegarde et de restauration : Mettre en place des procédures de sauvegarde régulières et des plans de restauration.

4. Responsabilités en cas d'incident : Clarifier les rôles et responsabilités de l'équipe de gestion de crise.

Le Plan de Continuité Informatique (PCI) : Anticiper pour éviter

À la différence du PRI, le PCI se concentre sur la **prévention**. Il s'agit d'un ensemble de stratégies préventives visant à garantir que les systèmes restent opérationnels même en cas de perturbation. Le PCI va au-delà de la simple récupération après

sinistre en cherchant à **minimiser les risques potentiels** et à **maintenir la continuité des activités.**

Composantes Essentielles du PCI :

1. Analyse des risques : Identifier et évaluer les risques potentiels pour la continuité informatique.

2. Redondance des systèmes : Établir des systèmes redondants pour éviter les points uniques de défaillance.

3. Plans de sauvegarde et de relève : Développer des plans détaillés pour sauvegarder et restaurer les systèmes critiques.

4. Formation du personnel : S'assurer que le personnel est formé pour répondre efficacement aux incidents.

Pourquoi ces plans sont-ils cruciaux ?

1. Minimisation des risques : Les deux plans travaillent en tandem pour identifier et minimiser les risques potentiels.

2. Réaction rapide : Le PRI assure une réaction rapide en cas d'incident, tandis que le PCI prévient ces incidents autant que possible.

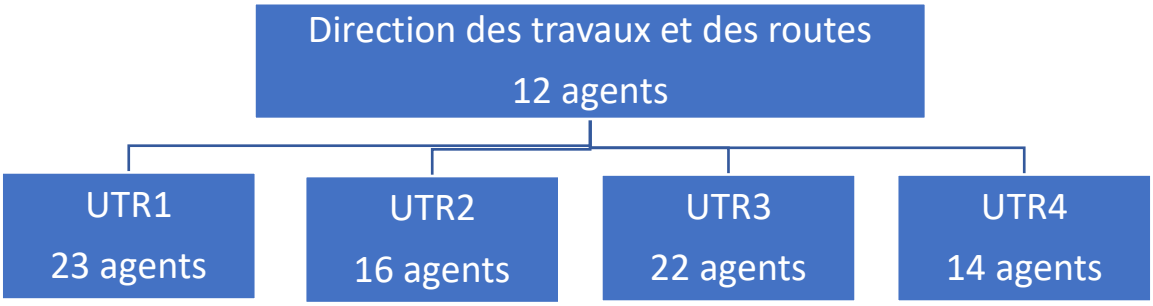
3. Continuité transparente : Ensemble, ils garantissent une continuité transparente des activités, même face aux défis les plus inattendus.

Le PRI et le PCI ne sont pas seulement des acronymes complexes, ce sont des **piliers cruciaux** de notre stabilité informatique. En les comprenant et en les mettant en œuvre, nous nous assurons que notre univers numérique reste robuste et résilient face à l'inattendu.

INGEDEP - Direction des travaux et des routes

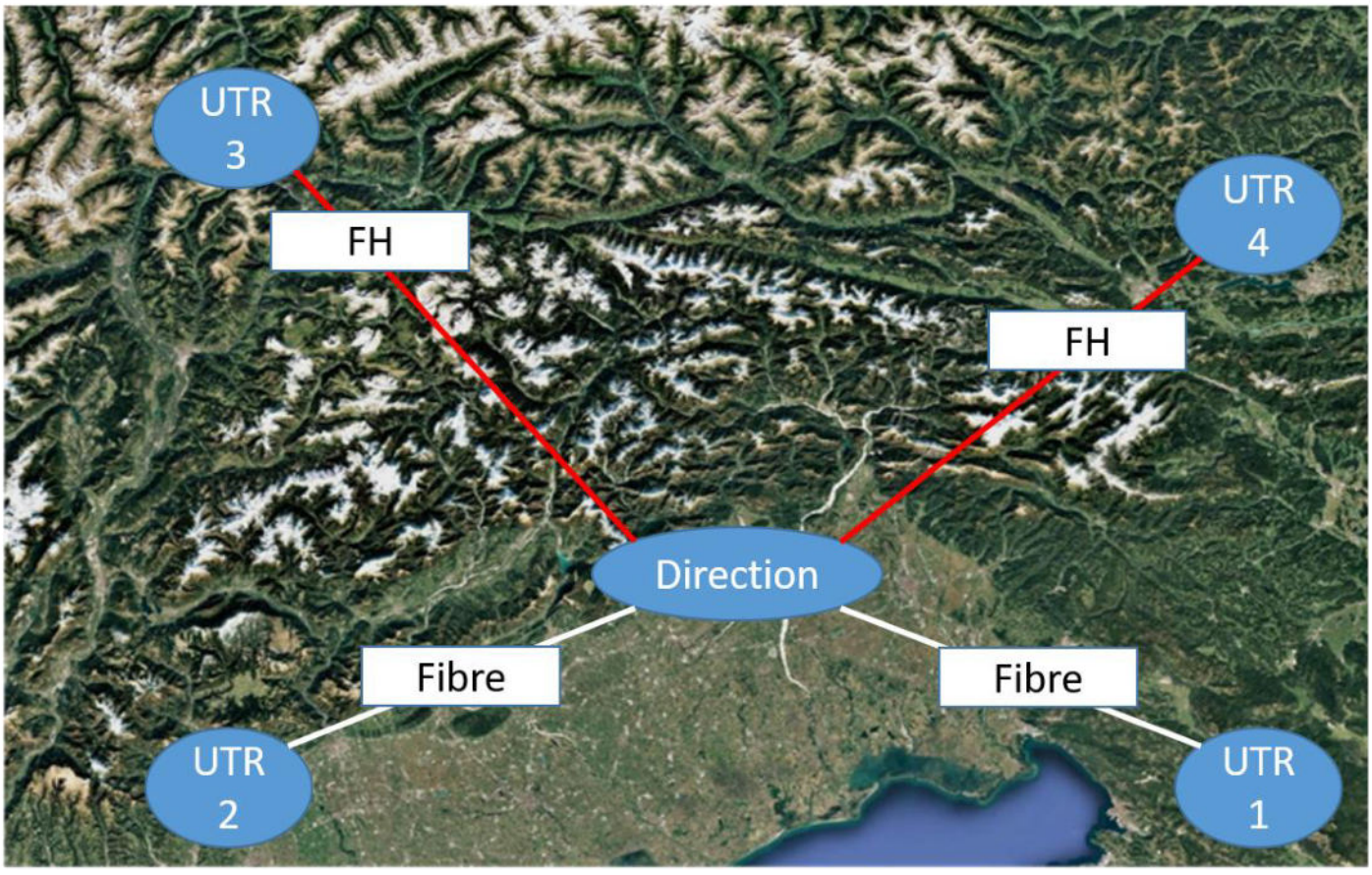
La Direction des travaux et des routes du département d'INGEDEP est en charge des travaux et de l'entretien des 4 000 kilomètres de routes départementales. Elle est répartie géographiquement sur le site central du conseil départemental et sur 4 unités territoriales routières.

Organigramme de la DTR :



Liaisons informatiques :

Historiquement les 4 unités territoriales sont reliées par faisceaux hertziens (FH). Le FH se prête bien au relief complexe. Les 2 UTR de plaine (UTR1 et UTR2) sont reliées depuis peu à la direction par fibre optique permettant le très haut débit.



Lien	Type	
Direction vers UTR1	**fibre**	Nouveau lien
Direction vers UTR2	**fibre**	Nouveau lien
Direction vers UTR1	**FH**	Ancien lien (encore fonctionnel)
Direction vers UTR2	**FH**	Ancien lien (encore fonctionnel)
Direction vers UTR3	**FH**	Lien historique fonctionnel
Direction vers UTR4	**FH**	Lien historique fonctionnel