# Sécuriser une machine

Mots de passe

Ecran anti-espion

Firewall

Anti-virus

Pas de connection au wifi public

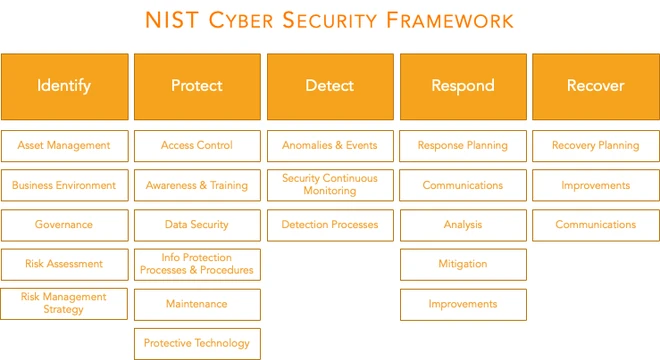
Clef usb avec certificat pour déverrouiller un pc

Changer le ssid

Configurer le routeur

# NIST





[CVE](https://www.redhat.com/fr/topics/security/what-is-cve)

# Cryptologie

Chiffrement symétrique et asymétrique

<https://www.ibm.com/fr-fr/topics/encryption#:~:text=Il%20existe%20deux%20principaux%20types,deux%20cl%C3%A9s%20cryptographiques%20asym%C3%A9triques%20s%C3%A9par%C3%A9es>.

<https://culturemath.ens.fr/thematiques/lycee/cryptographie-asymetrique-et-courbes-elliptiques>

<https://fr.wikipedia.org/wiki/M%C3%A9thode_de_Gutmann>

# Réseau

## Routeur

Un routeur est un appareil permettant de créer un réseau Wi-Fi. Il doit pour cela être relié à un modem. Il envoie les informations provenant d'Internet à vos appareils personnels (ordinateurs, téléphones et tablettes).

## IPS

Un système de prévention des intrusions (IPS) est une forme de sécurité de réseau qui sert à détecter et prévenir les menaces identifiées. Les systèmes de prévention des intrusions surveillent en permanence votre réseau, recherchent les éventuels actes de malveillance et capturent des informations à leur sujet.

## IDS

Les IDS (Intrusion Detection Systems) : analysent et surveillent le trafic réseau pour détecter des signes indiquant que des hackers utilisent une cybermenace connue afin de s'infiltrer dans votre réseau ou y voler des données.

## VPN

Un réseau privé virtuel (VPN) est un moyen de connecter des ordinateurs à distance en utilisant une connexion Internet sécurisée. Il permet de créer un lien direct entre deux ordinateurs, comme s'ils étaient connectés par une connexion réseau physique, tout en protégeant les données échangées grâce à des protocoles de sécurité. Les utilisateurs peuvent utiliser un VPN pour accéder à des réseaux d'entreprise à distance, naviguer sur Internet de manière anonyme ou contourner les restrictions géographiques.

# Firewall

Un pare-feu est un dispositif qui contrôle les paquets réseau entrant et sortant du réseau principalement en les laissant passer ou en les bloquant. Par conséquent, les journaux de pare-feu peuvent révéler beaucoup d'informations sur les paquets qui ont passé ou ont essayé de passer à travers le pare-feu.

## Pare-feu de réseau :

Un pare-feu réseau est placé entre deux réseaux pour contrôler le trafic réseau qui circule entre eux. ( NAT )

## Pare-feu d'application :

Un pare-feu d'application est conçu pour protéger les applications et les serveurs en filtrant le trafic entrant et sortant.

## Pare-feu de paquets :

Un pare-feu de paquets examine chaque paquet de données qui traverse le réseau et autorise ou bloque le trafic en fonction de règles définies.

## Pare-feu de circuit :

Un pare-feu de circuit surveille l'état des connexions réseau et ne permet que les connexions autorisées à traverser.

## Pare-feu de proxy :

Un pare-feu de proxy sert d'intermédiaire entre les clients et les serveurs, filtrant le trafic en fonction de règles de sécurité définies.

## Pare-feu sans fil :

Un pare-feu sans fil est utilisé pour protéger les réseaux sans fil contre les attaques.

## Pare-feu de machine virtuelle :

Un pare-feu de machine virtuelle est utilisé pour protéger les environnements de virtualisation contre les menaces.

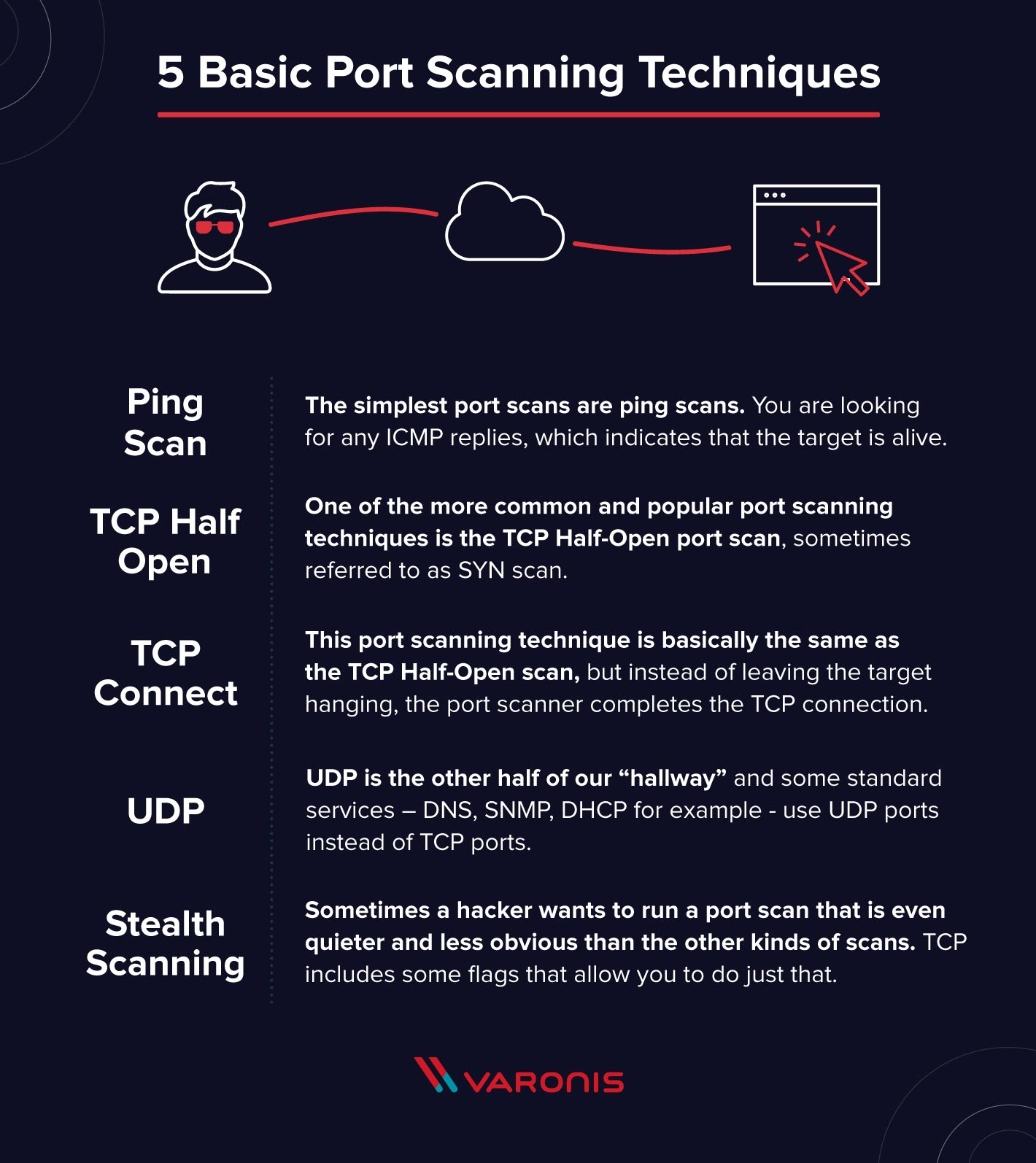
## Pare-feu personnel :

Un pare-feu personnel est un logiciel installé sur un ordinateur pour contrôler le trafic entrant et sortant.

## Pare-feu cloud :

Un pare-feu cloud est un service de sécurité qui offre une protection pour les applications et les données stockées dans le cloud.

## Balayage de port



# Advanced malware protection

Faille 0 day ( FAIRE PREVENTION )

# Travail

## A faire

–Première version–

* bonne pratique de sécurité du NIST
* bonne pratique
* approche comportementale de la cybersécurité
* sécurité basée sur le comportement
* NETflow
* Test d’intrusion

## Bonne pratique de sécurité du NIST

Le NIST (National Institute of Standards and Technology) est une agence gouvernementale américaine qui est responsable de la promotion des bonnes pratiques en matière de sécurité informatique. Le NIST a développé une série de bonnes pratiques en matière de sécurité connue sous le nom de "Framework for Improving Critical Infrastructure Cybersecurity" (Cadre pour améliorer la cybersécurité des infrastructures critiques), également appelé "Framework NIST".

Le Framework NIST est basé sur cinq fonctions principales de cybersécurité: identifier, protéger, détecter, répondre et récupérer. Voici un aperçu de chaque fonction:

* Identifier: Cette fonction implique de comprendre les systèmes, les données et les personnes qui font partie de l'infrastructure de l'entreprise. Il est important d'identifier les risques potentiels pour la sécurité de l'entreprise et de mettre en place des mesures de sécurité appropriées pour les prévenir.
* Protéger: Cette fonction implique de mettre en place des mesures de sécurité pour protéger les systèmes et les données de l'entreprise. Cela peut inclure des mesures telles que la gestion des accès, la gestion des mots de passe, la sécurité physique des locaux, etc.
* Détecter: Cette fonction implique de surveiller les systèmes de l'entreprise pour détecter les incidents de sécurité. Cela peut inclure la surveillance des journaux d'activité, l'analyse des anomalies de trafic, etc.
* Répondre: Cette fonction implique de réagir rapidement et efficacement en cas d'incident de sécurité. Cela peut inclure la mise en place d'un plan de réponse aux incidents, la formation du personnel, etc.
* Récupérer: Cette fonction implique de restaurer les systèmes de l'entreprise après un incident de sécurité. Cela peut inclure la restauration des sauvegardes, la réparation des systèmes endommagés, etc.

Le Framework NIST est une norme reconnue dans l'industrie pour la sécurité informatique et peut aider les entreprises à améliorer leur sécurité en suivant des bonnes pratiques éprouvées. Cependant, il est important de noter que chaque entreprise est différente et qu'une approche personnalisée de la sécurité est souvent nécessaire pour répondre aux besoins spécifiques de l'entreprise.

## Bonne pratique

La cybersécurité est devenue un enjeu majeur pour les entreprises et les particuliers à mesure que nous devenons de plus en plus dépendants de la technologie. Voici quelques bonnes pratiques en cybersécurité pour aider à protéger vos données et vos systèmes :

* Utiliser des mots de passe forts : Les mots de passe doivent être longs, complexes et uniques pour chaque compte. Évitez d'utiliser des informations personnelles ou faciles à deviner.
* Mettre à jour les logiciels régulièrement : Les mises à jour de sécurité sont souvent publiées pour corriger les vulnérabilités connues dans les logiciels. Assurez-vous de mettre à jour régulièrement tous les logiciels installés sur vos appareils.
* Utiliser une solution antivirus : Les programmes antivirus peuvent aider à détecter et à éliminer les logiciels malveillants qui pourraient compromettre votre système.
* Éviter les sites web non sécurisés : Les sites web non sécurisés peuvent être des cibles pour les pirates informatiques pour accéder à vos informations personnelles. Vérifiez toujours que le site web est sécurisé avant d'y entrer des informations sensibles.
* Sensibiliser les employés : La sécurité informatique est une responsabilité de tous les employés d'une entreprise. Assurez-vous que vos employés sont conscients des menaces potentielles et formez-les à des pratiques de sécurité de base.
* Utiliser la double authentification : La double authentification ajoute une couche de sécurité supplémentaire en exigeant une deuxième forme d'authentification, telle qu'un code envoyé par SMS, pour accéder à un compte.
* Sauvegarder régulièrement les données : Les sauvegardes régulières peuvent aider à réduire les pertes de données en cas d'incident de sécurité.
* Utiliser des réseaux privés virtuels (VPN) : Les VPN peuvent aider à sécuriser les connexions Internet en cryptant les données qui transitent entre les ordinateurs.
* Éviter les réseaux Wi-Fi publics : Les réseaux Wi-Fi publics sont souvent peu sécurisés et peuvent permettre aux pirates informatiques d'intercepter les données envoyées sur le réseau.
* Utiliser une analyse de vulnérabilité : Les analyses de vulnérabilité peuvent aider à identifier les vulnérabilités potentielles dans les systèmes et à les corriger avant qu'elles ne soient exploitées par des pirates informatiques.

## Approche comportementale de la cybersécurité

L'approche comportementale de la cybersécurité est une méthode qui met l'accent sur le comportement des utilisateurs en matière de sécurité informatique. L'approche consiste à identifier les comportements à risque des utilisateurs et à mettre en place des mesures pour encourager des comportements plus sécurisés.

Cette approche reconnaît que la plupart des incidents de sécurité informatique sont causés par des erreurs humaines, telles que l'utilisation de mots de passe faibles ou la réponse à des e-mails de phishing. En conséquence, l'approche comportementale vise à modifier ces comportements à risque en encourageant des pratiques de sécurité informatique plus saines.

Voici quelques éléments clés de l'approche comportementale de la cybersécurité :

* Sensibilisation à la sécurité : Les utilisateurs doivent être informés des menaces de sécurité informatique et des conséquences potentielles de ne pas suivre les meilleures pratiques de sécurité.
* Formation à la sécurité : Les utilisateurs doivent être formés aux pratiques de sécurité de base, telles que la création de mots de passe forts et la reconnaissance des e-mails de phishing.
* Encouragement du comportement sécurisé : Les utilisateurs doivent être encouragés à adopter des pratiques de sécurité informatique saines, telles que la mise à jour régulière des logiciels et la sauvegarde régulière des données.
* Communication régulière : La communication régulière entre les utilisateurs et les professionnels de la sécurité informatique peut aider à identifier les problèmes de sécurité potentiels et à trouver des solutions pour y remédier.
* Conception centrée sur l'utilisateur : Les produits de sécurité informatique doivent être conçus en gardant à l'esprit l'utilisateur final, de manière à encourager des comportements de sécurité plus sains.
* L'approche comportementale de la cybersécurité est une méthode complémentaire à l'approche traditionnelle axée sur la technologie, qui met l'accent sur la mise en place de barrières de sécurité pour empêcher les attaques. En combinant ces deux approches, les entreprises peuvent renforcer leur posture de sécurité et réduire les risques de compromission de données.