



Communauté Cisco

La Cybersécurité

Concepts sur les intrusions

KHERFALLAH Boubaker

Cisco Instructor Trainer - Expert CCNA

3 Mars 2020

Nouveautés et prochains événements



Événement : Demandez-moi N'importe Quoi



R&S : Configuration d'un routeur IPv6 et meilleures pratiques

Foire aux Questions jusqu'au
vendredi 6 Mars

avec Harold Ritter

Demandez-moi N'importe Quoi | R&S

Configuration d'un routeur IPv6
et meilleures pratiques

Animé par : Harold Ritter

Du 24 Février au 6 Mars

Connectez-vous sur
Community.Cisco.com en français

Posez une question

Suivez le lien

<http://bit.ly/DNQ2-fev20>

Événement : Community Live mardi 7 avril



Data Center – Introduction à VxLAN (BGP-EVPN)

Webcast en ligne
Inscrivez-vous

avec Michael Di Bartolomeo
Événement public

Community Live | Data Center

Introduction à VxLAN
(BGP-EVPN)

Animé par : Michael Di Bartolomeo et Maxime Dessambre

Avril 7
09:30 hrs Montréal
15:30 hrs Paris

S'inscrire ici

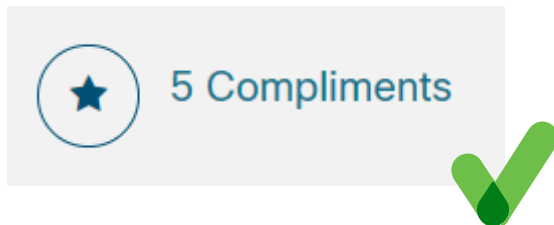
Suivez le lien

<http://bit.ly/WEB-FRapr20>

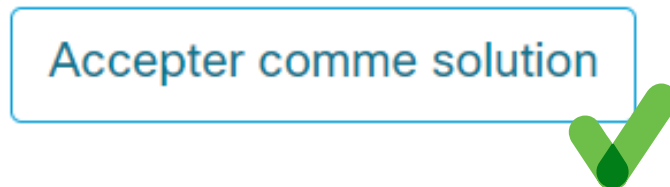
Évaluez le contenu de la Communauté Cisco

Discussions, Documents, Blogs et Vidéos

Aidez-nous à identifier les contenus de qualité et à reconnaître l'effort des membres de la Communauté Cisco en français.



Identifiez les experts



Repérez les solutions

Apprenez à mieux utiliser la plateforme et exploiter toutes ses ressources.

Suivez le lien

<http://bit.ly/PilotVideoFR>

Reconnaissance aux Top Contributeurs

Devenez un Top Contributeur pour le mois de février !

La reconnaissance aux **Top Contributeurs** est conçue pour reconnaître et remercier ceux qui ont collaboré avec nous en fournissant des contenus techniques de qualité ainsi que les participants plus actifs qui ont permis à notre communauté de devenir un des Top sites pour les passionnés de la technologie de Cisco.

Suivez le lien

<http://bit.ly/FRCC-SpotlightAwards>



The Community Spotlight Awards recognizes members whose significant contributions designate leadership and commitment to their peers within their respective communities, including Cisco Community, Cisco Learning Network (CLN), and Cisco Developers Network (CDN). Spotlight awards are designed to recognize and thank individuals who help make our communities the premier online destination for Cisco enthusiasts. [FAQs](#)

2019 2018 2017 2016 2015 2014 2013 2012

janvier février mars avril mai **juin** juillet août septembre octobre novembre décembre

French Member's Choice, June 2019



Luis Cordova
2019 June

Les experts de la Communauté Cisco

Boubaker Kherfallah

ASC Academy Specialist
chez une Académie Cisco
(Algérie)

CCNA R&S, Security et Cybersecurity



Présentateur

Merci d'être avec
nous aujourd'hui !

Téléchargez la présentation sur

<http://bit.ly/WEBsld-mar20>



Participez avec nous et posez des questions

La présentation comprendra aussi quelques questions du public. Nous vous invitons cordialement à participer activement aux questions que vous pourrez poser pendant cette séance sur le panneau à droite « Q&R ».

Résolvez vos doutes et partagez votre opinion



Au programme



Introduction à la
Cybersécurité



Menaces, vulnérabilités et
attaques



Comprendre les mécanismes
de défense



Principe de la nouvelle génération
des Pare-feu et prévention des
intrusions NGIPS.



Démonstration pratique

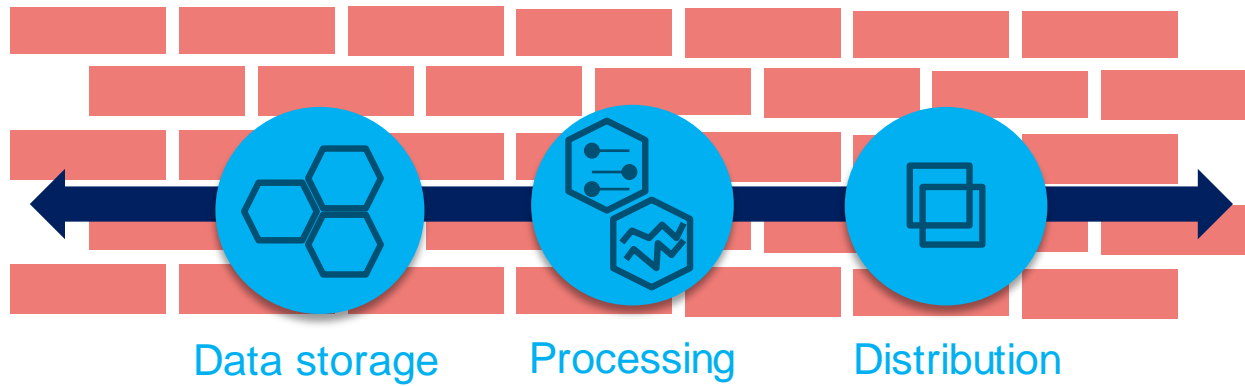
Introduction

Données : stockées, en traitement ou en transit



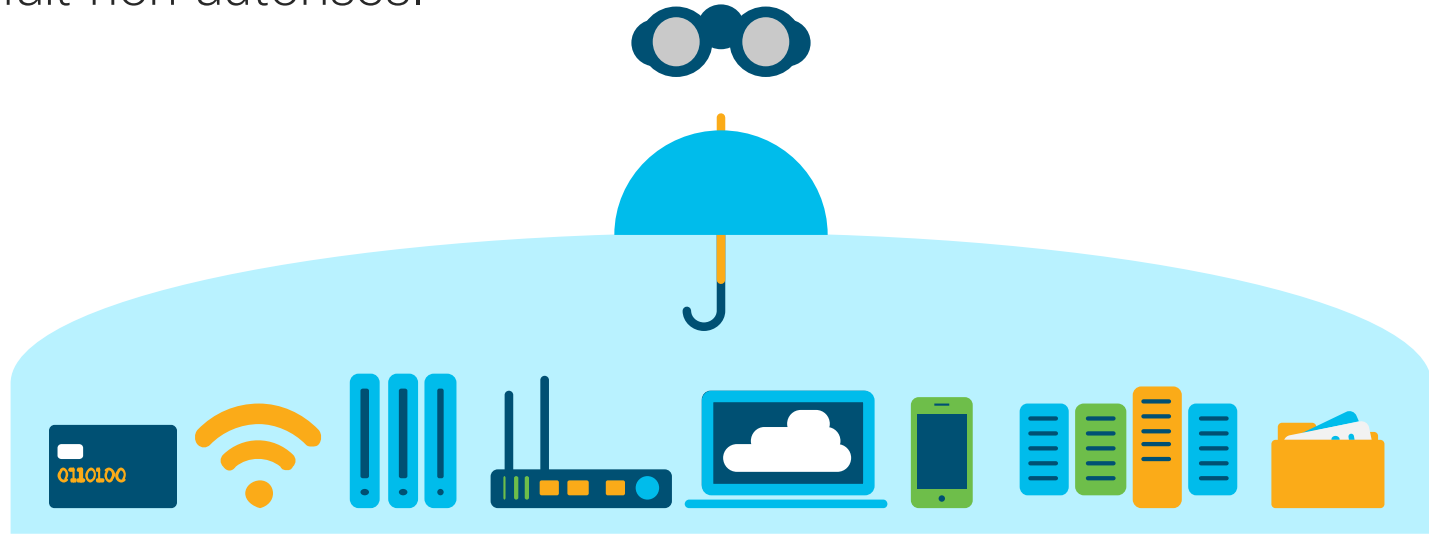
Qu'est-ce que la cybersécurité ?

- La **cybersécurité** est l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberspace et susceptibles de compromettre la **disponibilité**, l'**intégrité** ou la **confidentialité** des données **stockées**, **traitées** ou **transmises**.

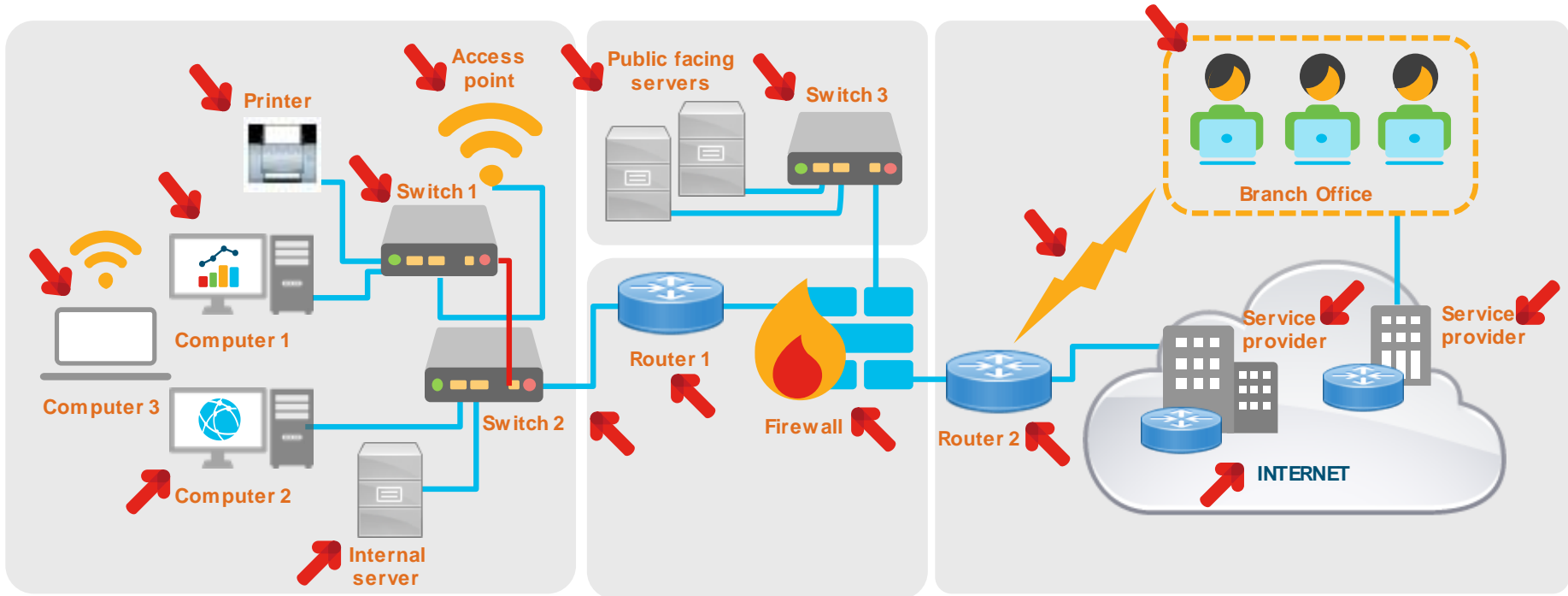


Autrement dit

- La **cybersécurité** consiste en l'effort continu pour protéger les systèmes mis en réseau et les données contre l'utilisation ou le méfait non autorisés.



Surface d'attaque



Connaître les risques !

Vulnérabilité, Menaces et Attaques

- I. Les vulnérabilités d'un système
- II. Malwares et codes malveillants
- III. Les attaques



I. Les vulnérabilités d'un système

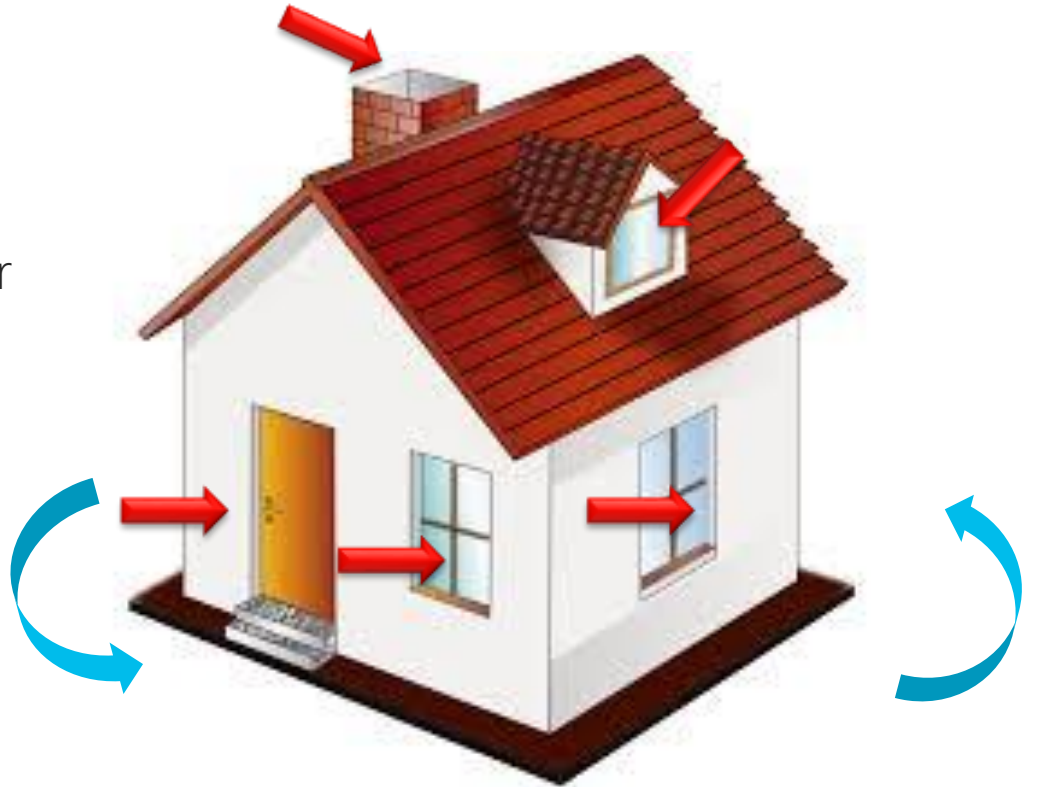
1. Vulnérabilité

- Une vulnérabilité est une faiblesse d'un système ou de sa conception, qui peut être exploitée par une menace (un point faible, maillon faible, etc.)



Exemple de maison

Chercher une vulnérabilité
=
Chercher un point d'entrée pour
accéder à une cible



Types de vulnérabilité de Sécurité

1. Failles Technologiques
2. Failles de Configuration
3. Failles de la Politique de Sécurité

Network security weaknesses:

TCP/IP protocol weakness

- Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP) and Internet Control Message Protocol (ICMP) are inherently insecure.
- Simple Network Management Protocol (SNMP) and Simple Mail Transfer Protocol (SMTP) are related to the inherently insecure structure upon which TCP was designed.

Operating system weakness

- Each operating system has security problems that must be addressed.
- UNIX, Linux, Mac OS, Mac OS X, Windows Server 2012, Windows 7, Windows 8
- They are documented in the Computer Emergency Response Team (CERT) archives at <http://www.cert.org>.

Network equipment weakness

Various types of network equipment, such as routers, firewalls, and switches have security weaknesses that must be recognized and protected against. Their weaknesses include password protection, lack of authentication, routing protocols, and firewall holes.

2. Menace

- Une menace est un danger potentiel pour les biens. Les menaces sont souvent réalisées par le biais d'une attaque ou d'un exploit qui tire parti d'une vulnérabilité existante.

3. Risque

- Le risque est la possibilité qu'un accès non autorisé compromette, détruise ou endommage un bien. C'est aussi la probabilité qu'une menace particulière utilisant une attaque spécifique exploite une vulnérabilité particulière d'un actif.



II. Malwares et codes malveillants

- Virus
- Vers
- Cheval de Troie
- Bombes logiques
- Portes dérobées et rootkits
- Ransomware
- ...

Un logiciel conçu pour perturber le bon fonctionnement d'un ordinateur ou obtenir l'accès à des systèmes informatiques à l'insu ou sans l'autorisation de l'utilisateur.





III. Les attaques

En plus d'**attaques de codes malveillants** , il est possible pour les réseaux de **tomber en proie** à **diverses attaques réseau** :

1. **Attaques** de reconnaissance
2. **Attaques** d'accès
3. **Déni** de service

1. Attaques de reconnaissance



Requêtes Internet



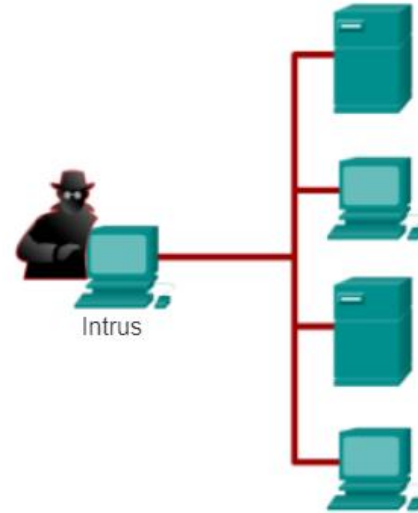
Balayages ping



Balayages de ports



Analyseurs de paquets

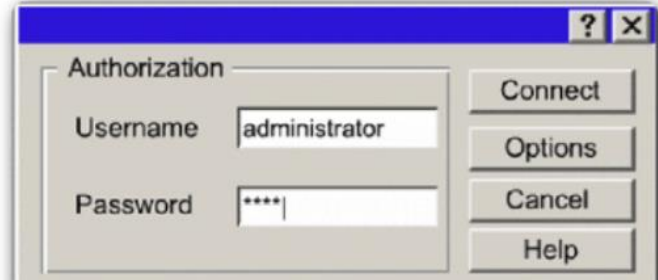


2. Attaques d'accès

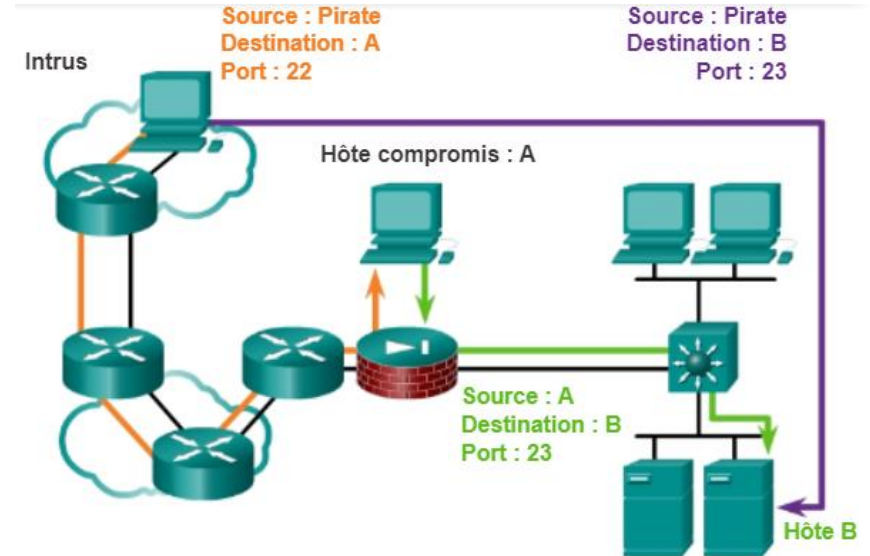
a. Attaque de mot de passe

Les pirates peuvent lancer différents types d'attaques de mots de passe :

- Attaques en force
- Chevaux de Troie
- Analyseurs de paquets

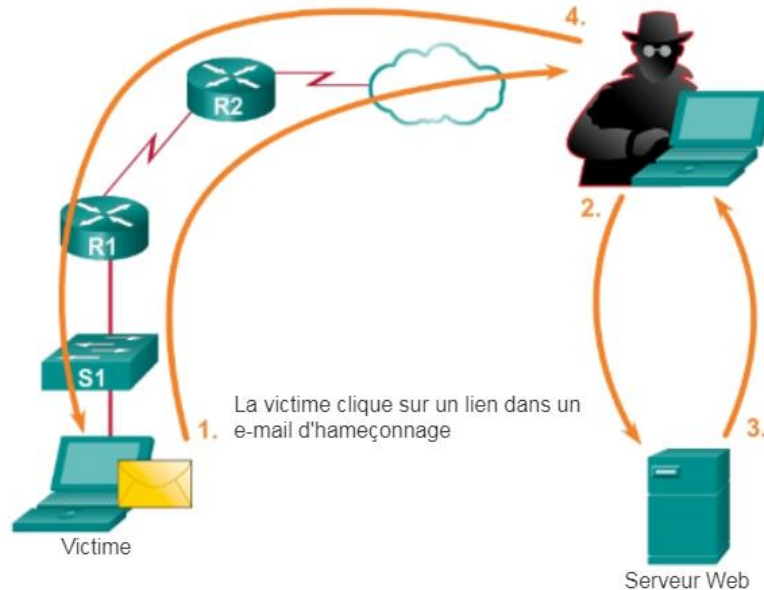


b. Redirection des ports



c. Man-in-the-Middle

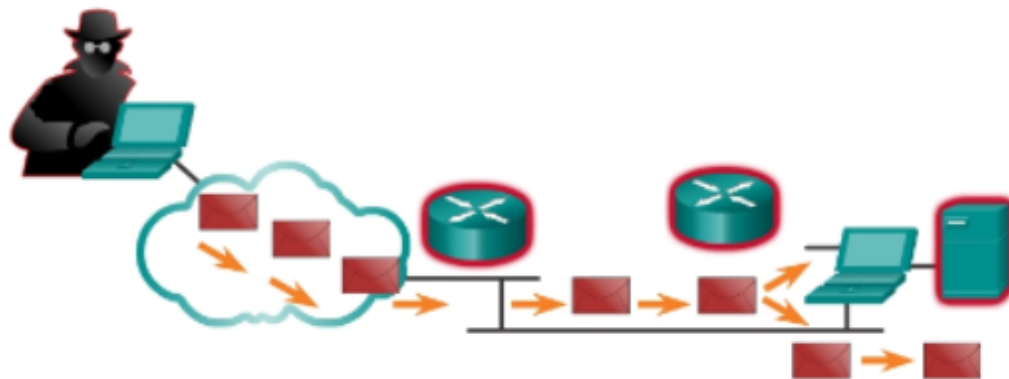
- Le hacker intercepte les communications entre plusieurs ordinateurs pour voler les informations en transit sur le réseau.



3. Déni de service (Dos)

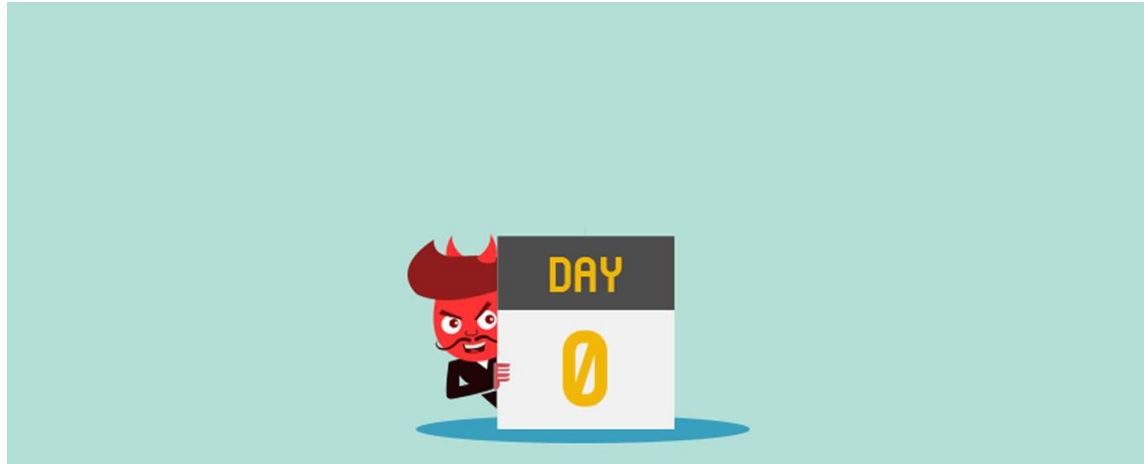
- Une attaque par déni de service (DoS) se traduit par une interruption des services de réseau pour les utilisateurs, les appareils ou les applications.

Surcharge des ressources	Données mal formées
Espace disque, bande passante, tampons	Paquets surdimensionnés (ping fatal)
Inondation de paquets ping (Smurf)	Chevauchement de paquets (Winuke)
Inondations de paquets (bombes UDP, attaques Fraggle)	Données non traitées (Teardrop)



Attaques de type « zero-day »

- Ces attaques ont la particularité de tirer parti de telles vulnérabilités **non encore identifiées**, ainsi que de variantes de malware pour exploiter une faille de sécurité particulière.



Comprendre les
mécanismes de défense

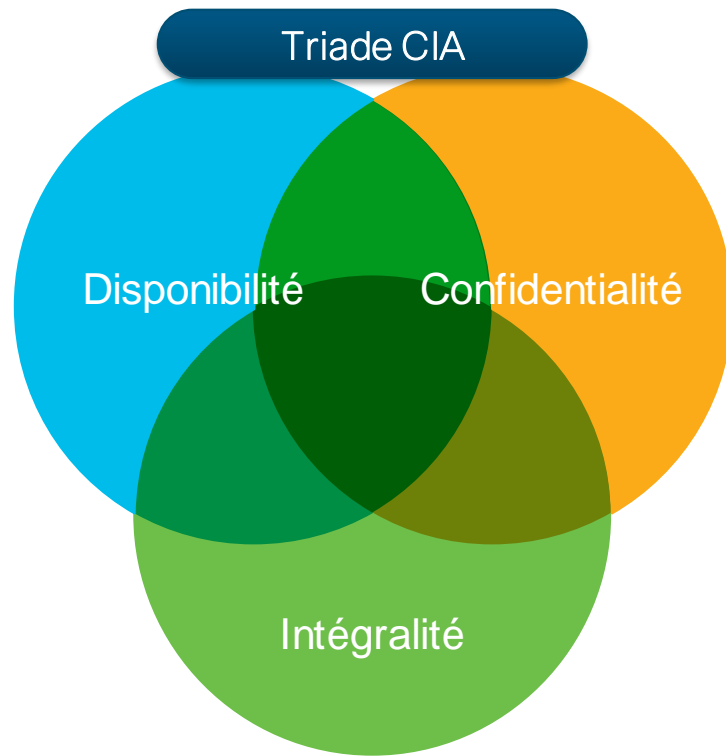
Confidentialité
Intégrité
Disponibilité

- Cryptage
- AAA
- Hachage
- Signature numérique
- Certificat
- Cinq neuf



Confidentialité, intégrité et disponibilité

- Chaque outil déployé et chaque procédure mise en place répond toujours à au moins un de ces éléments :





La Confidentialité

- Consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées ;
 - ➔ Rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction.

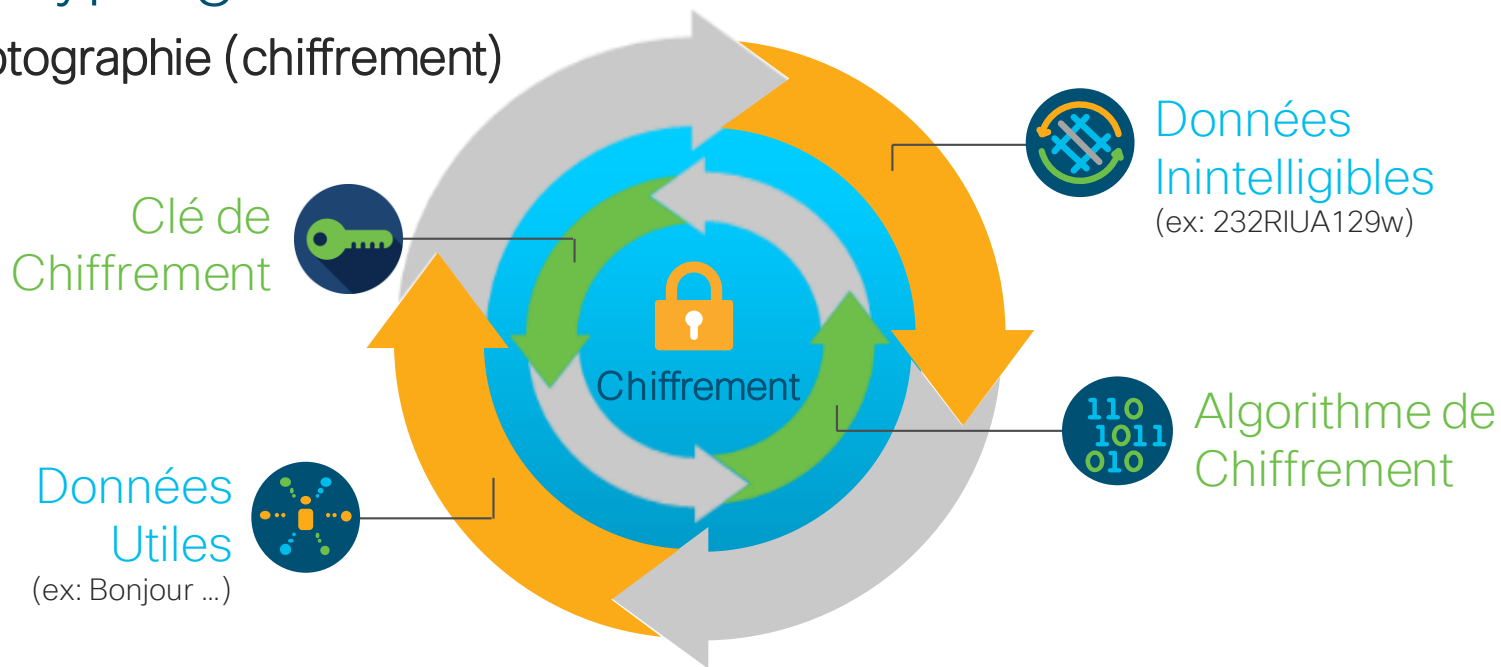




Technologies liées à la confidentialité

I. Cryptage

Cryptographie (chiffrement)



Cryptographie symétrique :

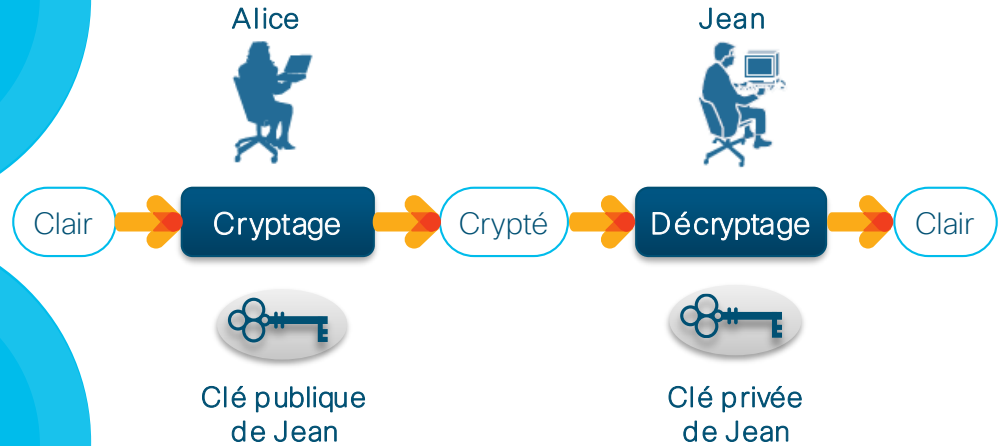


Une seule clé pour chiffrer
et déchiffrer un message

?

L'échange des clés

Cryptographie asymétrique :



II. AAA

- Authentification, Autorisation et comptabilisation noté (AAA ou “triple A”)
- **Authentification** (*Authentication*): Les utilisateurs et les administrateurs doivent **prouver leur identité**. Elle peut être établie en utilisant :
 - Combinaisons de **nom d'utilisateur** et **mot de passe**,
 - Enjeu (challenge) de **questions/réponse**,
 - Cartes à jeton
 - Autres méthodes.
- **Autorisation** (*Authorization*): les **ressources** auxquelles l'utilisateur peut accéder et les **opérations** que l'utilisateur est autorisé à effectuer.
- **Comptabilisation** (*Accounting*) : enregistre quelles actions on a effectué lors de l'accès au réseau ou système, la **durée d'accès** à la ressource, et **toute modification apportée**.

Certificat Numérique

☛ Pourquoi utiliser les certificats ?

- Pour prouver **l'identité** de nos services (Web, Courriel...).
- Pour offrir **une confidentialité des données** envoyées par l'intermédiaire du chiffrement.



L'intégrité

- Les données font l'objet de nombreuses opérations telles que **la capture, le stockage, la récupération, la mise à jour et le transfert.**
 - ➔ Cependant, elles ne doivent, à aucun moment, être **altérées** par des entités non autorisées.





Technologies liées l'intégrité

1. Algorithmes de hachage

Exemple d'algorithmes: MD5 - SHA

Données de longueur arbitraire



Fonction de hachage

Hash de longueur fixe

e883ba0a24d011

Authentification par hachage (HMAC)

Données de longueur arbitraire

Message en texte clair



Clé secrète

Fonction de hachage

Hash de longueur fixe

e883ba0a24d011

1. Algorithmes de hachage

Exemple

Emetteur : Alice



Clé secrète

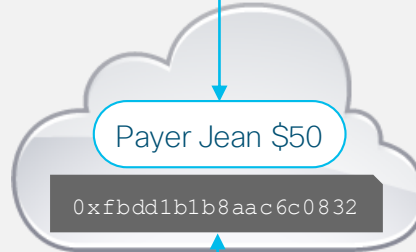
Données

Payer Jean \$50

Algorithme de hachage

0xfbdd1b1b8aac6c0832

HMAC
Empreinte digitale
authentifiée



Clé secrète



Récepteur : Jean

Payer Jean \$50

Algorithme de hachage

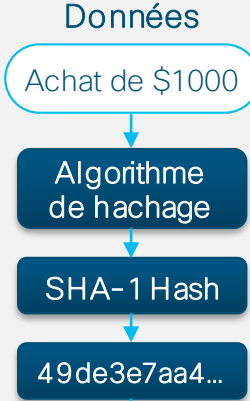
0xfbdd1b1b8aac6c0832

HMAC
Vérfié

2. Signature numérique

Exemple

Emetteur : Jean

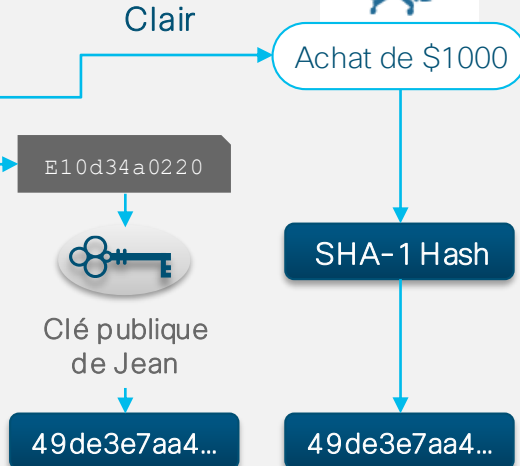


Clé privée de Jean



E10d34a0220...
Signature RSA

Récepteur : Alice





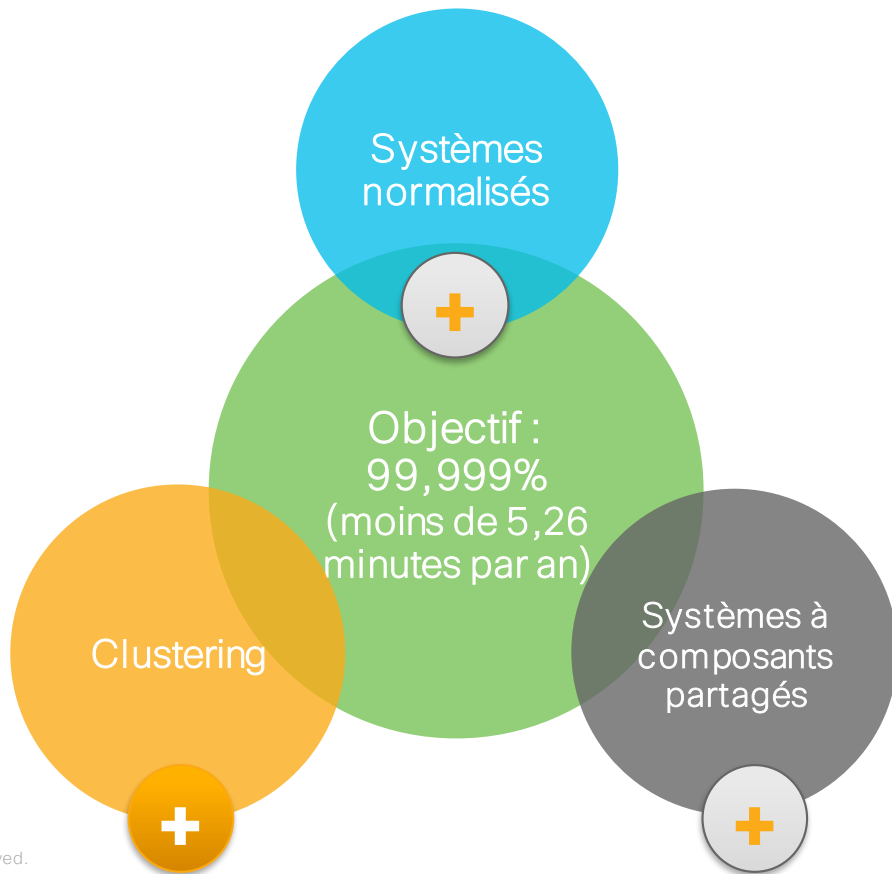
La disponibilité

- Principe selon lequel il est nécessaire d'assurer une disponibilité en continu des systèmes et services d'information.
- Certains dysfonctionnements et attaques peuvent empêcher l'accès aux systèmes et services d'information.
- ➔ Le terme de **haute disponibilité** décrit des systèmes conçus pour éviter les interruptions.



Les « cinq neuf »

99,999%



NGIPS

- Fonctionnement IPS
- IPS vs Firewall
- NGIPS
- Principes



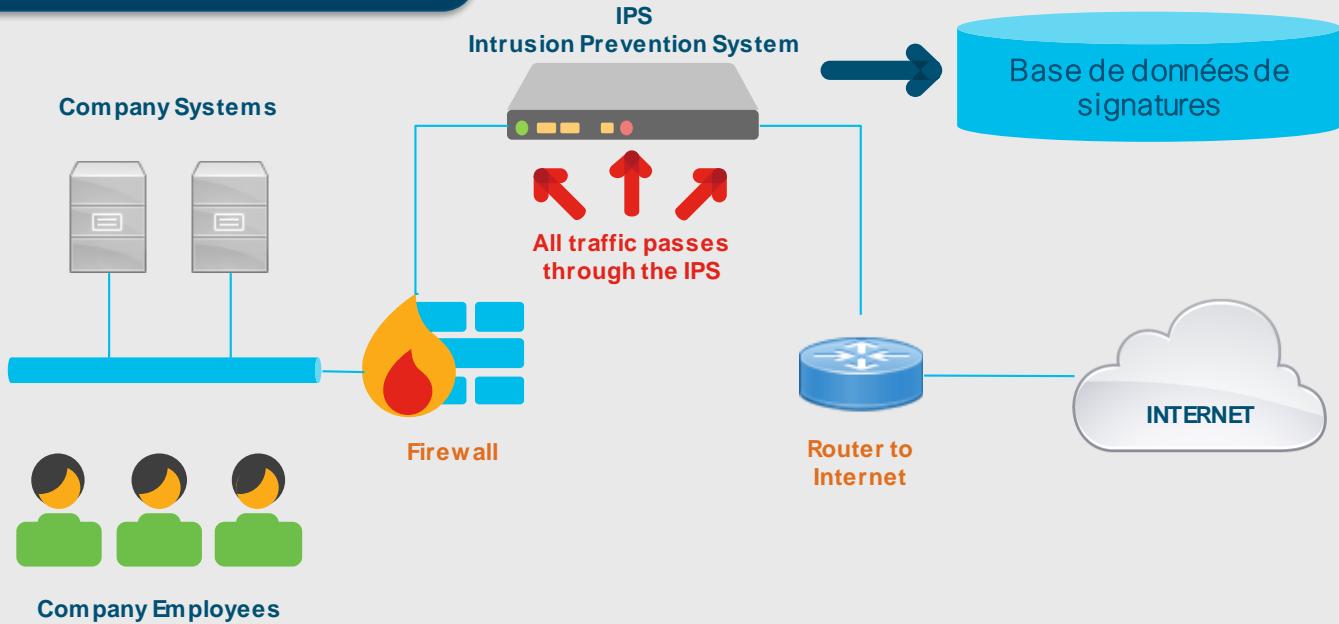
Fonctionnement IPS

- Analyse le trafic réseau en s'appuyant sur une **base de données de signatures** d'attaque et dès qu'il reconnaît une signature, **il en déduit que c'est une attaque.**
- Dans ce cas il peut prendre des mesures pour bloquer l'attaque avant qu'elle n'ait commencé en bloquant le flux malveillant.



IPS

IPS est en coupure sur le réseau



NIPS

NETWORK INTRUSION PREVENTION SYSTEM



Analyse le trafic réseau



S'appuie sur une base de données de signatures d'attaque



Bloque les flux malveillants

HIPS

HOST INTRUSION PREVENTION SYSTEM



Analyse les machines hôtes



Surveille différents éléments des machines hôtes



Bloque les activités suspectes



- Les **NIPS** (network intrusion prévention system) sont des IPS permettant de surveiller le trafic réseau.
- Les **HIPS** (host intrusion prévention system) sont des IPS permettant de suivre l'état de sécurité des machines hôtes. Le HIPS réalise cela à travers **la surveillance des différentes éléments de la machine** : les processus, les drivers, les .dll etc.

- les IPS ne sont pas fiables à 100 % mais le principal risque c'est de bloquer du trafic légitime en cas d'erreur d'analyse
- Le deuxième inconvénient de l'IPS est que, il est vulnérable et attaquable puisqu'il est en coupure sur le réseau.





IPS vs Firewall

- Le rôle d'un **IPS réseau** est de détecter des attaques sur un réseau à partir **d'une base de données de signatures d'attaque** (comme un anti virus) et de les bloquer si nécessaire.
- Le rôle d'un **firewall** est différent puisque son but est de faire du **filtrage d'accès en définissant les communications autorisés ou interdites.**

Faire face aux attaques sophistiquées

- Les pirates informatiques d'aujourd'hui sont parfaitement équipés et possèdent l'expertise et la ténacité pour compromettre la sécurité de n'importe quelle entreprise et à tout moment. Les méthodes de protection traditionnelles ne sont plus efficaces contre les attaques de plus en plus sophistiquées dont les vecteurs d'attaque se multiplient.

Pourquoi une nouvelle approche est nécessaire ?

➤ Impossible de protéger ce qu'on ne voit pas !

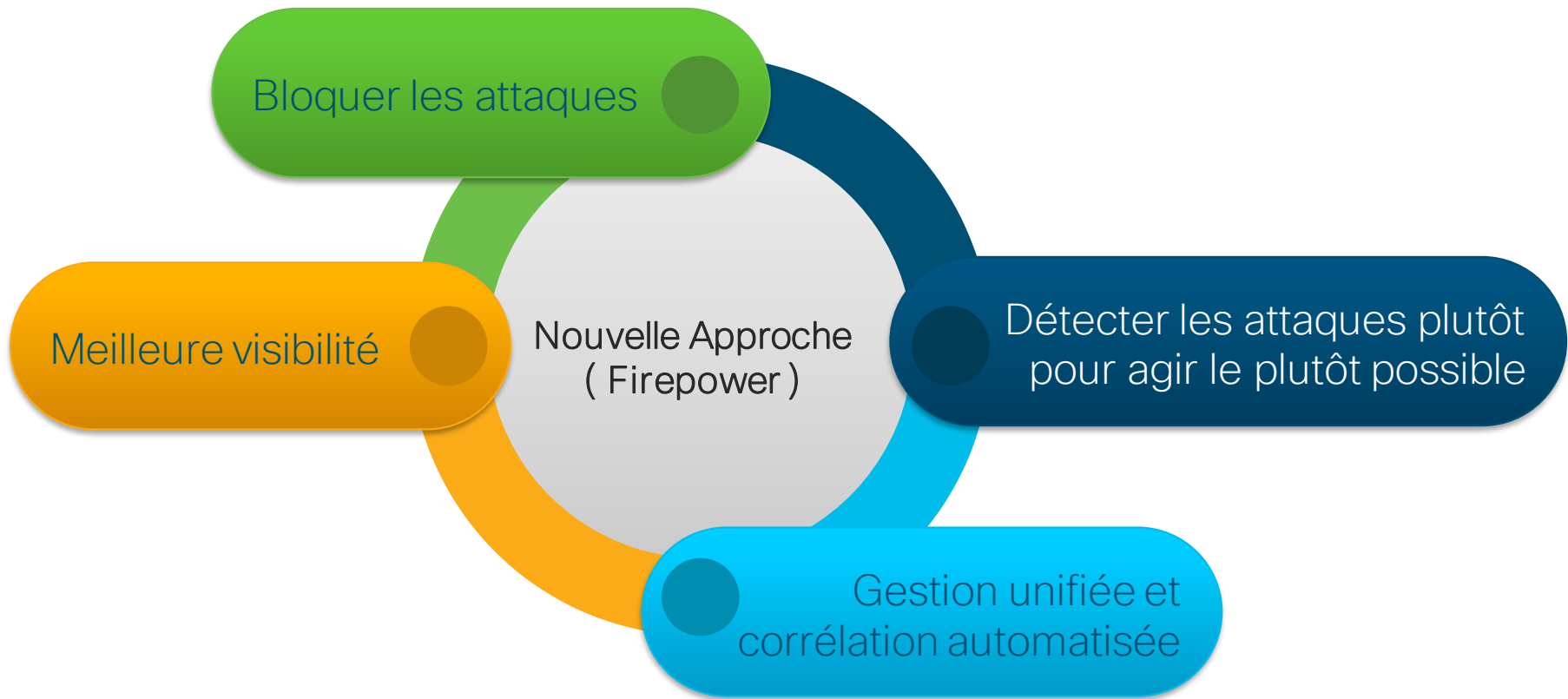


➤ Nécessité de collection des informations concernant ce qui se passe sur le réseau.



➤ Un mécanisme d'automatisation intelligente permet de voir et en temps réel le maximum de données **corrélées**.

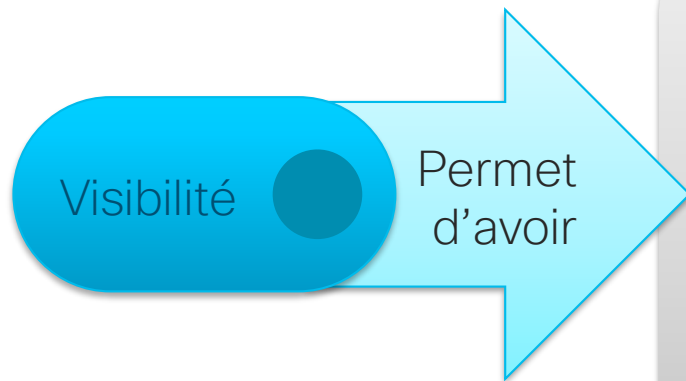






NGIPS

- Gestion des menaces **avant**, **pendant** et **après les attaques** en remontant dans le temps si nécessaire pour mieux identifier les dommages.



Les informations contextuelles dont nous avons besoin pour évaluer correctement les utilisateurs, les hôtes et les applications sur le réseau, pour détecter les menaces multivecteurs et pour élaborer une réponse automatisée.



NGIPS

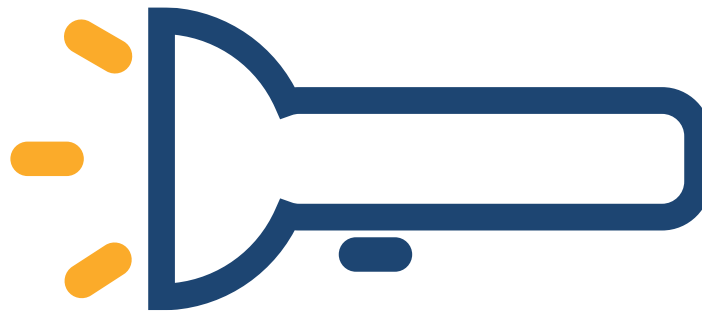
☞ Rassemble donc :

- Des fonctions de firewall.
- De contrôle des applications.
- De protection contre les malwares.
- De prévention des intrusions.

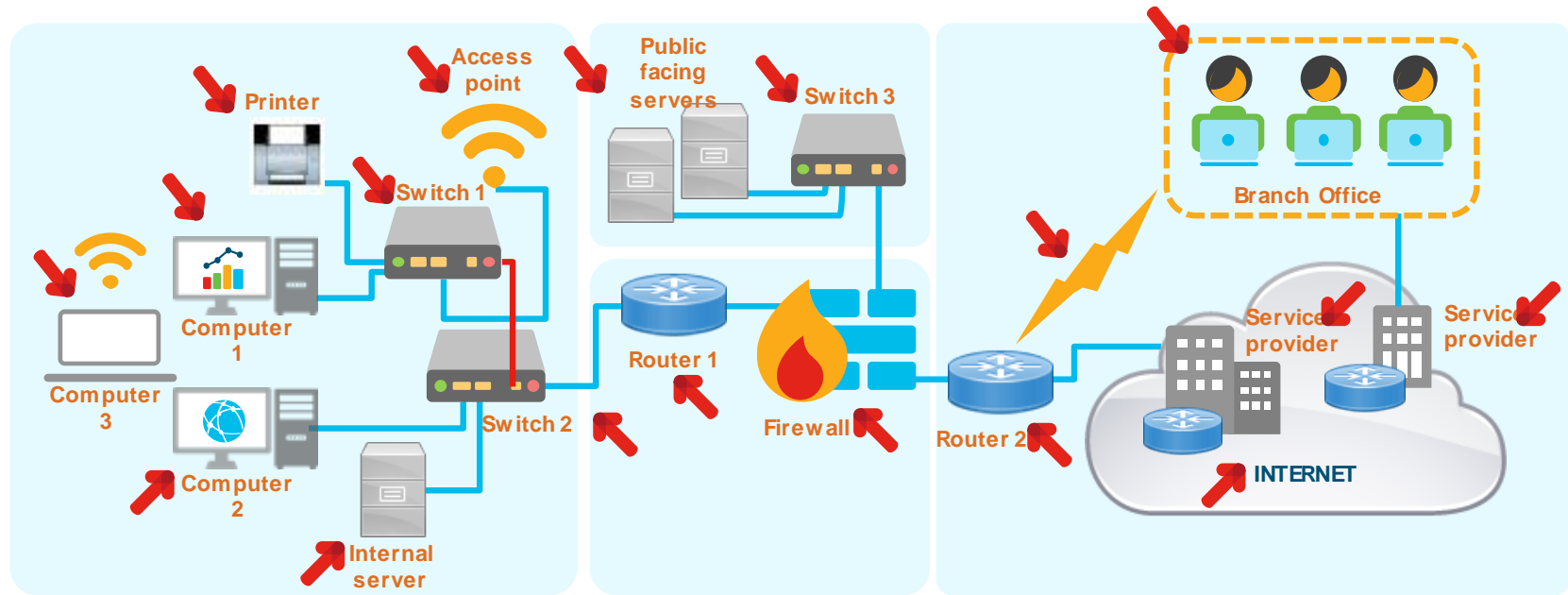
Sur une seule plateforme, afin de fournir une protection en continu.



Les applications, les utilisateurs, les appareils, les systèmes d'exploitation, les vulnérabilités, les services, les processus, les comportements réseau, les fichiers et les menaces.



Corrélation de grandes quantités de données



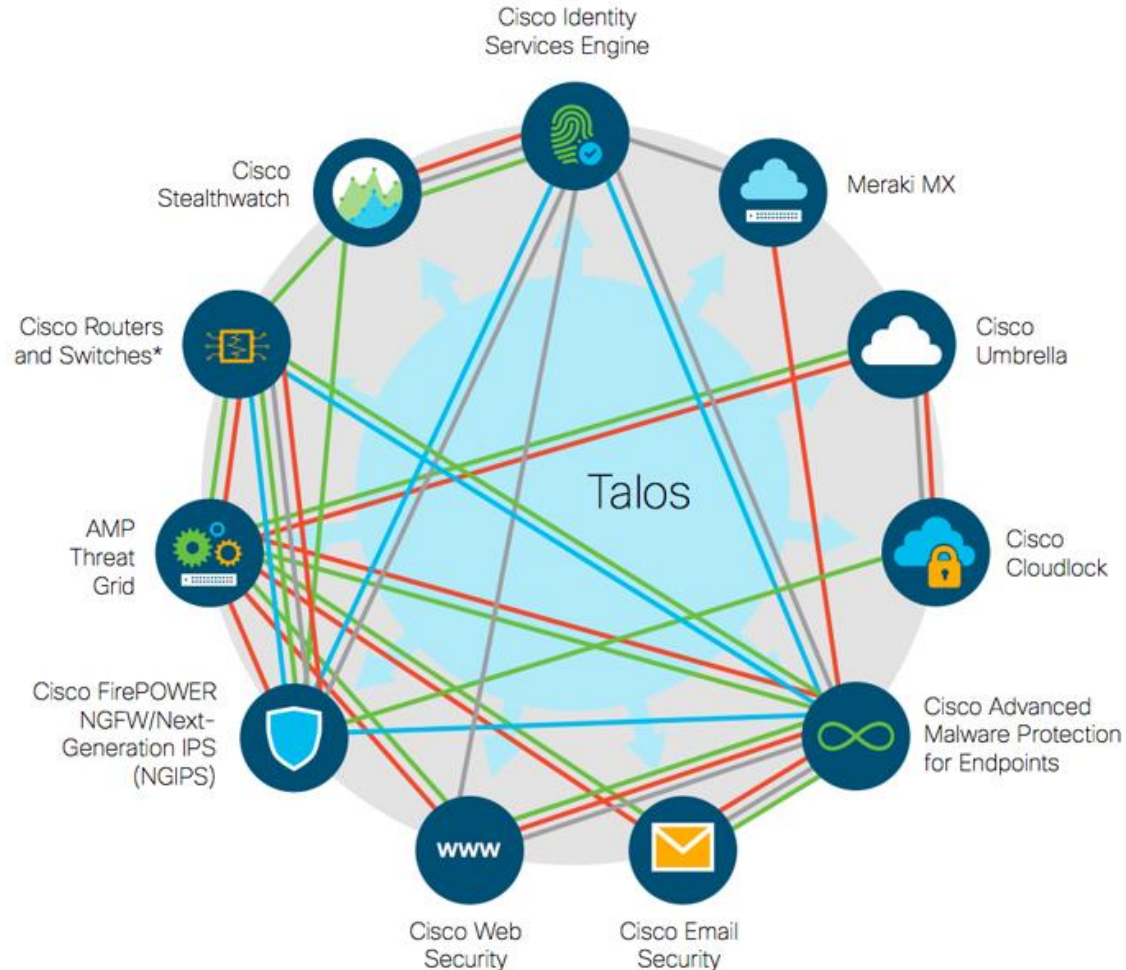
Difficile à rassembler des informations concernant: **les hôtes ciblés**, **les versions des systèmes d'exploitation**, **les serveurs et les applications en cours d'exécution**, **les terminaux mobiles**, **les activités des utilisateurs en temps réel** dans un seul endroit à portée de clic.



- Détecter les attaques plus tôt pour agir plus vite.
- Gestion unifiée et de la corrélation automatisée des attaques par le biais de fonctions de sécurité étroitement intégrées.

Flexibilité

- NGIPS reçoit de nouvelles règles de politique et signatures toutes les deux heures, donc votre sécurité est toujours à jour.
- **Cisco Talos** exploite le plus grand réseau de détection des menaces du monde pour apporter une efficacité de sécurité à chaque produit de sécurité Cisco.



Laboratoire



Objectif : pour mieux se défendre

Une des pratiques et des méthodologies utilisées par les hackers dans le cadre d'intrusions sur les réseaux et les applications.

Metasploit ?

Il s'agit d'un Framework (sur Linux) de test d'intrusion qui simplifie le piratage. Un outil essentiel pour de nombreux attaquants, **mais aussi pour les défenseurs des systèmes informatiques.**



Dissipez vos
doutes



Utilisez le panneau « Q&R » pour
poser vos questions

Cisco Community – Demandez-moi ...

Avez-vous encore des questions sur la Cybersécurité ?

Foire aux Questions
Jusqu'au 13 mars

avec Boubaker Kherfallah
Événement public

Suivez le lien

<http://bit.ly/AMA-mar20>



The banner features a dark blue background with a central image of a modern office interior. In the top left corner, there is an orange pill-shaped button with a thumbs-up icon and the word "Questions". On the right side, there is a circular portrait of a man in a blue shirt, surrounded by several colorful question marks in shades of blue, orange, and green. Below the office image, the text "Demandez-moi N'importe Quoi à propos de ..." is written in white, followed by "La Cybersécurité : Concepts sur les intrusions" in a larger white font. At the bottom, there is a dark blue bar containing the text "Avec Boubaker Kherfallah" and "Foire aux Questions | Jusqu'au 13 mars" in white. On the right side of this bar, there is a bright blue pill-shaped button with the text "Posez vos Questions !" in white.

Questions

Demandez-moi N'importe Quoi à propos de ...
La Cybersécurité : Concepts sur les intrusions

Avec Boubaker Kherfallah
Foire aux Questions | Jusqu'au 13 mars

Posez vos Questions !

La communauté est disponible dans d'autres langues

Si vous parlez anglais, espagnol, portugais, russe, chinois ou japonais, vous pouvez participer aussi dans les autres communautés Cisco.

[Cisco Community](#)

Anglais

[Сообщество Cisco](#)

Russe

[Comunidad de Cisco](#)

Espagnol

[Comunidade da Cisco](#)

Portugais

[思科服务支持社区](#)

Chinois

[シスココミュニティ](#)

Japonais

Nous vous invitons à nous suivre dans les réseaux sociaux et à partager nos prochains événements

Cisco Community

- Facebook/CiscoSupportCommunity
- Twitter @cisco_support
- YouTube ciscosupportchannel
- LinkedIn Cisco Community
<https://www.linkedin.com/showcase/3544800/>
- Instagram ciscosupportcommunity
<https://www.instagram.com/ciscosupportcommunity/>



Votre avis nous
intéresse !



Veillez remplir le sondage qui
apparaîtra sur votre écran à la fin
de cette présentation.



Merci pour votre participation !



