

# Chapitre 1 : Les menaces modernes de la sécurité réseau

CCNA Security v2.0

Samir DIABI



# Sommaire

- 1.0 Introduction
- 1.1 Sécuriser des réseaux
- 1.2 Les menaces réseaux
- 1.3 Atténuer les menaces
- 1.4 Résumé

# Section 1.1 : Sécuriser des réseaux

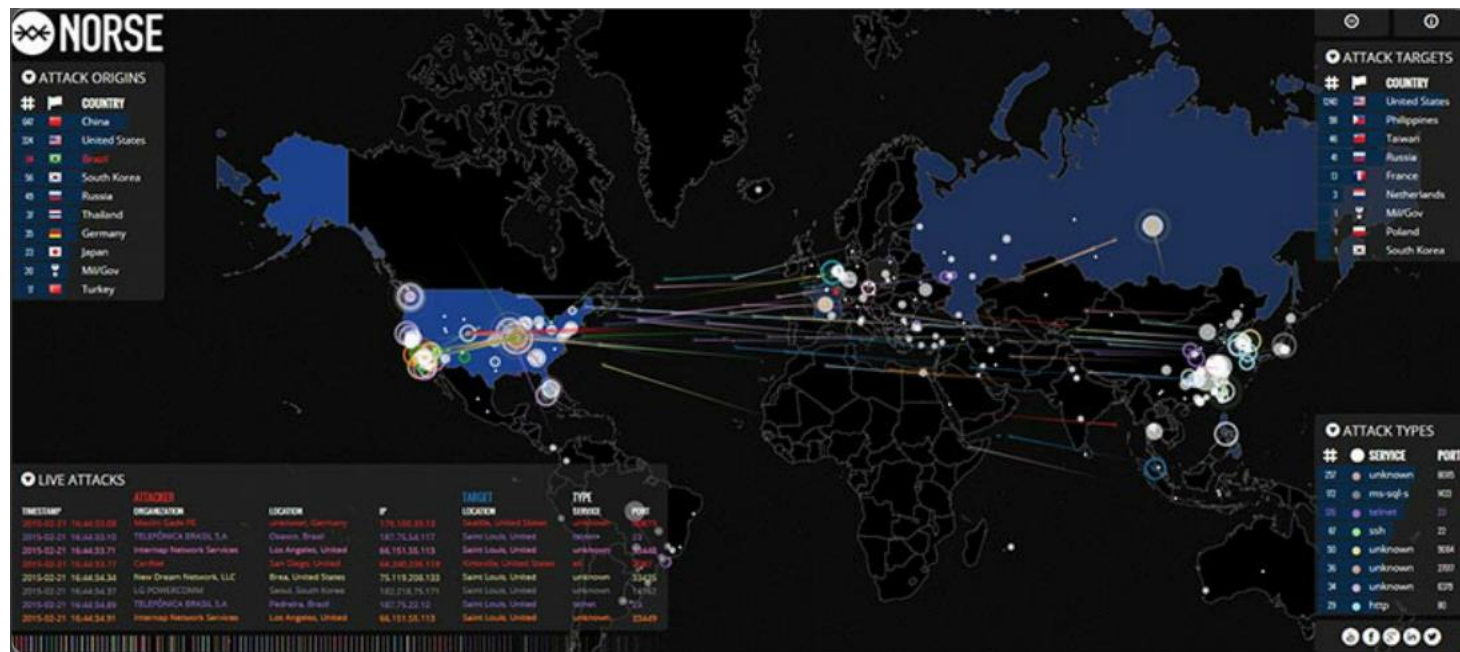
À la fin de cette section, vous devriez être en mesure de :

- Décrire le contexte actuel de la sécurité réseau.
- Expliquer comment tous les types de réseaux doivent être protégés.

## Rubrique 1.1.1 : Situation actuelle



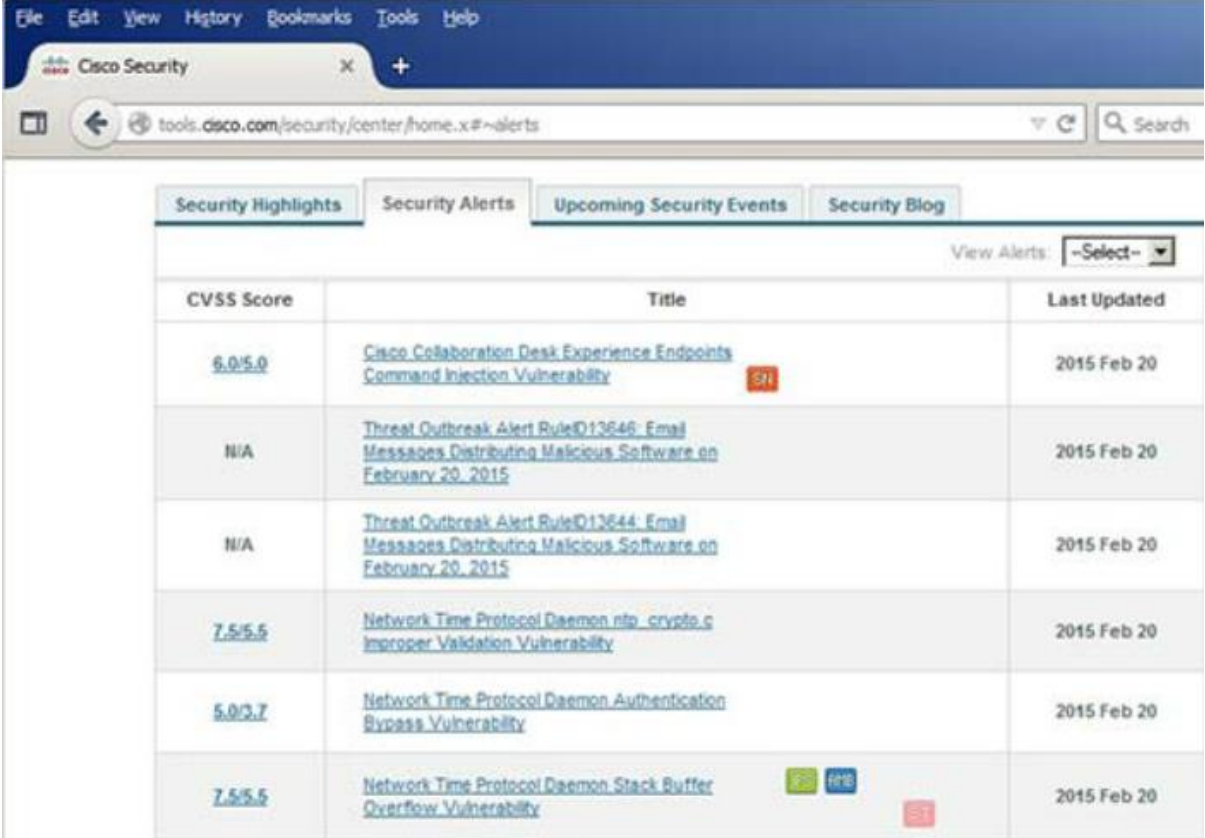
# Les réseaux sont des cibles



# Guides pour la sécurité du réseau

Les termes courants de sécurité réseau :

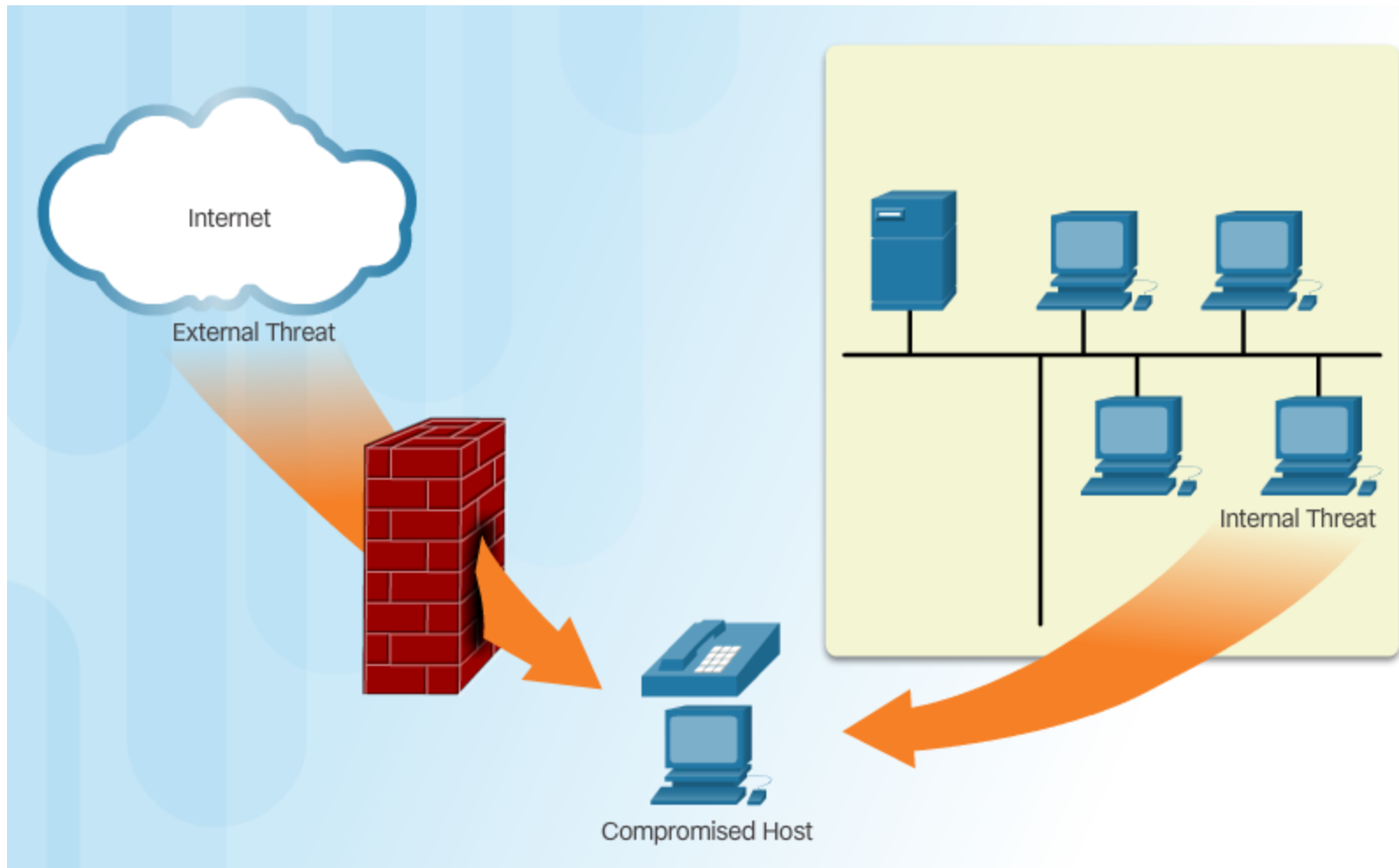
- menace
- vulnérabilité
- atténuation
- risque



The screenshot shows the Cisco Security Center web interface. The browser address bar displays 'tools.cisco.com/security/center/home.x#~alerts'. The interface includes tabs for 'Security Highlights', 'Security Alerts', 'Upcoming Security Events', and 'Security Blog'. A 'View Alerts' dropdown menu is set to '-Select-'. Below the tabs is a table with three columns: 'CVSS Score', 'Title', and 'Last Updated'. The table lists several security alerts, including a 'Cisco Collaboration Desk Experience Endpoints Command Injection Vulnerability' with a CVSS score of 6.0/5.0 and a 'Network Time Protocol Daemon Stack Buffer Overflow Vulnerability' with a CVSS score of 7.5/5.5. Each entry includes a link to the vulnerability details and a 'Last Updated' date of 2015 Feb 20.

CVSS Score	Title	Last Updated
6.0/5.0	<a href="#">Cisco Collaboration Desk Experience Endpoints Command Injection Vulnerability</a>	2015 Feb 20
N/A	<a href="#">Threat Outbreak Alert RuleID13646: Email Messages Distributing Malicious Software on February 20, 2015</a>	2015 Feb 20
N/A	<a href="#">Threat Outbreak Alert RuleID13644: Email Messages Distributing Malicious Software on February 20, 2015</a>	2015 Feb 20
7.5/5.5	<a href="#">Network Time Protocol Daemon ntp_crypto.c Improper Validation Vulnerability</a>	2015 Feb 20
5.0/3.7	<a href="#">Network Time Protocol Daemon Authentication Bypass Vulnerability</a>	2015 Feb 20
7.5/5.5	<a href="#">Network Time Protocol Daemon Stack Buffer Overflow Vulnerability</a>	2015 Feb 20

# Vecteurs d'attaques réseaux



# Perte de données

Vecteurs de perte de données :

- Courriel / Webmail
- Dispositifs non cryptés
- Périphériques de stockage Cloud
- Média amovible
- Copie conforme
- Contrôle d'accès incorrect

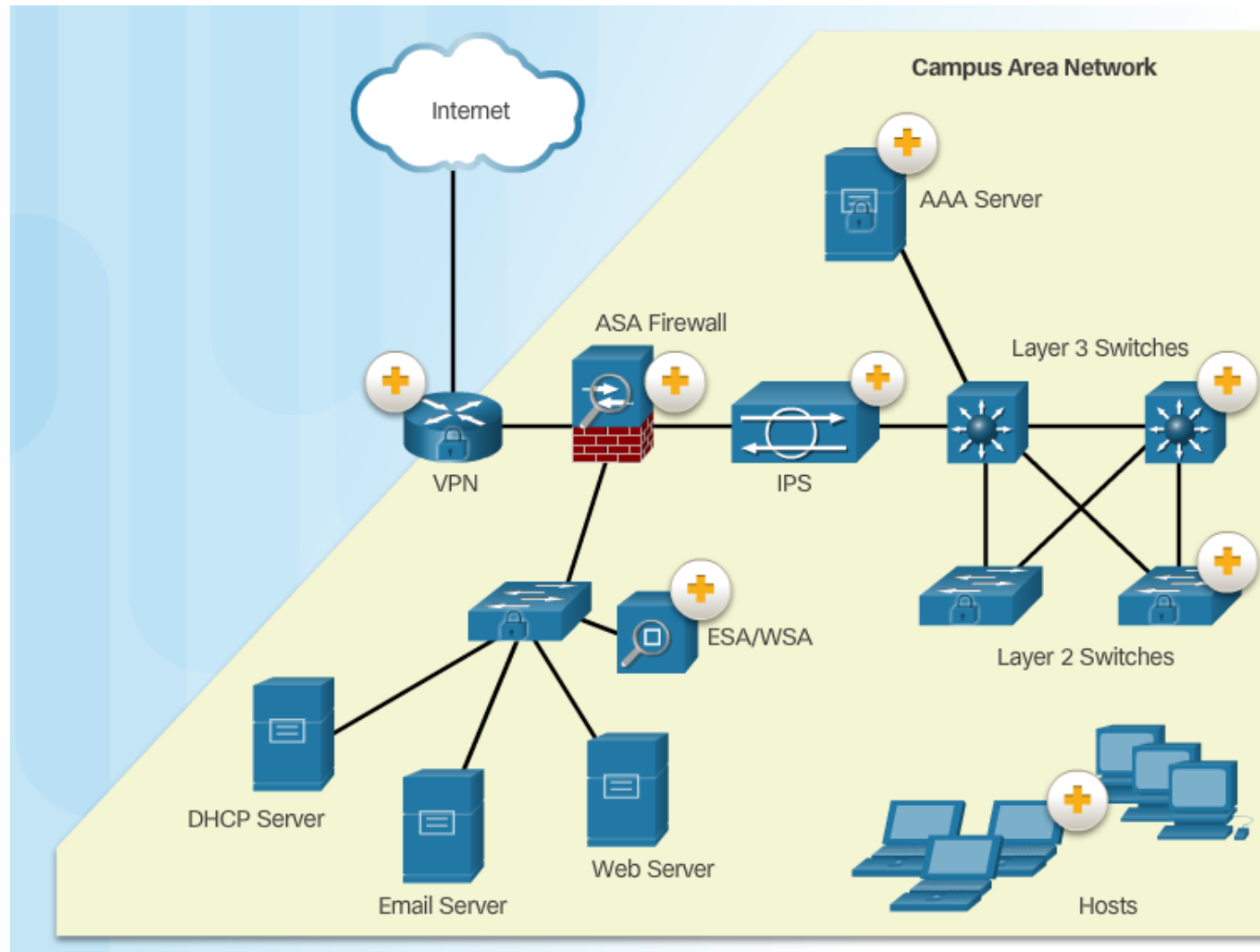




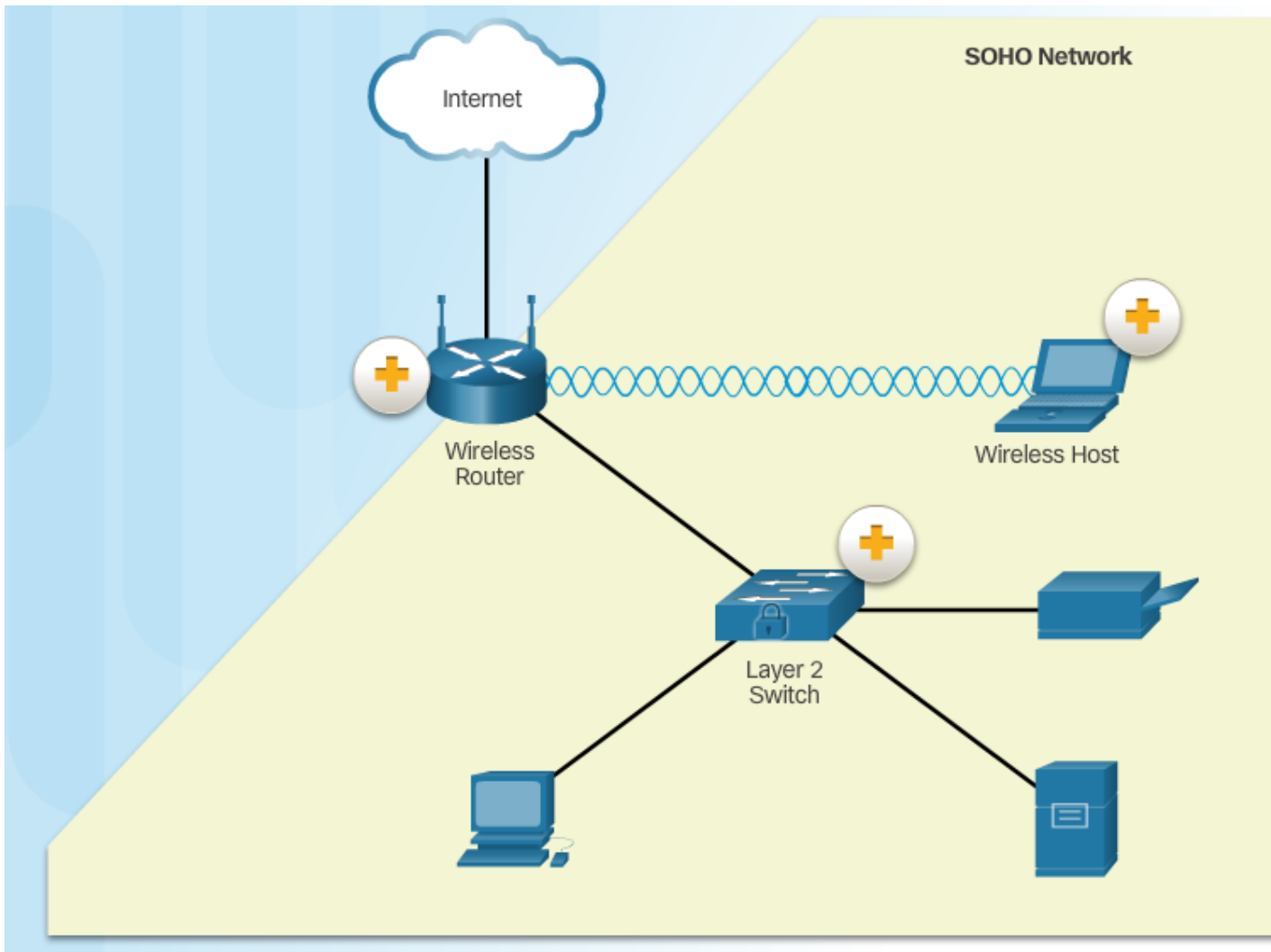
## Rubrique 1.1.2 : aperçu des topologies réseaux



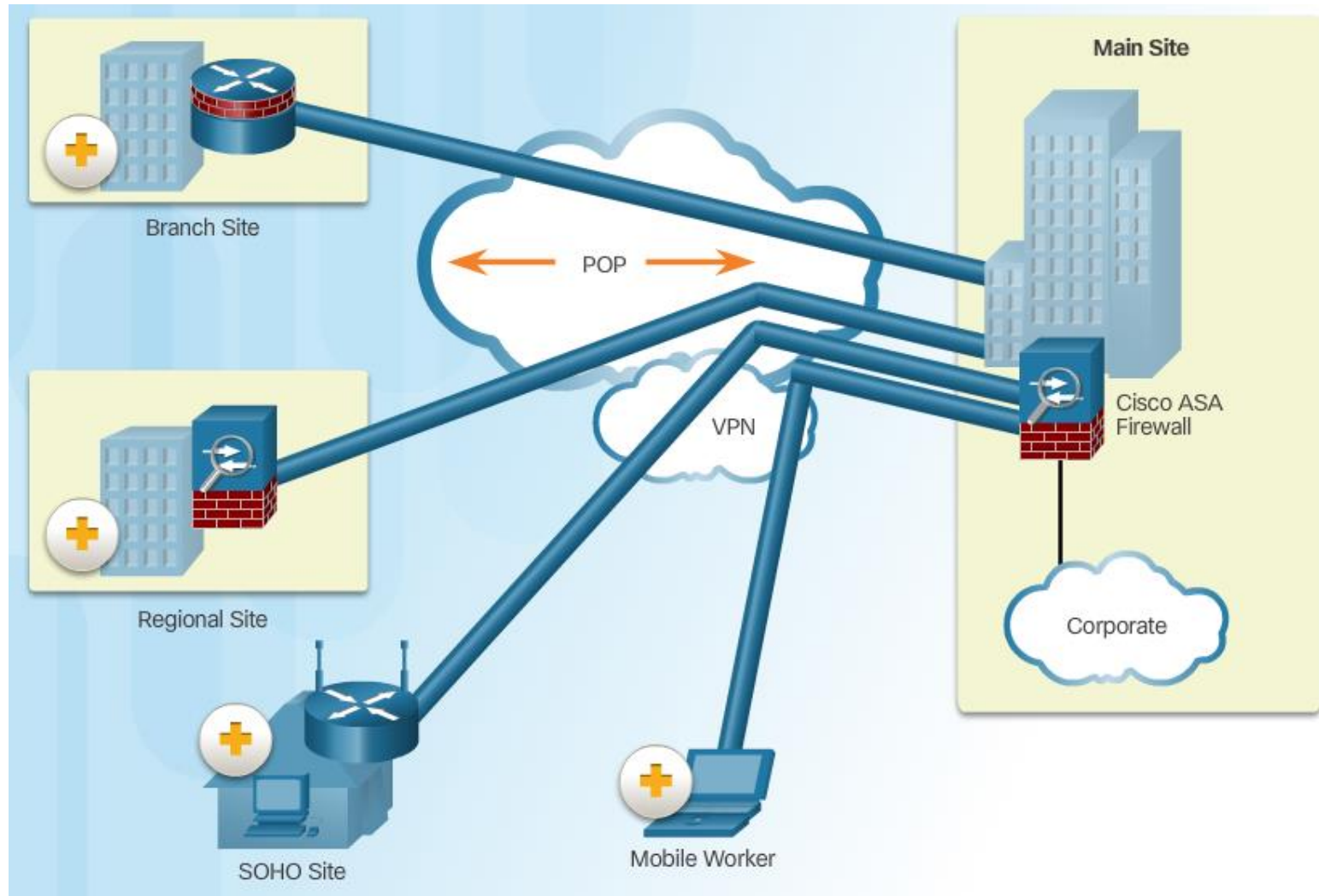
# Les réseaux campus



# Petites et moyennes entreprises



# Les réseaux étendus



# Réseaux des datacenter

## Sécurité extérieure du périmètre.

- agents de sécurité sur place
- Clôtures et portails
- Surveillance vidéo continue
- Alarmes de violation de sécurité



## Sécurité à l'intérieur du périmètre.

- Détecteurs de mouvements électroniques
- Pièges de sécurité
- Surveillance vidéo continue
- Capteurs biométriques d'accès et de sortie



# Nuages et réseaux virtuels

## Menaces spécifiques à VM.

- Hyperjacking
- Activation instantanée
- Tempête d'antivirus

## Composants d'un datacenter sécurisé.

- Segmentation sécurisée
- Défense de la menace
- Visibilité

# La frontière du réseau évolutif

## Fonctions critiques pour les réseaux BYOD.

- Cryptage des données
- Imposer utilisation de PIN / schéma ,,
- Supprimer les données
- Prévention des pertes de données
- Détection de Jailbreak / root

# Section 1.2 :

## Menaces des réseau

À la fin de la section, vous devriez être en mesure de :

- Décrire l'évolution de la sécurité réseau.
- Décrire les différents types d'outils d'attaque utilisés par les pirates.
- Décrire les logiciels malveillants.
- Expliquer les attaques de réseau répandus.

## Rubrique 1.2.1 : Qui pirate nos réseaux ?





# Le pirate & l'évolution des pirates



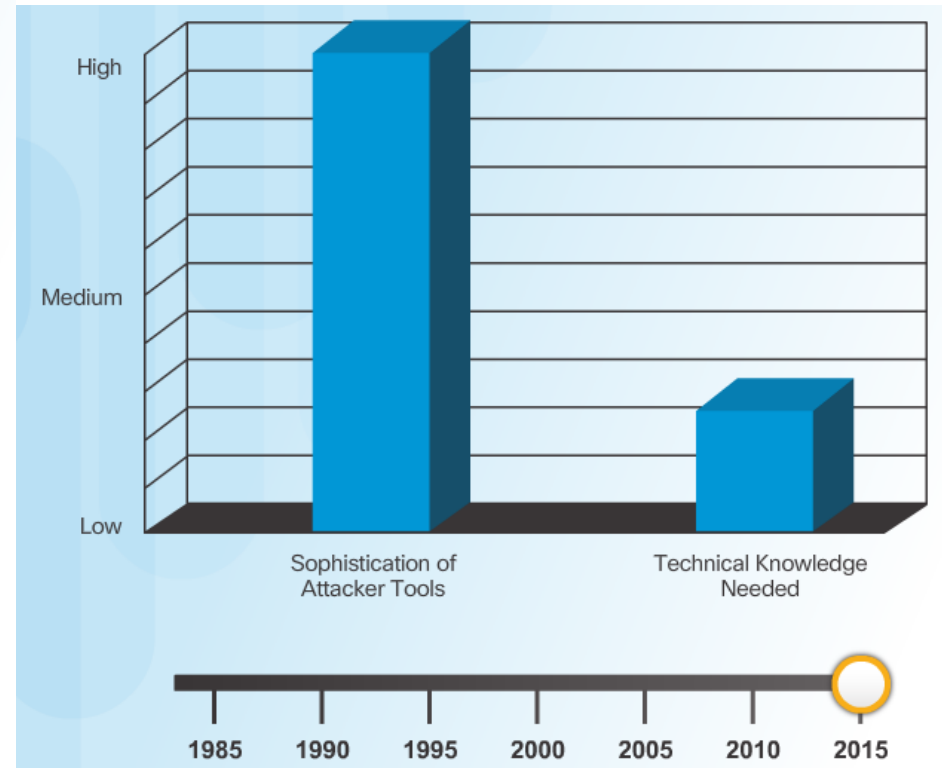
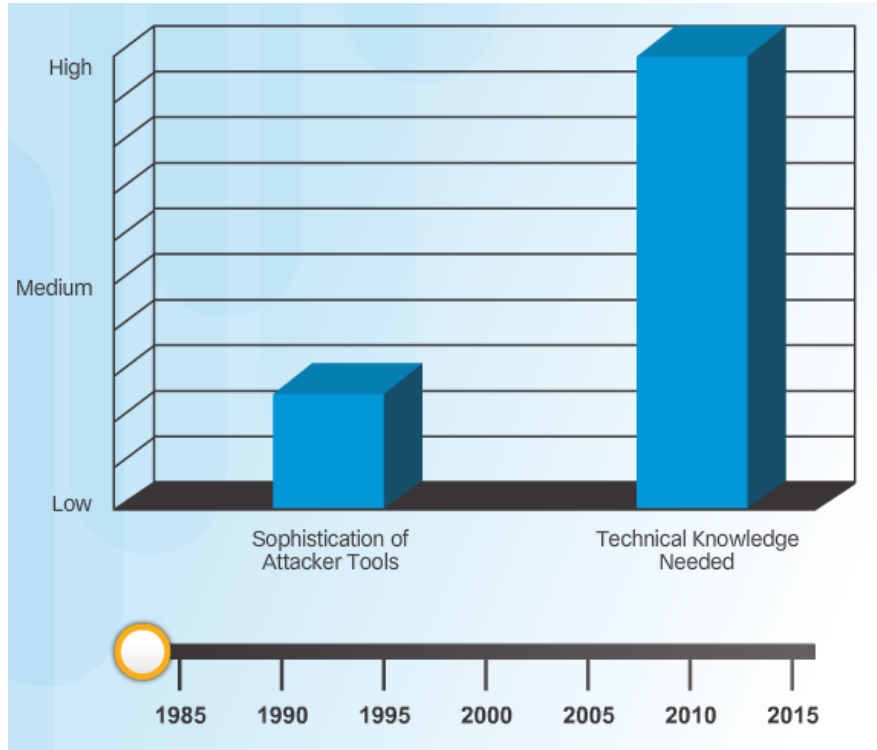
Titres de piratage modernes:

- Script Kiddies
- Commerçants de vulnérabilités
- Hacktivistes
- Cybercriminels
- Les pirates informatiques

## Rubrique 1.2.2 : Outils de Hacker



# Intoduction d'outils d'attaque



# Évolution des outils de sécurité

## Outils de test de pénétration.

- Mot de passe crackers
- Le piratage réseau sans fil
- Numérisation réseau et piratage
- Packet crafting (Formatage de paquets)
- Renifleurs de paquets
- Détecteurs de rootkits
- Outils de recherche des vulnérabilités
- Exploitation de la vulnérabilité
- Scanners de vulnérabilité
- Débogueurs



# Catégories des outils d'attaque

## Attaques de piratage réseau:

- L'écoute électronique
- Modification des données
- Spoofing d'adresse IP
- Attaques de mot de passe
- Dénî de service
- L'homme du milieu
- Clé compromise
- Sniffer



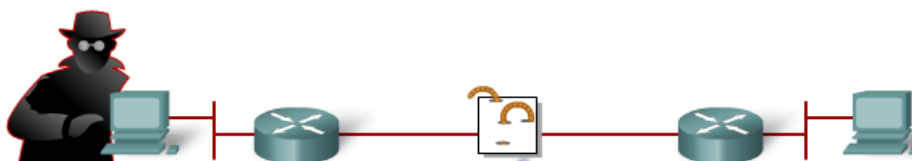
## Rubrique 1.2.3 : Malware



# Différents Types de Malwares



Un virus est un logiciel malveillant intégré à un autre programme pour exécuter des fonctions particulières indésirables sur l'ordinateur de l'utilisateur.



Un ver exécute un code arbitraire et installe des copies de lui-même dans la mémoire de l'ordinateur infecté, ce qui infecte d'autres ordinateurs hôtes.



Un cheval de Troie se distingue uniquement par le fait qu'il a été entièrement conçu pour ressembler à une application normale, alors qu'il s'agit d'un instrument d'attaque.

# Virus

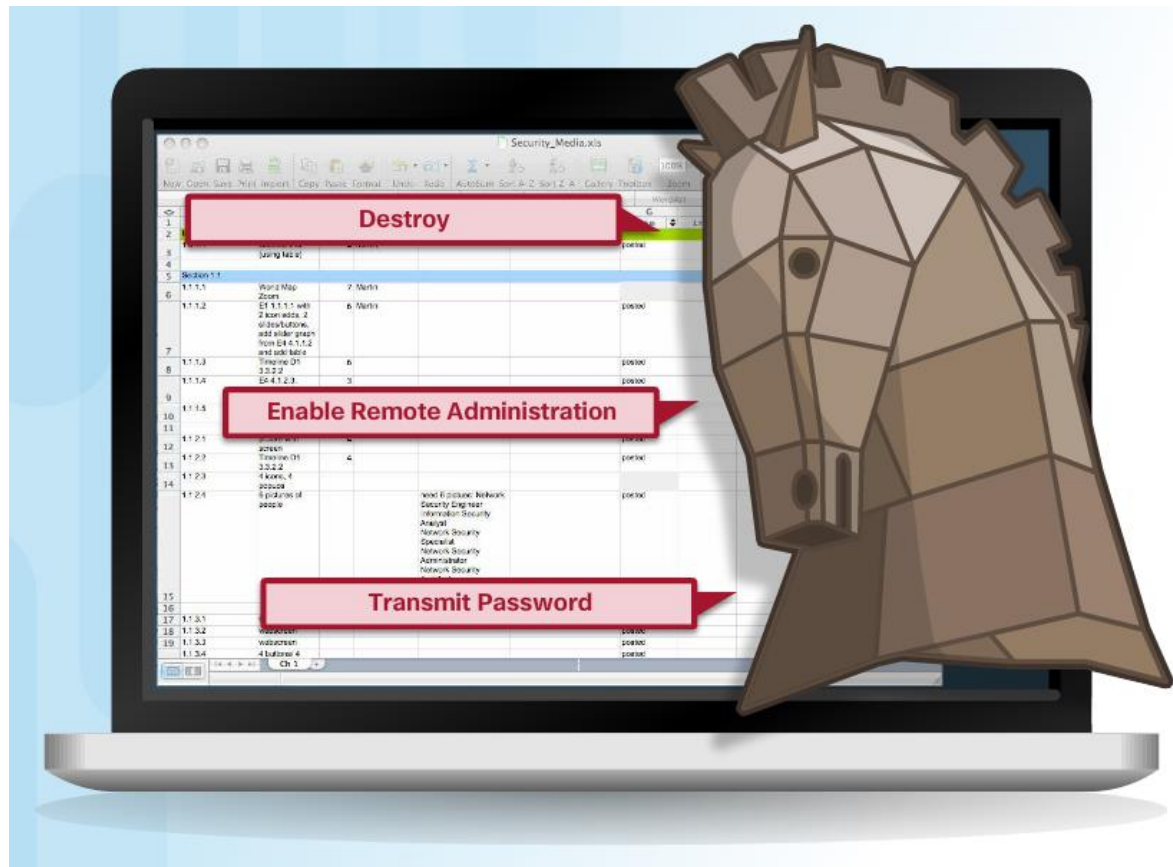




# Classement des chevaux de Troie

## Classifications:

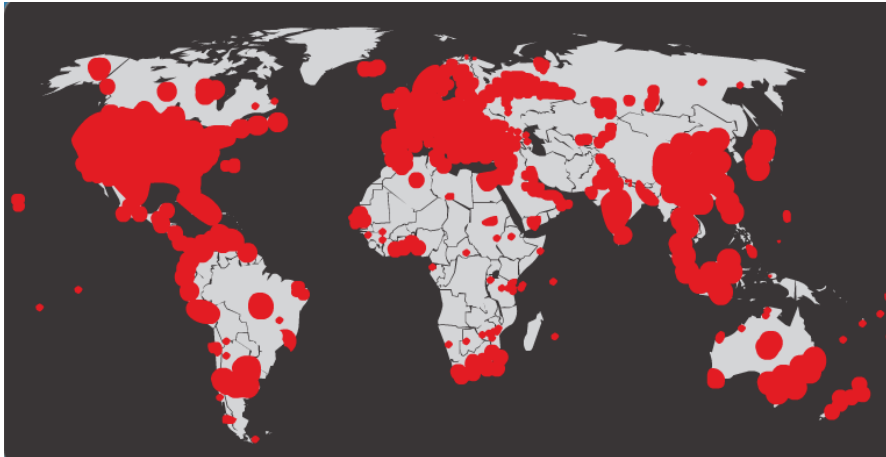
- Interrupteur logiciel de sécurité
- Accès à distance
- Envoi de données
- Destructeur
- Proxy
- FTP
- DoS



# Les vers : Code Red



Infection par le ver

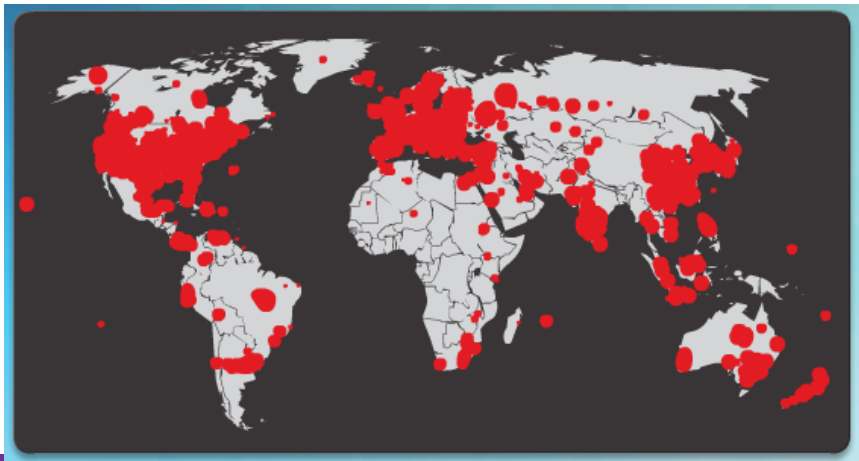


Infection par le ver 19 heures plus tard

# Les vers : SQL Slammer



**Infection initiale par le ver SQL Slammer**

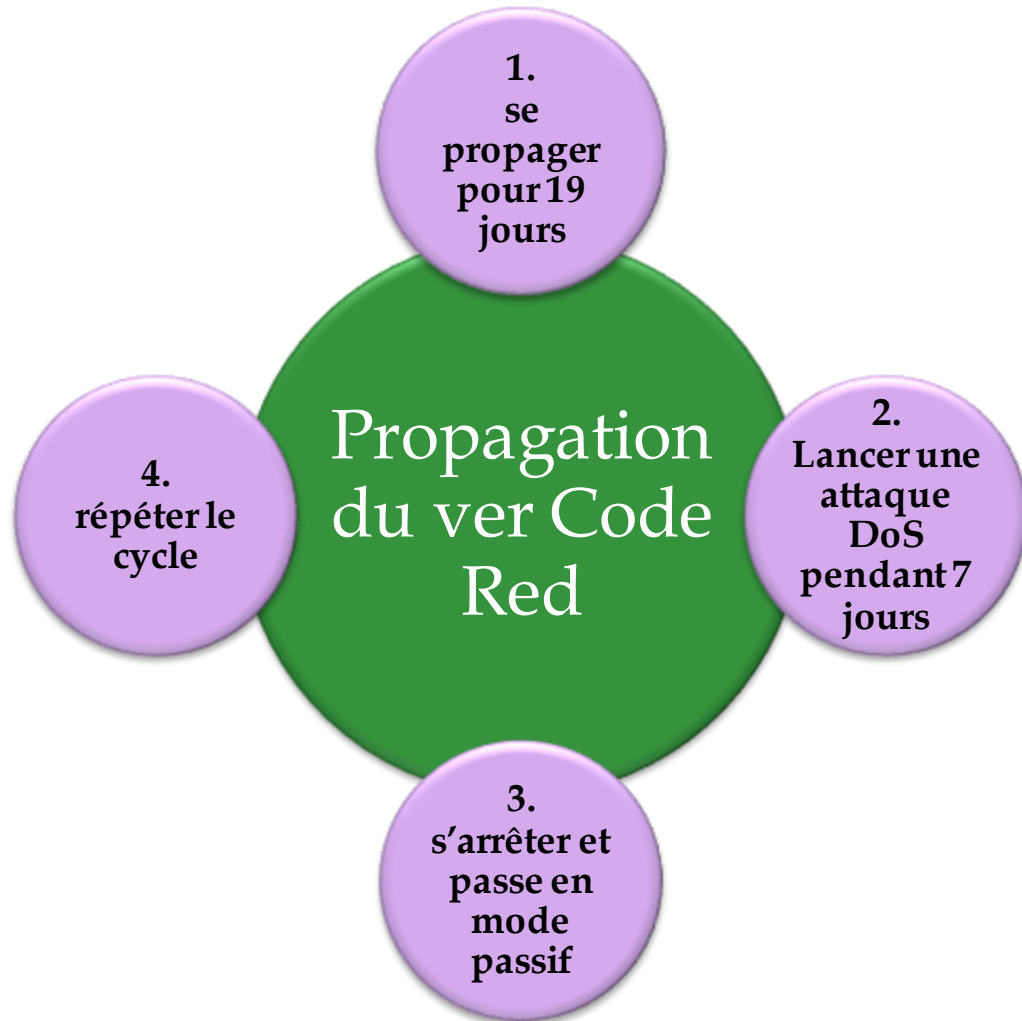


**Infection par le ver SQL Slammer  
1/2 heure après**

# Composants de ver

## Composants:

- Activation de la vulnérabilité
- Mécanisme de propagation
- Charge utile



# Autres Malware



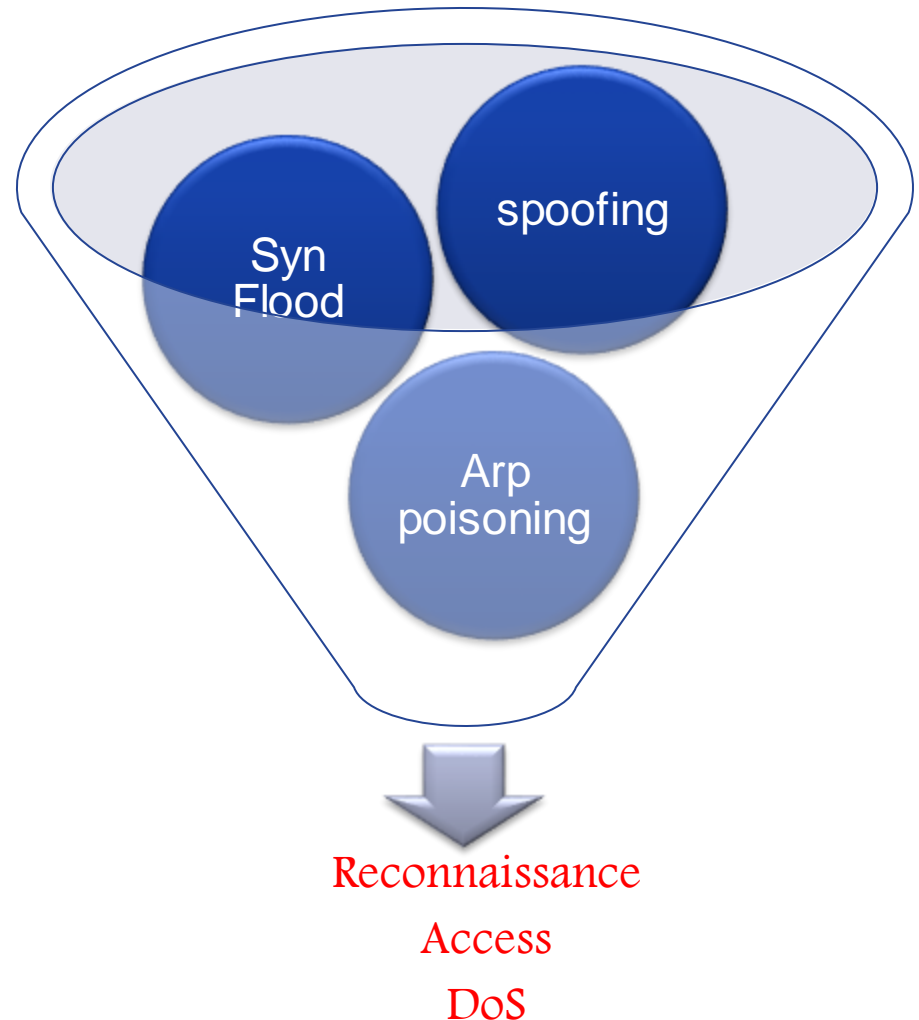
## Sujet 1.2.4 : Les attaques modernes des réseaux





# Types d'attaques de réseau

- Il existe énormément d'attaques réseaux.
- Pourquoi les attaques réseaux ?
- Quelles sont les objectifs des pirates à travers de telles attaques.
- Pour mieux comprendre; catégoriser :
  - **Reconnaissance**
  - **Accès**
  - **Déni de service**



# Attaques de reconnaissance

- Requête initiale d'une cible
- Balayage ping du réseau cible
- Balayage des ports d'adresses IP actives
- Scanneurs de vulnérabilité





# Attaques d'accès

## Quelques raisons pour lesquelles les pirates utilisent les attaques d'accès:

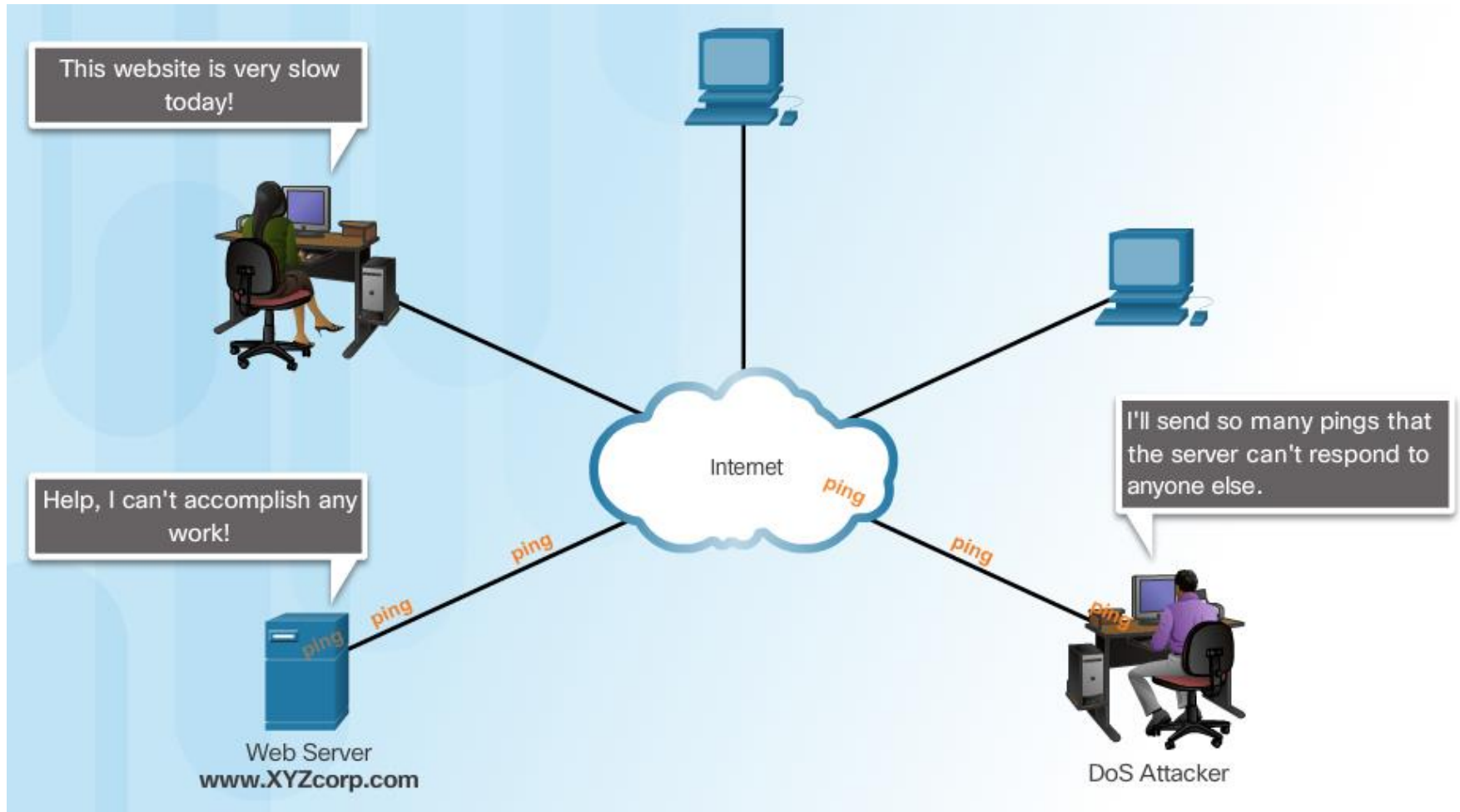
- Pour récupérer des données
- Obtenir l'accès
- Pour augmenter les privilèges d'accès

## Quelques types d'attaques d'accès incluent:

- Mot de passe
- Confiance dans l'exploitation
- Redirection de port
- Man-in-the-middle
- Buffer overflow
- IP, MAC, DHCP spoofing

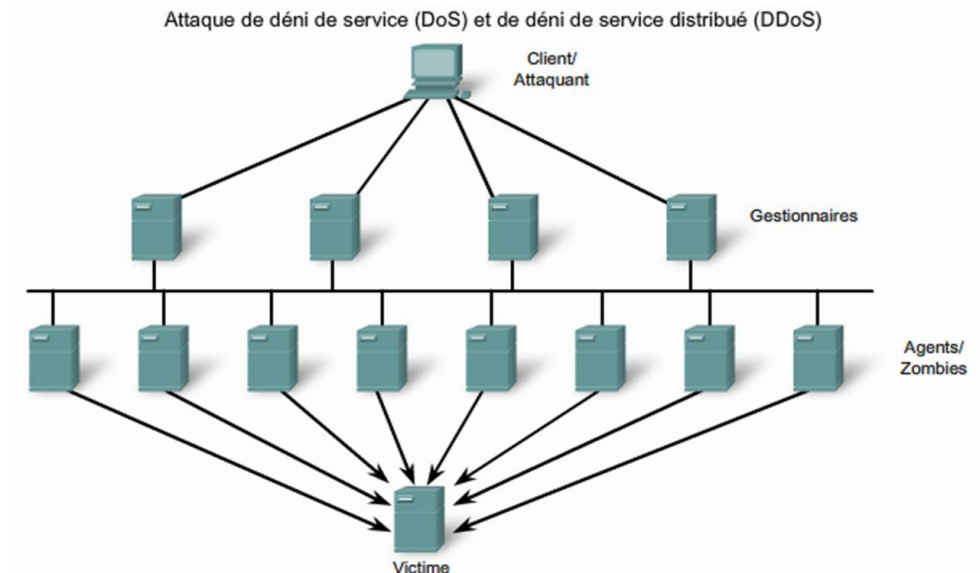
- E-MAIL AUFMACHUNG SOZIALE ENGINEER METHODE DUMPFSTER MÜGLICHE MONAT VERTRÄGLICHEN ES STEHT

# Attaques de déni de service



# Attaques DDoS

1. Les pirates informatique construisent un réseau des machines infectées
  - Un réseau des hôtes infectés est appelé un botnet.
  - Les ordinateurs compromis sont appelés des zombies.
  - Les Zombies sont contrôlés par un gestionnaire système.
2. Les ordinateurs zombies continuent de balayer et d'infecter d'autres cibles.
3. Au moment opportun, Les pirates indiquent au gestionnaire système d'activer le botnet de zombies pour mener l'attaque DDoS.



# 1.3 Atténuer les menaces

À la fin de cette section, vous devriez être en mesure de ::

- Décrire les méthodes et ressources pour protéger les réseaux.
- Décrire un ensemble de domaines pour la sécurité du réseau.
- Expliquer le but de l'Architecture de SecureX Cisco.
- Décrire les techniques utilisées pour atténuer les attaques modernes de réseau.
- Expliquer comment sécuriser les trois domaines fonctionnels des routeurs et commutateurs Cisco.

## Rubrique 1.3.1 : Défendre le réseau



# Professionnels de la sécurité du réseau

- ✓ Actualiser constamment ses compétences et ses connaissances par rapport aux nouvelles menaces.
- ✓ Suivre des formations et des workshops.
- ✓ S'abonner aux newsletters temps réel sur les menaces.
- ✓ Suivre les sites de sécurité quotidiennement et avec grande attention.
- ✓ Garder contact avec les organisations de sécurité réseau. Ces organisations fournissent les dernières nouveautés liées aux menaces et aux vulnérabilités.





# Organismes de sécurité réseau





# Organisme marocain de sécurité des systèmes d'information

ADMINISTRATION DE LA DEFENSE NATIONALE

**DIRECTION GENERALE DE LA SECURITE  
DES SYSTEMES D'INFORMATION**

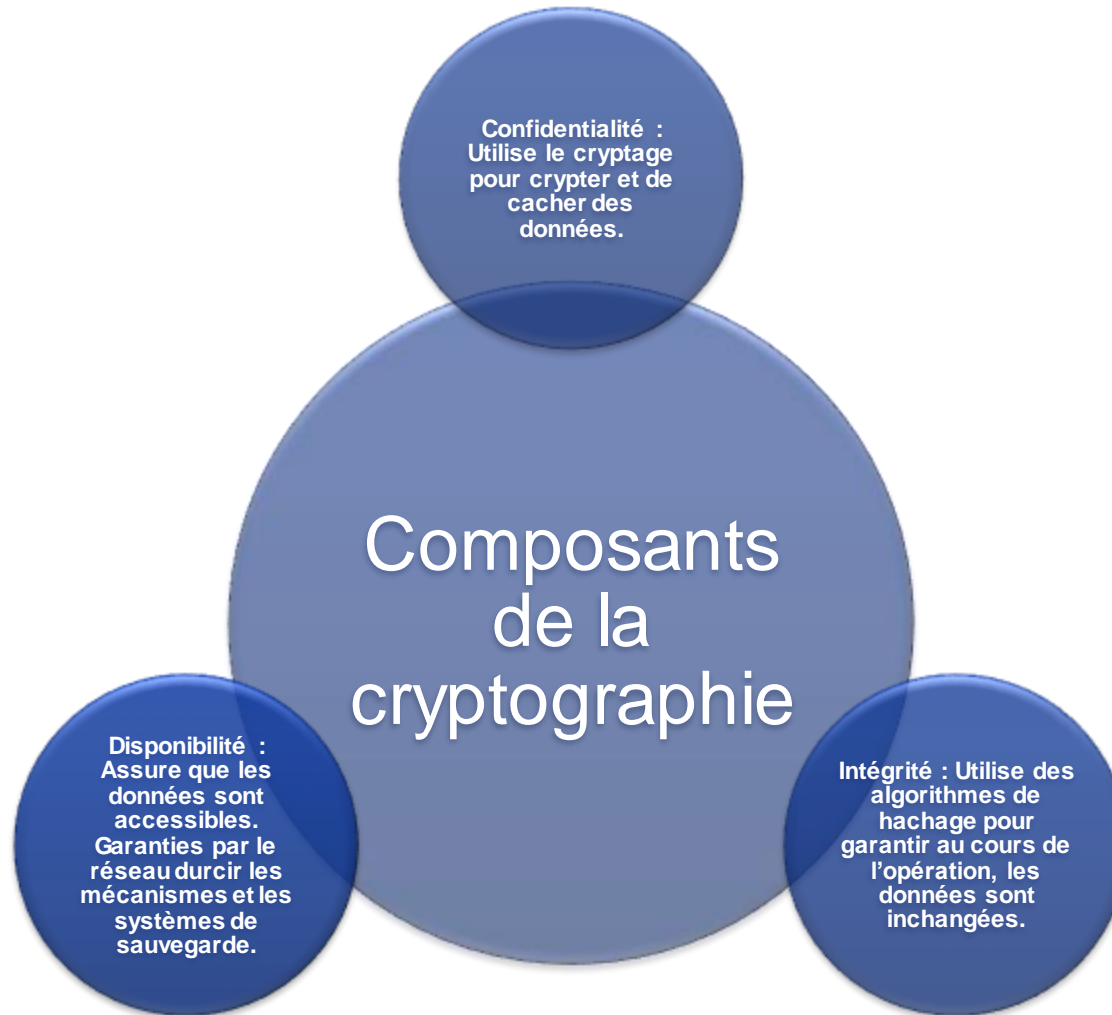


إدارة الدفاع الوطني  
المديرية العامة لأمن  
نظم المعلومات

- Direction Générale de la Sécurité des Systèmes d'Information.

<http://www.dgssi.gov.ma/>

# Confidentialité, Intégrité, Disponibilité



## Rubrique 1.3.2 : Domaines de la sécurité réseau



# Domaines de sécurité réseau

- L'évaluation des risques
- Politique de sécurité
- Organisation de la sécurité de l'information
- La gestion d'actifs
- Sécurité des ressources humaines
- Sécurité physique et environnementale
- Gestion des communications et des opérations
- Acquisition, développement et maintenance de systèmes d'information
- Contrôle d'accès
- Gestion des incidents de sécurité de l'information
- Gestion de la continuité des activités
- Conformité

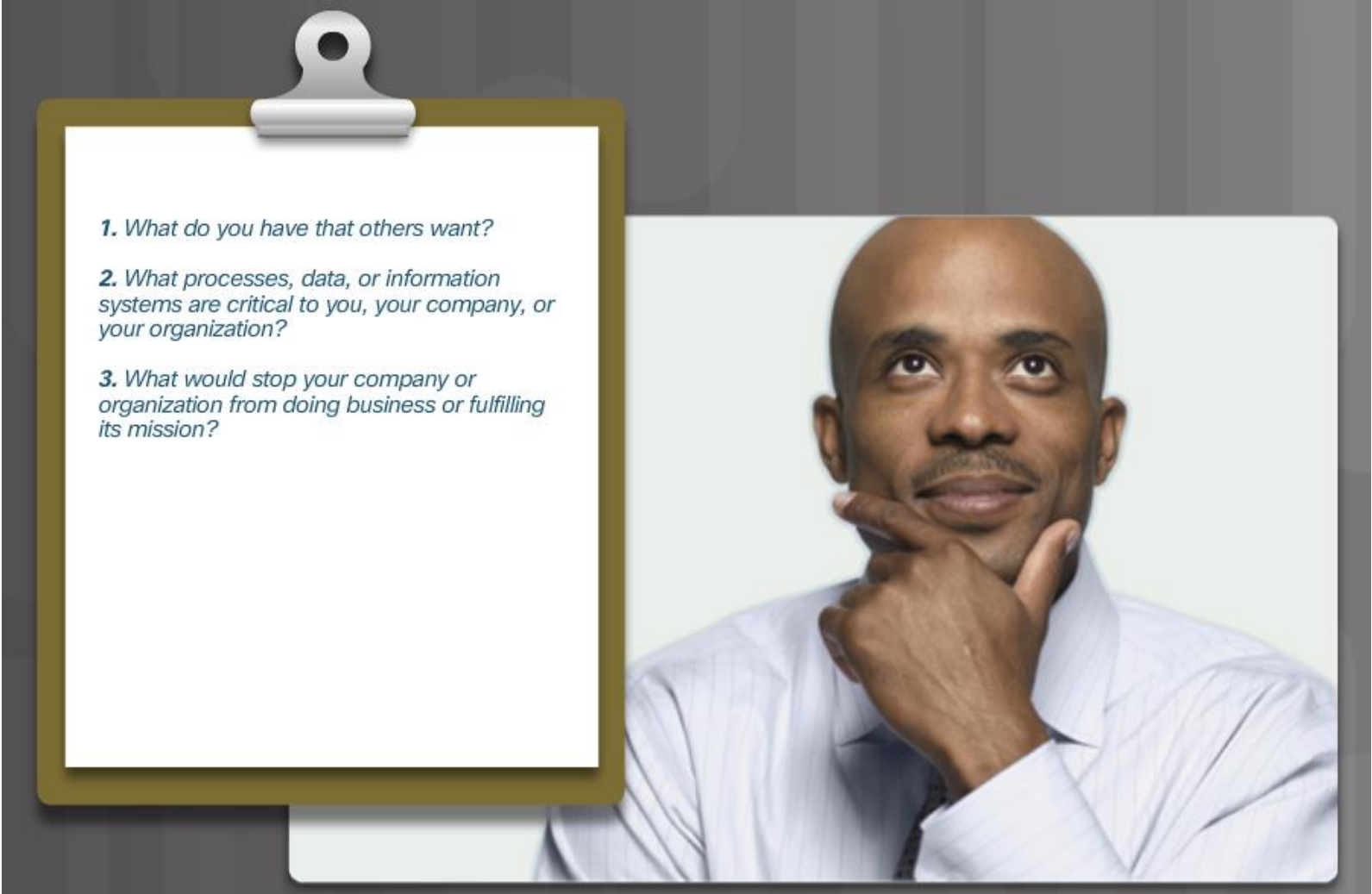
# Politique de sécurité réseau

Le prochain point sur la politique de sécurité à discuter est les règles des accès réseaux.

Nous devons garder en mémoire que nous avons des télé-travailleurs. Ils auront des règles d'accès différents que nos employés sur place.

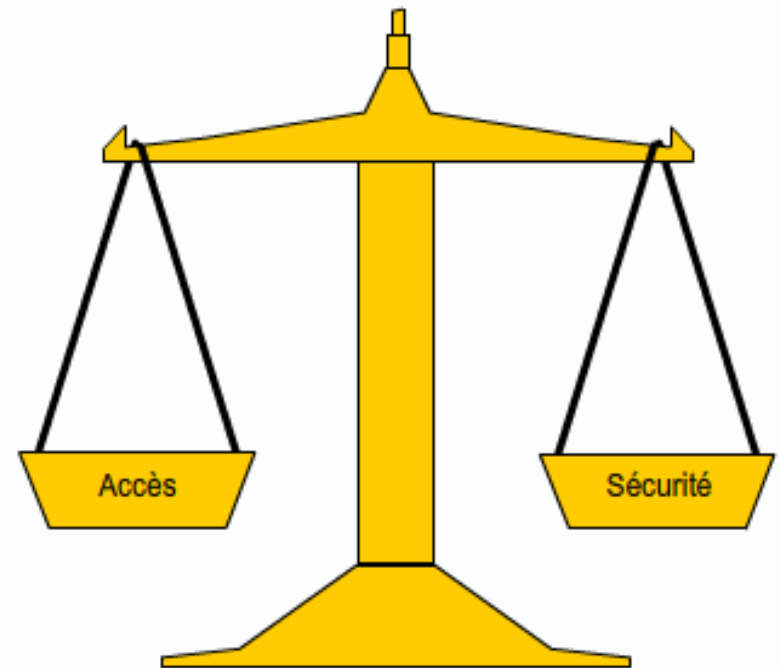


# Objectifs de la politique de sécurité réseau

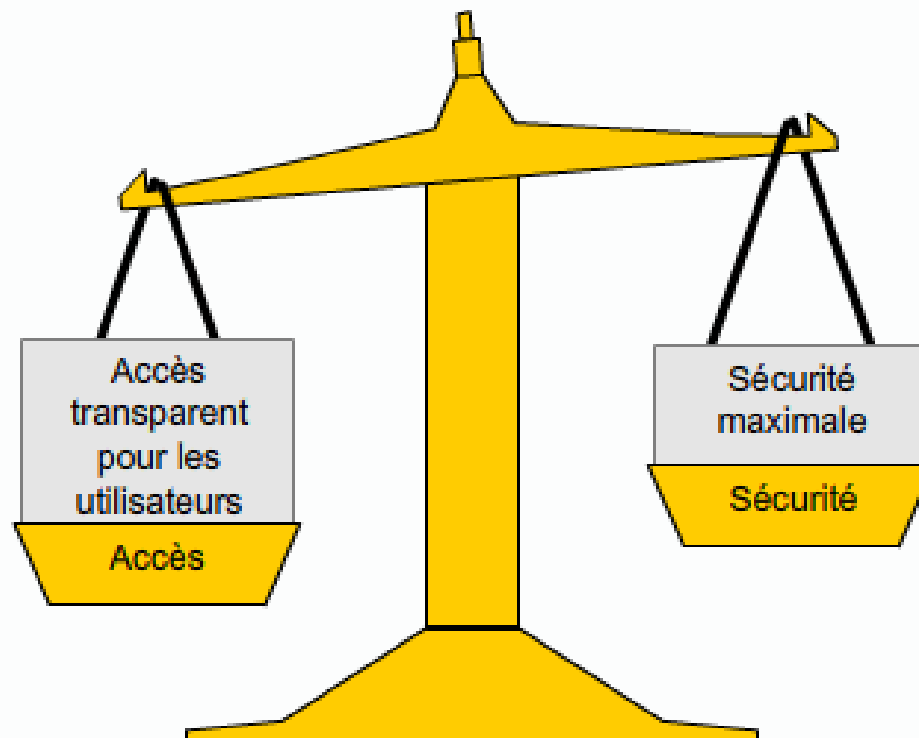
- 
1. *What do you have that others want?*
2. *What processes, data, or information systems are critical to you, your company, or your organization?*
3. *What would stop your company or organization from doing business or fulfilling its mission?*

# Réseaux ouverts et réseaux fermés

- Le défi de sécurité global auquel les administrateurs réseau doivent faire face est de trouver un juste équilibre entre deux exigences importantes :  
garder une certaine ouverture pour permettre la prise en charge des opportunités de commerce évolutives et protéger les données privées et personnelles, ainsi que les données stratégiques des entreprises.



# Réseau ouvert

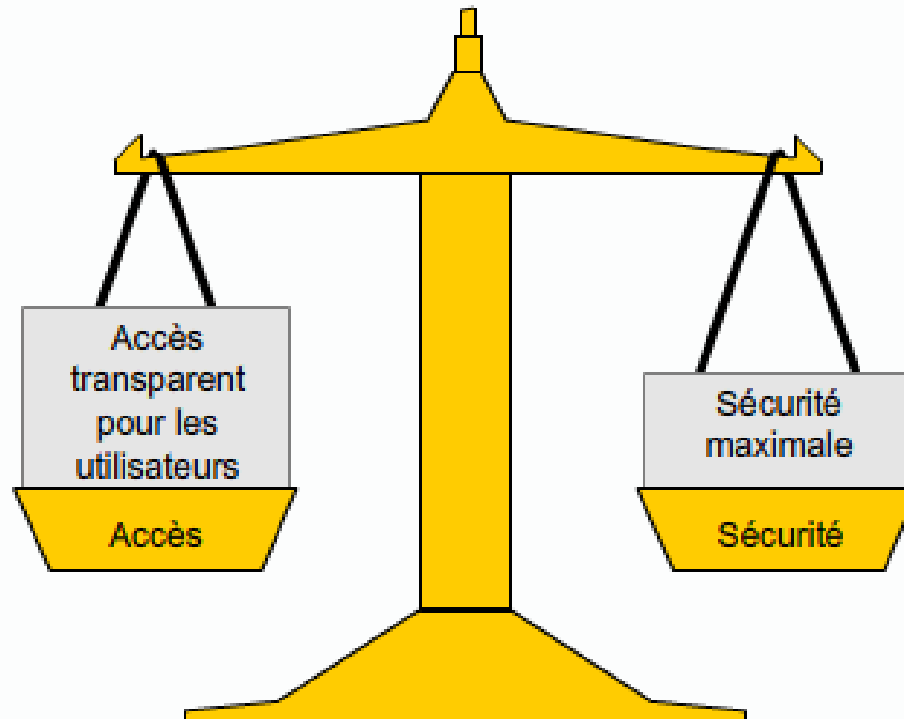


Permet tout ce qui n'est pas explicitement refusé :

- Facile à configurer et à gérer
- Accès facile des utilisateurs finaux aux ressources du réseau
- Frais de sécurisation les moins élevés



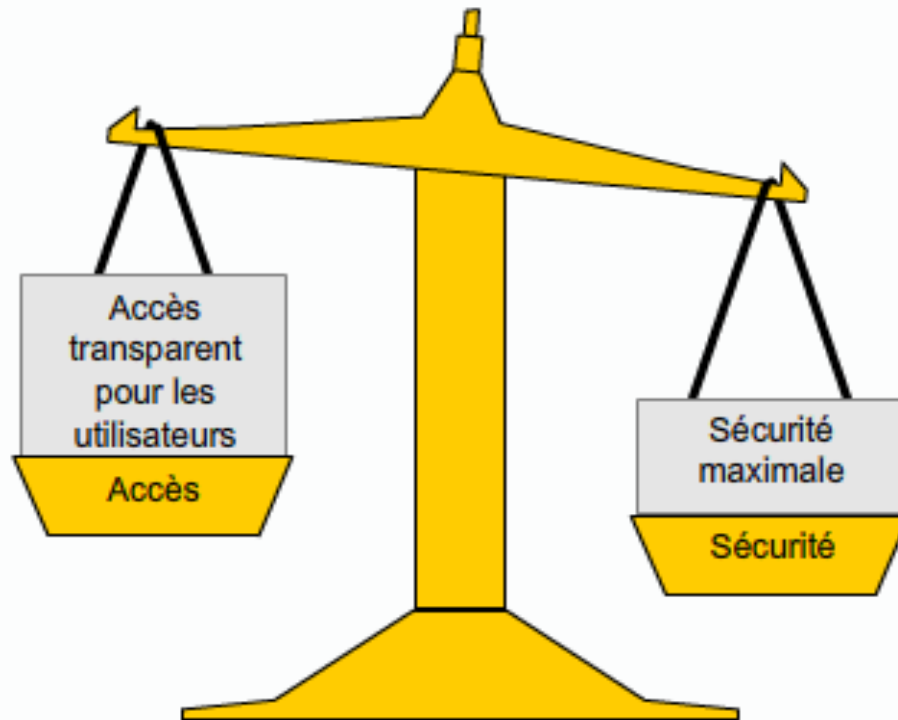
# Réseau restrictif



## Combinaison d'autorisations et de restrictions spécifiques :

- Plus difficile à configurer et à gérer
- Accès plus difficile des utilisateurs finaux aux ressources du réseau
- Frais de sécurisation plus élevés

# Réseau fermé



Tout ce qui n'est pas explicitement autorisé est refusé :

- Le plus difficile à configurer et à gérer
- Accès le plus difficile aux ressources du réseau pour les utilisateurs finaux
- Frais de sécurisation les plus élevés

# Développement d'une stratégie de sécurité

- La première étape qu'une organisation devrait entreprendre pour se prémunir et protéger ses données contre les risques consiste à développer une stratégie de sécurité.
- Une stratégie est un ensemble de principes qui guident les prises de décision et permettent aux dirigeants d'une organisation de déléguer l'autorité en toute confiance.
- Le document RFC2196 stipule « **qu'une stratégie de sécurité est une déclaration formelle des règles qui doivent être respectées par les personnes qui ont accès aux ressources technologiques et aux données vitales de l'entreprise** ».

# Développement d'une stratégie de sécurité

- Une stratégie de sécurité peut se présenter comme de simples règles du bon usage des ressources du réseau ou, à l'inverse, comprendre des centaines de pages et détailler chaque élément de connectivité et les règles correspondantes.
- Une stratégie de sécurité vise les buts suivants :
  - informer les utilisateurs, le personnel et les responsables de leur obligation de protéger les données vitales et les ressources technologiques de l'entreprise ;
  - spécifier les mécanismes permettant de respecter ces exigences ;
  - fournir une base de référence à partir de laquelle acquérir, configurer et auditer les systèmes informatiques pour qu'ils soient conformes à la stratégie.

# Constitution d'une stratégie de sécurité

- La norme ISO/CEI 27002 doit servir de base commune et de ligne directrice pratique pour élaborer les référentiels de sécurité de l'organisation et les pratiques efficaces de gestion de la sécurité.
- Ce document comprend les 12 sections suivantes :

Évaluation des risques

Stratégie de sécurité

Organisation de la sécurité des informations

Gestion des biens

Sécurité liée aux ressources humaines

Sécurité physique et environnementale

Gestion opérationnelle et gestion des communications

Contrôle d'accès

Acquisition, développement et maintenance des systèmes d'information

Gestion des incidents liés à la sécurité des informations

Gestion de la continuité de l'activité

Conformité

# Exemple de règles d'une stratégie de sécurité

- **Matériel, périphériques et équipement divers :**

Fournir une alimentation électrique continue aux équipements critiques.

Utiliser des modems PSTN/ISDN ou des lignes DSL avec précaution:

Contrôler l'infrastructure d'interconnexion informatique (câblage réseau).

Supprimer les données sur les matériels obsolètes qui ne sont plus utilisés.

Verrouiller chaque station de travail (par exemple via un écran de veille avec verrou) lorsque son utilisateur n'est pas à son poste.

# Exemple de règles d'une stratégie de sécurité ( Suite )

- Travail en dehors de locaux de l'organisation et utilisation de personnel externe :

Définir correctement le cadre associé à la mission d'un prestataire de services informatiques externe.

Sensibiliser le personnel quant aux risques liés à l'utilisation d'ordinateurs portables par le personnel.

Sensibiliser le personnel quant aux risques liés à l'utilisation d'un accès distant (VPN, télétravail, etc.).

# Exemple de règles d'une stratégie de sécurité ( Suite )

- Contrôle de l'accès aux systèmes d'information et aux contenus qui y sont présents

Mettre en place une méthode d'authentification uniforme, maîtrisée et gérée de manière centralisée.

Classifier chaque information mise à disposition sur l'infrastructure informatique et l'associer à des profils d'utilisation.

Interdire aux utilisateurs "standards" de s'identifier sur leur poste de travail en utilisant un compte d'administrateur local ou réseau.

Définir une politique de sélection de mot de passe pour les comptes informatiques.

Placer les systèmes informatiques sensibles (serveur, router, commutateur, etc.) dans des locaux à accès restreint.



# Exemple de règles d'une stratégie de sécurité ( Suite )

- **Traitement de l'information**

Réserver l'installation et la gestion de l'infrastructure réseau à du personnel qualifié.

Réserver tous les actes d'administration système à du personnel qualifié.

# Exemple de règles d'une stratégie de sécurité ( Suite )

- **Messagerie électronique et accès Internet/Intranet/Extranet**

Soumettre tout mail (entrant et sortant) et tout document téléchargé à partir d'une source non fiable (Internet par exemple) à une détection des virus et code malicieux.

Utiliser des outils de confidentialité pour l'échange de courriers électroniques concernant des informations sensibles.

Mettre en place un firewall.

Traiter avec précaution tout courrier électronique non sollicité.

Tout document reçu depuis une source non identifiée doit être considéré comme suspect et immédiatement supprimé.

Vérifier les adresses de destinations lors de l'envoi ou du suivi d'un courrier électronique.

Envoyer avec discernement les courriers électroniques dont la taille est imposante (plusieurs Mb).

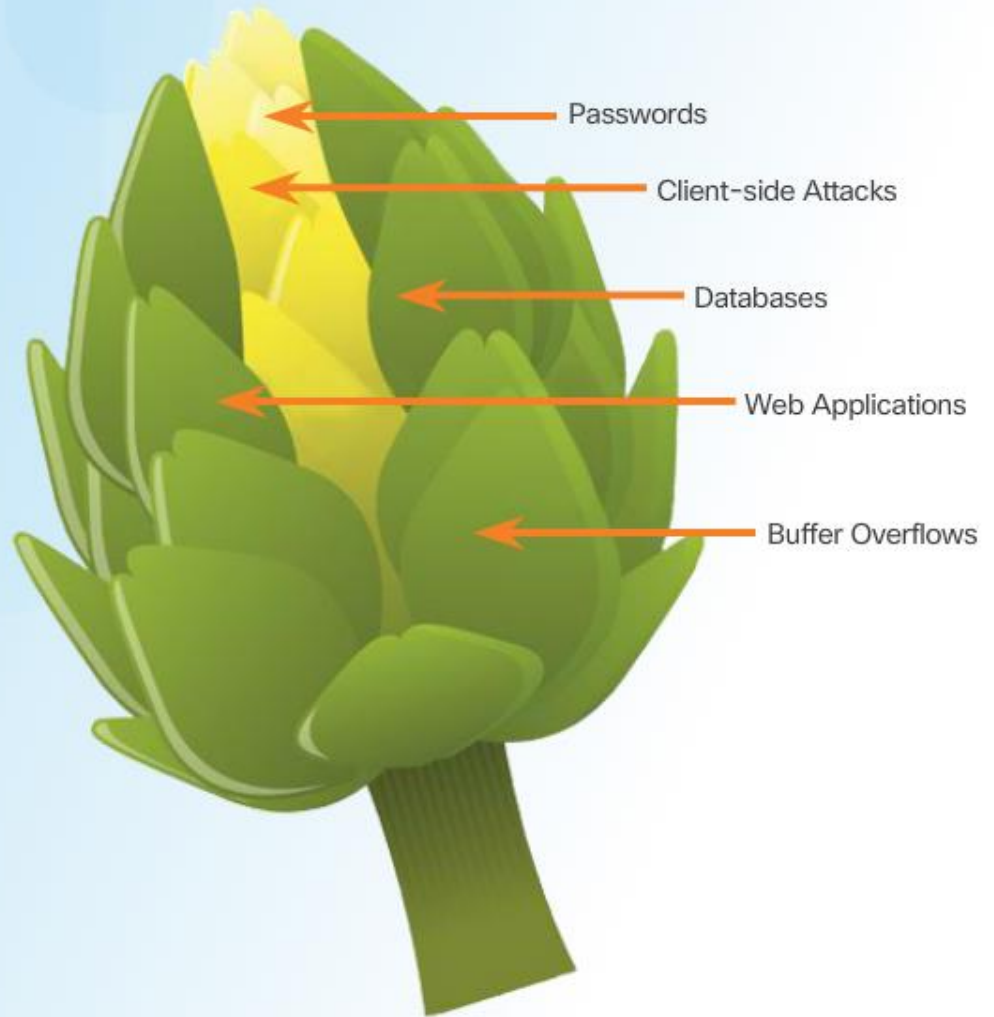
## Rubrique 1.3.3 : Introduction à l'Architecture de SecureX Cisco



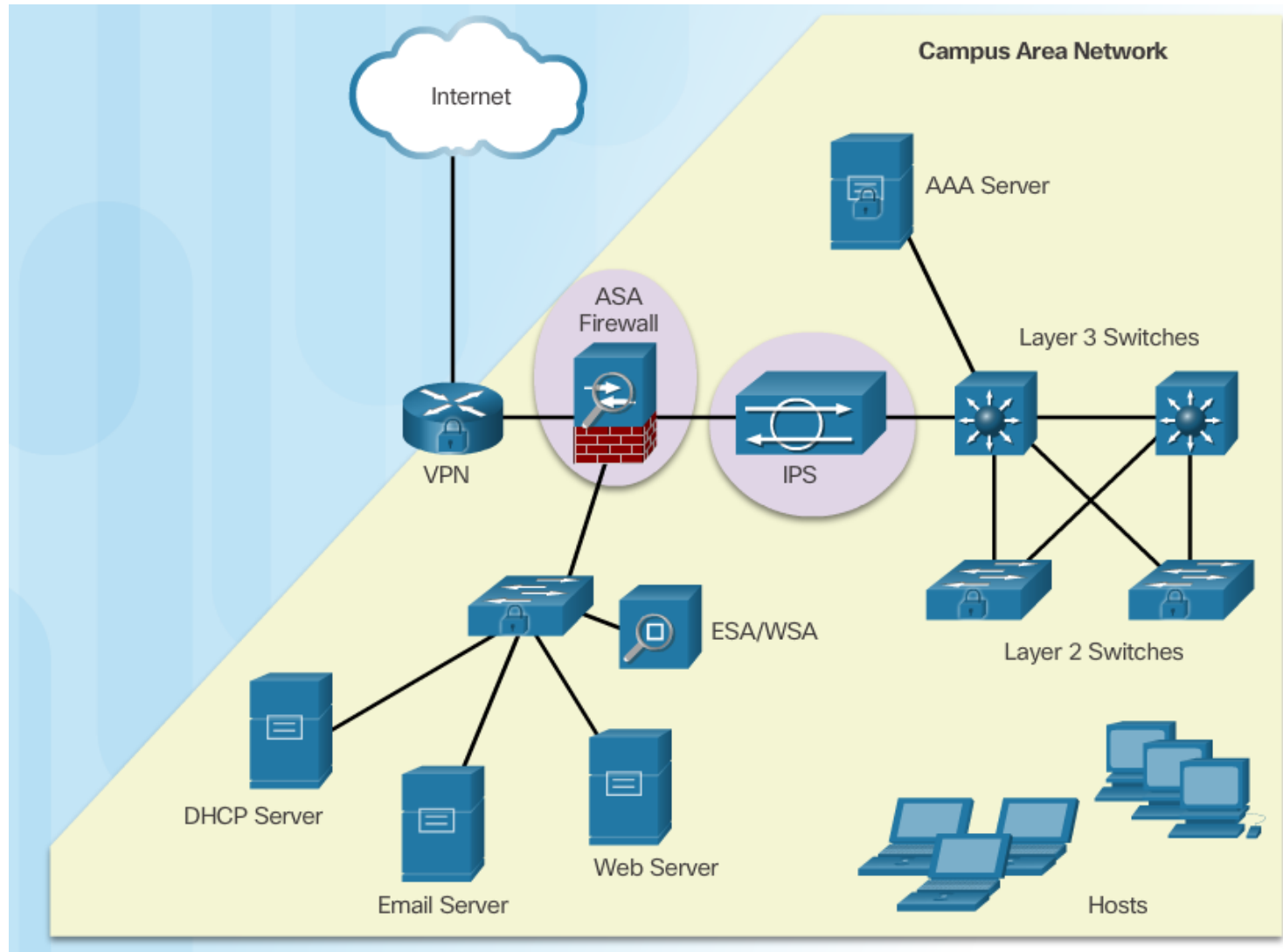
# L'Artichaut de sécurité

## The Artichoke of Attack

Modern hackers chip away at the hard-core exterior along the perimeter of the network to get to the heart of the enterprise. They remove certain "leaves" to reveal sensitive data that is either unprotected, or secured by weak defenses, such as easy-to-crack passwords and IDs.



# Évolution des outils de sécurité réseau



# Familles de produits SecureX



# Technologie de sécurité SecureX

## Architecture Cisco SecureX:

- Moteurs de balayage
- Mécanismes de livraison
- Opérations de renseignement de sécurité (SIO)
- Consoles de gestion des politiques
- Point final de la prochaine génération

# Élément de numérisation réseau centralisé et contextuel

Définit les stratégies de sécurité basées sur cinq paramètres:

- Type d'appareil utilisé pour l'accès
- Identité de la personne
- Application en cours d'utilisation
- Emplacement
- Heure d'accès





# Opérations de renseignement de sécurité Cisco



# Opérations de renseignement de sécurité Cisco



## Rubrique 1.3.4 : Atténuer les menaces modernes de réseau

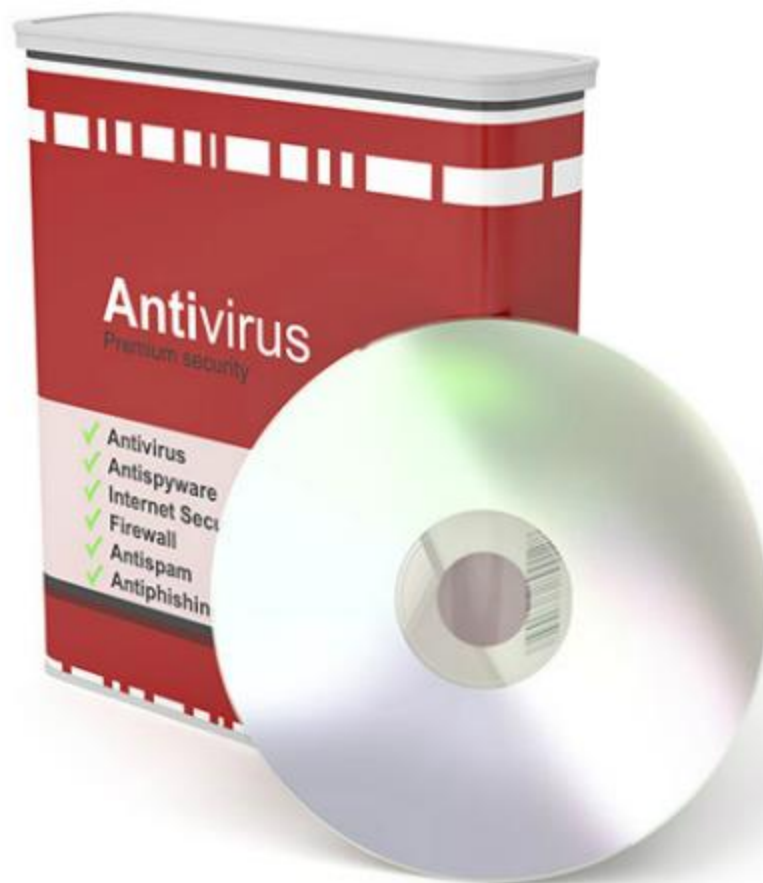


# Défendre le réseau

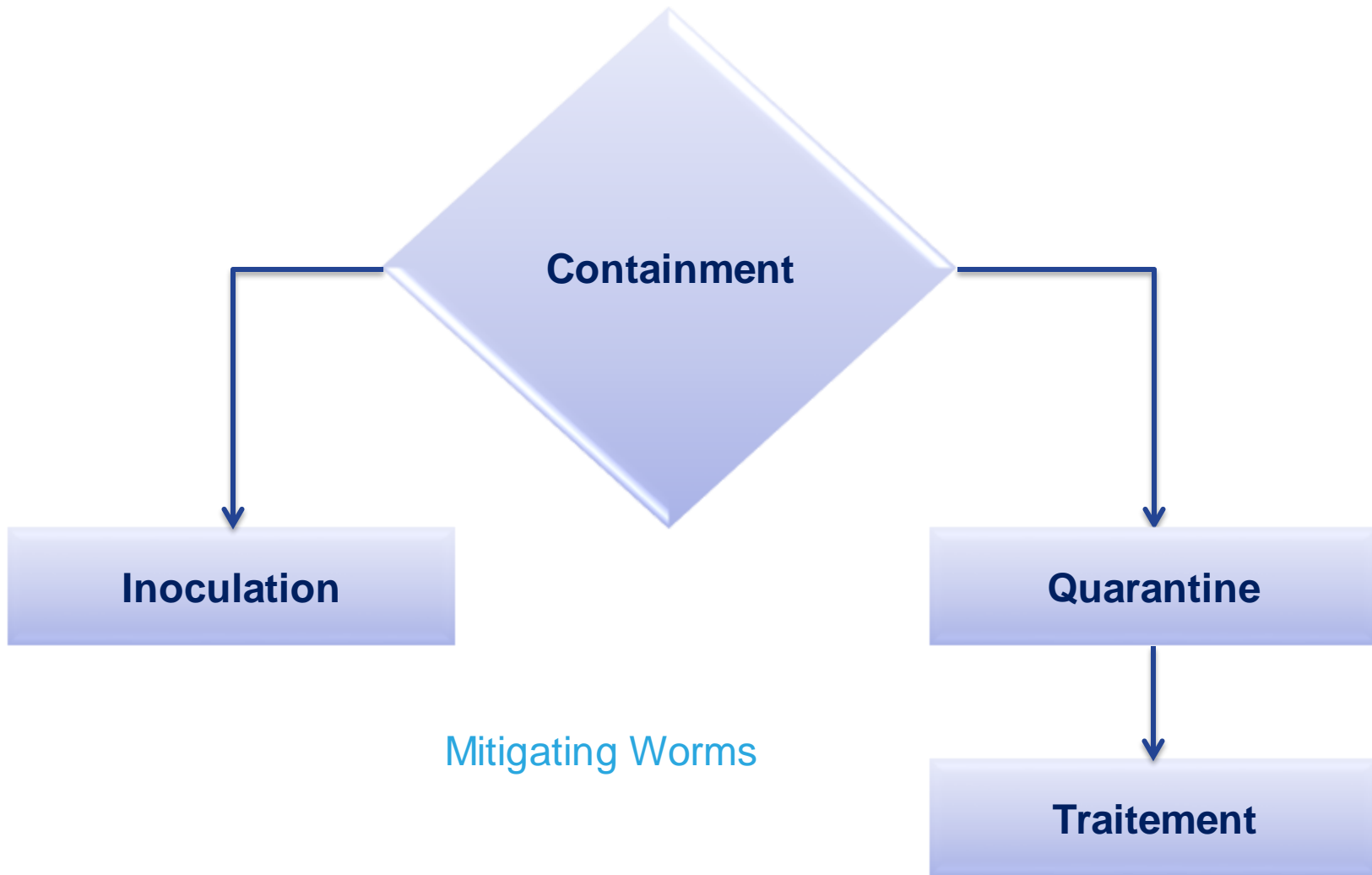
## Meilleures pratiques :

- Développer une politique de sécurité écrites.
- Sensibiliser les employés aux risques d'ingénierie sociale et élaborer des stratégies pour valider les identités par téléphone, par courriel ou en personne. Contrôler l'accès physique aux systèmes. Control physical access to systems.
- Utilisez des mots de passe forts et changez-les souvent
- Crypter et protéger les données sensibles.
- Implémenter la sécurité matérielle et logicielle.
- Effectuer des sauvegardes et tester la sauvegarde des fichiers sur une base régulière.
- Fermer les ports et les services inutiles.
- Maintenir correctifs à jour en installant les hebdomadaires ou quotidiennes pour empêcher les attaques par buffer overflow et privilège escalade.
- Effectuer des audits de sécurité pour tester le réseau.

# Atténuer les Malwares



# Atténuer les vers




# Atténuation des attaques de reconnaissance



Reconnaissance Attack Mitigation Techniques include:

- Implement authentication to ensure proper access.
- Use encryption to render packet sniffer attacks useless.
- Use anti-sniffer tools to detect packet sniffer attacks.
- Implement a switched infrastructure.
- Use a firewall and IPS.

# Atténuation des attaques d'accès



THINK

Using a password based on a dictionary word may result in someone abusing your account and misusing our server.

- Strong password security
- Principle of minimum trust
- Cryptography
- Applying operating system and application patches



# Atténuation des attaques DoS

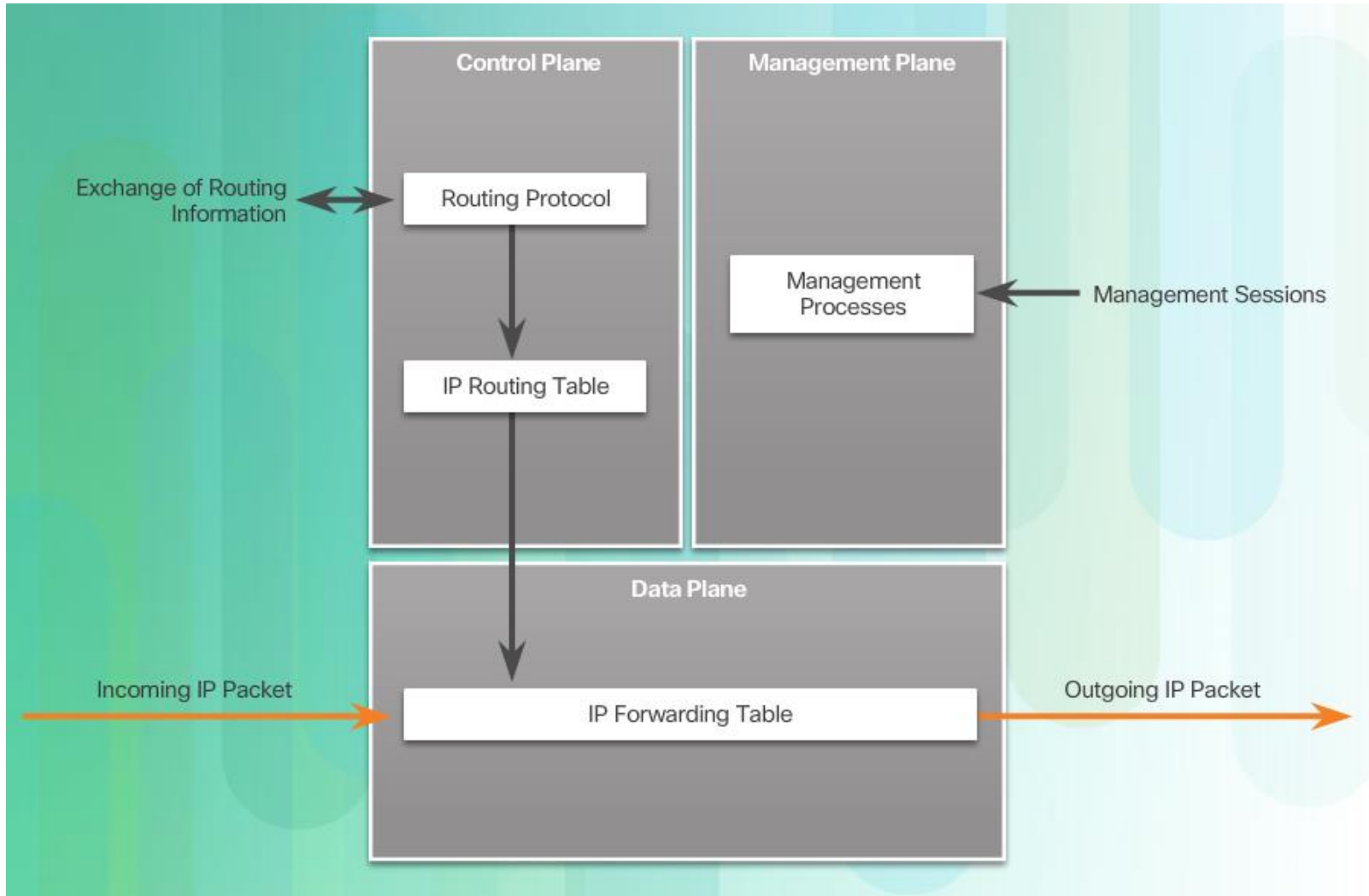


- IPS and firewalls (Cisco ASAs and ISRs)
- Antispoofing technologies
- Quality of Service-traffic policing

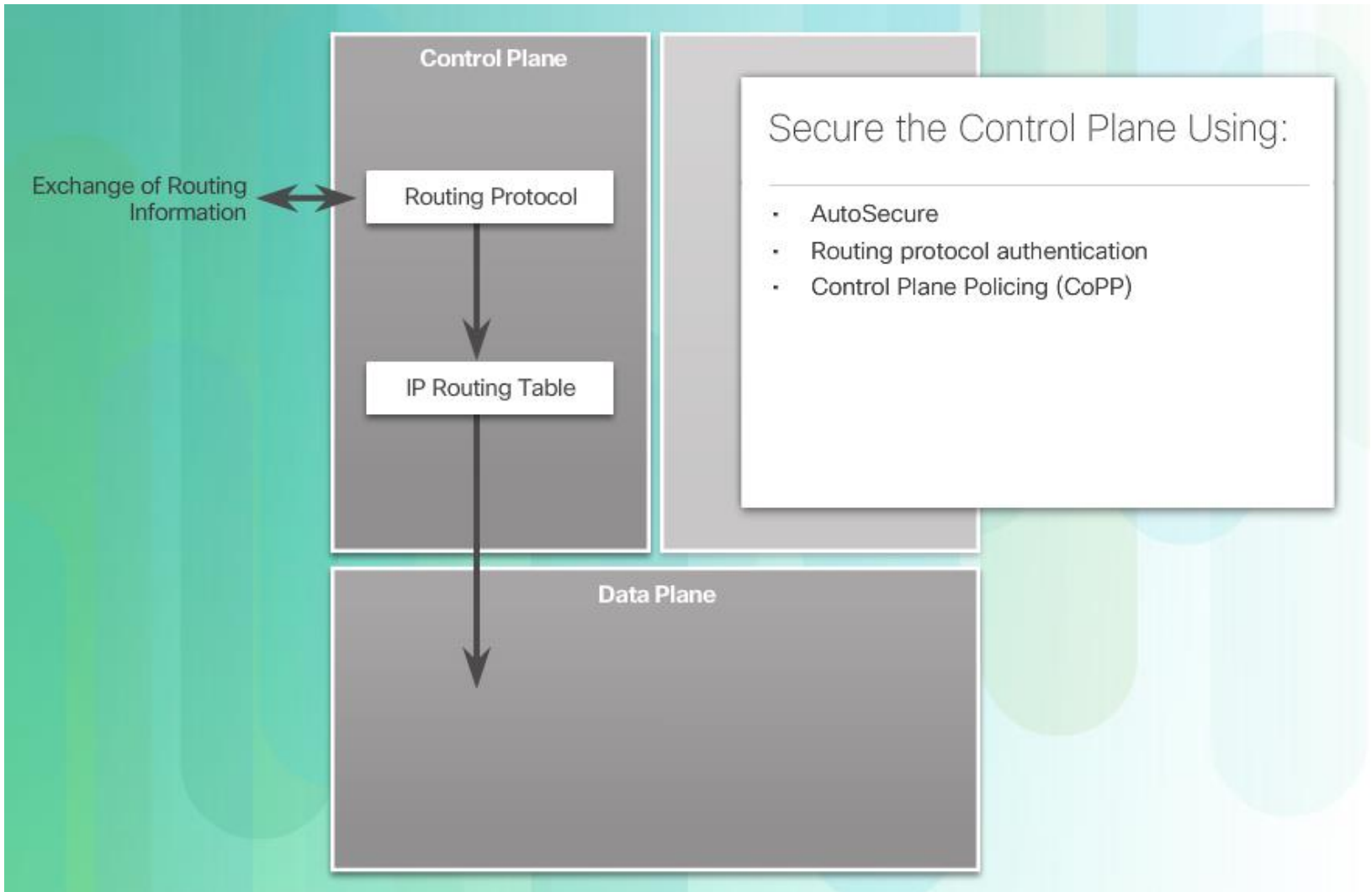
# Sujet 1.3.5: Framework de protection de Cisco Network Foundation



# NFP Framework



# Sécurisation du plan de contrôle



# Sécurisation du plan de gestion

## Secure the Management Plane By:

- Enabling login and password policy
- Presenting legal notification
- Ensuring the confidentiality of data using SSH and HTTPS
- Enabling role-based access control
- Authorizing actions
- Enabling management access reporting

Management Plane

Management Processes

Management Sessions

# Sécurisation du plan de données



# Section 1.4:

## Sommaire

Objectifs du chapitre :

- Expliquer la sécurité réseau.
- Décrire les différents types de menaces et d'attaques.
- Expliquer les outils et procédures visant à atténuer les effets des programmes malveillants et les attaques de réseau commun.

Thank you.



Cisco Networking Academy  
Mind Wide Open



# Les ressources d'instructeur

- N'oubliez pas, tutoriels utiles et guides de l'utilisateur sont disponibles via votre page d'accueil de NetSpace.  
(<https://www.netacad.com>)
- Ces ressources couvrent un éventail de sujets, y compris la navigation, les évaluations et les affectations.
- Une capture d'écran a été apportée ici mettant en évidence les tutoriels liés à l'activation des examens, gestion des évaluations et la création de quiz.

