

Chapitre 5 : Infrastructure réseau

BENJAMIN
DESROSIERS-BOSSÉ

2023

Chapitre 12 - Sections et objectifs

Les appareils de communication réseau

- Expliquer comment les périphériques réseau assurent les communications réseau filaires et sans fil.
- Expliquer comment les périphériques réseau assurent les communications réseau.
- Expliquer comment les périphériques réseau sans fil assurent les communications réseau.

L'infrastructure de sécurité du réseau

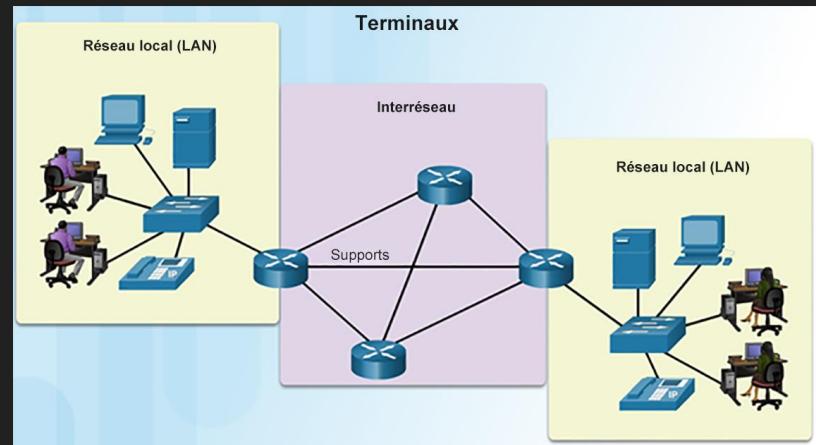
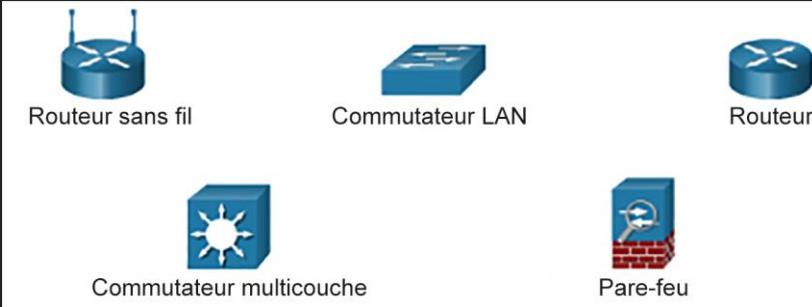
- Expliquer comment les périphériques et les services renforcent la sécurité du réseau.
- Expliquer comment les périphériques spécialisés renforcent la sécurité du réseau.
- Expliquez comment les services réseau renforcent la sécurité du réseau.

Représentation du réseau

- Expliquer comment les réseaux et les topologies réseau sont représentés.
- Expliquer comment les conceptions réseau sont représentées par des symboles interconnectés.

Pérophériques de communication réseau





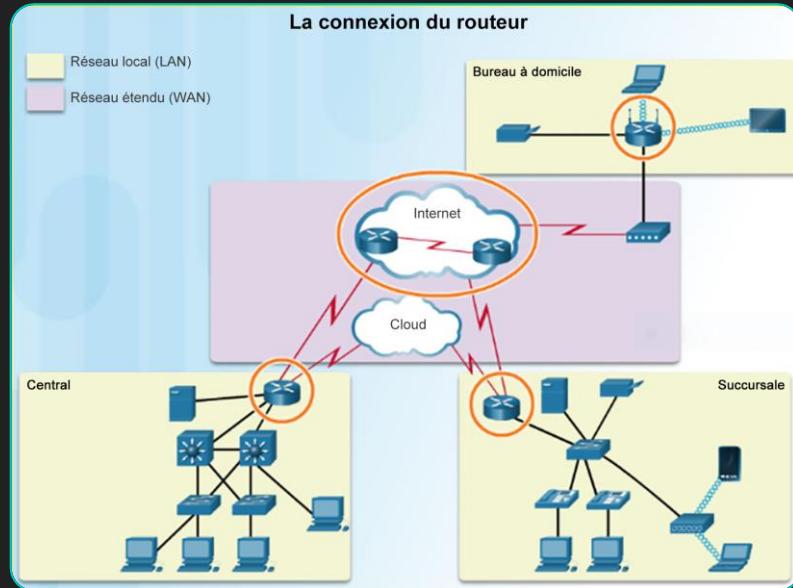
Périphériques réseau Terminaux

- Terminaux :
 - Ordinateurs, ordinateurs portables, serveurs, imprimantes, appareils intelligents et terminaux mobiles.
 - Chaque terminal est connecté au réseau via des appareils intermédiaires.
- Périphériques intermédiaires :
 - Ils connectent chaque appareil au réseau et peuvent connecter plusieurs réseaux individuels afin de former un interréseau.
 - Ils assurent la connectivité et les flux de données sur tout le réseau.

Périphériques réseau

Routeurs

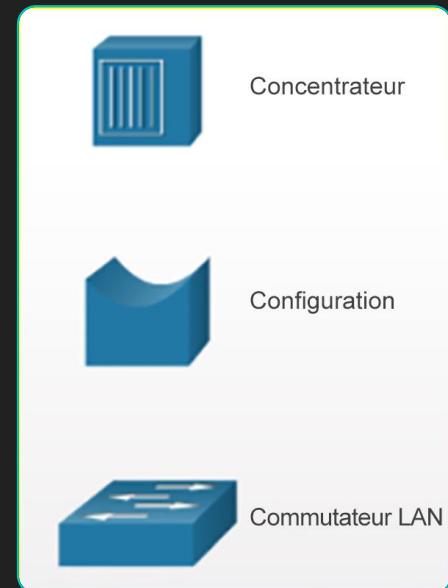
- Fonction d'un routeur :
 - Chargé de déterminer le chemin d'accès et de transférer les paquets.
 - Il est responsable de l'encapsulation et de la désencapsulation des paquets.
 - Il utilise une table de routage pour déterminer le meilleur chemin à emprunter pour envoyer des paquets à un réseau spécifique.
- Table de routage :
 - Il contient les routes connectées directement et les routes distantes.
 - Le routeur recherche dans sa table de routage une adresse réseau qui correspond à l'adresse IP de destination du paquet.
 - Utilise la passerelle de dernier recours si elle a été intégrée ou configurée ; dans le cas contraire, le paquet est rejeté.

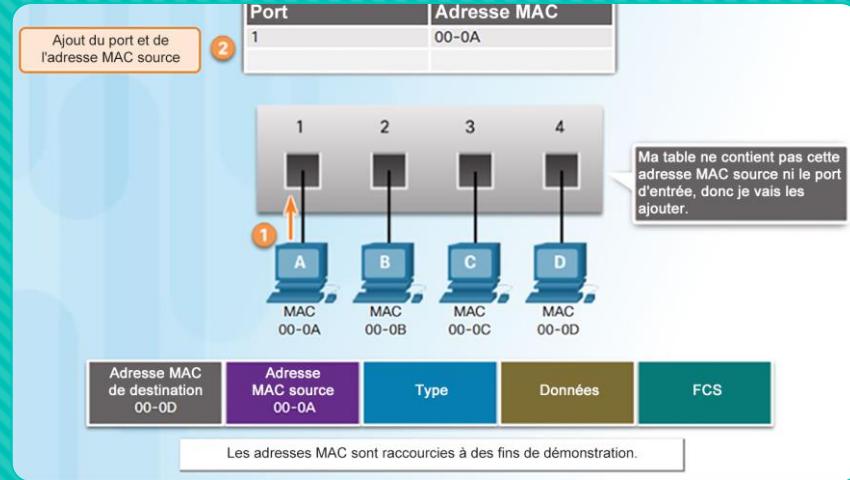
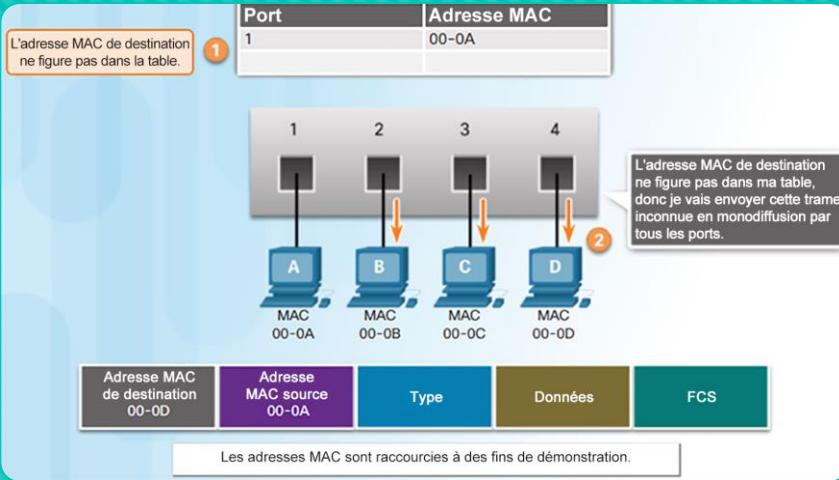


Périphériques réseau

Concentrateurs, ponts, commutateurs de réseau local

- Un concentrateur Ethernet agit comme un répéteur multiport qui reçoit un signal électrique entrant (données) sur un port. Il transmet ensuite immédiatement un signal régénéré sur tous les autres ports. Les concentrateurs utilisent le traitement de la couche physique pour transférer les données.
- Les ponts ont deux interfaces et sont connectés entre les concentrateurs afin de diviser le réseau en plusieurs domaines de collision. Chaque domaine de collision ne peut avoir qu'un seul expéditeur à la fois.
- Les commutateurs de réseau local sont essentiellement des ponts multiports qui relient les périphériques dans une topologie en étoile. Comme les ponts, les commutateurs segmentent un réseau local en domaines de collision distincts, à raison d'un pour chaque port du commutateur. Un commutateur décide du réacheminement des données sur la base des adresses MAC Ethernet.



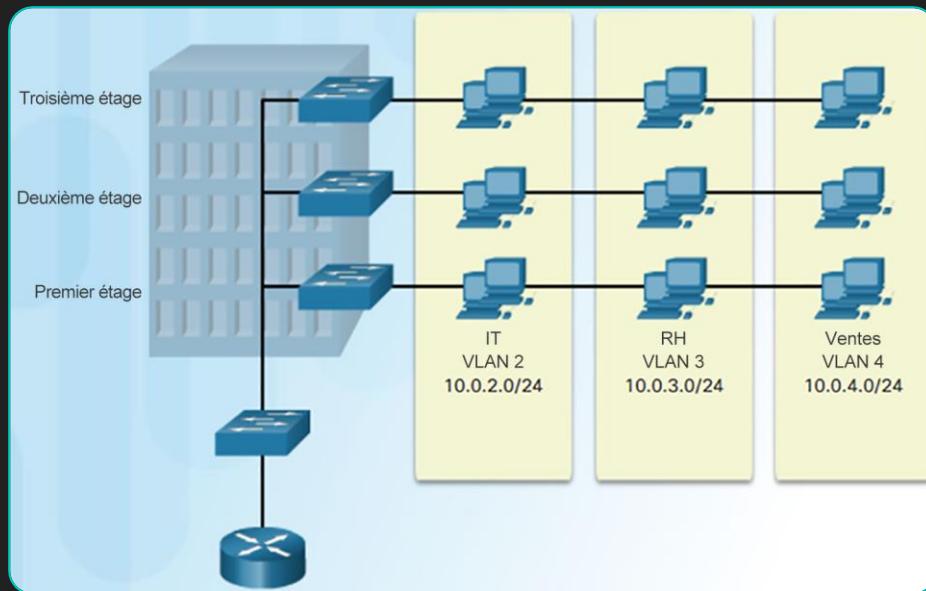


Périphériques réseau Fonctionnement de la commutation

Périphériques réseau VLAN

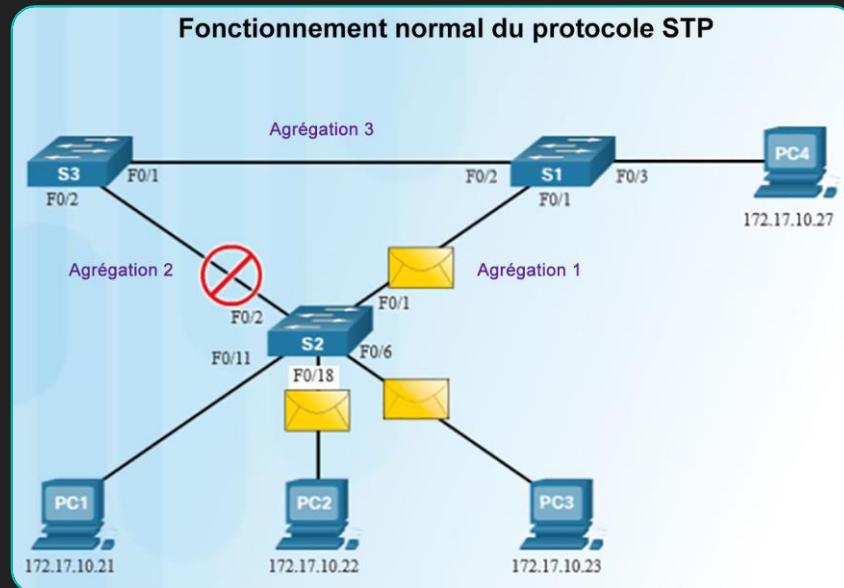
- Segmente les réseaux d'après plusieurs facteurs (fonction, équipe de projet ou application), quel que soit leur emplacement physique.
- Crée des domaines de diffusion logiques qui peuvent s'étendre sur plusieurs segments de réseau local physique.
- Améliore les performances réseau en divisant de vastes domaines de diffusion en domaines plus petits.
- Empêche les utilisateurs situés sur des VLAN différents de s'espionner mutuellement.

Pourquoi on crée des Vlans? Quelle est la meilleure stratégie selon-vous?



Périphériques réseau STP

- Protocole STP (Spanning Tree Protocol)
 - Garantit la présence d'un seul chemin logique entre toutes les destinations sur le réseau en bloquant les chemins redondants.
 - Empêche les boucles en utilisant des ports bloqués stratégiquement placés.
 - Utilise des trames d'unité BDPU (Bridged Protocol Data Unit) pour empêcher la formation de boucles.

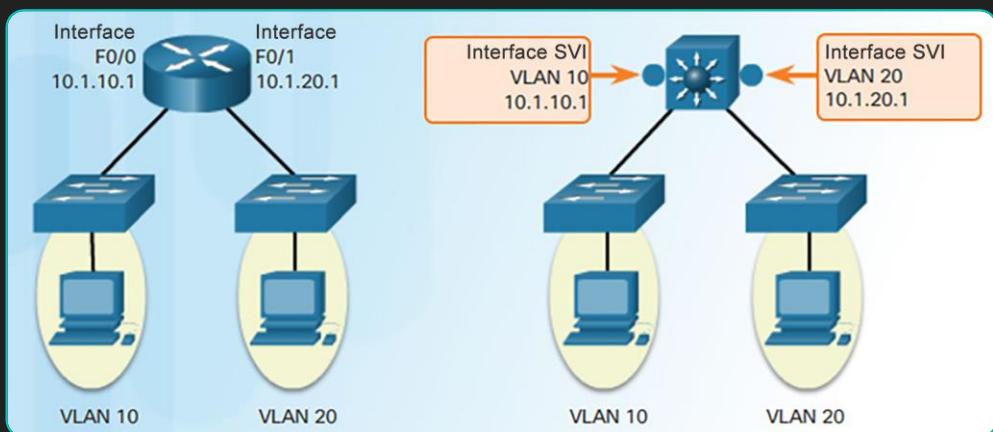


Périphériques réseau

Commutation multicouche

- Les commutateurs multicouches prennent en charge les ports routés et les interfaces virtuelles commutées pour transmettre des trames en fonction des informations de couche 3.
 - Ports routés** : le port physique se comporte comme une interface sur un routeur, il n'est associé à aucun VLAN.
 - Interface SVI** : l'interface virtuelle peut être configurée pour n'importe quel VLAN au sein d'un commutateur multicouche.

Pourquoi on utilise des routeurs si on a des commutateurs multicouches?



Communications sans fil

Protocoles et fonctions

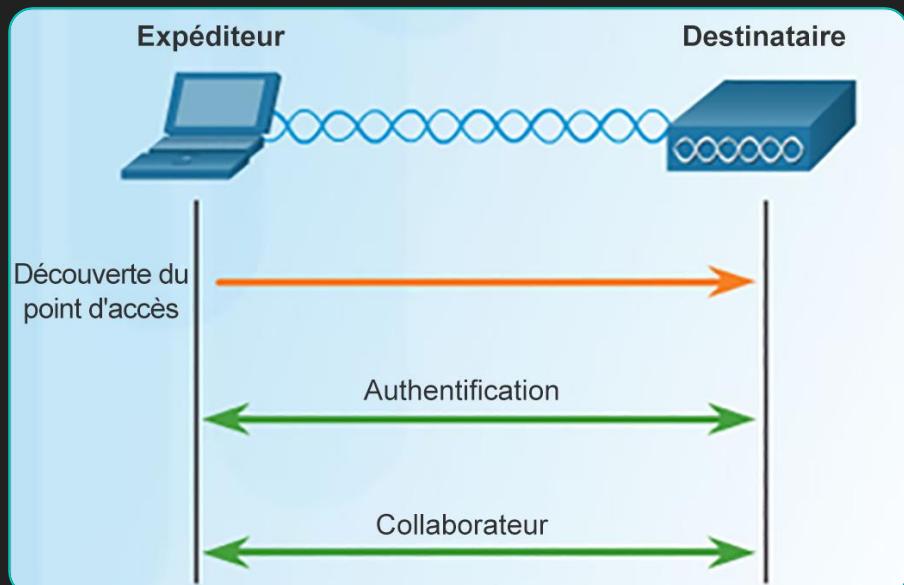
- LAN sans fil (WLAN) :
 - Ils utilisent des fréquences radio au lieu de câbles au niveau de la couche physique et de la sous-couche MAC de la couche liaison de données.
 - Ils connectent des clients au réseau via un point d'accès sans fil ou un routeur sans fil, au lieu d'un commutateur Ethernet.

Caractéristique	Réseau local sans fil 802.11	Réseaux locaux Ethernet 802.3
Couche physique	fréquence radio ou radiofréquence (RF)	Câble
Accès aux supports	Évitement de collision	Détection de collisions
Disponibilité	Quiconque est équipé d'une carte réseau radio à portée d'émission d'un point d'accès	Connexion par câble requise
Interfaces de signalisation	Oui	Sans conséquence
Réglementation	Réglementation supplémentaire par les autorités nationales	Norme IEEE

Communications sans fil

Fonctionnement des réseaux sans fil

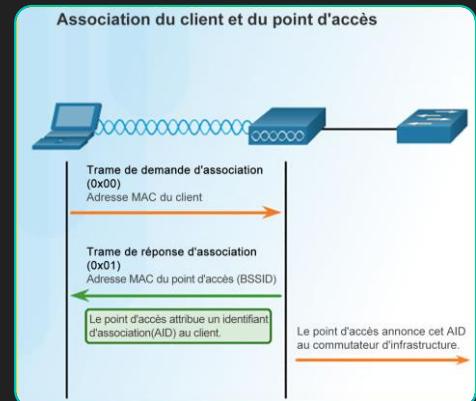
- Le processus d'associations de clients sans fil avec point d'accès inclut la découverte d'un nouveau point d'accès, l'authentification avec ce point d'accès, puis l'association à ce point d'accès.
- Les paramètres sans fil communs configurables incluent :
 - Mode réseau
 - SSID
 - Paramètres de canal
 - Mode de sécurité
 - Gestion
 - Mot de passe
- Les périphériques sans fil doivent détecter un point d'accès ou un routeur sans fil et s'y connecter. Ce processus peut être passif ou actif.
- La norme 802.11 a été développée à l'origine avec deux mécanismes d'authentification : **l'authentification ouverte** fournit une connectivité sans fil à un périphérique sans fil et la technique **d'authentification à clé partagée** est basée sur une clé prépartagée entre le client et le point d'accès.



Communications sans fil

Processus d'association entre le client et le point d'accès

- Un client sans fil passe par un processus en trois étapes pour s'associer à un point d'accès.
- Découverte : un client sans fil localise le point d'accès à associer.
- Authentification :
 - Le client sans fil envoie une trame d'authentification au point d'accès.
 - Le point d'accès répond en envoyant un texte de sécurité.
 - Le client chiffre le message à l'aide de sa clé partagée et renvoie le texte chiffré au point d'accès.
 - Le point d'accès déchiffre le message à l'aide de sa clé partagée.
 - Si le texte chiffré correspond au texte de sécurité, le point d'accès authentifie le client.
- Association :
 - Le client sans fil envoie une trame de demande d'association contenant son adresse MAC.
 - Le point d'accès répond avec une réponse d'association, qui contient son adresse MAC.
 - Le point d'accès mappe un port logique au client sans fil.



Communications sans fil

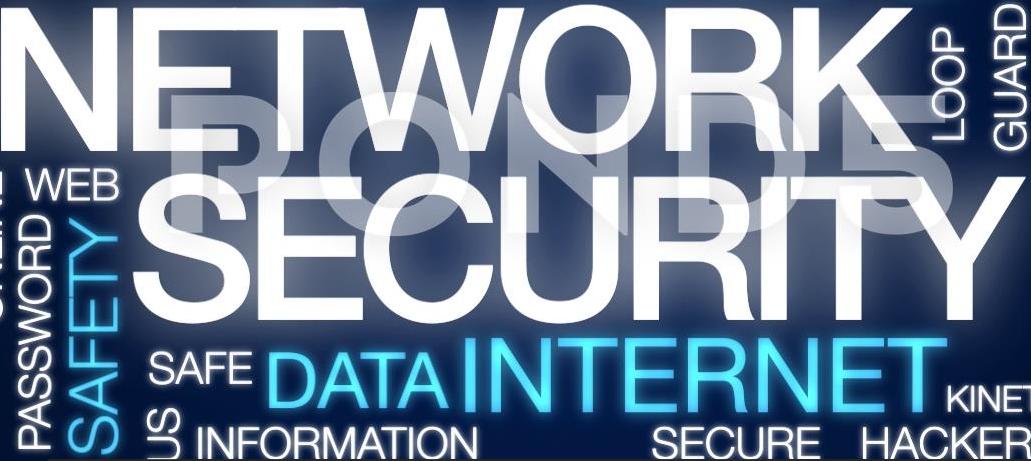
Périphériques sans fil – Point d'accès, LWAP, WLC

- Point d'accès :
 - **Réseau de petite taille** : généralement un routeur sans fil qui intègre les fonctions d'un routeur.
 - **Réseau de grande taille** : peut inclure de nombreux points d'accès.
- Contrôleur LAN sans fil (WLC) :
 - Contrôle et gère les fonctions des points d'accès sur un réseau.
 - Simplifie la configuration et la surveillance de nombreux points d'accès.
- Lightweight AP (LWAP) :
 - Gestion centralisée de WLC.
 - N'agit plus de façon autonome.



[Comment fonctionne le Wifi au collège vs à la maison?](#)

PRIVACY SYSTEM CONCEPT ACCESS
PROTECT DIGITAL TECHNOLOGY
POLICY SECRECY KEYHOLE
SECURITY NETWORK GUARD
UNLOCK CONNECTION LOOP
DISPLAY BINARY COMPUTER SCREEN
CRIME ONLINE MODERN FIREWALL
PASSWORD WEB BUSINESS SOFTWARE
SAFETY US INFORMATION SECURE KINETIC
SAFE DATA INTERNET HACKER

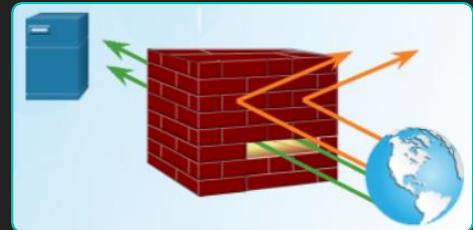


L'infrastructure de sécurité du réseau

Périphériques de sécurité

Pare-feu

- Voici certaines propriétés que partagent les pare-feu :
 - Les pare-feu résistent aux attaques réseau.
 - Tout le trafic traverse le pare-feu.
 - Les pare-feu appliquent la politique de contrôle d'accès.
- Il existe plusieurs avantages à utiliser un pare-feu dans un réseau :
 - Il empêche les utilisateurs non fiables d'accéder aux hôtes, aux ressources et aux applications sensibles.
 - Assainit le flux de protocoles.
 - Il bloque les données malveillantes provenant des serveurs et des clients.
 - Il simplifie la gestion de la sécurité.
- Les pare-feu présentent également certaines limites :
 - Un pare-feu mal configuré peut avoir des conséquences graves pour le réseau.
 - Les données de nombreuses applications ne peuvent pas traverser les pare-feu en toute sécurité.
 - Les utilisateurs recherchent des moyens de contourner le pare-feu afin de recevoir des documents bloqués.
 - Les performances du réseau peuvent baisser.
 - Le trafic non autorisé peut être tunnellié comme trafic légitime à travers le pare-feu.



Périphériques de sécurité

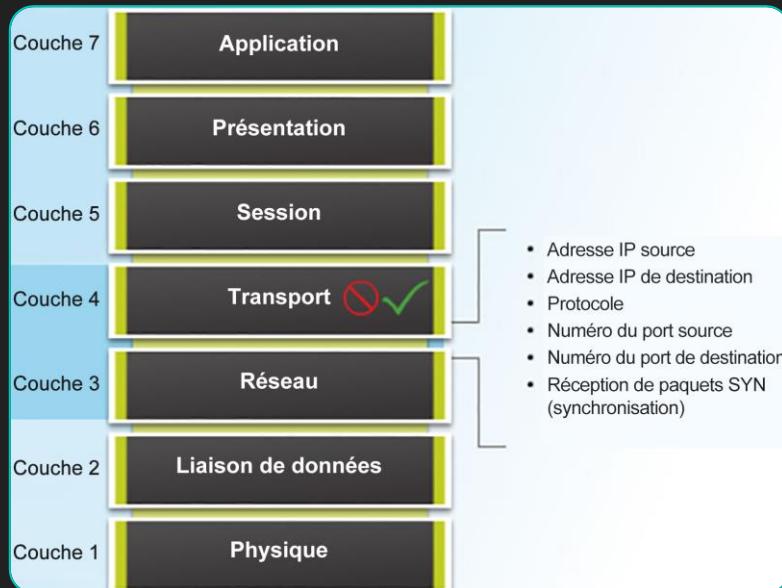
Description des types de pare-feu

- **Pare-feu de filtrage de paquets (sans état)** : font généralement partie d'un pare-feu de routeur, qui autorise ou interdit le trafic en fonction des informations des couches 3 et 4.
- **Pare-feu stateful** :
 - Autorise ou bloque le trafic en fonction de l'état, du port et du protocole.
 - Il surveille toute l'activité, de l'ouverture d'une connexion jusqu'à sa fermeture.
- **Pare-feu de la passerelle d'applications (pare-feu proxy)** : filtre les informations au niveau des couches 3, 4, 5 et 7 du modèle de référence OSI.
- **Pare-feu d'hôte (serveur et personnel)** : un PC ou serveur sur lequel s'exécute le logiciel de pare-feu.
- **Pare-feu transparent** : filtre le trafic IP entre une paire d'interfaces reliées par un pont.
- **Pare-feu hybride** : combinaison des divers types de pare-feu.

Périphériques de sécurité

Pare-feu de filtrage des paquets

- Généralement un composant d'un pare-feu de routeur, qui autorise ou interdit le trafic en fonction des informations des couches 3 et 4.
- Pare-feu « sans état » qui effectuent une recherche simple dans une table de politiques afin de filtrer le trafic en fonction de critères précis.



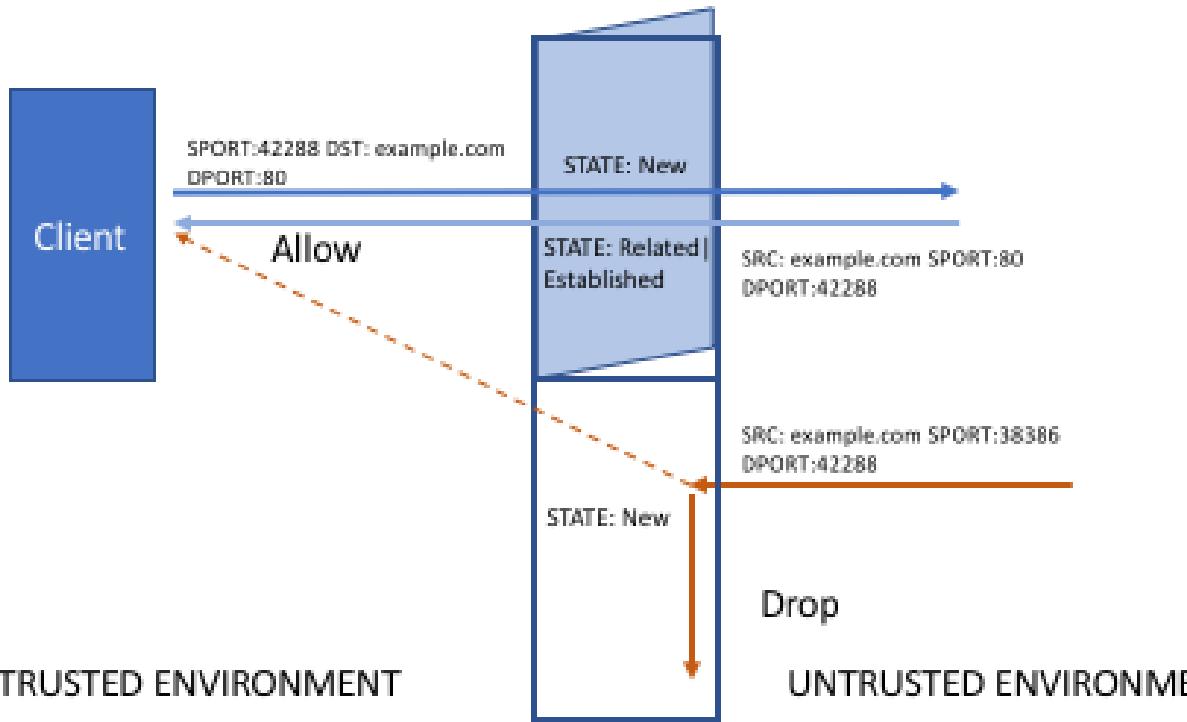
Périphériques de sécurité

Pare-feu avec état

- La technologie de pare-feu la plus polyvalente et la plus répandue.
- Ils effectuent un filtrage dynamique des paquets à l'aide des informations de connexion mises à jour dans une table d'états.
- Ils font partie de la couche réseau, mais ils analysent aussi le trafic au niveau des couches OSI 4 et 5.



Leave the door open for reply or established connection



Dispositifs de sécurité

Pare-feu nouvelle génération

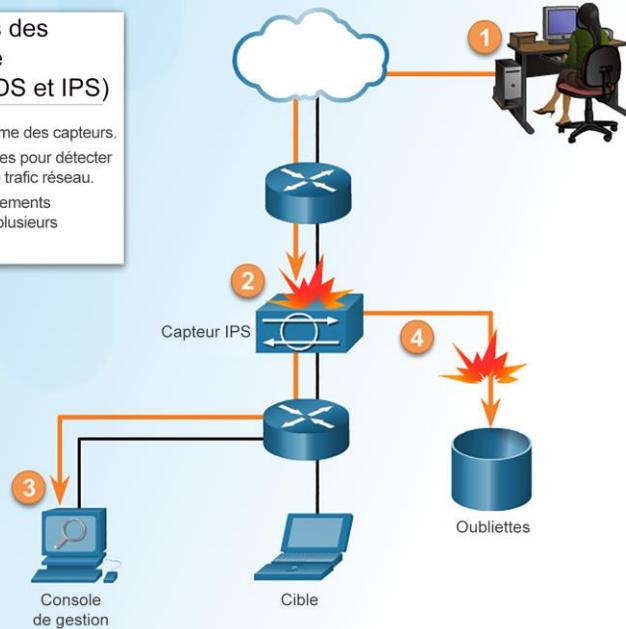
- Ils assurent les mêmes fonctions qu'un pare-feu standard telles que l'inspection « stateful ».
- Ils proposent des fonctions intégrées de prévention des intrusions.
- Ils tirent parti de la reconnaissance et du contrôle des applications pour détecter et bloquer celles qui présentent un risque.
- Ils fournissent des mises à niveau afin d'inclure les futurs flux d'informations.
- Ils implémentent des techniques pour faire face à l'évolution des menaces de sécurité.

Démo NGFW

- Tentez de visiter un site populaire qui devrait être bloquer. Que remarquez-vous?

Caractéristiques communes des systèmes de détection et de prévention des intrusions (IDS et IPS)

- Les deux solutions sont déployées comme des capteurs.
- Les deux solutions utilisent des signatures pour détecter les modèles d'utilisation abusive dans le trafic réseau.
- Les deux peuvent détecter des comportements atomiques (un paquet) ou composites (plusieurs paquets).

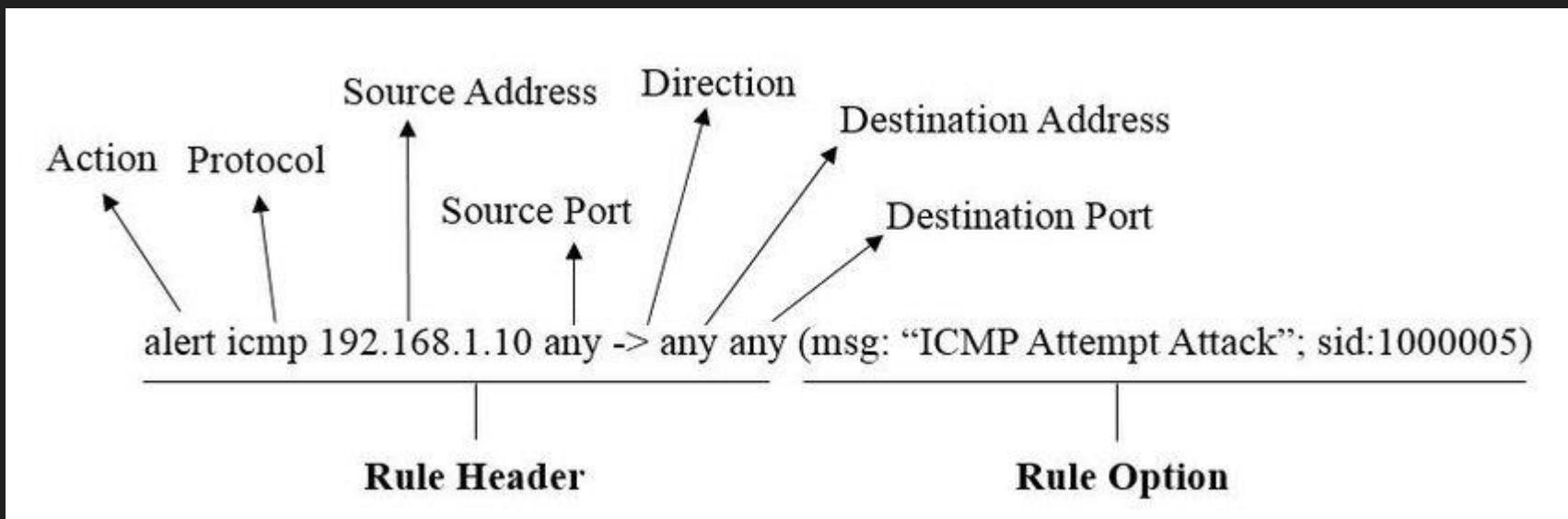


Dispositifs de sécurité Dispositifs de prévention et de détection des intrusions

Règle IPS/IDS (exemple)

```
alert tcp $HOME_NET 21 -> any any (msg:"FTP failed login"; content:"Login or password incorrect"; sid:1000003; rev:1;)
```

Ça ressemble à quelques chose de familier?



	Avantages	Inconvénients
IDS	<ul style="list-style-type: none"> ▪ Aucune incidence sur le réseau (latence, gigue) ▪ Aucune incidence sur le réseau en cas de panne du capteur ▪ Aucune incidence sur le réseau en cas de surcharge du capteur 	<ul style="list-style-type: none"> ▪ Les mesures d'intervention n'arrêtent pas les paquets déclencheurs ▪ Le bon réglage est requis pour les mesures d'intervention ▪ Plus vulnérable aux techniques de contournement des défenses du réseau
IPS	<ul style="list-style-type: none"> ▪ Arrête les paquets déclencheurs ▪ Peut utiliser des techniques de normalisation des flux 	<ul style="list-style-type: none"> ▪ Les problèmes de capteur peuvent avoir une incidence sur le trafic réseau ▪ La surcharge du capteur affecte le réseau ▪ Une certaine incidence sur le réseau (latence, gigue)

Dispositifs de sécurité Avantages et inconvénients d'IDS et IPS

Dispositifs de sécurité

Types d'IPS

- IPS basé sur l'hôte (HIPS) :
 - Logiciel installé sur un seul hôte pour surveiller et analyser toute activité suspecte.
 - Permet de surveiller et de protéger les processus du système d'exploitation et les processus système critiques qui sont propres à l'hôte concerné.
 - Combine logiciels antivirus, antimalware et pare-feu.
- IPS en réseau :
 - Peut être implémenté en utilisant un dispositif IPS dédié ou non.
 - Élément essentiel à la prévention des intrusions.
 - Les capteurs détectent en temps réel toute activité malveillante et non autorisée, et peuvent prendre des mesures si nécessaire.

	Avantages	Inconvénients
IPS basé sur l'hôte	<ul style="list-style-type: none">• Offre une protection spécifique à un système d'exploitation hôte• Offre une protection au niveau du système d'exploitation et des applications• Protège l'hôte après déchiffrement du message	<ul style="list-style-type: none">• Dépend du système d'exploitation• Doit être installé sur tous les hôtes



Dispositifs de sécurité

Appareils de sécurité spécialisés

- **Cisco Advanced Malware Protection (AMP) :**
 - Solution intégrée d'analyse et de protection contre les malwares qui visent les entreprises.
 - Fournit aux entreprises une protection complète contre les logiciels malveillants avant, pendant et après une attaque.
- **Appliance Cisco pour la sécurité du web (WSA) avec fonctionnalités de sécurisation du web (CWS) :**
 - WSA protège le réseau en bloquant automatiquement les sites à risque et en testant les sites inconnus avant de permettre aux utilisateurs d'y accéder.
 - WSA offre une protection contre les logiciels malveillants, permet la visibilité et le contrôle des applications, propose des rapports intelligents et assure la sécurité mobile.
 - CWS assure une communication sécurisée vers et depuis Internet.
 - CWS fournit aux travailleurs distants le même niveau de sécurité qu'aux employés sur site.
- **Appareil Cisco de sécurité de la messagerie (ESA)**
 - Défend les systèmes de messagerie stratégiques.
 - Permet de détecter et de mettre en corrélation les menaces à l'aide d'un système de surveillance de base de données mondial.

Office 365 ATP protection stack

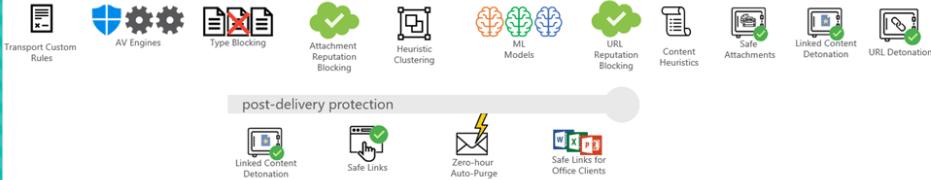
edge protection



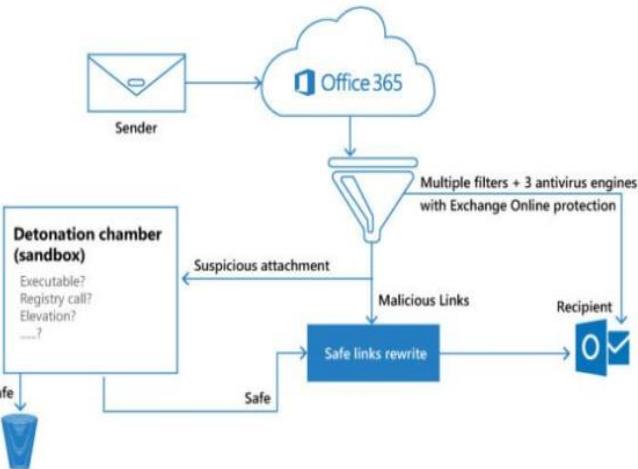
sender intelligence



content filtering



post-delivery protection

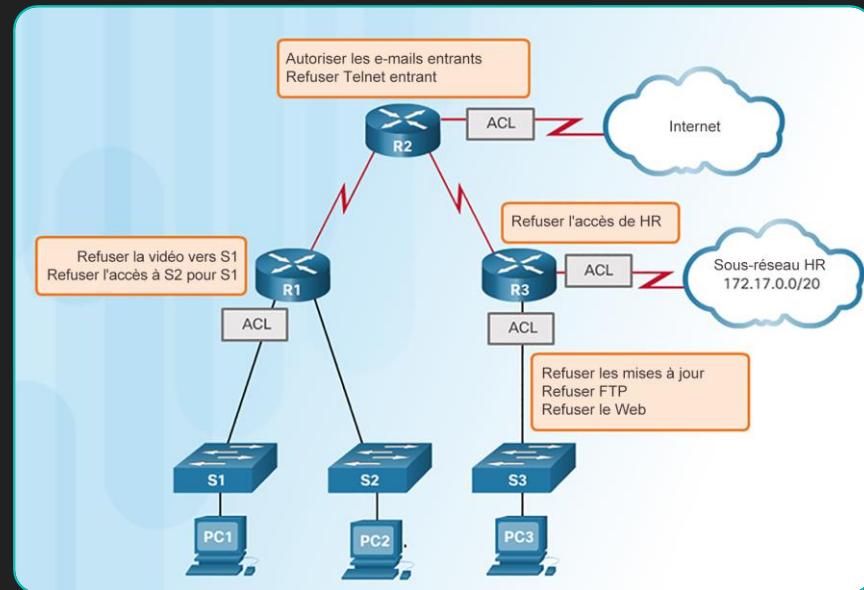


Office 365 ATP

Services de sécurité

Contrôle du trafic avec des ACL

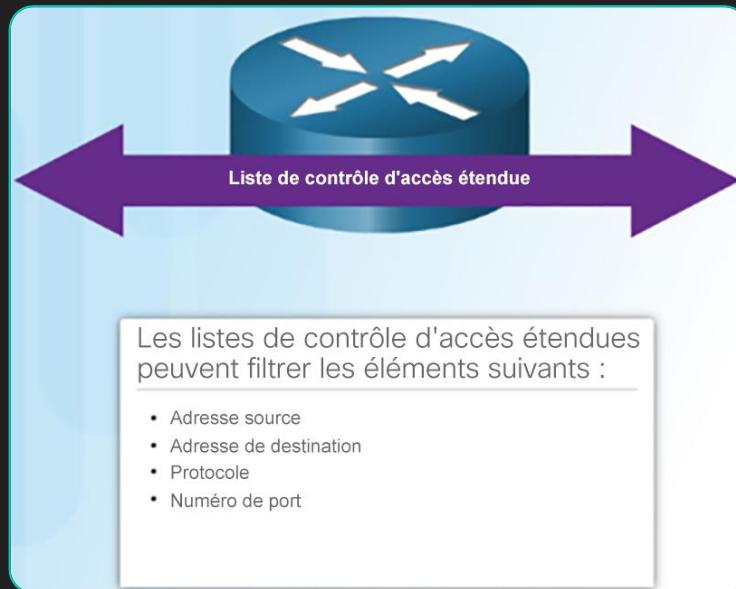
- Une liste de contrôle d'accès (ACL, Access Control List) est une série de commandes qui déterminent si un appareil achemine ou abandonne les paquets en fonction des informations contenues dans l'en-tête de paquet :
 - Elles limitent le trafic réseau pour accroître les performances réseau.
 - Elles contrôlent le flux de trafic.
 - Elles fournissent un niveau de sécurité de base pour l'accès réseau.
 - Elles filtrent le trafic en fonction de son type.
 - Elles filtrent les hôtes pour autoriser ou refuser l'accès aux services sur le réseau.



Services de sécurité

ACL : fonctionnalités importantes

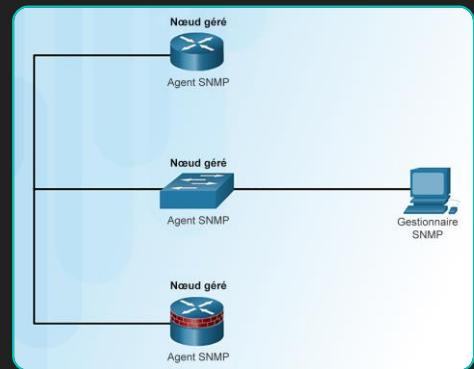
- Il existe deux types de listes de contrôle d'accès IPv4 Cisco : les listes standard et les listes étendues.
- Les listes de contrôle d'accès standard peuvent être utilisées pour autoriser ou refuser le trafic uniquement depuis des adresses IPv4 source. Les listes de contrôle d'accès étendues filtrent les paquets IPv4 en fonction de plusieurs critères :
 - Type de protocole
 - Adresse IPv4 source
 - Adresse IPv4 de destination
 - Ports TCP ou UDP source
 - Ports TCP ou UDP de destination
 - Informations facultatives sur le type de protocole pour un contrôle plus précis
- Les listes de contrôle d'accès standard et étendues et leur liste d'instructions peuvent être identifiées par un numéro ou par un nom.
- Un message ACL peut être généré et consigné lorsque le trafic répond aux critères d'autorisation ou de refus définis dans l'ACL.



Services de sécurité

SNMP

- Le protocole SNMP permet aux administrateurs de gérer les appareils tels que les serveurs, les stations de travail, les routeurs, les commutateurs et les appareils de sécurité.
- Le système SNMP se compose de trois éléments :
 - Un gestionnaire qui exécute le logiciel de gestion SNMP
 - Des agents qui correspondent aux nœuds surveillés et gérés
 - Une base de données MIB : une base de données sur l'agent qui stocke les données et des statistiques opérationnelles relatives à l'appareil



Hauptseite Geräte Bibliotheken Sensoren Alarme Maps Berichte Protokoll Tickets Konfiguration

Gruppe Root

Übersicht 0 Tage 30 Tage 365 Tage Alarne Protokoll Verwaltung Einstellungen Benachrichtigungen

Status: Sensorientiert: OK von 1010

Sensoren: 36 17 19 771 144 23

Sucher: P Suche...

Root

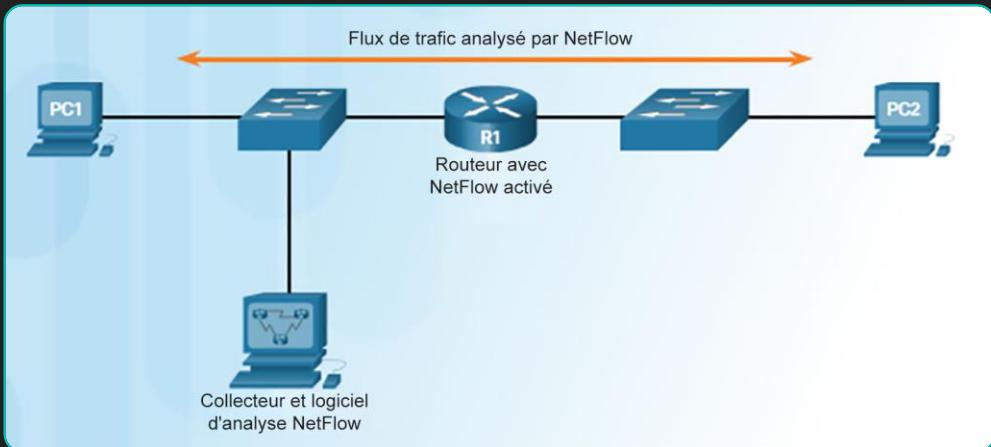
Local Probe

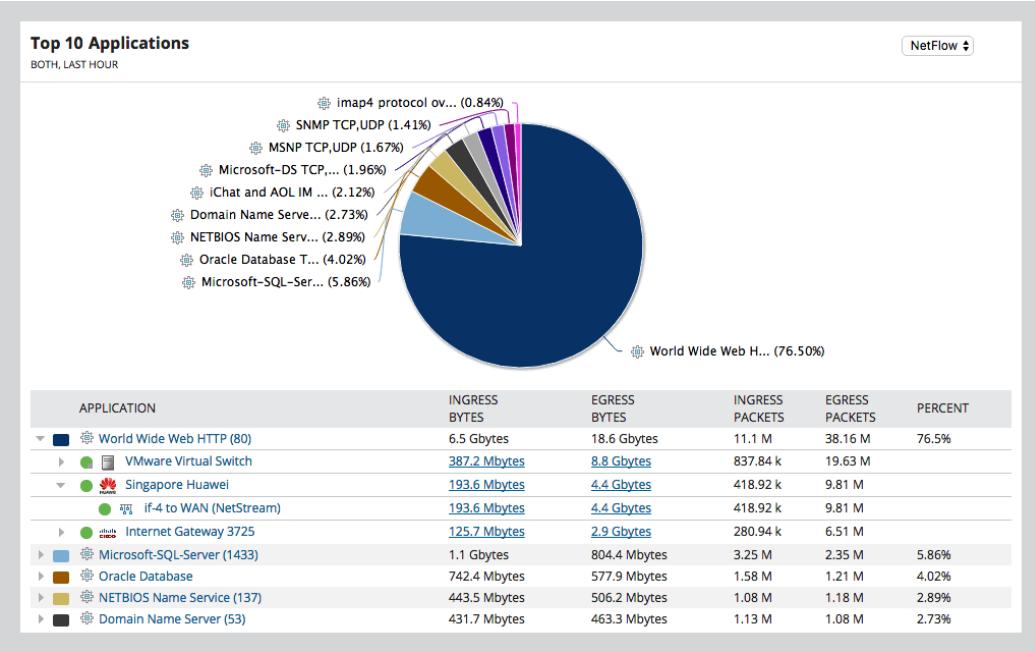
- AWS
 - Probe AWS
 - Probe AWS
 - Cloud (0 Gruppen und 2 Geräte)
 - Port-Checks
 - Port 443
 - SSL 443 231 ms
 - SQL Security Check Only Storing Protocols Available
 - AD Critical Ports 227 ms
 - NetFlow v5
 - NetFlow v5 1
 - NetFlow v5 (Custom)
 - Port 443
 - Port 443 227 ms
 - Network
 - FlowSensor
 - FlowSensor
 - IP 20
 - 020 Alias 20
 - 013 Alias 19
 - 012 Alias 12
 - 011 Alias 11
 - IP 20 path-Jitter (Erweitert)
 - 2 Sensoren
 - 1 Sensoren
 - 51 Sensoren
 - SAN / NAS / DAS
 - 1 Sensoren
 - 27 Sensoren
 - Server
 - Ring 127 ms
 - 2 Sensoren
 - 4 Sensoren
 - 47 Sensoren
 - Webserver Master
 - HTTP Transaction PRTG 1331 ms
 - HTTP Advanced PRTG Login 1331 ms
 - 1 Sensoren
 - 16 Sensoren
 - Webserver Failover
 - HTTP Transaction PRTG 1331 ms
 - 16 Sensoren
 - Workstations
 - PING 7
 - PING 2
 - 2 Sensoren
 - 1 Sensoren
 - Global Company Network
 - HTTP 1 342 ms
 - 15 Sensoren
 - Office365
 - Backup Check 10.948 ms
 - Exchange Online Roundtrip 1 Sensoren
 - Probe Candidates
 - Dpack

Services de sécurité

NetFlow

- Une technologie Cisco IOS qui fournit des statistiques sur les paquets qui transitent via un routeur ou un commutateur multicouche Cisco.
- NetFlow fournit des données qui facilitent la surveillance du réseau et de la sécurité, la planification du réseau, l'analyse du trafic et la comptabilité IP à des fins de facturation.

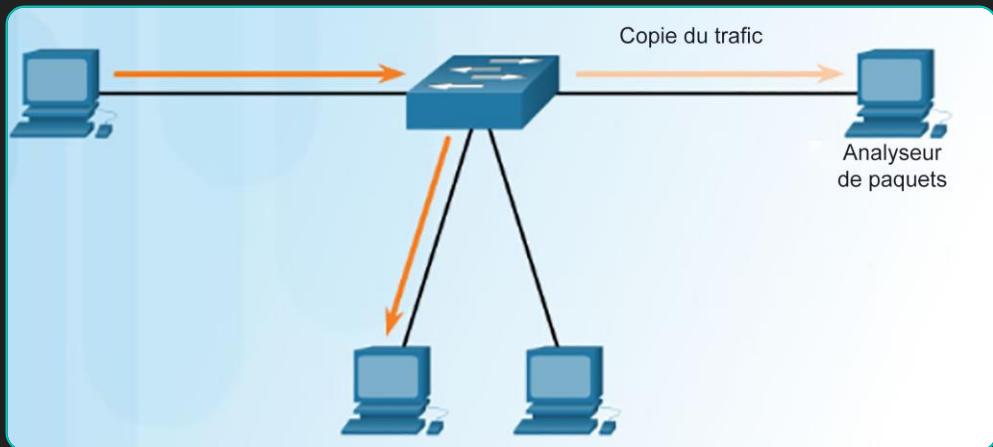




Services de sécurité

Mise en miroir du port

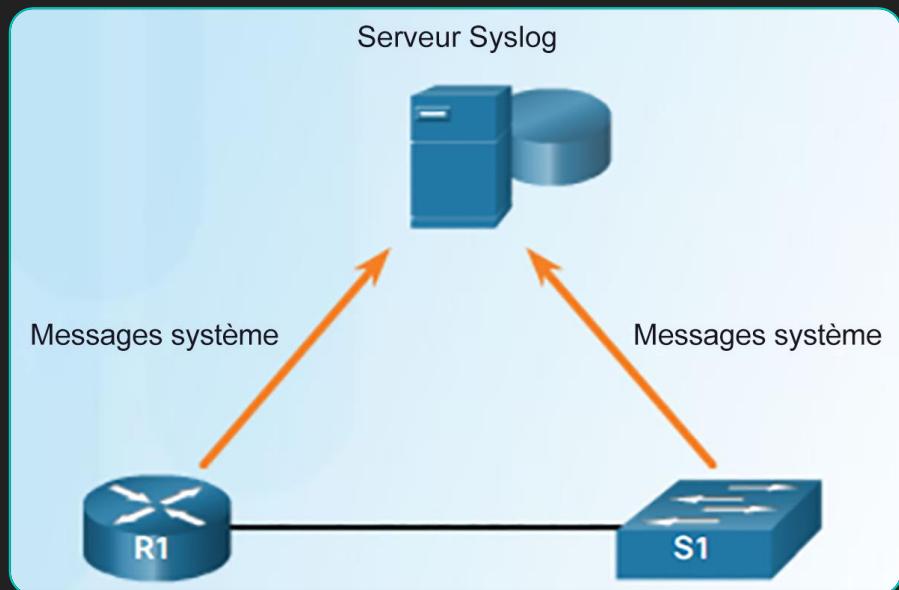
- Une fonctionnalité qui permet à un commutateur de dupliquer des copies du trafic qui transite via un commutateur, puis d'envoyer les données depuis un port équipé d'un système de surveillance du réseau.
- Le trafic d'origine est transmis de la manière habituelle.

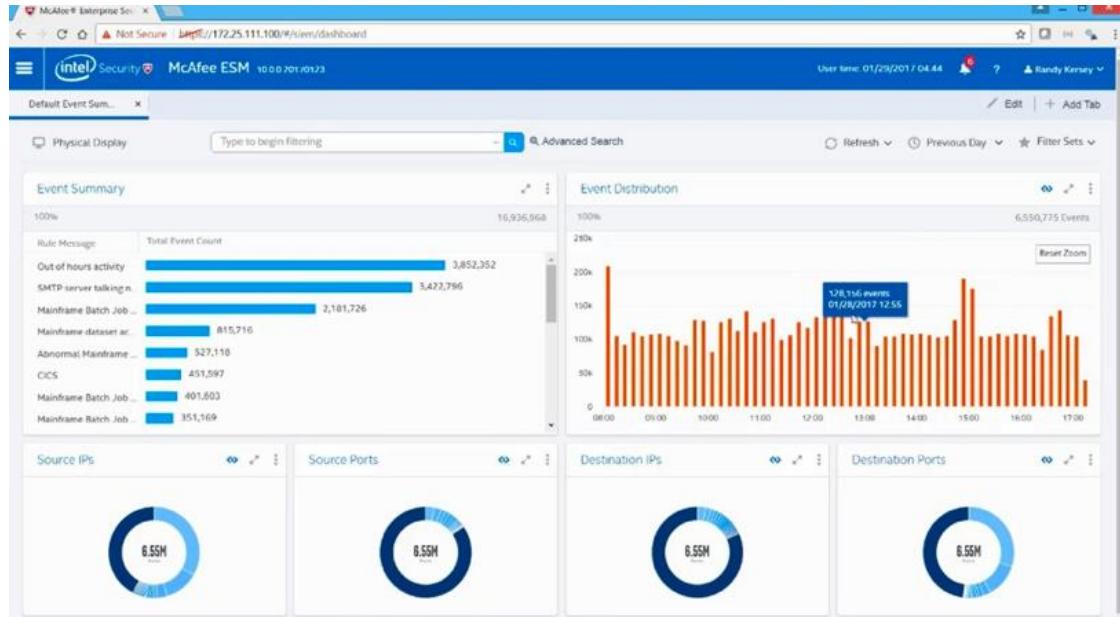
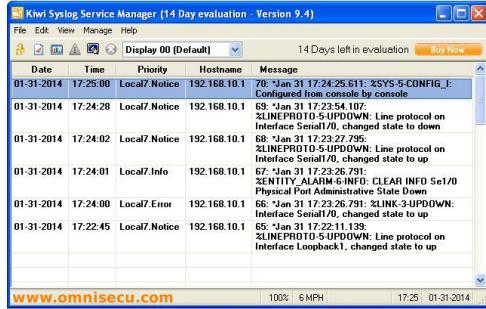


Services de sécurité

Serveurs Syslog

- La méthode la plus courante pour accéder à des messages système.
- Syslog permet aux appareils réseau d'envoyer leurs messages système sur tout le réseau aux serveurs Syslog.
- Le service de journalisation du protocole Syslog assume trois fonctions principales :
 - Collecter les informations de journalisation à des fins de surveillance et de dépannage
 - Sélectionner le type d'informations de journalisation capturées
 - Spécifier la destination des messages Syslog capturés

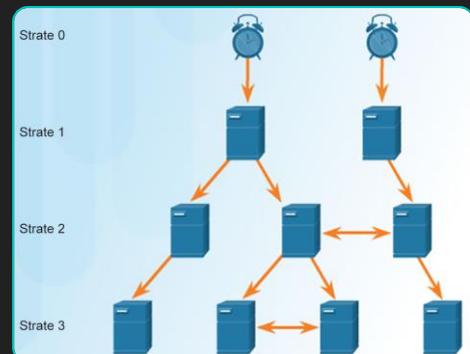




Services de sécurité

NTP

- Il permet aux routeurs du réseau de synchroniser leurs paramètres de date et d'heure avec un serveur NTP et d'utiliser des strates.
- Le protocole NTP peut être configuré de sorte qu'il se synchronise à une horloge principale privée ou à un serveur NTP public disponible sur Internet.
- Les serveurs NTP sont disposés en niveaux, appelés strates :
 - Strate 0** : périphériques haute précision censés être exacts et avec peu ou pas de retard.
 - Strate 1** : serveurs directement connectés aux sources temporelles faisant autorité. Ils représentent la principale référence temporelle du réseau.
 - Strate 2 et inférieure** : connectés aux périphériques de strate 1 via des connexions réseau. Les périphériques de strate 2 synchronisent leur horloge à l'aide des paquets NTP des serveurs de la strate 1. Ils peuvent également servir de serveurs pour les périphériques de la strate 3.



Services de sécurité

Serveurs AAA

- Les services AAA sont un ensemble de trois fonctions de sécurité indépendantes : authentification, autorisation et traçabilité/audit.
- Authentification** : les utilisateurs et les administrateurs doivent prouver leur identité.
 - Vous pouvez utiliser des combinaisons de nom d'utilisateur et de mot de passe, des questions d'authentification, des jetons et d'autres méthodes.
 - L'authentification AAA centralise le contrôle d'accès réseau.
- Autorisation** : après l'authentification, elle détermine les ressources auxquelles les utilisateurs peuvent accéder et les opérations qu'ils sont autorisés à effectuer.
- Traçabilité et audit** : les services de traçabilité consignent les actions de l'utilisateur, notamment les ressources auxquelles il accède et pendant combien de temps, et toutes les modifications apportées. Ces services permettent de contrôler la manière dont les ressources réseau sont utilisées.

	TACACS+	RADIUS
Fonctionnalités	Sépare le protocole AAA en fonction de l'architecture AAA, ce qui permet de mettre en œuvre le serveur de sécurité de manière modulaire	Combiné des fonctions d'authentification et d'autorisation, mais sépare la comptabilité réseau, ce qui offre moins de souplesse dans la mise en œuvre que le protocole TACACS +
Standard	Principalement les standards pris en charge par Cisco	Standard ouvert/RFC
Protocole de transport	TCP	UDP
CHAP	Défis et réponses bidirectionnels comme dans le protocole d'authentification CHAP	Défis et réponses unidirectionnels du serveur de sécurité RADIUS vers le client RADIUS
Confidentialité	Chiffrement des paquets complets	Mot de passe chiffré
Personnalisation	Autorise les commandes des routeurs en fonction de l'utilisateur et du groupe	Pas de possibilité d'autoriser les commandes des routeurs en fonction de l'utilisateur et du groupe
La journalisation	Limitée	Étendue

cisco Identity Services Engine

Home Operations | Policy | Administration |

Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Exceptions (1)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	WiFi Guest	If (WLC_Web_Authentication AND Guest_WLAN)	then PermitAccess
<input checked="" type="checkbox"/>	WiFi Basic Access	If (Wireless_PEAP AND Personal_Device_WLAN)	then PermitAccess
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones ISE	If Cisco-IP-Phone	then Cisco IP Phones
<input checked="" type="checkbox"/>	Profiled Non Cisco IP Phones ISE	If Non_Cisco_Profied_Phones	then Non Cisco IP Phones
<input checked="" type="checkbox"/>	Campus WiFi MAB	If MAB_Devices AND (Wireless_MAB AND Campus_Controller)	then Campus WiFi MAB
<input checked="" type="checkbox"/>	Branch WiFi MAB	If MAB_Devices AND (Wireless_MAB AND Branch_Controller)	then Branch WiFi MAB

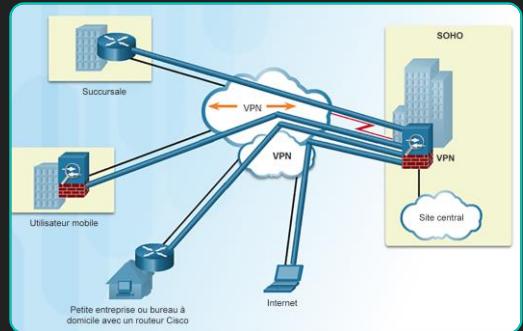
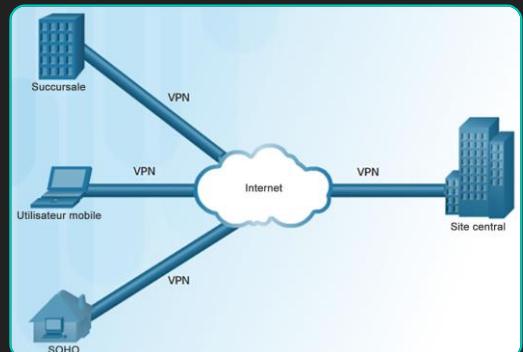
Authorization policy rule which allows access for devices using PEAP authentication and connected to the employee personal devices WLAN

294070

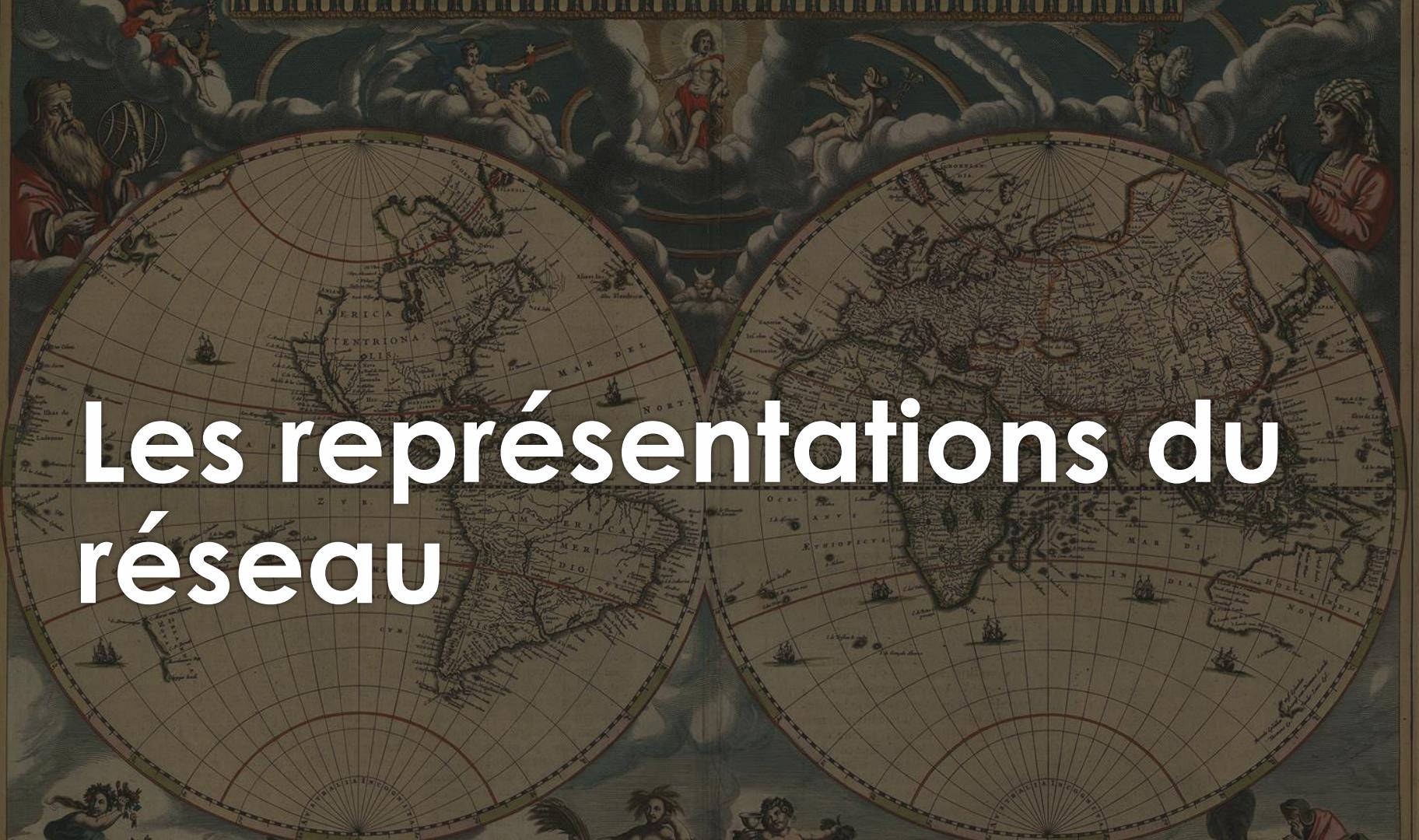
Services de sécurité

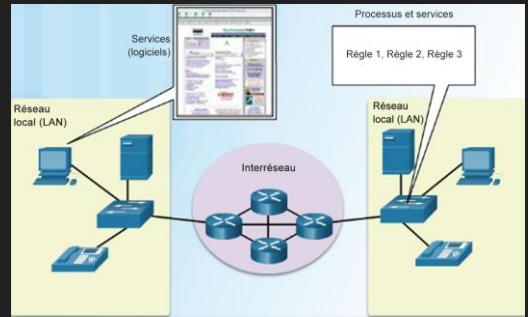
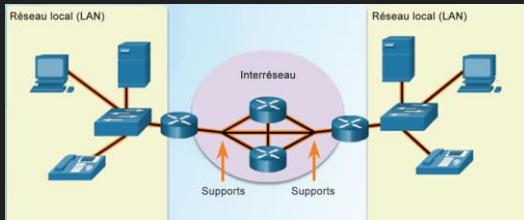
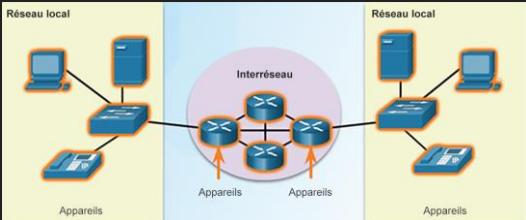
VPN

- Un réseau privé créé sur un réseau public.
- Un VPN est privé, dans le sens où le trafic est chiffré pour assurer la confidentialité des données pendant qu'il transite sur le réseau public.
- Les services IPsec se chargent de l'authentification, de l'intégrité, du contrôle d'accès et de la confidentialité.



Les représentations du réseau





Topologies du réseau

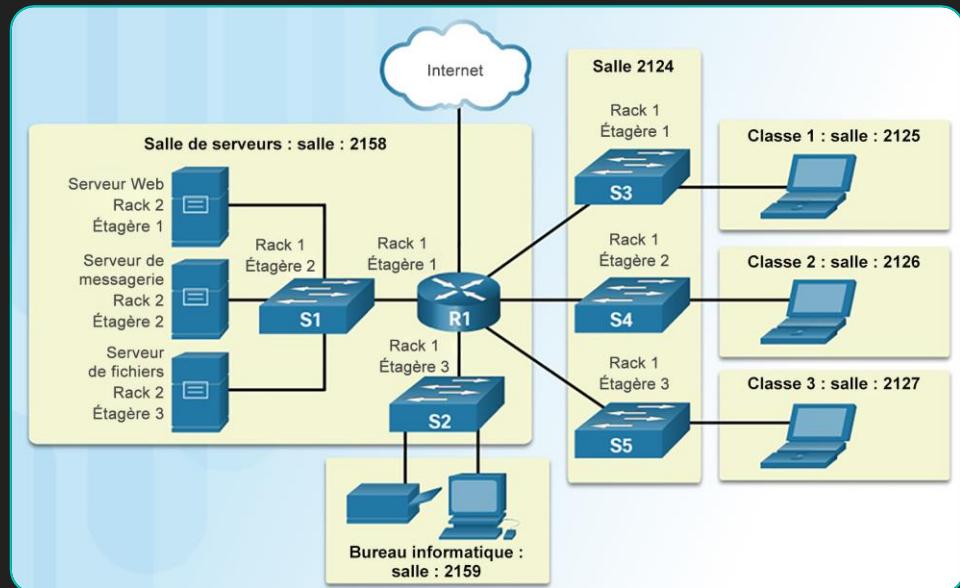
Présentation des composants réseau

- L'infrastructure de réseau comprend trois catégories de composants réseau :
- Appareils
- Supports
- Services

Topologies du réseau

Topologies physiques et logiques

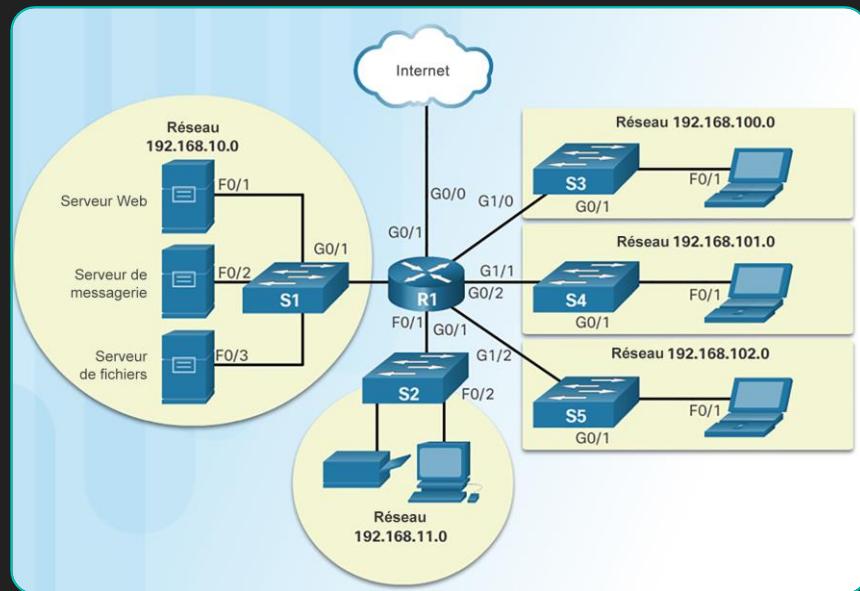
- La topologie physique fait référence aux connexions physiques et identifie les interconnexions entre les terminaux et les appareils de l'infrastructure.



Topologies du réseau

Topologies physiques et logiques (suite)

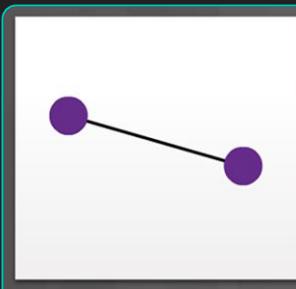
- La topologie logique désigne la manière dont un réseau transfère les trames d'un nœud à l'autre.



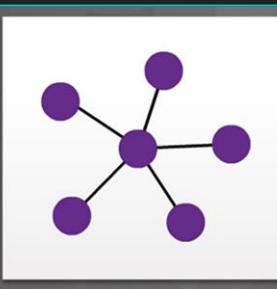
Topologies du réseau

Topologies WAN

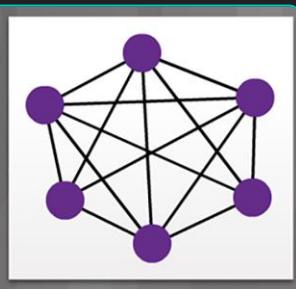
- **Point à point** : liaison permanente entre deux terminaux.
- **Hub and Spoke** : version WAN de la topologie en étoile, dans laquelle un site central connecte entre eux les sites des filiales à l'aide de liaisons point à point.
- **Maillée** : cette topologie offre une haute disponibilité, mais nécessite que tous les systèmes finaux soient connectés entre eux.



Topologie point à point



Topologie en étoile (Hub and Spoke)

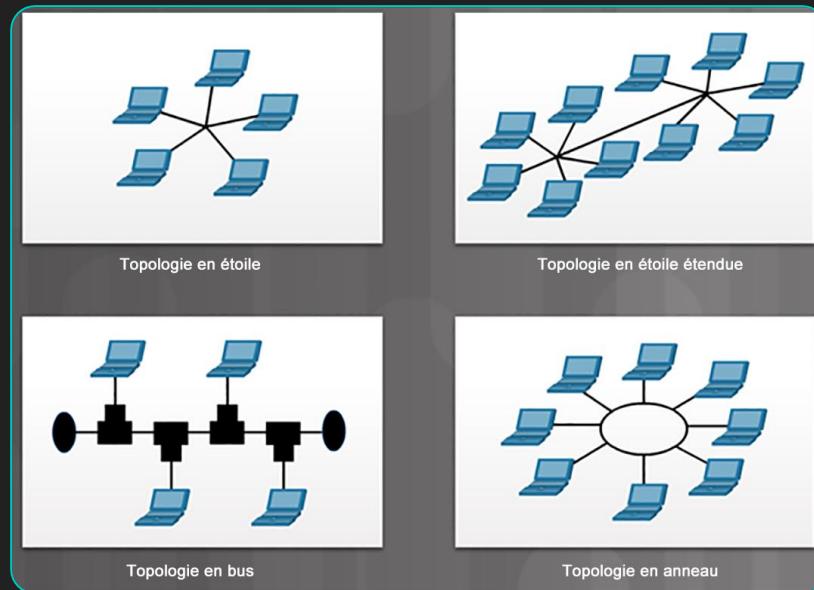


Topologie à maillage global

Topologies du réseau

Topologies LAN

- **Topologie en étoile** : les périphériques finaux sont connectés à un périphérique intermédiaire central.
- **Topologie en étoile étendue** : dans une topologie en étoile étendue, les périphériques Ethernet supplémentaires sont interconnectés avec d'autres topologies en étoile. R
- **Topologie en bus** : tous les systèmes finaux sont reliés entre eux en formant une chaîne et le réseau est terminé à chaque extrémité par un bouchon de terminaison.
- **Anneau** : les terminaux sont connectés à leurs voisins respectifs, constituant un anneau. Contrairement à la topologie en bus, l'anneau n'a pas besoin d'être terminé.

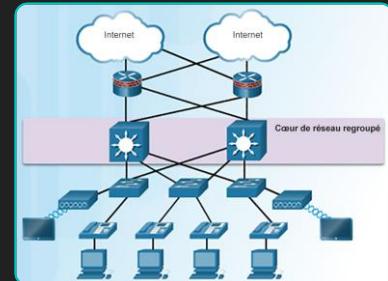
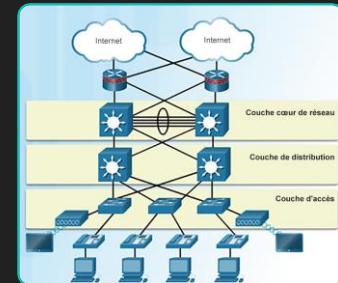


Topologies du réseau

Modèle de conception de réseau à trois couches

Modèle hiérarchique à trois couches

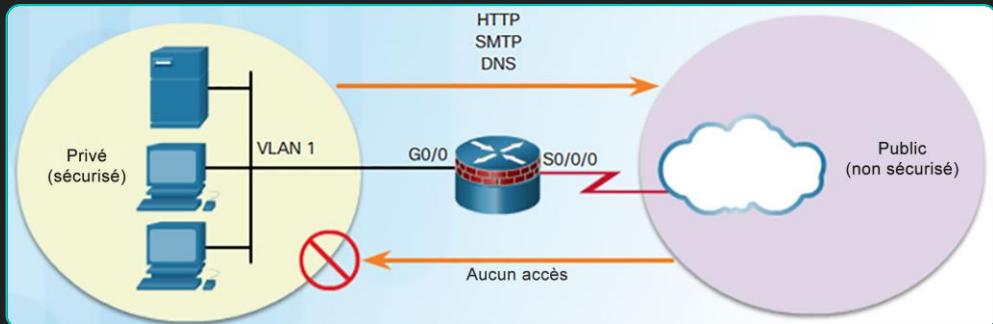
- Couche d'accès :
 - Fournit aux terminaux et aux utilisateurs un accès direct au réseau.
 - Le trafic utilisateur est initié au niveau de cette couche.
- Couche de distribution
 - Regroupe les couches d'accès.
 - Assure la connectivité aux services.
- Couche cœur de réseau
 - Assure la connectivité entre les couches de distribution.
- Cœur de réseau regroupé
 - Les couches principales et les couches de distribution sont souvent réunies en une seule couche.
 - Réduit les coûts et la complexité.



Topologies du réseau

Architectures de sécurité courantes

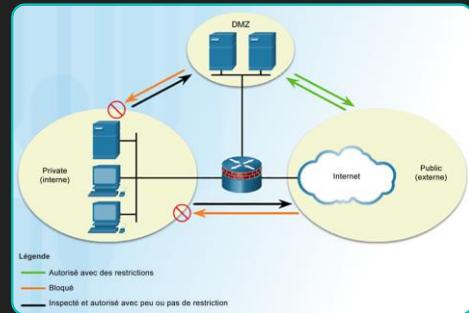
- La conception des pare-feu repose principalement sur des interfaces d'appareils qui autorisent ou refusent le trafic en fonction de la source, de la destination et du type de trafic. Certains modèles sont aussi simples que la désignation d'un réseau externe et d'un réseau interne. Un pare-feu avec deux interfaces est configuré comme suit :
 - Le trafic provenant du réseau privé est autorisé et inspecté au fur et à mesure qu'il se déplace vers le réseau public. Le trafic retour inspecté provenant du réseau public et associé au trafic issu du réseau privé est autorisé.
 - Le trafic provenant du réseau public et voyageant vers le réseau privé est généralement bloqué.



Topologies de réseau

Architectures de sécurité courantes (suite)

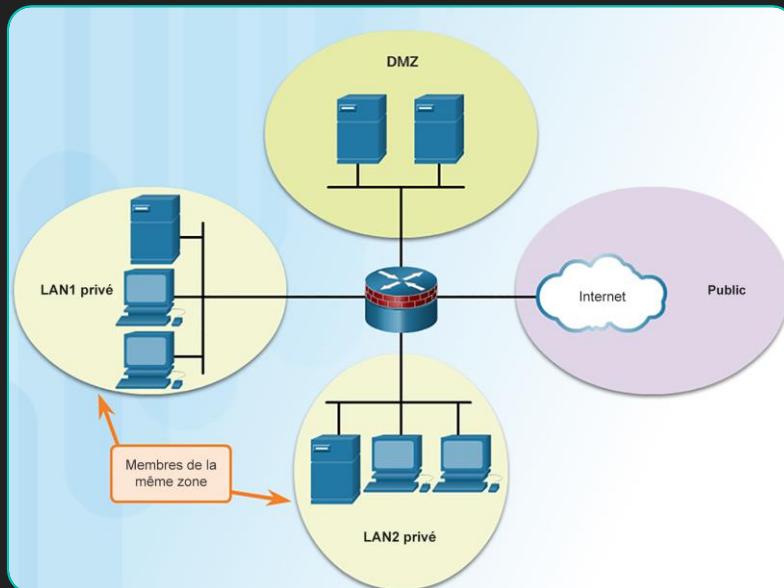
- Une zone démilitarisée (DMZ) est un système de pare-feu comportant généralement une interface interne connectée au réseau privé, une interface externe connectée au réseau public et une interface DMZ :
 - Le trafic provenant du réseau privé est inspecté lorsqu'il se déplace vers le réseau public ou la DMZ. Ce trafic est autorisé avec peu ou pas de restriction. Le trafic de retour est généralement autorisé.
 - Le trafic provenant du réseau DMZ et se déplaçant vers le réseau privé est généralement bloqué.
 - Le trafic provenant du réseau DMZ et voyageant vers le réseau public est autorisé de manière sélective en fonction des exigences du service.
 - Le trafic provenant du réseau public et voyageant vers la DMZ est inspecté et autorisé de manière sélective. Le trafic de retour est autorisé dynamiquement.
 - Le trafic provenant du réseau public et voyageant vers le réseau privé est bloqué.



Topologies de réseau

Architectures de sécurité courantes (suite)

- Les pare-feu à politique basée sur les zones (ZPF) utilisent le concept de zones pour assurer une meilleure flexibilité.
- Une zone est un groupe d'une ou plusieurs interfaces partageant des fonctions ou des caractéristiques similaires.





Récapitatif

Récapitulatif

- Les périphériques intermédiaires connectent les périphériques finaux individuels au réseau et peuvent connecter plusieurs réseaux individuels afin de former un interréseau.
- Les routeurs sont chargés de déterminer le chemin d'accès et de transférer les paquets.
- La table de routage recherche les résultats dans un réseau connecté directement, dans un réseau distant ou là où aucune route n'est déterminée.
- Les entrées de réseau de destination de la table de routage peuvent être ajoutées par les interfaces de route locale, les interfaces connectées directement, les routes statiques ou via un protocole de routage dynamique.
- Un concentrateur Ethernet agit également comme un répéteur multiport, les ponts ont deux interfaces et sont connectés entre les concentrateurs, et les commutateurs LAN connectent les périphériques dans une topologie en étoile.
- Les commutateurs LAN déterminent comment traiter les trames de données entrantes en gérant la table d'adresses MAC.
- Les appareils d'un VLAN se comportent comme s'ils se trouvaient chacun sur leur propre réseau indépendant, même s'ils partagent une infrastructure commune avec d'autres VLAN.

Récapitulatif (suite)

- Le protocole STP garantit la présence d'un seul chemin logique entre toutes les destinations sur le réseau en bloquant intentionnellement les chemins redondants susceptibles de provoquer une boucle.
- Les commutateurs multicouches (également connus sous le nom de commutateurs de couche 3) effectuent la commutation de couche 2, mais transmettent également des trames en fonction des informations des couches 3 et 4.
- Les réseaux sans fil (WLAN) utilisent des fréquences radio au lieu de câbles au niveau de la couche physique et de la sous-couche MAC de la couche de liaison de données.
- Des trames de gestion sont utilisées par les périphériques sans fil pour effectuer le processus en trois étages de détection de point d'accès (AP), d'authentification et d'association.
- Lorsque vous utilisez un contrôleur LAN sans fil (WLC), les points d'accès n'agissent plus de manière autonome, mais plutôt comme des points d'accès légers (LWAP).
- Un pare-feu est un système, ou un groupe de systèmes, qui impose une politique de contrôle d'accès entre des réseaux.

Récapitulatif (suite)

- Il existe de nombreux types de pare-feu : pare-feu de filtrage de paquets (sans état), pare-feu avec état, pare-feu de passerelle d'application (pare-feu proxy), pare-feu basé sur l'hôte (serveur et personnel), pare-feu transparent et pare-feu hybride.
- Les pare-feu de filtrage de paquets font généralement partie d'un pare-feu de routeur, qui autorise ou interdit le trafic en fonction des informations des couches 3 et 4.
- Les pare-feu dynamiques effectuent un filtrage dynamique des paquets à l'aide d'informations de connexion mises à jour dans une table d'états.
- Les pare-feu de nouvelle génération vont au-delà des pare-feu avec état en fournissant des fonctionnalités de pare-feu standard, la prévention intégrée des intrusions, la reconnaissance des applications, les chemins de mise à niveau permettant d'inclure les futurs flux d'informations et des techniques de gestion face à l'évolution constante des menaces de sécurité.
- Lorsque vous implémentez IDS ou IPS, il est important de connaître les types de systèmes disponibles, à savoir les approches basées sur l'hôte et sur le réseau, le positionnement de ces systèmes, le rôle des catégories de signature et les mesures possibles qu'un routeur Cisco IOS peut prendre quand une attaque est détectée.

Récapitulatif (suite)

- Le choix de l'implémentation d'IDS et d'IPS à utiliser repose sur les objectifs de sécurité de l'entreprise définis dans sa politique de sécurité réseau.
- Il existe deux types principaux de systèmes de prévention des intrusions : hôte et réseau.
- Les appliances de sécurité spécialisées telles que l'appliance de sécurisation du web, l'appliance de sécurisation de la messagerie électronique et les pare-feu de nouvelle génération offrent une protection complète contre les malwares et contribuent à réduire les menaces véhiculées par e-mail.
- Une liste de contrôle d'accès (ACL, Access Control List) est une série de commandes qui déterminent si un appareil achemine ou abandonne les paquets en fonction des informations contenues dans l'en-tête de paquet.
- Les listes de contrôle d'accès standard peuvent être utilisées pour autoriser ou refuser le trafic uniquement depuis des adresses IPv4 source, tandis que les listes de contrôle d'accès étendues filtrent les adresses IPv4 en fonction de différents attributs.
- Le protocole SNMP (Simple Network Management Protocol) permet aux administrateurs de gérer les terminaux sur un réseau IP et permet aux administrateurs réseau de surveiller et gérer les performances du réseau, de rechercher et résoudre les problèmes de réseau et de planifier la croissance de ce dernier.

Récapitulatif (suite)

- NetFlow fournit des données permettant la surveillance du réseau et de la sécurité, la planification réseau, l'analyse du trafic destinée à identifier les goulots d'étranglement du réseau ainsi que la comptabilité IP à des fins de facturation.
- La mise en miroir du port est une fonctionnalité qui permet à un commutateur de dupliquer des copies du trafic qui le traverse, puis d'envoyer les données depuis un port équipé d'un système de surveillance du réseau.
- Le protocole Syslog permet aux périphériques réseau d'envoyer leurs messages système sur le réseau aux serveurs Syslog.
- Le protocole NTP (Network Time Protocol) permet aux routeurs du réseau de synchroniser leurs paramètres temporels avec un serveur NTP.
- AAA est un cadre architectural pour configurer l'authentification, l'autorisation et la traçabilité.
- Un VPN connecte deux points de terminaison, comme un bureau à distance et un bureau central, sur un réseau public, pour constituer une connexion logique.

Récapitulatif (suite)

- L'infrastructure réseau comprend trois catégories de composants réseau : les périphériques, les supports et les services.
- Les topologies LAN et WAN peuvent être vues de deux façons : topologie physique ou topologie logique.
- Les réseaux étendus sont généralement interconnectés selon la topologie physique point à point, Hub and Spoke ou maillée.
- Les terminaux peuvent être interconnectés selon des topologies physiques en étoile, en bus, en anneau ou en étoile étendue.
- Une conception LAN hiérarchique inclut les couches d'accès, de distribution et de cœur de réseau.
- La conception des pare-feu repose principalement sur des interfaces d'appareils qui autorisent ou refusent le trafic en fonction de la source, de la destination et du type de trafic.

Chapitre 12

Nouveaux termes et nouvelles commandes

- Liste de contrôle d'accès (ACL)
- couche d'accès
- Pare-feu de passerelle applicative (pare-feu proxy)
- Table de mémoire associative (CAM)
- couche cœur de réseau
- CSMA/CA
- CSMA/CD
- Zone démilitarisée (DMZ)
- couche distribution
- protocole de routage dynamique
- encapsulation GRE (Generic Routing Encapsulation)
- IPS basé sur l'hôte (HIPS)
- périphérique intermédiaire
- IPS
- Points d'accès légers (LWAP)
- Topologie logique
- Commutateur multicouche
- NetFlow
- Protocole NTP (Network Time Protocol)
- analyseur de paquets
- Pare-feu de filtrage des paquets (sans état)
- Transfert de paquets