



Gwenn Feunteun
gwenn@acceis.fr

Architecture & sécurité réseau

Comment se protéger



Se protéger

Comment se protéger contres les attaques réseaux (mais aussi un parfois applicatives) ?

- **En mettant en œuvre une architecture réseau sécurisé.** Afin de rendre difficile les compromissions ou d'en limiter les impacts.
- **En protégeant les flux de communication.** Afin de potentiellement détecter les attaques et d'assurer la confidentialité et l'intégrité des échanges.

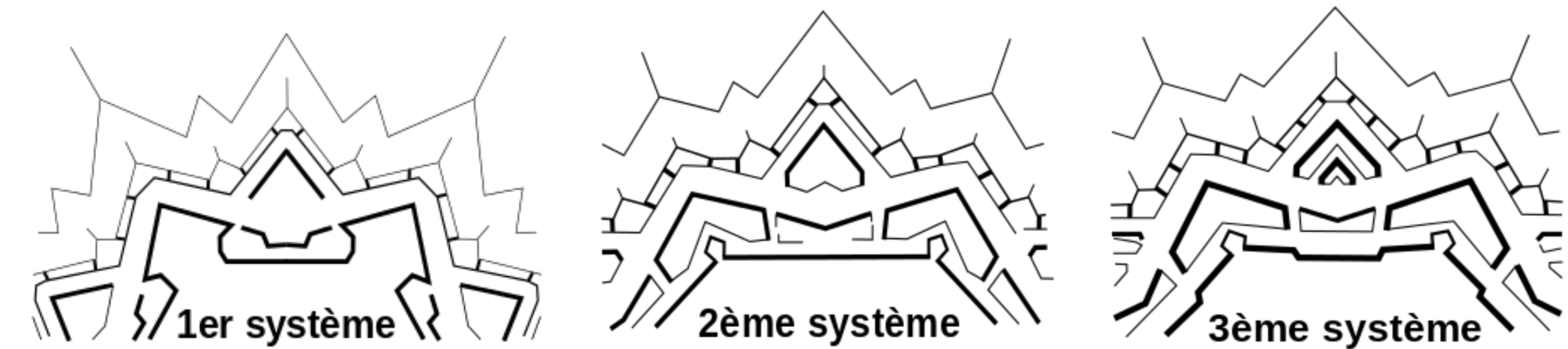
Introduction

Se protéger par l'architecture

Principe général : la défense en profondeur




Sébastien Le Prestre, Marquis de Vauban



Principe général : la défense en profondeur

Il faut empiler les couches de sécurité afin de rendre les attaques trop complexes ou trop coûteuses par rapport au gain visé.

- **Défense passive** : à chaque couche du modèle OSI (ou presque) sa mesure de sécurité intrinsèque ;
- **Défense active** : utilisation de composants de sécurité dédiés ;
- **Approche temporelle sur trois axes** : prévention / protection / remédiation.

 **Cloisonnement + Filtrage + Chiffrement**

Quelques mesures :

Passives

Actives

Application	Séparation fonctionnelle (n-tiers)	Filtrage applicatif (WAF, DPI)
Transport	Chiffrement des communications	Filtrage « traditionnel » (pare-feu, ACL)
Réseau	Segmentation en sous-réseaux (DMZ) Chiffrement des communications	
Liaison	Cloisonnement par VLAN	Contrôle d'accès (filtrage MAC, 802.1x)
Physique	Utilisation d'équipements différents	

Le cloisonnement

Comment cloisonner ?

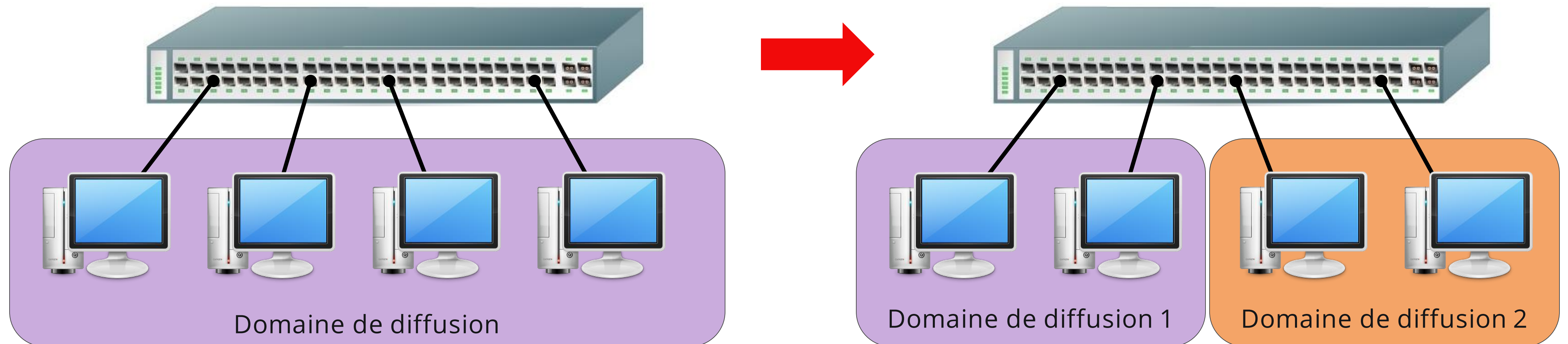
L'objectif du cloisonnement est de regrouper les équipements de l'infrastructure au sein de « bulle » fonctionnelles afin, dans un second temps, de réduire au strict nécessaire les possibilités de communication entre-elles. Les critères de regroupement peuvent être très variés : par nature d'équipement (postes de travail, serveurs, etc.), par service (services web, bases de données, etc.), par type d'accès, par zone géographique...

On distingue généralement deux types de cloisonnement, situés au niveau des couches basses du modèle OSI :

- Le **cloisonnement physique**, utilisant des matériels dédiés pour chaque domaine. Le mécanisme le plus efficace, mais aussi le plus coûteux et le moins souple d'usage.
- Le **cloisonnement logique**, moins cher, plus souple, mais moins sûr. Il s'agit généralement de mettre en place une discrimination au niveau de la couche liaison en fonction de critères particuliers.

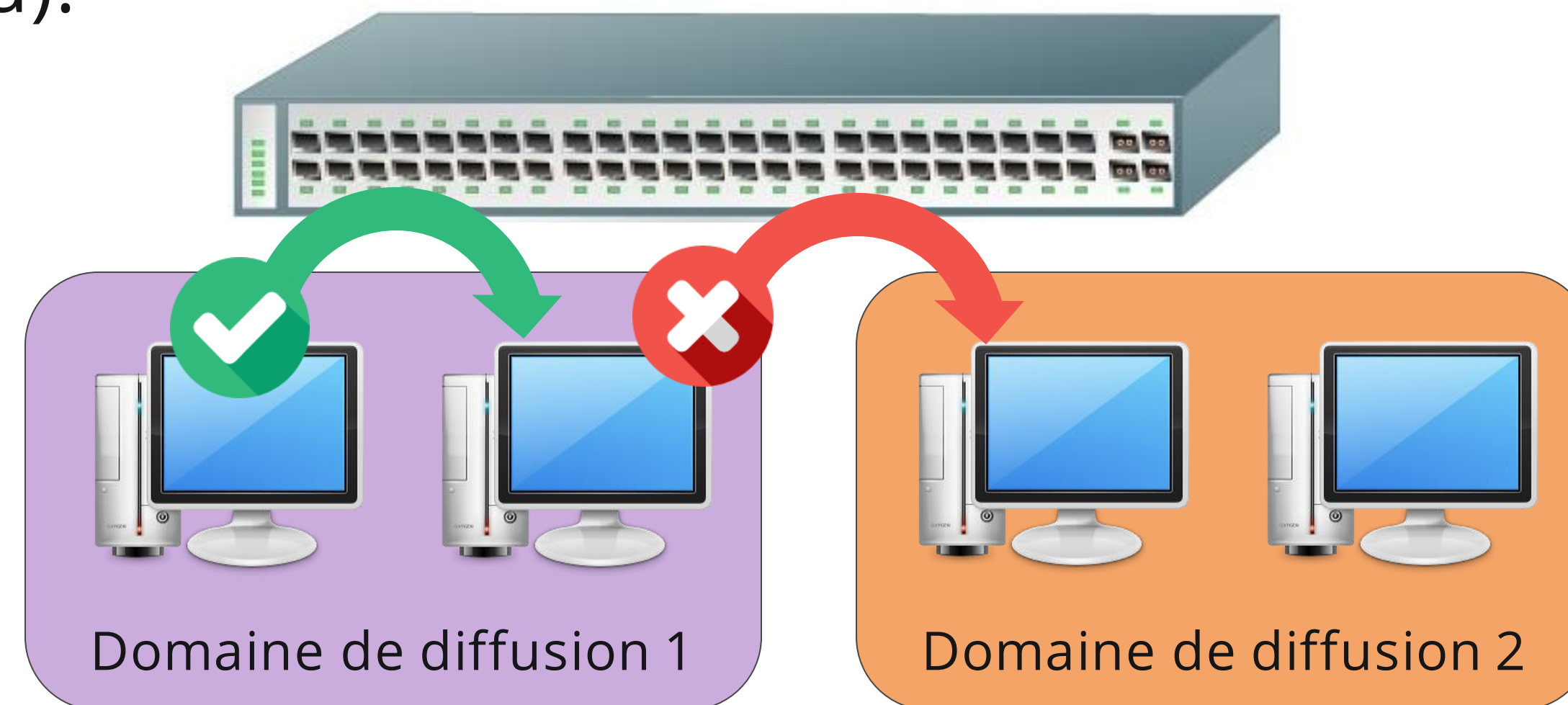
Les VLAN

C'est le mode de cloisonnement le plus couramment employé. Il intervient au niveau 2 du modèles OSI (liaison) et sert à compartimenter le réseau en plusieurs sous-réseaux virtuel (Virtual Local Area Network), chacun correspondant à un domaine de diffusion particulier. Il s'agit donc d'une fonction prise en charge par les **commutateurs**.



Les VLAN

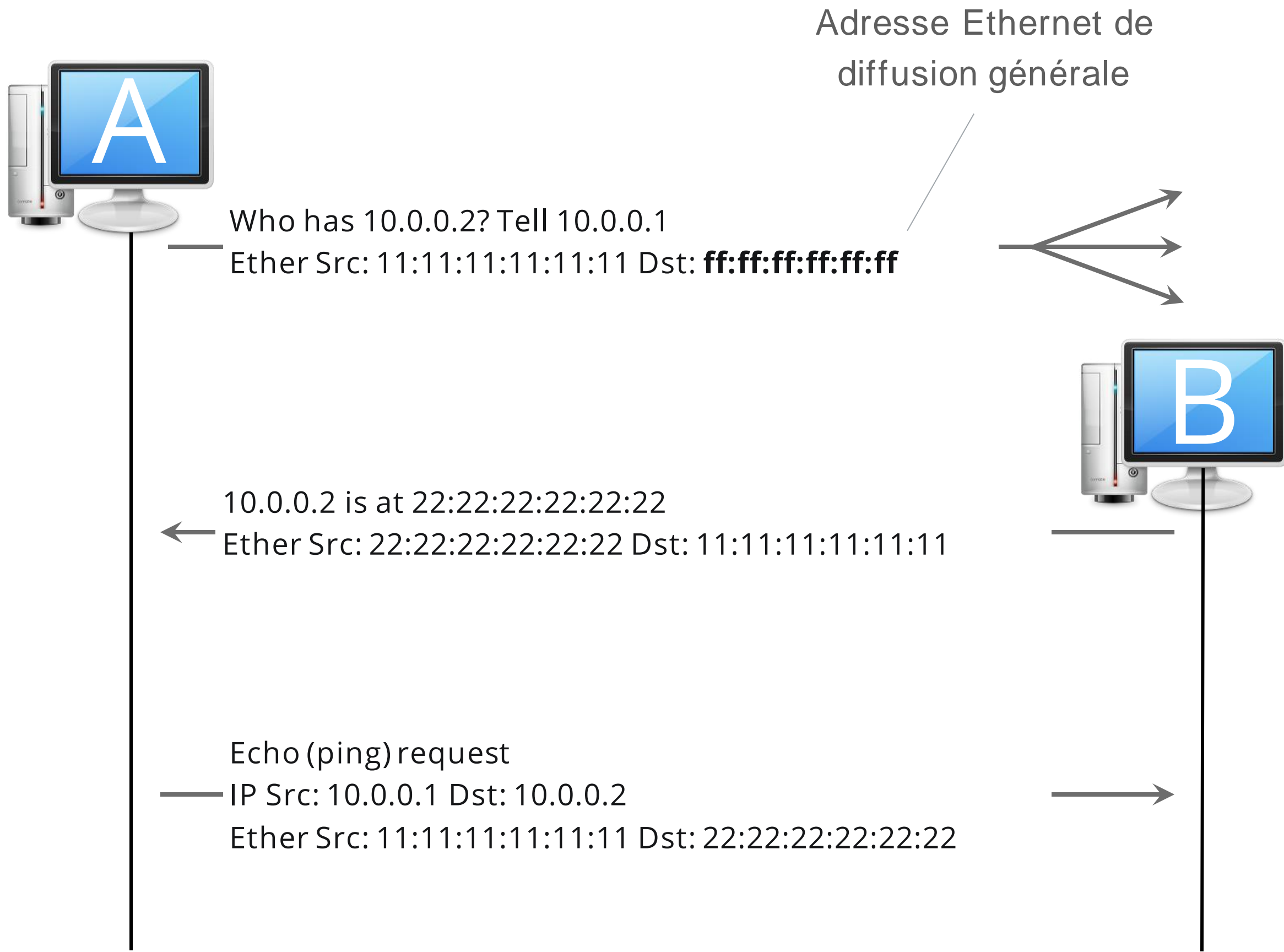
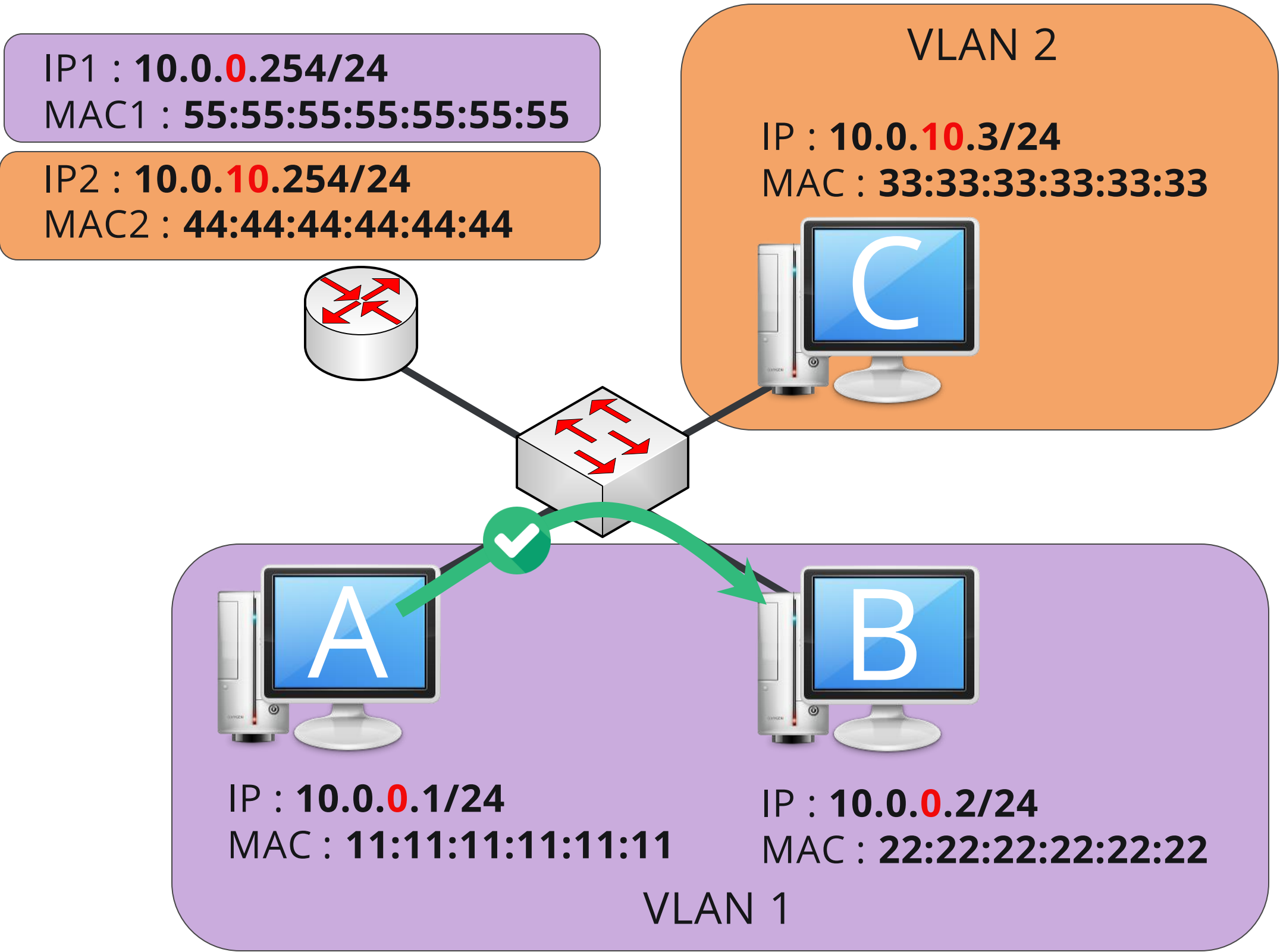
Rappel : seules les machines appartenant au même domaine de diffusion (*broadcast domain*) peuvent échanger directement entre-elles. Dans le cas contraire, elle doivent passer par un routeur pour communiquer (comportement natif des piles réseau).



➡ 1 VLAN = 1 sous-réseau IP (sauf si on utilise un mandataire ARP)

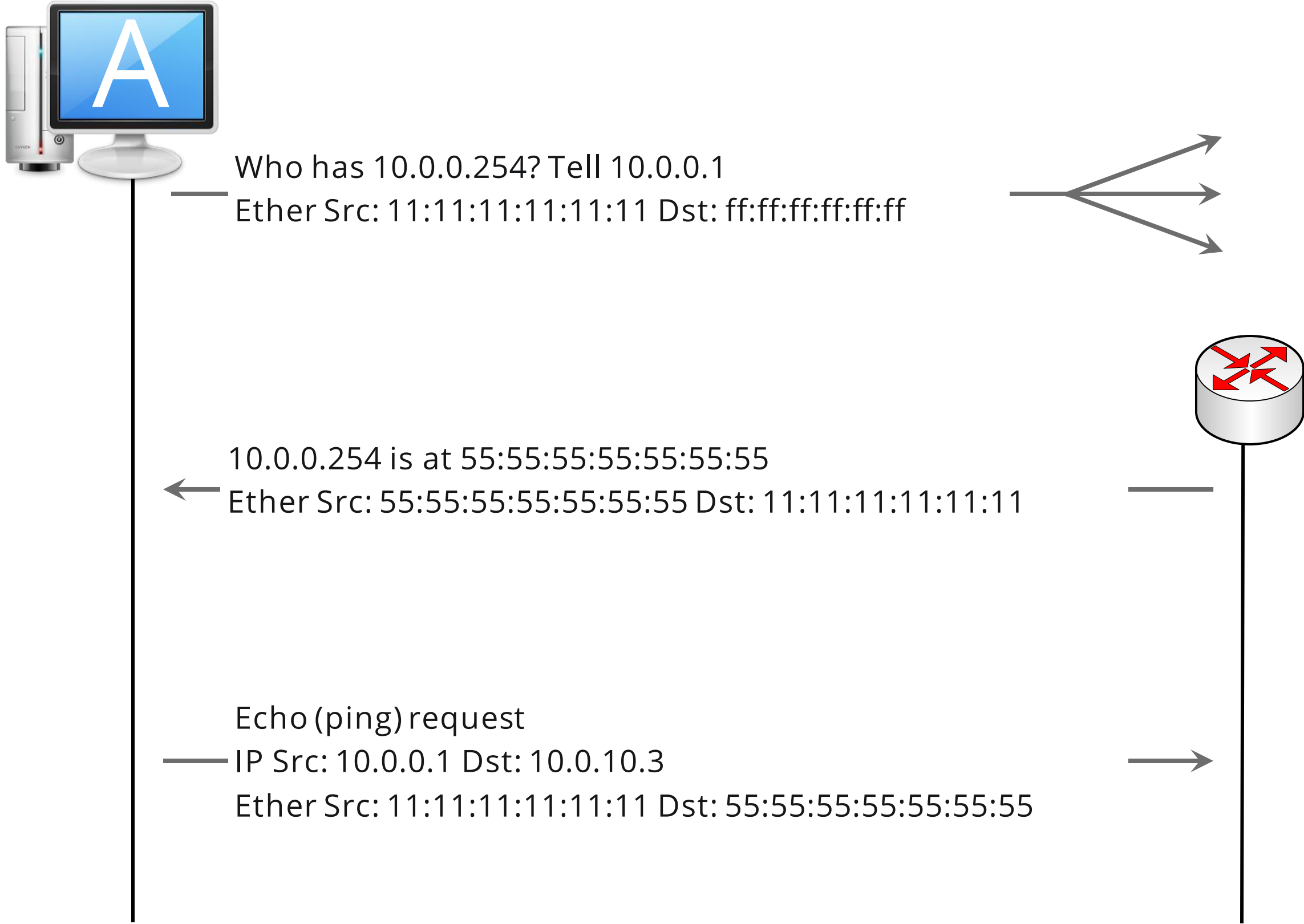
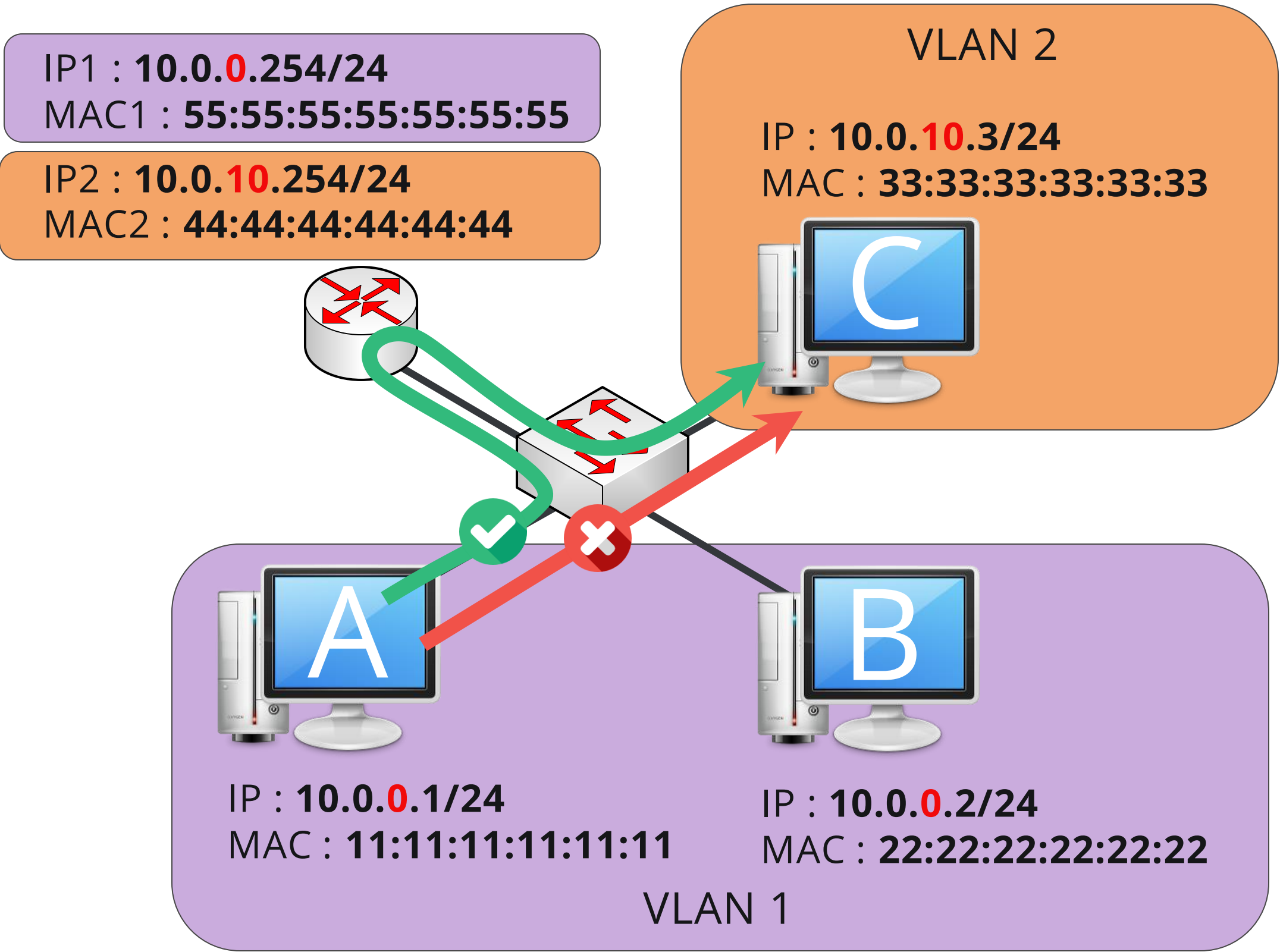
Les VLAN

Exemple 1 : A veut échanger (ping) avec B, qui est dans le même VLAN que lui.



Les VLAN

Exemple 2 : A veut échanger (ping) avec C, qui est dans un VLAN différent.



Les VLAN

On distingue trois types de VLAN :

- VLAN de niveau 1 ou **VLAN de port**, qui regroupe les stations en fonction du port physique du commutateur sur lequel elles sont raccordées. C'est le plus courant et le plus robuste ;
- VLAN de niveau 2 ou **VLAN de MAC**, qui regroupe les stations en fonction de leur adresse MAC ;
- VLAN de niveau 3 ou **VLAN d'IP**, qui regroupe les stations en fonction de leur adresse IP.



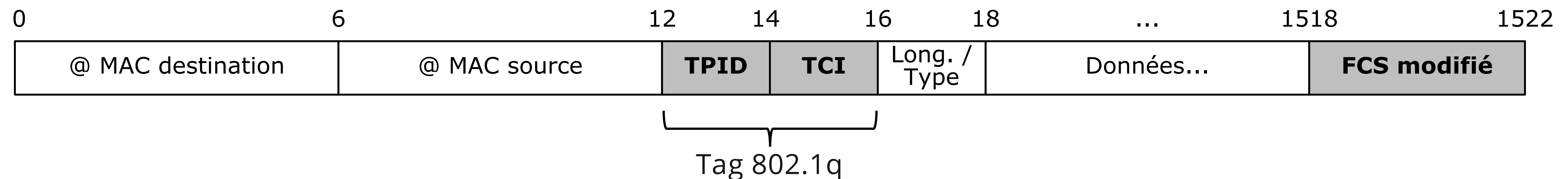
Les VLAN d'IP et de MAC ne permettent pas d'assurer un cloisonnement efficace contre un attaquant, car il lui suffit d'usurper les adresses légitimes pour s'insérer dans un VLAN.

La norme 802.1q

- Comment regrouper un grand nombre de machines (des postes utilisateurs par exemple) dans un même VLAN alors que les commutateurs du commerce les plus courants n'ont pas plus de 50 ports physiques ?
- Comment faire en sorte que deux stations situées sur des sites physiques différents (séparés de quelques dizaines de mètres ou de plusieurs centaines de kilomètres) soient dans le même VLAN ?
 - ➔ **En interconnectant les commutateurs** ; Et afin de s'affranchir de la nécessité d'utiliser un câble d'interconnexion par VLAN, l'IEEE a défini la norme **802.1q** qui permet d'échanger les trames Ethernet entre les commutateur sur un même lien (appelé **trunk**) tout en conservant l'information de leur VLAN d'appartenance.

La norme 802.1q

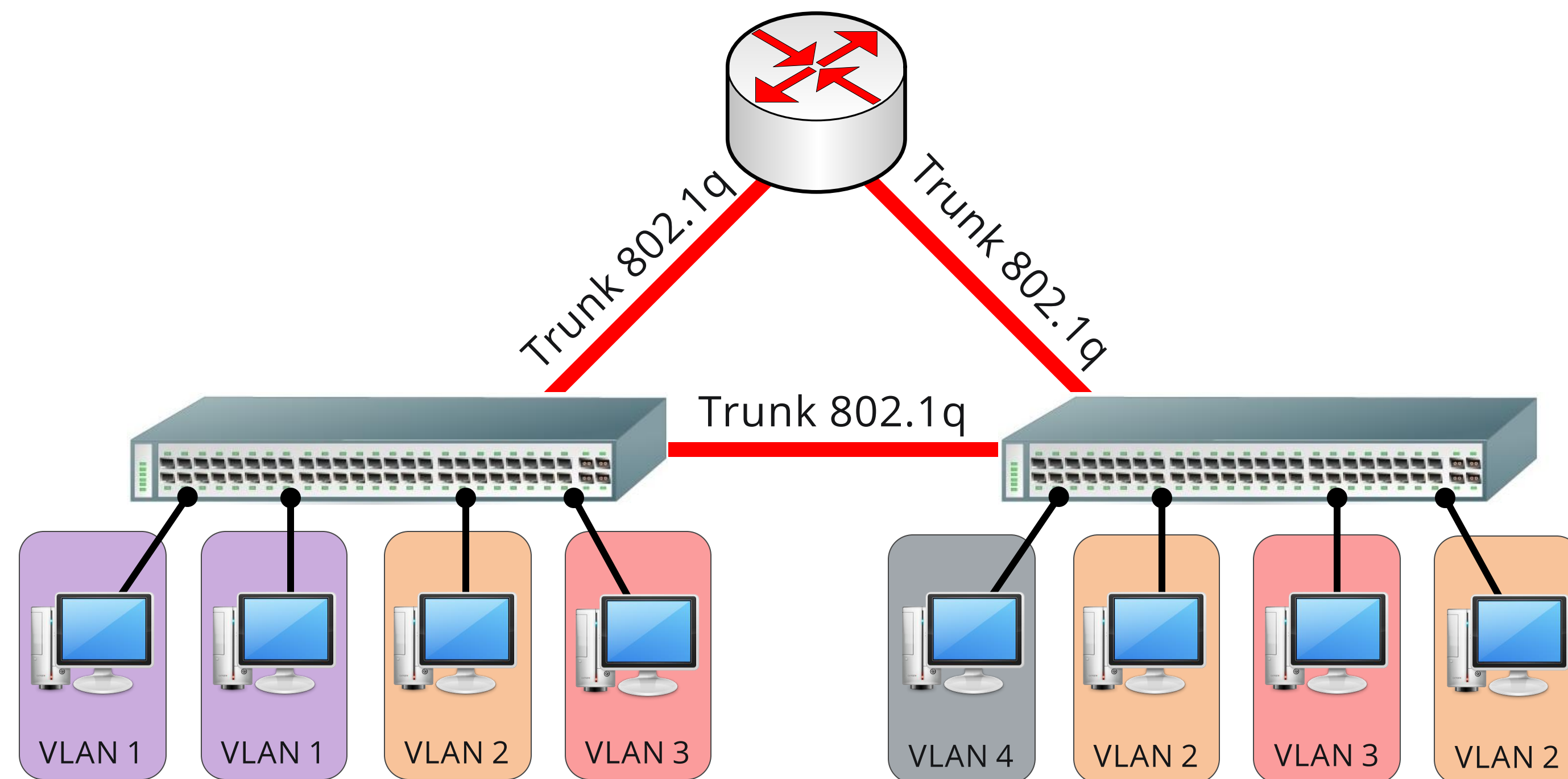
Les trames Ethernet sont modifiées pour y insérer un *tag*. La somme de contrôle est également recalculée pour prendre en compte cet ajout.



- **TPID** – Tag Protocol Identifier. 2 octets servant à identifier le protocole de la balise insérée (valeur fixe à 0x8100 dans le cas du 802.1q);
- **TCI** – Tag Control Information, également de 2 octets. Il est composé de plusieurs informations :
 - Priorité (3 bits);
 - *Canonical Format Indicator* ou CFI (1 bit), généralement mis à 0 ;
 - Identification de VLAN ou **VID** (12 bits), utilisé pour indiquer à quel VLAN appartient la trame. Sa valeur est comprise entre 1 et 4094. Une valeur à 0 signifie qu'il n'y a pas de VLAN et les ID de 1002 à 1005 et 4095 sont réservés.

La norme 802.1q

Le schéma suivant illustre une architecture simple mettant en œuvre des VLAN et un lien de type *trunk* entre les commutateurs. Le routeur, nécessaire à la communication inter-VLAN, est également relié aux commutateur via un *trunk*. Dans le cas contraire, il faudrait un câble (et une interface réseau) par VLAN.



Configuration des VLAN

Les commutateurs autorisent généralement au moins deux modes de fonctionnement pour leurs port (dans le cadre de l'usage de VLAN) :

- Le mode **access**. Le port est destiné à être connecté à un terminal (un poste de travail par exemple), agnostique de toute notion de VLAN. Les trames ne sont pas marquées.
- Le mode **trunk**. Le port est utilisé pour être connecté à un autre équipement réseau prenant en charge le protocole 802.1q. Les trames sont alors marquées. Par défaut, tous les VLAN y circulent.

Il est également possible de rencontrer un mode **hybride**, permettant la cohabitation de flux marqués et non marqués (placés alors dans un VLAN prédéfini). Ce type de configuration se rencontre fréquemment dans le cadre de l'usage de téléphones IP sur lesquels sont branchés des postes bureautiques.

Configuration des VLAN

Les commutateurs proposent souvent de nombreuses fonctionnalités de configuration automatique présentant des risques de sécurité et notamment la détection automatique du mode de fonctionnement. Le port est basculé du mode *access* au mode *trunk* (ou inversement) s'il détecte que l'équipement distant utilise le même mode. Cisco propose même un protocole permettant de négocier le mode du lien : DTP (*Dynamic Trunking Protocol*), activé par défaut.

Configuration des VLAN

Il existe deux VLAN particulier dont l'usage peut poser des problèmes de sécurité :

- **Le VLAN par défaut** (souvent le VLAN 1), qui est celui dans lequel les interfaces sont placées par défaut tant qu'elles n'ont été attribuées à aucun VLAN.
- **le VLAN natif** correspond au VLAN dans lequel sont affectées les trames non marquées circulant sur un *trunk* (il s'agit généralement aussi du VLAN 1). Il est souvent utilisé pour par les commutateurs pour s'échanger des informations nécessaires au fonctionnement de certains services (par exemple STP, CDP et VTP).

Configuration des VLAN

Une mauvaise configuration du VLAN natif sur les commutateurs peut avoir plusieurs impacts sur la sécurité du SI :

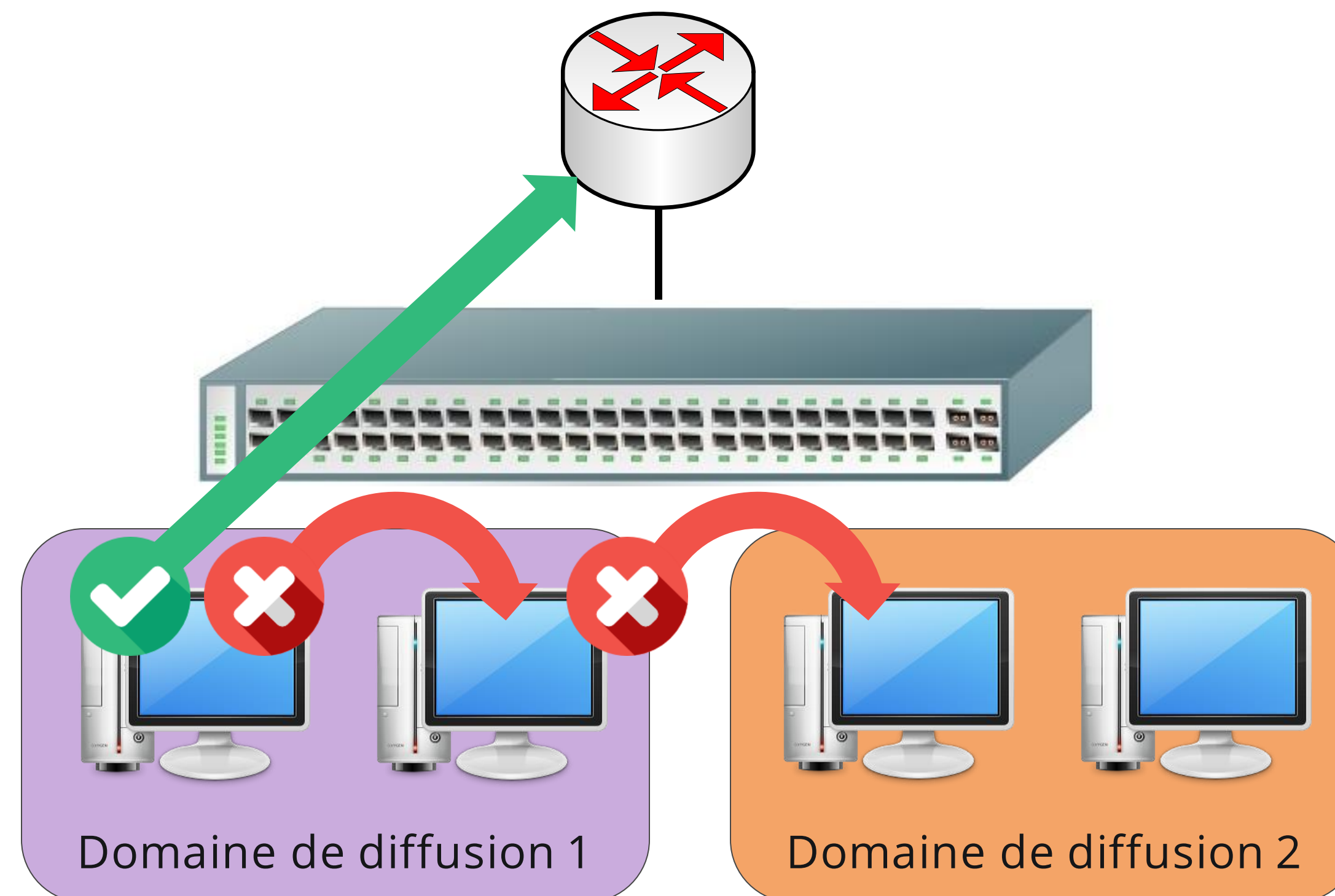
- En configuration par défaut, un terminal se connectant à un port non configuré a accès à tout le trafic circulant sur le VLAN natif et peut donc attaquer certains services l'utilisant ;
- Si des commutateurs d'un même domaine de diffusion sont configurés avec comme VLAN natif des numéros de VLAN différents, un phénomène de saut de VLAN peut se produire de manière permanente au niveau d'un port trunk ;
- Si un attaquant connecté à un port *trunk* du commutateur envoie une trame marquée deux fois avec comme premier marquage visible le numéro du VLAN natif et comme second marquage le VLAN de destination du paquet, un saut de VLAN peut se produire. Cependant, si cette attaque réussit, seul un sens de communication fonctionne, il n'y a pas de retour.



Risque

Private VLAN

Le PVLAN permet d'ajouter un niveau supplémentaire de cloisonnement en interdisant également les flux de communication entre les hôtes d'un même VLAN à l'exception d'un port défini comme un port ascendant (*uplink port*).



Private VLAN

La VLAN primaire (celui d'origine) est divisés en sous-VLAN (dits secondaires). Ces derniers possèdent eux-aussi un numéro, ce qui permet de les propager au travers d'un lien 802.1q. Les ports définis dans les PVLAN peuvent être utilisés selon trois modes :

- **Promiscuité** : il peut communiquer avec tout ce qui fait partie du VLAN primaire ou d'un des VLAN secondaires (c'est le port ascendant).
- **Isolé** : le port ne peut communiquer qu'avec les ports en mode promiscuité.
- **Communautaire** : il communique avec les ports en mode promiscuité et ceux de sa communauté.

Private VLAN

Le mécanisme de **Protected Port** ou **Port Isolation** est semblable à celui du *Private VLAN isolated* au détail près qu'il n'agit qu'au niveau local d'un commutateur. Il permet d'interdire le trafic direct entre différents terminaux connectés au même commutateur, même si ceux-ci sont dans un même VLAN.

C'est un mode qui se retrouve souvent sur les points d'accès WiFi.



Contrôle d'accès & filtrage

802.1X

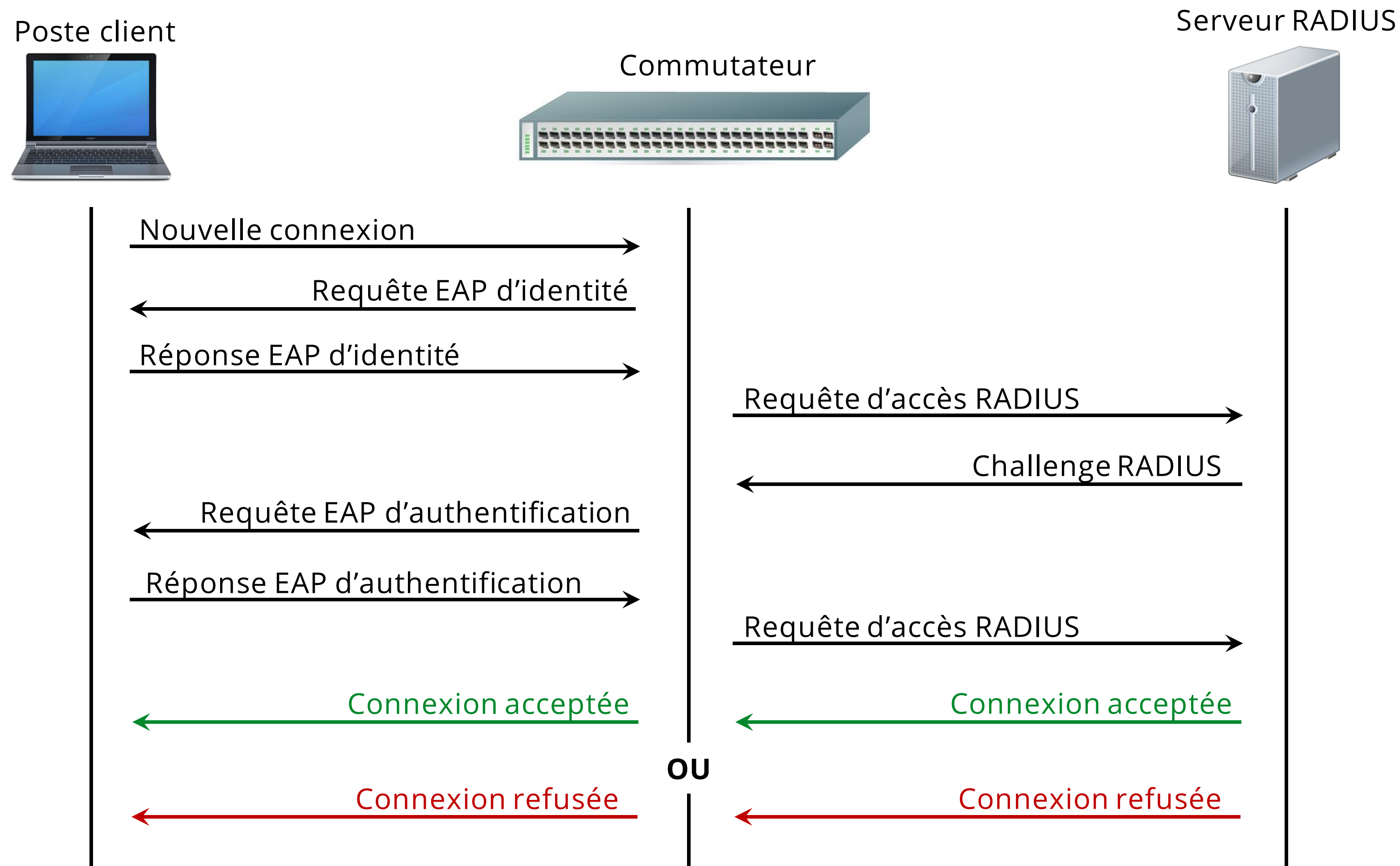
802.1X est un standard de l'IEEE conçu pour permettre la gestion des accès aux ports des équipements réseaux via un mécanisme d'authentification (*Network Access Control* ou **NAC**). Il définit comment encapsuler le protocole **EAP** (*Extensible Authentication Protocol*) au dessus d'un flux de niveau liaison (notamment 802.3 et 802.11). C'est pour cela qu'on le rencontre parfois sous la dénomination « *EAP over LAN* » ou **EAPOL**.

EAP

Trois briques de base sont nécessaires pour assurer une authentification EAP :

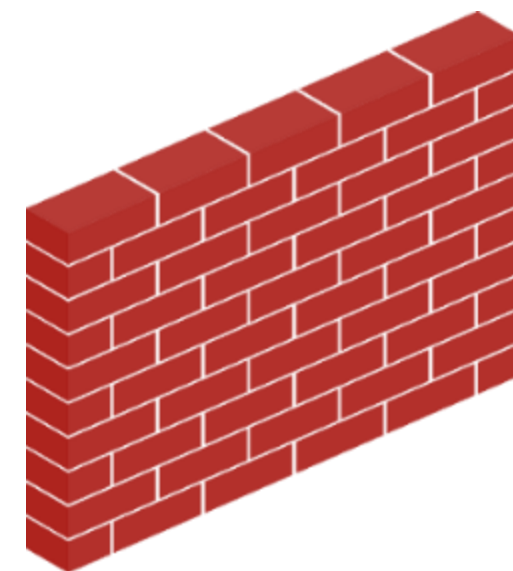
- Un **client** (*supplicant*) ; correspondant à l'entité qui souhaite accéder au réseau. Cette fonction est prise en charge par un logiciel installé sur le poste de travail ;
- Un **authentificateur** (*authenticator*) ; correspondant à l'équipement réseau qui assure les échange d'authentification de proximité avec le client et autorise ou non *in fine* l'accès au réseau ;
- Un **serveur d'authentification** ; auprès de qui le client réalise sont authentification. Il support le référentiel ou sert de mandataire pour un système tiers (RADIUS, TACACS, CAS, etc.).

EAP



Pare-feu

Le pare-feu est une solution logicielle ou matérielle, placé en rupture des flux de communication, dont l'objectif est de contrôler le trafic entre différentes zones de confiance du système d'information (incluant éventuellement Internet). Historiquement, il effectue un filtrage en fonction de critères relevant des **niveaux 3 et 4** du modèle OSI (adresses IP, nature des protocoles, ports sources et de destination, etc.).

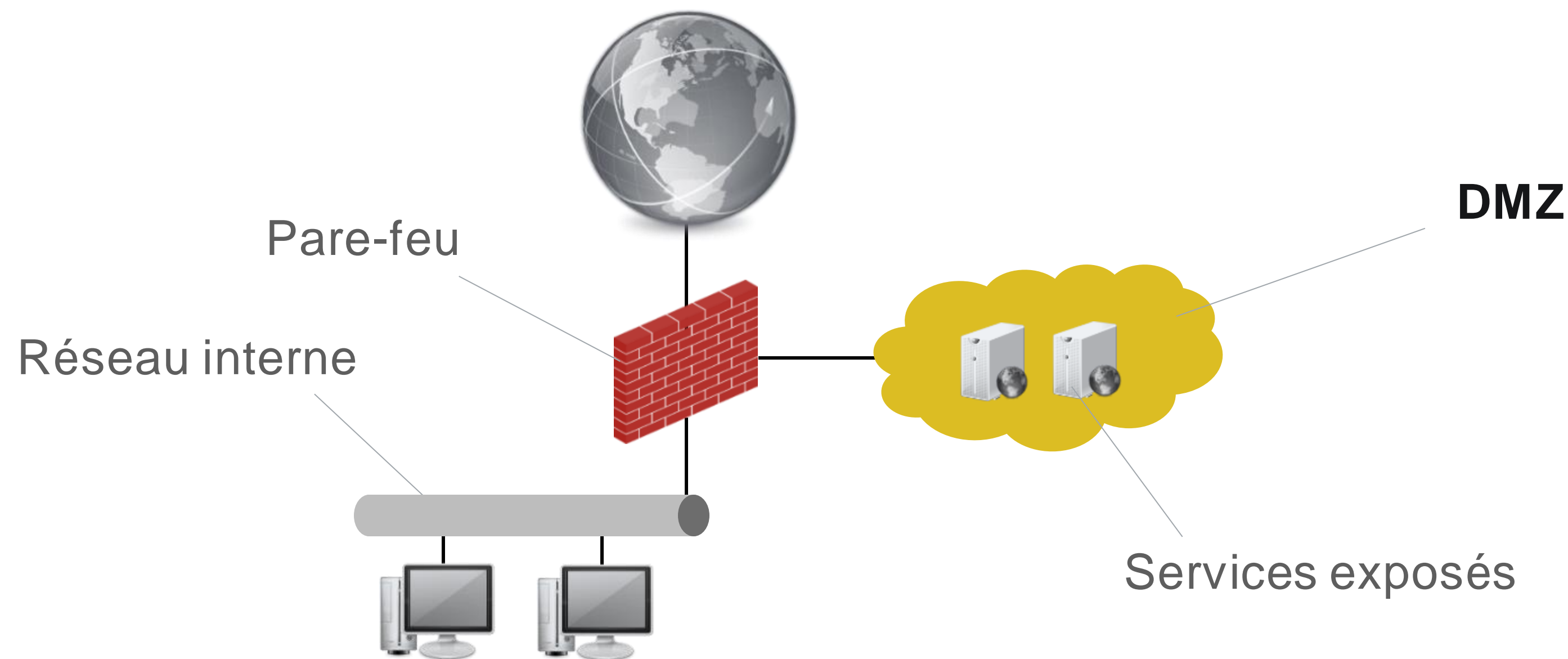


Il est considéré comme la pierre angulaire de la sécurité d'une infrastructure réseau.

Zoning

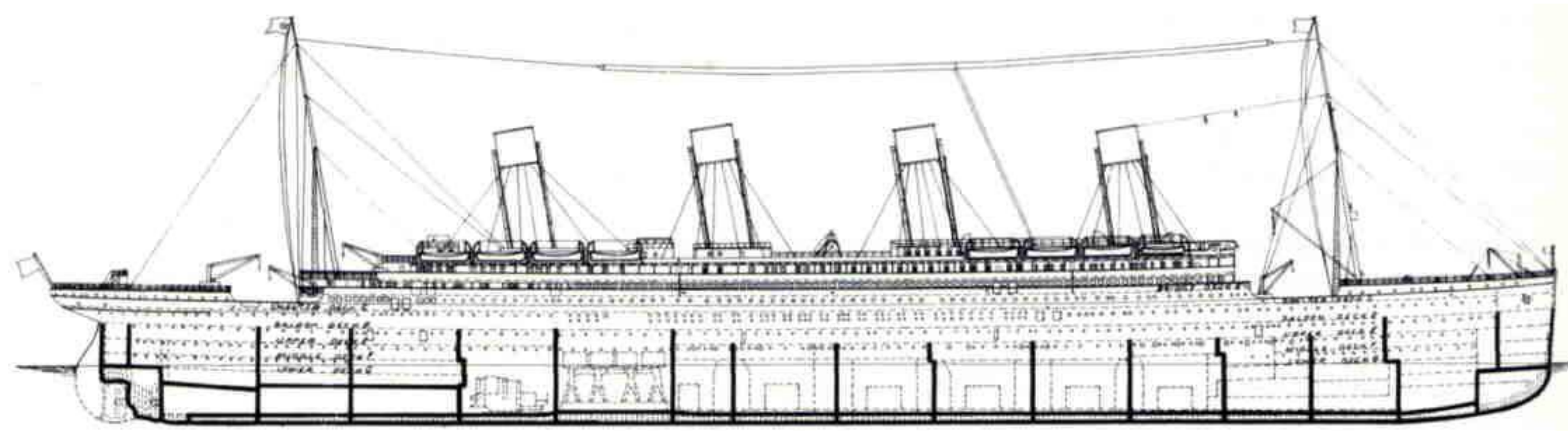
La DMZ

La zone démilitarisée (ou DMZ, de l'anglais *demilitarized zone*) est un sous-réseaux, isolé du réseau local, dont l'accès est contrôlé par un équipement de filtrage (un pare-feu traditionnellement). Son objectif est de servir de « tampon » entre deux zones présentant des niveaux de sécurité différents (Internet et le réseau interne par exemple).



La DMZ

Plusieurs DMZ peuvent (doivent) cohabiter au sein d'un système d'information. Elles sont utilisées pour effectuer un cloisonnement fonctionnel des services et permettre de réaliser un filtrage des communications. Elles sont au cœur de la mise en œuvre du principe de défense en profondeur dans la conception d'architectures sécurisées. A ce titre, elles peuvent être comparées aux compartiments étanches d'un bateau dont le but est de limiter l'impact d'une voie d'eau.



La DMZ

Le découpage en DMZ est tout un art et les critères sont très variables : nature des services, typologie des accès (externes, internes), protocoles utilisés, coût de mise en œuvre, facilité d'administration, etc.

Il existe toutefois quelques règles générales qui doivent présider à la conception d'architectures :

- Une même zone ne doit contenir que des équipements présentant des besoins de sécurité équivalents (DIC) ;
- Les accès à une zone doivent être contrôlés de manière stricte par un équipement de filtrage dédié ;
- Tout ce qui n'est pas explicitement autorisé (et nécessaire) est formellement interdit ;
- Seuls les flux initiés depuis une zone de confiance à destination d'une autre de moindre confiance sont autorisés. Ceux établis en sens inverse, quand ils n'existe pas d'alternative, doivent faire l'objet d'une vigilance accrue.

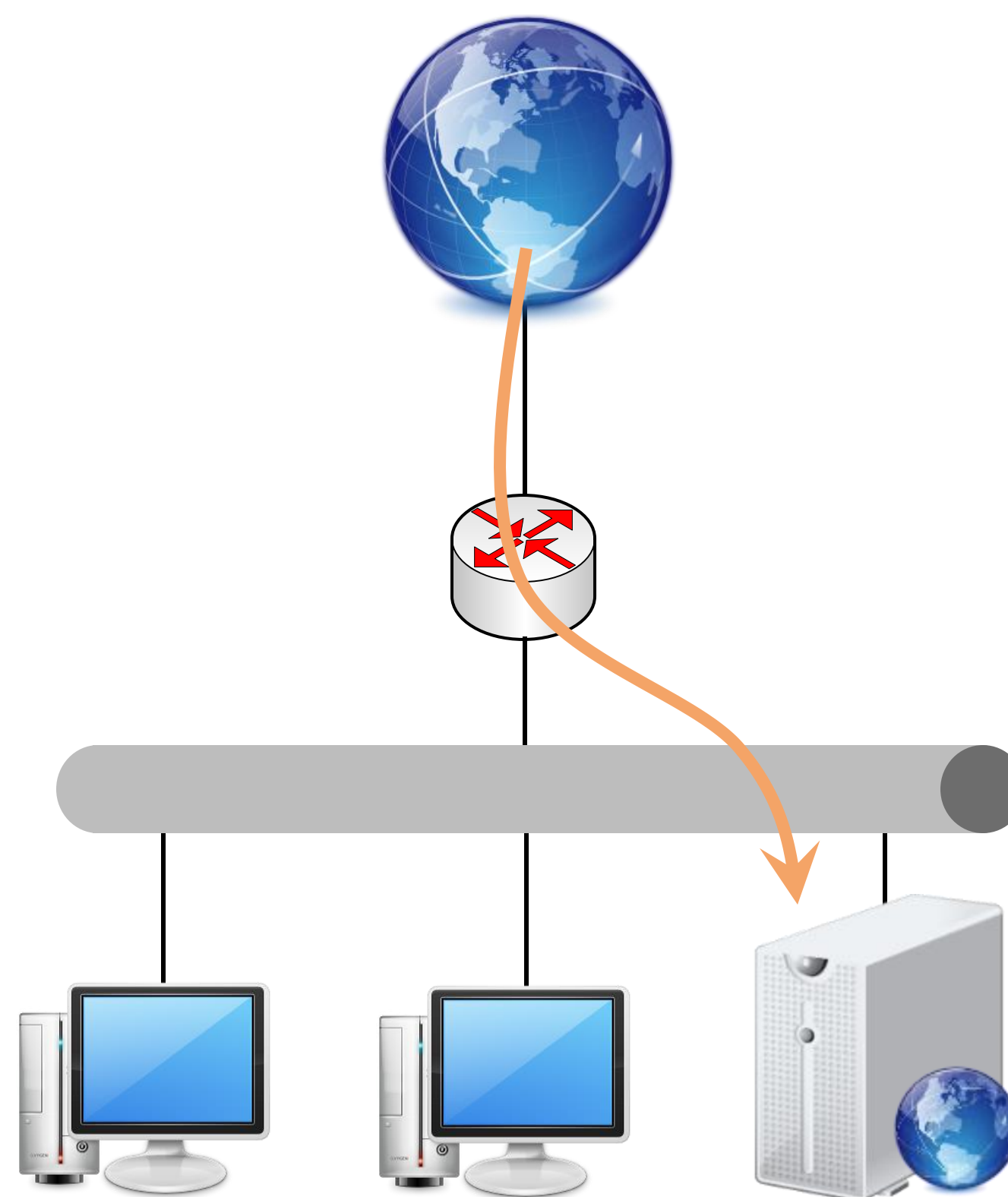
Réseau d'administration

Un réseau d'administration interconnecte, entre autres, les postes ou serveurs d'administration et les interfaces d'administration des équipements. Dans la logique de segmentation du réseau global de l'entité, il est indispensable de cloisonner spécifiquement le réseau d'administration, notamment vis-à-vis du réseau d'exploitation, pour se prémunir de toute compromission par rebond depuis un poste utilisateur vers une ressource d'administration.

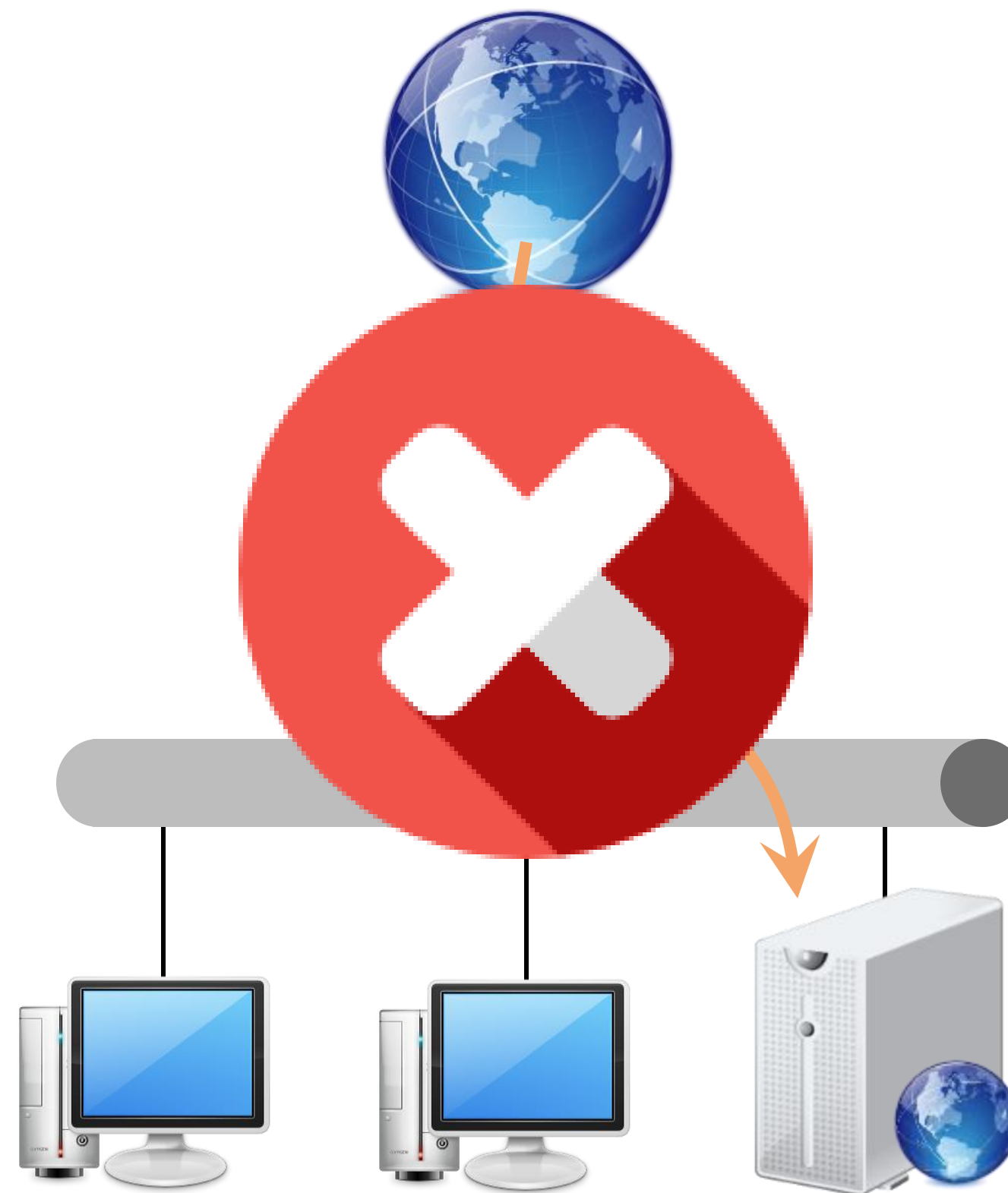
Dans l'idéal, les opérations d'administration ne sont réalisées directement depuis les postes de travail, mais en passant par un **bastion d'administration** qui prend en charge l'authentification (parfois forte) et surtout la traçabilité des opérations.

Cas d'usage

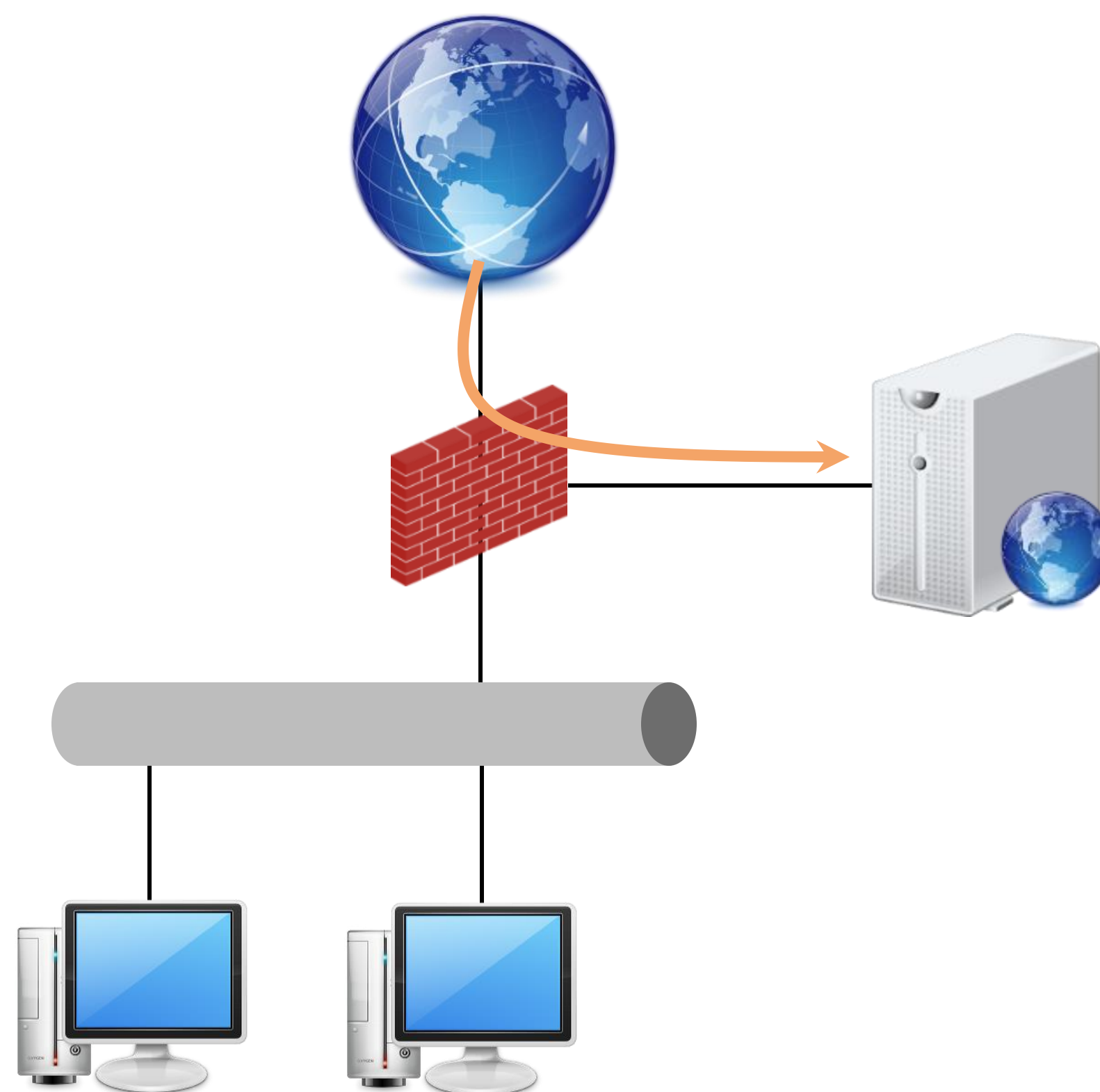
Hôte bastion



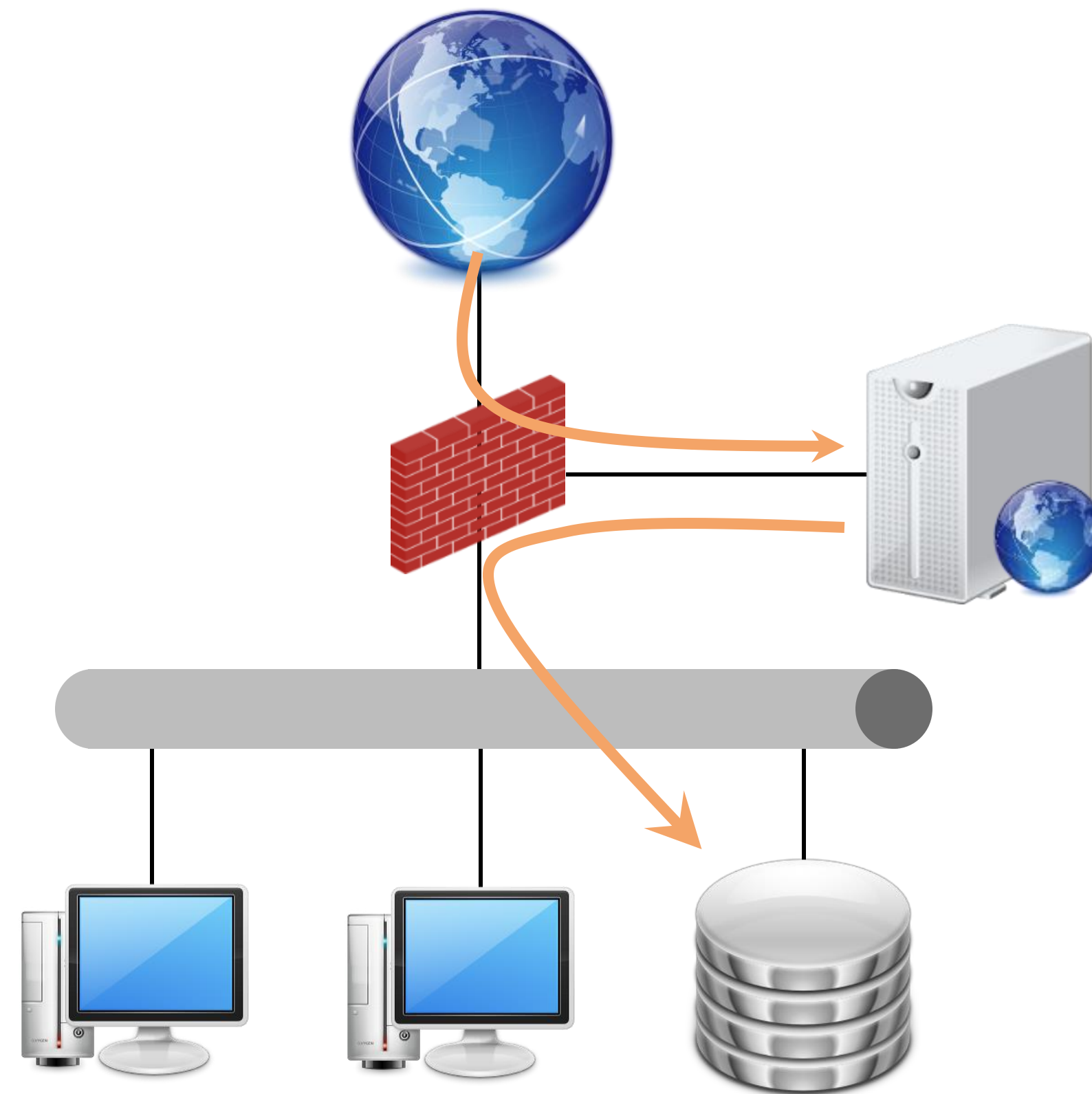
Hôte bastion



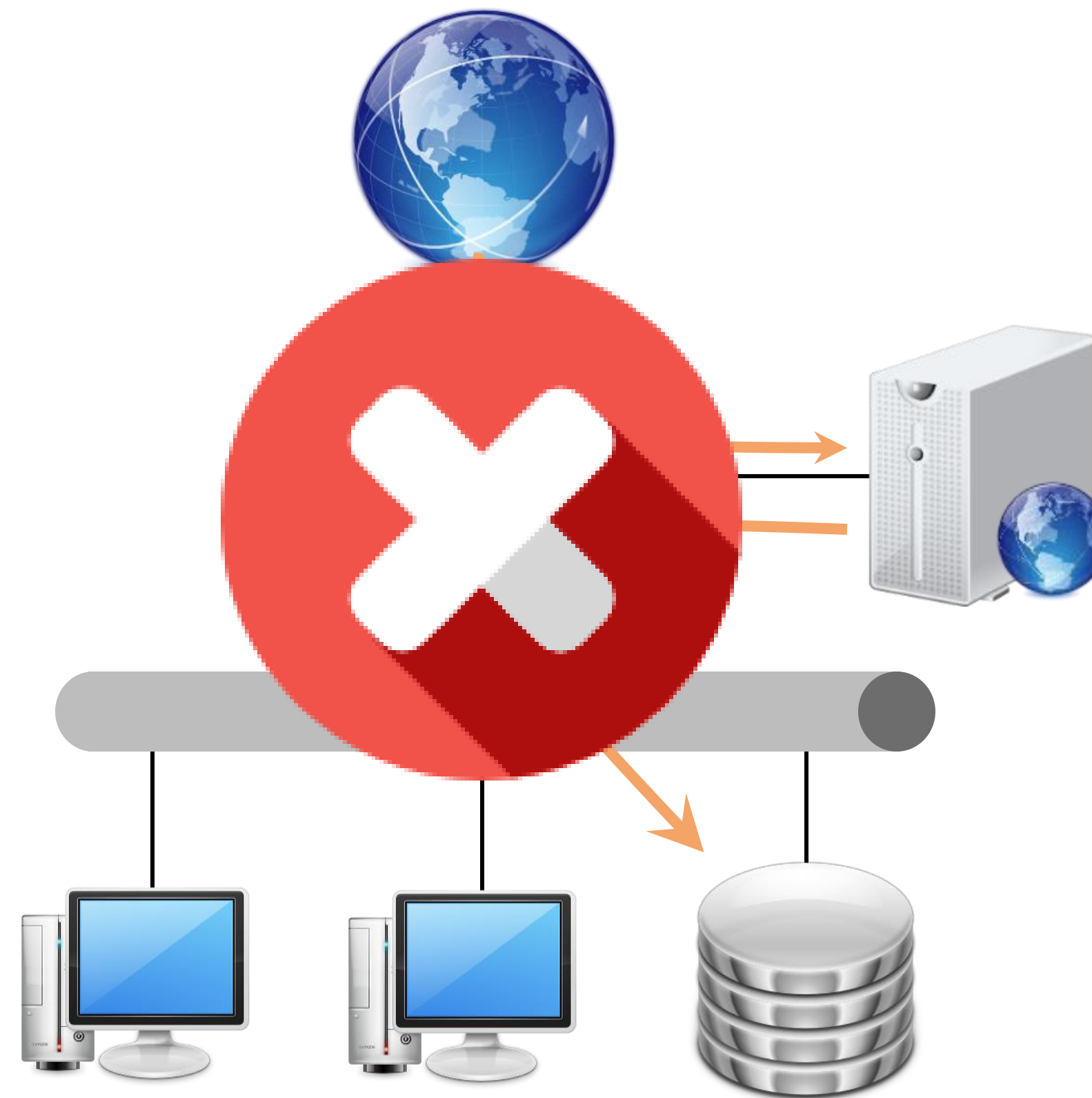
DMZ



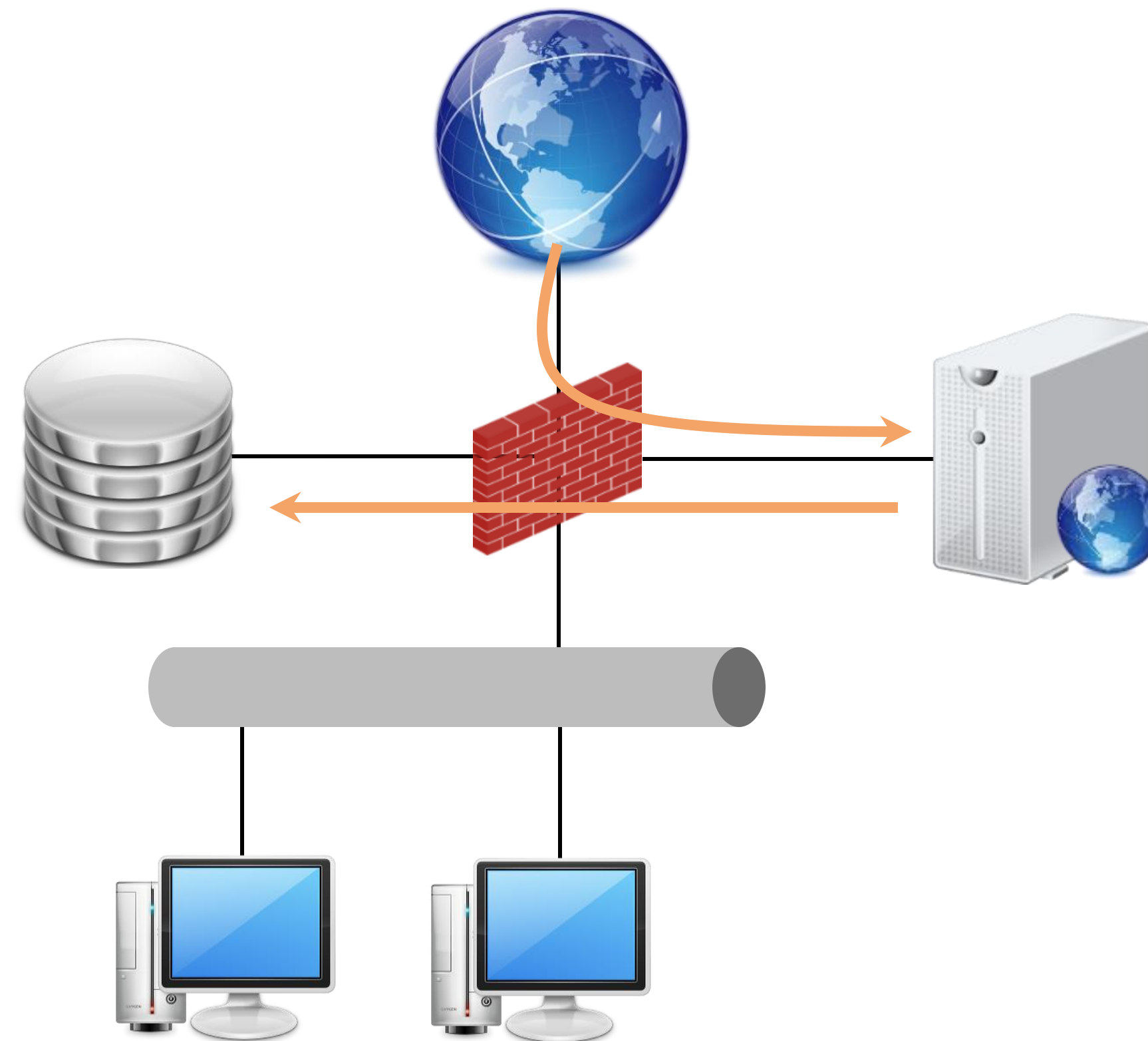
DMZ + base interne



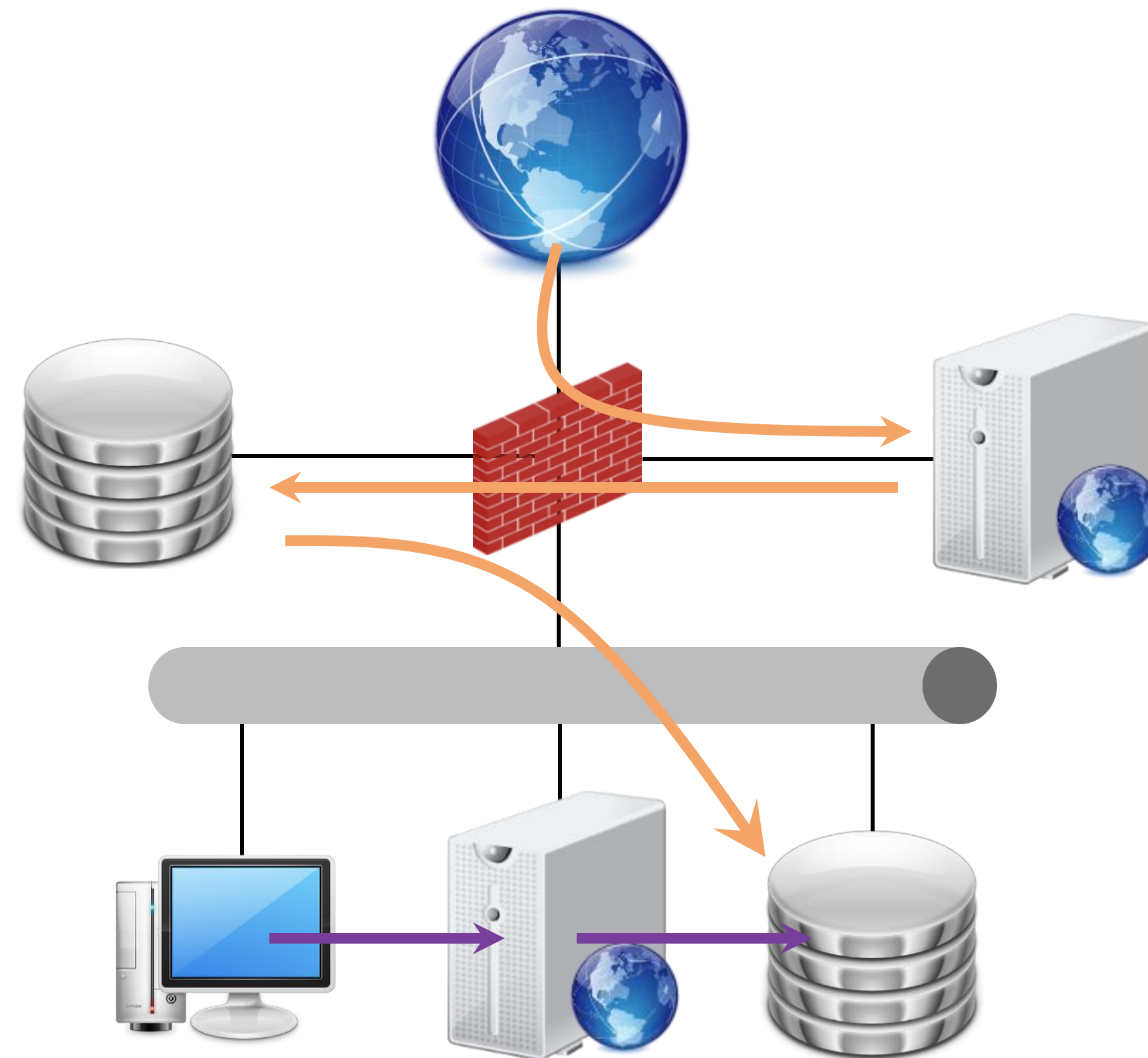
DMZ + base interne



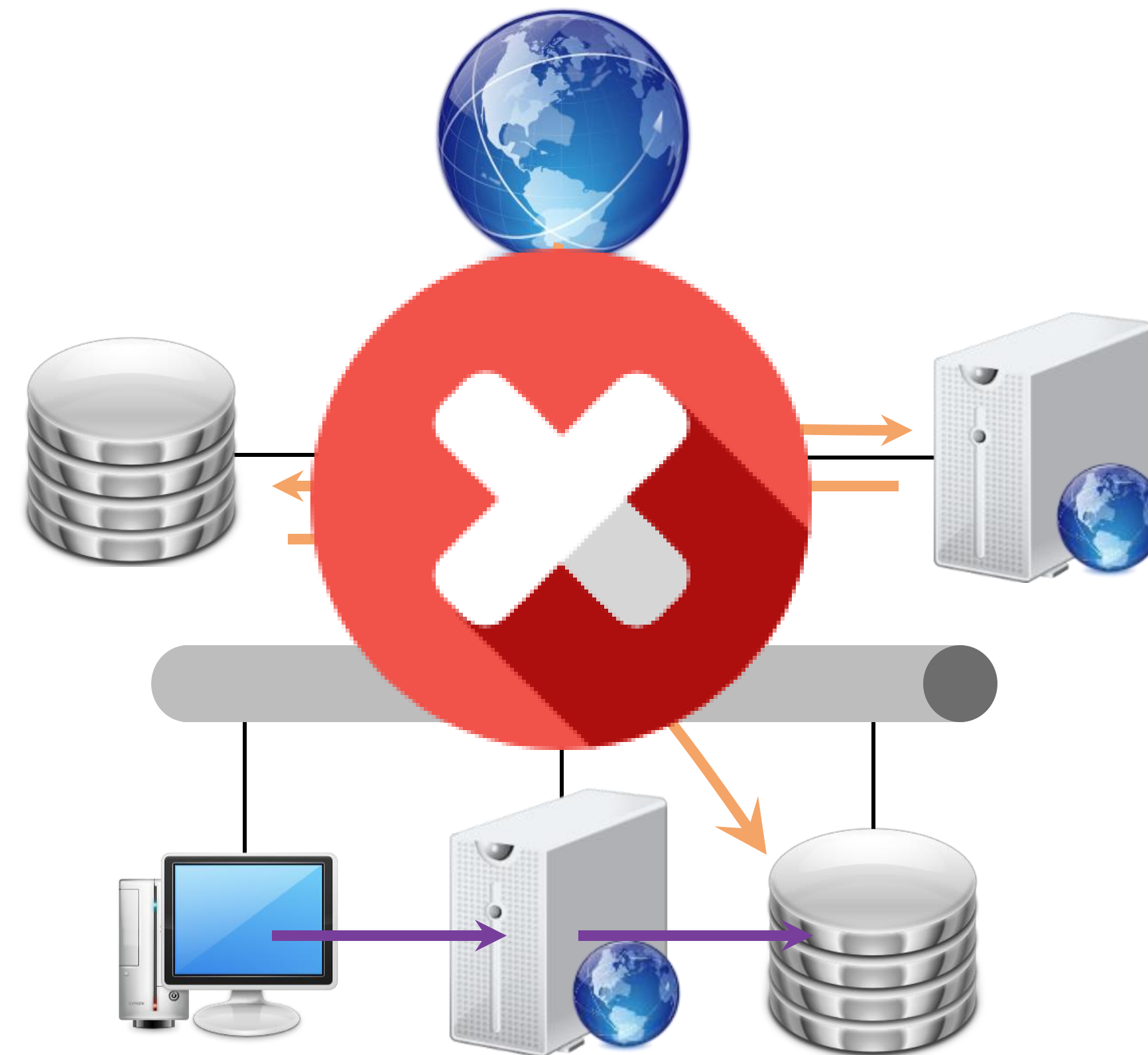
DMZ *everywhere*



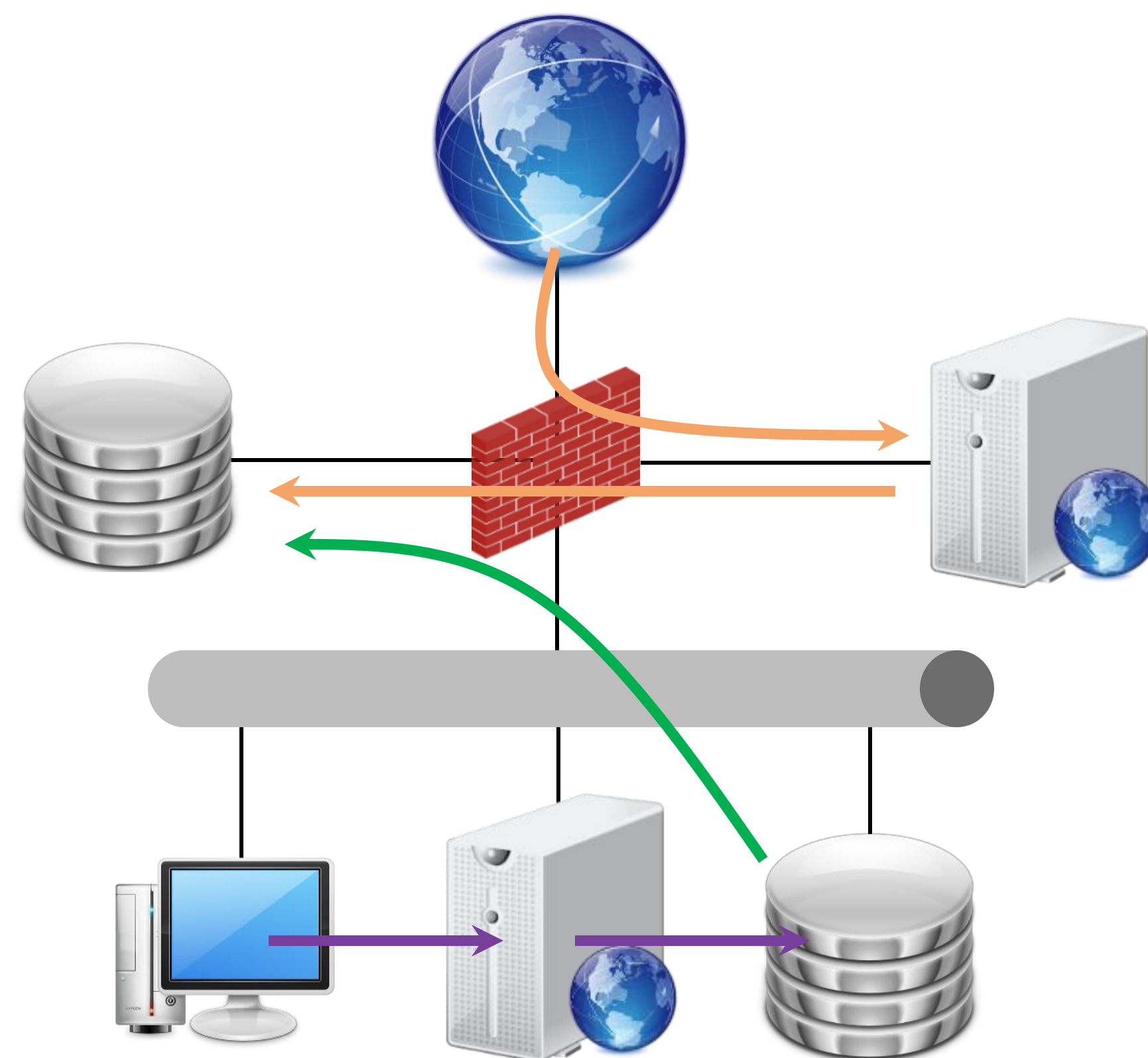
Synchronisation interne



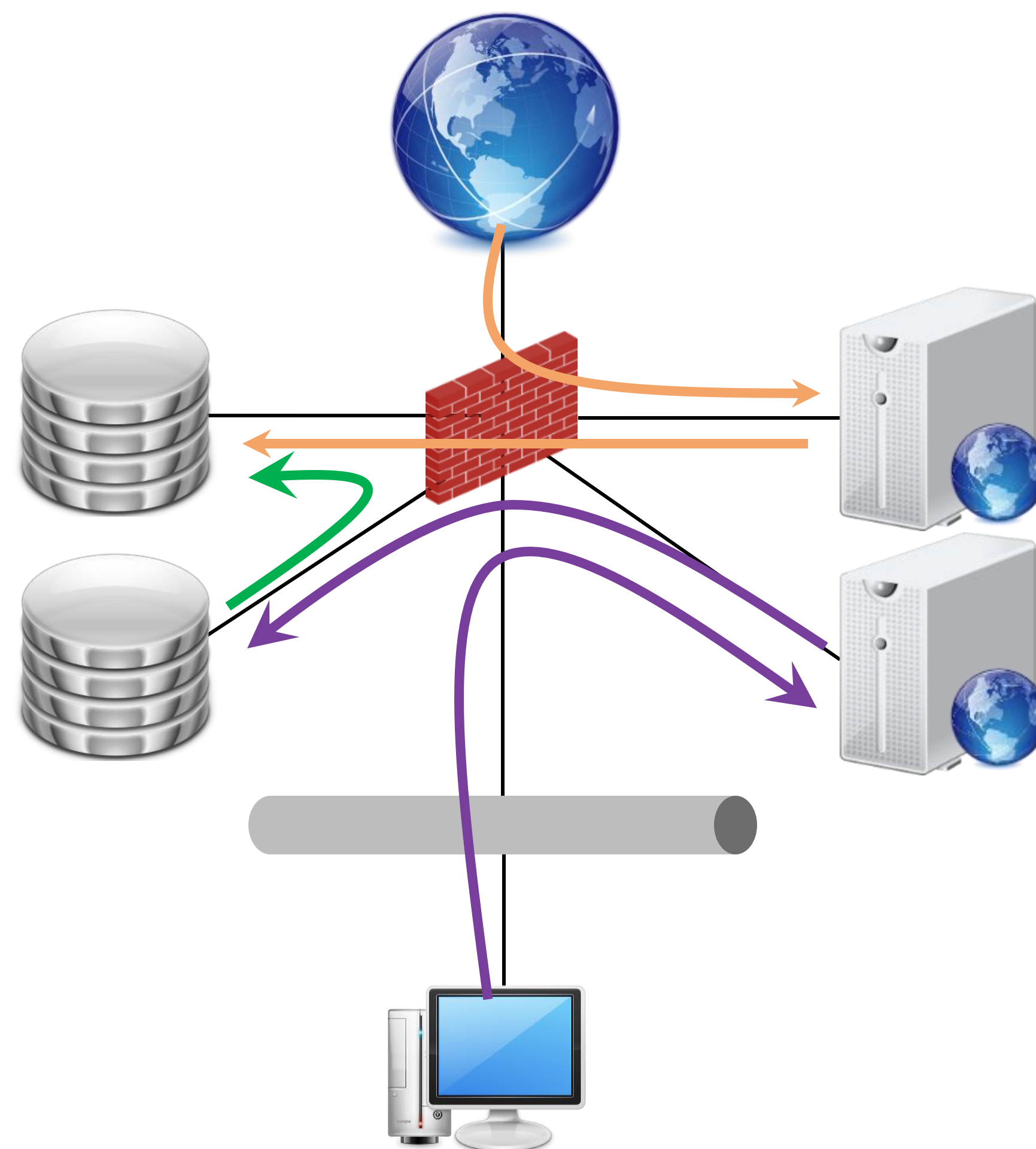
Synchronisation interne



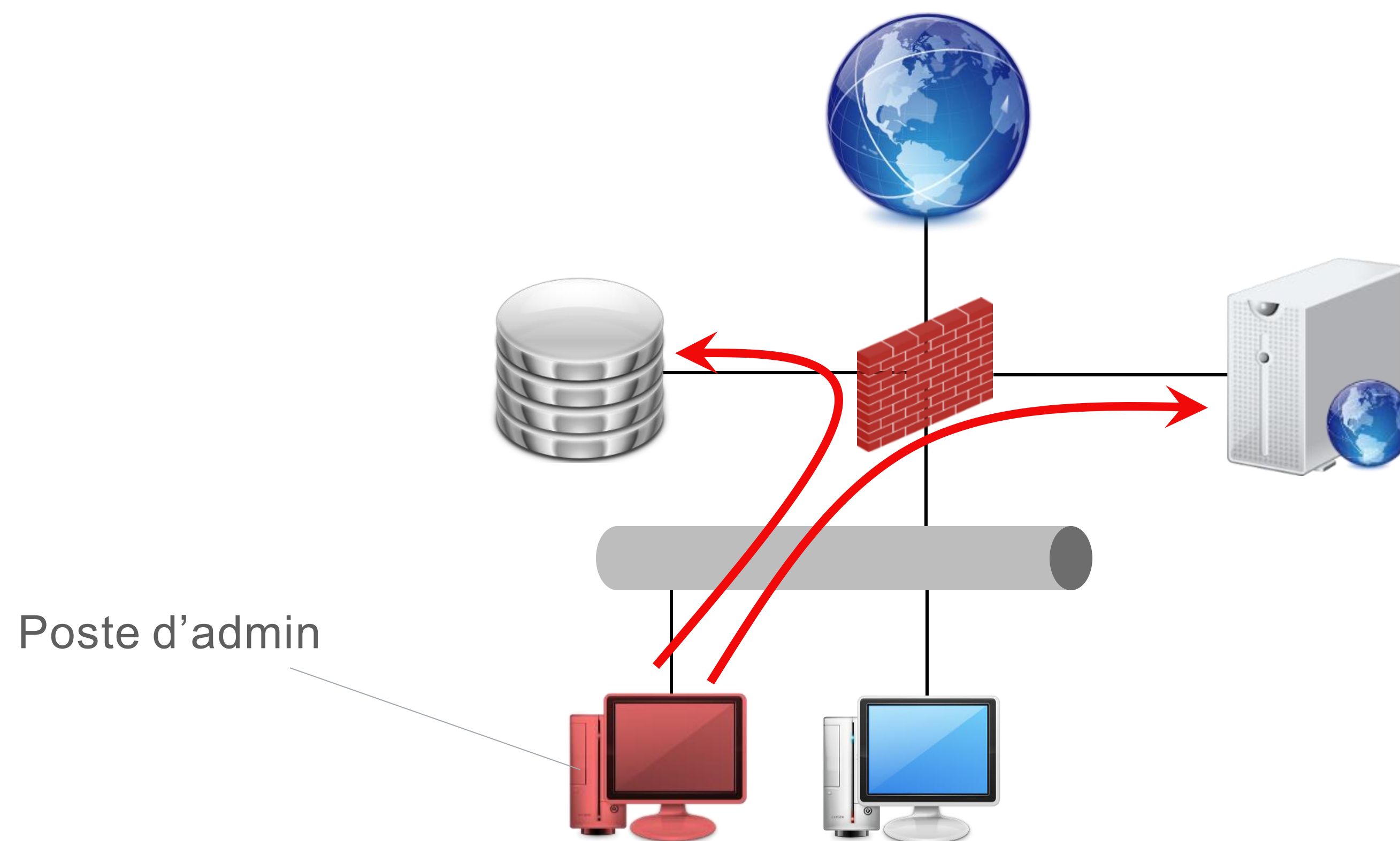
Synchronisation interne



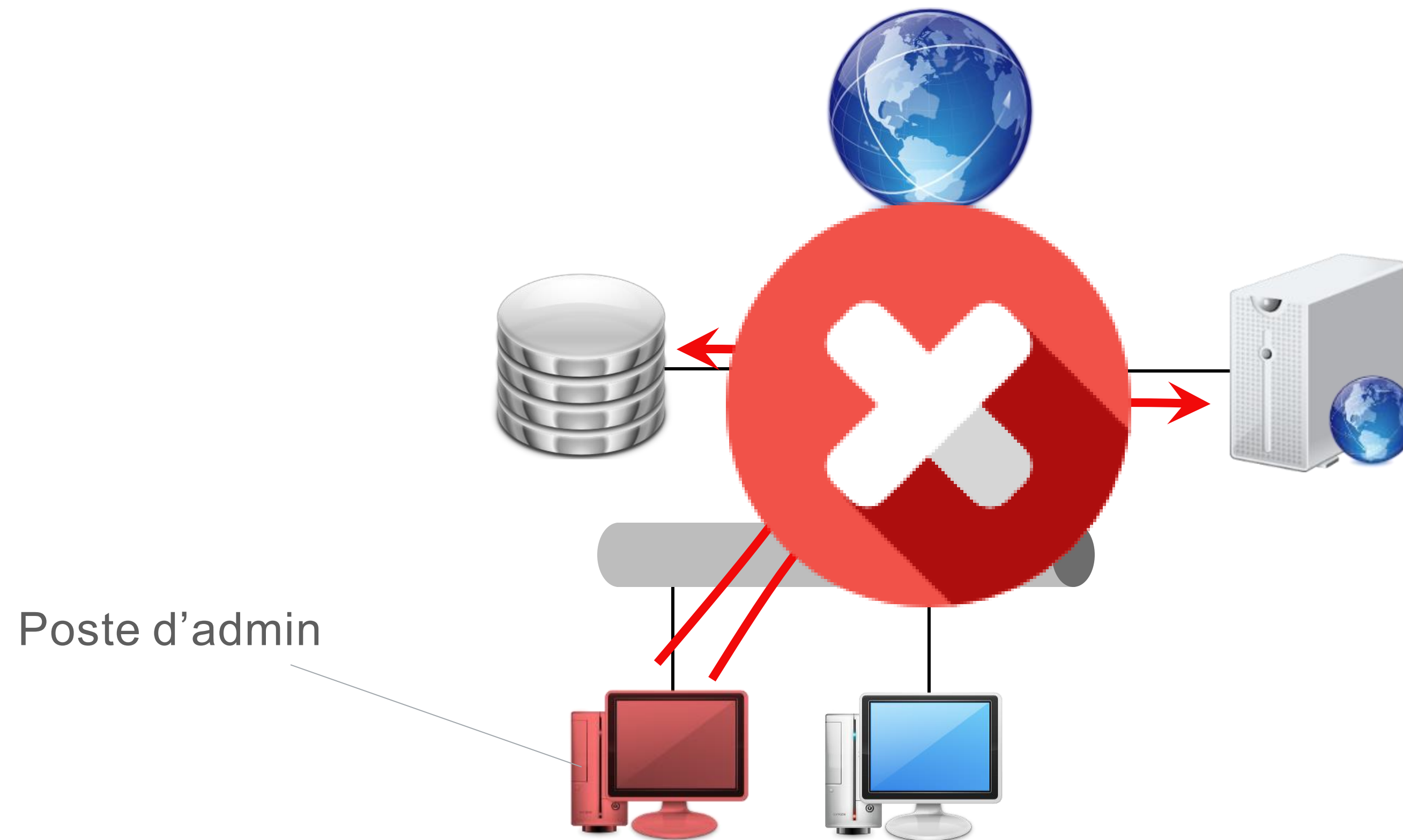
Synchronisation interne



Administration

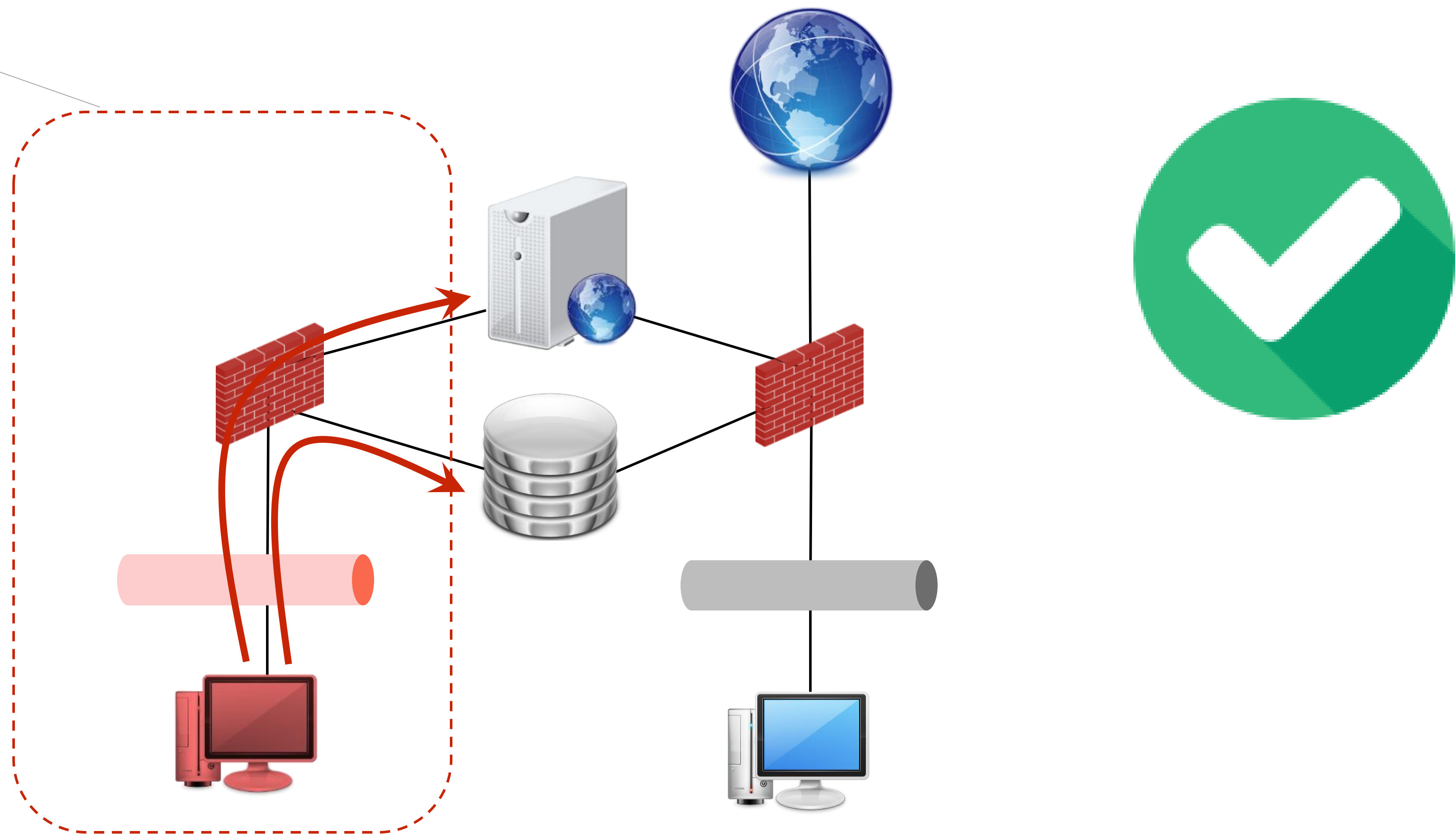


Administration



Administration

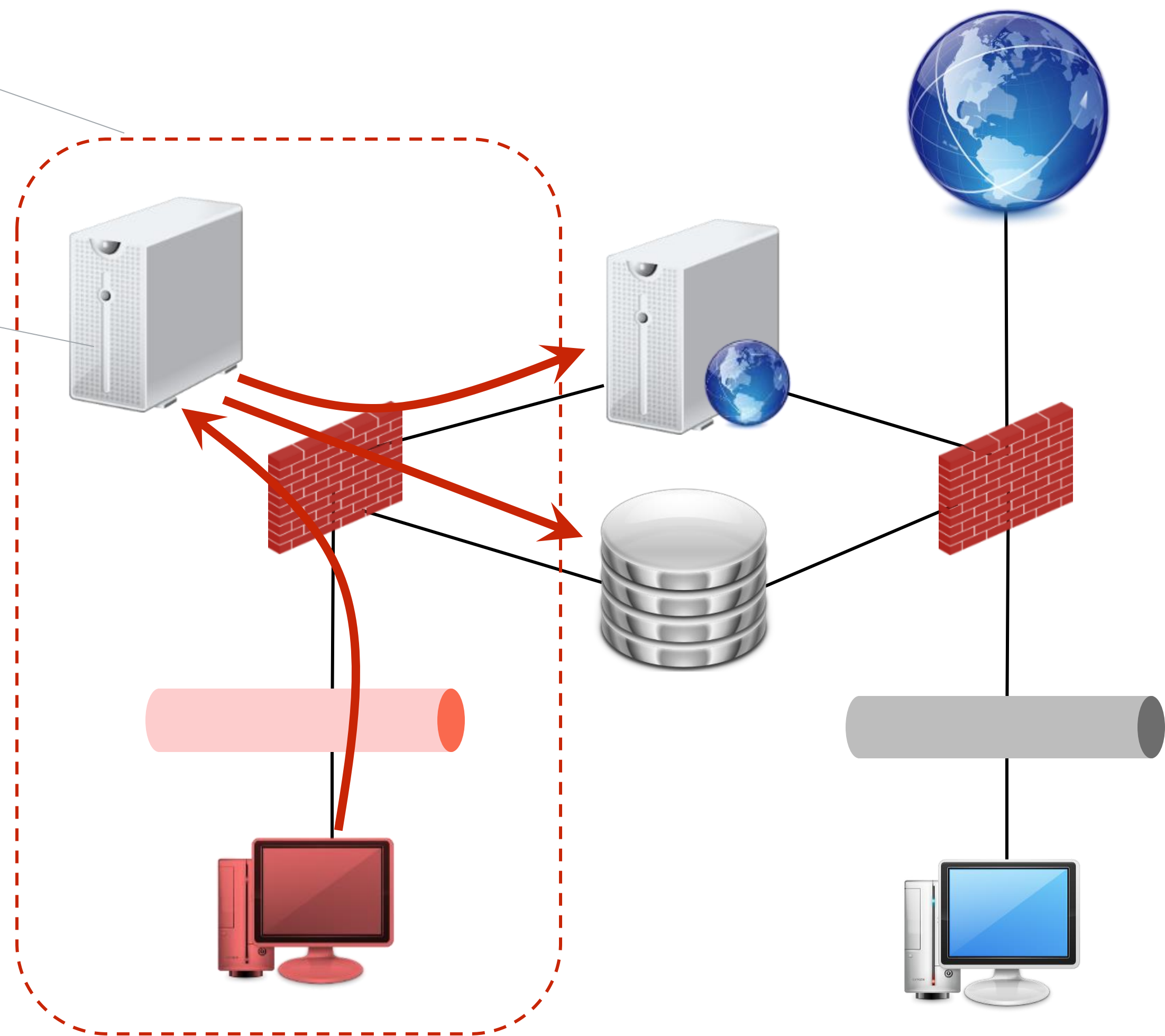
Réseau d'admin



Administration

Réseau d'admin

Bastion d'admin





Merci de votre attention.

Gwenn Feunteun

gwenn@acceis.fr

