Mécanismes de sécurité des systèmes

10e cours

Louis Salvail

Objectifs

Objectifs

- La sécurité des réseaux permet que les communications d'un système à un autre soient sûres.

Objectifs

- La sécurité des réseaux permet que les communications d'un système à un autre soient sûres.
- La sécurité des systèmes s'intéresse aux mécanismes qui évitent les intrusions.

Objectifs

- La sécurité des réseaux permet que les communications d'un système à un autre soient sûres.
- La sécurité des systèmes s'intéresse aux mécanismes qui évitent les intrusions.
- De tels mécanismes ont déjà été mentionnés : mots de passe, sécurité matérielle et biométrie.

Objectifs

- La sécurité des réseaux permet que les communications d'un système à un autre soient sûres.
- La sécurité des systèmes s'intéresse aux mécanismes qui évitent les intrusions.
- De tels mécanismes ont déjà été mentionnés : mots de passe, sécurité matérielle et biométrie.
  - Les mots de passe permettent aussi de se protéger contre les intrusions à partir d'un réseau.

Objectifs

- La sécurité des réseaux permet que les communications d'un système à un autre soient sûres.
- La sécurité des systèmes s'intéresse aux mécanismes qui évitent les intrusions.
- De tels mécanismes ont déjà été mentionnés : mots de passe, sécurité matérielle et biométrie.
  - Les mots de passe permettent aussi de se protéger contre les intrusions à partir d'un réseau.
- Nous allons maintenant voir d'autres méthodes qui protègent contre les intrusions à partir d'un réseau.

Objectifs

- La sécurité des réseaux permet que les communications d'un système à un autre soient sûres.
- La sécurité des systèmes s'intéresse aux mécanismes qui évitent les intrusions.
- De tels mécanismes ont déjà été mentionnés [illegible] de passe, sécurité matérielle et biométrie.
  - Les mots de passe permettent aussi d[illegible] contre les intrusions à partir d'un rése[illegible]
- Nous allons maintenant voir d'autres méthodes qui protègent contre les intrusions à partir d'un réseau.

voyons d'abord les types d'intrusions que nous voulons repousser!

Types d'attaques (I)

Types d'attaques (I)

- Cheval de Troie : Petit programme malveillant d'apparence anodine qui peut causer des dégâts une fois installé (virus classique, permettre de prendre le contrôle de l'ordinateur à distance).

Types d'attaques (I)

- Cheval de Troie : Petit programme malveillant d'apparence anodine qui peut causer des dégâts une fois installé (virus classique, permettre de prendre le contrôle de l'ordinateur à distance).
- Porte dérobée («backdoor») : Un point d'entrée dans un programme ou un système plus ou moins secret. Généralement une sécurité pour débloquer un code d'accès perdu ou pour le débogage. C'est aussi le point d'entrée des pirates. Ils peuvent même les créer pour les utiliser ultérieurement.

Types d'attaques (I)

- Cheval de Troie : Petit programme malveillant d'apparence anodine qui peut causer des dégâts une fois installé (virus classique, permettre de prendre le contrôle de l'ordinateur à distance).
- Porte dérobée («backdoor») : Un point d'entrée dans un programme ou un système plus ou moins secret. Généralement une sécurité pour débloquer un code d'accès perdu ou pour le débogage. C'est aussi le point d'entrée des pirates. Ils peuvent même les créer pour les utiliser ultérieurement.
- Reniflage («sniffing») : Écouter une ligne de transmission par laquelle transitent des données pour les récupérer à la volée. Cette technique peut être utilisée à l'interne pour le débogage ou de manière abusive par un pirate cherchant, par exemple, à se procurer un mot de passe. Vise surtout à intercepter les données non chiffrées. Dans certains réseaux (non commutés, reliés par «hub» [concentrateur reliant plusieurs ordinateurs d'un réseau] ou câbles coaxiaux), l'ensemble des messages est transmis à tous. En changeant l'état de l'interface réseau (c.-à-d. mode espion, «promiscuous mode»), l'adversaire peut intercepter toutes les communications pour les analyser.

Types d'attaques (I)

- Cheval de Troie : Petit programme malveillant d'apparence anodine qui peut causer des dégâts une fois installé (virus classique, permettre de prendre le contrôle de l'ordinateur à distance).
- Porte dérobée («backdoor») : Un point d'entrée dans un programme ou un système plus ou moins secret. Généralement une sécurité pour débloquer un code d'accès perdu ou pour le débogage. C'est aussi le point d'entrée des pirates. Ils peuvent même les créer pour les utiliser ultérieurement.
- Reniflage («sniffing») : Écouter une ligne de transmission par laquelle transitent des données pour les récupérer à la volée. Cette technique peut être utilisée à l'interne pour le débogage ou de manière abusive par un pirate cherchant, par exemple, à se procurer un mot de passe. Vise surtout à intercepter les données non chiffrées. Dans certains réseaux (non commutés, reliés par «hub» [concentrateur reliant plusieurs ordinateurs d'un réseau] ou câbles coaxiaux), l'ensemble des messages est transmis à tous. En changeant l'état de l'interface réseau (c.-à-d. mode espion, «promiscuous mode»), l'adversaire peut intercepter toutes les communications pour les analyser.
- Mystification («spoofing») : Technique d'intrusion consistant à envoyer à un serveur des paquets qui semblent provenir d'une adresse IP connue par le coupe-feu. La machine est rendue inatteignable par le pirate pour pouvoir intercepter les codes de communication et établir la liaison pirate.

Types d'attaques (I)

- Cheval de Troie : Petit programme malveillant d'apparence anodine qui peut causer des dégâts une fois installé (virus classique, permettre de prendre le contrôle de l'ordinateur à distance).
- Porte dérobée («backdoor») : Un point d'entrée dans un programme ou un système plus ou moins secret. Généralement une sécurité pour débloquer un code d'accès perdu ou pour le débogage. C'est aussi le point d'entrée des pirates. Ils peuvent même les créer pour les utiliser ultérieurement.
- Reniflage («sniffing») : Écouter une ligne de transmission par laquelle transitent des données pour les récupérer à la volée. Cette technique peut être utilisée à l'interne pour le débogage ou de manière abusive par un pirate cherchant, par exemple, à se procurer un mot de passe. Vise surtout à intercepter les données non chiffrées. Dans certains réseaux (non commutés, reliés par «hub» [concentrateur reliant plusieurs ordinateurs d'un réseau] ou câbles coaxiaux), l'ensemble des messages est transmis à tous. En changeant l'état de l'interface réseau (c.-à-d. mode espion, «promiscuous mode»), l'adversaire peut intercepter toutes les communications pour les analyser.
- Mystification («spoofing») : Technique d'intrusion consistant à envoyer à un serveur des paquets qui semblent provenir d'une adresse IP connue par le coupe-feu. La machine est rendue inatteignable par le pirate pour pouvoir intercepter les codes de communication et établir la liaison pirate.

Types d'attaques (I)

- Cheval de Troie : Petit programme malveillant d'apparence anodine qui peut causer des dégâts une fois installé (virus classique, permettre de prendre le contrôle de l'ordinateur à distance).
- Porte dérobée («backdoor») : Un point d'entrée dans un programme ou un système plus ou moins secret. Généralement une sécurité pour débloquer un code d'accès perdu ou pour le débogage. C'est aussi le point d'entrée des pirates. Ils peuvent même les créer pour les utiliser ultérieurement.
- Reniflage («sniffing») : Écouter une ligne de transmission par laquelle transitent des données pour les récupérer à la volée. Cette technique peut être utilisée à l'interne pour le débogage ou de manière abusive par un pirate cherchant, par exemple, à se procurer un mot de passe. Vise surtout à intercepter les données non chiffrées. Dans certains réseaux (non commutés, reliés par «hub» [concentrateur reliant plusieurs ordinateurs d'un réseau] ou câbles coaxiaux), l'ensemble des messages est transmis à tous. En changeant l'état de l'interface réseau (c.-à-d. mode espion, «promiscuous mode»), l'adversaire peut intercepter toutes les communications pour les analyser.

Usurpation

- Mystification («spoofing») : Technique d'intrusion consistant à envoyer à un serveur des paquets qui semblent provenir d'une adresse IP connue par le coupe-feu. La machine est rendue inatteignable par le pirate pour pouvoir intercepter les codes de communication et établir la liaison pirate.

Types d'attaques (II)

Types d'attaques (II)

- Attaque par rebond («bounce attack») : Menée via un autre ordinateur qui se retrouve complice involontaire. Cet ordinateur expédie des messages d'attaque à la victime, masquant l'identité du pirate.

Types d'attaques (II)

- Attaque par rebond («bounce attack») : Menée via un autre ordinateur qui se retrouve complice involontaire. Cet ordinateur expédie des messages d'attaque à la victime, masquant l'identité du pirate.
- Attaque de l'homme du milieu : Le pirate se place entre deux ordinateurs et se fait passer pour un afin d'obtenir le mot de passe de l'autre. Il peut alors se retourner contre le premier avec un mot de passe valide pour l'attaquer.

Types d'attaques (II)

- Attaque par rebond («bounce attack») : Menée via un autre ordinateur qui se retrouve complice involontaire. Cet ordinateur expédie des messages d'attaque à la victime, masquant l'identité du pirate.
- Attaque de l'homme du milieu : Le pirate se place entre deux ordinateurs et se fait passer pour un afin d'obtenir le mot de passe de l'autre. Il peut alors se retourner contre le premier avec un mot de passe valide pour l'attaquer.
- Déni de service («denial of service») : Une attaque cherchant à rendre un ordinateur hors service en le submergeant de trafic inutile. Par exemple, un serveur entièrement occupé à répondre à de fausses requêtes de connexion. Des machines peuvent être à l'origine de l'attaque généralement à l'insu de leur propriétaire.

Types d'attaques (II)

- Attaque par rebond («bounce attack») : Menée via un autre ordinateur qui se retrouve complice involontaire. Cet ordinateur expédie des messages d'attaque à la victime, masquant l'identité du pirate.
- Attaque de l'homme du milieu : Le pirate se place entre deux ordinateurs et se fait passer pour un afin d'obtenir le mot de passe de l'autre. Il peut alors se retourner contre le premier avec un mot de passe valide pour l'attaquer.
- Déni de service («denial of service») : Une attaque cherchant à rendre un ordinateur hors service en le submergeant de trafic inutile. Par exemple, un serveur entièrement occupé à répondre à de fausses requêtes de connexion. Des machines peuvent être à l'origine de l'attaque généralement à l'insu de leur propriétaire.
- Trébuchage sans fil («war-driving») : Dans le cas des réseaux sans fil. Consiste à circuler dans la ville avec un portable ou un assistant numérique personnel («PDA») pour repérer et pénétrer les réseaux locaux non protégés.

Prévention

Le nécessaire :

Prévention

Le nécessaire :

- Disposer d'une sauvegarde de ses données.

Prévention

Le nécessaire :

- Disposer d'une sauvegarde de ses données.
- Faire un audit des accès inutilement ouverts.

Prévention

Le nécessaire :

- Disposer d'une sauvegarde de ses données.
- Faire un audit des accès inutilement ouverts.
- Les comptes d'administration ont des mots de passe sécurisés.

Prévention

Le nécessaire :

- Disposer d'une sauvegarde de ses données.
- Faire un audit des accès inutilement ouverts.
- Les comptes d'administration ont des mots de passe sécurisés.
- Suppression des comptes utilisateurs non utilisés.

Prévention

Le nécessaire :

- Disposer d'une sauvegarde de ses données.
- Faire un audit des accès inutilement ouverts.
- Les comptes d'administration ont des mots de passe sécurisés.
- Suppression des comptes utilisateurs non utilisés.
- Désactiver les services (p. ex. internet) non utilisés sur les machines et supprimer les partages de fichiers qui ne sont pas nécessaires.

Prévention

Le souhaitable :

Prévention

Le souhaitable :

- Mettre à jour les logiciels à l'aide des dernières rustines («patches») de sécurité officielles pour fermer les brèches.

Prévention

Le souhaitable :

- Mettre à jour les logiciels à l'aide des dernières rustines («patches») de sécurité officielles pour fermer les brèches.
- Installer un coupe-feu.

Prévention

Le souhaitable :

- Mettre à jour les logiciels à l'aide des dernières rustines («patches») de sécurité officielles pour fermer les brèches.
- Installer un coupe-feu.
- Structurer les réseaux en zones étanches par activité et sensibilité (VLAN). Instituer un système de mots de passe. Isoler les serveurs Internet. VLAN : Virtual Local Area Network, regroupe les machines de façon logique et non physique.

Prévention

Le souhaitable :

- Mettre à jour les logiciels à l'aide des dernières rustines («patches») de sécurité officielles pour fermer les brèches.
- Installer un coupe-feu.
- Structurer les réseaux en zones étanches par activité et sensibilité (VLAN). Instituer un système de mots de passe. Isoler les serveurs Internet. VLAN : Virtual Local Area Network, regroupe les machines de façon logique et non physique.
- S'abonner aux lettres d'information («newsletters») de sécurité des différents fournisseurs.

Coupe-feu

Coupe-feu

- Un coupe-feu permet de couper l'accès à un réseau local. C'est le seul point d'accès à un réseau local à partir de l'extérieur.

Coupe-feu

- Un coupe-feu permet de couper l'accès à un réseau local. C'est le seul point d'accès à un réseau local à partir de l'extérieur.
- Les techniques que nous avons vues jusqu'à maintenant ne permettent pas d'éviter de communiquer avec des adversaires.

Coupe-feu

- Un coupe-feu permet de couper l'accès à un réseau local. C'est le seul point d'accès à un réseau local à partir de l'extérieur.
- Les techniques que nous avons vues jusqu'à maintenant ne permettent pas d'éviter de communiquer avec des adversaires.
    - Même si nous insistons pour faire un échange de clé authentifié avec quelqu'un, une certaine quantité d'information échangée avec des adversaires potentiels ne peut être évitée.

Coupe-feu

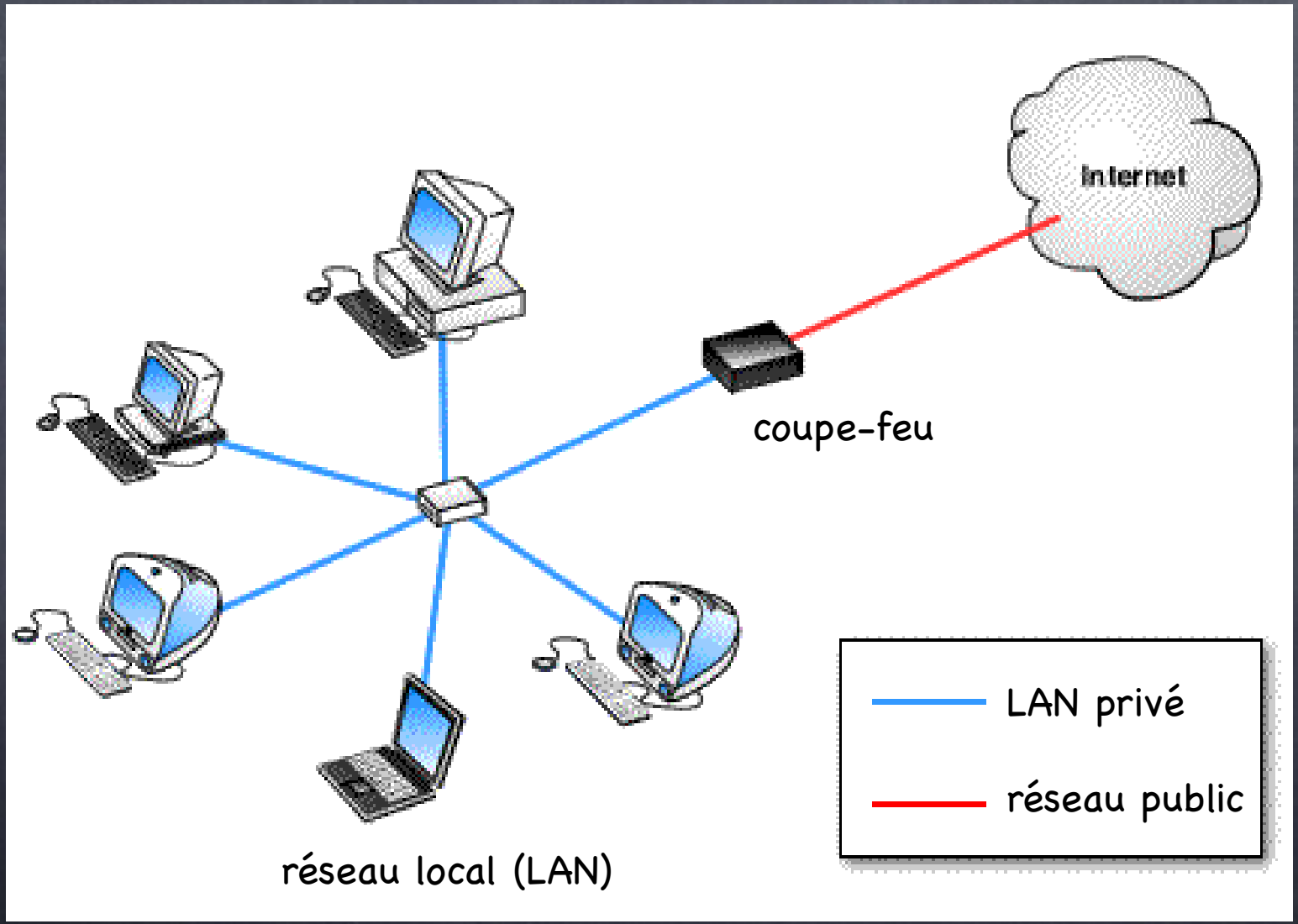
- Un coupe-feu permet de couper l'accès à un réseau local. C'est le seul point d'accès à un réseau local à partir de l'extérieur.
- Les techniques que nous avons vues jusqu'à maintenant ne permettent pas d'éviter de communiquer avec des adversaires.
  - Même si nous insistons pour faire un échange de clé authentifié avec quelqu'un, une certaine quantité d'information échangée avec des adversaires potentiels ne peut être évitée.
  - Ceci pourrait permettre à l'adversaire de pirater un ordinateur en utilisant une attaque par débordement de tampon.

Coupe-feu

- Un coupe-feu permet de couper l'accès à un réseau local. C'est le seul point d'accès à un réseau local à partir de l'extérieur.
- Les techniques que nous avons vues jusqu'à maintenant ne permettent pas d'éviter de communiquer avec des adversaires.
  - Même si nous insistons pour faire un échange de clé authentifié avec quelqu'un, une certaine quantité d'information échangée avec des adversaires potentiels ne peut être évitée.
  - Ceci pourrait permettre à l'adversaire de pirater un ordinateur en utilisant une attaque par débordement de tampon.
- Le concept du coupe-feu : L'adversaire ne peut attaquer un ordinateur avec lequel il ne communique pas!

L'aspect d'un coupe-feu

L'aspect d'un coupe-feu



Coupe-feu : filtrage de paquets

- Un coupe-feu est simplement une machine ou un logiciel qui arrête ou retire une partie de la circulation sur un réseau.
- Il est habituellement placé sur la connexion entre le réseau local et l'Internet. Le trafic de réseau doit donc passer par celui-ci pour relier le réseau local à l'Internet.
- La manière la plus simple d'utiliser un coupe-feu consiste à lui demander de couper toute communication qui tente de se connecter à une machine que vous ne voulez pas voir communiquer avec l'extérieur.

Filtrage de paquets : comment?

Filtrage de paquets : comment?

- Souvenons-nous que les connexions TCP demandent que des paquets spéciaux soient transmis et acceptés dans le but d'établir une connexion.

Filtrage de paquets : comment?

- Souvenons-nous que les connexions TCP demandent que des paquets spéciaux soient transmis et acceptés dans le but d'établir une connexion.
- Ces paquets sont faciles à reconnaître, car certains drapeaux («flags») seront activés. Les paquets suivants pourront être associés à une connexion établie précédemment.

Filtrage de paquets : comment?

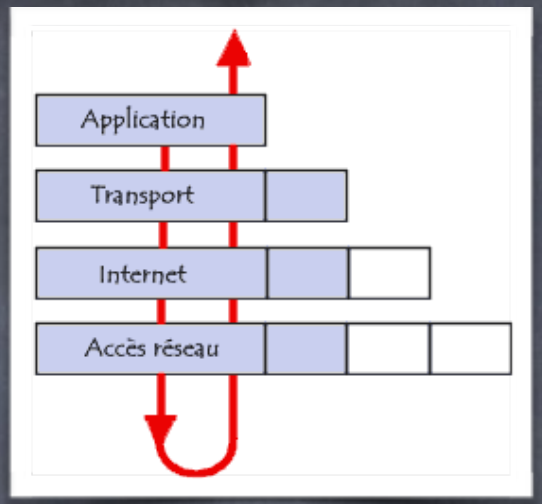
- Souvenons-nous que les connexions TCP demandent que des paquets spéciaux soient transmis et acceptés dans le but d'établir une connexion.
- Ces paquets sont faciles à reconnaître, car certains drapeaux («flags») seront activés. Les paquets suivants pourront être associés à une connexion établie précédemment.
- Le protocole UDP établit une communication sans être orienté connexion. Un paquet est transmis en espérant qu'il se rende à destination. L'UDP est utilisé pour communiquer avec les serveurs DNS qui traduisent les adresses sous une forme lisible en adresses IP.

Filtrage de paquets : comment?

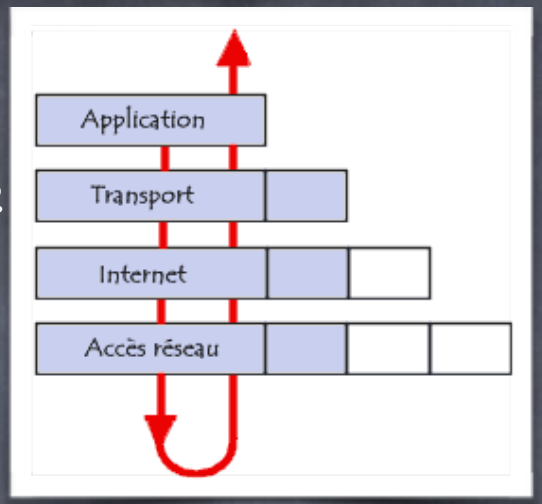
- Souvenons-nous que les connexions TCP demandent que des paquets spéciaux soient transmis et acceptés dans le but d'établir une connexion.
- Ces paquets sont faciles à reconnaître, car certains drapeaux («flags») seront activés. Les paquets suivants pourront être associés à une connexion établie précédemment.
- Le protocole UDP établit une communication sans être orienté connexion. Un paquet est transmis en espérant qu'il se rende à destination. L'UDP est utilisé pour communiquer avec les serveurs DNS qui traduisent les adresses sous une forme lisible en adresses IP.
- Le coupe-feu peut tout simplement éliminer les paquets établissant une connexion TCP sur une machine locale et tout le trafic UDP. Ceci est nommé filtrage simple des paquets.

Filtrage de paquets : comment?

Filtrage de paquets : comment?

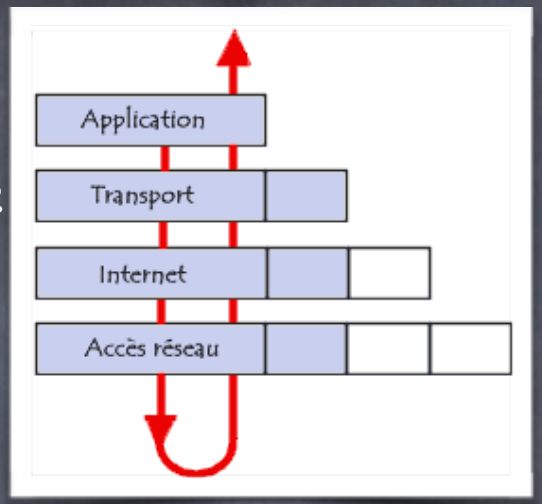


Filtrage de paquets : comment?



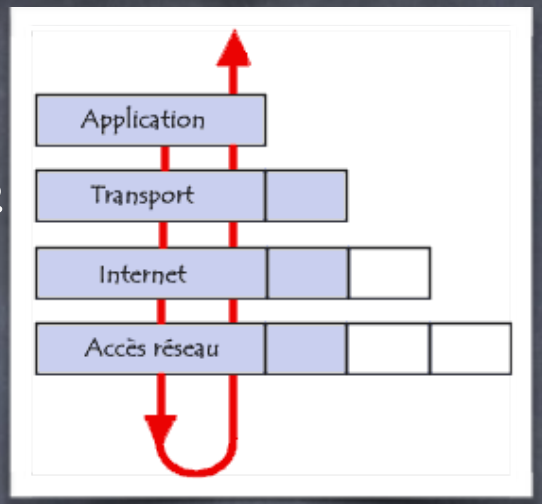
- Un coupe-feu par filtrage de paquets réside très bas dans la pile TCP/IP, au niveau Internet ou même Réseau. C'est la seule façon de s'assurer que tout ce qui va du réseau local ou vient de l'Internet sera observé.

Filtrage de paquets : comment?



- Un coupe-feu par filtrage de paquets réside très bas dans la pile TCP/IP, au niveau Internet ou même Réseau. C'est la seule façon de s'assurer que tout ce qui va du réseau local ou vient de l'Internet sera observé.
- Le filtrage des paquets peut être configuré par une politique qui détermine quels paquets seront bloqués ou autorisés.

Filtrage de paquets : comment?



- Un coupe-feu par filtrage de paquets réside très bas dans la pile TCP/IP, au niveau Internet ou même Réseau. C'est la seule façon de s'assurer que tout ce qui va du réseau local ou vient de l'Internet sera observé.
- Le filtrage des paquets peut être configuré par une politique qui détermine quels paquets seront bloqués ou autorisés.
- Il s'agit du coupe-feu original, le plus simple et le plus facile à réaliser. Il peut être très sûr, car il peut bloquer toute la circulation. Il est cependant nécessaire de permettre des accès, ce qui rend possibles certaines attaques.

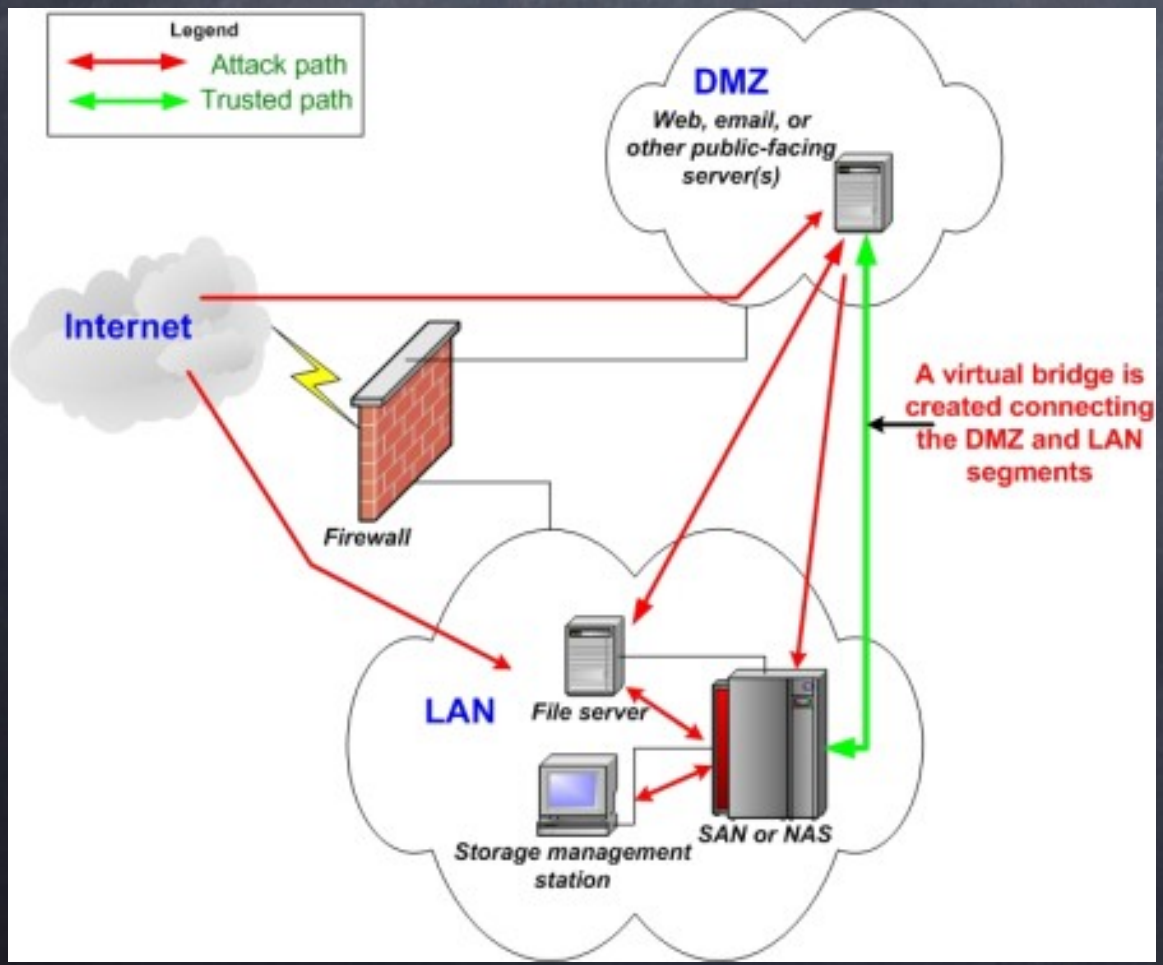
Les limites du filtrage de paquets

Les limites du filtrage de paquets

Évidemment, toutes les connexions ne peuvent être éliminées : les serveurs Web et de courriel doivent bien être autorisés à communiquer (ils ont besoin, entre autres choses, de communiquer avec le serveur DNS via UDP)!

Les limites du filtrage de paquets

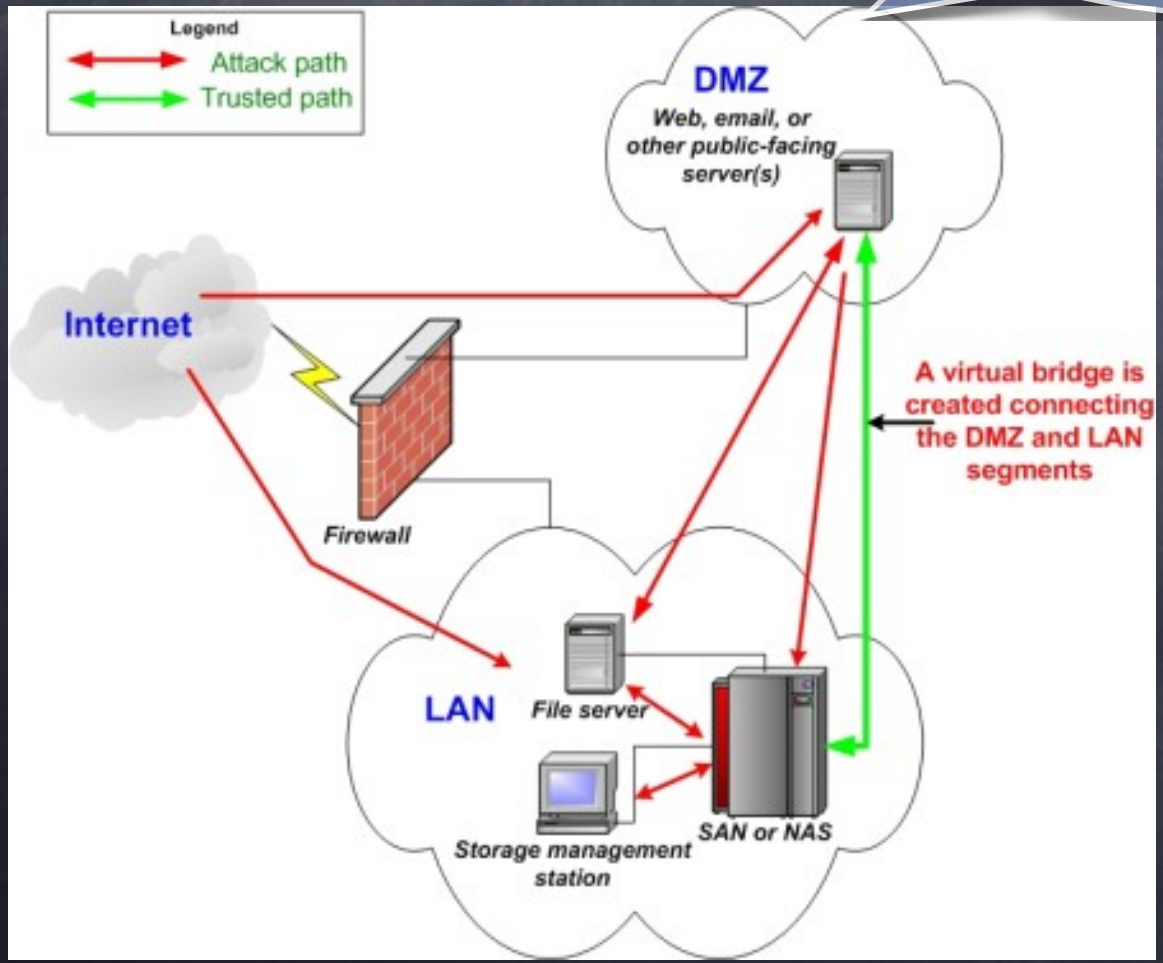
Évidemment, toutes les connexions ne peuvent être éliminées : les serveurs Web et de courriel doivent bien être autorisés à communiquer (ils ont besoin, entre autres choses, de communiquer avec le serveur DNS via UDP)!



Les limites du filtrage de paquets

Évidemment, toutes les connexions ne peuvent être éliminées : les serveurs Web et de courriel doivent bien être autorisés à communiquer (ils ont besoin, entre autres choses, de communiquer avec le serveur DNS via UDP)!

Nous pouvons déplacer ce serveur à l'extérieur, mais comment alors le mettre à jour?

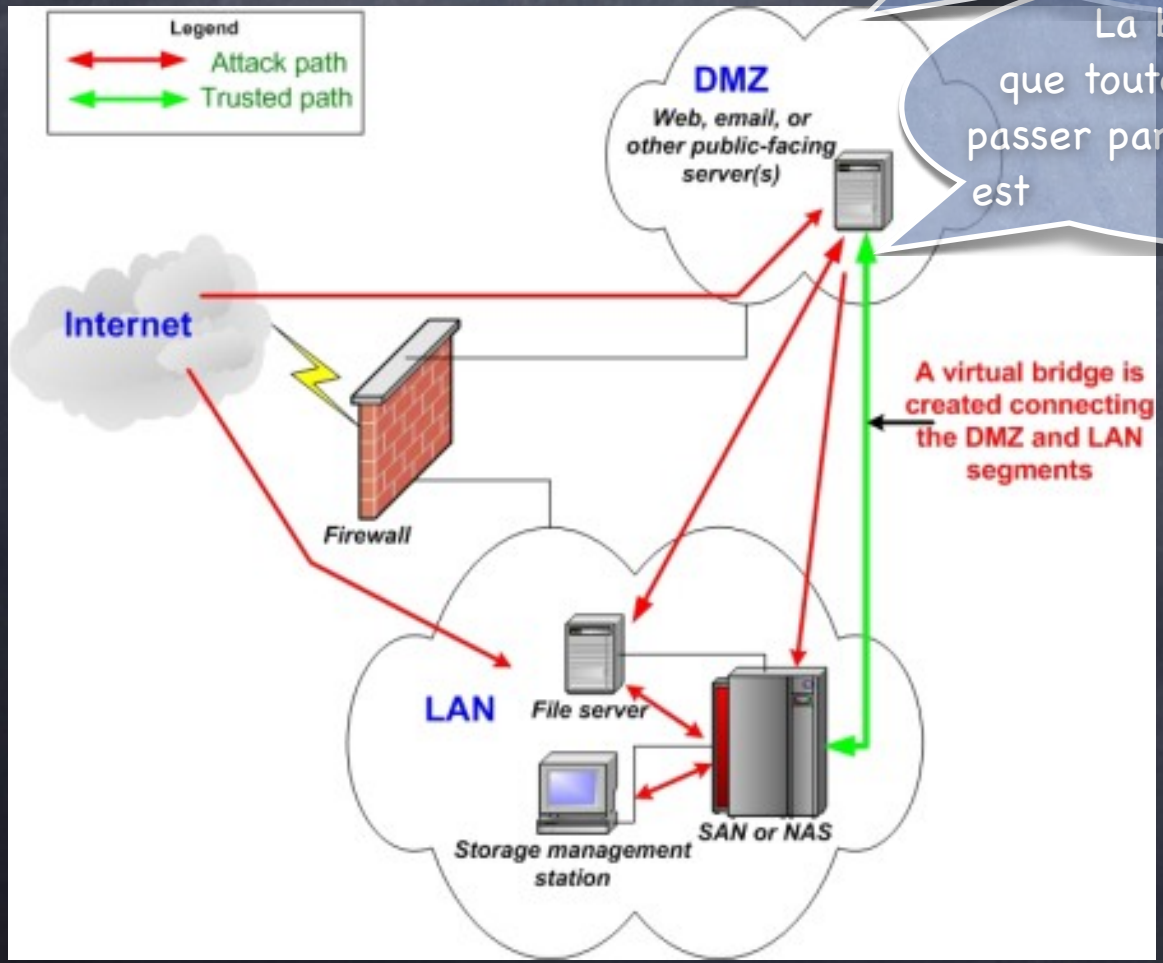


Les limites du filtrage de paquets

Évidemment, toutes les connexions ne peuvent être éliminées : les serveurs Web et de courriel doivent bien être autorisés à communiquer (ils ont besoin, entre autres choses, de communiquer avec le serveur DNS via UDP)!

Nous pouvons déplacer ce serveur à l'extérieur, mais comment alors le mettre à jour?

La bonne nouvelle est que toutes les attaques devront passer par ce serveur si le filtrage est strict!

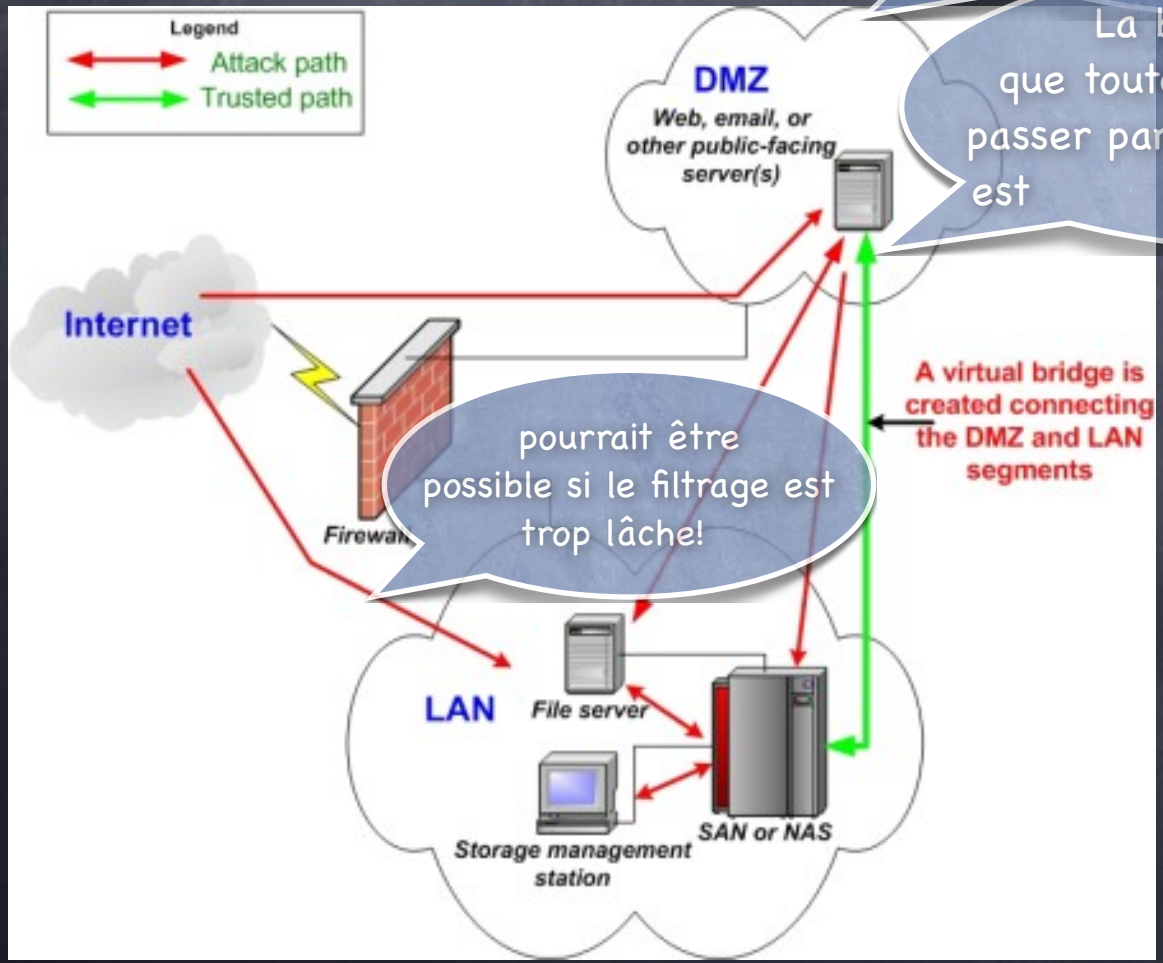


Les limites du filtrage de paquets

Évidemment, toutes les connexions ne peuvent être éliminées : les serveurs Web et de courriel doivent bien être autorisés à communiquer (ils ont besoin, entre autres choses, de communiquer avec le serveur DNS via UDP)!

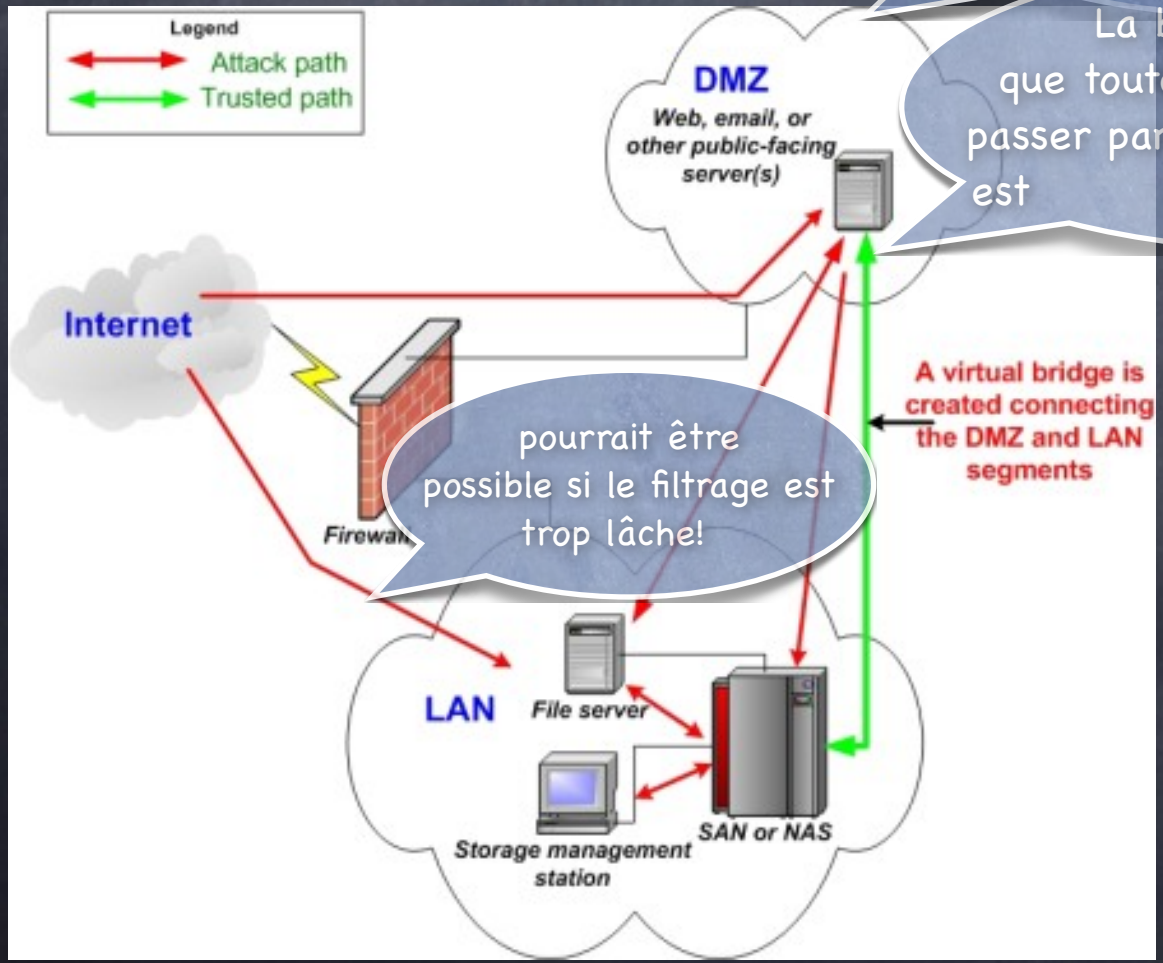
Nous pouvons déplacer ce serveur à l'extérieur, mais comment alors le mettre à jour?

La bonne nouvelle est que toutes les attaques devront passer par ce serveur si le filtrage est strict!



Les limites du filtrage de paquets

Évidemment, toutes les connexions ne peuvent être éliminées : les serveurs Web et de courriel doivent bien être autorisés à communiquer (ils ont besoin, entre autres choses, de communiquer avec le serveur DNS via UDP)!



Nous pouvons déplacer ce serveur à l'extérieur, mais comment alors le mettre à jour?

La bonne nouvelle est que toutes les attaques devront passer par ce serveur si le filtrage est strict!

pourrait être possible si le filtrage est trop lâche!

DMZ («Demilitarized zone») : une zone «démilitarisée» entre l'Internet et le réseau interne dans laquelle on peut placer les serveurs WEB accessibles depuis l'extérieur. La zone est munie d'un coupe-feu pour cette tâche. Les coupe-feu peuvent avoir une sortie DMZ pour le serveur Web.

Politiques de filtrage

Politiques de filtrage

- Souvenons-nous que les paquets contiennent les informations suivantes :

Politiques de filtrage

- Souvenons-nous que les paquets contiennent les informations suivantes :
  - les données,

Politiques de filtrage

- Souvenons-nous que les paquets contiennent les informations suivantes :
  - les données,
  - l'adresse IP d'origine et de destination (incluant le port de destination),

Politiques de filtrage

- Souvenons-nous que les paquets contiennent les informations suivantes :
  - les données,
  - l'adresse IP d'origine et de destination (incluant le port de destination),
  - l'information sur le protocole par lequel ils doivent être manipulés,

Politiques de filtrage

- Souvenons-nous que les paquets contiennent les informations suivantes :
  - les données,
  - l'adresse IP d'origine et de destination (incluant le port de destination),
  - l'information sur le protocole par lequel ils doivent être manipulés,
  - l'information sur des erreurs éventuelles et

Politiques de filtrage

- Souvenons-nous que les paquets contiennent les informations suivantes :
  - les données,
  - l'adresse IP d'origine et de destination (incluant le port de destination),
  - l'information sur le protocole par lequel ils doivent être manipulés,
  - l'information sur des erreurs éventuelles et
  - de l'information sur le type de données en transit.

Politiques de filtrage

- Souvenons-nous que les paquets contiennent les informations suivantes :
  - les données,
  - l'adresse IP d'origine et de destination (incluant le port de destination),
  - l'information sur le protocole par lequel ils doivent être manipulés,
  - l'information sur des erreurs éventuelles et
  - de l'information sur le type de données en transit.
- Un politique de filtrage énonce une liste d'autorisations et d'interdictions des types :

Politiques de filtrage

- Souvenons-nous que les paquets contiennent les informations suivantes :
  - les données,
  - l'adresse IP d'origine et de destination (incluant le port de destination),
  - l'information sur le protocole par lequel ils doivent être manipulés,
  - l'information sur des erreurs éventuelles et
  - de l'information sur le type de données en transit.
- Un politique de filtrage énonce une liste d'autorisations et d'interdictions des types :
  - autorise/interdit les paquets selon l'adresse IP d'origine/destination

Politiques de filtrage

- Souvenons-nous que les paquets contiennent les informations suivantes :
  - les données,
  - l'adresse IP d'origine et de destination (incluant le port de destination),
  - l'information sur le protocole par lequel ils doivent être manipulés,
  - l'information sur des erreurs éventuelles et
  - de l'information sur le type de données en transit.
- Un politique de filtrage énonce une liste d'autorisations et d'interdictions des types :
  - autorise/interdit les paquets selon l'adresse IP d'origine/destination
  - autorise/interdit les paquets selon leur port de destination,

Politiques de filtrage

- Souvenons-nous que les paquets contiennent les informations suivantes :
  - les données,
  - l'adresse IP d'origine et de destination (incluant le port de destination),
  - l'information sur le protocole par lequel ils doivent être manipulés,
  - l'information sur des erreurs éventuelles et
  - de l'information sur le type de données en transit.
- Un politique de filtrage énonce une liste d'autorisations et d'interdictions des types :
  - autorise/interdit les paquets selon l'adresse IP d'origine/destination
  - autorise/interdit les paquets selon leur port de destination,
  - autorise/interdit les paquets selon le protocole.

Conclusion (filtrage de paquets)

Conclusion (filtrage de paquets)

- Pour être complètement sûr, le filtrage de paquets doit être très restrictif, ce qui peut trop limiter l'accès au réseau.

Conclusion (filtrage de paquets)

- Pour être complètement sûr, le filtrage de paquets doit être très restrictif, ce qui peut trop limiter l'accès au réseau.
- Si le filtrage est plus lâche, alors il pourrait devenir possible à l'adversaire de communiquer avec des machines du réseau local :

Conclusion (filtrage de paquets)

- Pour être complètement sûr, le filtrage de paquets doit être très restrictif, ce qui peut trop limiter l'accès au réseau.
- Si le filtrage est plus lâche, alors il pourrait devenir possible à l'adversaire de communiquer avec des machines du réseau local :
  - Ceci demande à l'adversaire de tenter beaucoup d'adresses IP jusqu'à ce qu'une machine réponde...

Conclusion (filtrage de paquets)

- Pour être complètement sûr, le filtrage de paquets doit être très restrictif, ce qui peut trop limiter l'accès au réseau.
- Si le filtrage est plus lâche, alors il pourrait devenir possible à l'adversaire de communiquer avec des machines du réseau local :
  - Ceci demande à l'adversaire de tenter beaucoup d'adresses IP jusqu'à ce qu'une machine réponde...
- En conclusion, les coupe-feu devraient faire quelque chose de plus intelligent que le simple filtrage.

Conclusion (filtrage de paquets)

- Pour être complètement sûr, le filtrage de paquets doit être très restrictif, ce qui peut trop limiter l'accès au réseau.
- Si le filtrage est plus lâche, alors il pourrait devenir possible à l'adversaire de communiquer avec des machines du réseau local :
  - Ceci demande à l'adversaire de tenter beaucoup d'adresses IP jusqu'à ce qu'une machine réponde...
- En conclusion, les coupe-feu devraient faire quelque chose de plus intelligent que le simple filtrage.
  - Ils doivent examiner les paquets en détail pour décider quoi faire avec ceux-ci. Ils devraient même être capables de modifier des paquets si nécessaire...

Coupe-feu : proxy

Coupe-feu : proxy

- Les proxy («serveurs mandataires») permettent de faire du filtrage intelligent. Il ne permet aucune connexion sur une machine locale à partir de l'extérieur.

Coupe-feu : proxy

- Les proxy («serveurs mandataires») permettent de faire du filtrage intelligent. Il ne permet aucune connexion sur une machine locale à partir de l'extérieur.
- Le proxy gère toutes les connexions au nom des machines de réseau local.

Coupe-feu : proxy

- Les proxy («serveurs mandataires») permettent de faire du filtrage intelligent. Il ne permet aucune connexion sur une machine locale à partir de l'extérieur.
- Le proxy gère toutes les connexions au nom des machines de réseau local.
  - Si une machine locale a un logiciel qui désire accéder à l'Internet alors celui-ci devra être configuré pour communiquer avec le coupe-feu à la place. Le coupe-feu établira alors la connexion.

Coupe-feu : proxy

- Les proxy («serveurs mandataires») permettent de faire du filtrage intelligent. Il ne permet aucune connexion sur une machine locale à partir de l'extérieur.
- Le proxy gère toutes les connexions au nom des machines de réseau local.
  - Si une machine locale a un logiciel qui désire accéder à l'Internet alors celui-ci devra être configuré pour communiquer avec le coupe-feu à la place. Le coupe-feu établira alors la connexion.
  - Vu de l'extérieur, le réseau local est complètement caché derrière le coupe-feu. Seul celui-ci est visible.

Coupe-feu : proxy

- Les proxy («serveurs mandataires») permettent de faire du filtrage intelligent. Il ne permet aucune connexion sur une machine locale à partir de l'extérieur.
- Le proxy gère toutes les connexions au nom des machines de réseau local.
  - Si une machine locale a un logiciel qui désire accéder à l'Internet alors celui-ci devra être configuré pour communiquer avec le coupe-feu à la place. Le coupe-feu établira alors la connexion.
  - Vu de l'extérieur, le réseau local est complètement caché derrière le coupe-feu. Seul celui-ci est visible.
  - Essayer plusieurs adresses IP pour espérer une réponse ne fonctionne pas ici.

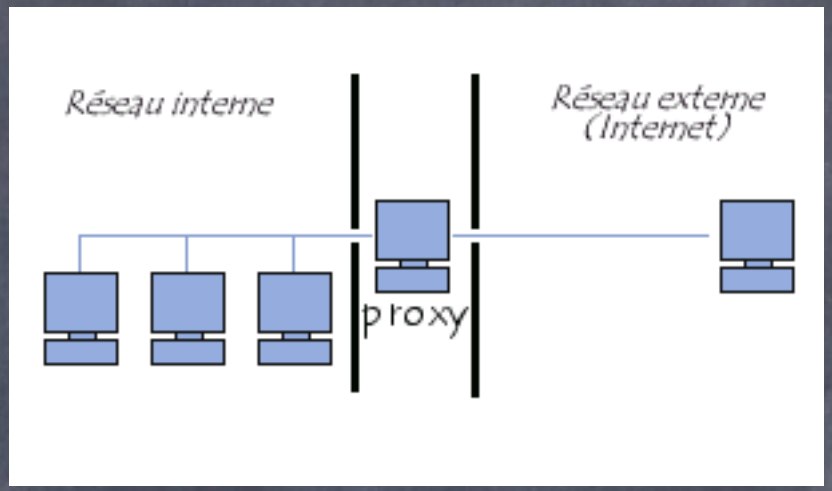
Coupe-feu : proxy

- Les proxy («serveurs mandataires») permettent de faire du filtrage intelligent. Il ne permet aucune connexion sur une machine locale à partir de l'extérieur.
- Le proxy gère toutes les connexions au nom des machines de réseau local.
  - Si une machine locale a un logiciel qui désire accéder à l'Internet alors celui-ci devra être configuré pour communiquer avec le coupe-feu à la place. Le coupe-feu établira alors la connexion.
  - Vu de l'extérieur, le réseau local est complètement caché derrière le coupe-feu. Seul celui-ci est visible.
  - Essayer plusieurs adresses IP pour espérer une réponse ne fonctionne pas ici.
  - Une attaque doit s'en prendre au proxy. Une machine est plus facile à protéger que plusieurs.

Proxy en images

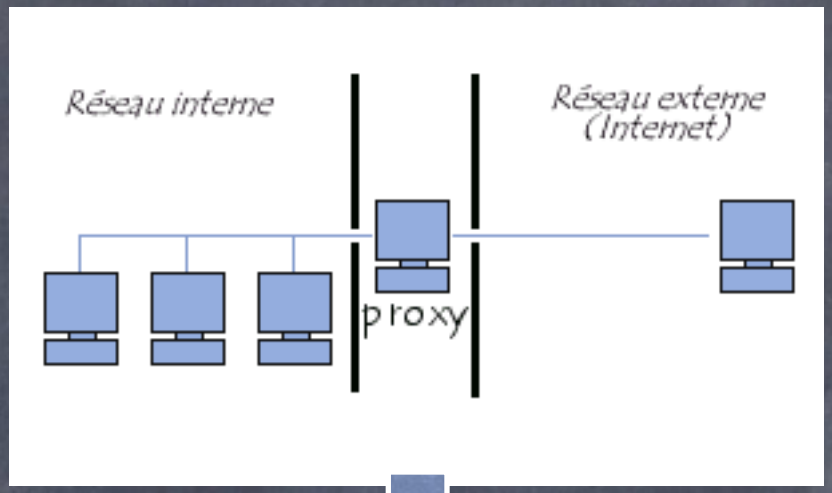
Proxy en images

Le proxy comme une zone tampon entre l'Internet et un réseau local

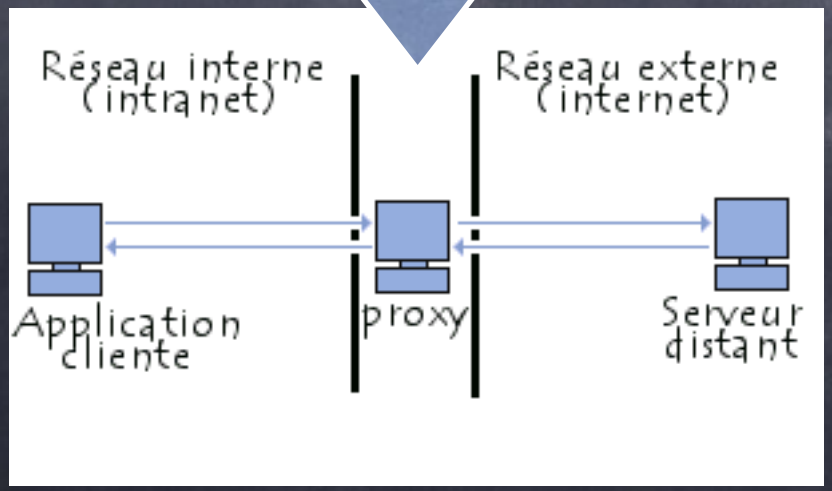


Proxy en images

Le proxy comme une zone tampon entre l'Internet et un réseau local



Pendant une connexion internet



Cacher votre adresse IP

Cacher votre adresse IP

- Votre adresse IP révèle votre point d'entrée sur l'Internet :

Cacher votre adresse IP

- Votre adresse IP révèle votre point d'entrée sur l'Internet :
  - Peut permettre de retrouver votre fournisseur, le réseau de votre employeur, votre école ou votre terminal public.

Cacher votre adresse IP

- Votre adresse IP révèle votre point d'entrée sur l'Internet :
  - Peut permettre de retrouver votre fournisseur, le réseau de votre employeur, votre école ou votre terminal public.
  - Il s'agit de l'identité de votre machine pendant que vous êtes en ligne. Sa porte sur le monde.

Cacher votre adresse IP

- Votre adresse IP révèle votre point d'entrée sur l'Internet :
  - Peut permettre de retrouver votre fournisseur, le réseau de votre employeur, votre école ou votre terminal public.
  - Il s'agit de l'identité de votre machine pendant que vous êtes en ligne. Sa porte sur le monde.
  - Vous pouvez dissimuler votre adresse IP sur le Web en utilisant un serveur proxy anonyme.

Cacher votre adresse IP

- Votre adresse IP révèle votre point d'entrée sur l'Internet :
  - Peut permettre de retrouver votre fournisseur, le réseau de votre employeur, votre école ou votre terminal public.
  - Il s'agit de l'identité de votre machine pendant que vous êtes en ligne. Sa porte sur le monde.
  - Vous pouvez dissimuler votre adresse IP sur le Web en utilisant un serveur proxy anonyme.
  - Un serveur proxy spécialisé pour la navigation Web anonyme utilise sa propre adresse IP à la place de la vôtre pour chaque requête sortante.

Cacher votre adresse IP

- Votre adresse IP révèle votre point d'entrée sur l'Internet :
  - Peut permettre de retrouver votre fournisseur, le réseau de votre employeur, votre école ou votre terminal public.
  - Il s'agit de l'identité de votre machine pendant que vous êtes en ligne. Sa porte sur le monde.
  - Vous pouvez dissimuler votre adresse IP sur le Web en utilisant un serveur proxy anonyme.
  - Un serveur proxy spécialisé pour la navigation Web anonyme utilise sa propre adresse IP à la place de la vôtre pour chaque requête sortante.
  - Il peut même chiffrer les communications Web, ne permettant plus la surveillance de vos actions.

Proxy : pour et contre

Proxy : pour et contre

- Un proxy permet de protéger un réseau local d'une façon très efficace. Un seul point faible nécessite notre attention.

Proxy : pour et contre

- Un proxy permet de protéger un réseau local d'une façon très efficace. Un seul point faible nécessite notre attention.
- Cette solution n'est pas très flexible. Les logiciels clients des machines locales doivent savoir comment utiliser un proxy. Sinon, rien ne fonctionnera puisque celles-ci sont invisibles.

Proxy : pour et contre

- Un proxy permet de protéger un réseau local d'une façon très efficace. Un seul point faible nécessite notre attention.
- Cette solution n'est pas très flexible. Les logiciels clients des machines locales doivent savoir comment utiliser un proxy. Sinon, rien ne fonctionnera puisque celles-ci sont invisibles.
  - Nous pourrions peut-être faire croire au client que le service est donné par le coupe-feu, mais celui-ci doit savoir quoi faire pour acheminer la connexion vers sa destination. Ceci demande de configurer chaque type de connexion.

Exemple de Proxy: Tor

Exemple de Proxy: Tor

Exemple de Proxy: Tor

Proxy WEB

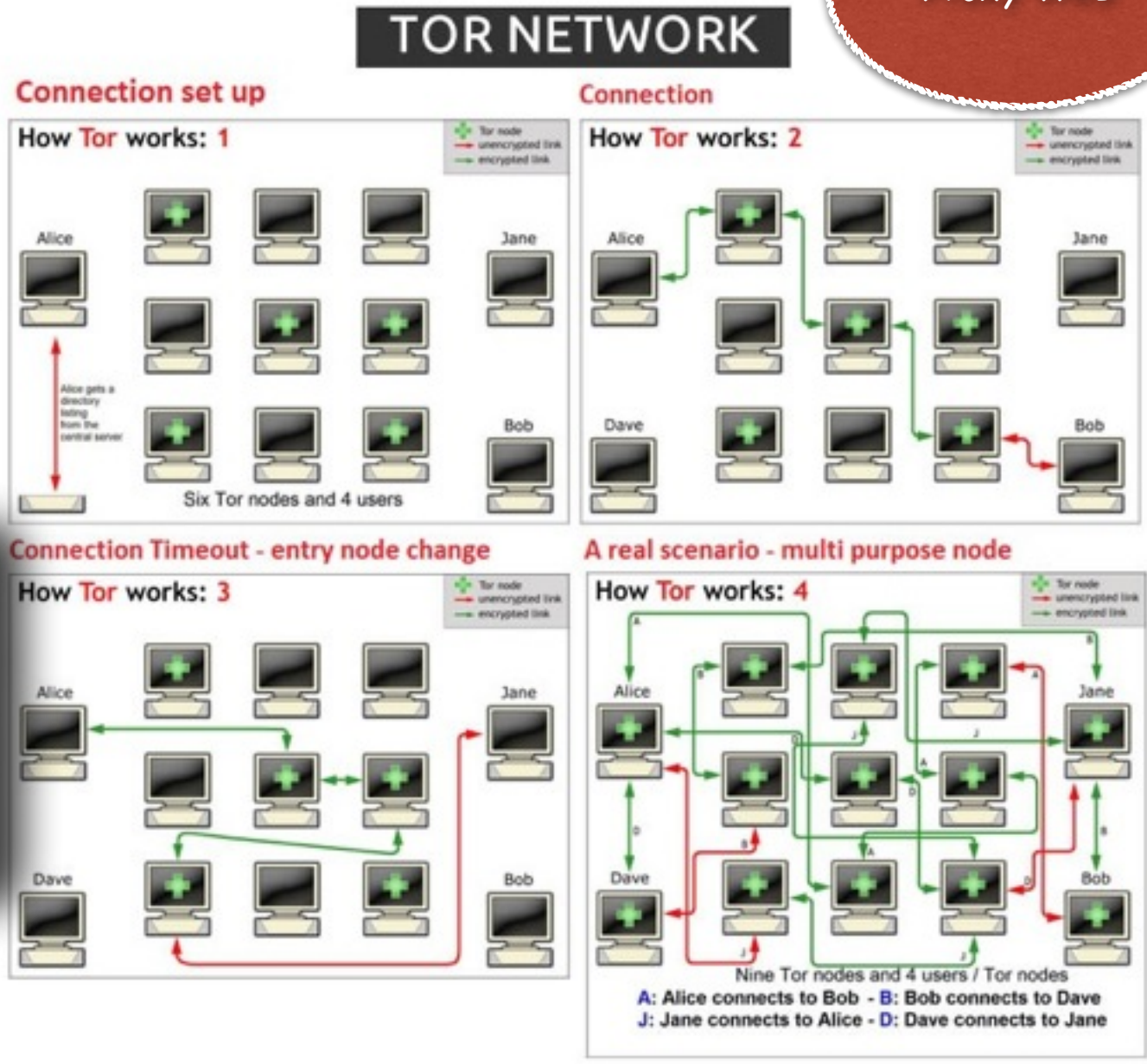
Exemple de Proxy: Tor

Proxy WEB

Pourquoi un oignon? Parce l'information est chiffrée en couche, y compris les adresses IPs. Chaque serveur Tor enlève une couche et transmet au prochain serveur.....

Exemple de Proxy: Tor

Proxy WEB



Pourquoi un oignon? Parce l'information est chiffrée en couche, y compris les adresses IPs. Chaque serveur Tor enlève une couche et transmet au prochain serveur.....

Coupe-feu dynamique («stateful firewall»)

Coupe-feu dynamique («stateful firewall»)

- Nous avons vu que les coupe-feu statiques à filtrage de paquets interviennent en fonction de paquets individuels.

Coupe-feu dynamique («stateful firewall»)

- Nous avons vu que les coupe-feu statiques à filtrage de paquets interviennent en fonction de paquets individuels.
  - Un serveur FTP va ouvrir des connexions sur des ports de hautes valeurs. Le filtrage de paquets ne peut pas savoir qu'une connexion sur le port 6783 appartient à une connexion FTP légitime. Ces paquets seront éliminés...

Coupe-feu dynamique («stateful firewall»)

- Nous avons vu que les coupe-feu statiques à filtrage de paquets interviennent en fonction de paquets individuels.
  - Un serveur FTP va ouvrir des connexions sur des ports de hautes valeurs. Le filtrage de paquets ne peut pas savoir qu'une connexion sur le port 6783 appartient à une connexion FTP légitime. Ces paquets seront éliminés...
  - Le coupe-feu dynamique résout ce problème en mémorisant les connexions ouvertes par des connexions légitimes.

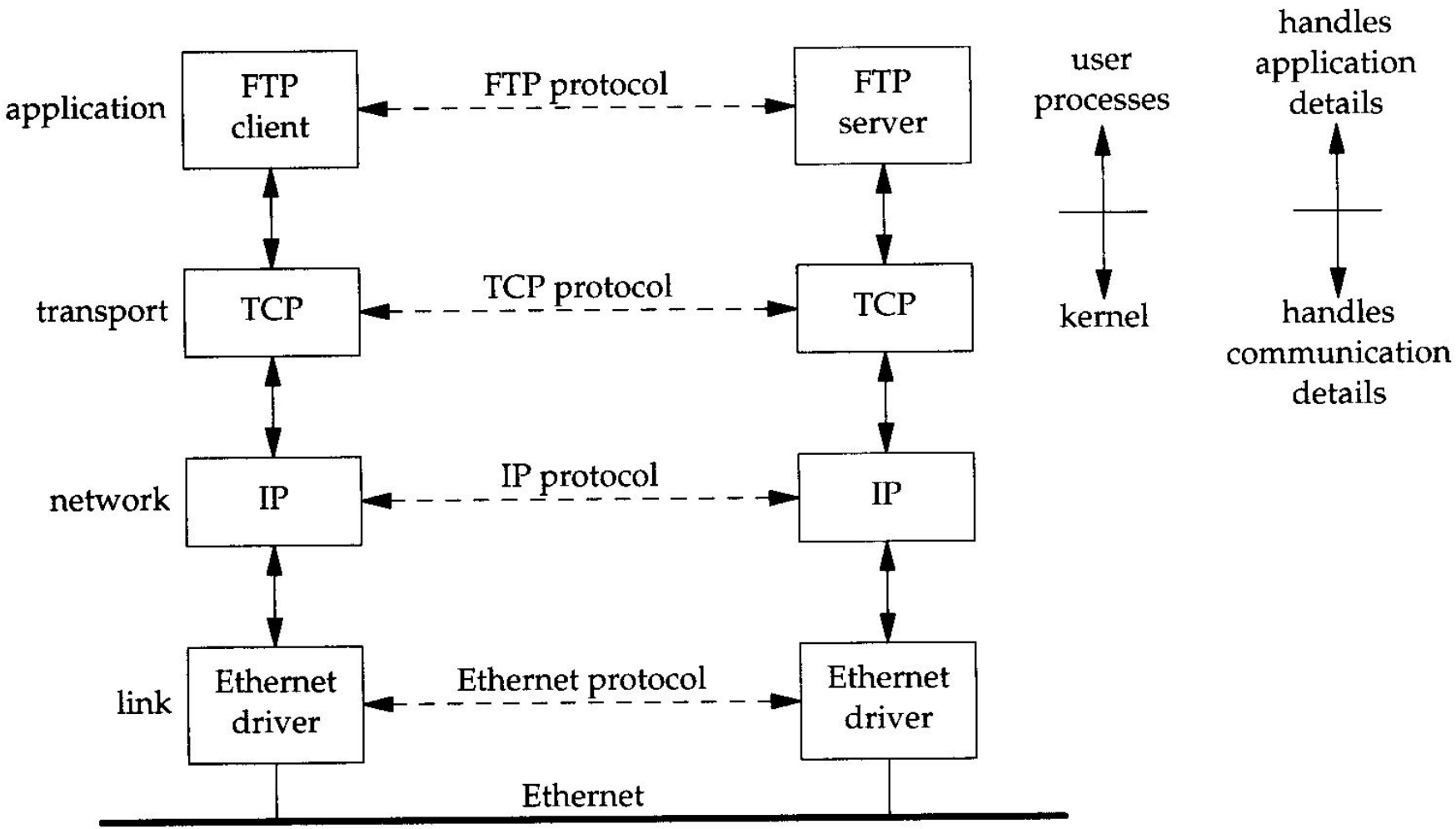
Coupe-feu dynamique («stateful firewall»)

- Nous avons vu que les coupe-feu statiques à filtrage de paquets interviennent en fonction de paquets individuels.
  - Un serveur FTP va ouvrir des connexions sur des ports de hautes valeurs. Le filtrage de paquets ne peut pas savoir qu'une connexion sur le port 6783 appartient à une connexion FTP légitime. Ces paquets seront éliminés...
  - Le coupe-feu dynamique résout ce problème en mémorisant les connexions ouvertes par des connexions légitimes.
- Il est aussi possible de transformer l'adresse IP d'une machine locale par quelque chose de différent. Le coupe-feu à mascarade permet d'éviter les attaques qui consistent à essayer des adresses IP dans le but d'obtenir une réponse.

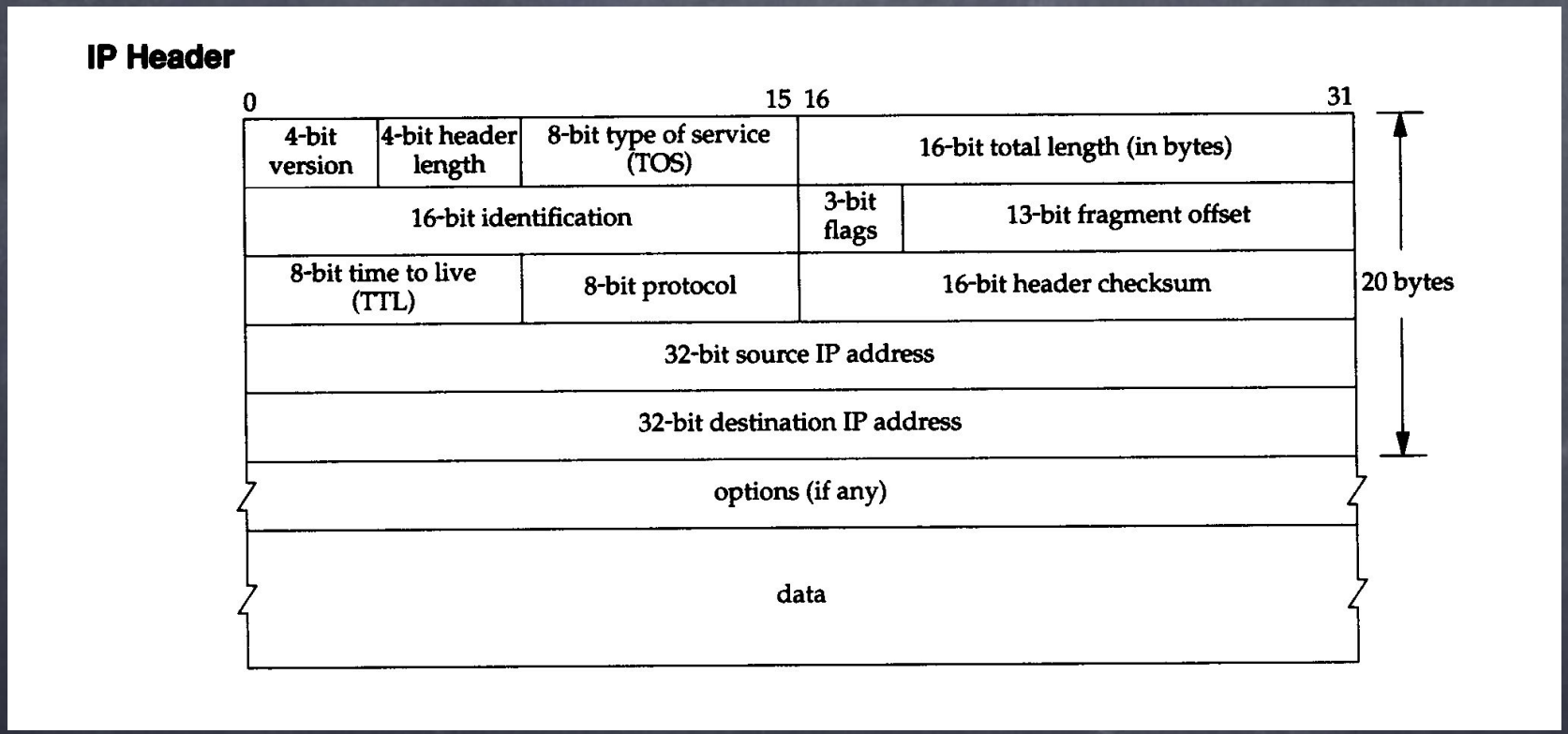
Coupe-feu dynamique («stateful firewall»)

- Nous avons vu que les coupe-feu statiques à filtrage de paquets interviennent en fonction de paquets individuels.
  - Un serveur FTP va ouvrir des connexions sur des ports de hautes valeurs. Le filtrage de paquets ne peut pas savoir qu'une connexion sur le port 6783 appartient à une connexion FTP légitime. Ces paquets seront éliminés...
  - Le coupe-feu dynamique résout ce problème en mémorisant les connexions ouvertes par des connexions légitimes.
- Il est aussi possible de transformer l'adresse IP d'une machine locale par quelque chose de différent. Le coupe-feu à mascarade permet d'éviter les attaques qui consistent à essayer des adresses IP dans le but d'obtenir une réponse.
- Le coupe-feu peut être configuré pour éliminer les connexions qui font des trucs bizarres, comme la transmission d'une chaîne trop longue.

Toujours la pile TCP/IP

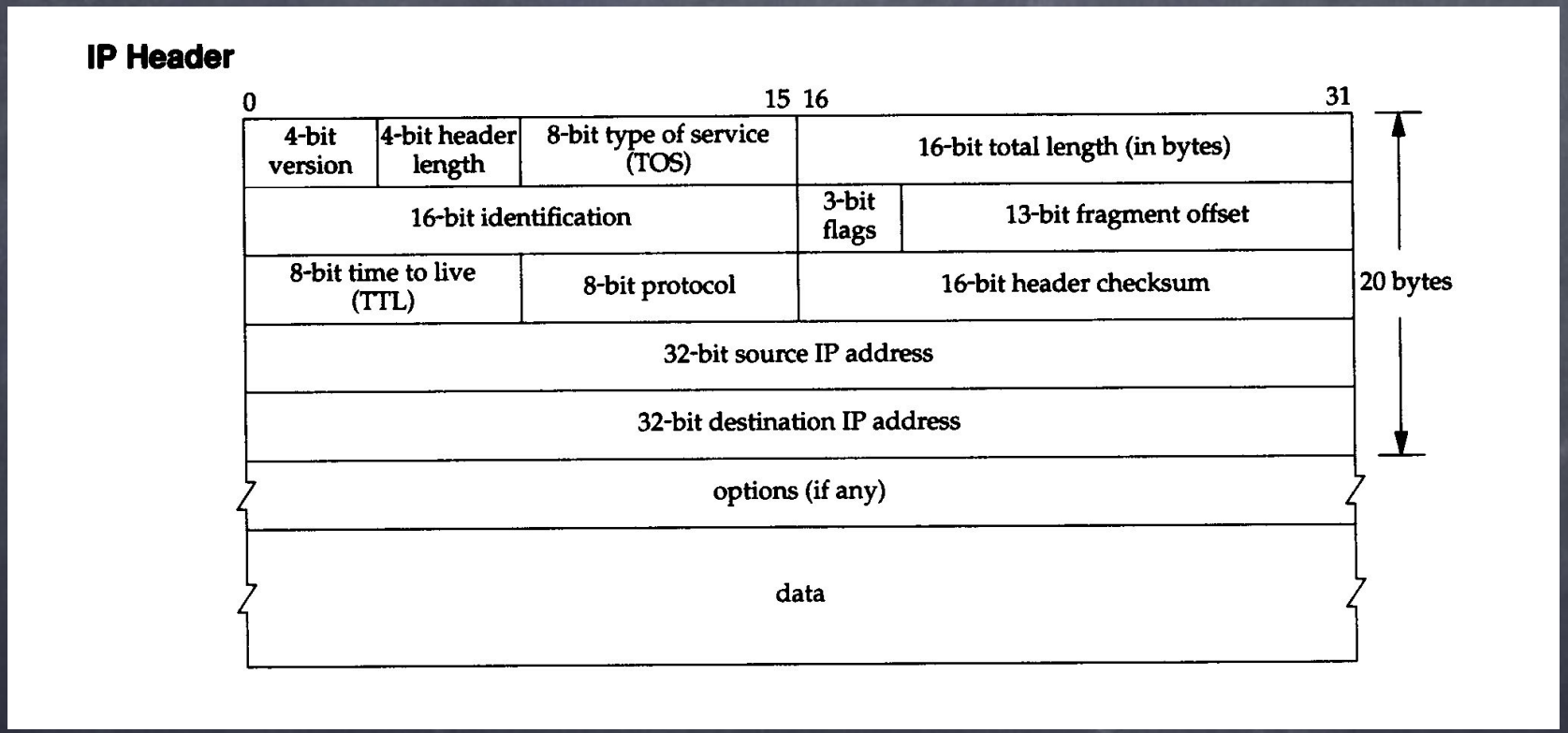


Champs du protocole IP



Champs utiles pour le protocole IP

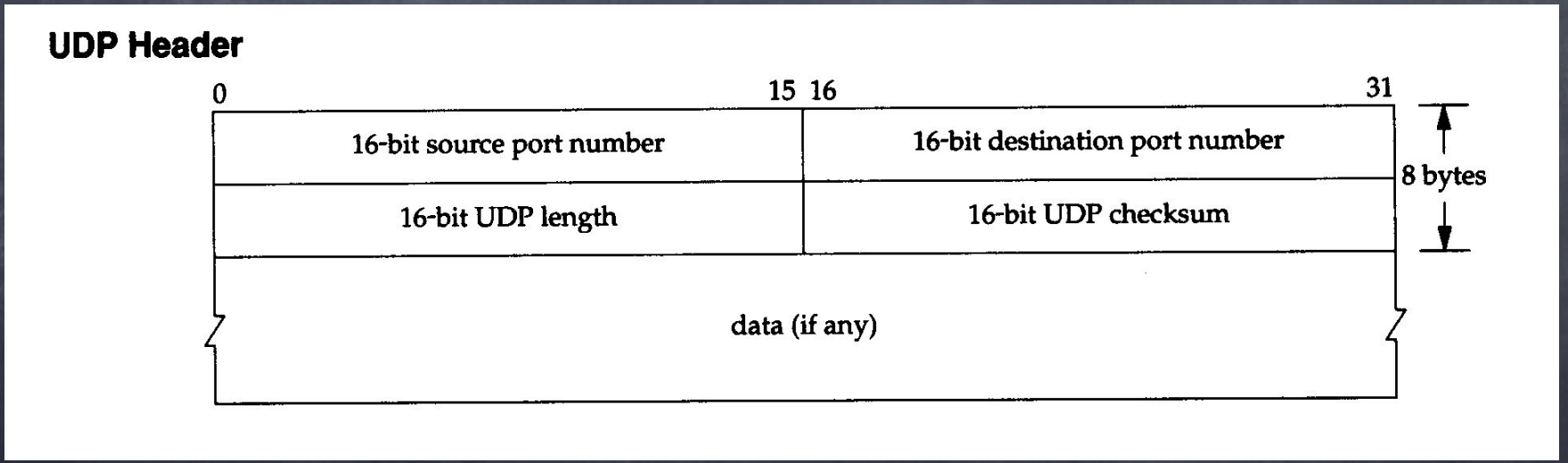
Champs du protocole IP



Champs utiles pour le protocole IP

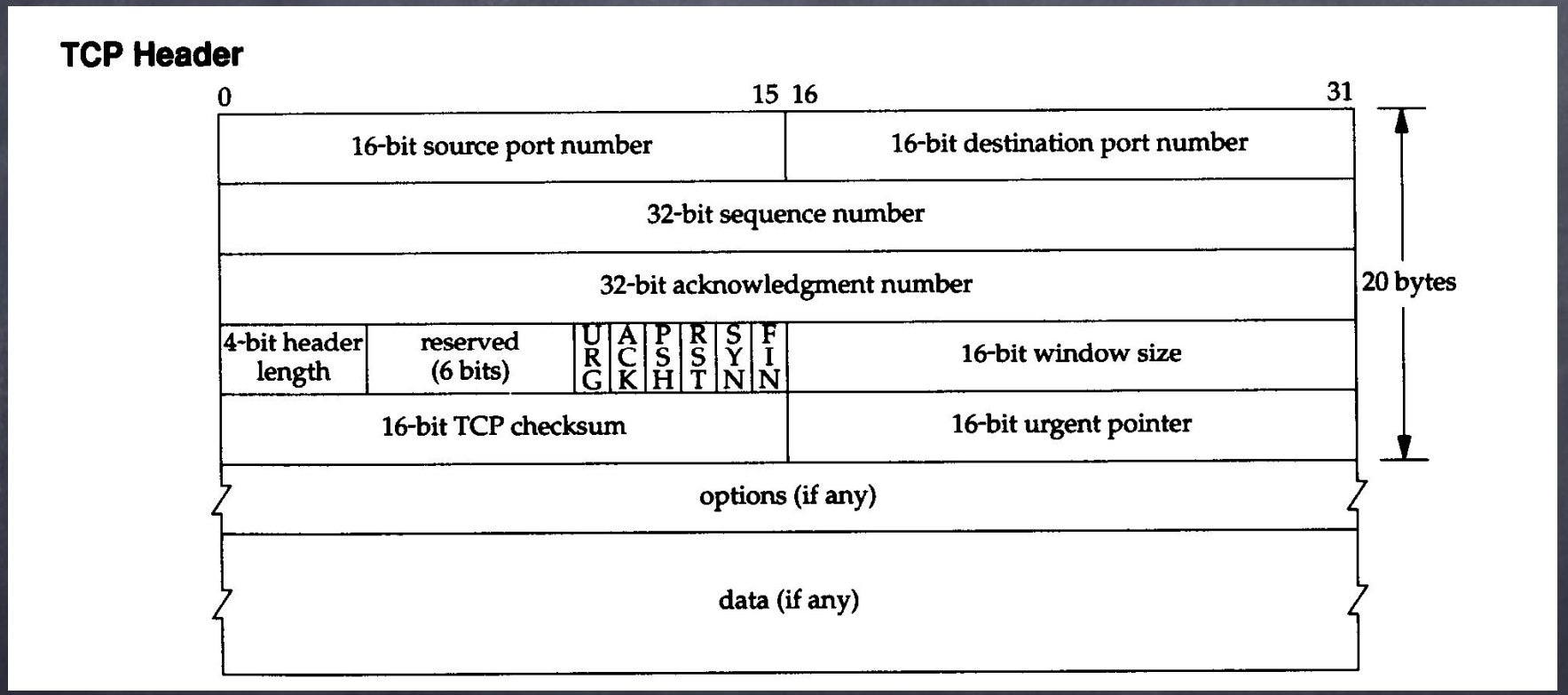
Le protocole IP fonctionne à partir de segments.

Protocole UDP (ses champs utiles)



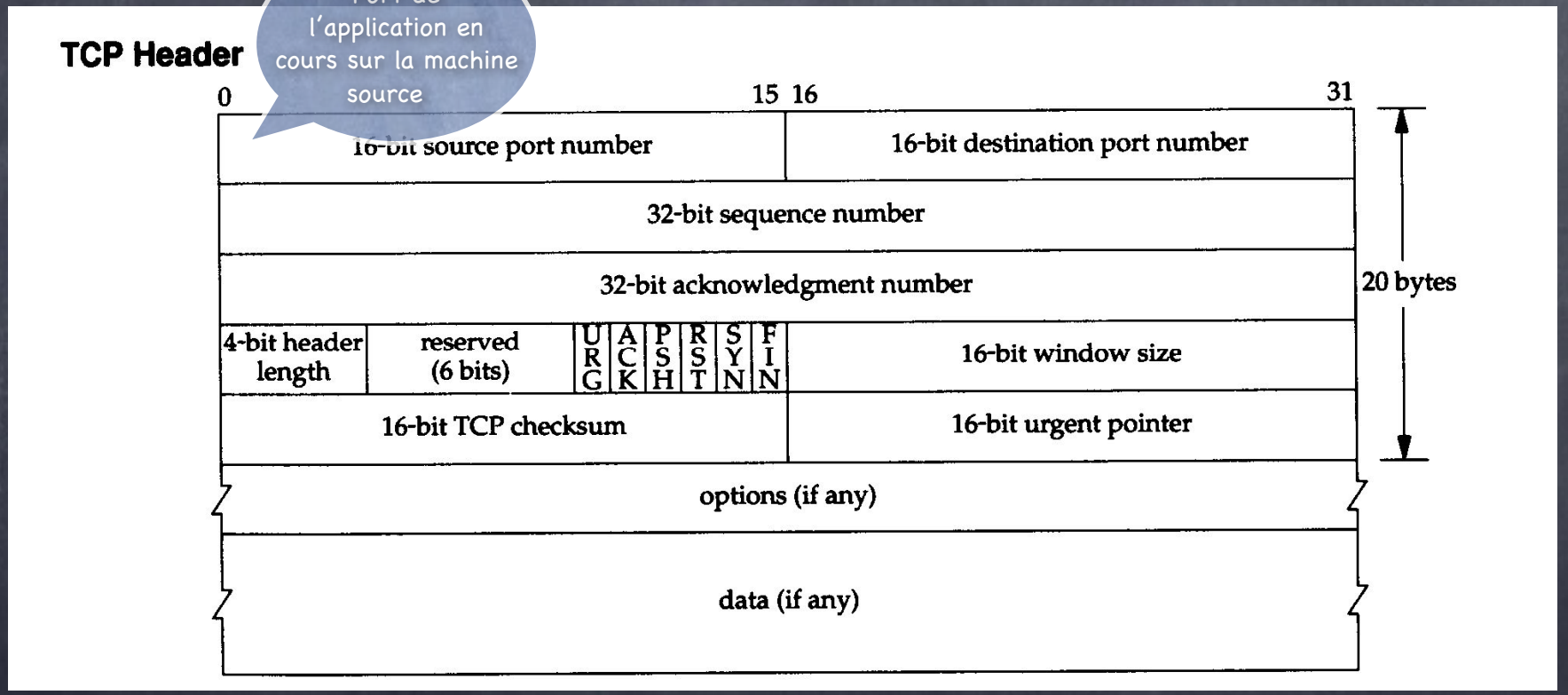
Champs utiles pour le protocole UDP

Protocole TCP (ses champs utiles)



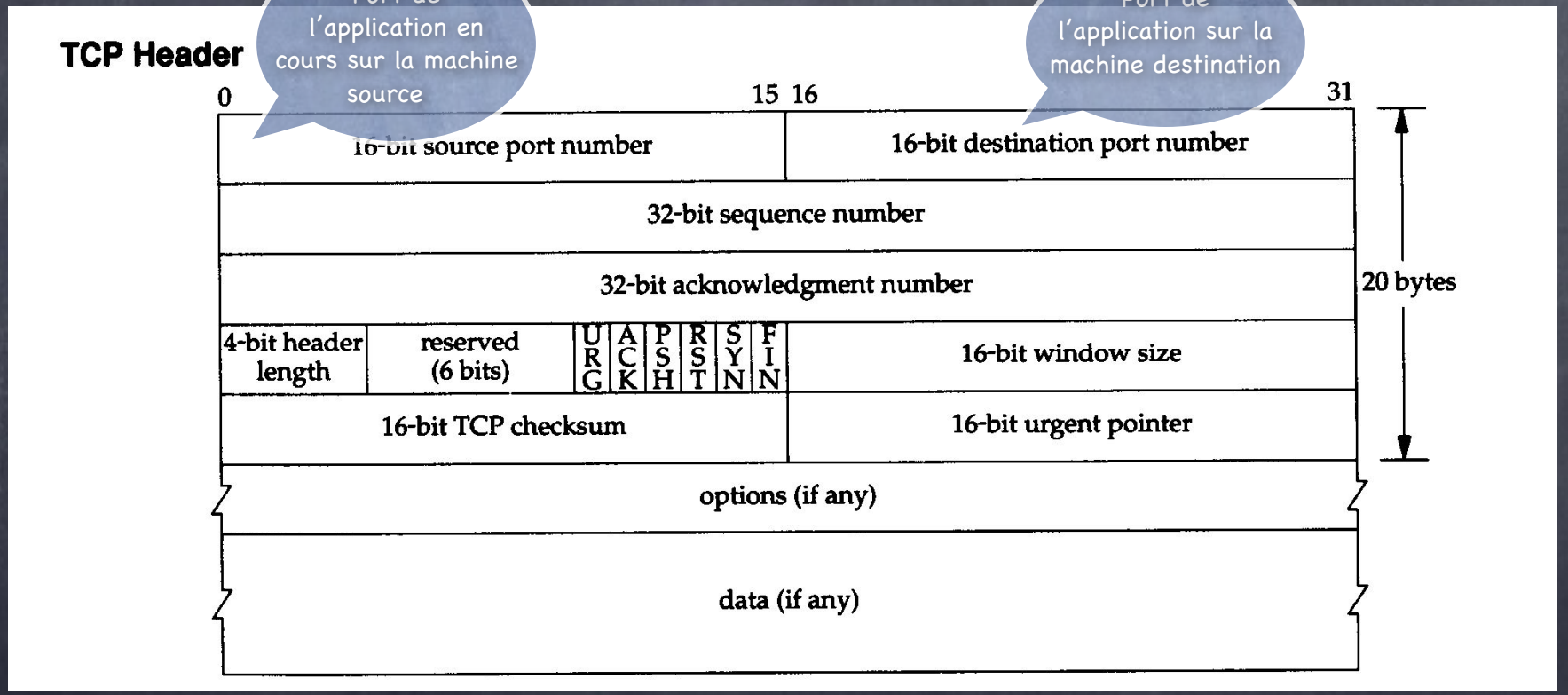
Champs utiles pour le protocole TCP

Protocole TCP (ses champs utiles)



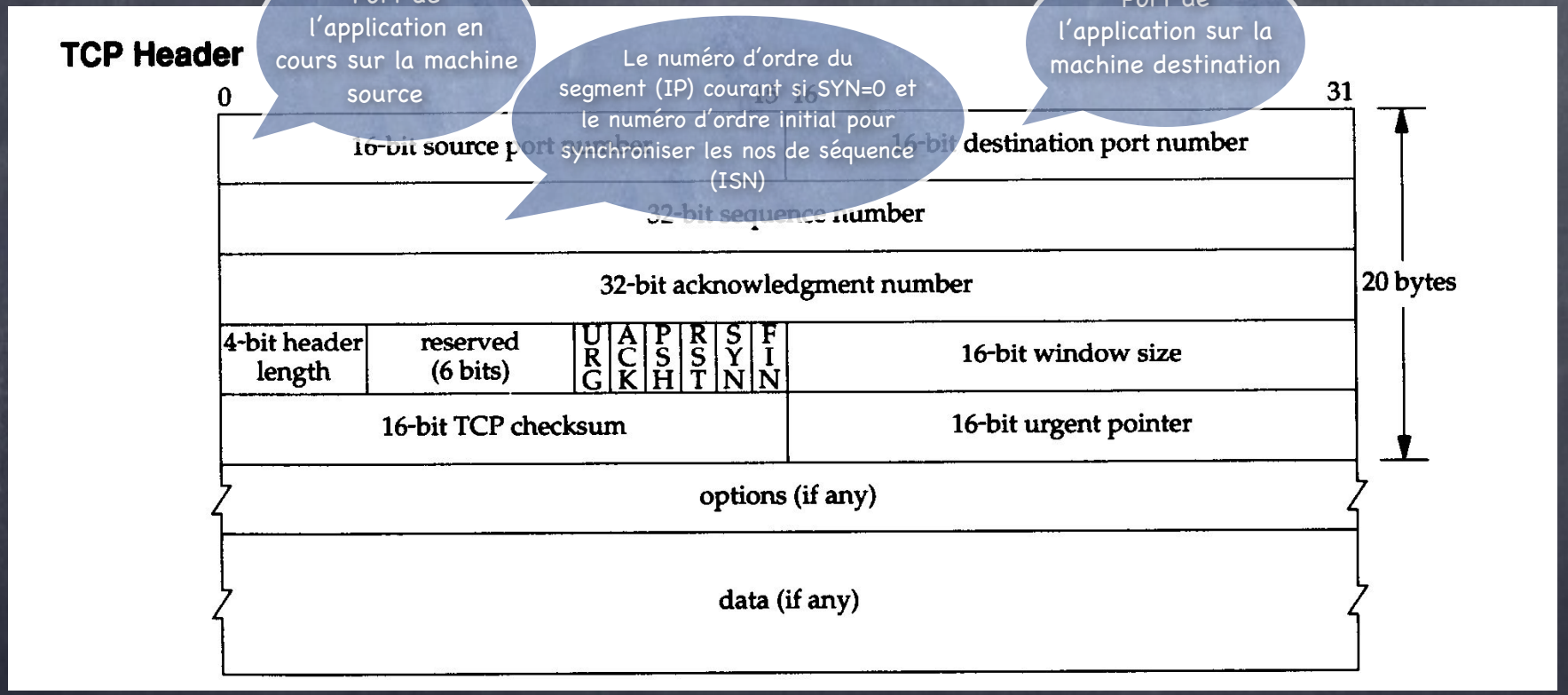
Champs utiles pour le protocole TCP

Protocole TCP (ses champs utiles)



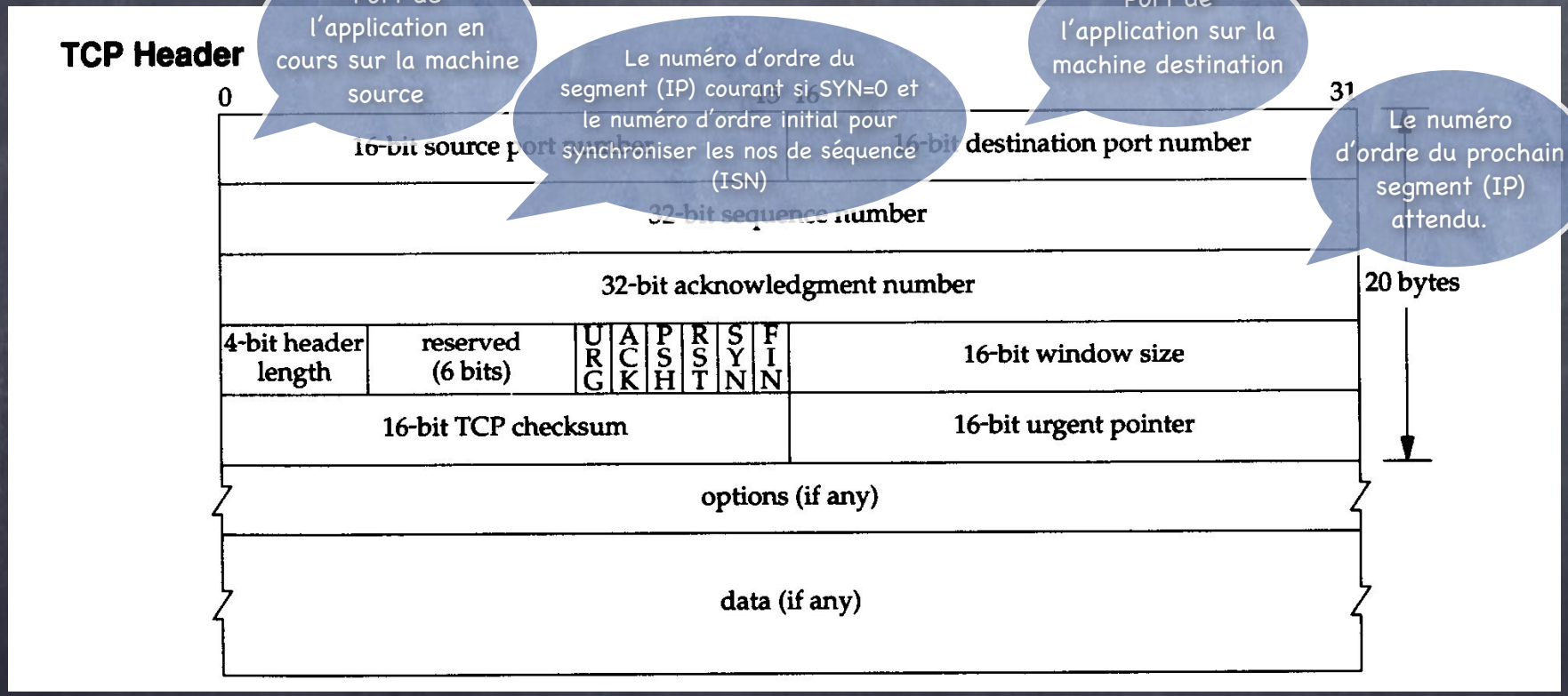
Champs utiles pour le protocole TCP

Protocole TCP (ses champs utiles)



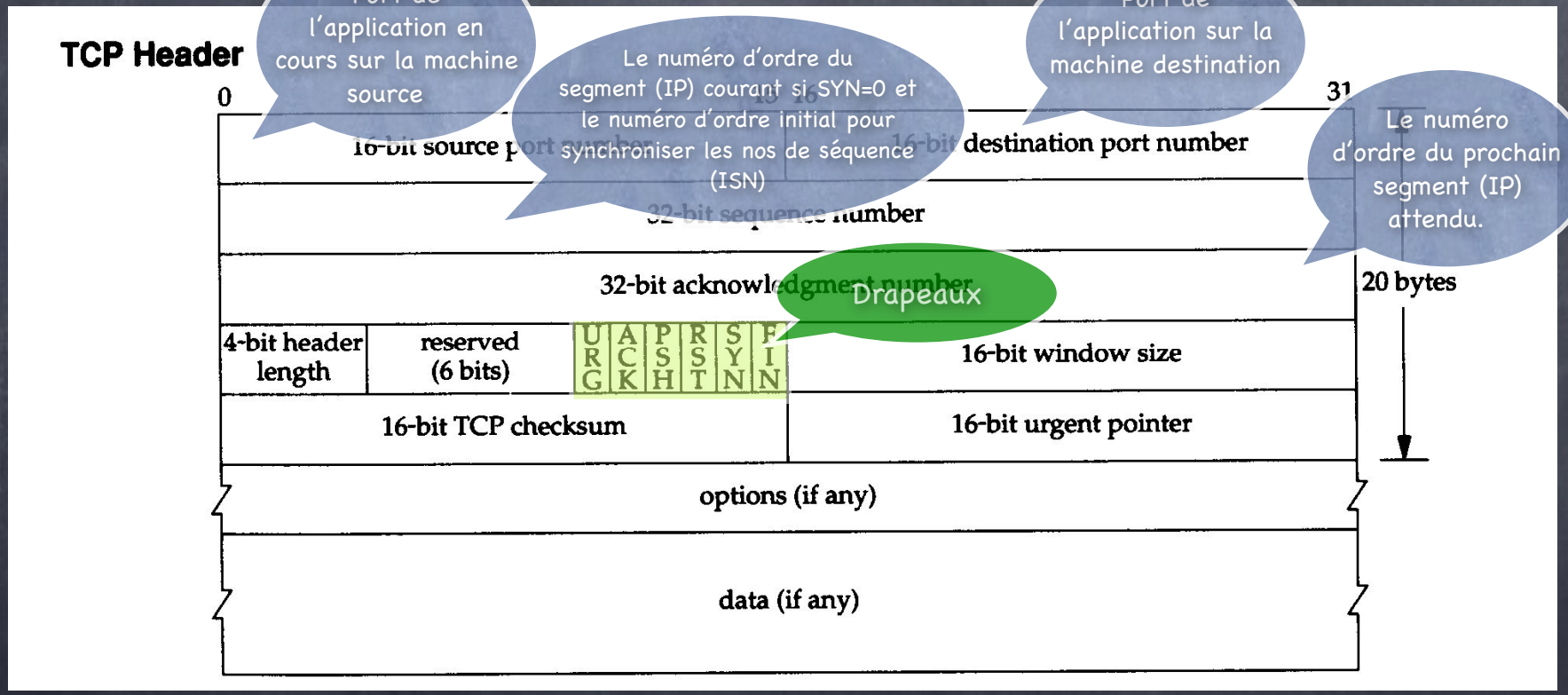
Champs utiles pour le protocole TCP

Protocole TCP (ses champs utiles)



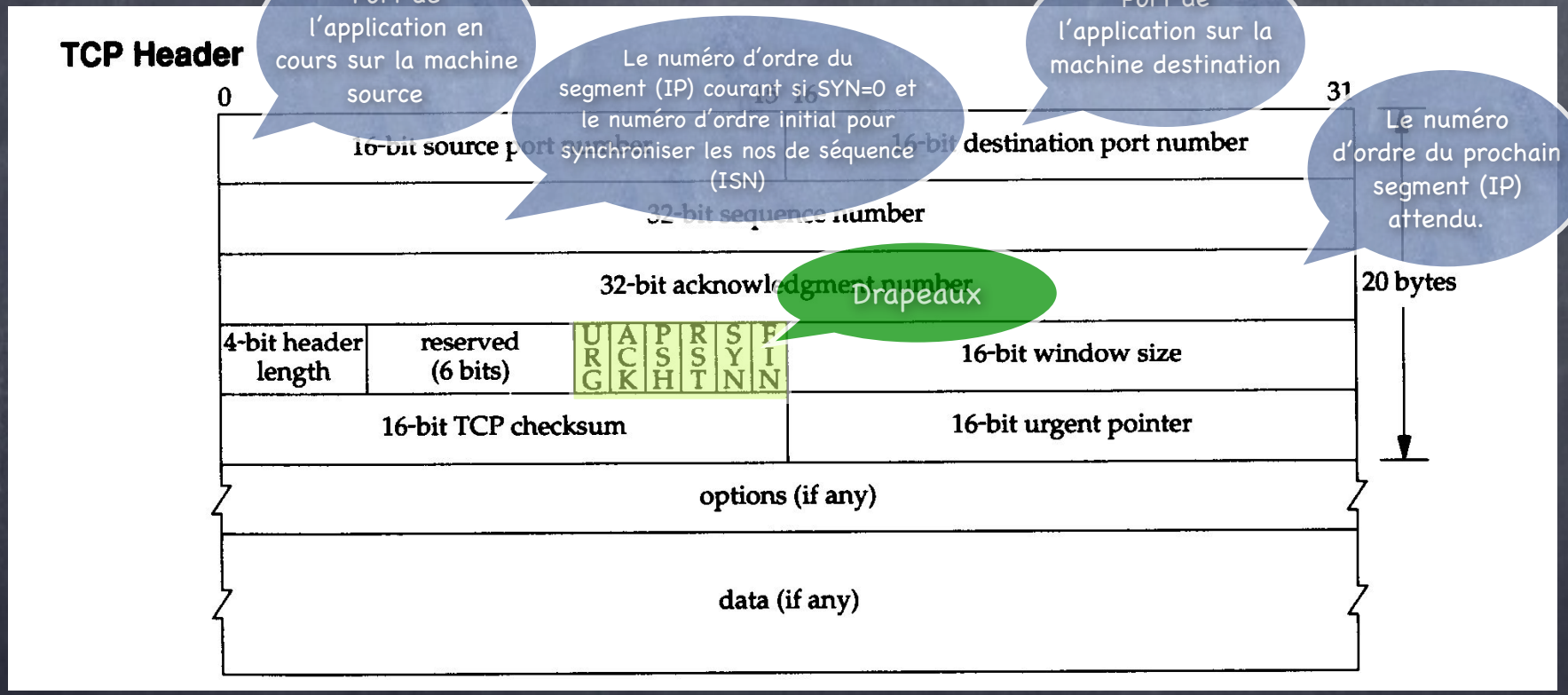
Champs utiles pour le protocole TCP

Protocole TCP (ses champs utiles)



Champs utiles pour le protocole TCP

Protocole TCP (ses champs utiles)



Champs utiles pour le protocole TCP

URG : paquet à traiter de façon urgente.
ACK : paquet est un accusé de réception.
PSH : paquet fonctionne selon la méthode push.
RST : connexion réinitialisée.
SYN : indique une demande d'établissement de connexion.
FIN : indique une interruption de connexion.

Filtrage extrême

Filtrage extrême

- TCP est orienté connexion. Pour en établir une de A vers B, on doit transmettre SYN=1 dans le premier paquet de l'établissement de connexion à trois étapes («three-way handshake»).

Filtrage extrême

- TCP est orienté connexion. Pour en établir une de A vers B, on doit transmettre SYN=1 dans le premier paquet de l'établissement de connexion à trois étapes («three-way handshake»).
- Un filtrage simple consiste à laisser tomber tous les paquets qui ne contiennent que le drapeau SYN=1.

Filtrage extrême

- TCP est orienté connexion. Pour en établir une de A vers B, on doit transmettre SYN=1 dans le premier paquet de l'établissement de connexion à trois étapes («three-way handshake»).
- Un filtrage simple consiste à laisser tomber tous les paquets qui ne contiennent que le drapeau SYN=1.
- Il devient impossible d'établir une connexion TCP de l'extérieur du mur.

Filtrage extrême

- TCP est orienté connexion. Pour en établir une de A vers B, on doit transmettre SYN=1 dans le premier paquet de l'établissement de connexion à trois étapes («three-way handshake»).
- Un filtrage simple consiste à laisser tomber tous les paquets qui ne contiennent que le drapeau SYN=1.
- Il devient impossible d'établir une connexion TCP de l'extérieur du mur.
- Si, en plus, les paquets UDP sont éliminés, alors la situation devrait être très sûre!

Filtrage extrême

- TCP est orienté connexion. Pour en établir une de A vers B, on doit transmettre SYN=1 dans le premier paquet de l'établissement de connexion à trois étapes («three-way handshake»).
- Un filtrage simple consiste à laisser tomber tous les paquets qui ne contiennent que le drapeau SYN=1.
- Il devient impossible d'établir une connexion TCP de l'extérieur du mur.
- Si, en plus, les paquets UDP sont éliminés, alors la situation devrait être très sûre!
- Cette politique ne permet pas de se connecter au serveur Web cependant...

Activer le serveur Web et accès à un DNS

Activer le serveur Web et accès à un DNS

- Pour donner accès au serveur Web, nous pourrions faire la chose suivante :

Activer le serveur Web et accès à un DNS

- Pour donner accès au serveur Web, nous pourrions faire la chose suivante :
  - Nous autorisons une exception à la règle précédente.

Activer le serveur Web et accès à un DNS

- Pour donner accès au serveur Web, nous pourrions faire la chose suivante :
  - Nous autorisons une exception à la règle précédente.
  - Nous autorisons les paquets SYN=1 pour le serveur Web sur le port 80 (port http).

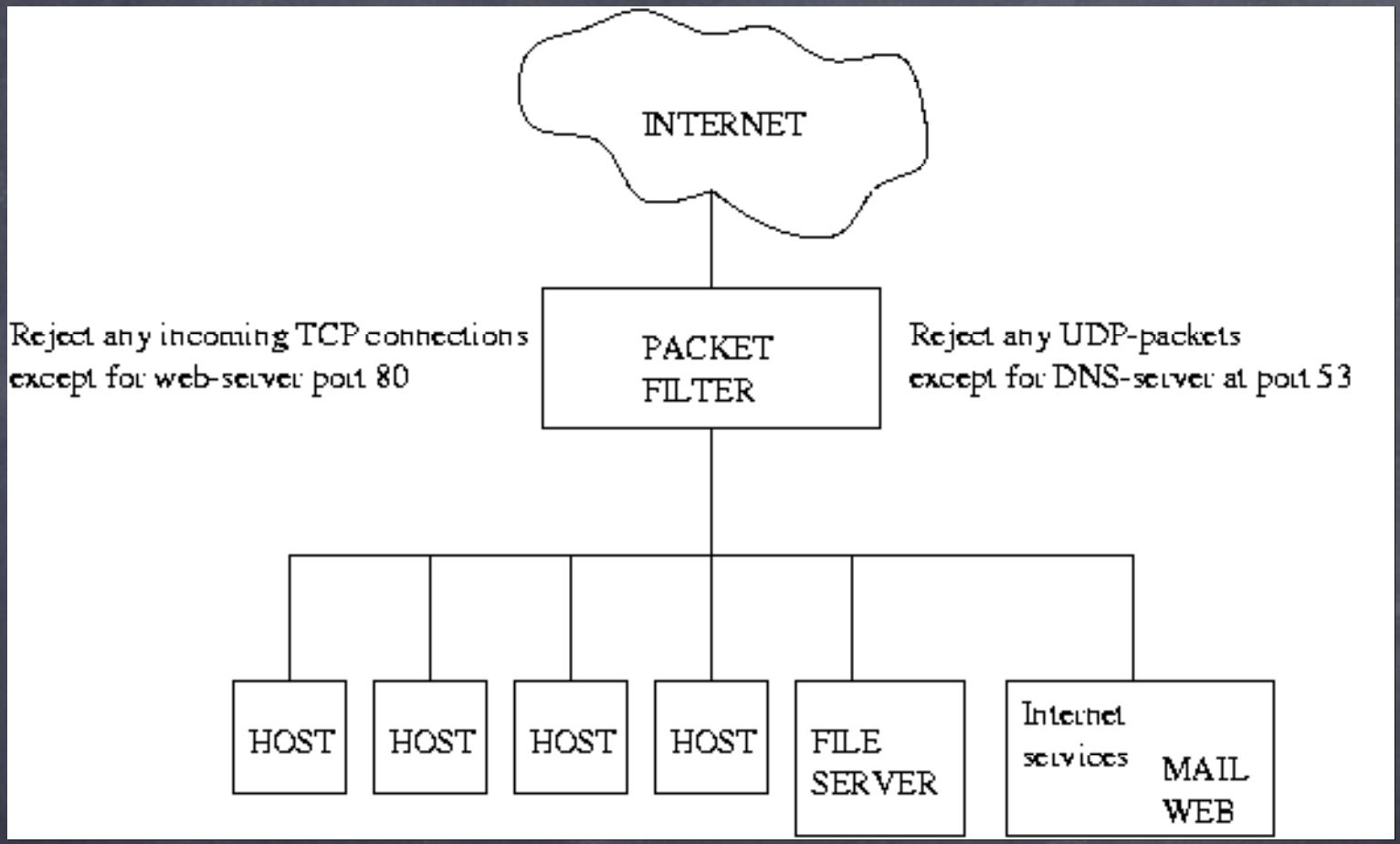
Activer le serveur Web et accès à un DNS

- Pour donner accès au serveur Web, nous pourrions faire la chose suivante :
  - Nous autorisons une exception à la règle précédente.
  - Nous autorisons les paquets SYN=1 pour le serveur Web sur le port 80 (port http).
- Nous voudrions aussi permettre l'accès à un serveur DNS pour la conversion d'adresse comme http://www.iro.umontreal.ca en 132.204.24.179.

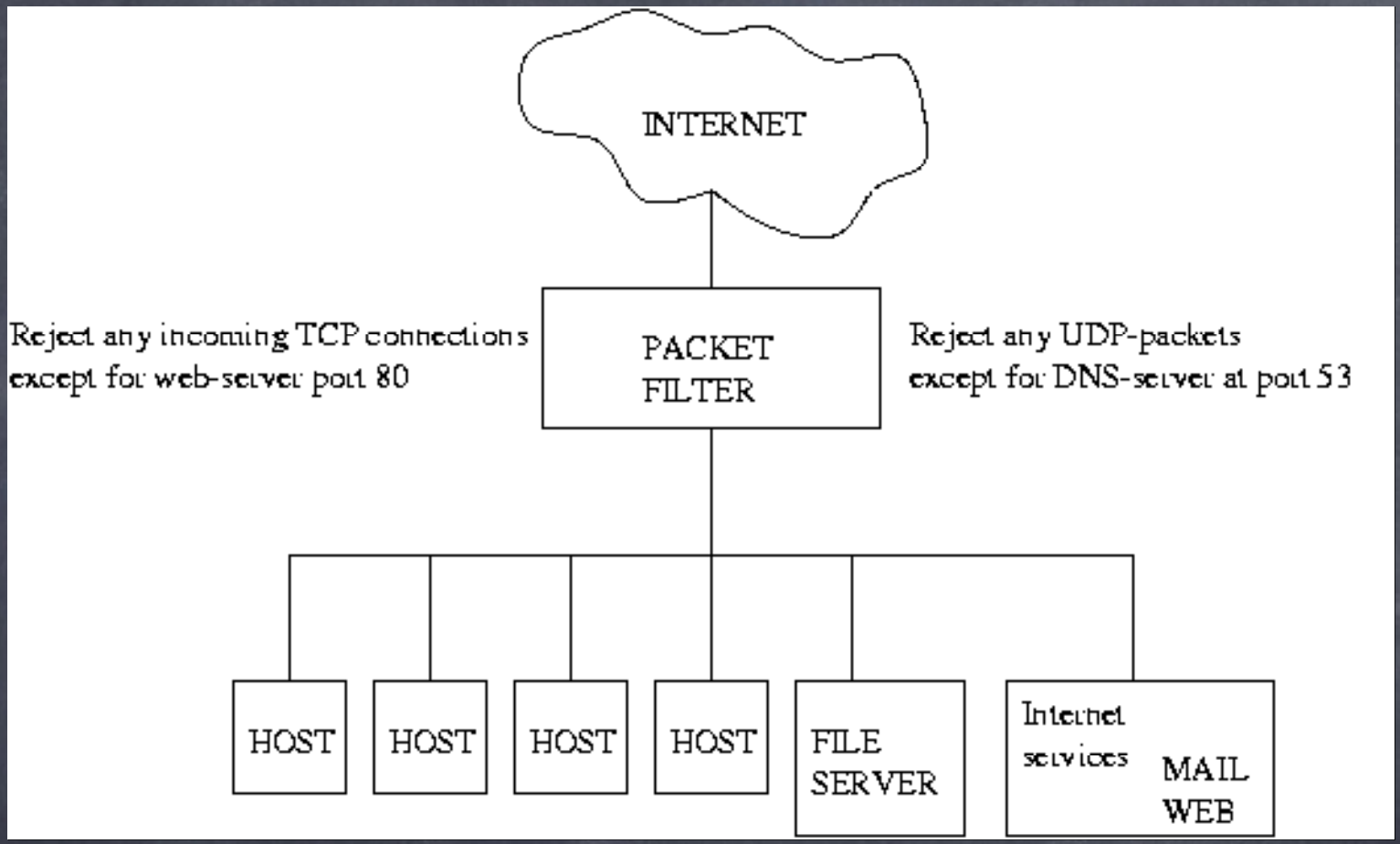
Activer le serveur Web et accès à un DNS

- Pour donner accès au serveur Web, nous pourrions faire la chose suivante :
  - Nous autorisons une exception à la règle précédente.
  - Nous autorisons les paquets SYN=1 pour le serveur Web sur le port 80 (port http).
- Nous voudrions aussi permettre l'accès à un serveur DNS pour la conversion d'adresse comme http://www.iro.umontreal.ca en 132.204.24.179.
  - Il suffit de laisser les paquets UDP vers et depuis au moins un serveur DNS sur le port 53 (UDP).

Le résultat

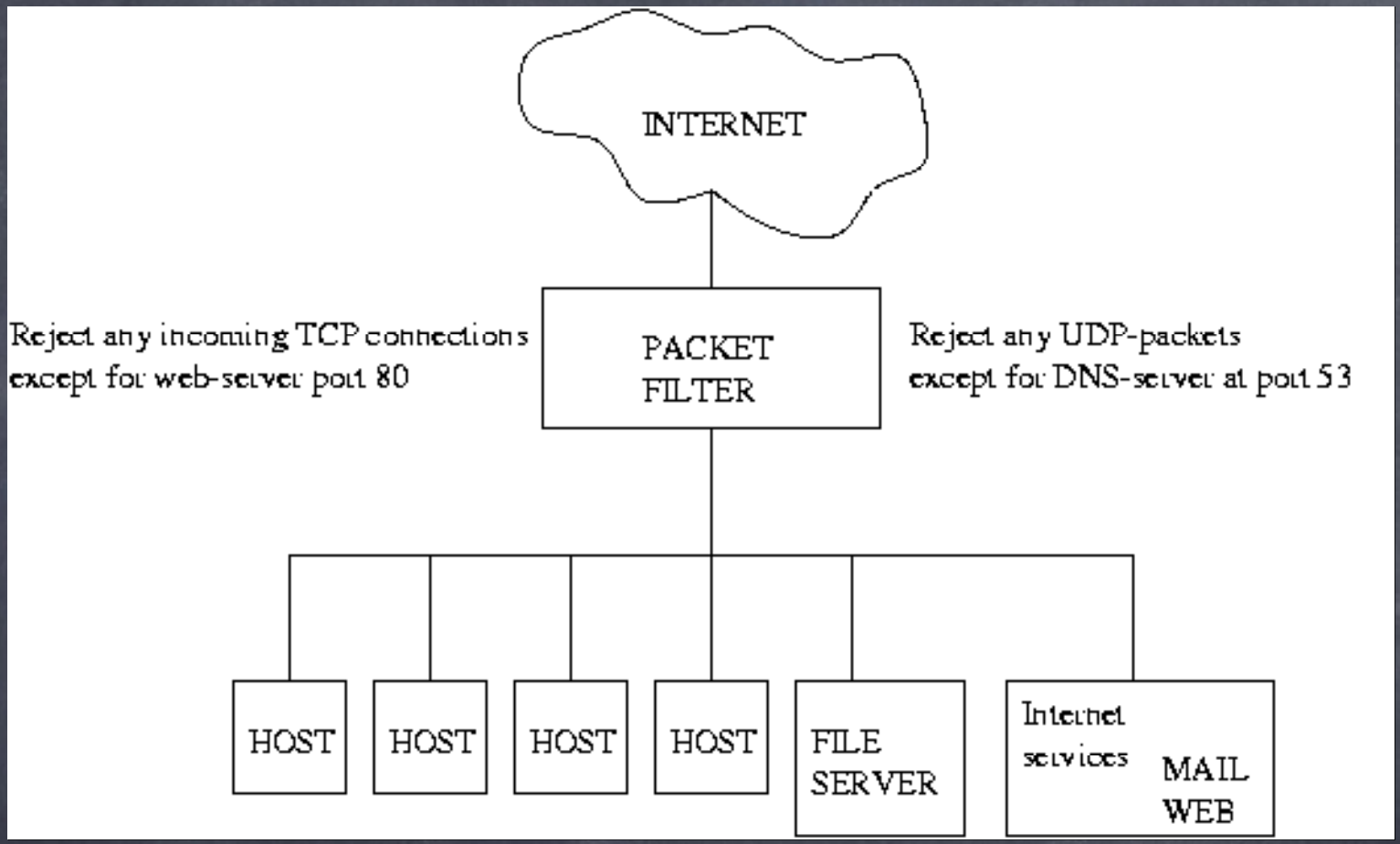

INTERNET
Reject any incoming TCP connections except for web-server port 80
PACKET FILTER
Reject any UDP-packets except for DNS-server at port 53
HOST
HOST
HOST
HOST
FILE SERVER
Internet services
MAIL
WEB

Le résultat



Si le pirate trouve une faille sur le serveur Web, alors il pourrait attaquer le réseau local.

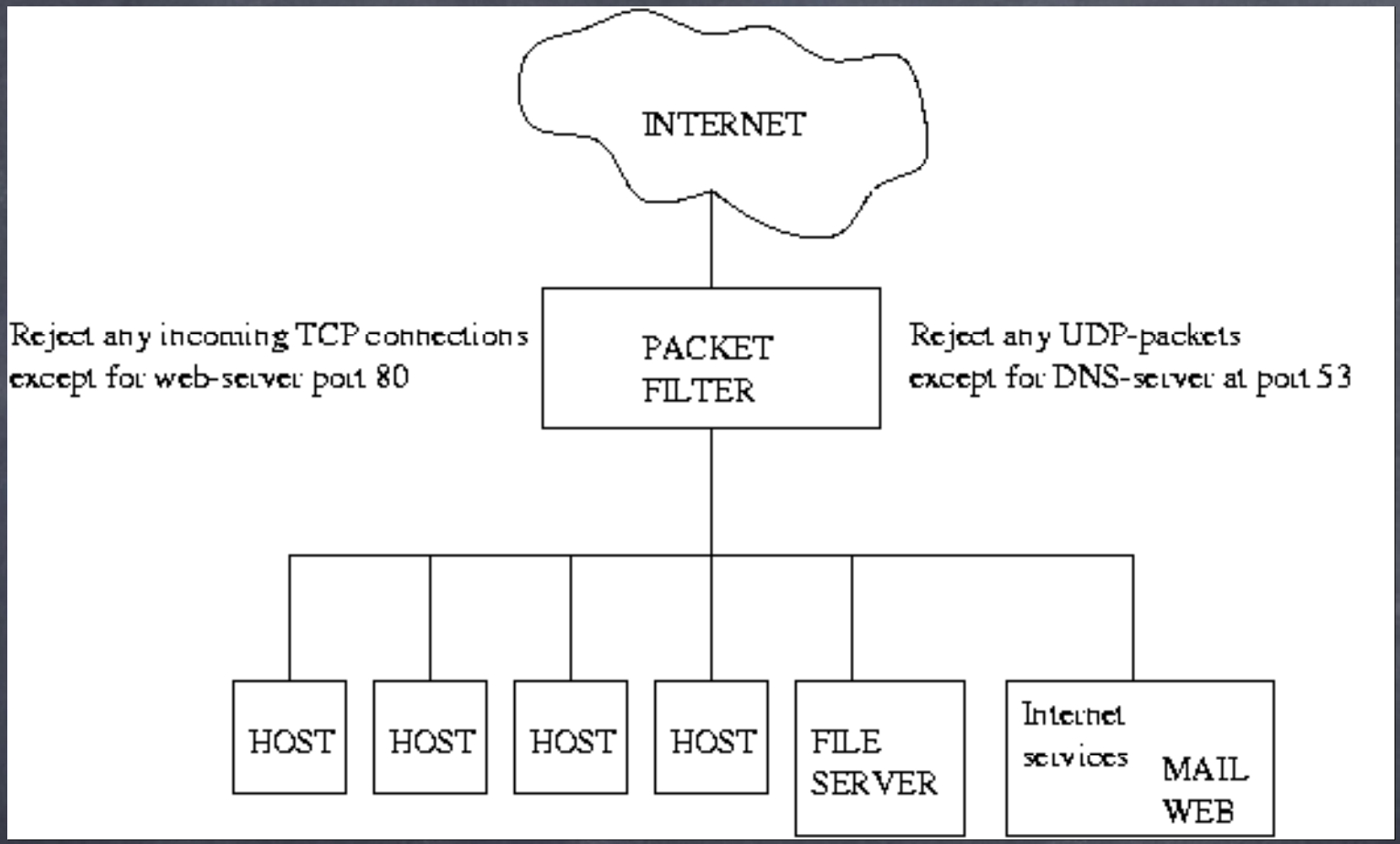
Le résultat



Si le pirate trouve une faille sur le serveur Web, alors il pourrait attaquer le réseau local.

Pour éviter ceci, il faut séparer le serveur Web des autres.

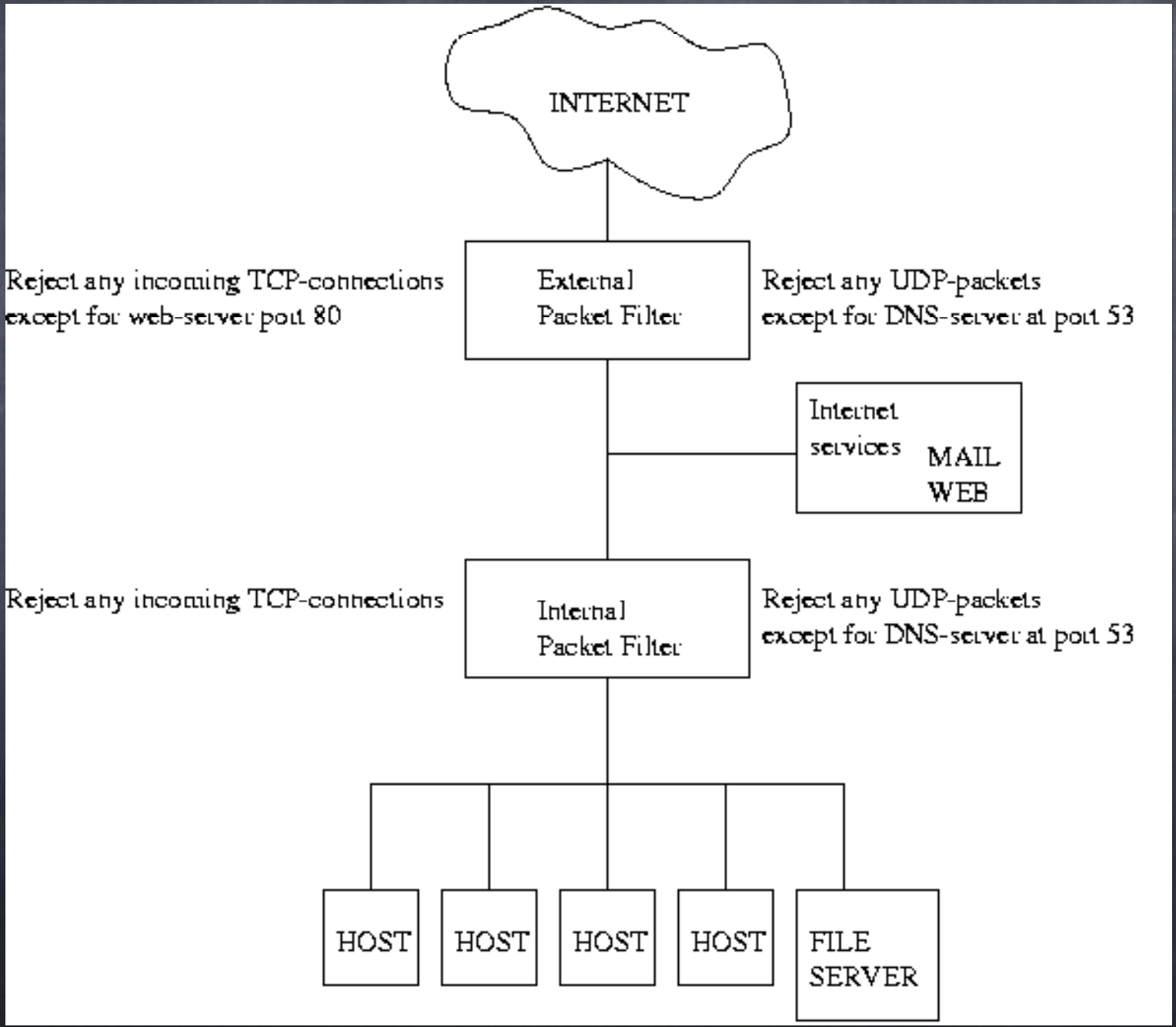
Le résultat



Si le pirate trouve une faille sur le serveur Web, alors il pourrait attaquer le réseau local.

Pour éviter ceci, il faut séparer le serveur Web des autres. Le filtrage par paquets est insuffisant!

Deux filtres valent mieux qu'un



Proxy

Proxy

- Il y a d'autres services sur l'Internet qui utilisent le protocole UDP : flux de données vidéo, jeux vidéo, ...

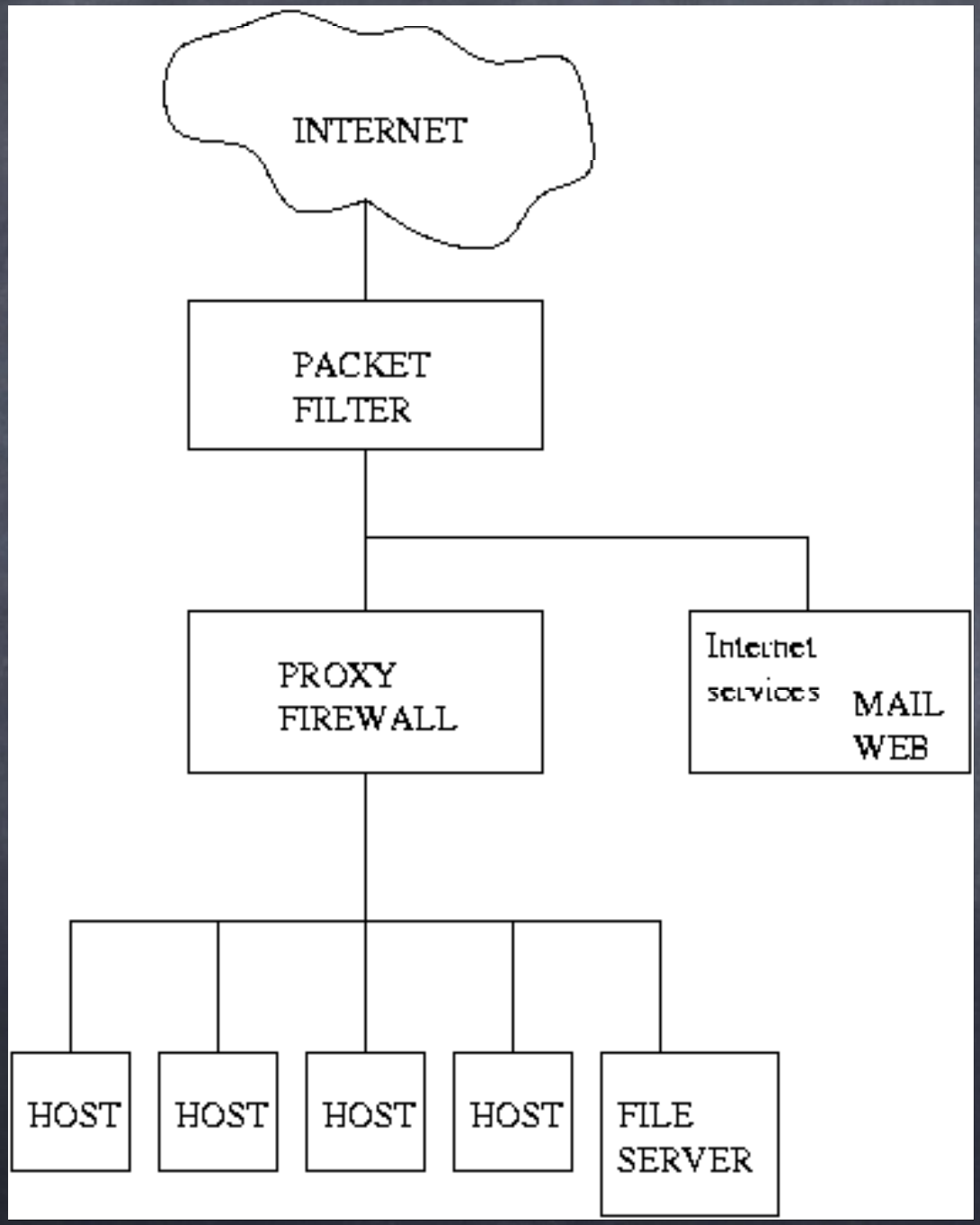
Proxy

- Il y a d'autres services sur l'Internet qui utilisent le protocole UDP : flux de données vidéo, jeux vidéo, ...
- De plus, excepté pour les paquets SYN=1, il est possible de transmettre des paquets TCP aux ordinateurs du réseau local.

Proxy

- Il y a d'autres services sur l'Internet qui utilisent le protocole UDP : flux de données vidéo, jeux vidéo, ...
- De plus, excepté pour les paquets SYN=1, il est possible de transmettre des paquets TCP aux ordinateurs du réseau local.
- Le proxy peut rendre les machines du réseau local invisibles, pas le filtrage simple de paquets.

Approche proxy



Coupe-feu dynamiques

Coupe-feu dynamiques

- Les proxys ne sont pas très flexibles. Les coupe-feu dynamiques permettent d'utiliser les logiciels d'une façon plus transparente.

Coupe-feu dynamiques

- Les proxys ne sont pas très flexibles. Les coupe-feu dynamiques permettent d'utiliser les logiciels d'une façon plus transparente.
  - Il s'agit d'un filtre avancé qui permet de vérifier que les paquets appartiennent à une connexion déjà établie. C'est seulement lorsque c'est le cas que le paquet peut passer.

Coupe-feu dynamiques

- Les proxys ne sont pas très flexibles. Les coupe-feu dynamiques permettent d'utiliser les logiciels d'une façon plus transparente.
  - Il s'agit d'un filtre avancé qui permet de vérifier que les paquets appartiennent à une connexion déjà établie. C'est seulement lorsque c'est le cas que le paquet peut passer.
  - Parce qu'il est conscient d'une connexion, il peut appliquer NAT et/ou PAT :

Coupe-feu dynamiques

- Les proxys ne sont pas très flexibles. Les coupe-feu dynamiques permettent d'utiliser les logiciels d'une façon plus transparente.
  - Il s'agit d'un filtre avancé qui permet de vérifier que les paquets appartiennent à une connexion déjà établie. C'est seulement lorsque c'est le cas que le paquet peut passer.
  - Parce qu'il est conscient d'une connexion, il peut appliquer NAT et/ou PAT :
    - NAT Dynamique («Dynamic Network Address Translation») : Le coupe-feu traduit les adresses du réseau. Toutes les machines du réseau possèdent, vu de l'extérieur, la même adresse IP.

Coupe-feu dynamiques

- Les proxys ne sont pas très flexibles. Les coupe-feu dynamiques permettent d'utiliser les logiciels d'une façon plus transparente.
  - Il s'agit d'un filtre avancé qui permet de vérifier que les paquets appartiennent à une connexion déjà établie. C'est seulement lorsque c'est le cas que le paquet peut passer.
  - Parce qu'il est conscient d'une connexion, il peut appliquer NAT et/ou PAT :
    - NAT Dynamique («Dynamic Network Address Translation») : Le coupe-feu traduit les adresses du réseau. Toutes les machines du réseau possèdent, vu de l'extérieur, la même adresse IP.
    - PAT («Port Address Translation») : Le coupe-feu traduit les numéros de port par lesquels les paquets arrivent sur les hôtes locaux.

Coupe-feu dynamiques

- Les proxys ne sont pas très flexibles. Les coupe-feu dynamiques permettent d'utiliser les logiciels d'une façon plus transparente.
  - Il s'agit d'un filtre avancé qui permet de vérifier que les paquets appartiennent à une connexion déjà établie. C'est seulement lorsque c'est le cas que le paquet peut passer.
  - Parce qu'il est conscient d'une connexion, il peut appliquer NAT et/ou PAT :
    - NAT Dynamique («Dynamic Network Address Translation») : Le coupe-feu traduit les adresses du réseau. Toutes les machines du réseau possèdent, vu de l'extérieur, la même adresse IP.
    - PAT («Port Address Translation») : Le coupe-feu traduit les numéros de port par lesquels les paquets arrivent sur les hôtes locaux.
  - Ces coupe-feu sont appelés coupe-feu avec mascarade.

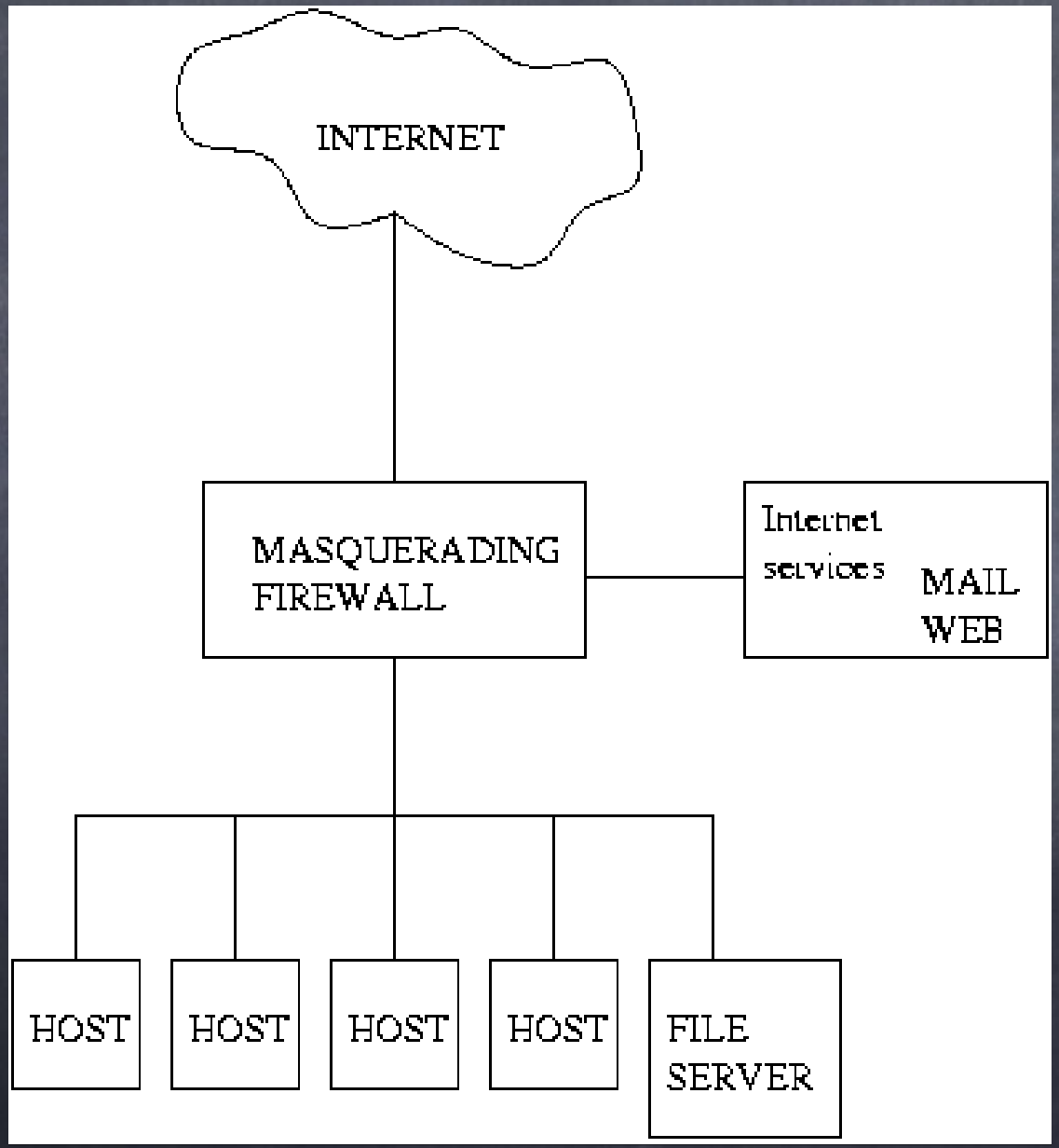
Coupe-feu dynamiques

- Les proxys ne sont pas très flexibles. Les coupe-feu dynamiques permettent d'utiliser les logiciels d'une façon plus transparente.
  - Il s'agit d'un filtre avancé qui permet de vérifier que les paquets appartiennent à une connexion déjà établie. C'est seulement lorsque c'est le cas que le paquet peut passer.
  - Parce qu'il est conscient d'une connexion, il peut appliquer NAT et/ou PAT :

    NAT a été mis au point à l'origine pour répondre à la pénurie d'adresses IP avec le protocole IPv4.

    - NAT Dynamique («Dynamic Network Address Translation») : Le coupe-feu traduit les adresses du réseau. Toutes les machines du réseau possèdent, vu de l'extérieur, la même adresse IP.
    - PAT («Port Address Translation») : Le coupe-feu traduit les numéros de port par lesquels les paquets arrivent sur les hôtes locaux.
  - Ces coupe-feu sont appelés coupe-feu avec mascarade.

Coupe-feu à mascarade



Filtrage dynamique étendu

Filtrage dynamique étendu

- Le filtrage des coupe-feu dynamiques n'est pas limité aux protocoles TCP/IP.

Filtrage dynamique étendu

- Le filtrage des coupe-feu dynamiques n'est pas limité aux protocoles TCP/IP.
- Pour des applications usuelles, le filtrage peut s'appliquer au protocole.

Filtrage dynamique étendu

- Le filtrage des coupe-feu dynamiques n'est pas limité aux protocoles TCP/IP.
- Pour des applications usuelles, le filtrage peut s'appliquer au protocole.
- Le coupe-feu peut ainsi détecter des comportements inhabituels.

Filtrage dynamique étendu

- Le filtrage des coupe-feu dynamiques n'est pas limité aux protocoles TCP/IP.
- Pour des applications usuelles, le filtrage peut s'appliquer au protocole.
- Le coupe-feu peut ainsi détecter des comportements inhabituels.
- Peut aussi filtrer certaines parties des données transmises :

Filtrage dynamique étendu

- Le filtrage des coupe-feu dynamiques n'est pas limité aux protocoles TCP/IP.
- Pour des applications usuelles, le filtrage peut s'appliquer au protocole.
- Le coupe-feu peut ainsi détecter des comportements inhabituels.
- Peut aussi filtrer certaines parties des données transmises :
  - Pour le protocole HTTP, le filtre peut supprimer les applications Java,

Filtrage dynamique étendu

- Le filtrage des coupe-feu dynamiques n'est pas limité aux protocoles TCP/IP.
- Pour des applications usuelles, le filtrage peut s'appliquer au protocole.
- Le coupe-feu peut ainsi détecter des comportements inhabituels.
- Peut aussi filtrer certaines parties des données transmises :
  - Pour le protocole HTTP, le filtre peut supprimer les applications Java,
  - Pour le protocole SMTP, le filtre peut supprimer les pièces jointes d'un certain type.

Conclusion sur les coupe-feu

Conclusion sur les coupe-feu

- Les coupe-feu permettent de filtrer le trafic entre le réseau local et l'Internet en n'administrant qu'une seule machine.

Conclusion sur les coupe-feu

- Les coupe-feu permettent de filtrer le trafic entre le réseau local et l'Internet en n'administrant qu'une seule machine.
- Les coupe-feu ne sont cependant pas une solution magique pour résoudre les problèmes causés par les attaques extérieures à un réseau local :

Conclusion sur les coupe-feu

- Les coupe-feu permettent de filtrer le trafic entre le réseau local et l'Internet en n'administrant qu'une seule machine.
- Les coupe-feu ne sont cependant pas une solution magique pour résoudre les problèmes causés par les attaques extérieures à un réseau local :
  - Les coupe-feu pour un seul ordinateur personnel peuvent offrir une solution sans trop d'entretien.

Conclusion sur les coupe-feu

- Les coupe-feu permettent de filtrer le trafic entre le réseau local et l'Internet en n'administrant qu'une seule machine.
- Les coupe-feu ne sont cependant pas une solution magique pour résoudre les problèmes causés par les attaques extérieures à un réseau local :
  - Les coupe-feu pour un seul ordinateur personnel peuvent offrir une solution sans trop d'entretien.
  - Les coupe-feu nécessitent des mises à jour fréquentes lorsque le réseau local est de bonne taille. Lorsque le réseau local change, la configuration du coupe-feu doit aussi changer.

Conclusion sur les coupe-feu

- Les coupe-feu permettent de filtrer le trafic entre le réseau local et l'Internet en n'administrant qu'une seule machine.
- Les coupe-feu ne sont cependant pas une solution magique pour résoudre les problèmes causés par les attaques extérieures à un réseau local :
  - Les coupe-feu pour un seul ordinateur personnel peuvent offrir une solution sans trop d'entretien.
  - Les coupe-feu nécessitent des mises à jour fréquentes lorsque le réseau local est de bonne taille. Lorsque le réseau local change, la configuration du coupe-feu doit aussi changer.
- Penser que l'installation d'un coupe-feu rend votre réseau sûr est un peu de la pensée magique (nécessaire, mais pas suffisant).

Logiciels malveillants

Logiciels malveillants

- Un adversaire peut, une fois passé le coupe-feu et les autres défenses, vouloir installer un programme malveillant sur la machine locale. Ceux-ci sont de trois types :

Logiciels malveillants

- Un adversaire peut, une fois passé le coupe-feu et les autres défenses, vouloir installer un programme malveillant sur la machine locale. Ceux-ci sont de trois types :
  - Chevaux de Troie : Programme qui semble tout à fait utile mais qui cache une fonction malveillante. Par exemple, donne accès à des données privées, donne des droits d'accès non autorisés ou détruit des données.

Logiciels malveillants

- Un adversaire peut, une fois passé le coupe-feu et les autres défenses, vouloir installer un programme malveillant sur la machine locale. Ceux-ci sont de trois types :
  - Chevaux de Troie : Programme qui semble tout à fait utile mais qui cache une fonction malveillante. Par exemple, donne accès à des données privées, donne des droits d'accès non autorisés ou détruit des données.
  - Virus : Programme qui infecte un autre programme sur votre ordinateur. À partir du programme infecté, le virus se propage vers d'autres programmes. Après un certain temps ou événement, les virus peuvent entreprendre certaines actions. Celles-ci peuvent être l'élimination de fichiers, la détérioration de fonctions du système d'exploitation, etc.

Logiciels malveillants

- Un adversaire peut, une fois passé le coupe-feu et les autres défenses, vouloir installer un programme malveillant sur la machine locale. Ceux-ci sont de trois types :
  - Chevaux de Troie : Programme qui semble tout à fait utile mais qui cache une fonction malveillante. Par exemple, donne accès à des données privées, donne des droits d'accès non autorisés ou détruit des données.
  - Virus : Programme qui infecte un autre programme sur votre ordinateur. À partir du programme infecté, le virus se propage vers d'autres programmes. Après un certain temps ou événement, les virus peuvent entreprendre certaines actions. Celles-ci peuvent être l'élimination de fichiers, la détérioration de fonctions du système d'exploitation, etc.
  - Vers : Programmes qui infectent un ordinateur sans avoir à être hébergés par d'autres programmes. Ils sont des programmes indépendants. Ils se multiplient en exploitant différentes ressources. Les objectifs de ces programmes peuvent être l'espionnage, l'ouverture de portes dérobées, émettre des requêtes vers un site Internet jusqu'à saturation...

Exemple

Exemple

- I Love You : Un ver lancé en 2000 et qui a atteint 3,1 millions de machines en 4 jours.

Exemple

- I Love You : Un ver lancé en 2000 et qui a atteint 3,1 millions de machines en 4 jours.
  - Infection : Le ver était dissimulé en pièce jointe d'un courriel. Cette pièce jointe était présentée comme Love-Letter-for-you.txt.vbs. L'extension vbs indique que le fichier est un script Visual Basic. Comme l'extension n'apparaît pas sur Windows, les utilisateurs voyaient la pièce jointe comme Love-Letter-for-you.txt.

Exemple

- I Love You : Un ver lancé en 2000 et qui a atteint 3,1 millions de machines en 4 jours.
  - Infection : Le ver était dissimulé en pièce jointe d'un courriel. Cette pièce jointe était présentée comme Love-Letter-for-you.txt.vbs. L'extension vbs indique que le fichier est un script Visual Basic. Comme l'extension n'apparaît pas sur Windows, les utilisateurs voyaient la pièce jointe comme Love-Letter-for-you.txt.
  - Objectif : Le script lisait la liste des contacts de l'utilisateur pour envoyer ce même message à ceux-ci. La plate-forme Windows était visée. Des fichiers étaient détruits et remplacés par ce script. Il changeait la page d'accueil d'Internet Explorer pour télécharger un cheval de Troie.

Exemple

Exemple

- Code Red : Un ver qui a infecté 359 000 ordinateurs en moins de 14 heures le 19 juillet 2001 :

Exemple

- Code Red : Un ver qui a infecté 359 000 ordinateurs en moins de 14 heures le 19 juillet 2001 :
  - Infections : Le ver se multipliait en essayant des adresses IP aléatoires pour ensuite infecter des serveurs qui faisaient tourner Microsoft IIS avec une faille de sécurité.

Exemple

- Code Red : Un ver qui a infecté 359 000 ordinateurs en moins de 14 heures le 19 juillet 2001 :
  - Infections : Le ver se multipliait en essayant des adresses IP aléatoires pour ensuite infecter des serveurs qui faisaient tourner Microsoft IIS avec une faille de sécurité.
  - Objectif : Monter une attaque par déni de service (DOS) contre la Maison-Blanche.

Exemple

- Code Red : Un ver qui a infecté 359 000 ordinateurs en moins de 14 heures le 19 juillet 2001 :
  - Infections : Le ver se multipliait en essayant des adresses IP aléatoires pour ensuite infecter des serveurs qui faisaient tourner Microsoft IIS avec une faille de sécurité.
  - Objectif : Monter une attaque par déni de service (DOS) contre la Maison-Blanche.
  - L'attaque a été facile à repousser, car le ver vérifiait, avant de lancer l'attaque, que le serveur à l'adresse IP (au lieu du nom de domaine) de la Maison-Blanche écoutait le port 80 (le port des serveurs Web). En changeant l'adresse IP de la Maison-Blanche, l'attaque a été repoussée.

Exemple

Exemple

- Cabir : Est un virus/ver (démonstration de faisabilité, «proof of concept») qui s'attaque à la téléphonie mobile. C'est un fichier de 15 ko nommé CARIBE.SIS :

Exemple

- Cabir : Est un virus/ver (démonstration de faisabilité, «proof of concept») qui s'attaque à la téléphonie mobile. C'est un fichier de 15 ko nommé CARIBE.SIS :
  - Infection : Se propage par la téléphonie mobile grâce à la technologie Bluetooth et le système d'exploitation Symbian OS.

Exemple

- Cabir : Est un virus/ver (démonstration de faisabilité, «proof of concept») qui s'attaque à la téléphonie mobile. C'est un fichier de 15 ko nommé CARIBE.SIS :
  - Infection : Se propage par la téléphonie mobile grâce à la technologie Bluetooth et le système d'exploitation Symbian OS.
  - Action : À chaque fois que le téléphone infecté est ouvert, le mot «Caribe» s'affiche. Il tente de se propager aux périphériques BlueTooth de la zone du téléphone infecté. Il n'est pas méchant, n'avait pour but que de démontrer la faisabilité...

Antivirus

Antivirus

- Les antivirus sont des programmes qui détectent les virus, les vers et les chevaux de Troie sur votre ordinateur. Ils les éliminent.

Antivirus

- Les antivirus sont des programmes qui détectent les virus, les vers et les chevaux de Troie sur votre ordinateur. Ils les éliminent.
- Ils visitent les fichiers sur votre disque dans le but de trouver des bouts de programmes reconnus comme dangereux.

Antivirus

- Les antivirus sont des programmes qui détectent les virus, les vers et les chevaux de Troie sur votre ordinateur. Ils les éliminent.
- Ils visitent les fichiers sur votre disque dans le but de trouver des bouts de programmes reconnus comme dangereux.
- Ceci est possible étant donné une base de données à jour contenant les virus connus sous la forme de signatures de virus. Une signature est un motif («pattern») qui caractérise un virus donné.

Antivirus

- Les antivirus sont des programmes qui détectent les virus, les vers et les chevaux de Troie sur votre ordinateur. Ils les éliminent.
- Ils visitent les fichiers sur votre disque dans le but de trouver des bouts de programmes reconnus comme dangereux.
- Ceci est possible étant donné une base de données à jour contenant les virus connus sous la forme de signatures de virus. Une signature est un motif («pattern») qui caractérise un virus donné.
- Un antivirus n'est efficace que si sa base de données est mise à jour constamment. Les compagnies d'antivirus vont vite pour mettre à jour leur base de données lorsqu'un nouveau virus est identifié.

Antivirus

- Les antivirus sont des programmes qui détectent les virus, les vers et les chevaux de Troie sur votre ordinateur. Ils les éliminent.
- Ils visitent les fichiers sur votre disque dans le but de trouver des bouts de programmes reconnus comme dangereux.
- Ceci est possible étant donné une base de données à jour contenant les virus connus sous la forme de signatures de virus. Une signature est un motif («pattern») qui caractérise un virus donné.
- Un antivirus n'est efficace que si sa base de données est mise à jour constamment. Les compagnies d'antivirus vont vite pour mettre à jour leur base de données lorsqu'un nouveau virus est identifié.
- Malheureusement, les utilisateurs tardent à mettre leur copie à jour causant bien des infections.

Tromper les antivirus

Tromper les antivirus

- De nouveaux virus utilisent les méthodes de la cryptographie pour déjouer les antivirus...

Tromper les antivirus

- De nouveaux virus utilisent les méthodes de la cryptographie pour déjouer les antivirus...
  - Des virus sont chiffrés pour les rendre non reconnaissables par les antivirus, car ils ont toujours un aspect différent.

Tromper les antivirus

- De nouveaux virus utilisent les méthodes de la cryptographie pour déjouer les antivirus...
  - Des virus sont chiffrés pour les rendre non reconnaissables par les antivirus, car ils ont toujours un aspect différent.
  - Ces virus ont un petit code en clair qui permet de les décoder et de les charger en mémoire pour être exécutés. Ce code est ce que les antivirus doivent détecter...

Tromper les antivirus

- De nouveaux virus utilisent les méthodes de la cryptographie pour déjouer les antivirus...
  - Des virus sont chiffrés pour les rendre non reconnaissables par les antivirus, car ils ont toujours un aspect différent.
  - Ces virus ont un petit code en clair qui permet de les décoder et de les charger en mémoire pour être exécutés. Ce code est ce que les antivirus doivent détecter...
- Ces virus sont de trois types :

Tromper les antivirus

- De nouveaux virus utilisent les méthodes de la cryptographie pour déjouer les antivirus...
  - Des virus sont chiffrés pour les rendre non reconnaissables par les antivirus, car ils ont toujours un aspect différent.
  - Ces virus ont un petit code en clair qui permet de les décoder et de les charger en mémoire pour être exécutés. Ce code est ce que les antivirus doivent détecter...
- Ces virus sont de trois types :
  - Oligomorphique : Le virus est chiffré à chaque réplication.

Tromper les antivirus

- De nouveaux virus utilisent les méthodes de la cryptographie pour déjouer les antivirus...
  - Des virus sont chiffrés pour les rendre non reconnaissables par les antivirus, car ils ont toujours un aspect différent.
  - Ces virus ont un petit code en clair qui permet de les décoder et de les charger en mémoire pour être exécutés. Ce code est ce que les antivirus doivent détecter...
- Ces virus sont de trois types :
  - Oligomorphique : Le virus est chiffré à chaque réplication.
  - Polymorphique : Le virus est chiffré et la routine de déchiffrement est capable de changer certaines de ses instructions au fil des réplications.

Tromper les antivirus

- De nouveaux virus utilisent les méthodes de la cryptographie pour déjouer les antivirus...
  - Des virus sont chiffrés pour les rendre non reconnaissables par les antivirus, car ils ont toujours un aspect différent.
  - Ces virus ont un petit code en clair qui permet de les décoder et de les charger en mémoire pour être exécutés. Ce code est ce que les antivirus doivent détecter...
- Ces virus sont de trois types :
  - Oligomorphique : Le virus est chiffré à chaque réplication.
  - Polymorphique : Le virus est chiffré et la routine de déchiffrement est capable de changer certaines de ses instructions au fil des réplications.
  - Métamorphique : Le virus change de forme au fil des réplications.

Intrusions

Intrusions

- Pour qu'un virus, ver ou cheval de Troie soit délétère, encore faut-il qu'il s'installe sur votre machine.

Intrusions

- Pour qu'un virus, ver ou cheval de Troie soit délétère, encore faut-il qu'il s'installe sur votre machine.
- Même si un adversaire peut parler à votre machine, ceci n'implique pas qu'il peut installer un logiciel sur celle-ci, encore moins s'il n'en est pas un utilisateur.

Intrusions

- Pour qu'un virus, ver ou cheval de Troie soit délétère, encore faut-il qu'il s'installe sur votre machine.
- Même si un adversaire peut parler à votre machine, ceci n'implique pas qu'il peut installer un logiciel sur celle-ci, encore moins s'il n'en est pas un utilisateur.
- Pour ce faire, les adversaires peuvent essayer diverses stratégies :

Intrusions

- Pour qu'un virus, ver ou cheval de Troie soit délétère, encore faut-il qu'il s'installe sur votre machine.
- Même si un adversaire peut parler à votre machine, ceci n'implique pas qu'il peut installer un logiciel sur celle-ci, encore moins s'il n'en est pas un utilisateur.
- Pour ce faire, les adversaires peuvent essayer diverses stratégies :
  - Faiblesses du système d'exploitation ou du logiciel du serveur. Nous allons voir un exemple de ce type d'attaque : attaques par débordement. Une page Web n'est pas un objet passif. Elle peut contenir du code (JavaScript, Perl, etc.) malveillant.

Intrusions

- Pour qu'un virus, ver ou cheval de Troie soit délétère, encore faut-il qu'il s'installe sur votre machine.
- Même si un adversaire peut parler à votre machine, ceci n'implique pas qu'il peut installer un logiciel sur celle-ci, encore moins s'il n'en est pas un utilisateur.
- Pour ce faire, les adversaires peuvent essayer diverses stratégies :
  - Faiblesses du système d'exploitation ou du logiciel du serveur. Nous allons voir un exemple de ce type d'attaque : attaques par débordement. Une page Web n'est pas un objet passif. Elle peut contenir du code (JavaScript, Perl, etc.) malveillant.
  - Tromper l'utilisateur : C'est peut-être plus simple. Cas spécial du piratage psychologique. Cliquer ici pour installer un joli logiciel... il faut espérer que l'antivirus détecte ceci avant qu'il ne soit trop tard.

Détecter les intrusions

Détecter les intrusions

- Une façon différente de détecter les logiciels ou utilisateurs malveillants consiste à détecter les comportements malveillants.

Détecter les intrusions

- Une façon différente de détecter les logiciels ou utilisateurs malveillants consiste à détecter les comportements malveillants.
- Un système peut surveiller les processus pour détecter les comportements malveillants.

Détecter les intrusions

- Une façon différente de détecter les logiciels ou utilisateurs malveillants consiste à détecter les comportements malveillants.
- Un système peut surveiller les processus pour détecter les comportements malveillants.
- Une telle approche a l'avantage de ne pas dépendre d'information sur les virus et les attaques.

Détecter les intrusions

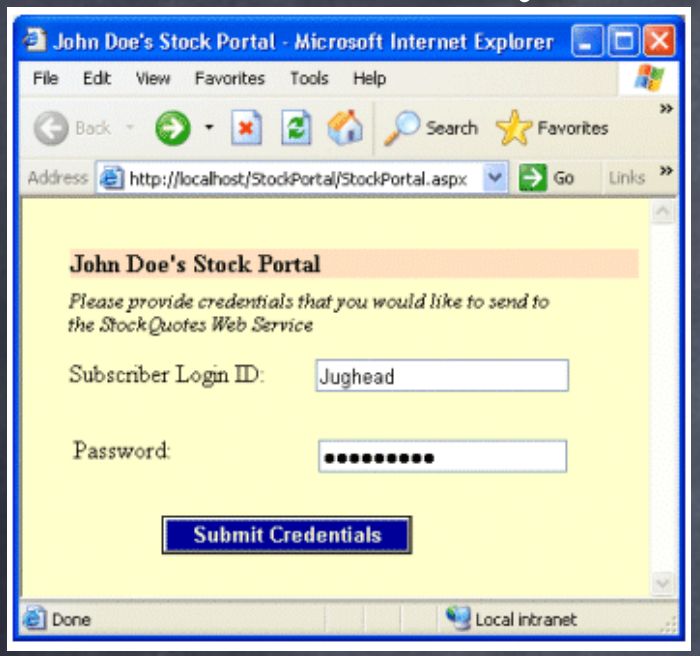
- Une façon différente de détecter les logiciels ou utilisateurs malveillants consiste à détecter les comportements malveillants.
- Un système peut surveiller les processus pour détecter les comportements malveillants.
- Une telle approche a l'avantage de ne pas dépendre d'information sur les virus et les attaques.
- Un coupe-feu dynamique est un exemple de cette approche :

Détecter les intrusions

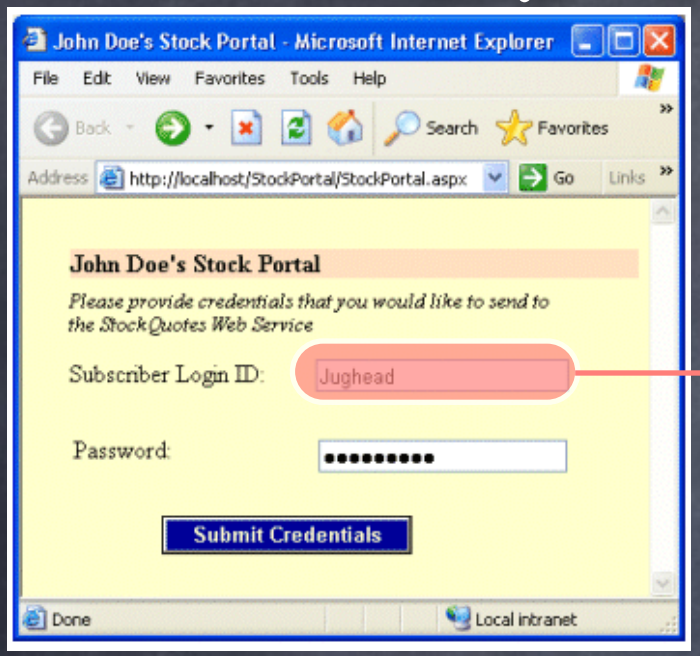
- Une façon différente de détecter les logiciels ou utilisateurs malveillants consiste à détecter les comportements malveillants.
- Un système peut surveiller les processus pour détecter les comportements malveillants.
- Une telle approche a l'avantage de ne pas dépendre d'information sur les virus et les attaques.
- Un coupe-feu dynamique est un exemple de cette approche :
  - Il surveille les connexions et tente de déterminer si un client transmet des données à contenu suspect (comme la taille).

Requêtes malveillantes

Requêtes malveillantes

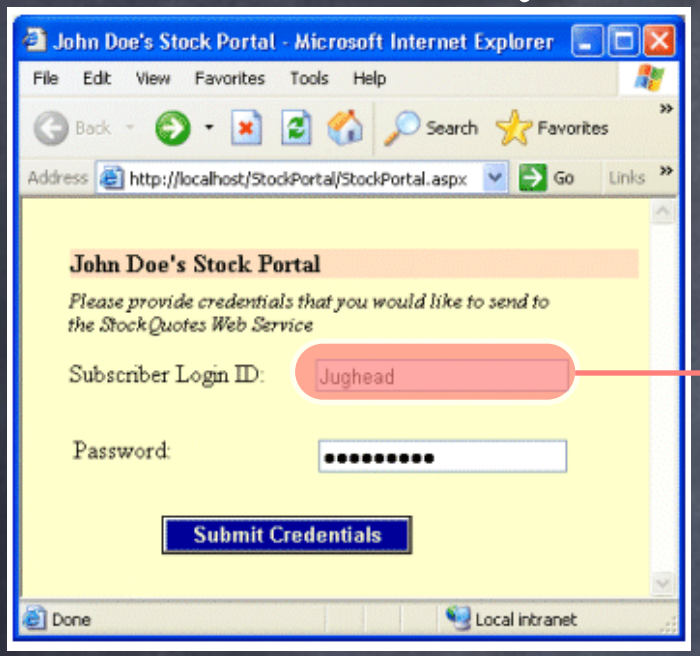


Requêtes malveillantes



dlkjfdsflkjsd fjdskl ;gfjdls;kewqewewewewhdfbfbfbww
jaskhfdkjsahfkjhsdkjfhkjhfkasjhjkfhakjfhaskjhfjkashf
wewqewqewqewqewqewqeweekjwweeqqqsxcswdsddddds
ffhasjfkhsakjfhkjashfkjsahfkjsahfkjsahkjsahhjsakfhsa
kjhfkaslhfklahsflkhaskhffwewaaeewfrfdsdfcddsdqqwwq
d;gdhsgkjdsjgnbfds,gmnnbfdngbdfmngbmds,nfbgsd,bgds
hgfkdshhgjdkshgklsjhdgkjhsoieruoiwueroiuwqehdas,mnf,
mnsdfgswjuoiewuorasnf,mnsdaf,mnbdsf,ghdskjgfhdsgfiho
iehjrfswewqewqewqewqewqewqeweekwqwqwefdscxcccj
ffhasjfkhsakjfhkjashfkjsahfkjsahfkjsahkjsahhjsakfhsa
kjhfkaslhfklahsflkhaskhffweqeewqwedqcxcxcxzcxzcwq
d;gdhsgkjdsjgnbfds,gmnnbfdngbdfmngbmds,nfbgsd,bgds
hgfkdshhgjdkshgklsjhdgkjhsoieruoiwueroiuwqehdas,mnf,
mnsdfgswjuoiewuorasnf,mnsdaf,mnbdsf,ghdskjgfhdsgfiho
iehjrfs.....saDSADSADSAD.DS.D.S.DSSD.SD.S.....

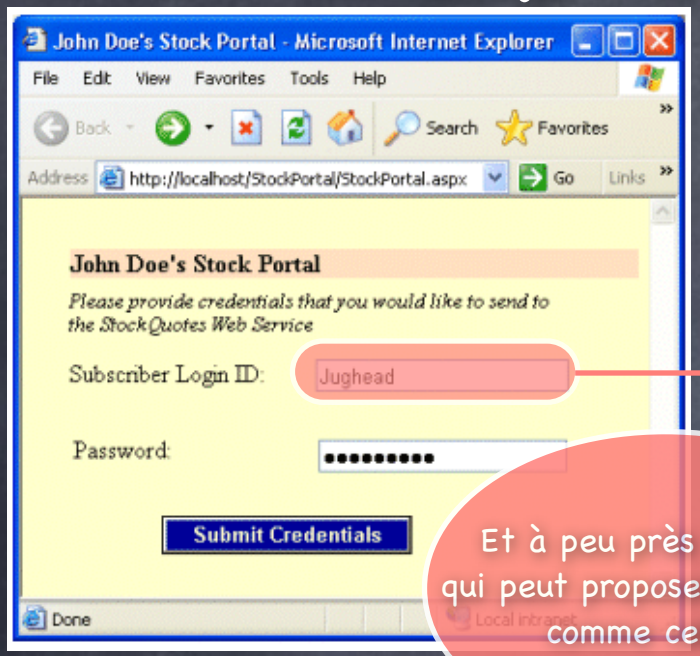
Requêtes malveillantes



dlkjfdsflkjsd fjdskl ;gfjdls;kewqewewewewhdfbfbfbww
jaskhfdkjsahfkjhsdkjfhkjhfkasjhjkfhakjfhaskjhfjkashf
wewqewqewqewqewqewqeweekjwweeqqqsxcswdsddddds
ffhasjfkhsakjfhkjashfkjsahfkjsahfkjsahkjsahhjsakfhsa
kjhfkaslhfklahsflkhaskhffwewaaeewfrfdsdfcddsdqqwwq
d;gdhsgkjdsjgnbfds,gmnnbfdngbdfmngbmds,nfbgsd,bgds
hgfkdshhgjdkshgklsjhdgkjhsoieruoiwueroiuwqehdas,mnf,
mnsdfgswjuoiewuorasnf,mnsdaf,mnbdsf,ghdskjgfhdsgfiho
iehjrfswewqewqewqewqewqewqeweekwqwqwefdscxcccj
ffhasjfkhsakjfhkjashfkjsahfkjsahfkjsahkjsahhjsakfhsa
kjhfkaslhfklahsflkhaskhffweqeewqwedqcxcxcxzcxzcwq
d;gdhsgkjdsjgnbfds,gmnnbfdngbdfmngbmds,nfbgsd,bgds
hgfkdshhgjdkshgklsjhdgkjhsoieruoiwueroiuwqehdas,mnf,
mnsdfgswjuoiewuorasnf,mnsdaf,mnbdsf,ghdskjgfhdsgfiho
iehjrfs.....saDSADSADSAD.DS.D.S.DSSD.SD.S.....

Il arrive que de longues requêtes puissent faire planter un système mal programmé. Un adversaire peut donc soumettre des chaînes très longues dans le but de rendre le système inopérant (ou même pire, assujetti!) comme nous le verrons plus loin...

Requêtes malveillantes

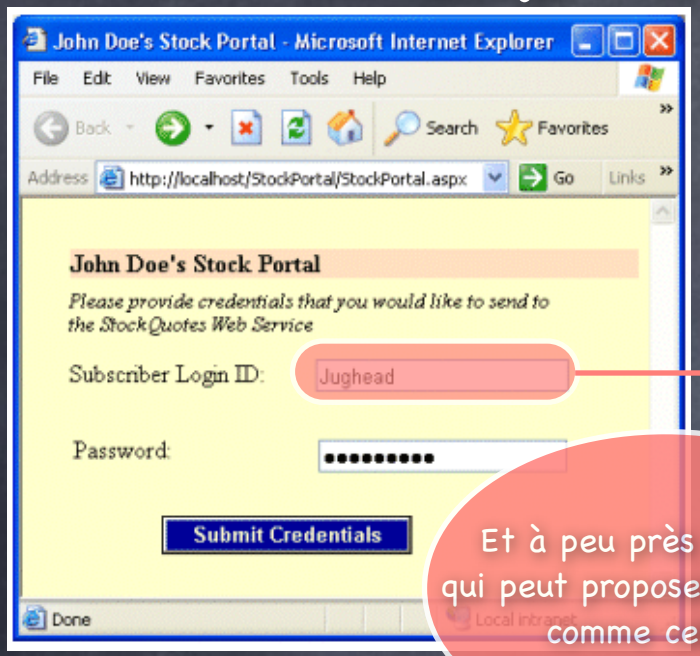


Et à peu près n'importe qui peut proposer un service comme celui-ci.

dlkjfdsflkjsd fjdskl ;gfjdls;kewqewewewewhdfbfbfbww
jaskhfdkjsahfkjhsdkjfhkjhfkasjhjkfhakjfhaskjhfjkashf
wewqewqewqewqewqewqeweekjwweeqqqsxcswdsddddds
ffhasjfkhsakjfhkjashfkjsahfkjsahfkjsahkjsahhjsakfhsa
kjhfkaslhfklahsflkhaskhffwewaaeewfrfdsdfcddsdqqwwq
d;gdhsgkjdsjgnbfds,gmnnbfdngbdfmngbmds,nfbgsd,bgds
hgfkdshhgjdkshgklsjhdgkjhsoieruoiwueroiuwqehdas,mnf,
mnsdfgswjuoiewuorasnf,mnsdaf,mnbdsf,ghdskjgfhdsgfiho
iehjrfswewqewqewqewqewqewqeweekwqwqwefdscxcccj
ffhasjfkhsakjfhkjashfkjsahfkjsahfkjsahkjsahhjsakfhsa
kjhfkaslhfklahsflkhaskhffweqeewqwedqcxcxcxzcxzcwq
d;gdhsgkjdsjgnbfds,gmnnbfdngbdfmngbmds,nfbgsd,bgds
hgfkdshhgjdkshgklsjhdgkjhsoieruoiwueroiuwqehdas,mnf,
mnsdfgswjuoiewuorasnf,mnsdaf,mnbdsf,ghdskjgfhdsgfiho
iehjrfs.....saDSADSADSAD.DS.D.S.DSSD.SD.S.....

Il arrive que de longues requêtes puissent faire planter un système mal programmé. Un adversaire peut donc soumettre des chaînes très longues dans le but de rendre le système inopérant (ou même pire, assujetti!) comme nous le verrons plus loin...

Requêtes malveillantes



Et à peu près n'importe qui peut proposer un service comme celui-ci.

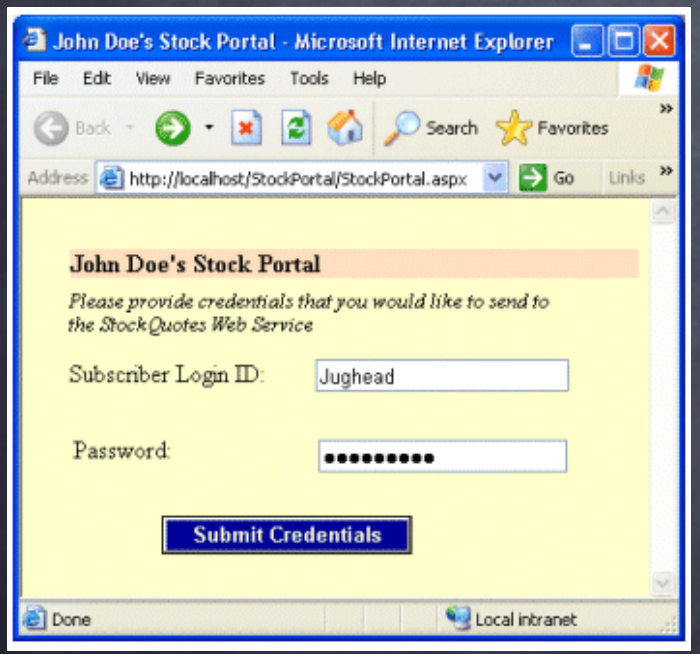
dlkjfdsflkjsd fjdskl ;gfjdls;kewqewewewewhdfbfbfbww
jaskhfdkjsahfkjhsdkjfhkjhfkasjhjkfhakjfhaskjhfjkashf
wewqewqewqewqewqewqeweekjwweeqqqsxcswdsddddds
ffhasjfkhsakjfhkjashfkjsahfkjsahfkjsahkjsahhjsakfhsa
kjhfkaslhfklahsflkhaskhffwewaaeewfrfdsdfcddsdqqwwq
d;gdhsgkjdsjgnbfds,gmnnbfdngbdfmngbmds,nfbgsd,bgds
hgfkdshhgjdkshgklsjhdgkjhsoieruoiwueroiuwqehdas,mnf,
mnsdfgswjuoiewuorasnf,mnsdaf,mnbdsf,ghdskjgfhdsgfiho
iehjrfswewqewqewqewqewqewqeweekwqwqwefdscxcccj
ffhasjfkhsakjfhkjashfkjsahfkjsahfkjsahkjsahhjsakfhsa
kjhfkaslhfklahsflkhaskhffweqeewqwedqcxcxcxzcxzcwq
d;gdhsgkjdsjgnbfds,gmnnbfdngbdfmngbmds,nfbgsd,bgds
hgfkdshhgjdkshgklsjhdgkjhsoieruoiwueroiuwqehdas,mnf,
mnsdfgswjuoiewuorasnf,mnsdaf,mnbdsf,ghdskjgfhdsgfiho
iehjrfs.....saDSADSADSAD.DS.D.S.DSSD.SD.S.....

Il arrive que de longues requêtes puissent faire planter un système mal programmé. Un adversaire peut donc soumettre des chaînes très longues dans le but de rendre le système inopérant (ou même pire, assujetti!) comme nous le verrons plus loin...

Un coupe-feu peut filtrer les requêtes anormalement longues pour les ignorer. Même les systèmes avec programmes erronés seront à l'abri de ce type d'attaque.

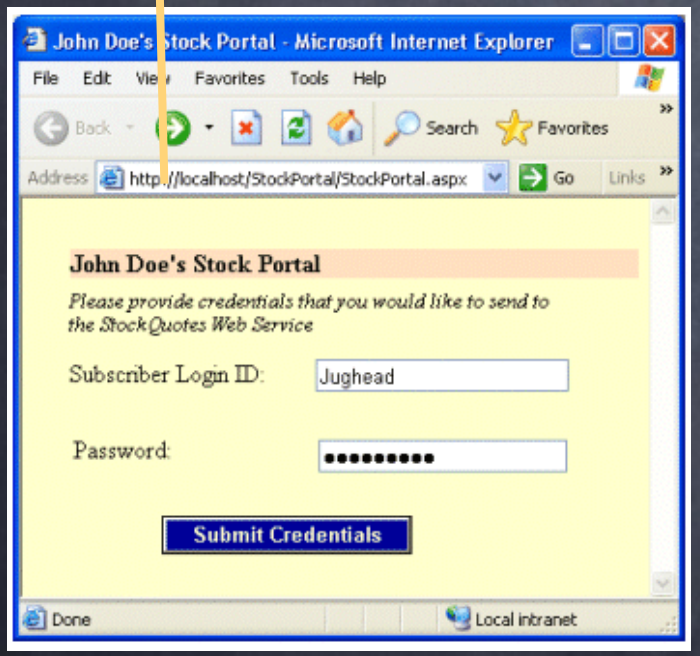
Requêtes malveillantes

Requêtes malveillantes



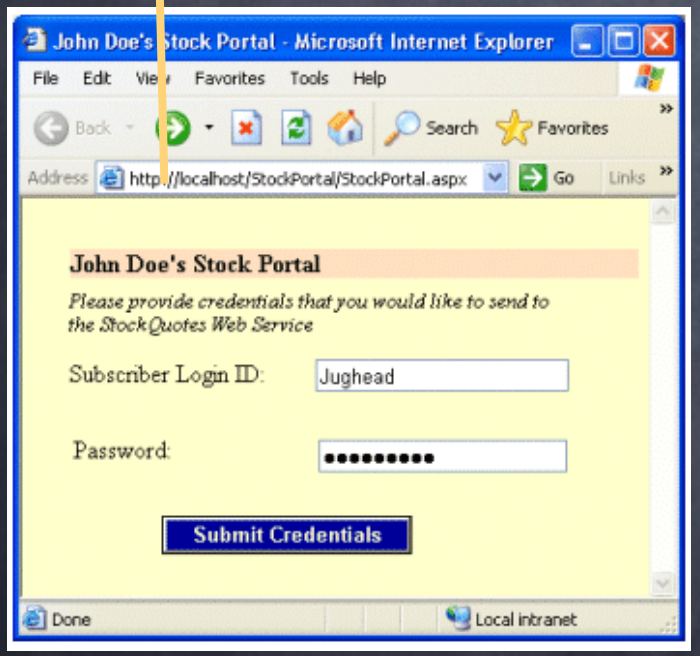
Requêtes malveillantes

HTTPS://...



Requêtes malveillantes

HTTPS://...

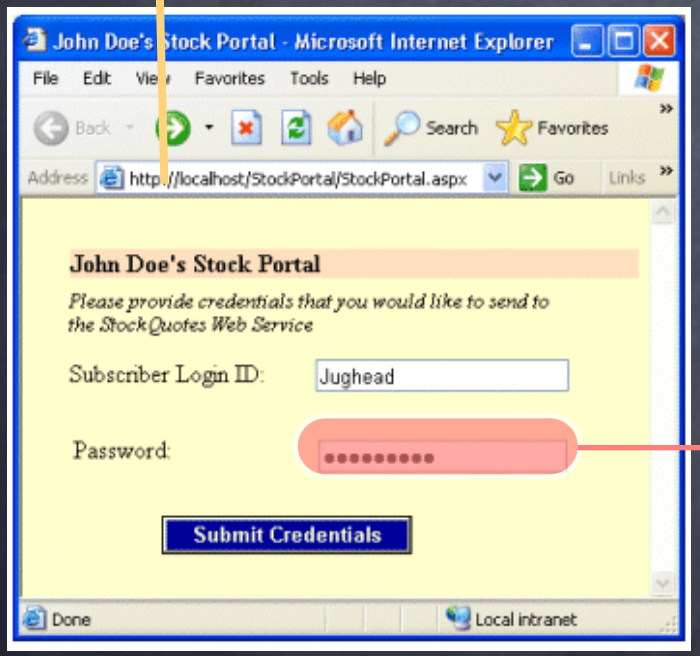


Script du serveur

```
R-SQL <-'SELECT *
        FROM Passwords
        WHERE user=$input1 AND password=$input2'
SI Execute(R-SQL) est vide ALORS AVORTER.
...
```

Requêtes malveillantes

HTTPS://...



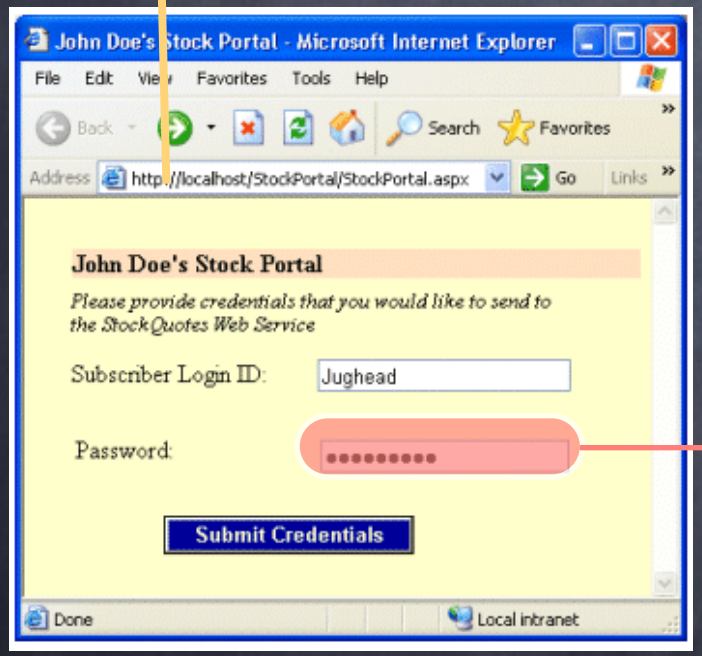
Script du serveur

```
R-SQL <-'SELECT *
        FROM Passwords
        WHERE user=$input1 AND password=$input2'
SI Execute(R-SQL) est vide ALORS AVORTER.
...
```

Password : x' OR '1'='1

Requêtes malveillantes

HTTPS://...



Script du serveur

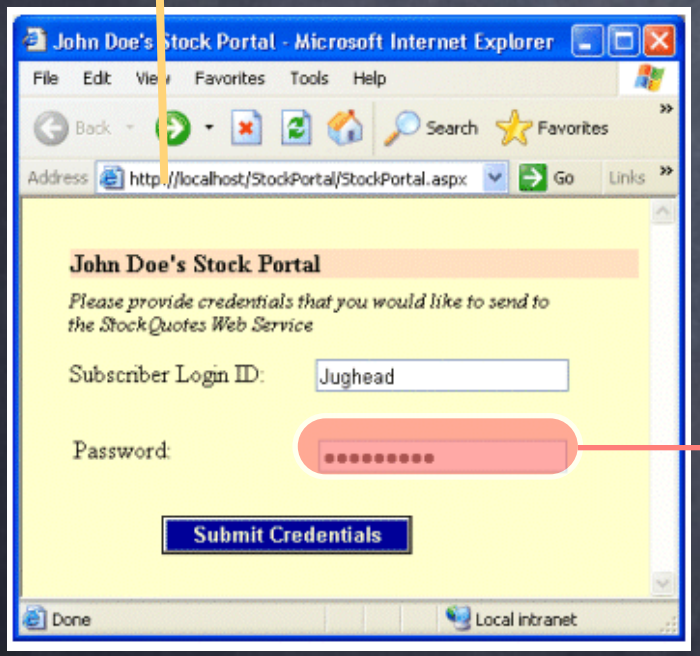
```
R-SQL <-'SELECT *
        FROM Passwords
        WHERE user=$input1 AND password=$input2'
SI Execute(R-SQL) est vide ALORS AVORTER.
...
```

Password : x' OR '1'='1

```
SELECT *
FROM Passwords
WHERE user='Jughead' AND password='x' OR
'1'='1'
```

Requêtes malveillantes

HTTPS://...



Script du serveur

```
R-SQL <-'SELECT *
        FROM Passwords
        WHERE user=$input1 AND password=$input2'
SI Execute(R-SQL) est vide ALORS AVORTER.
...
```

Password : x' OR '1'='1

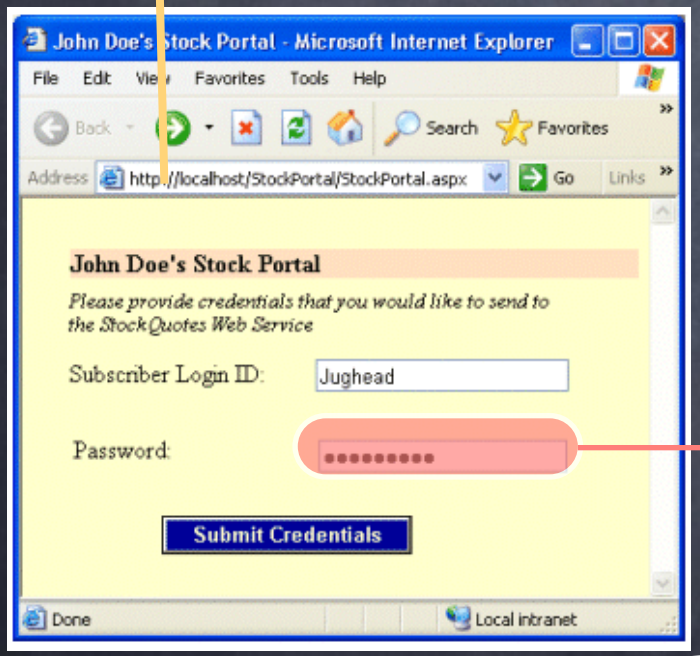
```
SELECT *
FROM Passwords
WHERE user='Jughead' AND password='x' OR
'1'='1'
```

Un coupe-feu dynamique peut filtrer des requêtes bizarres comme

x' OR '1'='1

Requêtes malveillantes

HTTPS://...



Script du serveur

```
R-SQL <-'SELECT *
        FROM Passwords
        WHERE user=$input1 AND password=$input2'
SI Execute(R-SQL) est vide ALORS AVORTER.
...
```

Password : x' OR '1'='1

```
SELECT *
FROM Passwords
WHERE user='Jughead' AND password='x' OR
'1'='1'
```

Ceci est beaucoup plus difficile à réaliser par un coupe-feu que l'exemple précédent.

Un coupe-feu dynamique peut filtrer des requêtes bizarres comme x' OR '1'='1

Approche comportementale

Approche comportementale

- Une autre approche pour la détection d'intrusions consiste à observer certains aspects du comportement des utilisateurs et programmes :

Approche comportementale

- Une autre approche pour la détection d'intrusions consiste à observer certains aspects du comportement des utilisateurs et programmes :
  - activités de connexion et de session,

Approche comportementale

- Une autre approche pour la détection d'intrusions consiste à observer certains aspects du comportement des utilisateurs et programmes :
  - activités de connexion et de session,
  - activités reliées à l'exécution de programme et d'accès aux fichiers.

Approche comportementale

- Une autre approche pour la détection d'intrusions consiste à observer certains aspects du comportement des utilisateurs et programmes :
  - activités de connexion et de session,
  - activités reliées à l'exécution de programme et d'accès aux fichiers.
- Il y a deux approches pour la détection de comportements suspects :

Approche comportementale

- Une autre approche pour la détection d'intrusions consiste à observer certains aspects du comportement des utilisateurs et programmes :
  - activités de connexion et de session,
  - activités reliées à l'exécution de programme et d'accès aux fichiers.
- Il y a deux approches pour la détection de comportements suspects :
  - Par règles (rule-based) : Un ensemble de règles décrivant les comportements normaux est établi. Les comportements anormaux (trop loin des normaux) sont rejetés.

Approche comportementale

- Une autre approche pour la détection d'intrusions consiste à observer certains aspects du comportement des utilisateurs et programmes :
  - activités de connexion et de session,
  - activités reliées à l'exécution de programme et d'accès aux fichiers.
- Il y a deux approches pour la détection de comportements suspects :
  - Par règles (rule-based) : Un ensemble de règles décrivant les comportements normaux est établi. Les comportements anormaux (trop loin des normaux) sont rejetés.
  - Statistique : Des statistiques sur les utilisateurs normaux sont créées. Le comportement de l'utilisateur/programme observé est comparé aux statistiques. Un comportement montrant un trop grand écart avec les statistiques est rejeté.

Problèmes avec les systèmes de détection d'intrusion (IDS)

Problèmes avec les systèmes de détection d'intrusion (IDS)

- Le problème majeur avec l'approche est le même qu'avec la biométrie. Le système qui surveille doit être assez tolérant pour autoriser les comportements normaux, mais suffisamment restrictif pour attraper les acteurs malveillants :

Problèmes avec les systèmes de détection d'intrusion (IDS)

- Le problème majeur avec l'approche est le même qu'avec la biométrie. Le système qui surveille doit être assez tolérant pour autoriser les comportements normaux, mais suffisamment restrictif pour attraper les acteurs malveillants :
  - Ce problème n'est pas très bien compris et les solutions proposées ne sont pas tout à fait satisfaisantes.

Problèmes avec les systèmes de détection d'intrusion (IDS)

- Le problème majeur avec l'approche est le même qu'avec la biométrie. Le système qui surveille doit être assez tolérant pour autoriser les comportements normaux, mais suffisamment restrictif pour attraper les acteurs malveillants :
  - Ce problème n'est pas très bien compris et les solutions proposées ne sont pas tout à fait satisfaisantes.
- La détection d'intrusion est bien inutile si le système ne réagit pas de la bonne façon lorsqu'une intrusion est détectée. La partie du système qui alerte l'administrateur, qui interdit l'accès, qui effectue quelque autre tâche pour éliminer la menace est tout aussi importante que celle qui détecte.

Le pot de miel

Le pot de miel

- Le pot de miel («honey pot») est un truc pratique pour la détection d'intrusions.

Le pot de miel

- Le pot de miel («honey pot») est un truc pratique pour la détection d'intrusions.
  - Une ressource bidon qui semble intéressante pour un adversaire est créée.

Le pot de miel

- Le pot de miel («honey pot») est un truc pratique pour la détection d'intrusions.
  - Une ressource bidon qui semble intéressante pour un adversaire est créée.
  - Puisque celle-ci est bidon, on peut supposer que si quelqu'un y accède, c'est qu'il s'adonne à une activité malveillante.

Le pot de miel

- Le pot de miel («honey pot») est un truc pratique pour la détection d'intrusions.
  - Une ressource bidon qui semble intéressante pour un adversaire est créée.
  - Puisque celle-ci est bidon, on peut supposer que si quelqu'un y accède, c'est qu'il s'adonne à une activité malveillante.
  - En consultant les traces, il peut être possible de retrouver l'utilisateur malveillant.

Le pot de miel

- Le pot de miel («honey pot») est un truc pratique pour la détection d'intrusions.
  - Une ressource bidon qui semble intéressante pour un adversaire est créée.
  - Puisque celle-ci est bidon, on peut supposer que si quelqu'un y accède, c'est qu'il s'adonne à une activité malveillante.
  - En consultant les traces, il peut être possible de retrouver l'utilisateur malveillant.
  - Ceci peut se faire à l'insu de l'intrus...

Exemple

Exemple

- Un hôpital américain soupçonnait que quelqu'un consultait les dossiers de patients sans en avoir l'autorisation.

Exemple

- Un hôpital américain soupçonnait que quelqu'un consultait les dossiers de patients sans en avoir l'autorisation.
- Ils ont créé des fichiers pour des patients qui n'existent pas.

Exemple

- Un hôpital américain soupçonnait que quelqu'un consultait les dossiers de patients sans en avoir l'autorisation.
- Ils ont créé des fichiers pour des patients qui n'existent pas.
- Les accès à ces fichiers ont alors été retracés jusqu'à l'utilisateur malveillant.

Les attaques de l'intérieur

Les attaques de l'intérieur

- Presque tout ce que nous avons vu a pour but la protection contre les attaques venues de l'extérieur.

Les attaques de l'intérieur

- Presque tout ce que nous avons vu a pour but la protection contre les attaques venues de l'extérieur.
- Les attaques peuvent très bien émaner de l'intérieur et peuvent causer des problèmes sérieux.

Les attaques de l'intérieur

- Presque tout ce que nous avons vu a pour but la protection contre les attaques venues de l'extérieur.
- Les attaques peuvent très bien émaner de l'intérieur et peuvent causer des problèmes sérieux.
- Le première chose à comprendre est qu'il n'est pas possible de se prémunir contre ces attaques si les utilisateurs ont tous les droits sur le système cible.

Les attaques de l'intérieur

- Presque tout ce que nous avons vu a pour but la protection contre les attaques venues de l'extérieur.
- Les attaques peuvent très bien émaner de l'intérieur et peuvent causer des problèmes sérieux.
- Le première chose à comprendre est qu'il n'est pas possible de se prémunir contre ces attaques si les utilisateurs ont tous les droits sur le système cible.
- Il est donc nécessaire qu'une partie du système soit garantie de fonctionner selon ses spécifications, même sous attaque.

Les attaques de l'intérieur

- Presque tout ce que nous avons vu a pour but la protection contre les attaques venues de l'extérieur.
- Les attaques peuvent très bien émaner de l'intérieur et peuvent causer des problèmes sérieux.
- Le première chose à comprendre est qu'il n'est pas possible de se prémunir contre ces attaques si les utilisateurs ont tous les droits sur le système cible.
- Il est donc nécessaire qu'une partie du système soit garantie de fonctionner selon ses spécifications, même sous attaque.
- Sans cette hypothèse, le système est sous le contrôle complet de l'adversaire.

Base informatique sécurisée

«trusted computing base» (TCB)

Base informatique sécurisée
«trusted computing base» (TCB)

- Une base sécurisée peut être établie en utilisant de la sécurité matérielle, logicielle, par mot de passe par exemple.

Base informatique sécurisée

«trusted computing base» (TCB)

- Une base sécurisée peut être établie en utilisant de la sécurité matérielle, logicielle, par mot de passe par exemple.
- Le rôle de ce système de base est de contrôler l'accès aux ressources et le flux d'information sur celui-ci.

Base informatique sécurisée
«trusted computing base» (TCB)

- Une base sécurisée peut être établie en utilisant de la sécurité matérielle, logicielle, par mot de passe par exemple.
- Le rôle de ce système de base est de contrôler l'accès aux ressources et le flux d'information sur celui-ci.
- Pour bien comprendre comment ces protections fonctionnent, nous devons mettre de l'ordre dans nos idées. Nous devons voir à quoi ressemble une politique de sécurité dans ce scénario.

Base informatique sécurisée
«trusted computing base» (TCB)

- Une base sécurisée peut être établie en utilisant de la sécurité matérielle, logicielle, par mot de passe par exemple.
- Le rôle de ce système de base est de contrôler l'accès aux ressources et le flux d'information sur celui-ci.
- Pour bien comprendre comment ces protections fonctionnent, nous devons mettre de l'ordre dans nos idées. Nous devons voir à quoi ressemble une politique de sécurité dans ce scénario.
- C'est notre prochain sujet...