# Réseaux fixes
# II.3 Sécurité
# Généralités et ACL

Luc Deneire

EII-5, Option Réseaux et Objets Connectés (ROC)

# Objectifs de la partie “généralités”

| | |
|---|---|
| **État actuel de la cybersécurité:** | Décrire l'état actuel de la cybersécurité et les vecteurs de perte de données. |
| **Acteurs de menace** | Décrire les outils utilisés par les acteurs de menace pour attaquer les réseaux. |
| **Logiciel malveillant** | Décrire les types des Logiciels malveillants. |
| **Attaques réseau courantes** | Décrire les attaques réseau courantes. |
| **Menaces et vulnérabilités liées au protocole IP** | Expliquer comment les vulnérabilités liées au protocole IP sont exploitées par les acteurs de menace. |
| **Vulnérabilités liées aux protocoles TCP et UDP** | Expliquer comment les vulnérabilités liées aux protocoles TCP et UDP sont exploitées par les acteurs de menace. |
| **Services IP** | Expliquer comment les services IP sont exploités par les acteurs de menace. |
| **Meilleures pratiques de sécurité réseau** | Décrire les meilleures pratiques de protection d'un réseau. |
| **Cryptographie** | Décrire les processus cryptographiques courants utilisés pour protéger les données en transit. |

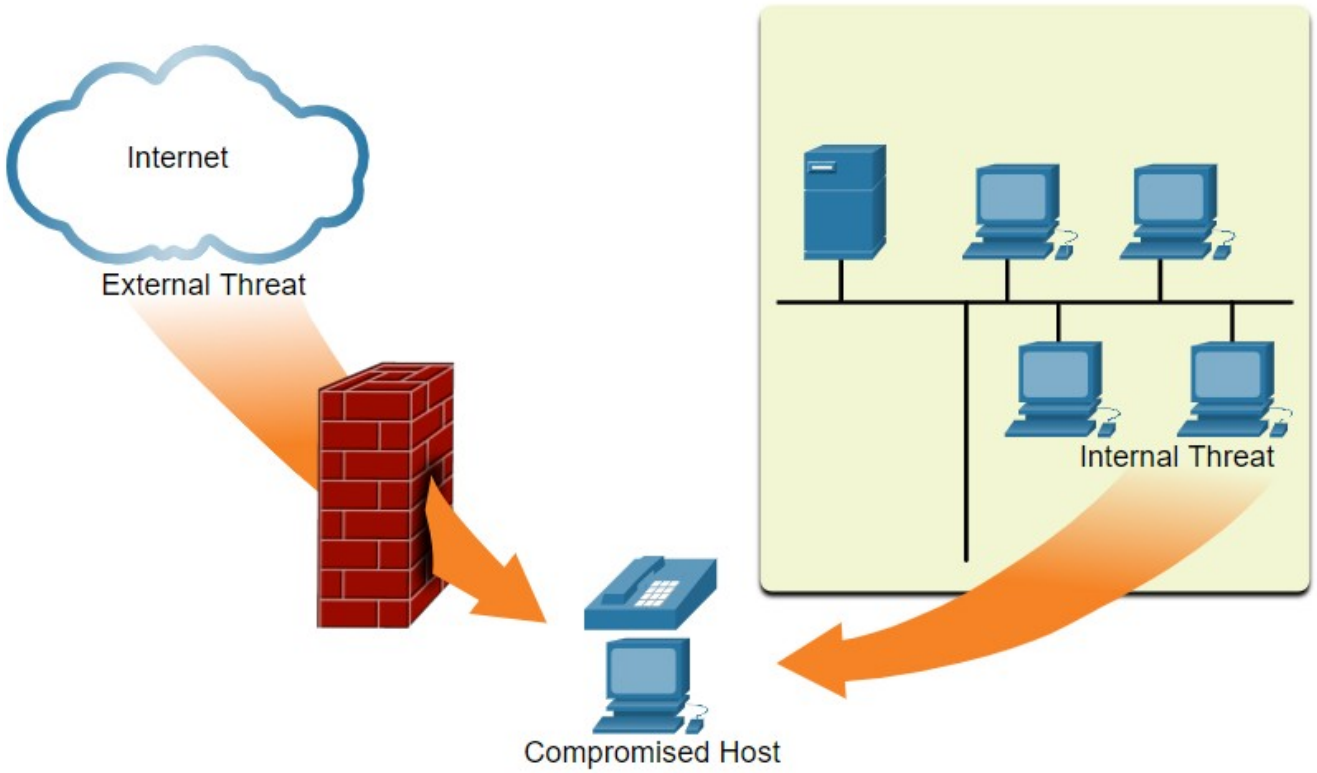
# État actuel des affaires

- Les cybercriminels disposent désormais de l'expertise et des outils nécessaires pour éliminer les infrastructures et les systèmes critiques. Leurs outils et techniques continuent d'évoluer.
- Le maintien d'un réseau sécurisé garantit la sécurité des utilisateurs du réseau et protège les intérêts commerciaux. Tous les utilisateurs doivent connaître les termes de sécurité du tableau.

| Termes de sécurité | Description |
|---|---|
| **Actifs (asset)** | Un actif est tout ce qui a de la valeur pour l'organisation. Cela comprend les personnes, l'équipement, les ressources et les données. |
| **Vulnérabilité** | Une vulnérabilité est une faiblesse d'un système, ou de sa conception, qui pourrait être exploitée par une menace. |
| **Menace** | Une menace est un danger potentiel pour les actifs, les données ou les fonctionnalités réseau d'une entreprise. |
| **Exploiter** | Un exploit est un mécanisme qui tire parti d'une vulnérabilité. |
| **Atténuation** | L'atténuation est la contre-mesure qui réduit la probabilité ou la gravité d'une menace ou d'un risque potentiel. La sécurité du réseau implique plusieurs techniques d'atténuation. |
| **Risque** | Le risque est la probabilité qu'une menace exploite la vulnérabilité d'un actif, dans le but d'affecter négativement une organisation. Le risque est mesuré en utilisant la probabilité de survenance d'un événement et ses conséquences. |

# Vecteurs d'attaques réseau

- Un vecteur d'attaque est un chemin par lequel un acteur de menace peut accéder à un serveur, un hôte ou un réseau. Les vecteurs d'attaque proviennent de l'intérieur ou de l'extérieur du réseau d'entreprise, comme le montre la figure.
- Les menaces internes ont le potentiel de causer des dommages plus importants que les menaces externes car les utilisateurs internes ont un accès direct au bâtiment et à ses équipements d'infrastructure.



# Perte de données

La perte ou l'exfiltration de données se produit lorsque les données sont intentionnellement ou involontairement perdues, volées ou divulguées au monde extérieur. La perte de données peut entraîner:

- Dommages à la marque et perte de réputation
- Perte d'avantage concurrentiel
- Perte de clients
- Perte de revenus
- Litiges/actions en justice entraînant des amendes et des sanctions civiles
- Coûts et efforts importants pour informer les parties concernées et se remettre de la violation

Les professionnels de la sécurité réseau doivent protéger les données de l'organisation. Divers contrôles de prévention des pertes de données (DLP) doivent être mis en œuvre qui combinent des mesures stratégiques, opérationnelles et tactiques.

# Perte de données (suite)

| Vecteurs de perte de données | Description |
|---|---|
| **Courriel / Réseaux sociaux** | Les e-mails ou les messages instantanés interceptés peuvent être capturés et révéler des informations confidentielles. |
| **Appareils non chiffrés** | Si les données ne sont pas stockées à l'aide d'un algorithme de cryptage, le voleur peut récupérer des données confidentielles précieuses. |
| **Périphériques de stockage cloud** | Les données sensibles peuvent être perdues si l'accès au cloud est compromis en raison de faibles paramètres de sécurité. |
| **Supports amovibles** | L'un des risques est qu'un employé puisse effectuer un transfert non autorisé de données vers une clé USB. Un autre risque est la perte d'une clé USB contenant de précieuses données d'entreprise. |
| **Copie conforme** | Les données confidentielles doivent être déchiquetées lorsqu'elles ne sont plus nécessaires. |
| **Contrôle d'accès incorrect** | Les mots de passe ou les mots de passe faibles qui ont été compromis peuvent fournir à un acteur de la menace un accès facile aux données de l'entreprise. |

# Le pirate

Pirate est un terme commun utilisé pour décrire un acteur de menace

| Type de pirate | Description |
|---|---|
| **Pirates au chapeau blanc** | Il s'agit de pirates éthiques qui utilisent leurs compétences en matière de programmation à des fins bénéfiques, éthiques et légales. Les vulnérabilités de sécurité sont signalées aux développeurs afin qu'ils les corrigent avant qu'elles ne puissent être exploitées. |
| **Pirates au chapeau gris** | Il s'agit de personnes qui commettent des délits et dont l'éthique est discutable, mais qui ne le font pas pour leur gain personnel ou pour causer des dommages. Les hackers au chapeau gris peuvent dévoiler une vulnérabilité à l'entreprise affectée après avoir compromis son réseau. |
| **Pirates au chapeau noir** | Ce sont des criminels contraires à l'éthique qui compromettent la sécurité des ordinateurs et des réseaux à des fins personnelles ou pour des raisons malveillantes, telles que des attaques de réseaux. |

# L'évolution des pirates

Le tableau affiche les termes de piratage modernes et une brève description de chacun.

| Terme de piratage | Description |
|---|---|
| **Les script kiddies (hackers néophytes)** | Ce sont des adolescents ou des pirates informatiques inexpérimentés qui exécutent des scripts, des outils et des exploits existants, pour causer du tort, mais généralement sans but lucratif. |
| **Courtier de vulnérabilité** | Ce sont généralement des pirates du chapeau gris qui tentent de découvrir des exploits et de les signaler aux fournisseurs, parfois pour des prix ou des récompenses. |
| **Les hacktivistes** | Ce sont des pirates du chapeau gris qui protestent publiquement contre des organisations ou des gouvernements en publiant des articles, des vidéos, des fuites d'informations sensibles et des attaques de réseau. |
| **Cybercriminels** | Il s'agit de hackers au chapeau noir qui travaillent à leur compte ou pour de grandes organisations de piratage informatique. |
| **Sponsorisé par l'État** | Ils peuvent être vus comme des hackers en chapeau blanc ou en chapeau noir qui volent des secrets du gouvernement, collectent des renseignements et sabotent les réseaux. Ils ciblent généralement les gouvernements étrangers, les groupes terroristes et les grandes entreprises. La plupart des pays du monde participent dans une certaine mesure au piratage parrainé par l'État |

## Acteurs de menace

On estime que les cybercriminels volent des milliards de dollars aux consommateurs et aux entreprises. Les cybercriminels opèrent dans une économie souterraine où ils achètent, vendent et échangent des kits d'outils d'attaque, du code d'exploitation zero day, des services de botnet, des chevaux de Troie bancaires, des enregistreurs de frappe et bien plus encore. Ils achètent et vendent également les informations privées et la propriété intellectuelle qu'ils volent. Les cybercriminels ciblent les petites entreprises et les consommateurs, ainsi que les grandes entreprises et des industries entières.

Anonymous et l'armée syrienne électronique sont deux exemples de groupes hacktivistes. Bien que la plupart des groupes hacktivistes ne soient pas bien organisés, ils peuvent causer des problèmes importants aux gouvernements aux entreprises. Les hacktivistes ont tendance à s'appuyer sur des outils assez simples et disponibles gratuitement.

Les pirates informatiques sponsorisés par l'État créent un code d'attaque avancé et personnalisé, utilisant souvent des vulnérabilités logicielles non découvertes appelées vulnérabilités zero-day. Un exemple d'attaque parrainée par l'État concerne le malware Stuxnet qui a été créé pour endommager les capacités d'enrichissement nucléaire de l'Iran.

# Évolution des outils de sécurité

Le tableau présente les catégories d'outils de test de pénétration courants. Remarquez comment certains outils sont utilisés par les chapeaux blancs et les chapeaux noirs. Gardez à l'esprit que la liste n'est pas exhaustive car de nouveaux outils sont toujours en développement.

| Outil de test de pénétration | Description |
|---|---|
| Craqueurs de mots de passe | Les outils de piratage de mot de passe sont souvent appelés outils de récupération de mot de passe et peuvent être utilisés pour casser ou récupérer un mot de passe. Les craqueurs de mot de passe font des suppositions à plusieurs reprises afin de casser le mot de passe. Des exemples d'outils de craquage de mot de passe incluent John the Ripper, Ophcrack, L0phtCrack, THC Hydra, Rainbow Crack et Medusa. |
| Outils de piratage sans fil | Les outils de piratage sans fil sont utilisés pour pirater intentionnellement un réseau sans fil afin de détecter les vulnérabilités de sécurité. Des exemples d'outils de piratage sans fil incluent Aircrack-ng, Kismet, InSSIDer, KisMAC, Firesheep et ViStumbler. |
| Analyse du réseau et outils de piratage | Les outils d'analyse réseau sont utilisés pour sonder les périphériques réseau, les serveurs et les hôtes pour les ports TCP ou UDP ouverts. Des exemples d'outils d'analyse incluent Nmap, SuperScan, Angry IP Scanner et NetScanTools. |
| Outils de fabrication de paquets | Ces outils sont utilisés pour sonder et tester la robustesse d'un pare-feu à l'aide de paquets forgés spécialement conçus. Les exemples incluent Hping, Scapy, Socat, Yersinia, Netcat, Nping et Nemesis. |
| Renifleurs de paquets | Ces outils sont utilisés pour capturer et analyser les paquets au sein des réseaux locaux ou WLAN Ethernet traditionnels. Les outils incluent Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy et SSLstrip. |

# Évolution des outils de sécurité (suite)

| Outil de test de pénétration | Description |
|---|---|
| Détecteurs de rootkit | Il s'agit d'un vérificateur d'intégrité des répertoires et des fichiers utilisé par les chapeaux blancs pour détecter les root kits installés. Exemples d'outils: AIDE, Netfilter et PF: OpenBSD Packet Filter. |
| Fuzzers pour rechercher des vulnérabilités | Les fuzzers sont des outils utilisés par les acteurs de menace pour découvrir les vulnérabilités de sécurité d'un ordinateur. Les exemples de fuzzers incluent Skipfish, Wapiti et W3af. |
| Outils d'investigation | Ces outils sont utilisés par les pirates du chapeau blanc pour flairer toute trace de preuves existant dans un ordinateur. Des exemples d'outils incluent Sleuth Kit, Helix, Maltego et Encase. |
| Débogueurs | Ces outils sont utilisés par les hackers au chapeau noir pour faire du reverse engineering sur des fichiers binaires lors de l'écriture d'exploits. Ils sont également utilisés par les chapeaux blancs lors de l'analyse des logiciels malveillants. Les outils de débogage incluent GDB, WinDbg, IDA Pro et Immunity Debugger. |
| Piratage de systèmes d'exploitation | Ce sont des systèmes d'exploitation spécialement conçus préchargés avec des outils optimisés pour le piratage. Des exemples de systèmes d'exploitation de piratage spécialement conçus incluent Kali Linux, BlackBox Linux. |
| Outils de chiffrement | Les outils de chiffrement utilisent des schémas d'algorithmes pour coder les données afin d'empêcher tout accès non autorisé aux données chiffrées. Des exemples de ces outils incluent VeraCrypt, CipherShed, OpenSSH, OpenSSL, Tor, OpenVPN et Stunnel. |
| Outils d'exploitation des vulnérabilités | Ces outils identifient si un hôte distant est vulnérable à une attaque de sécurité. Des exemples d'outils d'exploitation de vulnérabilité comprennent Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit et Netsparker. |
| Analyseurs de vulnérabilité | Ces outils analysent un réseau ou un système pour identifier les ports ouverts. Ils peuvent également être utilisés pour rechercher des vulnérabilités connues et analyser les VM, les dispositifs BYOD et les bases de données des clients. Des exemples d'outils incluent Nipper, Core Impact, Nessus, SAINT et OpenVAS |

# Types d'attaque

| Type d'attaque | Description |
|---|---|
| Attaque d'écoute | C'est à ce moment qu'un acteur de menace capture et «écoute» le trafic réseau. Cette attaque est également appelée reniflement ou surveillance. |
| Attaque par modification de données | Si les acteurs de menace ont capturé le trafic d'entreprise, ils peuvent modifier les données du paquet à l'insu de l'expéditeur ou du destinataire. |
| Attaque par usurpation d'adresse IP | Un acteur de menace construit un paquet IP qui semble provenir d'une adresse valide à l'intérieur de l'intranet de l'entreprise. |
| Attaques basées sur un mot de passe | Si les acteurs de menace découvrent un compte d'utilisateur valide, les acteurs de menace ont les mêmes droits que l'utilisateur réel. Les acteurs de menace peuvent utiliser ce compte valide pour obtenir des listes d'autres utilisateurs, des informations sur le réseau, changer les configurations de serveur et de réseau et modifier, réacheminer ou supprimer des données. |
| Attaque par déni de service | Une attaque DoS empêche l'utilisation normale d'un ordinateur ou d'un réseau par des utilisateurs valides. Une attaque DoS peut inonder un ordinateur ou l'ensemble du réseau de trafic jusqu'à ce qu'un arrêt se produise en raison de la surcharge. Une attaque DoS peut également bloquer le trafic et donc empêcher les utilisateurs autorisés d'accéder aux ressources du réseau. |
| Attaque de l'homme-au-milieu (man in the middle) | Cette attaque se produit lorsque les acteurs de menace se sont positionnés entre une source et une destination. Ils peuvent désormais surveiller, capturer et contrôler activement la communication de manière transparente. |
| Attaque à clé compromise | Si un acteur de menace obtient une clé secrète, cette clé est appelée clé compromise. Une clé compromise peut être utilisée pour accéder à une communication sécurisée sans que l'expéditeur ou le destinataire ne soit au courant de l'attaque. |
| Attaque de renifleur | Un renifleur est une application ou un appareil qui peut lire, surveiller et capturer des échanges de données réseau et lire des paquets réseau. Si les paquets ne sont pas chiffrés, un renifleur fournit une vue complète des données à l'intérieur du paquet |

# Virus et chevaux de Troie (Trojan Horses)

- Le premier type de programme malveillant, et le plus répandu, est le virus. Les virus nécessitent une action humaine pour se propager et infecter d'autres ordinateurs.
- Le virus se cache en s'attachant au code informatique, aux logiciels ou aux documents sur l'ordinateur. Une fois ouvert, le virus s'exécute et infecte l'ordinateur.
- Les virus peuvent:
  - Modifier, corrompre, supprimer des fichiers ou effacer des disques entiers.
  - Cause des problèmes de démarrage de l'ordinateur et des applications corrompues.
  - Capturer et envoyer des informations sensibles aux acteurs de menace.
  - Accéder et utiliser des comptes de messagerie pour vous propager.
  - Rester en sommeil jusqu'à ce qu'il soit convoqué par l'acteur de menace.

# Virus et chevaux de Troie (Trojan Horses) (suite)

Les virus modernes sont développés pour des objectifs spécifiques tels que ceux répertoriés dans le tableau.

| Types de virus | Description |
|---|---|
| Virus du secteur de démarrage | Le virus attaque le secteur de démarrage, la table de partition de fichiers ou le système de fichiers. |
| Virus de micrologiciel | Le virus attaque le micrologiciel du périphérique. |
| Virus macro | Le virus utilise la fonctionnalité macro de MS Office de façon malveillante. |
| Virus de programme | Le virus s'insère dans un autre programme exécutable. |
| Virus de script | Le virus attaque l'interpréteur du système d'exploitation utilisé pour exécuter des scripts. |

# Virus et chevaux de Troie (Trojan Horses) (suite)

Les acteurs de menace utilisent des chevaux de Troie pour compromettre les hôtes. Un cheval de Troie est un programme qui semble utile mais qui contient également du code malveillant. Les chevaux de Troie sont souvent fournis avec des programmes en ligne gratuits, tels que des jeux informatiques. Il existe plusieurs types de chevaux de Troie, comme décrit dans le tableau.

| Type de cheval de Troie | Description |
|---|---|
| Accès distant | Le cheval de Troie permet un accès à distance non autorisé. |
| Envoi de données | Le cheval de Troie fournit à l'acteur de menace des données sensibles, telles que des mots de passe. |
| Destructeur | Le cheval de Troie corrompt ou supprime des fichiers. |
| Proxy | Le cheval de Troie utilisera l'ordinateur de la victime comme périphérique source pour lancer des attaques et effectuer d'autres activités illégales. |
| FTP | Le cheval de Troie permet des services de transfert de fichiers non autorisés sur des dispositifs terminaux. |
| Désactivation des logiciels de sécurité | Le cheval de Troie empêche les programmes antivirus ou les pare-feu de fonctionner. |
| Déni de service (DoS) | Le cheval de Troie ralentit ou arrête l'activité du réseau. |
| Enregistreur de frappe | Le cheval de Troie tente activement de voler des informations confidentielles, telles que les numéros de carte de crédit, en enregistrant les frappes de touches saisies dans un formulaire Web. |

Logiciels malveillants

# Types de Logiciels malveillants

| Logiciel malveillant | Description |
|---|---|
| Logiciel publicitaire (Adware) | •Le logiciel publicitaire est généralement distribué lors du téléchargement de logiciels en ligne.<br>•Les logiciels publicitaires peuvent afficher des publicités non sollicitées à l'aide de fenêtres de navigateur Web contextuelles, de nouvelles barres d'outils ou rediriger de manière inattendue une page Web vers un autre site Web.<br>•Les fenêtres contextuelles sont souvent difficiles à contrôler, car de nouvelles fenêtres contextuelles s'ouvrent plus rapidement que l'utilisateur ne peut les fermer. |
| Ransomware | •Un ransomware empêche généralement un utilisateur d'accéder à ses fichiers en chiffrant les fichiers, puis en affichant un message demandant une rançon pour la clé de décodage.<br>•Les utilisateurs qui ne disposent pas de sauvegardes à jour doivent payer la rançon pour déchiffrer leurs fichiers.<br>•Le paiement est généralement effectué par virement bancaire ou par des crypto-monnaies telles que Bitcoin. |
| Rootkit | •Les rootkits sont utilisés par les acteurs de menace pour obtenir un accès administrateur à un ordinateur au niveau du compte.<br>•Ils sont très difficiles à détecter, car ils peuvent modifier le pare-feu, la protection antivirus, les fichiers système et même les commandes du système d'exploitation pour dissimuler leur présence.<br>•Ils peuvent fournir une porte dérobée aux acteurs de menace en leur donnant accès au PC, en leur permettant de télécharger des fichiers et d'installer de nouveaux logiciels à utiliser dans une attaque DDoS.<br>•Des outils spéciaux de suppression de rootkit doivent être utilisés pour les supprimer, ou une réinstallation complète du système d'exploitation peut être nécessaire. |
| Logiciel espion (Spyware) | •Comme un logiciel de publicité, mais utilisé pour collecter des informations sur l'utilisateur et envoyer aux acteurs de menace sans le consentement de l'utilisateur.<br>•Les logiciels espions peuvent être une menace faible, collectant des données de navigation, ou une menace élevée capturant des informations personnelles et financières. |
| Ver (Worm) | •Un ver est un programme de réplication automatique qui se propage automatiquement sans intervention de l'utilisateur en exploitant les vulnérabilités des logiciels légitimes.<br>•Il utilise le réseau pour rechercher d'autres victimes ayant la même vulnérabilité.<br>•L'intention d'un ver est généralement de ralentir ou de perturber les opérations réseau. |

# Présentation des attaques réseau courantes

- Lorsque des logiciels malveillants sont livrés et installés, la charge utile peut être utilisée pour provoquer diverses attaques liées au réseau.
- Pour atténuer les attaques, il est utile de comprendre les types d'attaques. En catégorisant les attaques de réseau, il est possible de traiter des types d'attaques plutôt que des attaques individuelles.
- Les réseaux sont sensibles aux types d'attaques suivants:
  - Attaques de reconnaissance
  - Attaques par accès
  - Attaques DoS

# Attaques de reconnaissance

- La reconnaissance est la collecte d'informations.
- Les acteurs de menace utilisent des attaques de reconnaissance (ou recon) pour effectuer la découverte et la cartographie non autorisées de systèmes, de services ou de vulnérabilités. Les attaques Recon précèdent les attaques d'accès ou les attaques DoS.

# Attaques de reconnaissance (suite)

Certaines des techniques utilisées par les acteurs de menace malveillants pour mener des attaques de reconnaissance sont décrites dans le tableau.

| Technique | Description |
|---|---|
| **Exécuter une requête d'information sur une cible** | L'acteur de menace recherche les premières informations sur une cible. Divers outils peuvent être utilisés, notamment la recherche Google, le site Web des organisations, le whois, etc. |
| **Lancer un balayage ping du réseau cible** | La requête d'informations révèle généralement l'adresse réseau de la cible. L'acteur de menace peut désormais lancer un balayage ping pour déterminer quelles adresses IP sont actives. |
| **Lancer l'analyse des ports des adresses IP actives** | Ceci est utilisé pour déterminer quels ports ou services sont disponibles. Exemples d'analyseurs de ports: Nmap, SuperScan, Angry IP Scanner et NetScanTools. |
| **Exécuter des scanners de vulnérabilité** | Il s'agit d'interroger les ports identifiés pour déterminer le type et la version de l'application et du système d'exploitation qui s'exécutent sur l'hôte. Des exemples d'outils incluent Nipper, Core Impact, Nessus, SAINT et Open VAS. |
| **Exécuter des outils d'exploitation** | L'acteur de menace tente maintenant de découvrir des services vulnérables qui peuvent être exploités. Des exemples d'outils d'exploitation de vulnérabilité comprennent Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit et Netsparker. |

# Attaques d'accès

- Les attaques par accès exploitent les vulnérabilités connues des services d'authentifications, services FTP et services web pour accéder à des comptes web, des bases de données confidentielles ou accéder à d'autres ressources. Le but de ces types d'attaques est d'accéder à des comptes Web, à des bases de données confidentielles et à d'autres informations sensibles.
- Les acteurs de menace utilisent des attaques d'accès sur les périphériques réseau et les ordinateurs pour récupérer des données, y accéder ou pour augmenter les privilèges d'accès au statut d'administrateur.
- **Attaques par mot de passe:** lors d'une attaque par mot de passe, l'acteur de la menace tente de découvrir des mots de passe système critiques en utilisant diverses méthodes. Les attaques par mot de passe sont très courantes et peuvent être lancées à l'aide d'une variété d'outils de craquage de mot de passe.
- **Attaques d'usurpation d'identité:** lors d'attaques d'usurpation d'identité, le dispositif d'acteur de menace tente de se faire passer pour un autre appareil en falsifiant des données. Les attaques d'usurpation d'identité courantes incluent l'usurpation d'adresse IP, l'usurpation d'adresse MAC et l'usurpation d'identité DHCP. Ces attaques d'usurpation seront discutées plus en détail plus loin dans ce module
- Les autres attaques d'accès incluent:
  - Exploiter la confiance
  - Redirection de port
  - Attaques de l'homme-au-milieu
  - Attaques par débordement de la mémoire tampon

# Attaques d'ingénierie sociale

- L'ingénierie sociale est une attaque d'accès qui tente de manipuler des individus pour effectuer des actions ou divulguer des informations confidentielles. Certaines techniques d'ingénierie sociale sont réalisées en personne tandis que d'autres peuvent utiliser le téléphone ou Internet.
- Les ingénieurs sociaux comptent souvent sur la volonté des gens d’être utiles. Ils exploitent également les faiblesses des gens.

# Attaques d'ingénierie sociale (suite)

| Attaque d'ingénierie sociale | Description |
|---|---|
| Prétexte | Un acteur de menace prétend avoir besoin de données personnelles ou financières pour confirmer l'identité du destinataire. |
| Hameçonnage (Phishing) | Un acteur de menace envoie un e-mail frauduleux déguisé en une source légitime et fiable pour inciter le destinataire à installer un logiciel malveillant sur son appareil ou pour partager des informations personnelles ou financières. |
| Hameçonnage ciblé | Un acteur de menace crée une attaque de phishing ciblée adaptée à un individu ou une organisation spécifique. |
| Courrier indésirable (spam) | Également connu sous le nom de courrier indésirable, il s'agit d'un courrier électronique non sollicité qui contient souvent des liens nuisibles, des logiciels malveillants ou du contenu trompeur. |
| Contrepartie (Something for Something) | Parfois appelé «Quid pro quo», c'est lorsqu'un acteur de menace demande des informations personnelles à une partie en échange de quelque chose comme un cadeau. |
| Appâtage | Un acteur de menace laisse un lecteur flash infecté par un logiciel malveillant dans un lieu public. Une victime trouve le lecteur et l'insère sans méfiance dans son ordinateur portable, installant involontairement des logiciels malveillants. |
| Usurpation d'identité | Ce type d'attaque est l'endroit où un acteur de menace prétend être quelqu'un qu'il ne doit pas gagner la confiance d'une victime. |
| Accès non autorisé (Tailgating) | Un acteur de menace suit rapidement une personne autorisée dans un endroit sécurisé pour accéder à une zone sécurisée. |
| Espionnage par-dessus l'épaule (Shoulder Surfing) | Un acteur de menace regarde discrètement par-dessus l'épaule de quelqu'un pour voler ses mots de passe ou d'autres informations. |
| Fouille de poubelles (Dumpster Diving) | Un acteur de menace fouille dans des poubelles pour découvrir des documents confidentiels |

# Attaques d'ingénierie sociale (suite)

- Le Social Engineering Toolkit (SET) a été conçu pour aider les pirates informatiques et autres professionnels de la sécurité des réseaux à créer des attaques d'ingénierie sociale pour tester leurs propres réseaux.
- Les entreprises doivent éduquer leurs utilisateurs sur les risques de l'ingénierie sociale et développer des stratégies pour valider les identités par téléphone, par e-mail ou en personne.
- La figure montre les pratiques recommandées qui devraient être suivies par tous les utilisateurs.

# Attaques DoS et DDoS

- Une attaque par déni de service (DoS) crée une sorte d'interruption des services réseau pour les utilisateurs, les appareils ou les applications. Il existe deux principaux types d'attaques DoS:
  - **Quantité écrasante de trafic** - L'acteur de menace envoie une énorme quantité de données à un débit que le réseau, l'hôte ou l'application ne peut pas gérer. Cela ralentit la transmission et le temps de réponse. Il peut également planter un appareil ou un service.
  - **Paquets formatés de manière malveillante** -L'acteur de menace envoie un paquet formaté de manière malveillante à un hôte ou une application et le récepteur n'est pas en mesure de le gérer. Cela provoque un ralentissement de l'appareil récepteur ou une panne.
- Les attaques DoS sont un risque majeur car elles interrompent la communication et provoquent une perte de temps et d'argent importante. Ces attaques sont relativement simples à mener, même par un acteur de menace non qualifié.
- Une attaque DoS distribuée (DDoS) est similaire à une attaque DoS, mais elle provient de plusieurs sources coordonnées.

# IPv4 et IPv6

- l'IP ne valide pas si l'adresse IP source contenue dans un paquet provient réellement de cette source. Pour cette raison, les acteurs de menace peuvent envoyer des paquets à l'aide d'une adresse IP source usurpée. Les analystes de sécurité doivent comprendre les différents champs des en-têtes IPv4 et IPv6.
- Certaines des attaques liées à l'IP les plus courantes sont présentées dans le tableau

| Techniques d'attaque IP | Description |
|---|---|
| **Attaques ICMP** | Les acteurs de menace utilisent des paquets d'écho (ping) ICMP (Internet Control Message Protocol) pour découvrir les sous-réseaux et les hôtes sur un réseau protégé, pour générer des attaques par inondation DoS et pour modifier les tables de routage des hôtes. |
| **Amplification et attaques par réflexion** | Les acteurs de menace tentent d'empêcher les utilisateurs légitimes d'accéder aux informations ou aux services à l'aide d'attaques DoS et DDoS. |
| **Attaques par usurpation d'adresse** | Les acteurs de menace usurpent l'adresse IP source dans un paquet IP pour effectuer une usurpation aveugle ou une usurpation non aveugle. |
| **Attaques de l'homme-au-milieu (MITM)** | Les acteurs de menace se positionnent entre une source et une destination pour surveiller, capturer et contrôler de manière transparente la communication. Ils pourraient espionner en inspectant les paquets capturés, ou modifier les paquets et les transmettre à leur destination d'origine. |
| **Détournement de session** | Les acteurs de menace accèdent au réseau physique, puis utilisent une attaque MITM pour détourner une session |

# Attaques ICMP

- Les acteurs de menace utilisent ICMP pour les attaques de reconnaissance et de scan. Ils peuvent lancer des attaques de collecte d'informations pour cartographier une topologie de réseau, découvrir quels hôtes sont actifs (accessibles), identifier le système d'exploitation hôte (empreinte du système d'exploitation) et déterminer l'état d'un pare-feu. Les acteurs de menace utilisent également ICMP pour les attaques DoS.
- **Remarque**: ICMP pour IPv4 (ICMPv4) et ICMP pour IPv6 (ICMPv6) sont sensibles à des types d'attaques similaires.
- Les réseaux doivent avoir un filtrage strict de la liste de contrôle d'accès (ACL) ICMP sur la périphérie du réseau pour éviter les sondages ICMP à partir d'Internet. Dans le cas de grands réseaux, les dispositifs de sécurité tels que les pare-feu et les systèmes de détection d'intrusion (IDS) détectent de telles attaques et génèrent des alertes aux analystes de sécurité.

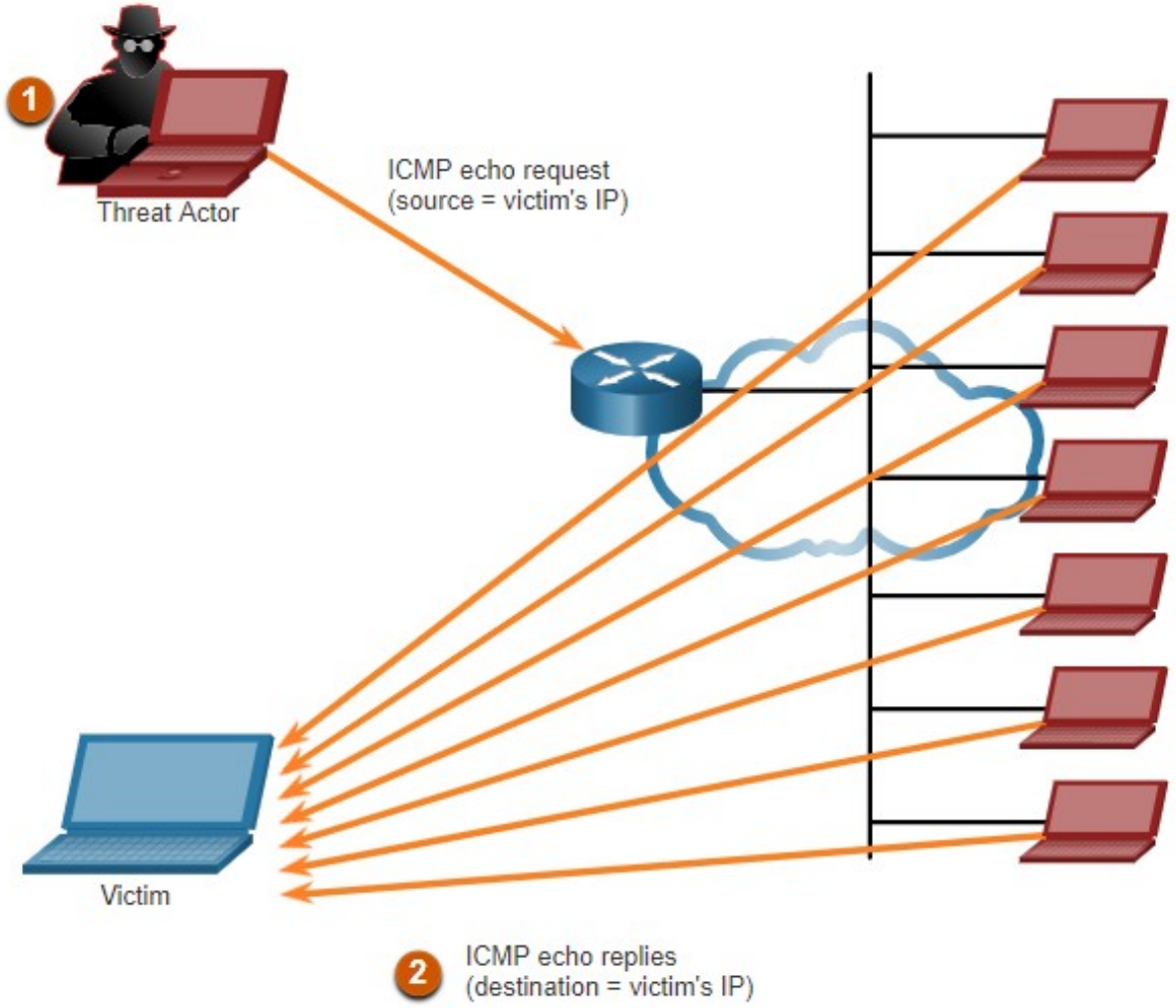
# Attaques ICMP (suite)

Les messages communs d'ICMP qui intéressent les acteurs de menace sont énumérés dans le tableau.

| Messages ICMP utilisés par les pirates | Description |
|---|---|
| **Demande d'écho ICMP et réponse d'écho** | Ceci est utilisé pour effectuer une vérification de l'hôte et des attaques DoS. |
| **ICMP inaccessible** | Il est utilisé pour effectuer des attaques de reconnaissance et de balayage de réseau. |
| **Réponse de masque ICMP** | Ceci est utilisé pour mapper un réseau IP interne. |
| **Redirection ICMP** | Ceci est utilisé pour attirer un hôte cible dans l'envoi de tout le trafic via un appareil compromis et créer une attaque MITM. |
| **Découverte du routeur ICMP** | Ceci est utilisé pour injecter des entrées de route fausses dans la table de routage d'un hôte cible. |

# Attaques par amplification et réflexion

- Les acteurs de menace utilisent souvent des techniques d'amplification et de réflexion pour créer des attaques DoS. L'exemple de la figure illustre une attaque Smurf utilisée pour submerger un hôte cible.
  - **Remarque**: De nouvelles formes d'attaques d'amplification et de réflexion telles que les attaques de réflexion et d'amplification basées sur DNS et les attaques d'amplification NTP (Network Time Protocol) sont désormais utilisées.
- Les acteurs de menace utilisent également des attaques d'épuisement des ressources pour planter un hôte cible ou pour consommer les ressources d'un réseau.

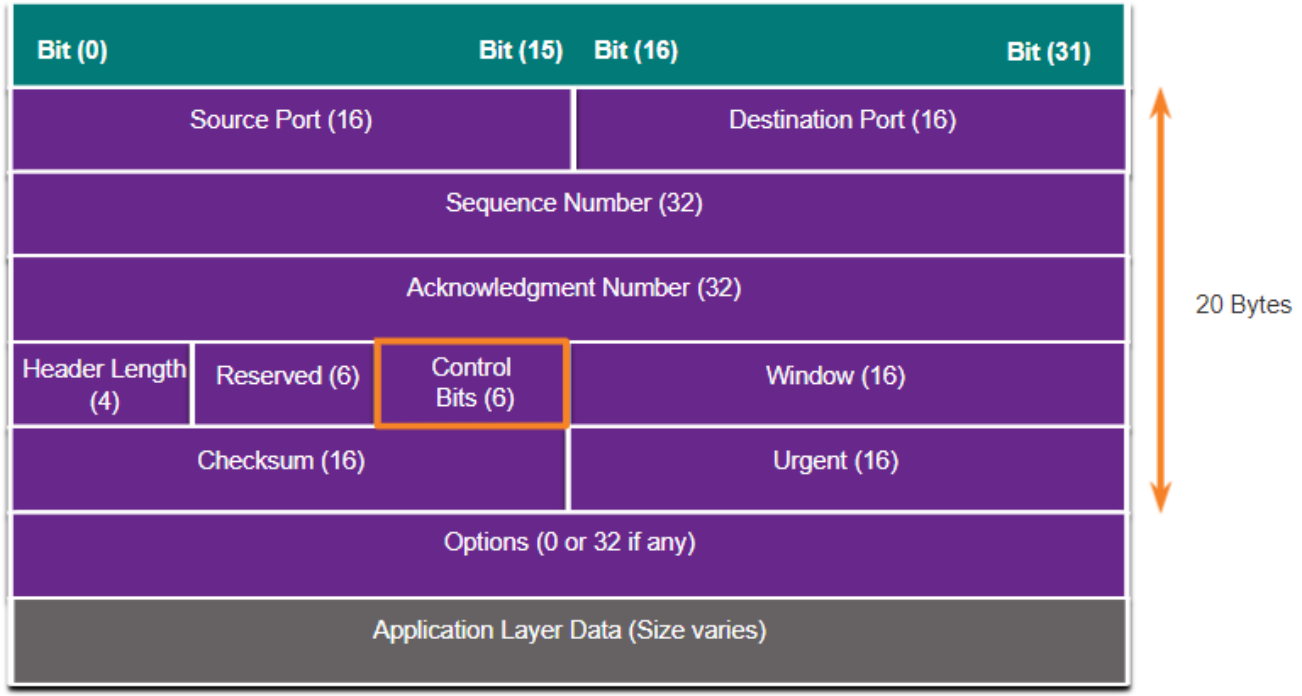


# Attaques par usurpation d'adresse

- Les attaques d'usurpation d'adresse IP se produisent lorsqu'un acteur de menace crée des paquets contenant de fausses informations d'adresse IP source pour masquer l'identité de l'expéditeur ou pour se faire passer pour un autre utilisateur légitime. L'usurpation d'identité est généralement intégrée à une autre attaque telle qu'une attaque de Smurf.
- Les attaques d'usurpation d'identité peuvent être non aveugles ou aveugles:
  - **Usurpation d'identité non aveugle** - L'acteur de menace peut voir le trafic qui est envoyé entre l'hôte et la cible. L'usurpation non aveugle détermine l'état d'un pare-feu et la prédiction du numéro de séquence. Il peut également détourner une session autorisée.
  - **Usurpation aveugle** - L'acteur de menace ne peut pas voir le trafic envoyé entre l'hôte et la cible. L'usurpation aveugle est utilisée dans les attaques DoS.
- Les attaques d'usurpation d'adresse MAC sont utilisées lorsque les acteurs de menace ont accès au réseau interne. Les acteurs de menace modifient l'adresse MAC de leur hôte pour correspondre à une autre adresse MAC connue d'un hôte cible.

# En-tête de segment TCP

- Les informations de segment TCP apparaissent immédiatement après l'en-tête IP. Les champs du segment TCP et les drapeaux du champ Control Bits sont affichés sur la figure.
- Voici les six bits de contrôle du segment TCP:
  - **URG** - Champ de pointeur urgent significatif (Urgent pointer field significant)
  - **ACK** - Champ d'acquittement significatif (Acknowledgment field significant)
  - **PSH** - Fonction push (Push function)
  - **RST**- -Réinitialiser la connexion
  - **SYN** -Synchroniser les numéros de séquence
  - **FIN** - Plus de données de l'expéditeur



# Services TCP

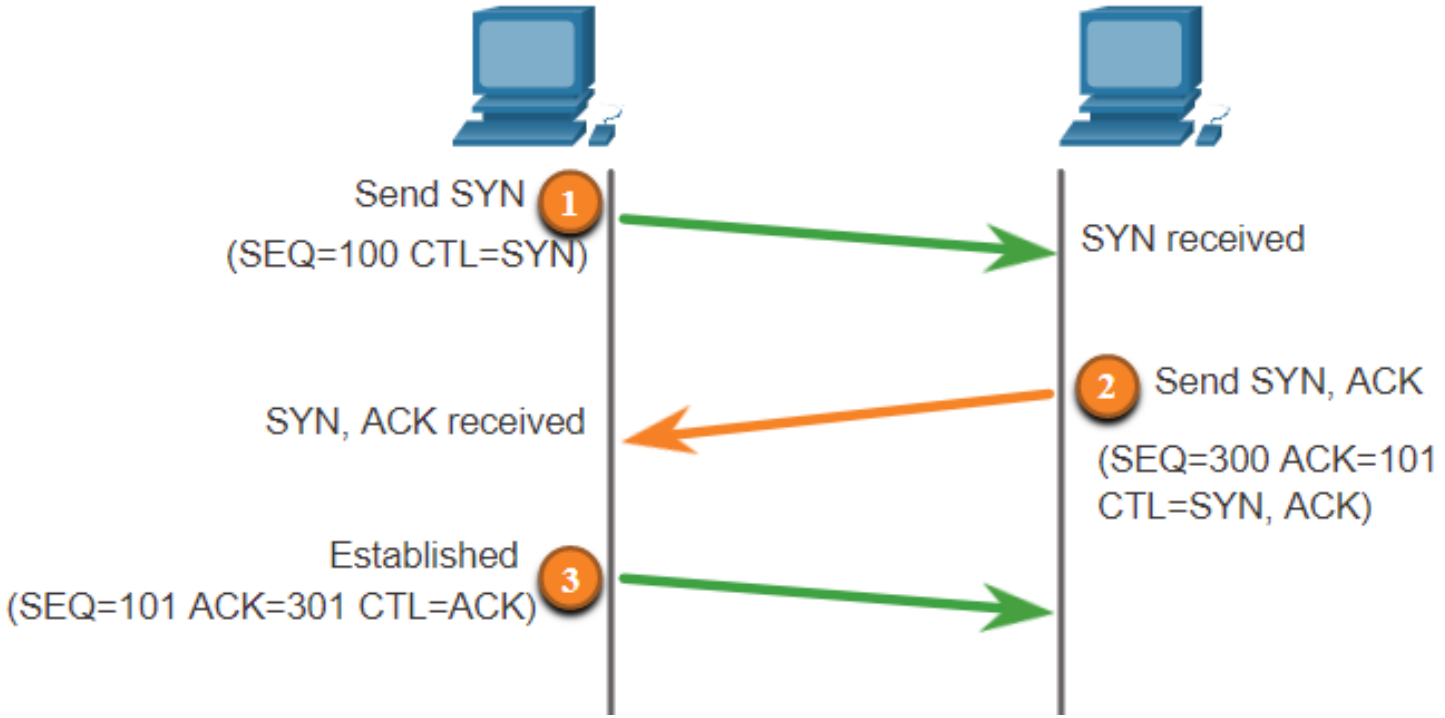
TCP fournit ces services:

- **Livraison fiable** - TCP intègre des accusés de réception (ACQ) pour garantir la livraison. Si un accusé de réception en temps opportun n'est pas reçu, l'expéditeur retransmet les données. La demande d'accusé de réception des données reçues peut entraîner des retards importants. Des exemples de protocoles de couche d'application qui utilisent la fiabilité TCP incluent HTTP, SSL / TLS, FTP, les transferts de zone DNS et autres.
- **Contrôle de flux** - TCP implémente un contrôle de flux pour résoudre ce problème. Plutôt que d'accuser la réception d'un segment à la fois, plusieurs segments peuvent être acquittés avec un seul segment d'accusé de réception.
- **Communication avec état** - La communication avec état TCP entre deux parties se produit pendant la prise de contact à trois étapes TCP.

# Services TCP (suite)

Une connexion TCP est établie en trois étapes :

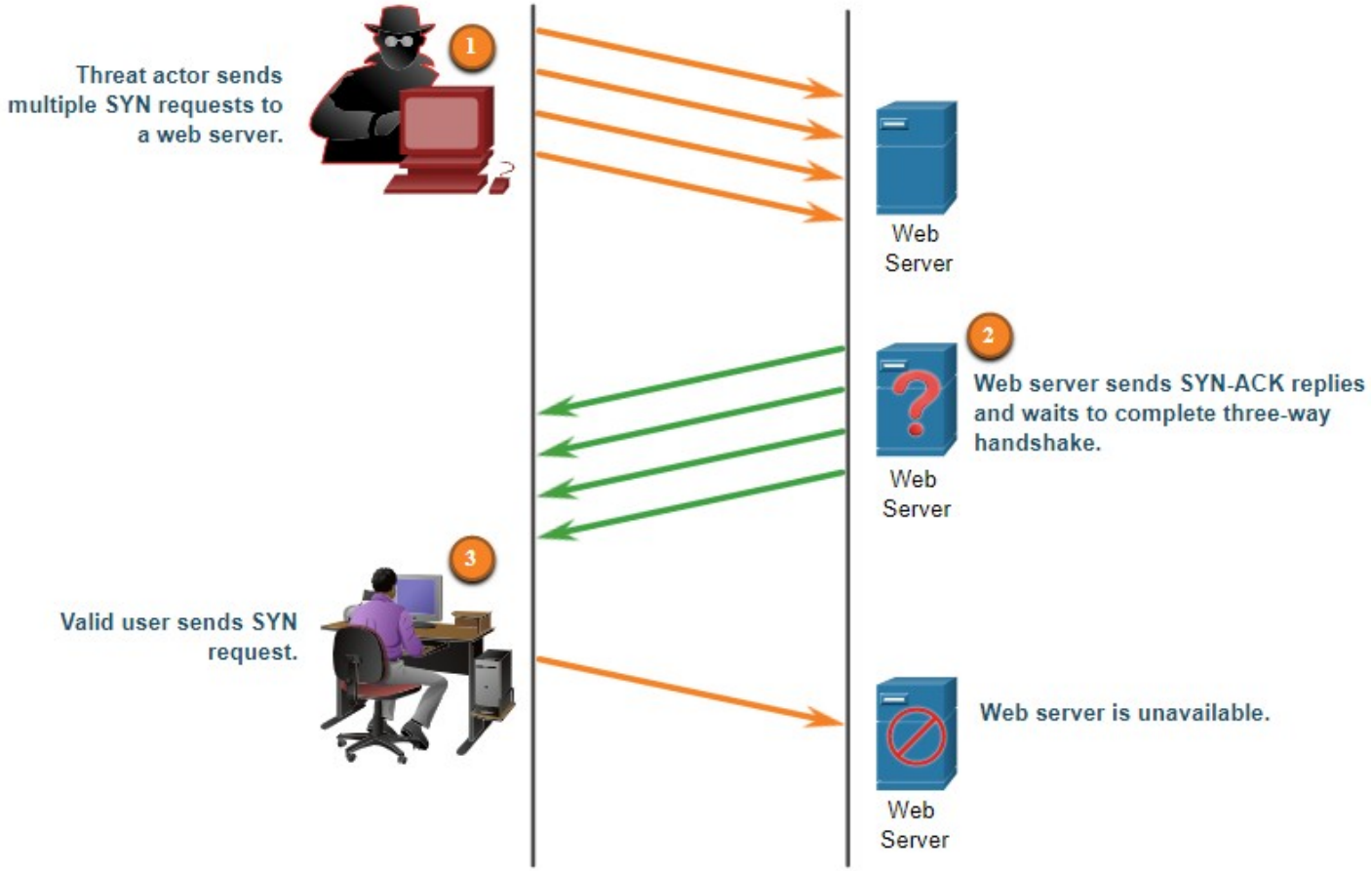
1. Le client demande l'établissement d'une session de communication client-serveur avec le serveur.
2. Le serveur accuse réception de la session de communication client-serveur et demande l'établissement d'une session de communication serveur-client.
3. Le client accuse réception de la session de communication serveur-client.



# Attaques TCP

## TCP SYN Attaque par inondation

1. L'acteur de menace envoie plusieurs demandes SYN à un serveur Web.
2. Le serveur Web répond avec des SYN-ACK pour chaque demande SYN et attend de terminer la négociation. L'acteur de menace ne répond pas aux SYN-ACK.
3. Un utilisateur valide ne peut pas accéder au serveur Web car le serveur Web possède trop de connexions TCP semi-ouvertes.

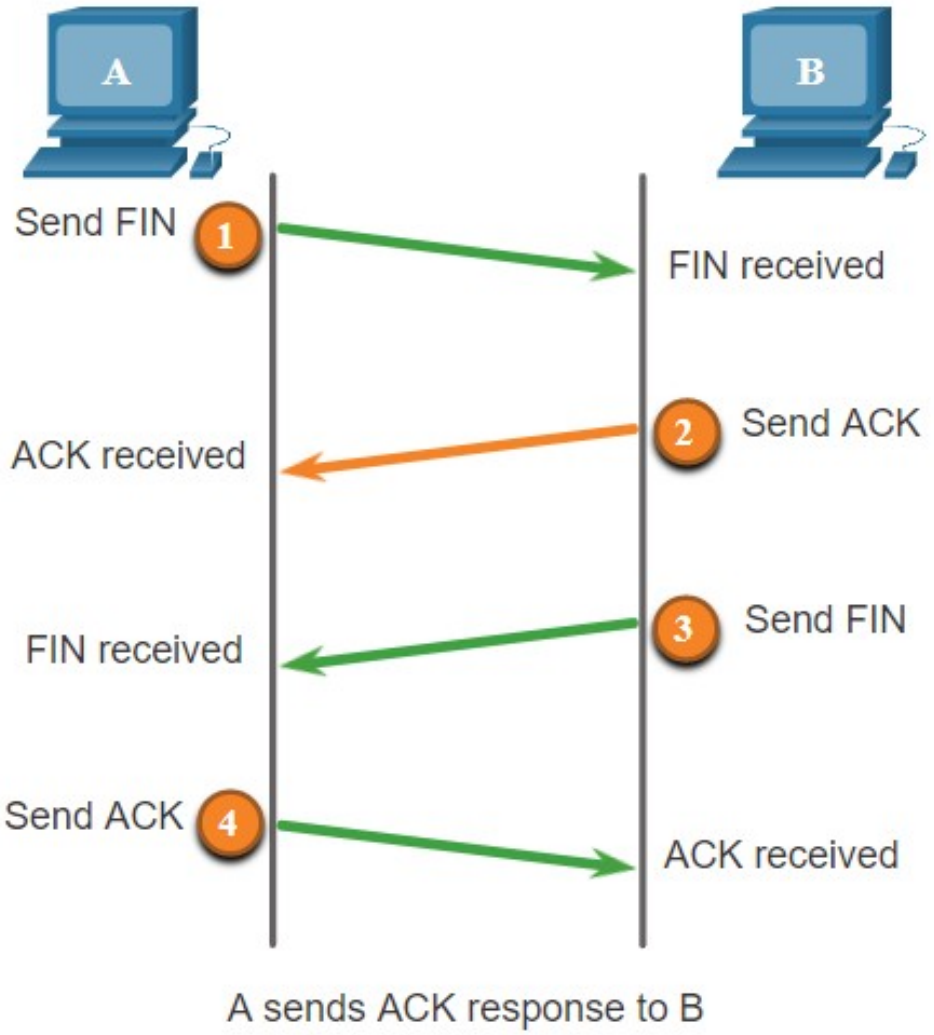


# Attaques TCP (suite)

La fin d'une session TCP utilise le processus d'échange à quatre voies suivant:

1. Quand le client n'a plus de données à envoyer dans le flux, il envoie un segment dont l'indicateur FIN est défini.
2. Le serveur envoie un segment ACK pour informer de la bonne réception du segment FIN afin de fermer la session du client au serveur.
3. Le serveur envoie un segment FIN au client pour mettre fin à la session du serveur au client.
4. Le client répond à l'aide d'un segment ACK pour accuser réception du segment FIN envoyé par le serveur.

Un acteur de menace pourrait effectuer une attaque de réinitialisation TCP et envoyer un paquet usurpé contenant un TCP RST à un ou aux deux points de terminaison.

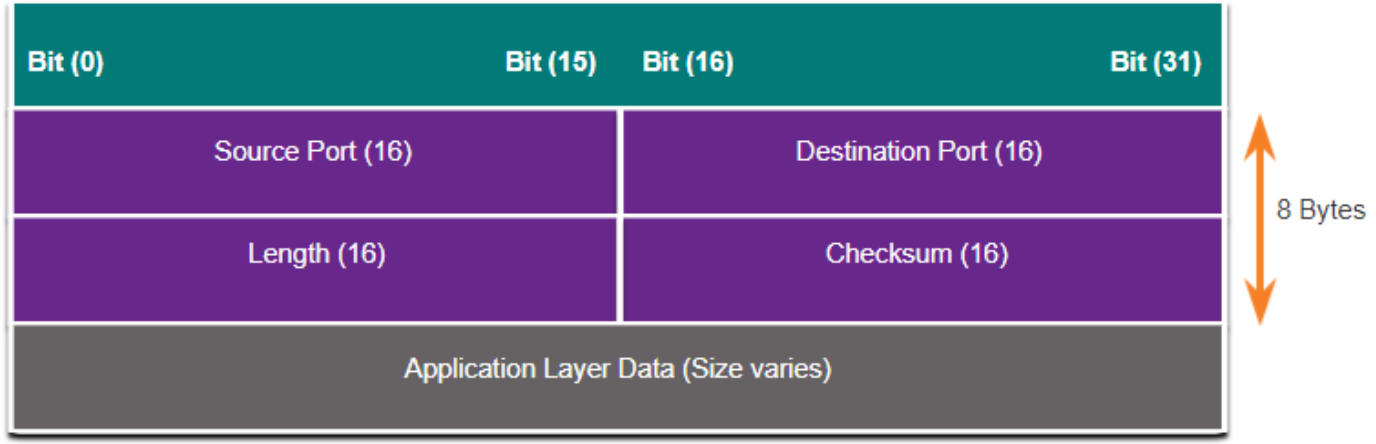


# Attaques TCP (suite)

Le détournement de session TCP apparaît comme une autre vulnérabilité TCP. Bien que difficile à mener, un acteur de menace prend le contrôle d'un hôte déjà authentifié lors de sa communication avec la cible. L'acteur de menace doit usurper l'adresse IP d'un hôte, prédire le numéro de séquence suivant et envoyer un ACK à l'autre hôte. En cas de succès, l'acteur de menace pourrait envoyer, mais pas recevoir, des données de l'appareil cible.

# En-tête et fonctionnement du segment UDP

- Le protocole UDP est généralement utilisé par les protocoles DNS, TFTP, NFS et SNMP. Il est aussi utilisé par les applications en temps réel comme la diffusion multimédia en flux continu ou les transmissions VoIP. Le protocole UDP s'inscrit comme un protocole de couche transport sans connexion. Il crée beaucoup moins de surcharge que le protocole TCP car il est sans connexion et n'offre pas de mécanismes sophistiqués de fiabilité (retransmission, séquençage et contrôle de flux).
- Ces fonctions de fiabilité ne sont pas fournies par le protocole de couche transport et doivent être implémentées ailleurs si nécessaire.
- La faible surcharge d'UDP le rend très souhaitable pour les protocoles qui effectuent des transactions de demande et de réponse simples.



# Attaques UDP

- Le protocole UDP n'est pas protégé par chiffrement. Vous pouvez ajouter un chiffrement à UDP, mais il n'est pas disponible par défaut. L'absence de cryptage signifie que n'importe qui peut voir le trafic, le modifier et l'envoyer à sa destination.
- **UDP Flood Attacks:** L'acteur de menace utilise un outil comme UDP Unicorn ou Low Orbit Ion Cannon. Ces outils envoient un flot de paquets UDP, souvent à partir d'un hôte usurpé, vers un serveur du sous-réseau. Le programme balaye tous les ports connus afin de trouver les ports fermés. Par conséquent, le serveur répond avec un message Port ICMP inaccessible. Étant donné qu'il existe de nombreux ports fermés sur le serveur, cela crée beaucoup de trafic sur le segment, qui utilise la majeure partie de la bande passante. Le résultat est très similaire à celui d'une attaque DoS.

# Vulnérabilités ARP

- Les hôtes diffusent une demande ARP à d'autres hôtes sur le segment pour déterminer l'adresse MAC d'un hôte avec une adresse IP particulière. L'hôte dont l'adresse IP correspond à la requête ARP envoie une réponse ARP.
- Tout client peut envoyer une réponse ARP non sollicitée appelée «ARP gratuit». Lorsqu'un hôte envoie un ARP gratuit, les autres hôtes du sous-réseau stockent l'adresse MAC et l'adresse IP contenues dans l'ARP gratuit dans leurs tables ARP.
- Cette fonctionnalité d'ARP signifie également que tout hôte peut prétendre être le propriétaire de n'importe quelle adresse IP ou MAC. Un acteur de menace peut empoisonner le cache ARP des appareils sur le réseau local, créant une attaque MITM pour rediriger le trafic.

# Empoisonnement du cache ARP

L'empoisonnement du cache ARP peut être utilisé pour lancer diverses attaques de l'homme-au-milieu.

1. PC-A requiert l'adresse MAC de sa passerelle par défaut (R1); par conséquent, il envoie une demande ARP pour l'adresse MAC de 192.168.10.1.
2. R1 met à jour son cache ARP avec les adresses IP et MAC de PC-A. R1 envoie une réponse ARP à PC-A, qui met ensuite à jour son cache ARP avec les adresses IP et MAC de R1.
3. L'acteur de menace envoie deux réponses ARP usurpées gratuitement en utilisant sa propre adresse MAC pour les adresses IP de destination indiquées. PC-A met à jour son cache ARP avec sa passerelle par défaut qui pointe maintenant vers l'adresse MAC hôte de l'acteur de la menace. R1 met également à jour son cache ARP avec l'adresse IP de PC-A pointant vers l'adresse MAC de l'acteur de menace.

L'attaque d'empoisonnement ARP peut être passive ou active. L'empoisonnement passif par ARP est l'endroit où les acteurs de la menace volent des informations confidentielles. L'empoisonnement ARP actif est l'endroit où les acteurs de menace modifient les données en transit ou injectent des données malveillantes.

# Attaques DNS

- Le protocole DNS (Domain Name Service) définit un service automatisé qui fait correspondre les noms de ressources, tels que www.unice.fr, avec l'adresse réseau numérique requise, telle que l'adresse IPv4 ou IPv6. Il inclut le format des requêtes, des réponses et des données, et utilise les enregistrements de ressource (RR) pour identifier le type de réponse DNS.
- La sécurisation du protocole DNS est souvent négligée. Toutefois, celui-ci est indispensable à l'exploitation d'un réseau et doit être sécurisé en conséquence.
- Les attaques DNS sont les suivantes:
  - Attaques DNS résolveur ouvert
  - Attaques furtives DNS
  - Les attaques de shadowing de domaine DNS
  - Attaques de Tunnellisation (tunneling) DNS

# Attaques DNS (suite)

Attaques du résolveur ouvert DNS: un résolveur ouvert DNS répond aux requêtes des clients en dehors de son domaine administratif. Les résolveurs ouverts DNS sont vulnérables à plusieurs activités malveillantes décrites dans le tableau.

| Vulnérabilités du résolveur DNS | Description |
|---|---|
| **Attaques d'empoisonnement du cache DNS** | Les acteurs de menace envoient des informations de ressource d'enregistrement (RR) falsifiées à un résolveur DNS pour rediriger les utilisateurs de sites légitimes vers des sites malveillants. Les attaques d'empoisonnement du cache DNS peuvent toutes être utilisées pour informer le résolveur DNS d'utiliser un serveur de noms malveillant qui fournit des informations RR pour les activités malveillantes. |
| **Attaques par amplification et réflexion du DNS** | Les acteurs de menace utilisent des attaques DoS ou DDoS sur les résolveurs ouverts DNS pour augmenter le volume des attaques et masquer la véritable source d'une attaque. Les acteurs de menace envoient des messages DNS aux résolveurs ouverts en utilisant l'adresse IP d'un hôte cible. Ces attaques sont possibles car le résolveur ouvert répondra aux requêtes de toute personne posant une question. |
| **Attaques d'utilisation des ressources DNS** | Une attaque DoS qui consomme les ressources des résolveurs ouverts DNS. Cette attaque DoS consomme toutes les ressources disponibles pour affecter négativement les opérations du résolveur ouvert DNS. L'impact de cette attaque DoS peut nécessiter le redémarrage du résolveur ouvert DNS ou l'arrêt et le redémarrage des services. |

# Attaques DNS (suite)

Attaques furtives DNS: pour masquer leur identité, les acteurs de menace utilisent également les techniques de furtivité DNS décrites dans le tableau pour mener leurs attaques.

| Techniques DNS furtives | Description |
|---|---|
| **Flux rapide** | Les auteurs de menace utilisent cette technique pour masquer leurs sites de phishing et de diffusion de logiciels malveillants derrière un réseau en évolution rapide d'hôtes DNS compromis. Les adresses IP du protocole DNS changent continuellement après quelques minutes. Les botnets utilisent souvent des techniques Flux rapide pour cacher efficacement la détection de serveurs malveillants. |
| **Double flux IP** | Les acteurs de menace utilisent cette technique pour changer rapidement le nom d'hôte en mappages d'adresses IP et également pour changer le serveur de noms faisant autorité. Cela augmente la difficulté d'identifier la source de l'attaque. |
| **Algorithmes de génération de domaine** | Les auteurs de menace utilisent cette technique dans les logiciels malveillants pour générer de manière aléatoire des noms de domaine qui peuvent ensuite être utilisés comme points de rendez-vous vers leurs serveurs de commande et de contrôle (C&C). |

# Attaques DNS (suite)

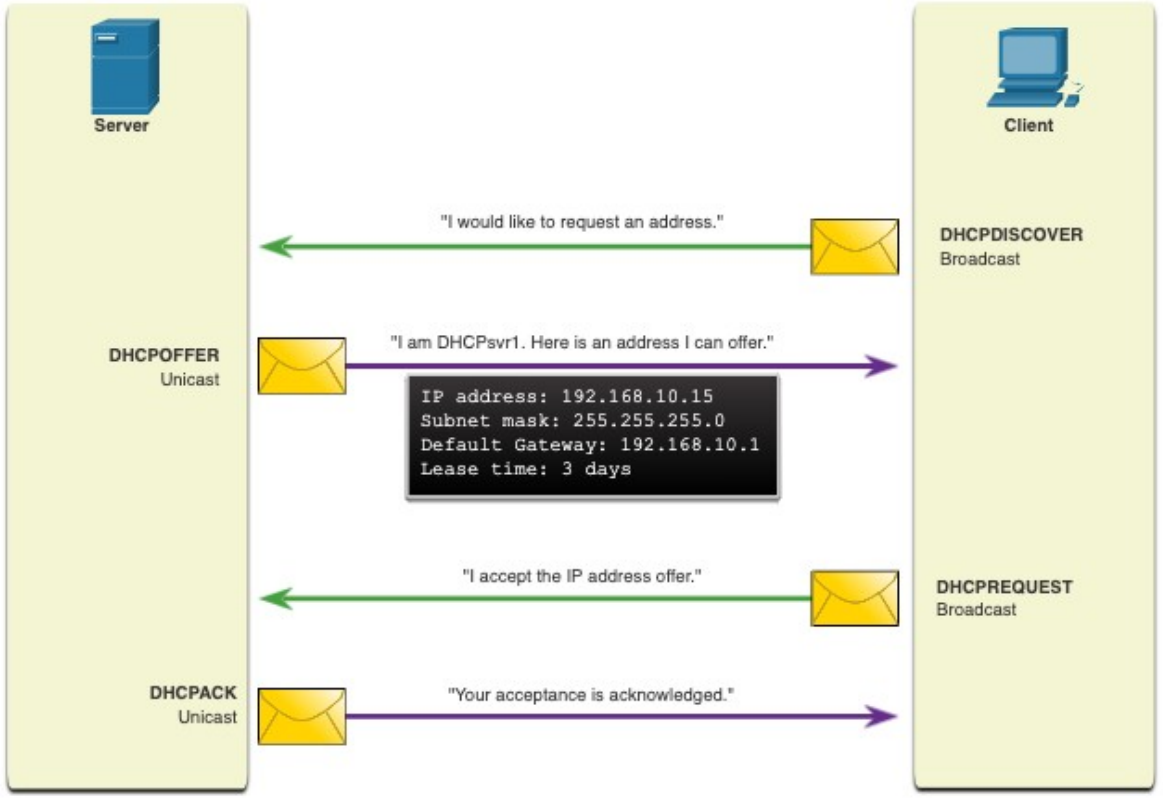
Attaques d'ombrage (shadowing) de domaine DNS : La surveillance de domaine implique que l'acteur de menace recueille des informations sur le compte du domaine afin de créer silencieusement plusieurs sous-domaines à utiliser lors des attaques. Ces sous-domaines pointent généralement vers des serveurs malveillants sans alerter le propriétaire réel du domaine parent.

# Tunnellisation (tunneling) DNS

- Les acteurs de menace qui utilisent la tunnellisation DNS placent le trafic non DNS dans le trafic DNS. Cette méthode contourne souvent les solutions de sécurité lorsqu'un acteur de menace souhaite communiquer avec des bots à l'intérieur d'un réseau protégé ou exfiltrer des données de l'organisation. Voici comment fonctionne la tunnelisation DNS pour les commandes CnC envoyées à un botnet:
  1. Les données de commande sont divisées en plusieurs blocs codés.
  2. Chaque bloc est placé sous une étiquette de nom de domaine d'un niveau inférieur à celui de la requête DNS.
  3. Étant donné qu'il n'y a pas de réponse du DNS local ou en réseau pour la requête, la demande est envoyée aux serveurs DNS récursifs du ISP.
  4. Le service DNS récursif transmet la requête au serveur de noms faisant autorité de l'acteur de menace.
  5. Le processus est répété jusqu'à ce que toutes les requêtes contenant les blocs soient envoyées.
  6. Lorsque le serveur de noms faisant autorité de l'acteur de menace reçoit les requêtes DNS des appareils infectés, il envoie des réponses pour chaque requête DNS, qui contiennent les commandes CnC encapsulées et encodées.
  7. Le logiciel malveillant (malware) sur l'hôte compromis recombine les morceaux et exécute les commandes cachées dans l'enregistrement DNS.
- Pour arrêter la tunnellisation DNS, l'administrateur réseau doit utiliser un filtre qui inspecte le trafic DNS. Portez une attention particulière aux requêtes DNS qui sont plus longues que la moyenne, ou celles qui ont un nom de domaine suspect.

# DHCP

- Les serveurs DHCP fournissent dynamiquement des informations de configuration IP aux clients.
- Dans la figure, un client diffuse un message de découverte DHCP. Le DHCP répond avec une offre de monodiffusion qui inclut les informations d'adressage que le client peut utiliser. Le client diffuse une requête DHCP pour indiquer au serveur que le client accepte l'offre. Le serveur répond par un accusé de réception monodiffusion acceptant la demande.



# Attaques DHCP

- Une **attaque d'usurpation DHCP** se produit lorsqu'un serveur DHCP non autorisé est connecté au réseau et fournit de faux paramètres de configuration IP aux clients légitimes. Un serveur non autorisé peut fournir une variété d'informations trompeuses:
  - **Passerelle par défaut incorrecte** - L'acteur de menace fournit une passerelle non valide ou l'adresse IP de son hôte pour créer une attaque MITM. Cela peut ne pas être détecté car l'intrus intercepte le flux de données à travers le réseau.
  - **Serveur DNS incorrect** - L'acteur de menace fournit une adresse de serveur DNS incorrecte orientant l'utilisateur vers un site Web malveillant.
  - **Adresse IP incorrecte** - L'acteur de menace fournit une adresse IP non valide, une adresse IP de passerelle par défaut non valide, ou les deux. L'acteur de la menace crée ensuite une attaque DoS sur le client DHCP.

# Attaques DHCP (suite)

Supposons qu'un acteur de menace ait correctement connecté un serveur DHCP non autorisé à un port de commutateur sur le même sous-réseau que les clients cibles. Le but du serveur non autorisé est de fournir aux clients de fausses informations de configuration IP.

1. Le client diffuse une demande de découverte DHCP à la recherche d'une réponse d'un serveur DHCP. Les deux serveurs reçoivent le message.
2. Les serveurs DHCP légitimes et escrocs répondent chacun avec des paramètres de configuration IP valides. Le client répond à la première offre reçue
3. Le client a d'abord reçu l'offre frauduleuse. Il diffuse une requête DHCP acceptant les paramètres du serveur non autorisé. Le serveur légitime et escroc reçoit chacun la demande.
4. Seul le serveur non autorisé envoie un message de réponse au client pour accuser réception de sa demande. Le serveur légitime cesse de communiquer avec le client car la demande a déjà été acquittée.

# Confidentialité, disponibilité et intégrité

- La sécurité du réseau consiste à protéger les informations et les systèmes d'information contre tout accès, utilisation, divulgation, interruption, modification ou destruction non autorisés.
- La plupart des organisations suivent la triade de sécurité de l'information de la “CIA”:
  - **Confidentialité** - Seuls les individus, entités ou processus autorisés peuvent accéder aux informations sensibles. Cela peut nécessiter l'utilisation d'algorithmes de cryptage cryptographiques tels que AES pour crypter et décrypter les données.
  - **Intégrité** -Désigne la protection des données contre toute altération non autorisée. Il nécessite l'utilisation d'algorithmes de hachage cryptographiques tels que SHA.
  - **Disponibilité** (Availibility) - Les utilisateurs autorisés doivent avoir un accès ininterrompu aux ressources et données importantes. Cela nécessite la mise en œuvre de services, de passerelles et de liaisons redondants.

# L'approche de défense en profondeur

- Pour garantir des communications sécurisées sur les réseaux publics et privés, vous devez sécuriser les appareils, y compris les routeurs, les commutateurs, les serveurs et les hôtes. La plupart des organisations utilisent une approche de défense en profondeur de la sécurité. Cela nécessite une combinaison de périphériques réseau et de services fonctionnant ensemble.
- Plusieurs dispositifs et services de sécurité sont mis en œuvre.
  - **VPN**
  - **Pare-feu**
  - **Serveur AAA**
  - **……**
- Tous les périphériques réseau, y compris le routeur et les commutateurs, sont renforcés.
- Vous devez également sécuriser les données lorsqu'elles transitent par différents liens.

# Pare-feu

Un pare-feu est un système ou un groupe de systèmes qui applique une stratégie de contrôle d'accès entre les réseaux.

**Allow** traffic from any external address to the web server.

**Allow** traffic to FTP server.

**Allow** traffic to SMTP server.

**Allow** traffic to internal IMAP server.

**Deny** all inbound traffic with network addresses matching internal-registered IP addresses.

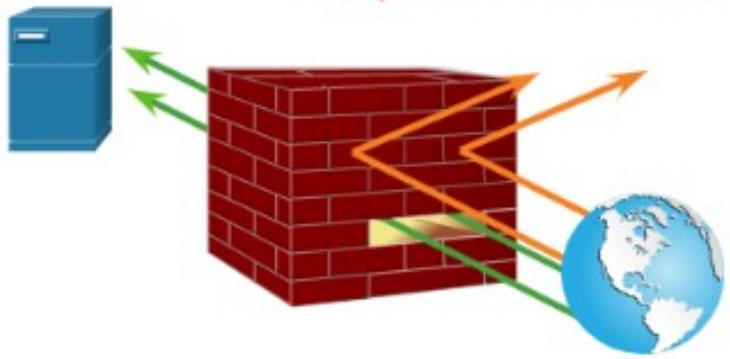
**Deny** all inbound traffic to server from external addresses.

**Deny** all inbound ICMP echo request traffic.

**Deny** all inbound MS Active Directory queries.

**Deny** all inbound traffic to MS SQL server queries.

**Deny** all MS Domain Local Broadcasts.



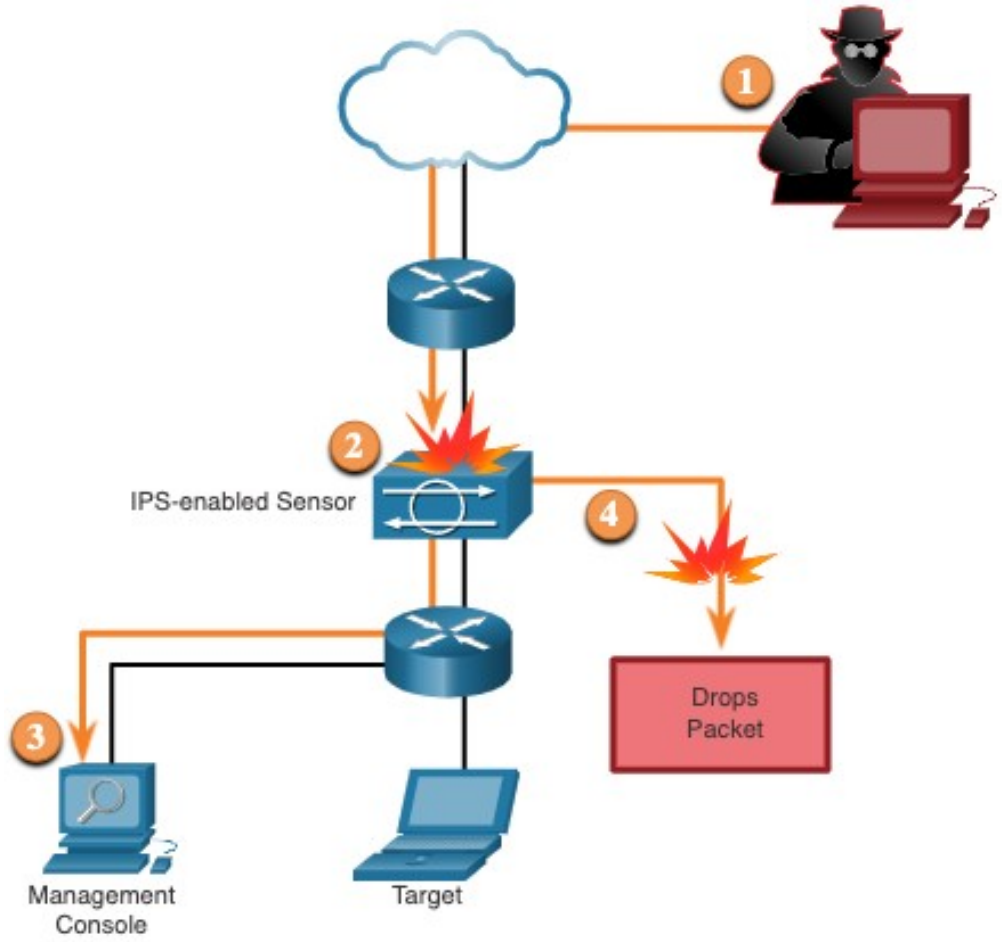
# IPS/IDS (système de prévention/détection d'intrusion)

- Pour vous défendre contre les attaques rapides et évolutives, vous pouvez avoir besoin de systèmes de détection et de prévention économiques intégrés aux points d'entrée et de sortie du réseau.
- Les technologies IDS et IPS partagent plusieurs caractéristiques. Les technologies IDS et IPS sont toutes deux déployées comme des capteurs. Un capteur IDS ou IPS peut se présenter sous la forme de plusieurs appareils différents:
  - Un routeur configuré avec le logiciel Cisco IOS IPS
  - Un appareil spécialement conçu pour fournir des services IDS ou IPS dédiés
  - Un module réseau installé dans un dispositif de sécurité adaptatif ASA (Adaptive Security Appliance), un commutateur ou un routeur
  - Les technologies IDS et IPS détectent les modèles de trafic réseau à l'aide de signatures, qui sont un ensemble de règles utilisées pour détecter les activités malveillantes. Les technologies IDS et IPS peuvent détecter des modèles de signature atomique (mono-paquet) ou des modèles de signature composite (multi-paquet).

# IPS (suite)

La figure montre comment un IPS gère le trafic refusé.

1. L'acteur de menace envoie un paquet destiné à l'ordinateur portable cible.
2. L'IPS intercepte le trafic et l'évalue par rapport aux menaces connues et aux stratégies configurées.
3. L'IPS envoie un message de journal à la console de gestion.
4. L'IPS abandonne le paquet.



# Appareils de sécurité du contenu

- Appliance de sécurité de messagerie Cisco ESA (Cisco Email Security Appliance) est un appareil spécial conçu pour surveiller le protocole de transfert de courrier simple SMTP (Simple Mail Transfer Protocol). Cisco ESA est constamment mis à jour par des flux en temps réel de Cisco Talos. Ces données de renseignement sur les menaces sont extraites par Cisco ESA toutes les trois à cinq minutes.
- L'appareil de sécurité Web Cisco (WSA) est une technologie d'atténuation des menaces Web. Cisco WSA combine une protection avancée contre les logiciels malveillants, la visibilité et le contrôle des applications, des contrôles de politique d'utilisation acceptable et des rapports.
- Cisco WSA offre un contrôle complet sur la façon dont les utilisateurs accèdent à Internet. Le WSA peut effectuer la mise sur liste noire des URL, le filtrage des URL, l'analyse des logiciels malveillants, la catégorisation des URL, le filtrage des applications Web et le chiffrement et le déchiffrement du trafic Web.

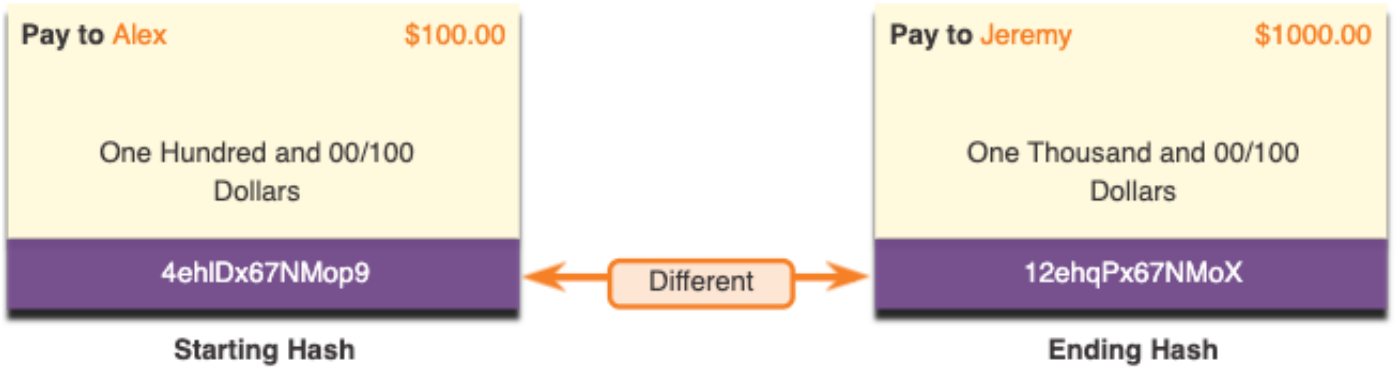
# Sécurisant les communications

- Les organisations doivent fournir un support pour sécuriser les données au fur et à mesure qu'elles traversent les liens. Cela peut inclure le trafic interne, mais il est encore plus important de protéger les données qui circulent en dehors de l'organisation.
- Ce sont les quatre éléments des communications sécurisées:
  - **Intégrité des données** -garantit que le message n'a pas été modifié. L'intégrité est assurée par l'implémentation de Message Digest version 5 (MD5) ou des algorithmes de génération de hachage SHA (Secure Hash Algorithm).
  - **Authentification d'origine** - Garantit que le message n'est pas une contrefaçon et qu'il provient du propriétaire. De nombreux réseaux modernes garantissent l'authentification avec des protocoles, par exemple le code HMAC (hash message authentication code).
  - **Confidentialité des données** - Garantit que seuls les utilisateurs autorisés peuvent lire le message. La confidentialité des données est implémentée à l'aide d'algorithmes de chiffrement symétrique et asymétrique.
  - **Non-répudiation des données** - Garantit que l'expéditeur ne peut pas répudier ou réfuter la validité d'un message envoyé. La non-répudiation repose sur le fait que seul l'expéditeur dispose des caractéristiques uniques ou de la signature relative au traitement du message.
- La cryptographie peut être utilisée presque partout où se produit une communication de données. En fait, la tendance est au cryptage (Chiffrement :) de toutes les communications.

# Intégrité des données

- Les fonctions de hash sont utilisées pour garantir l'intégrité d'un message. Ils garantissent que les données des messages n'ont pas été modifiées accidentellement ou intentionnellement.
- Sur la figure, l'expéditeur envoie un transfert d'argent de 100 $ à Alex. L'expéditeur souhaite s'assurer que le message n'est pas modifié sur son chemin vers le récepteur.

1. Le périphérique émetteur entre le message dans un algorithme de hachage et calcule son hachage de longueur fixe de 4ehiDx67NMop9.
2. Ce hash est ensuite joint au message et envoyé au récepteur. Le message et le hash sont en texte clair.
3. Le périphérique récepteur supprime le hash du message et saisit celui-ci dans le même algorithme de hash. Si le hash calculé est égal à celui joint au message, c'est que celui-ci n'a pas été modifié pendant l'envoi. Si les hachages ne sont pas égaux, l'intégrité du message ne peut plus être approuvée.

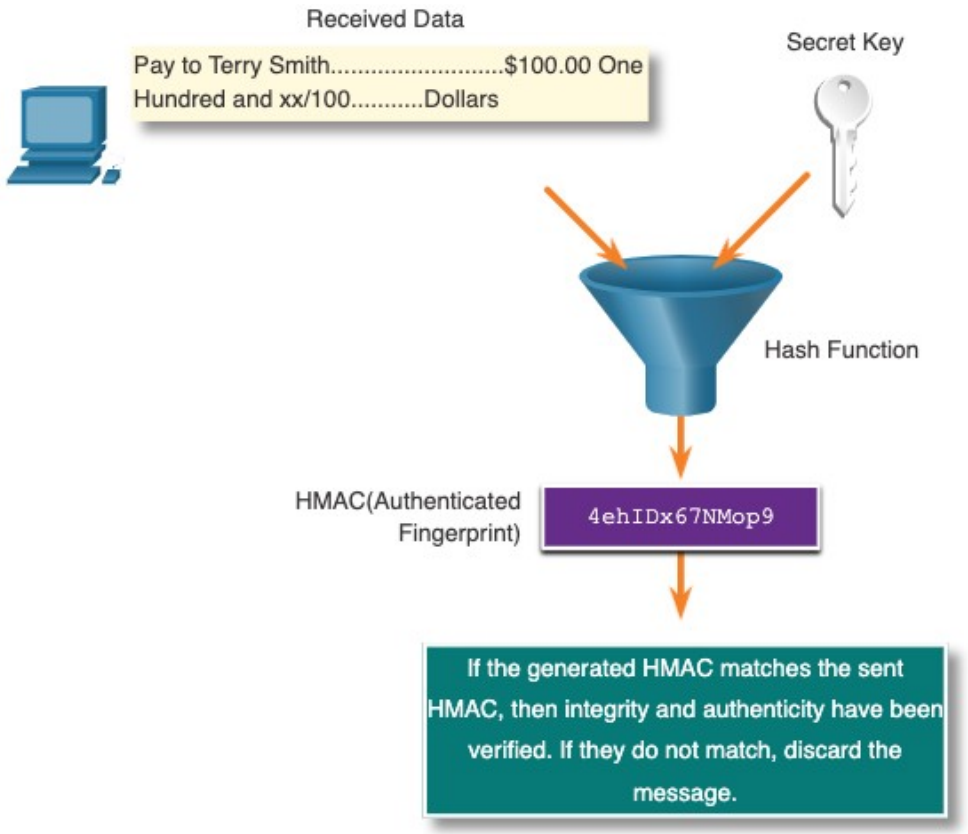


# Fonctions de hash

- Il existe trois fonctions de hachage bien connues.
  - **MD5 avec 128 bits Digest:** MD5 est une fonction unidirectionnelle qui produit un message haché de 128 bits. MD5 est un algorithme hérité qui ne devrait être utilisé que lorsqu'aucune meilleure alternative n'est disponible. Utilisez SHA-2 à la place.
  - **Algorithme de hachage SHA:** SHA-1 très similaire aux fonctions de hash MD5. SHA-1 crée un message haché de 160 bits et est légèrement plus lent que MD5. SHA-1 a des défauts connus et c'est un algorithme hérité. Utilisez SHA-2 lorsque cela est possible.
  - **SHA-2:** cela inclut SHA-224 (224 bits), SHA-256 (256 bits), SHA-384 (384 bits) et SHA-512 (512 bits). SHA-256, SHA-384 et SHA-512 sont des algorithmes de nouvelle génération et doivent être utilisés dans la mesure du possible.
- Bien que le hachage puisse être utilisé pour détecter des modifications accidentelles, il ne peut pas être utilisé pour se prémunir contre des modifications délibérées. Cela signifie que n'importe qui peut calculer un hash pour n'importe quelle donnée, à condition de disposer de la fonction de hash correcte.
- Par conséquent, le hachage est vulnérable aux attaques de l'homme-au-milieu et n'assure pas la sécurité des données transmises.

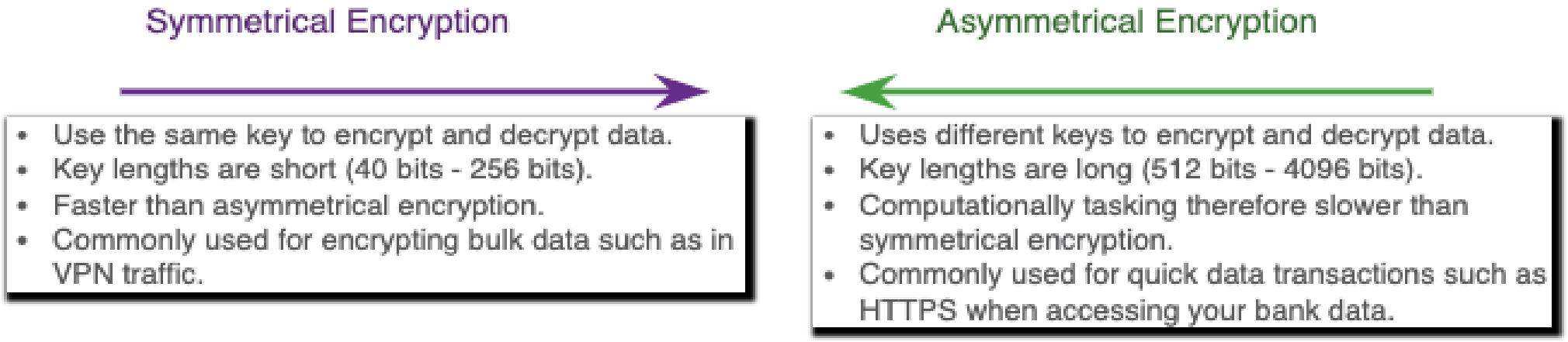
# Authentification de l'origine

- Pour ajouter l'authentification à l'assurance d'intégrité, utilisez un code d'authentification de message de hachage à clé (HMAC).
- Un HMAC est calculé à l'aide de tout algorithme cryptographique qui combine une fonction de hachage cryptographique avec une clé secrète.
- Seules les parties qui ont accès à cette clé secrète peuvent calculer le condensé d'une fonction HMAC. Cela permet de contrecarrer les attaques de type "homme-au-milieu" et d'authentifier l'origine des données.



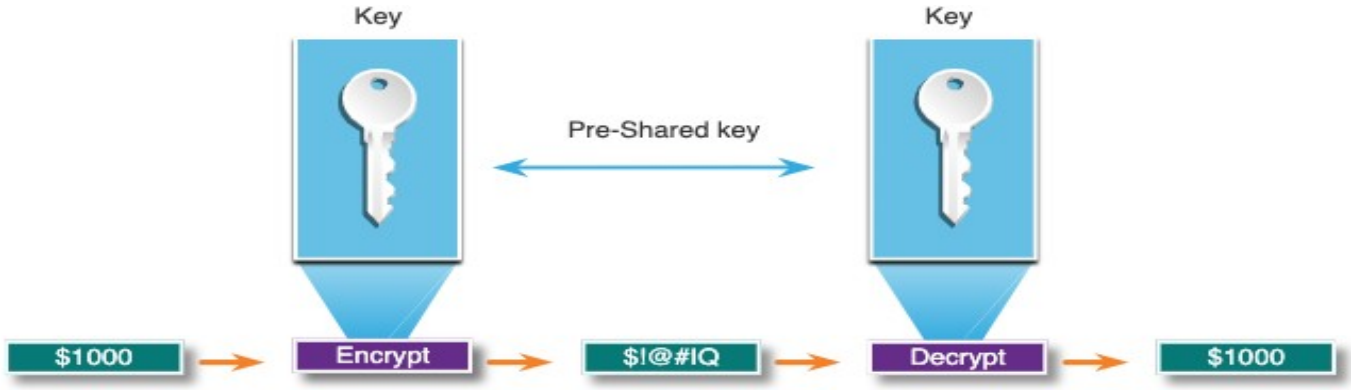
# Confidentialité des données

- Il existe deux classes de cryptage (bon ok, chiffrement) utilisées pour assurer la confidentialité des données. Ces deux classes diffèrent dans la façon dont elles utilisent les clés.
- Les algorithmes de chiffrement symétrique tels que (DES), 3DES et Advanced Encryption Standard (AES) sont basés sur l'hypothèse que chaque partie communicante connaît la clé pré-partagée. La confidentialité des données peut également être assurée à l'aide d'algorithmes asymétriques, notamment Rivest, Shamir et Adleman (RSA) et l'infrastructure à clé publique (PKI).
- La figure met en évidence les différences entre chaque méthode d'algorithme de chiffrement.



# Chiffrement symétrique

- Les algorithmes symétriques utilisent la même clé pré-partagée, également appelée clé secrète, pour crypter et décrypter les données. L'expéditeur et le destinataire connaissent une clé pré-partagée avant que toute communication chiffrée puisse avoir lieu.
- Les algorithmes de chiffrement symétriques sont couramment utilisés avec le trafic VPN car ils utilisent moins de ressources CPU que les algorithmes de chiffrement asymétriques.
- Lorsque vous utilisez des algorithmes de chiffrement symétriques, plus la clé est longue, plus il faudra du temps à quelqu'un pour découvrir la clé. Pour garantir la sécurité du cryptage, utilisez une longueur de clé minimale de 128 bits.



# Chiffrement symétrique (suite)

| Algorithmes de chiffrement symétriques | Description |
|---|---|
| **Algorithme de chiffrement des données (DES)** | Il s'agit d'un algorithme de chiffrement symétrique. Il peut être utilisé en mode de chiffrement de flux, mais fonctionne habituellement en mode bloc pour chiffrer les données dans une taille de bloc de 64 bits. Un chiffrement de flux chiffre un byte ou un bit à la fois. |
| **3DES (Triple DES)** | Il s'agit d'une version plus récente de DES, mais elle répète le processus d'algorithme DES trois fois. Il est considéré comme très fiable lorsqu'il est mis en œuvre en utilisant des durées de vie de clé très courtes. |
| **Norme de cryptage avancée (AES)** | AES est un algorithme sécurisé et plus efficace que l'algorithme 3DES.<br>Il s'agit d'un algorithme de chiffrement symétrique populaire et recommandé. Il propose neuf combinaisons de longueur de clé et de bloc en utilisant une longueur de clé variable de 128, 192 ou 256 bits pour crypter des blocs de données de 128, 192 ou 256 bits. |
| **Algorithme de chiffrement optimisé par logiciel (SEAL)** | SEAL est un algorithme de chiffrement symétrique alternatif plus rapide que DES, 3DES et AES. Il utilise une clé de cryptage 160 bits et a un impact moindre sur le processeur par rapport aux autres algorithmes logiciels. |
| **Algorithmes de la série Rivest Ciphers (RC)** | Cet algorithme a été développé par Ron Rivest. Plusieurs variantes ont été développées, mais le RC4 est le plus utilisé. RC4 est un chiffrement de flux et est utilisé pour sécuriser le trafic Web en SSL et TLS. |

# Chiffrement symétrique

- Les algorithmes asymétriques, également appelés algorithmes à clé publique, sont conçus pour que la clé utilisée pour le chiffrement soit différente de la clé utilisée pour le déchiffrement.
- Les algorithmes asymétriques utilisent une clé publique et une clé privée. La clé appariée complémentaire est requise pour le déchiffrement. Les données chiffrées avec la clé publique nécessitent la clé privée pour être déchiffrées. Les algorithmes asymétriques assurent la confidentialité, l'authentification et l'intégrité en utilisant ce processus.
- Étant donné qu'aucune des parties n'a un secret partagé, des longueurs de clé très longues doivent être utilisées. Le chiffrement asymétrique peut utiliser des longueurs de clé comprises entre 512 et 4 096 bits. Des longueurs de clé supérieures ou égales à 1024 bits peuvent être approuvées tandis que des longueurs de clé plus courtes sont considérées comme non fiables.

# Chiffrement asymétrique (suite)

- Voici des exemples de protocoles qui utilisent des algorithmes à clé asymétrique:
  - **Échange de clés Internet IKE (Internet Key Exchange) -** Il s'agit d'un composant fondamental des VPN IPsec.
  - **SSL (Secure Socket Layer) -** Ceci est maintenant implémenté en tant que TLS (Transport Layer Security) standard de l'IETF.
  - **SSH (Secure Shell) -** protocole qui assure une connexion à distance sécurisée aux appareils réseau.
  - **PGP (Pretty Good Privacy) -** Ce programme informatique fournit une confidentialité cryptographique et une authentification. Il est souvent utilisé pour augmenter la sécurité des communications par e-mail.
- Les algorithmes asymétriques sont sensiblement plus lents que les algorithmes symétriques. Leur conception est basée sur des problèmes de calcul, tels que la factorisation de très grands nombres ou le calcul de logarithmes discrets de très grands nombres.
- Parce qu'ils sont lents, les algorithmes asymétriques sont généralement utilisés dans les mécanismes cryptographiques à faible volume, tels que les signatures numériques et l'échange de clés.

Cryptographie

# Chiffrement asymétrique (suite)

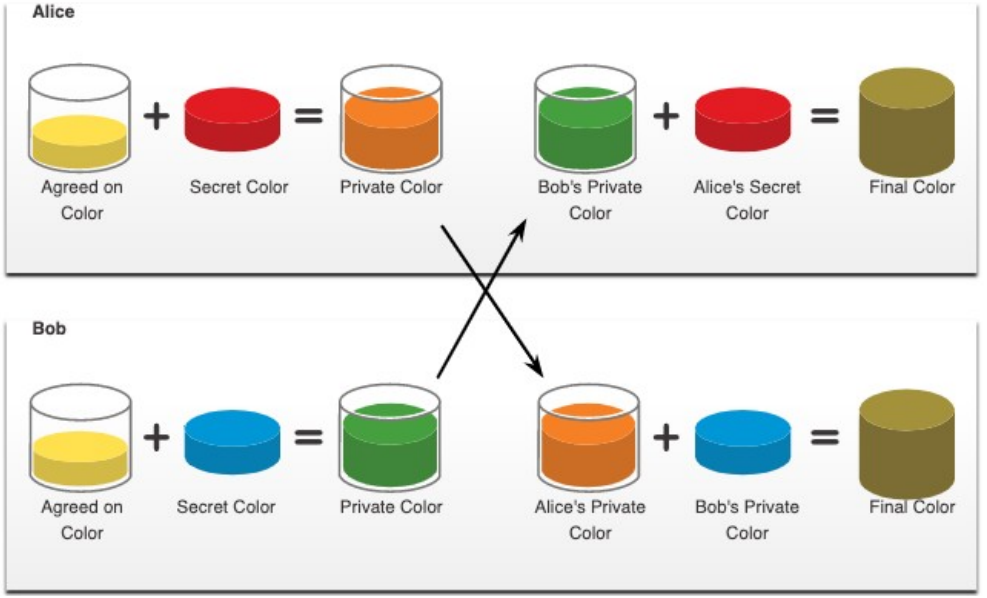
| Algorithmes de chiffrement asymétrique | Longueur de clé (Key Length) | Description |
|---|---|---|
| **Diffie-Hellman (DH)** | 512, 1024, 2048, 3072, 4096 | L'algorithme Diffie-Hellman permet à deux parties de s'entendre sur une clé qu'elles peuvent utiliser pour crypter les messages qu'elles souhaitent s'envoyer l'une à l'autre. La sécurité de cet algorithme dépend de l'hypothèse qu'il est facile d'élever un nombre à une certaine puissance, mais difficile de calculer quelle puissance a été utilisée compte tenu du nombre et du résultat. |
| **Norme de signature numérique (DSS) et algorithme de signature numérique (DSA)** | 512 - 1024 | DSS spécifie DSA comme algorithme pour les signatures numériques. DSA est un algorithme à clé publique basé sur le schéma de signature ElGamal. La vitesse de création de signature est similaire à RSA mais est 10 à 40 fois plus lente pour la vérification. |
| **Algorithmes de chiffrement Rivest, Shamir et Adleman (RSA)** | De 512 à 2048 | RSA est destiné à la cryptographie à clé publique basée sur la difficulté actuelle de factoriser de très grands nombres. Il s'agit du premier algorithme connu pour être adapté à la signature ainsi qu'au cryptage. Il est largement utilisé dans les protocoles de commerce électronique et est censé être sécurisé étant donné les clés suffisamment longues et l'utilisation d'implémentations à jour. |
| **ElGamal** | De 512 à 1024 | Un algorithme de chiffrement asymétrique de cryptographie à clé publique qui repose sur l'accord de clé Diffie-Hellman. Un inconvénient du système ElGamal est que le message crypté devient très gros, environ deux fois la taille du message d'origine et pour cette raison, il n'est utilisé que pour les petits messages tels que les clés secrètes. |
| **Techniques de courbe elliptique** | 160 | La cryptographie à courbe elliptique peut être utilisée pour adapter de nombreux algorithmes cryptographiques, tels que Diffie-Hellman ou ElGamal. Le principal avantage de la cryptographie sur les courbes elliptiques est que les clés peuvent être beaucoup plus petites. |

# Diffie-Hellman

- Diffie-Hellman (DH) est un algorithme mathématique asymétrique où deux ordinateurs génèrent une clé secrète partagée identique sans avoir communiqué auparavant. En réalité, la nouvelle clé partagée n'est pas véritablement échangée entre l'émetteur et le récepteur.
- Voici trois exemples d'instances où DH est couramment utilisé:
  - Les données sont échangées à l'aide d'un VPN IPsec.
  - Les données sont cryptées sur Internet à l'aide de SSL ou TLS.
  - Les données SSH sont échangées.
- La sécurité DH utilise des nombres incroyablement élevés dans ses calculs.
- Malheureusement, les systèmes à clé asymétrique sont extrêmement lents, quel que soit le mode de chiffrement par bloc. Par conséquent, il est courant de chiffrer la majeure partie du trafic à l'aide d'un algorithme symétrique, tel que 3DES ou AES, puis d'utiliser l'algorithme DH pour créer des clés qui seront utilisées par l'algorithme de chiffrement.

# Diffie-Hellman (suite)

- Les couleurs de la figure seront utilisées à la place des nombres pour simplifier le processus d'accord de clé DH. L'échange de clés DH commence par Alice et Bob se mettant d'accord sur une couleur commune arbitraire qui n'a pas besoin d'être gardée secrète. La couleur convenue dans notre exemple est le jaune.
- Ensuite, Alice et Bob doivent chacun choisir une couleur secrète. Alice choisit le rouge et Bob le bleu. Ces couleurs secrètes ne doivent jamais être partagées. La couleur secrète représente la clé privée choisie par chacune des parties.
- Alice et Bob mélangent maintenant la couleur commune partagée (le jaune) avec leur propre couleur secrète afin d'obtenir une couleur privée. Par conséquent, Alice mélange le jaune au rouge et obtient ainsi une couleur privée orange. Bob mélange le jaune au bleu et obtient ainsi une couleur privée verte.
- Alice envoie sa couleur privée (l'orange) à Bob et Bob envoie sa couleur privée (le vert) à Alice.
- Alice et Bob mélangent chacun la couleur qu'ils ont reçue avec leur couleur d'origine secrète (rouge pour Alice et bleu pour Bob). Le résultat est un mélange de couleurs marron final identique au mélange de couleurs final de l'autre. La couleur brune représente la clé secrète partagée résultante entre Bob et Alice.



# Réseaux fixes
# II.3 Sécurité
# Concepts ACL

Luc Deneire

EII-5, Option Réseaux et Objets Connectés (ROC)

# Qu'est-ce qu'une liste de contrôle d'accès?

Une liste de contrôle d'accès (ou ACL) est une série de commandes IOS qui déterminent si un routeur achemine ou abandonne les paquets en fonction des informations contenues dans l'en-tête de paquet. Par défaut, aucune ACL n'est configurée pour un routeur. Toutefois, lorsqu'une liste de contrôle d'accès est appliquée à une interface, le routeur évalue tous les paquets réseau lorsqu'ils traversent l'interface pour déterminer s'ils peuvent être acheminés.

- Une ACL utilise une liste séquentielle de déclarations d'autorisation ou de refus, connues sous le nom d'entrées de contrôle d'accès (ACE).

**Remarque:** Les ACE sont couramment appelées des instructions de liste de contrôle d'accès.

- Lorsque le trafic réseau traverse une interface configurée avec une liste de contrôle d'accès, le routeur compare les informations du paquet à chaque ACE, dans l'ordre séquentiel, afin de déterminer si le paquet correspond à l'une des entrées ACE. C’est ce que l’on appelle le filtrage de paquet.

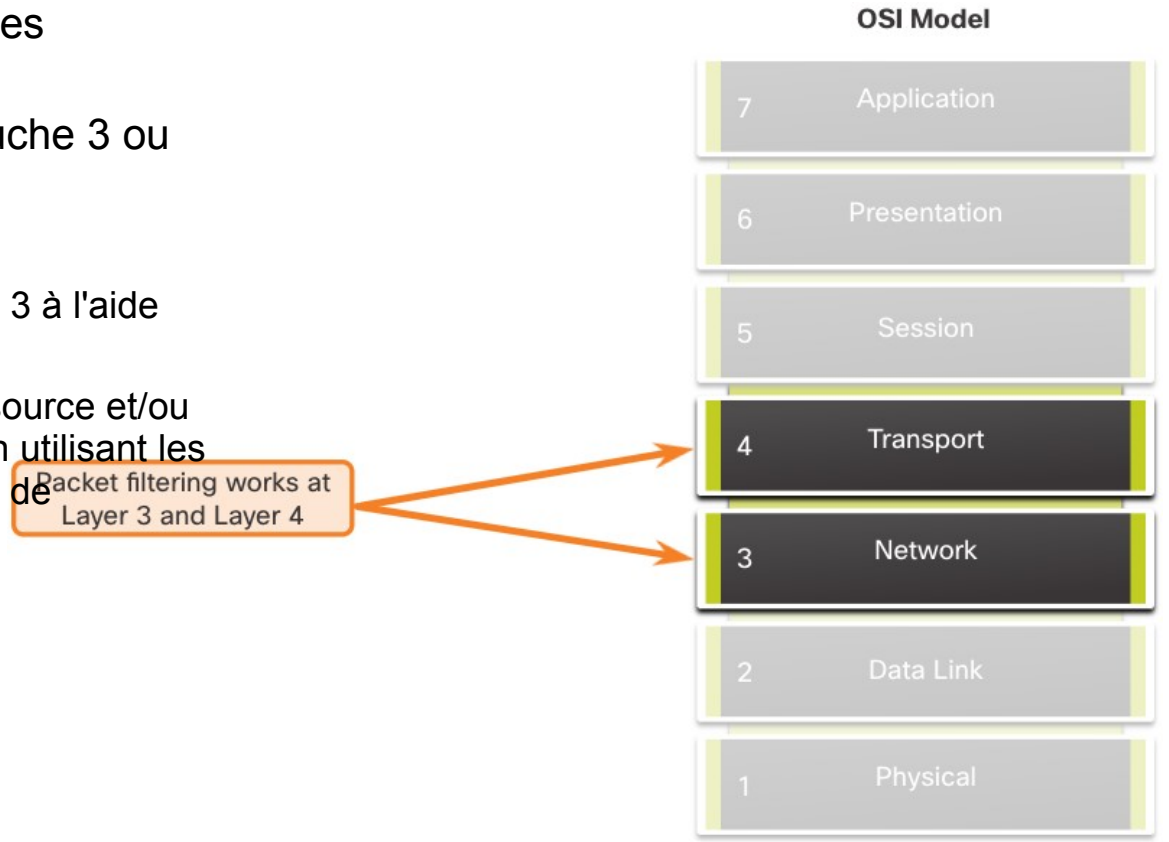
# Qu'est-ce qu'une liste de contrôle d'accès? (Suite)

Plusieurs tâches effectuées par les routeurs nécessitent l'utilisation d'ACL pour identifier le trafic:

- Limiter le trafic du réseau pour en augmenter les performances
- Elles contrôlent le flux de trafic.
- Elles fournissent un niveau de sécurité de base pour l'accès réseau.
- Elles filtrent le trafic en fonction de son type.
- Contrôler les hôtes pour autoriser ou refuser l'accès aux services de réseau
- Donner la priorité à certaines classes de trafic réseau

# Filtrage des paquets

- Le filtrage de paquets contrôle l'accès à un réseau en analysant les paquets entrants et/ou sortants et en les transmettant ou en les abandonnant en fonction de critères donnés.
- Le filtrage des paquets peut être effectué au niveau de la couche 3 ou de la couche 4.
- Les routeurs Cisco prennent en charge deux types de ACLs:
  - **ACL standard** - Les ACL filtrent uniquement au niveau de la couche 3 à l'aide de l'adresse IPv4 source uniquement.
  - **ACL étendues** - Filtre ACL à la couche 3 à l'aide de l'adresse IPv4 source et/ou destination. Ils peuvent également filtrer au niveau de la couche 4 en utilisant les ports TCP et UDP, ainsi que des informations facultatives sur le type de protocole pour un contrôle plus fin.



# Le fonctionnement des listes de contrôle d'accès

- Les listes de contrôle d'accès définissent des règles de contrôle pour les paquets arrivant par les interfaces d'entrée, passant par le routeur et atteignant leur destination par les interfaces de sortie.
- Les listes de contrôle d'accès peuvent être configurées pour s'appliquer au trafic entrant et au trafic sortant:

**Remarque**: Les ACL ne gèrent pas les paquets provenant du routeur lui-même.

- Une ACL entrante filtre les paquets avant qu'ils ne soient acheminés vers l'interface sortante. Une liste de contrôle d’accès entrante est efficace car elle réduit la charge des recherches de routage en cas d’abandon du paquet.
- Les listes de contrôle d'accès sortantes filtrent les paquets après qu'ils ont été routés, et ce, quelle que soit l'interface de sortie.

# Le fonctionnement des listes de contrôle d'accès (Suite)

Lorsqu'une ACL est appliquée à une interface, elle suit une procédure d'exploitation spécifique. Voici les étapes opérationnelles utilisées lorsque le trafic est entré dans une interface de routeur avec une ACL IPv4 standard entrante configurée:

1. Le routeur extrait l'adresse IPv4 source de l'en-tête du paquet.
2. Le routeur commence en haut de l'ACL et compare l'adresse IPv4 source à chaque ACE dans un ordre séquentiel.
3. Lorsqu'une correspondance est établie, le routeur exécute l'instruction, soit en autorisant soit en refusant le paquet, et les ACE restants dans l'ACL, le cas échéant, ne sont pas analysés.
4. Si l'adresse IPv4 source ne correspond à aucun ACE de l'ACL, le paquet est ignoré car un ACE de refus implicite est automatiquement appliqué à toutes les ACLs.

La dernière instruction d'une liste de contrôle d'accès est toujours une instruction deny implicite bloquant tout le trafic. Il est caché et non affiché dans la configuration.

**Remarque**: Une liste ACL doit avoir au moins une déclaration d'autorisation sinon tout le trafic sera refusé en raison de l'instruction ACE de refus implicite.

# Présentation de masques génériques

Un masque générique est similaire à un masque de sous-réseau en ce sens qu'il utilise le processus AnDing pour identifier les bits d'une adresse IPv4 à correspondre. En effet, contrairement à un masque de sous-réseau, où le chiffre binaire 1 équivaut à une correspondance et le chiffre binaire 0 à une non-correspondance, les masques génériques procèdent de façon inverse.

- Un ACE IPv4 utilise un masque générique 32 bits pour déterminer quels bits de l'adresse à examiner pour rechercher une correspondance.
- Les masques génériques respectent les règles suivantes pour faire correspondre les chiffres binaires 1 et 0:
  - **Bit 0 de masque générique** - permet de vérifier la valeur du bit correspondant dans l'adresse.
  - **Masque générique bit 1** - Ignorer la valeur du bit correspondant dans l'adresse

# Présentation de masques génériques (Suite)

| Masque générique | Dernier octet (en binaire) | Signification (0 - match, 1 - ignorer) |
|---|---|---|
| **0.0.0.0** | **00000000** | Correspond à tous les octets. |
| **0.0.0.63** | **00111111** | •Faites correspondre les trois premiers octets<br>•Correspond aux deux bits les plus à gauche du dernier octet<br>•Les 6 derniers bits d'adresse sont ignorés |
| **0.0.0.15** | **00001111** | •Faites correspondre les trois premiers octets<br>•Correspond aux quatre bits les plus à gauche du dernier octet<br>•Ignorer les 4 derniers bits du dernier octet |
| **0.0.0.248** | **11111100** | •Faites correspondre les trois premiers octets<br>•Ignorer les six bits les plus à gauche du dernier octet<br>•Faites correspondre les deux derniers bits |
| **0.0.0.255** | **11111111** | •Faites correspondre les trois premiers octet<br>•Ignorer le dernier octet |

# Types de masques génériques

**Caractère générique pour correspondre à un hôte:**

- Supposons que l'ACL 10 ait besoin d'un ACE qui autorise uniquement l'hôte avec l'adresse IPv4 192.168.1.1. Rappelez-vous que "0" équivaut à une correspondance et "1" à une ignorance. Pour correspondre à une adresse IPv4 d'hôte spécifique, un masque générique composé de tous les zéros (c.-à-d. 0.0.0.0) est requis.
- Lorsque l'ACE est traité, le masque générique n'autorisera que l'adresse 192.168.1.1. L'ACE résultant dans l'ACL 10 serait **access-list 10 permit 192.168.1.1 0.0.0.0.**

| | Décimal | Binaire |
|---|---|---|
| Adresse IPv4 | 192.168.1.1 | 11000000.10101000.00000001.00000001 |
| Masque générique | 0.0.0.0 | 00000000.00000000.00000000.00000000 |
| **Adresse IPv4 autorisée** | **192.168.1.1** | 11000000.10101000.00000001.00000001 |

# Types de masques génériques (Suite)

**Masques génériques correspondant à des sous-réseaux IPv4**

- ACL 10 a besoin d'un ACE qui autorise tous les hôtes du réseau 192.168.1.0/24. Le masque générique 0.0.0.255 stipule que les trois premiers octets doivent correspondre exactement, mais pas le quatrième octet.
- Lorsqu'il est traité, le masque générique 0.0.0.255 autorise tous les hôtes du réseau 192.168.1.0/24. L'ACE résultant dans l'ACL 10 serait **access-list 10 permit 192.168.1.0 0.0.0.255.**

| | Décimal | Binaire |
|---|---|---|
| Adresse IPv4 | 192.168.1.1 | 11000000.10101000.00000001.00000001 |
| Masque générique | 0.0.0.255 | 00000000.00000000.00000000.11111111 |
| **Adresse IPv4 autorisée** | **192.168.1.0/24** | 11000000.10101000.00000001.00000000 |

# Types de masques génériques (Suite)

**Masque générique pour correspondre à une plage d'adresses IPv4**

- ACL 10 a besoin d'un ACE qui autorise tous les hôtes des réseaux 192.168.16.0/24, 192.168.17.0/24,..., 192.168.31.0/24.
- Lorsqu'il est traité, le masque générique 0.0.15.255 autorise tous les hôtes des réseaux 192.168.16.0/24 à 192.168.31.0/24. L'ACE résultant dans l'ACL 10 serait **access-list 10 permit 192.168.16.0 0.0.15.255.**

| | Décimal | Binaire |
|---|---|---|
| Adresse IPv4 | 192.168.16.0 | 11000000.10101000.00010000.00000000 |
| Masque générique | 0.0.15.255 | 00000000.00000000.00001111.11111111 |
| **Adresse IPv4 autorisée** | **192.168.16.0/24 à 192.168.31.0/24** | 11000000.10101000.00010000.00000000<br>11000000.10101000.00011111.00000000 |

# Calcul de masque générique

Le calcul des masques génériques peut être complexe. La méthode la plus rapide consiste à soustraire le masque de sous-réseau de 255.255.255.255. Voici quelques exemples:

- Supposons que vous vouliez un ACE en ACL 10 pour permettre l'accès à tous les utilisateurs du réseau 192.168.3.0/24. Pour calculer le masque générique, soustrayez le masque de sous-réseau (c'est-à-dire 255.255.255.0) de 255.255.255.255. Cela génère le masque générique 0.0.0.255. L'ACE serait **access-list 10 permit 192.168.1.0 0.0.0.255.**
- Supposons que vous vouliez un ACE en ACL 10 pour permettre l'accès au réseau aux 14 utilisateurs du sous-réseau 192.168.3.32/28. Soustraire le sous-réseau (c'est-à-dire 255.255.255.240) de 255.255.255.255. Cela génère le masque générique 0.0.0.15. L'ACE serait **access-list 10 permit 192.168.3.32 0.0.0.15**
- Supposons que vous ayez besoin d'un ACE dans ACL 10 pour autoriser uniquement les réseaux 192.168.10.0 et 192.168.11.0. Ces deux réseaux pourraient être résumés comme 192.168.10.0/23 qui est un masque de sous-réseau de 255.255.254.0. Soustrayez 255.255.254.0 masque de sous-réseau de 255.255.255.255. Cela génère le masque générique 0.0.1.255. L'ACE serait **access-list 10 permit 192.168.10.0 0.0.1.255.**

# Les mots-clés des masques génériques

L'IOS de Cisco fournit deux mots clés pour identifier les utilisations les plus courantes du masquage générique. Les deux mots-clés sont:

- **host** - Ce mot-clé remplace le masque 0.0.0.0 Ce masque indique que tous les bits d'adresse IPv4 doivent correspondre pour pouvoir filtrer juste une adresse d'hôte.
- **any** - Ce mot clé remplace le masque 255.255.255.255 Ce masque indique qu'il convient d'ignorer l'intégralité de l'adresse IPv4 ou d'accepter n'importe quelle adresse.

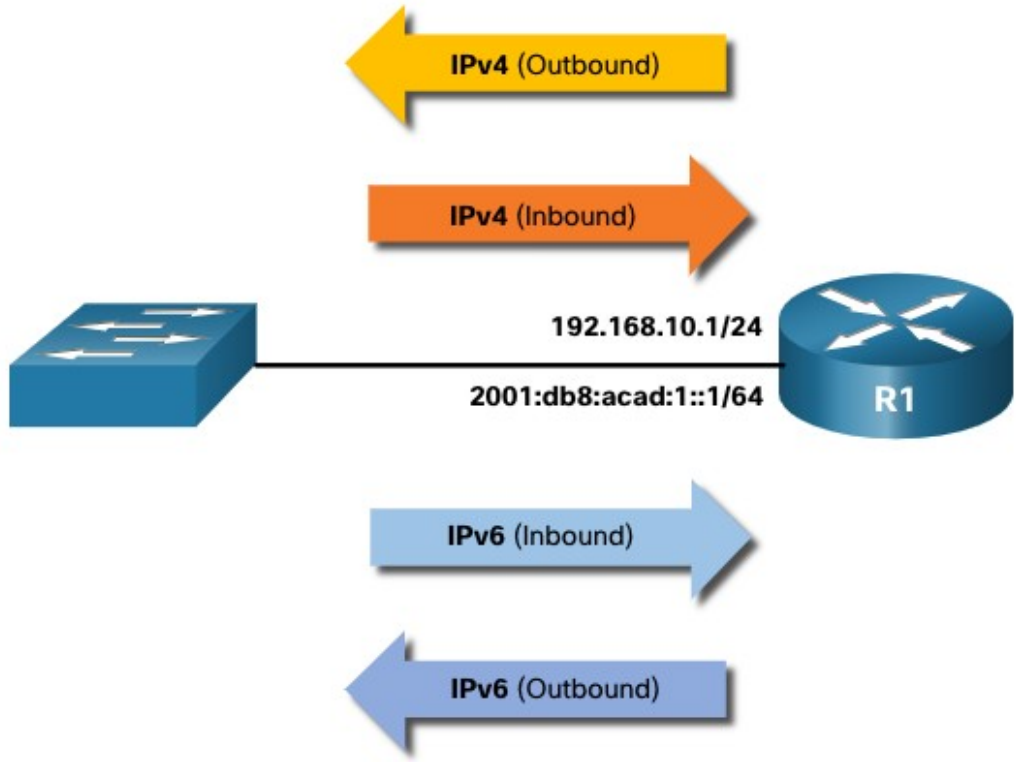
# Nombre limité d'ACL par interface

Le nombre de listes ACL pouvant être appliquées sur une interface de routeur est limité. Par exemple, une interface de routeur double empilée (c'est-à-dire IPv4 et IPv6) peut avoir jusqu'à quatre ACL appliquées, comme indiqué sur la figure.

Plus précisément, une interface de routeur peut avoir:

- Une liste ACL sortante IPv4.
- Une ACL IPv4 entrante.
- Une ACL IPv6 entrante.
- Une liste ACL IPv6 sortante.

**Remarque**: il n'est pas nécessaire de configurer les listes de contrôle d'accès dans les deux directions. Le nombre d'ACL et leur direction appliquée à l'interface dépendront de la stratégie de sécurité de l'organisation.



# Meilleure pratiques relatives aux listes de contrôle d'accès

L'utilisation des listes de contrôle d'accès nécessite beaucoup de précision et de soin. Les erreurs peuvent vous coûter cher et se solder par des pannes de réseau, d'importants efforts de dépannage et des services réseau médiocres. Une planification de base est nécessaire avant de configurer une ACL.

| Directive | Avantage |
|---|---|
| Créez vos listes de contrôle d'accès conformément à la stratégie de sécurité de votre entreprise. | Vous serez ainsi certain d'implémenter les instructions relatives à la sécurité organisationnelle. |
| Écrivez ce que vous voulez que l'ACL fasse. | Vous éviterez ainsi de créer d'éventuels problèmes d'accès par mégarde. |
| Utilisez un éditeur de texte pour créer, modifier et enregistrer les listes de contrôle d'accès. | Vous pourrez ainsi créer une bibliothèque de listes de contrôle d'accès réutilisables. |
| Documentez les ACL à l'aide de la commande **remark** . | Cela vous aidera (et d'autres) à comprendre le but d'un ACE. |
| Testez vos listes de contrôle d'accès sur un réseau de développement avant de les implémenter sur un réseau de production. | Vous éviterez ainsi de commettre des erreurs coûteuses. |

# Listes de contrôle d'accès standard et étendues

Types de listes de contrôle d'accès IPv4

- **ACL standard** - Ces listes autorisent ou refusent les paquets basés uniquement sur l'adresse IPv4 source.
- **ACL étendues** - Ces listes autorisent ou refusent les paquets basés sur l'adresse IPv4 source et l'adresse IPv4 de destination, le type de protocole, les ports TCP ou UDP source et destination et plus encore.

# Listes de contrôle d'accès numérotées et nommées

## Listes de contrôle d'accès numérotées

- Les ACL numérotées 1-99 ou 1300-1999 sont des ACL standard, tandis que les ACL numérotées 100-199 ou 2000-2699 sont des ACL étendues.

```
R1(config)# access-list ?
 <1-99> IP standard access list
 <100-199> IP extended access list
 <700-799> 48-bit MAC address access list
 <1300-1999> IP standard access list (expanded range)
 <200-299> Protocol type-code access list
 <2000-2699> IP extended access list (expanded range)
 <700-799> 48-bit MAC address access list
 rate-limit Simple rate-limit specific access list
 template Enable IP template acls
Router(config)# access-list
```

# Listes de contrôle d'accès numérotées et nommées (Suite)

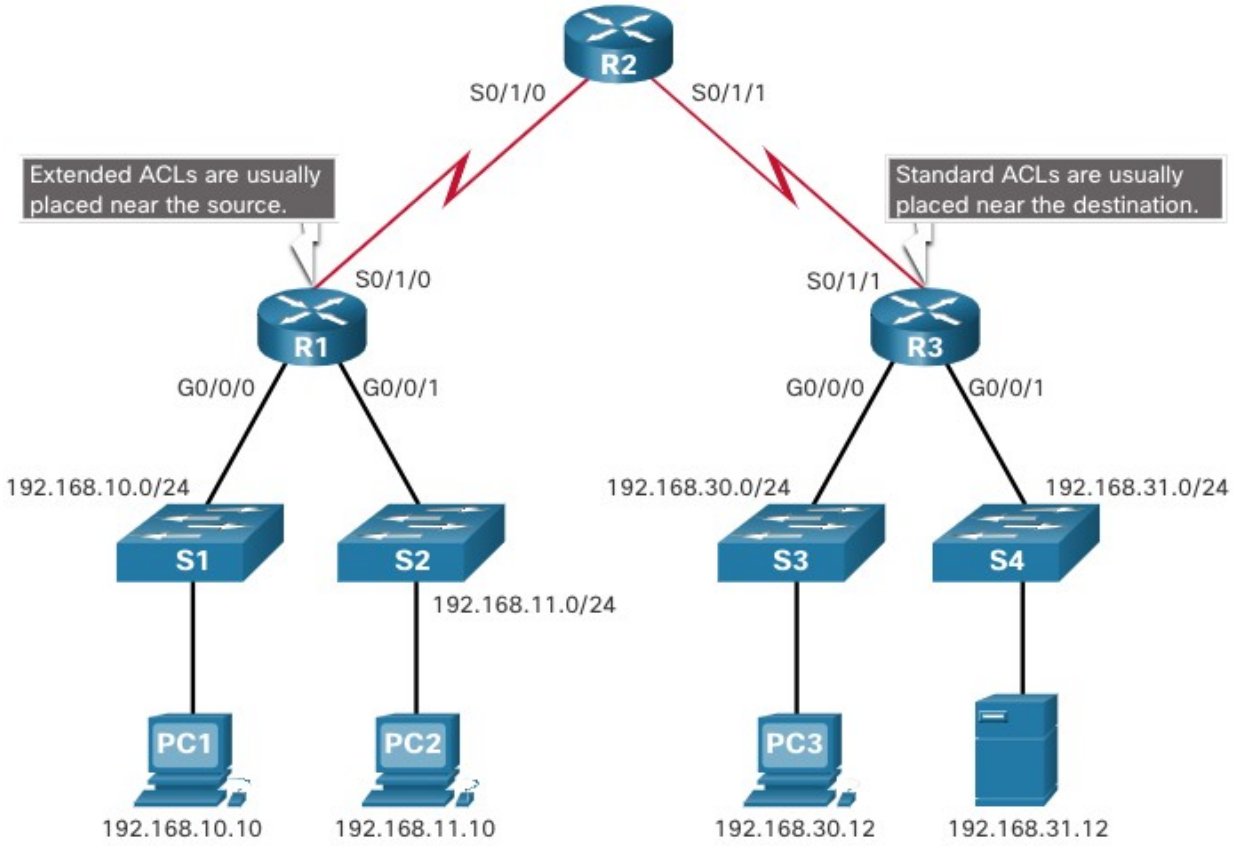
**Listes de contrôle d'accès nommées**

- Les ACL nommées sont la méthode préférée à utiliser lors de la configuration des ACL. Plus précisément, les listes ACL standard et étendues peuvent être nommées pour fournir des informations sur l'objet de la liste ACL. Par exemple, nommer un ACL FTP-FILTER étendu est beaucoup mieux que d'avoir une ACL numérotée 100.
- La commande de configuration globale **ip access-list** est utilisée pour créer une liste ACL nommée, comme illustré dans l'exemple suivant.

```
R1(config)# ip access-list extended FTP-FILTER
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq ftp
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq ftp-data R1(config-ext-nacl)#
```

# Où placer les listes de contrôle d'accès

- Chaque liste de contrôle d'accès doit être placée là où elle aura le plus grand impact sur les performances.
- Les listes de contrôle d'accès étendues doivent être placées le plus près possible de la source du trafic à filtrer.
- Les listes de contrôle d'accès standard doivent être placées le plus près possible de la destination.



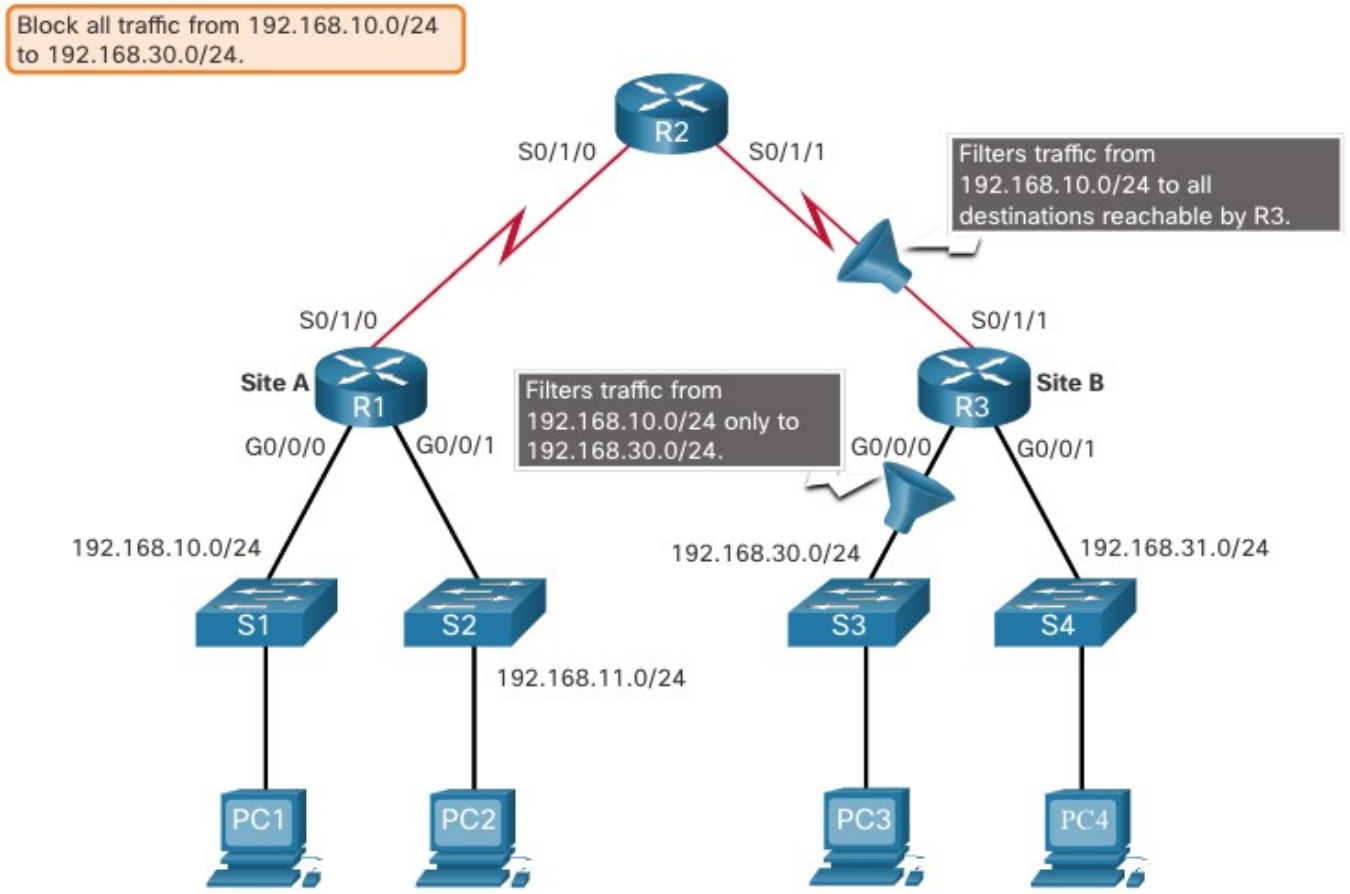
# Où placer les listes de contrôle d'accès (Suite)

| Facteurs influençant le placement des ACL | Explication |
|---|---|
| **L'étendue du contrôle organisationnel** | Le placement de l'ACL peut dépendre du fait que l'organisation contrôle ou non les réseaux source et destination. |
| **Bande passante des réseaux concernés** | Il peut être souhaitable de filtrer le trafic indésirable à la source pour empêcher la transmission de trafic qui consomme de la bande passante. |
| **Simplicité de configuration** | •Il peut être plus facile d'implémenter une liste ACL à destination, mais le trafic utilisera inutilement la bande passante.<br>•Une liste de contrôle d'accès étendue peut être utilisée sur chaque routeur d'où provient le trafic. Cela permet d'économiser de la bande passante en filtrant le trafic à la source, mais exige de créer des listes de contrôle d'accès étendues sur plusieurs routeurs. |

# Exemple d'emplacement de liste de contrôle d'accès standard

Sur la figure, l'administrateur souhaite empêcher le trafic provenant du réseau 192.168.10.0/24 d'accéder au réseau 192.168.30.0/24.

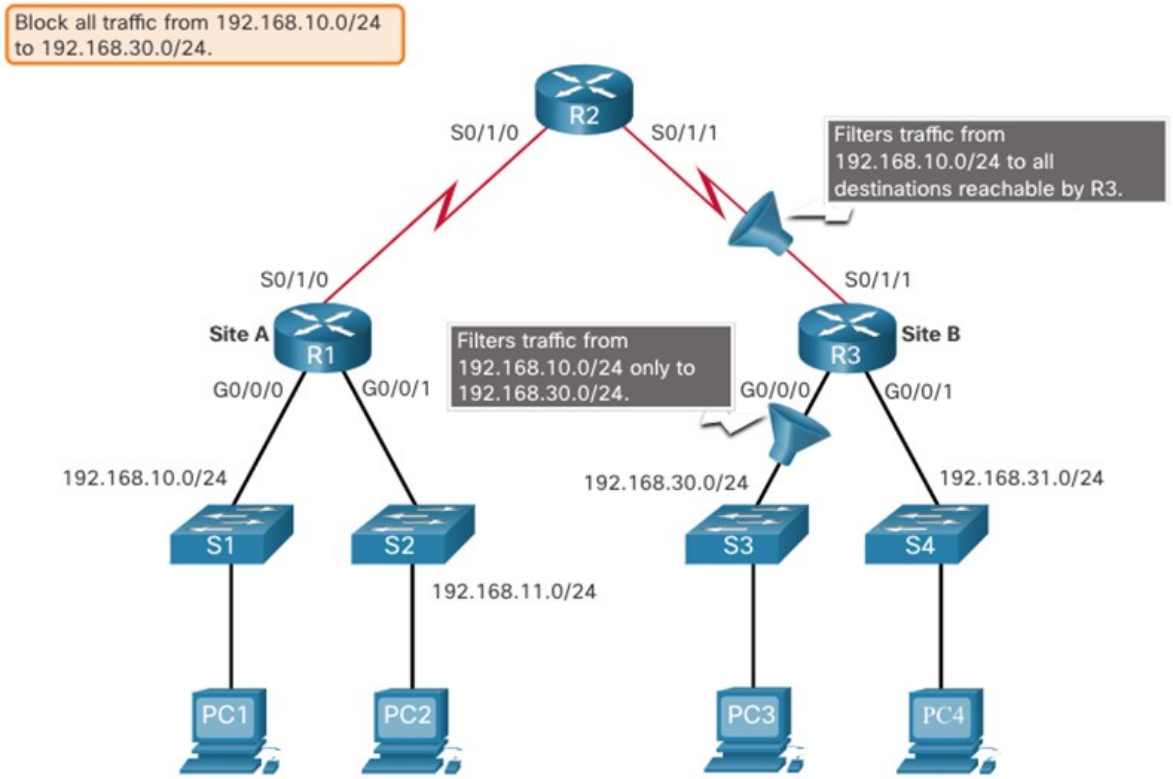
En suivant les instructions de placement de base, l'administrateur place une liste ACL standard sur le routeur R3.



# Exemple d'emplacement de liste de contrôle d'accès standard (Suite)

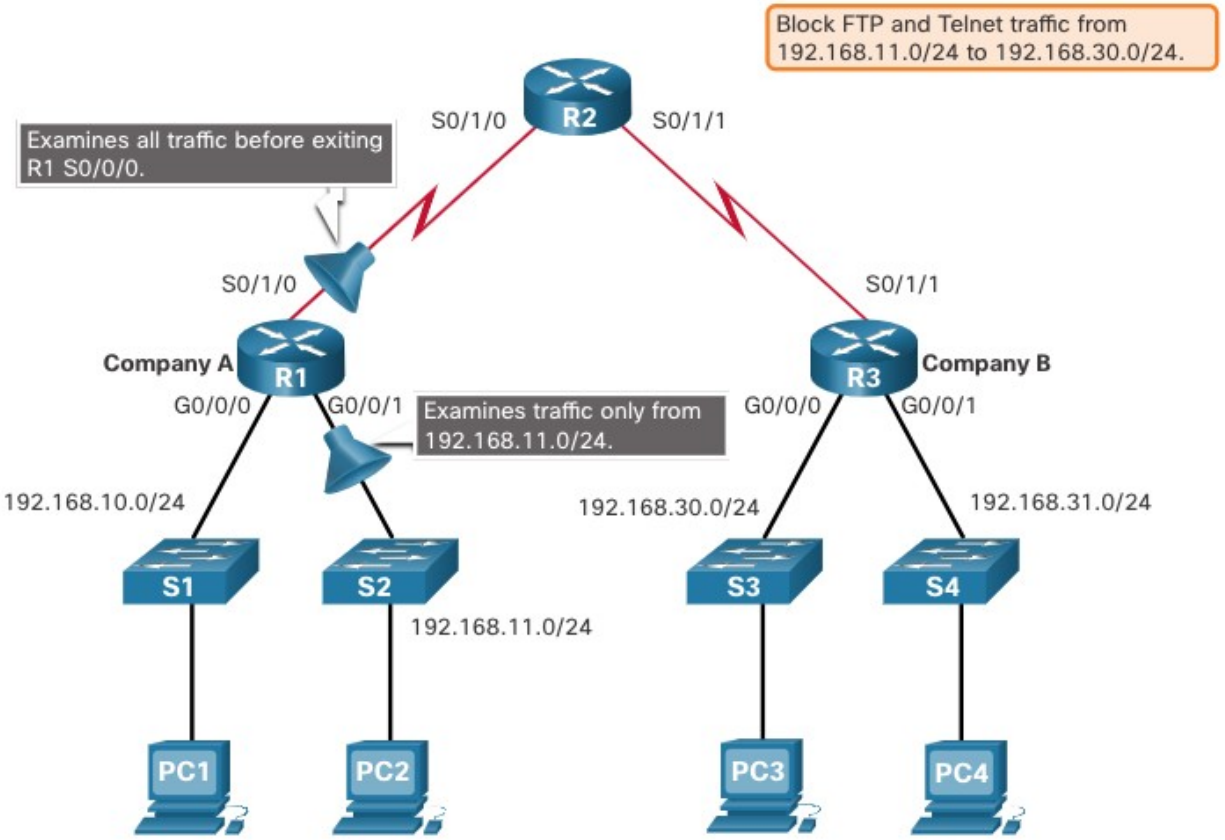
Il existe deux interfaces possibles sur R3 pour appliquer l'ACL standard:

- **Interface R3 S0/1/1 (entrante)** - L'ACL standard peut être appliquée entrante sur l'interface R3 S0/1/1 pour refuser le trafic à partir du réseau .10. Cependant, il filtre également le trafic .10 vers le réseau 192.168.31.0/24 (.31 dans cet exemple). Par conséquent, l'ACL standard ne doit pas être appliquée à cette interface.
- **Interface R3 G0/0 (sortante)** - L'ACL standard peut être appliquée sortante sur l'interface R3 G0/0/0. Cela n'affecte pas les autres réseaux accessibles par R3. Les paquets du réseau .10 pourront toujours atteindre le réseau .31. C'est la meilleure interface pour placer la liste ACL standard pour répondre aux exigences de trafic.



# Exemple d'emplacement d'une liste de contrôle d'accès étendue

- Les ACL étendus doivent être situés aussi près que possible de la source.
- Cependant, l'organisation ne peut placer des ACL que sur les appareils qu'elle contrôle. Par conséquent, cet emplacement doit être déterminé par la portée du contrôle dont dispose l'administrateur réseau.
- Dans la figure, par exemple, la société A veut refuser le trafic Telnet et FTP au réseau 192.168.30.0/24 de la société B à partir de son réseau 192.168.11.0/24 tout en autorisant tout autre trafic.



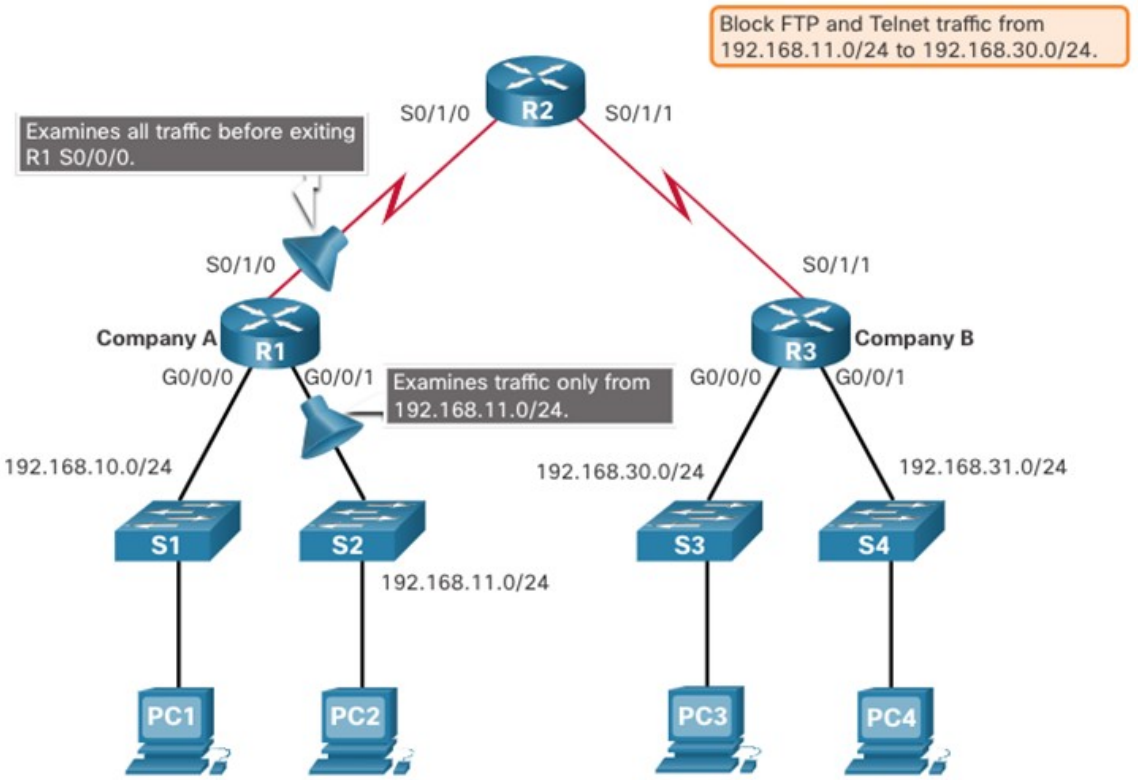
# Exemple d'emplacement d'une liste de contrôle d'accès étendue (Suite)

Un ACL étendu sur R3 permettrait d'accomplir la tâche, mais l'administrateur ne contrôle pas R3. En outre, cette solution autorise le passage du trafic indésirable sur l'ensemble du réseau avant de le bloquer lorsqu'il arrive à destination.

La solution consiste à placer une liste ACL étendue sur R1 qui spécifie à la fois les adresses source et de destination.

La figure illustre deux interfaces possibles sur R1 pour appliquer la liste de contrôle d'accès étendue:

- **interface R1 S0/1/0 (sortante)** - L'ACL étendue peut être appliquée sortante sur l'interface S0/1/0 Cette solution traitera tous les paquets quittant R1 y compris les paquets de 192.168.10.0/24.
- **Interface R1 G0/0/1 (entrante)** - L'ACL étendu peut être appliqué en entrée sur le G0/0/1 et seuls les paquets du réseau 192.168.11.0/24 sont soumis au traitement ACL sur R1 Puisque le filtre doit être limité aux seuls paquets quittant le réseau 192.168.11.0/24, l'application de la liste de contrôle d'accès étendue à G0/1 constitue la meilleure solution.



# Créer une ACL

Toutes les listes de contrôle d'accès (ACL) doivent être planifiées. Lors de la configuration d'une ACL complexe, il est suggéré de:

- Utiliser un éditeur de texte et écrire les spécificités de la stratégie à mettre en œuvre.
- Ajouter les commandes de configuration IOS pour accomplir ces tâches.
- Inclure des remarques pour documenter l'ACL.
- Copier et coller les commandes sur le périphérique.
- Tester toujours soigneusement une liste ACL pour vous assurer qu'elle applique correctement la stratégie souhaitée.

# Syntaxe des listes de contrôle d'accès IPv4 standard numérotées

Pour créer une liste ACL standard numérotée, utilisez la commande **access-list** .

```
Router(config)# access-list access-list-number {deny | permit | remark text} source [source-wildcard]
[log]
```

| Paramètre | Description |
|---|---|
| *access-list-number* | La plage de nombres est de 1 à 99 ou de 1300 à 1999 |
| **deny** | Refuse l'accès si les conditions sont respectées. |
| **permit** | Autorise l'accès si les conditions sont respectées. |
| **remark** *text* | (Facultatif) Ajoute une entrée de texte à des fins de documentation. |
| *Source* | Identifie l'adresse du réseau source ou de l'hôte à filtrer. |
| *source-wildcard* | (facultatif) Un masque générique de 32 bits qui est appliqué à la source |
| **log** | (Facultatif) Génère et envoie un message d'information lorsque l'ACE est apparié |

Remarque : Utilisez la commande de configuration globale **no access-list** *access-list-number* pour supprimer une ACL standard numérotée.

# Syntaxe des listes de contrôle d'accès IPv4 standard nommées

Pour créer une liste ACL standard numérotée, utilisez la commande **ip access-list standard** .

- Les noms des listes de contrôle d'accès doivent contenir uniquement des caractères alphanumériques, sont sensibles à la casse et doivent être uniques.
- Vous n'êtes pas obligés de mettre des majuscules aux noms des listes de contrôle d'accès. En revanche, si vous le faites, vous les verrez bien mieux en affichant la sortie de la commande running-config.

```
Router(config)# ip access-list standard access-list-name
```

```
R1(config)# ip access-list standard NO-ACCESS
R1(config-std-nacl)# ?
Standard Access List configuration commands:
  <1-2147483647>  Sequence Number
  default         Set a command to its defaults
  deny            Specify packets to reject
  exit            Exit from access-list configuration mode
  no              Negate a command or set its defaults
  permit          Specify packets to forward
  remark          Access list entry comment
R1(config-std-nacl)#
```

# Appliquer une listes de contrôle d'accès IPv4 standard numérotées

Une fois qu'une ACL IPv4 standard est configurée, elle doit être liée à une interface ou à une fonctionnalité.

- La commande **ip access-group** est utilisée pour lier une ACL IPv4 standard numérotée ou nommée à une interface.
- Pour supprimer une ACL d'une interface, entrez d'abord la commande de configuration de l'interface **no ip access-group**

```
Router(config-if) # ip access-group {access-list-number | access-list-name} {in | out}
```

# Exemple de liste de contrôle d’accès standard numérotées

L'exemple ACL autorise le trafic à partir de l'hôte 192.168.10.10 et de tous les hôtes sur l'interface de sortie réseau 192.168.20.0/24 série 0/1/0 sur le routeur R1.

```
R1(config)# access-list 10 remark ACE permits ONLY host 192.168.10.10 to the internet
R1(config)# access-list 10 permit host 192.168.10.10
R1(config)# do show access-lists
Standard IP access list 10
    10 permit 192.168.10.10
R1(config)#
```

```
R1(config)# access-list 10 remark ACE permits all host in LAN 2
R1(config)# access-list 10 permit 192.168.20.0 0.0.0.255
R1(config)# do show access-lists
Standard IP access list 10
    10 permit 192.168.10.10
    20 permit 192.168.20.0, wildcard bits 0.0.0.255
R1(config)#
```

```
R1(config)# interface Serial 0/1/0
R1(config-if)# ip access-group 10 out
R1(config-if)# end
R1#
```

# Exemple de liste de contrôle d’accès standard numérotées (Suite)

- Utilisez la commande **show running-config** pour consulter la configuration.
- Utilisez la commande **show ip interface** pour vérifier que l'ACL est appliquée à la bonne interface.

```
R1# show run | section access-list
access-list 10 remark ACE permits host 192.168.10.10
access-list 10 permit 192.168.10.10
access-list 10 remark ACE permits all host in LAN 2
access-list 10 permit 192.168.20.0 0.0.0.255
R1#
```

```
R1# show ip int Serial 0/1/0 | include access list
  Outgoing Common access list is not set
  Outgoing access list is 10
  Inbound Common access list is not set
  Inbound  access list is not set
R1#
```

# Exemple de liste de contrôle d’accès standard nommées

L'exemple ACL autorise le trafic à partir de l'hôte 192.168.10.10 et de tous les hôtes sur l'interface de sortie réseau 192.168.20.0/24 série 0/1/0 sur le routeur R1.

```
R1(config)# no access-list 10
R1(config)# ip access-list standard PERMIT-ACCESS
R1(config-std-nacl)# remark ACE permits host 192.168.10.10
R1(config-std-nacl)# permit host 192.168.10.10
R1(config-std-nacl)#
```

```
R1(config-std-nacl)# remark ACE permits host 192.168.10.10
R1(config-std-nacl)# permit host 192.168.10.10
R1(config-std-nacl)# remark ACE permits all hosts in LAN 2
R1(config-std-nacl)# permit 192.168.20.0 0.0.0.255
R1(config-std-nacl)# exit
R1(config)#
```

```
R1(config)# interface Serial 0/1/0
R1(config-if)# ip access-group PERMIT-ACCESS out
R1(config-if)# end
R1#
```

# Exemple de liste de contrôle d’accès standard nommées (Suite)

- Utilisez la commande **show access-list** pour consulter la configuration.
- Utilisez la commande **show ip interface** pour vérifier que l'ACL est appliquée à la bonne interface.

```
R1# show access-lists
Standard IP access list PERMIT-ACCESS
    10 permit 192.168.10.10
    20 permit 192.168.20.0, wildcard bits 0.0.0.255
R1# show run | section ip access-list
ip access-list standard PERMIT-ACCESS
 remark ACE permits host 192.168.10.10
 permit 192.168.10.10
 remark ACE permits all hosts in LAN 2
 permit 192.168.20.0 0.0.0.255
R1#
```

```
R1# show ip int Serial 0/1/0 | include access list
  Outgoing Common access list is not set
  Outgoing access list is PERMIT-ACCESS
  Inbound Common access list is not set
  Inbound  access list is not set
R1#
```

# Deux méthodes pour modifier une ACL

Une fois qu'une liste ACL est configurée, il peut être nécessaire de la modifier. Les ACL avec plusieurs ACE peuvent être complexes à configurer. Parfois, l'ACE configuré ne donne pas les comportements attendus.

Il existe deux méthodes à utiliser pour modifier une liste ACL:

- Utiliser un éditeur de texte
- Utiliser les numéros de séquence

# Méthode éditeur de texte

Les ACL avec plusieurs ACE doivent être créées dans un éditeur de texte. Cela vous permet de planifier les ACE nécessaires, de créer l'ACL, puis de le coller sur l'interface du routeur. Il simplifie également les tâches de modification et de correction d'une ACL.

Pour corriger une erreur dans une liste ACL:

- Copiez l'ACL à partir de la configuration en cours d'exécution et collez-la dans l'éditeur de texte.
- Effectuez les modifications nécessaires.
- Supprimez la liste ACL configurée précédemment sur le routeur.
- Copiez et collez la liste ACL modifiée sur le routeur.

```
R1# show run | section access-list
access-list 1 deny   19.168.10.10
access-list 1 permit 192.168.10.0 0.0.0.255
R1#
```

```
R1(config)# no access-list 1
R1(config)#
R1(config)# access-list 1 deny 192.168.10.10
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)#
```

# Méthode numéros de séquence

Un ACE ACL peut être supprimé ou ajouté à l'aide des numéros de séquence ACL.

- Utilisez la commande **ip access-list standard** pour modifier une ACL.
- Les instructions ne peuvent pas être remplacées par des instructions associées à un numéro de séquence existant déjà. l'instruction actuelle doit être supprimée d'abord avec la commande **no 10** . Ensuite, le bon ACE peut être ajouté en utilisant le numéro de séquence.

```
R1# show access-lists
Standard IP access list 1
    10 deny   19.168.10.10
    20 permit 192.168.10.0, wildcard bits 0.0.0.255
R1#
```

```
R1# conf t
R1(config)# ip access-list standard 1
R1(config-std-nacl)# no 10
R1(config-std-nacl)# 10 deny host 192.168.10.10
R1(config-std-nacl)# end
R1# show access-lists
Standard IP access list 1
    10 deny   192.168.10.10
    20 permit 192.168.10.0, wildcard bits 0.0.0.255
R1#
```

# Modifier une ACL nommée Exemple

Les ACL nommées peuvent également utiliser des numéros de séquence pour supprimer et ajouter des ACE. Dans l'exemple, un ACE est ajouté pour refuser les hôtes 192.168.10.11.

```
R1# show access-lists
Standard IP access list NO-ACCESS
    10 deny   192.168.10.10
    20 permit 192.168.10.0, wildcard bits 0.0.0.255
```

```
R1# configure terminal
R1(config)# ip access-list standard NO-ACCESS
R1(config-std-nacl)# 15 deny 192.168.10.5
R1(config-std-nacl)# end
R1#
R1# show access-lists
Standard IP access list NO-ACCESS
    15 deny   192.168.10.5
    10 deny   192.168.10.10
    20 permit 192.168.10.0, wildcard bits 0.0.0.255
R1#
```

# Statistiques des listes de contrôle d'accès

La commande **show access-lists** de l'exemple affiche des statistiques pour chaque instruction qui a été mise en correspondance.

- L'ACE de refus a été apparié 20 fois et le permis ACE a été apparié 64 fois.
- Notez que le refus implicite d'une instruction n'affiche aucune statistique. Pour suivre le nombre de paquets refusés implicitement appariés, vous devez configurer manuellement la commande **deny any** .
- Utilisez la commande **clear access-list counters** pour effacer les statistiques ACL.

```
R1# show access-lists
Standard IP access list NO-ACCESS
    10 deny   192.168.10.10  (20 matches)
    20 permit 192.168.10.0, wildcard bits 0.0.0.255  (64 matches)
R1# clear access-list counters NO-ACCESS
R1# show access-lists
Standard IP access list NO-ACCESS
    10 deny   192.168.10.10
    20 permit 192.168.10.0, wildcard bits 0.0.0.255
R1#
```

# La commande access-class

Une liste ACL standard peut sécuriser l'accès administratif à distance à un périphérique à l'aide des lignes vty en implémentant les deux étapes suivantes:

- Créez une liste ACL pour identifier les hôtes administratifs qui doivent être autorisés à accéder à distance.
- Appliquez l'ACL au trafic entrant sur les lignes vty.

```
R1(config-line)# access-class {access-list-number | access-list-name} { in | out }
```

# Exemple d'accès sécurisé aux VTY

Cet exemple montre comment configurer une liste ACL pour filtrer le trafic vty.

- Tout d'abord, une entrée de base de données locale pour une utilisateur **ADMIN** et mot de passe **class** est configurée.
- Les lignes vty sur R1 sont configurées pour utiliser la base de données locale pour l'authentification, autoriser le trafic SSH (?) et utiliser l'ACL ADMIN-HOST pour restreindre le trafic.

```
R1(config)# username ADMIN secret class
R1(config)# ip access-list standard ADMIN-HOST
R1(config-std-nacl)# remark This ACL secures incoming vty lines
R1(config-std-nacl)# permit 192.168.10.10
R1(config-std-nacl)# deny any
R1(config-std-nacl)# exit
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input telnet
R1(config-line)# access-class ADMIN-HOST in
R1(config-line)# end
R1#
```

# Vérifier la sécurité du port VTY

Une fois que la liste de contrôle d'accès aux lignes VTY est configurée, il est important de vérifier qu'elle fonctionne correctement.

Pour vérifier les statistiques ACL, exécutez la commande **show access-lists** .

- La correspondance dans la ligne d'autorisation de la sortie est le résultat d'une connexion SSH réussie par l'hôte avec l'adresse IP 192.168.10.10.
- La correspondance à l'instruction «deny» est due à l'échec de la de la tentative de créer une connexion SSH à partir d'un appareil sur un autre réseau.

```
R1#
Oct  9 15:11:19.544: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admin] [Source: 192.168.10.10]
[localport: 23] at 15:11:19 UTC Wed Oct 9 2019
R1# show access-lists
Standard IP access list ADMIN-HOST
    10 permit 192.168.10.10  (2 matches)
    20 deny   any  (2 matches)
R1#
```

# Les ACL étendues

Les ACL étendues offrent un plus grand degré de contrôle. Ils peuvent filtrer sur l'adresse source, l'adresse de destination, le protocole (c'est-à-dire IP, TCP, UDP, ICMP) et le numéro de port.

Les ACL étendues peuvent être créées comme suit:

- **ACL étendu numérotée** - Créé à l'aide de la commande de configuration globale **access-list** *access-list-number* .
- **ACL étendu nommée** - Créé à l'aide de la commande **ip access-list extended** *access-list-name* .

# Protocoles et ports

Les ACL étendues peuvent filtrer sur protocoles et ports d'internet. Utiliser le **?** pour obtenir de l'aide lors de la saisie d'un ACE complexe . Les quatre protocoles mis en évidence sont les options les plus populaires.

## Options de protocole

```
R1(config)# access-list 100 permit ?
  <0-255>        An IP protocol number
  ahp            Authentication Header Protocol
  dvmrp          dvmrp
  eigrp          Cisco's EIGRP routing protocol
  esp            Encapsulation Security Payload
  gre            Cisco's GRE tunneling
  icmp           Internet Control Message Protocol
  igmp           Internet Gateway Message Protocol
  ip             Any Internet Protocol
  ipinip         IP in IP tunneling
  nos            KA9Q NOS compatible IP over IP tunneling
  object-group   Service object group
  ospf           OSPF routing protocol
  pcp            Payload Compression Protocol
  pim            Protocol Independent Multicast
  tcp            Transmission Control Protocol
  udp            User Datagram Protocol
R1(config)# access-list 100 permit
```

# Protocoles et ports (Suite)

La sélection d'un protocole influence les options de port. De nombreuses options de port TCP sont disponibles, comme indiqué dans la sortie.

```
R1(config)# access-list 100 permit tcp any any eq ?
  <0-65535>     Port number
  bgp           Border Gateway Protocol (179)
  chargen       Character generator (19)
  cmd           Remote commands (rcmd, 514)
  daytime       Daytime (13)
  discard       Discard (9)
  domain        Domain Name Service (53)
  echo          Echo (7)
  exec          Exec (rsh, 512)
  finger        Finger (79)
  ftp           File Transfer Protocol (21)
  ftp-data      FTP data connections (20)
  gopher        Gopher (70)
  hostname      NIC hostname server (101)
  ident         Ident Protocol (113)
  irc           Internet Relay Chat (194)
  klogin        Kerberos login (543)
  kshell        Kerberos shell (544)
  login         Login (rlogin, 513)
  lpd           Printer service (515)
  msrpc         MS Remote Procedure Call (135)
  nntp          Network News Transport Protocol (119)
  onep-plain    Onep Cleartext (15001)
  onep-tls      Onep TLS (15002)
  pim-auto-rp   PIM Auto-RP (496)
  pop2          Post Office Protocol v2 (109)
  pop3          Post Office Protocol v3 (110)
  smtp          Simple Mail Transport Protocol (25)
  sunrpc        Sun Remote Procedure Call (111)
  syslog        Syslog (514)
  tacacs        TAC Access Control System (49)
  talk          Talk (517)
  telnet        Telnet (23)
  time          Time (37)
  uucp          Unix-to-Unix Copy Program (540)
  whois         Nicname (43)
  www           World Wide Web (HTTP, 80)
```

# Exemples de configuration de protocoles et de numéros de ports (Suite)

Les ACL étendues peuvent filtrer sur différentes options de numéro de port et de nom de port.

Cet exemple montre comment configurer une ACL 100 étendue pour filtrer le trafic HTTP. Le premier ACE utilise le nom de port **www** . Le deuxième ACE utilise le numéro de port **80**. Les deux ACE obtiennent exactement le même résultat.

```
R1(config)# access-list 100 permit tcp any any eq www
!or...
R1(config)# access-list 100 permit tcp any any eq 80
```

La configuration du numéro de port est requise lorsqu'aucun nom de protocole spécifique n'est répertorié tel que SSH (numéro de port 22) ou HTTPS (numéro de port 443), comme indiqué dans l'exemple suivant.

```
R1(config)# access-list 100 permit tcp any any eq 22
R1(config)# access-list 100 permit tcp any any eq 443
R1(config)#
```

# Appliquer une ACL IPv4 étendue numérotée

Dans cet exemple, l'ACL permet à la fois le trafic HTTP et HTTPS à partir du réseau 192.168.10.0 d'accéder à n'importe quelle destination.

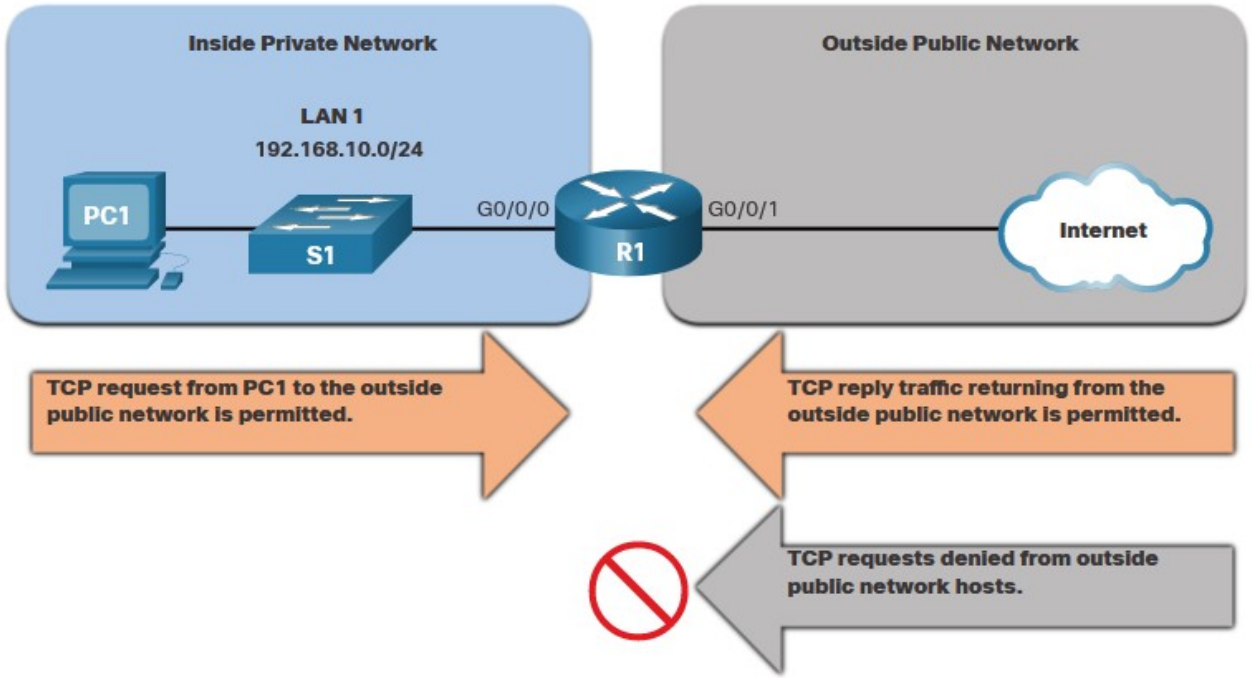
Les ACL étendues peuvent être appliquées à différents endroits. Cependant, elles sont couramment appliquées près de la source. Ici ACL 110 est appliquée en entrant sur l'interface R1 G0/0/0.

```
R1(config)# access-list 110 permit tcp 192.168.10.0 0.0.0.255 any eq www
R1(config)# access-list 110 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config)# interface g0/0/0
R1(config-if)# ip access-group 110 in
R1(config-if)# exit
R1(config)#
```

# ACL étendue établie par TCP

TCP peut également effectuer des services de pare-feu avec état de base à l'aide du mot-clé TCP **established** .

- Le mot-clé **established** permet au trafic intérieur de quitter le réseau privé intérieur et permet au trafic de réponse de retourner d'entrer dans le réseau privé intérieur.
- Le trafic TCP généré par un hôte externe et la tentative de communication avec un hôte interne est refusé.



# ACL étendue établie par TCP (Suite)

- ACL 120 est configurée pour autoriser uniquement le retour du trafic Web vers les hôtes internes. L'ACL est ensuite appliquée sortante sur l'interface R1 G0/0/0.
- La commande **show access-lists** indique que les hôtes internes accèdent aux ressources Web sécurisées à partir d'Internet.

**Remarque**: Il y a concordance si les bits ACK ou RST (réinitialisation) du segment TCP de retour sont définis, indiquant que le paquet appartient à une connexion existante.

```
R1(config)# access-list 120 permit tcp any 192.168.10.0 0.0.0.255 established
R1(config)# interface g0/0/0
R1(config-if)# ip access-group 120 out
R1(config-if)# end
R1# show access-lists
Extended IP access list 110
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443 (657 matches)
Extended IP access list 120
    10 permit tcp any 192.168.10.0 0.0.0.255 established (1166 matches)
R1#
```

# Syntaxe ACL étendue IPv4 nommée

Si vous attribuez un nom à une liste de contrôle d'accès, il vous sera plus facile d'en comprendre la fonction. Pour créer une liste ACL étendue nommée, utilisez la commande de configuration **ip access-list extended** .

Dans l'exemple, une liste ACL étendue nommée NO-FTP-ACCESS est créée et l'invite est modifiée en mode de configuration ACL étendue nommée. Les instructions ACE sont entrées dans le mode de sous-configuration ACL étendu nommé.

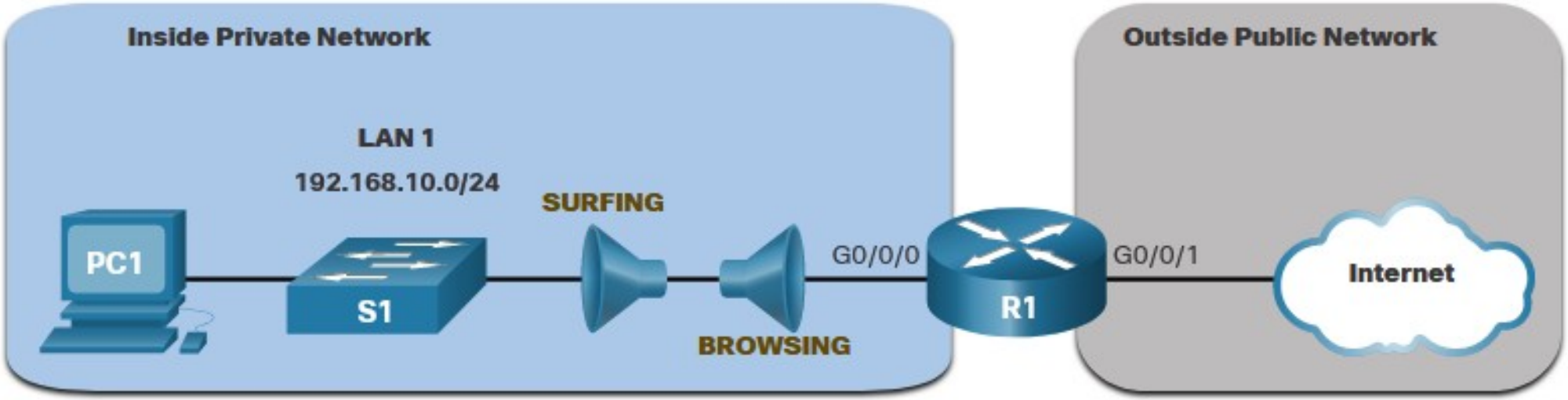
```
Router(config)# ip access-list extended access-list-name
```

```
R1(config)# ip access-list extended NO-FTP-ACCESS
R1(config-ext-nacl)#
```

# Exemple d'ACL étendue IPv4 nommée

La topologie ci-dessous permet de démontrer la configuration et l'application de deux ACL étendues IPv4 nommées à une interface:

- SURFING - Cela permettra à l'intérieur du trafic HTTP et HTTPS de quitter l'internet.
- **BROWSING** - Cela permettra uniquement de renvoyer le trafic Web aux hôtes internes alors que tout autre trafic sortant de l'interface R1 G0/0/0 est implicitement refusé.



# Exemple de liste ACL étendue IPv4 nommée (Suite)

- L'ACL SURFING permet au trafic HTTP et HTTPS des utilisateurs internes de quitter l'interface G0/0/1 connectée à l'internet. Le trafic Web revenant de l'internet est autorisé à revenir sur le réseau privé interne par l'ACL BROWSING.
- La liste ACL SURVING est appliquée entrante et la liste ACL BROWSING est appliquée sortante sur l'interface R1 G0/0/0.

```
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# Remark Permits inside HTTP and HTTPS traffic
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config-ext-nacl)# exit
R1(config)#
R1(config)# ip access-list extended BROWSING
R1(config-ext-nacl)# Remark Only permit returning HTTP and HTTPS traffic
R1(config-ext-nacl)# permit tcp any 192.168.10.0 0.0.0.255 established
R1(config-ext-nacl)# exit
R1(config)# interface g0/0/0
R1(config-if)# ip access-group SURFING in
R1(config-if)# ip access-group BROWSING out
R1(config-if)# end
R1# show access-lists
Extended IP access list SURFING
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443 (124 matches)
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established (369 matches)
R1#
```

# Exemple de liste ACL étendue IPv4 nommée (Suite)

**Pour vérifier les statistiques ACL, exécutez la commande show access-lists .**

```
R1# show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 19.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1#
```

# Modifier les ACL étendues

Une liste ACL étendue peut être modifiée à l'aide d'un éditeur de texte lorsque de nombreuses modifications sont nécessaires. Ou, si l'édition s'applique à un ou deux ACE, les numéros de séquence peuvent être utilisés.

**Exemple:**

- Le numéro de séquence ACE 10 dans l'ACL SURFING a une adresse de réseau IP source incorrecte.

```
R1# show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 19.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1#
```

# Modifier les ACL étendues (Suite)

- Pour corriger cette erreur, l'instruction d'origine est supprimée avec la commande **no** *sequence_#* et l'instruction corrigée est ajoutée en remplacement de l'instruction d'origine.
- La sortie de la commande **show access-lists** vérifie le changement de configuration.

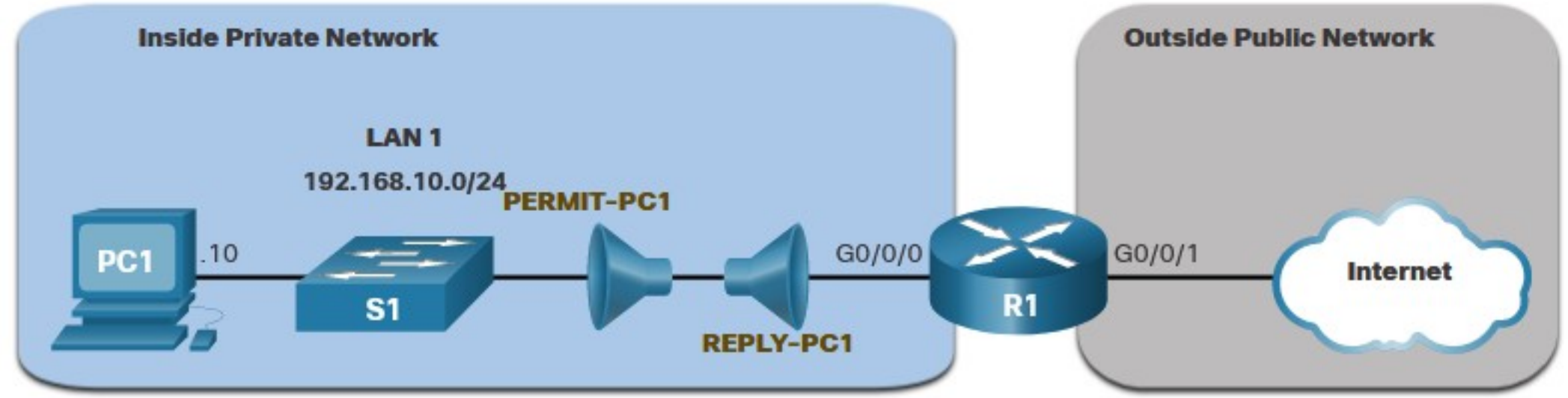
```
R1# configure terminal
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# no 10
R1(config-ext-nacl)# 10 permit tcp 192.168.10.0 0.0.0.255 any eq www
R1(config-ext-nacl)# end
```

```
R1# show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1#
```

# Autre exemple d'ACL étendue IPv4 nommée

Deux ACL étendues nommées seront créées:

- **PERMIT-PC1** - Cela permettra uniquement l'accès PC1 TCP à l'internet et refusera tous les autres hôtes du réseau privé.
- **REPLY-PC1** - Cela permettra uniquement le retour du trafic TCP spécifié à PC1 refuser implicitement tout autre trafic.



# Autre exemple d'ACL étendue IPv4 nommée (Suite)

- L'ACL **PERMIT-PC1** autorise PC1 (192.168.10.10) l'accès TCP au trafic FTP, SSH, Telnet, DNS, HTTP et HTTPS.
- La liste ACL **REPLY-PC1** permettra le retour du trafic vers PC1.
- La liste ACL **PERMIT-PC1** est appliquée en entrée et la liste ACL **REPLY-PC1** est appliquée en sortie sur l'interface R1 G0/0/0.

```
R1(config)# ip access-list extended PERMIT-PC1
R1(config-ext-nacl)# Remark Permit PC1 TCP access to internet
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 20
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 21
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 22
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 23
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 53
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 80
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 443
R1(config-ext-nacl)# deny ip 192.168.10.0 0.0.0.255 any
R1(config-ext-nacl)# exit
R1(config)#
R1(config)# ip access-list extended REPLY-PC1
R1(config-ext-nacl)# Remark Only permit returning traffic to PC1
R1(config-ext-nacl)# permit tcp any host 192.168.10.10 established
R1(config-ext-nacl)# exit
R1(config)# interface g0/0/0
R1(config-if)# ip access-group PERMIT-PC1 in
R1(config-if)# ip access-group REPLY-PC1 out
R1(config-if)# end
R1#
```

# Vérifier les listes de contrôle d'accès étendues

La commande **show ip interface** permet de vérifier la liste de contrôle d'accès sur l'interface et la direction dans laquelle elle a été appliquée.

```
R1# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up (connected)
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is REPLY-PC1
  Inbound  access list is PERMIT-PC1
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
R1#
R1# show ip interface g0/0/0 | include access list
Outgoing access list is REPLY-PC1
Inbound access list is PERMIT-PC1
R1#
```

# Vérifier les listes de contrôle d'accès étendues (Suite)

La commande **show access-lists** peut être utilisée pour confirmer que les ACL fonctionnent comme prévu. La commande affiche les compteurs statistiques qui augmentent chaque fois qu'un ACE est apparié.

**Remarque** : Le trafic doit être généré pour vérifier le fonctionnement de l'ACL.

```
R1# show access-lists
Extended IP access list PERMIT-PC1
10 permit tcp host 192.168.10.10 any eq 20
20 permit tcp host 192.168.10.10 any eq ftp
30 permit tcp host 192.168.10.10 any eq 22
40 permit tcp host 192.168.10.10 any eq telnet
50 permit tcp host 192.168.10.10 any eq domain
60 permit tcp host 192.168.10.10 any eq www
70 permit tcp host 192.168.10.10 any eq 443
80 deny ip 192.168.10.0 0.0.0.255 any
Extended IP access list REPLY-PC1
10 permit tcp any host 192.168.10.10 established
R1#
```

# Vérifier les listes de contrôle d'accès étendues (Suite)

La commande **show running-config** peut être utilisée pour valider ce qui a été configuré. La commande affiche également les remarques configurées.

```
R1# show running-config | begin ip access-list
ip access-list extended PERMIT-PC1
remark Permit PC1 TCP access to internet
permit tcp host 192.168.10.10 any eq 20
permit tcp host 192.168.10.10 any eq ftp
permit tcp host 192.168.10.10 any eq 22
permit tcp host 192.168.10.10 any eq telnet
permit tcp host 192.168.10.10 any eq domain
permit tcp host 192.168.10.10 any eq www
permit tcp host 192.168.10.10 any eq 443
deny ip 192.168.10.0 0.0.0.255 any
ip access-list extended REPLY-PC1
remark Only permit returning traffic to PC1
permit tcp any host 192.168.10.10 established
!
```