ACTIVITE 5.2
Configurer des ACL étendues

Pour renforcer la sécurité de votre réseau, vous allez configurer des ACL étendues numérotées ou nommées.

1 – Configurer une ACL numérotée étendue

Utilisez le fichier "Act 5.2 - Configurer des ACL étendues.pkt" pour la suite de l'activité.

Votre mission

Vous devez créer une liste ACL étendue nommée respectant la politique de sécurité réseau de l'entreprise :

- Bloquez l'accès HTTP et HTTPS de PC1 à Server1 et Server2. Les serveurs sont dans le cloud et vous êtes la seule personne qui connaît leur adresse IP.
- Bloquez l'accès FTP de PC2 à Server1 et Server2.
- Bloquez l'accès ICMP de PC3 à Server1 et Server2.

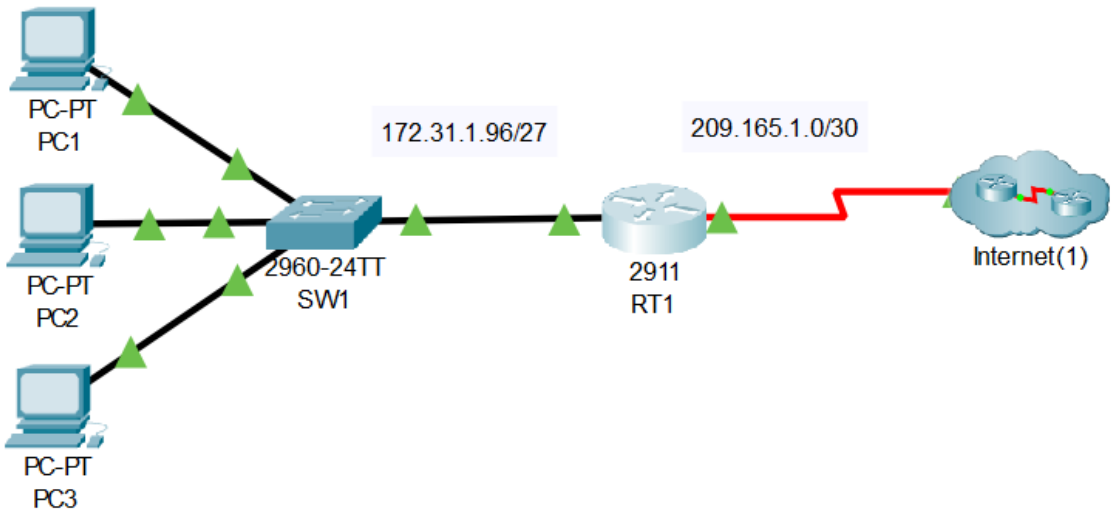

Table de routage

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
RT1	G0/0	172.31.1.126	255.255.255.224	S/O
RT1	S0/0/0	209.165.1.2	255.255.255.252	S/O
PC1	Carte réseau (NIC)	172.31.1.101	255.255.255.224	172.31.1.126
PC2	Carte réseau (NIC)	172.31.1.102	255.255.255.224	172.31.1.126
PC3	Carte réseau (NIC)	172.31.1.103	255.255.255.224	172.31.1.126
Serveur 1	Carte réseau (NIC)			
Serveur 2	Carte réseau (NIC)			

☞ 0 – Retrouvez les adresses IP, les masques de sous réseau et les passerelles des serveur 1 et 2. Cliquez sur "internet" pour accéder aux serveurs et touche pour revenir en arrière. Complétez la table de routage.

Refuser à PC1 l'accès aux services HTTP et HTTPS sur le serveur 1 et le serveur 2

☞ 1 – Créez une liste de contrôle d'accès IP nommée qui empêchera **PC1** d'accéder aux services HTTP et HTTPS de Serveur 1 et Serveur 2. Quatre instructions de contrôle d'accès sont requises.

Etape 1 : Nommez votre ACL "**RT1_ACL**".

Commande :

✍ 2 – Commencez la configuration de la liste de contrôle d'accès par une déclaration qui refuse l'accès de PC1 à Serveur 1, uniquement pour HTTP (port 80). Reportez-vous au tableau d'adressage pour connaître l'adresse IP de PC1 et de Serveur 1.

Commande :

✍ 3 – Ecrivez l'instruction qui refuse l'accès de **PC1** à Serveur 1, uniquement pour HTTPS (port 443). Elle ressemble fortement à celle de la question 2.

Commande :

✍ 4 – Ecrivez l'instruction qui refuse l'accès de **PC1** à Serveur 2, uniquement pour HTTP (port 80).

Commande :

✍ 5 – Ecrivez l'instruction qui refuse l'accès de **PC1** à Serveur 2, uniquement pour HTTPS (port 443).

Commande :

Refuser à PC2 l'accès aux services FTP sur Server1 et Server2

✍ 6 – Quels sont les deux ports utilisés par le protocole FTP. A quoi servent-ils ?

✍ 7 – Ecrivez l'instruction qui refuse l'accès de **PC2** à Serveur 1, uniquement pour FTP (port 21 uniquement).

Commande :

✍ 8 – Ecrivez l'instruction qui refuse l'accès de **PC2** à Serveur 2, uniquement pour FTP (port 21 uniquement).

Commande :

✍ 9 – Pourquoi bloque-t-on que le port 21 ?

Interdire au PC3 d'envoyer un ping à Serveur 1 et Serveur 2.

✍ 10 – Ecrivez l'instruction qui refuse l'accès ICMP de **PC3** à Serveur 1.
Commande :

✍ 11 – Ecrivez l'instruction qui refuse l'accès ICMP de **PC3** à Serveur 2.
Commande :

✍12 – Par défaut, une liste d'accès refuse tout trafic qui ne correspond à aucune règle de la liste. On souhaite éviter cette règle donc on va autoriser tout le trafic qui ne correspond à aucune des instructions de liste d'accès configurées … en clair : on autorise tous les autres cas non traités dans les huit règles précédentes.

Commande :

✍13 – Exécutez la commande **show access-list** et vérifiez qu'il n'y a pas d'erreurs typographiques et que les déclarations sont dans le bon ordre.
Commande :

Réponse routeur :

2 - Appliquer et vérifier la liste de contrôle d'accès étendue

Le trafic à filtrer vient du réseau 172.31.1.96 /27 et est destiné à des réseaux distants. Le placement approprié des ACL dépend de la relation du trafic par rapport à RT1. En général, les listes d'accès étendues doivent être placées sur l'interface la plus proche de la source du trafic.

✍14 – Sur quelle interface l'ACL nommée doit-elle être appliquée et dans quelle direction ?

✍15 – Passez en mode de configuration d'interface et appliquez la liste de contrôle d'accès.
Commande :

Testez l'ensemble des règles pour l'interface G0/0 du routeur RT1.

✍16 – Accédez aux sites Web de Serveur 1et Serveur 2 à l'aide du navigateur Web de PC1, PC2 et PC3. Utilisez à la fois les protocoles HTTP et HTTPS. Utilisez la commande show access-lists pour voir quelle liste d'accès a autorisé ou refusé le trafic.

Remarque : Pour effacer les compteurs d'une liste d'accès, utilisez la commande **clear access-list counters** .

Accès	PC1	PC2	PC3	Fonctionnement correct
Serveur 1 HTTP - HTTPS				
Serveur 2 HTTP - HTTPS				

✍17 – Depuis PC1, PC2 et PC3, testez l'accès FTP de Serveur1 et Serveur 2 : à partir de l'application "**command promt**", tapez **ftp + adresse IP du serveur.** Le nom d'utilisateur et le mot de passe sont tous deux **cisco**.

Accès	PC1	PC2	PC3	Fonctionnement correct
Serveur 1 FTP				
Serveur 2 FTP				

✍18 – Ping de PC1, PC2, PC3 vers les serveurs 1 et 2 pour vérifier le bon fonctionnement de la liste d'accès.

Accès	PC1	PC2	PC3	Fonctionnement correct
Ping vers Serveur 1 ICMP				
Ping vers Serveur 2 ICMP				