TP7 Configurer et vérifier les listes de contrôle d'accès IPv4 étendues

Topologie

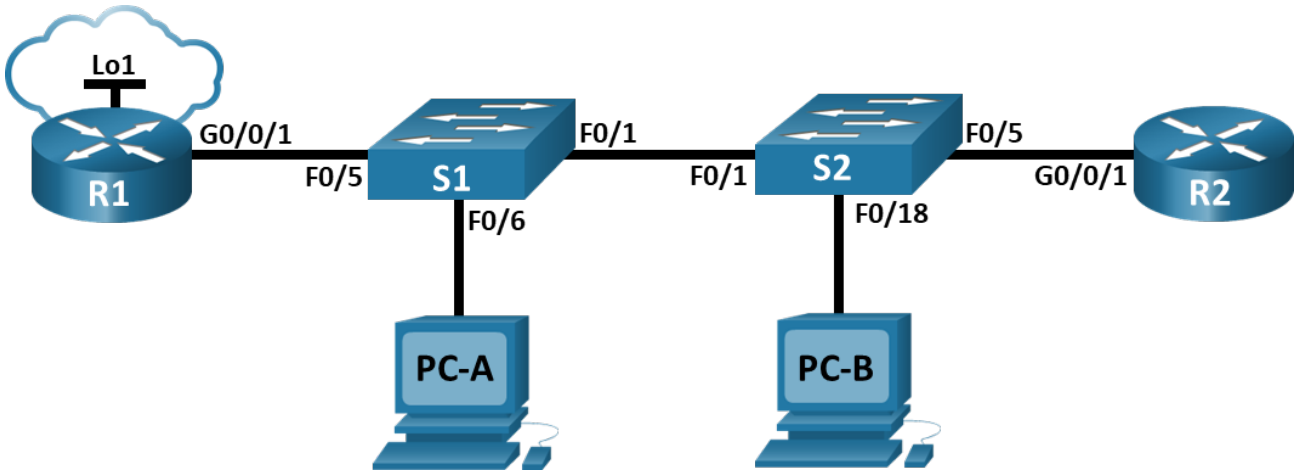

Table d'adressage

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/0/1	S/O	S/O	S/O
	G0/0/1.20	10.20.0.1	255.255.255.0	
	G0/0/1.30	10.30.0.1	255.255.255.0	
	G0/0/1.40	10.40.0.1	255.255.255.0	
	G0/0/1.1000	S/O	S/O	
	Loopback1	172.16.1.1	255.255.255.0	
R2	G0/0/1	10.20.0.4	255.255.255.0	S/O
S1	VLAN 20	10.20.0.2	255.255.255.0	10.20.0.1
S2	VLAN 20	10.20.0.3	255.255.255.0	10.20.0.1
PC-A	Carte réseau	10.30.0.10	255.255.255.0	10.30.0.1
PC-B	Carte réseau	10.40.0.10	255.255.255.0	10.40.0.1

Table de VLAN

VLAN	Nom	Interface attribuée
20	Gestion	S2: F0/5
30	Opérations	S1: F0/6
40	Ventes	S2: F0/18
999	ParkingLot	S1: F0/2-4, F0/7-24, G0/1-2 S2: F0/2-4, F0/6-17, F0/19-24, G0/1-2
1000	Natif	S/O

Objectifs

Partie 1: créer un réseau et configurer les paramètres de base des périphériques

Partie 2: Configurer et vérifier les listes de contrôle d'accès étendu

Contexte/scénario

Vous avez été chargé de configurer les listes de contrôle d'accès sur le réseau de petites entreprises. Les ACL sont l'un des moyens les plus simples et les plus directs pour contrôler le trafic de couche 3. R1 accueillera une connexion internet (simulée par l'interface de bouclage 1) et partagera les informations de route par défaut avec R2. Une fois la configuration initiale est terminée, l'entreprise a certaines exigences spécifiques en matière de sécurité du trafic que vous êtes responsable de mettre en œuvre.

Remarque: Les routeurs utilisés lors des travaux pratiques CCNA sont des routeurs Cisco 4221 équipés de Cisco IOS version 16.9.4 (universalk9 image). Les commutateurs utilisés dans les travaux pratiques sont des modèles Cisco Catalyst 2960s équipé de version 15.2.2 de Cisco IOS (image lanbasek9). D'autres routeurs, commutateurs et versions de Cisco IOS peuvent être utilisés. Selon le modèle et la version de Cisco IOS, les commandes disponibles et le résultat produit peuvent varier de ce qui est indiqué dans les travaux pratiques. Reportez-vous au tableau récapitulatif de l'interface du routeur à la fin de ces travaux pratiques pour obtenir les identifiants d'interface corrects.

Remarque: Assurez-vous que les routeurs et les commutateurs ont été réinitialisés et ne possèdent aucune configuration initiale. En cas de doute, contactez votre formateur.

Ressources requises

- … Sous Packet Tracer

Instructions

Partie 1: Créer le réseau et configurer les paramètres de base des périphériques

Étape 1: Câblez le réseau conformément à la topologie indiquée.

Connectez les équipements représentés dans le schéma de topologie et effectuez le câblage nécessaire.

Étape 2: Configurez les paramètres de base pour chaque routeur.

a. Attribuez un nom de l'appareil au routeur.

b. Désactivez la recherche DNS pour empêcher le routeur d'essayer de traduire les commandes saisies comme s'il s'agissait de noms d'hôtes.

c. Attribuez **class** comme mot de passe chiffré d'exécution privilégié.

d. Attribuez **cisco** comme mot de passe de console et activez la connexion.

e. Attribuez **cisco** comme mot de passe VTY et activez la connexion.

f. Cryptez les mots de passe en texte clair.

g. Créez une bannière qui avertit quiconque accède au périphérique que tout accès non autorisé est interdit.

h. Enregistrez la configuration en cours dans le fichier de configuration initiale.

Étape 3: Configurez les paramètres de base pour chaque commutateur.

a. Attribuez un nom de périphérique au commutateur.

b. Désactivez la recherche DNS pour empêcher le routeur d'essayer de traduire les commandes saisies comme s'il s'agissait de noms d'hôtes.

c. Attribuez **class** comme mot de passe chiffré d'exécution privilégié.

d. Attribuez **cisco** comme mot de passe de console et activez la connexion.

e. Attribuez **cisco** comme mot de passe VTY et activez la connexion.

f. Cryptez les mots de passe en texte clair.

g. Créez une bannière qui avertit quiconque accède à l'appareil que tout accès non autorisé est interdit.

h. Enregistrez la configuration en cours dans le fichier de configuration initiale.

Partie 2: Configurer les VLAN sur les commutateures.

Étape 1: Créez les VLAN sur les commutateurs.

a. Créez et nommez les VLANs requis sur chaque commutateur à partir du tableau ci-dessus.

b. Configurez et activez l'interface de gestion et la passerelle par défaut sur chaque commutateur en utilisant les informations relatives à l'adresse IP dans la table d'adressage.

c. Affectez tous les ports inutilisés du commutateur au VLAN du Parking Lot, configurez-les pour le mode d'accès statique et désactivez-les administrativement.

Remarque: La commande interface range est utile pour accomplir cette tâche avec autant de commandes que nécessaire.

Étape 2: Attribuez les VLAN aux interfaces de commutateur correctes.

a. Attribuez les ports utilisés au VLAN approprié (spécifié dans la table de VLAN ci-dessus) et configurez-les pour le mode d'accès statique.

b. Exécutez la commande **show vlan brief** et vérifiez que les VLAN sont attribués aux interfaces correctes

Partie 3: Configurez le trunking.

Étape 1: Configurez manuellement l'interface trunk F0/1.

a. Modifiez le mode de port de commutateur (switchport) sur l'interface F0/1 de manière à imposer le trunking. Veillez à effectuer cette opération sur les deux commutateurs.

b. Dans le cadre de la configuration du trunk, définissez le VLAN natif sur 1000 sur les deux commutateurs. Vous pouvez voir des messages d'erreur temporairement pendant que les deux interfaces sont configurées pour différents VLAN natifs.

c. Comme autre partie de la configuration du trunk, spécifiez que les VLAN 10, 20,30 et 1000 sont autorisés à traverser le trunk.

d. Exécutez la commande **show interfaces trunk** pour vérifier les ports de trunk, le VLAN natif et les VLAN autorisés sur le trunk.

Étape 2: Configurer manuellement l'interface F0/5 de S1.

a. Configurez l'interface F0/5 de S1 avec les mêmes paramètres de trunk de F0/1. C'est le trunk au routeur.

b. Enregistrez la configuration en cours dans le fichier de configuration initiale.

c. Exécutez la commande **show interfaces trunk** pour vérifier le trunk.

Partie 4: Configurer le routage.

Étape 1: Configurez le routage inter-VLAN

a. Activez l'interface G0/0/1 sur le routeur.

b. Configurez les sous-interfaces pour chaque VLAN comme spécifié dans la table d'adressage IP. Toutes les sous-interfaces utilisent l'encapsulation 802.1Q. Assurez-vous que la sous-interface du VLAN natif n'a pas d'adresse IP attribuée. Inclure une description pour chaque sous-interface.

c. Configurez l'interface de loopback1 sur R1 avec l'adressage à partir du tableau ci-dessus.

d. Utilisez la commande **show ip interface brief** pour vérifier que la configuration de la sous-interface est opérationnelle.

Étape 2: Configurez l'interface R2 g0/0/1 en utilisant l'adresse de la table et une route par défaut avec le tronçon suivant 10.20.0.1

Partie 5: Configurer l'accès pour la gestion à distance

Étape 1: Configurez tous les périphériques réseau pour la prise en charge SSH de base.

a. Créez un utilisateur local avec le nom d'utilisateur sshAdmin et le mot de passe crypté $cisco123!

b. Utilisez **ccna-lab.com** comme nom de domaine.

c. Générer des clés de chiffrement à l'aide d'un module 1024 bits.

d. Configurez les cinq premières lignes VTY sur chaque périphérique pour prendre en charge uniquement les connexions SSH et pour s'authentifier auprès de la base de données utilisateur locale.

Partie 6: Vérification de la connectivité

Étape 1: Configurez les PC hôtes.

Reportez-vous à la table d'adressage pour les informations d'adresses d'hôte de PC.

Étape 2: Effectuez les tests suivants. Tous devrait aboutir.

Remarque: Vous devrez peut-être désactiver le pare-feu du PC pour que les requêtes ping puissent aboutir.

Origine	Protocole	Destination
PC-A	Ping	10.40.0.10
PC-A	Ping	10.20.0.1
PC-B	Ping	10.30.0.10
PC-B	Ping	10.20.0.1
PC-B	Ping	172.16.1.1
PC-B	SSH	10.20.0.1
PC-B	SSH	172.16.1.1

Partie 7: Configurer et vérifier les listes de contrôle d'accès étendu

Lorsque la connectivité de base est vérifiée, l'entreprise exige que les stratégies de sécurité suivantes soient mises en œuvre:

Stratégie 1: Le réseau Ventes n'est pas autorisé à SSH au réseau Gestion (mais d'autres SSH est autorisé).

Stratégie 2: Le réseau Ventes n'est pas autorisé à envoyer des demandes d'écho ICMP aux réseaux Opérations ou Gestion. Les requêtes d'écho ICMP vers d'autres destinations sont autorisées.

Stratégie 3: Le réseau Opérations n'est pas autorisé à envoyer des demandes d'écho ICMP au réseau Ventes. Les requêtes d'écho ICMP vers d'autres destinations sont autorisées.

Étape 1: Analysez le réseau et les exigences de la stratégie de sécurité pour planifier la mise en œuvre de la liste ACL.

Étape 2: Élaborer et appliquer des listes d'accès étendues qui répondront aux instructions de politique de sécurité.

Étape 3: Vérifiez que les stratégies de sécurité sont appliquées par les listes d'accès déployées.

Effectuez les tests suivants. Les résultats attendus sont présentés dans le tableau:

Origine	Protocole	Destination	Les résultats
PC-A	Ping	10.40.0.10	FAIL
PC-A	Ping	10.20.0.1	Success
PC-B	Ping	10.30.0.10	FAIL
PC-B	Ping	10.20.0.1	FAIL
PC-B	Ping	172.16.1.1	Réussite
PC-B	SSH	10.20.0.4	FAIL
PC-B	SSH	172.16.1.1	Réussite