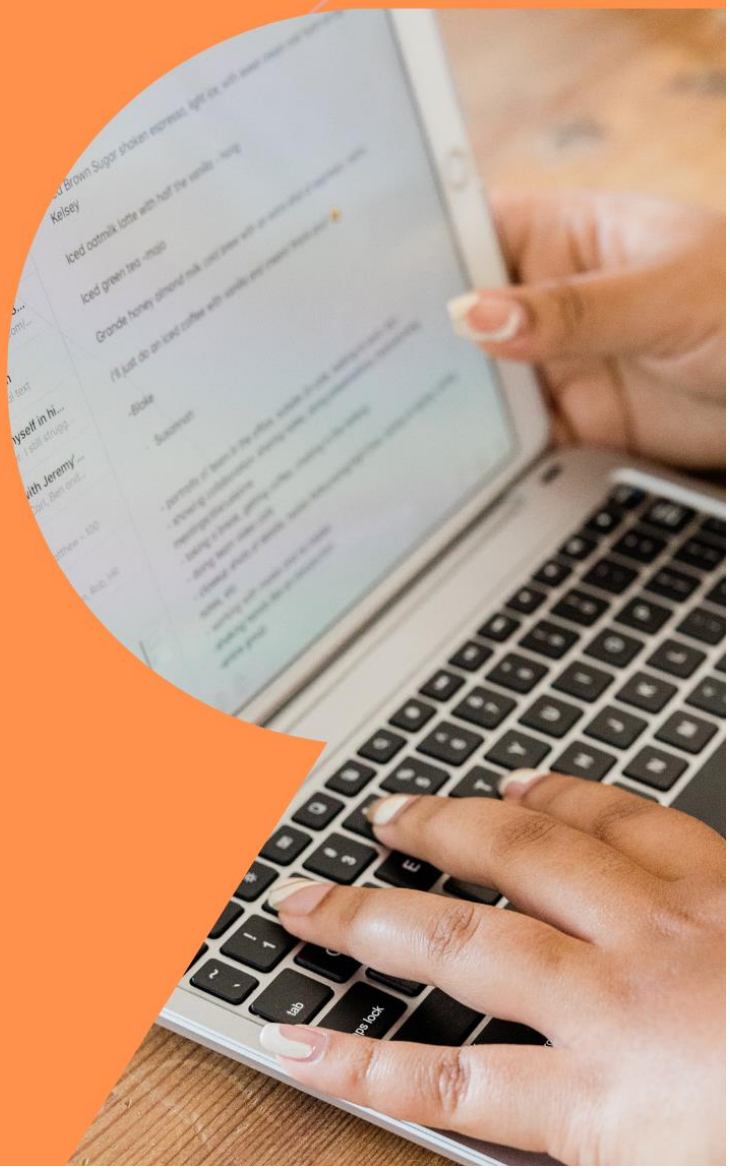
Epreuve E5

BTS SIO Session 2022

parcour SISR

Création d'access-list



PRÉSENTÉ PAR

Sandy Cerrato

2022

ÉPREUVE E4 : CONCEPTION ET MAINTENANCE DE SOLUTIONS INFORMATIQUES

PROJET PERSONNALISÉ ENCADRÉ

NOM PRENOM	N° CANDIDAT	PARCOURS
Cerrato Sandy		SISR

Augmentation du niveau de sécurité du server NAS

ÉPREUVE	⊗ Épreuve ponctuelle ◯ Contrôle en cours de formation			
MODALITÉS DE RÉALISATION	CONTEXTE BASÉ SUR LE CONTEXTE GÉNÉRAL DE LA : **M2L** MAISON DES LIGUES DE LORRAINE			
CONTEXTE GÉNÉRAL	**PÉRIODE**		**DURÉE ESTIMÉE**	
DESCRIPTION DE LA MISSION - DESCRIPTION DES BESOINS - RÉSULTATS ATTENDUS	Etudes des dispositifs qui permettent de sécuriser les SWITCH Cisco de niveau 2 et 3. Définition d'un mot de passe d'accès avec a minima un hachage MD5 au mode privilégié et création d'une bannière d'avertissement afin de lutter contre les connexions frauduleuses. Activer pour tous les équipements le supportant le protocole SSH ce qui aura pour effet de bannir le protocole TELNET pas assez sécuriser car en clair. Enfin créer des Access List interdisant l'accès au réseau ou l'autorisant à certains groupes uniquement.			
RESSOURCES MOBILISÉES	➢ Switch cisco Catalys 3560-CX series ➢ Switch cisco Catalys 2960-C Serie LL ➢ PC utilisateur Windows 10 ➢ Putty ➢ SSH ➢ Mémento			
PRINCIPAUX SAVOIR-FAIRE MOBILISÉS	➢ Étude de l'impact de l'intégration d'un service sur le système informatique. ➢ Étude des exigences liées à la qualité attendue d'un service. ➢ Gestion des identités et des habilitations. ➢ Proposition d'amélioration d'un service. ➢ Déployer un service. ➢ Mise en place et vérification des niveaux d'habilitations. ➢ Prise en compte du niveau de sécurité nécessaire à une infrastructure. ➢ Exploitation des référentiels, normes et standards adoptés par le prestataire. ➢ Recueil d'informations sur une configuration et ses éléments			
PRODUCTION ASSOCIÉES	Synoptique recto/verso, annexes descriptives + screenshot.			

MODALITÉS D'ACCÈS AUX PRODUCTIONS EN LIGNE	http://localhost:3000/index.php

RAPPORT D'ACTIVITE

ETAPE 1	Création de l'environnement de travail, définitions des objectifs		
OBJECTIF(S)	Avoir un environnement de travail fonctionnel et une vision clair de la marche à suivre		
RESSOURCE(S)	Connexion aux interfaces SWITCH vérification de leurs santé général		
CHRONOLOGIE DE RÉALISATION	➢ Analyse du niveau de sécurité des SWITCH cisco Catalys 3560-CX series et cisco Catalys 2960-C Serie LL ➢ Etudes de la configuration en place. ➢ Etudes des Access-List à déployer et de leurs contraintes. ➢ Prise en compte des vlan.		
ETAPE 2	Analyse de la politique de sécurité		
OBJECTIF(S)	Etude des dispositifs de sécurité déjà présent		
RESSOURCE(S)	SWICTH Réglages et sécurité ligne de commande		
CHRONOLOGIE DE RÉALISATION	➢ Etude des différents vlan et de leurs réseaux. ➢ Etude de la sécurité de ceux-ci (ici niveaux 3). ➢ Définition du type d'ACL à mettre en place. ➢ Définition du mot de passe MD5 à mettre en place et de la bannière. ➢ Vérifiez si le protocole SSH est applicable sur les deux switch		
ETAPE 3	Dispositif applicable		
OBJECTIF(S)	Mettre en place les dispositifs applicable sur nos deux SWITCH Cisco.		
RESSOURCE(S)	SWITCH ligne de commande/Configuration		
CHRONOLOGIE DE RÉALISATION	➢ Mise en place du mot de passe d'accès au compte privilégié sur les deux switch. ➢ Mise en place de la bannière d'avertissement sur les deux switch. ➢ Activer le couche de sécurité SSH sur les deux Switch (ils la supportent tous les deux .) ➢ Création des Access-List étendu en entrer d'instruction. ➢ Rédaction d'une procédure.		
ETAPE 4	Rédaction de la procédure		
OBJECTIF(S)	Fournir une procédure détaillé de la création d'Access-List a l'attention du client.		
RESSOURCE(S)	Word / ligne de commande		
CHRONOLOGIE DE RÉALISATION	➢ Création du document Word ➢ Insertion des screen shot et explication ➢ Rédaction et mise au propre		

Présentation de la configuration en place

Pour déclarer nos Access-List et configurer nos équipements comme indiqué dans le cas professionnel je me connecte d'abord sur mon Switch Catalys 3560-CX séries en ligne de commande et j'analyse la configuration déjà présente.

J'ai déjà créer des vlan pour les différents réseau de la M2L, on voit qu'ils ont tous une plage IP définit qui leur est attribué et qui correspond au différentes sections de l'entreprise.

Dans le cadre de la sécurisation de notre réseau nous allons avoir plusieurs missions :

- Mise en place du mot de passe d'accès au compte privilégié sur les deux switch.
- Mise en place de la bannière d'avertissement sur les deux switch.
- Activer le couche de sécurité SSH sur les deux Switch (ils la supportent tous les deux .)
- Création des Access-List étendu en entrer d'instruction.

Ce cas d'étude a était réaliser en 3 semaines dans les labos de mon école.

10.0.6.14 - PuTTY

```
interface GigabitEthernet0/10
!
interface GigabitEthernet0/11
!
interface GigabitEthernet0/12
!
interface Vlan1
 ip address 10.0.6.14 255.255.255.240
!
interface Vlan16
 ip address 10.0.6.30 255.255.255.240
!
interface Vlan32
 ip address 10.0.6.46 255.255.255.240
!
interface Vlan48
 ip address 10.0.6.62 255.255.255.240
!
interface Vlan64
 ip address 10.0.6.78 255.255.255.240
 ip helper-address 10.0.6.56
!
interface Vlan80
 ip address 10.0.6.94 255.255.255.240
!
interface Vlan96
 ip address 10.0.6.110 255.255.255.240
 ip helper-address 10.0.6.60
!
interface Vlan112
 ip address 10.0.6.126 255.255.255.240
!
interface Vlan128
 ip address 10.0.6.142 255.255.255.240
 ip helper-address 10.0.6.56
!
ip forward-protocol nd
no ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 172.20.6.1
!
```

Voici la configuration en place sur nos deux switch.

Il y a déjà des Vlan et des fourchettes IP associés.

Mise en place du mot de passe d'accès au compte privilégié.

Enable#

Conf t#enable secret YCH

Conf t#end

```
SW FED 6(config)#enable secret YCH
```

Voici la comande « enable secret » elle vas hasher avec un algo de force 5 par defaut.

```
enable secret 5 $1$lfyD$To993y6WYDG6hxkyVtsZq0
```

Voici comment apparait le mot de passe dans la configuration.

```
username YCH secret 5 $1$oMwi$jAizwgCGKlljTnUL7f9q1.
username YCH2022$ secret 5 $1$bNfY$w.vpi7fr6AZNadQzrJw3g0
```

Le mot de passe et le username sont crypté de bout en bout en sha 256 un logiciel proprietaire Cisco

Il existe deux commandes pour sécuriser un mot de passe sur cisco.

La premiere est «enable password» et la seconde «enable secret».

La difference entre les deux est qu' avec « enable password » le mot de passe défini est encodé en clair dans la config.
Tandis qu'avec la commande « enable secret » le mot de passe est stocké sous forme de hachage MD5, ce qui rend cette version beaucoup plus sécurisée…

Le HASH MD5 est une fonction irréversible, ce qui signifie qu'il n'existe pas d'algorithme ou de fonction permettant de retrouver la chaîne d'origine à partir de son HASH.

Mise en place de la bannière d'avertissement.

Enable#

Conf t#banner motd#unauthorized access to this device is prohibited!#

```
banner mood 'toutes connexions non autorise vous expose a des poursuites'
SW_FED_6(config)#
```

Ici nous avons pour des raisons juridique mis en place une bannière d'avertissement pour prévenir toute tentative de connexion qui ne serait pas autorisé sur l'équipement , elle est a déclaré dans la configuration global des switch.

Activer le couche de sécurité SSH

Line con 0

Line vty 0 4

Login local

Transport imput ssh

```
line con 0
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login
!
!
end
```

VTY est un port virtuel et utilisé pour obtenir un accès Telnet ou SSH à l'appareil.

VTY est uniquement utilisé pour les connexions entrantes vers l'appareil.

Ces connexions sont toutes virtuelles et aucun matériel n'y est associé.

Dans notre cas j'ai uniquement autorisé la connexion et le transport de donné via SSH et non telnet.

Création des Access-List étendu en entrer d'instruction.

Enable#

Config# access-list 101 deny tcp any host 10.0.6.14 eq 22

Config# access-list 101 permit ip any any

Config#do sh run

Config#interface vlan 48

Config-if#ip access-group 101 in

Config-if#exit

```
SW_FED_6(config)#access-list 101 deny tcp any host 10.0.6.14 eq 22
SW_FED_6(config)#acc
SW_FED_6(config)#access-list 101 permit ip any any
SW_FED_6(config)#do sh run
```

Avec la commande protocole « deny tcp any host 10.0.6.14 « je bloque tous le trafic à destination de cette adresse depuis le port 22 (SSh) .On termine toujours la commande de l'ACL avec permit ip any any sinon on bloque tout le trafic car de base l'instruction termine par deny any any

```
SW_FED_6(config)#interface vlan 48
SW_FED_6(config-if)#ip access-group 101 in
SW_FED_6(config-if)#exit
SW_FED_6(config)#
```

Ici je fais entré l'ACL sur le vlan 48 et la declarant « in » elle sera placé en debut d'instruction .

```
interface Vlan48
 ip address 10.0.6.62 255.255.255.240
 ip access-group 101 in
```

L'acl est bien lié au vlan 48

```
SW_FED_6(config)#interface vlan 80
SW_FED_6(config-if)#ip access-group 101 in
SW_FED_6(config-if)#exit
SW_FED_6(config)#interface vlan 96
SW_FED_6(config-if)#ip access-group 101 in
SW_FED_6(config-if)#exit
SW_FED_6(config)#interface vlan 112
SW_FED_6(config-if)#ip access-group 101 in
SW_FED_6(config-if)#exit
SW_FED_6(config)#interface vlan 128
SW_FED_6(config-if)#ip access-group 101 in
SW_FED_6(config-if)#
```

La création d'Access-List dans notre cas doit être étendu car les ACL étendu filtre sur la source, la destination, le numéro port ainsi que le protocole a l'inverse de la standard qui ne filtre que sur l'IP source, elles sont moins sécurisés.

Note

- Les ACL vous permettent de créer des règles autorisant ou interdisant l'accès à un réseau.

- Il existe deux types d'ACL :

    - Les standards qui permettent de configurer la source et doivent être placés au plus près de la destination.
    - Les étendues qui permettent de renseigner la source, la destination ainsi que le port et doivent être placées au plus près de la source.

- Les ACL peuvent soit autoriser soit interdire un réseau.

- Une fois créée L'ACL doit être associée à une interface.

- Les règles des ACL se lisent de haut en bas, l'ordre a donc une importance.

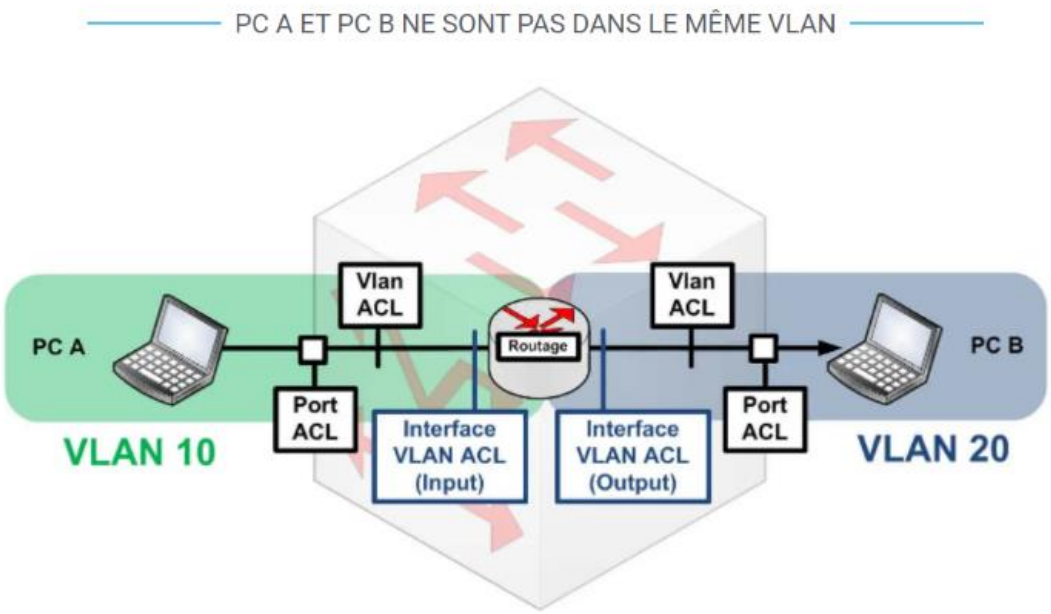
- Les règles les plus précises doivent être placées en haut et les plus générales en bas.

- Pour créer une ACL standard, il faut entrer la commande :

    - routeur(config)#access-list n°1-99 deny/permit réseau masque Inversé

- Pour créer une ACL étendue, il faut entrer la commande :

    - routeur(config)#access-list n°100-199 deny/permit protocole réseau Source masque Inversé réseau Destination masque Inversé n°port



Voici un réseau avec deux pc chacun dans un vlan (donc réseau) différents l'un de l'autre.
Ils peuvent communiquer mais pour des raisons de sécurité ils sont soumis à un contrôle via Access-List

L'Access-List vas intervenir après que le routeur est envoyé une requête de connexion et vas filtré en étudiant l'IP source et celle de destination ainsi que le protocole dans notre cas c'est donc bien une ACL étendu.
En fonction des résultat le pc A sera autorisé a communiqué avec le PC B et inversement.
Si une des conditions d'accès est refusé par l'ACL alors le trafic sera instantanément bloqué.
Il est important dans notre cas de mettre l'ACL au plus proche de la source a fin qu'elle sois la plus efficace possible

Les ACL sont de redoutable alliés dans la sécurisation d'un réseau.