



Une formation
Alphorm.com

Formation

La sécurité des réseaux avec Cisco

Partie 2



Hamza KONDAH



Une formation
Alphorm.com

Introduction

Cisco

Matériel réseau

Serveurs

Plusieurs gammes de produits

Plusieurs protocoles dédiés

Sécurité ☺





Une formation
Alphorm.com

Plan de la formation

Présentation de la formation

AAA

Sécurité Spanning Tree

La sécurité des protocoles

La sécurité ASA

Bonus : Durcissement

Conclusion et perspectives



Une formation
Alphorm.com

Public concerné

Administrateurs réseaux

Techniciens et ingénieurs

Auditeurs

RSSI

Toute personne désirant apprendre
de nouvelles choses 😊



Une formation
Alphorm.com

Objectifs de la formation

Gérer les composants des stratégies de sécurité des réseaux

Déployer et intégrer les mesures sécuritaires afin de protéger les éléments du réseau

Mettre en place les contrôles de menaces adéquats



Une formation
Alphorm.com

Objectifs de la formation

Mise en place de la sécurité AAA

Mise en place d'une connectivité VPN sécurisé

Mise en place d'un firewall Cisco ASA et sa configuration sécurisé

Sécuriser le protocole STP



Une formation
Alphorm.com

Prérequis

Formation Réseaux Cisco 1/2 : Maîtriser la sécurité
Maîtrisez tous les aspects de sécurité de vos réseaux Cisco



Une formation
Alphorm.com

Prérequis

Avoir des connaissances de base en réseaux

Avoir des connaissances de base en sécurité informatique

Avoir suivi les cours ICND1 et ICND2



Introduction à AAA



Hamza KONDAH



Plan

Le Modèle AAA

Authentification RADIUS

L'authentification RADIUS et 802.1X

Protocole EAP

Une formation
Alphorm.com



Le Modèle AAA

Authentication

- Authentifier l'identité du client.

Authorization

- Accorder des droits au client

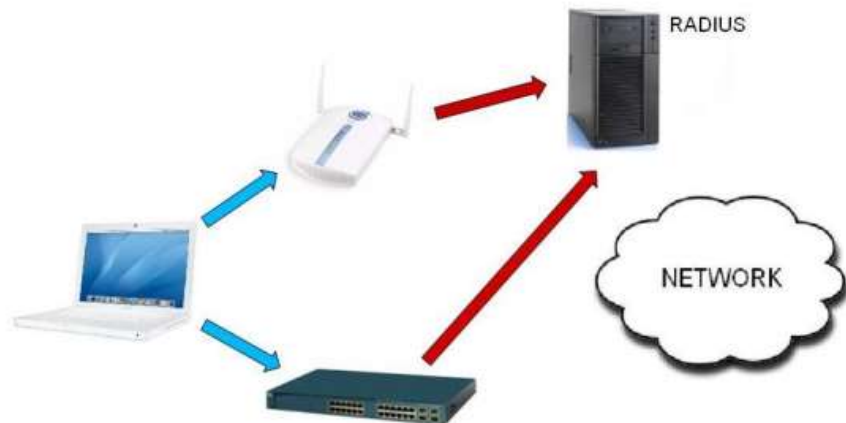
Accountability

- Enregistrer les données de l'usage du réseau par le client.

Une formation
Alphorm.com



Authentification RADIUS



Une formation
Alphorm.com



L'authentification RADIUS et 802.1X

Le standard 802.1X a été mis au point par l'IEEE en juin 2001

Il a pour but d'authentifier un client (en filaire ou en WiFi) afin de lui autoriser l'accès à un réseau

Une formation
Alphorm.com



L'authentification RADIUS et 802.1X

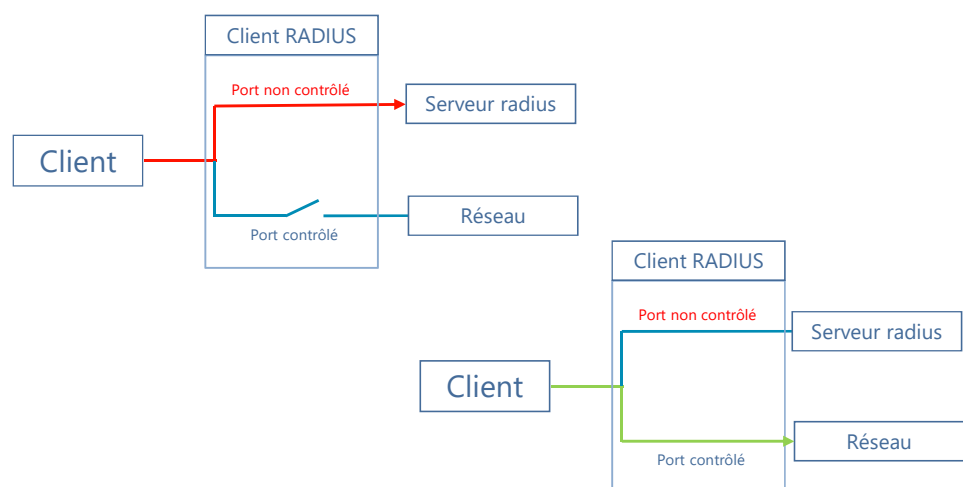
On utilise le protocole EAP (*Extensible Authentication Protocol*) et un serveur d'authentification qui est généralement un serveur RADIUS

Le serveur RADIUS va authentifier chaque client qui se connecte au réseau sur un port

Une formation
Alphorm.com



L'authentification RADIUS et 802.1X



Une formation
Alphorm.com



Une formation
Alphorm.com

Protocole EAP

Le protocole *Extended Authentication Protocol* sert pour le transport des données nécessaires à l'authentification

Ce protocole est extensible, car on peut définir de nouvelles méthodes d'authentification, car il est indépendant de la méthode utilisée



Une formation
Alphorm.com

Protocole EAP

EAP-MD5 : Authentification avec un mot de passe

EAP-TLS : Authentification avec un certificat électronique

EAP-TTLS : Authentification avec n'importe quelle méthode d'authentification, au sein d'un tunnel TLS



Protocole EAP

EAP-PEAP : Authentification avec n'importe quelle méthode d'authentification EAP, au sein d'un tunnel TLS

Une formation
Alphorm.com

Le protocole EAP

TYPE D'EAP	Méthode d'authentification	Caractéristique
EAP-MDS	login / password	Facile à implémenter
		Supporté par la plupart des serveurs
		Attaquable par dictionnaire hors-ligne
		Pas d'authentification mutuelle
EAP-TLS	certificat	Utilisation de certificats par le client et le serveur , de ce fait création d'un tunnel sur
		Authentification mutuelle entre le client et serveur
		Lourd à mettre en place à cause des certificats coté client
EAP-PEAP EAP-TTLS	login / password et certificat	Création d'un tunnel TLS
		Moins lourd que EAP-TLS , car pas de certificat du côté client
		Moins sur que EAP-TLS , car pas de certificat du côté client



Le protocole RADIUS

Le protocole RADIUS permet de centraliser les données d'authentification

Il répond au modèle AAA :

Authentication

- Authentifier l'identité du client

Authorization

- Accorder des droits au client

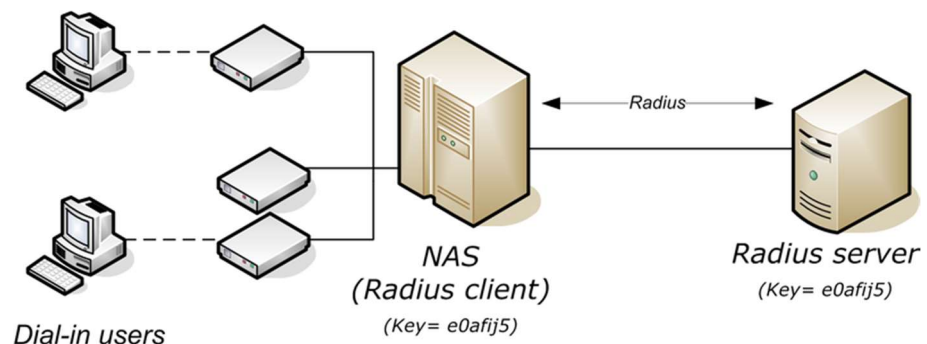
Accountability

- Enregistrer les données de l'usage du réseau par le client

Une formation
Alphorm.com



Le protocole RADIUS



Une formation
Alphorm.com

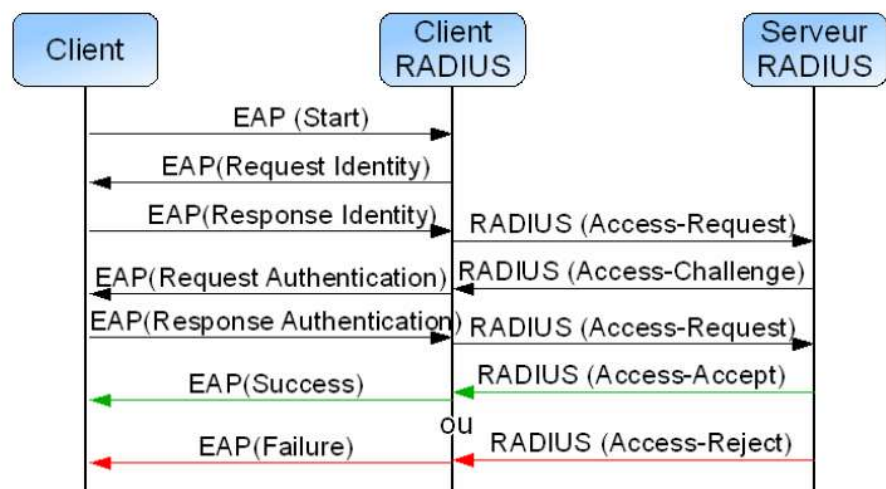
Le protocole

Ce protocole se situe au-dessus de la couche de transport UDP, sur les ports 1812 et 1813
Pour l'authentification il y a quatre types de paquets :

Access-Request	• Envoyé par le contrôleur d'accès, contenant les informations sur le client (login/mot de passe,...)
Access-Accept	• Envoyé par le serveur dans le cas où l'authentification est un succès
Access-Reject	• Envoyé par le serveur dans le cas où l'authentification est un échec, ou si il souhaite fermer la connexion
Access-Challenge	• Envoyé par le serveur pour demander des informations complémentaires, et donc la réémission d'un paquet Access-Request



L'authentification RADIUS et 802.1X





L'authentification RADIUS et 802.1X

Les types de paquets de base :

EAP Request : Envoyé par le contrôleur d'accès au client

EAP Response : Réponse du client au contrôleur d'accès

Une formation
Alphorm.com



L'authentification RADIUS et 802.1X

EAP Success : Paquet envoyé au client en fin d'authentification si elle est réussie

EAP Failure : Paquet envoyé au client en fin d'authentification si elle est ratée

Une formation
Alphorm.com



Mise en place d'une authentification RADIUS



Hamza KONDAH

Une formation
Alphorm.com



LAB : RADIUS

No.	Time	Source	Destination	Protocol	Length	Info
6988	86.89034600	HonHaiPr_03:41:39	Cisco_c6:a7:11	EAPOL	69	Start
6990	86.89167700	Cisco_c6:a7:11	HonHaiPr_03:41:39	EAP	116	Request, Identity
7023	86.91849300	HonHaiPr_03:41:39	Cisco_c6:a7:11	EAP	89	Response, Identity
7126	87.20702500	Cisco_c6:a7:11	HonHaiPr_03:41:39	EAP	116	Request, Identity
7132	87.21698800	HonHaiPr_03:41:39	Cisco_c6:a7:11	EAPOL	69	Start
7135	87.21844700	Cisco_c6:a7:11	HonHaiPr_03:41:39	EAP	116	Request, Identity
7164	87.30259600	HonHaiPr_03:41:39	Cisco_c6:a7:11	EAP	89	Response, Identity
7169	87.30670500	HonHaiPr_03:41:39	Cisco_c6:a7:11	EAP	89	Response, Identity
7170	87.30700000	Cisco_c6:a7:11	HonHaiPr_03:41:39	EAP	84	Response, Restricted, not
* Frame 7164: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0						
+ Radiotap Header v0, Length: 26						
+ IEEE 802.11 QoS Data, Flags:R..TC						
+ Logical Link Control						
+ 802.1X Authentication						
Version: 802.1X-2001 (1)						
Type: EAP Packet (0)						
Length: 21						
+ Extensible Authentication Protocol						
Code: Response (2)						
Id: 1						
Length: 21						
Type: Identity (1)						

Une formation
Alphorm.com



Paramétrer AAA à l'aide de Cisco Configuration Professional

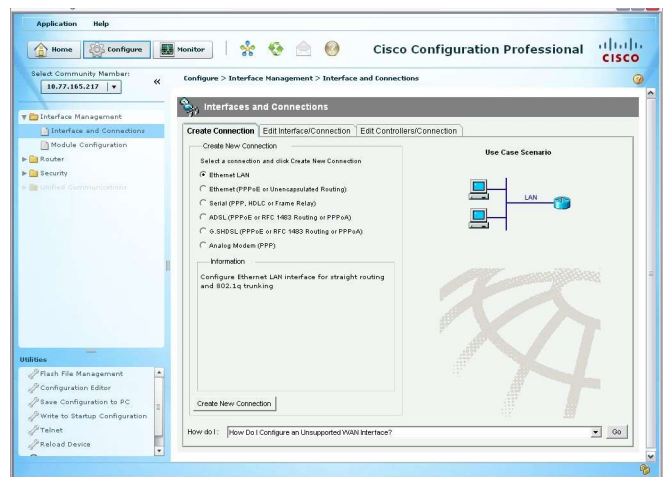


Hamza KONDAH

Une formation
Alphorm.com



Lab : Cisco Configurator Professionnel



Une formation
Alphorm.com



Une formation
Alphorm.com

Introduction au Spanning Tree Protocol (STP)



Hamza KONDAH



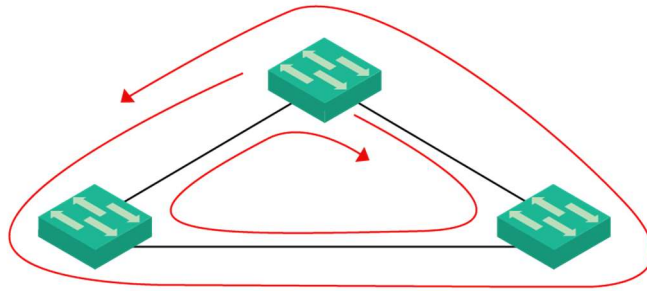
Une formation
Alphorm.com

Plan

Introduction
Fonctionnement
Root Bridge



Introduction

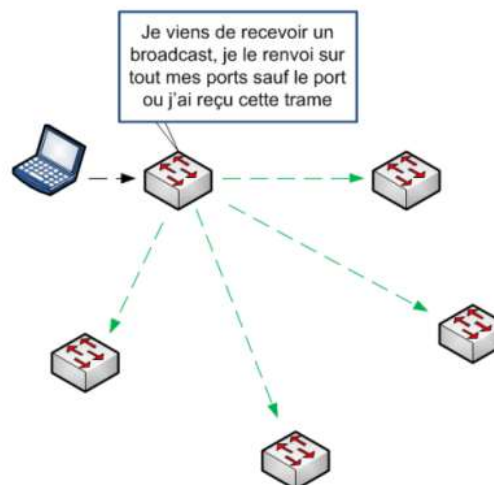


Une formation
Alphorm.com



Fonctionnement

ETAPE 1

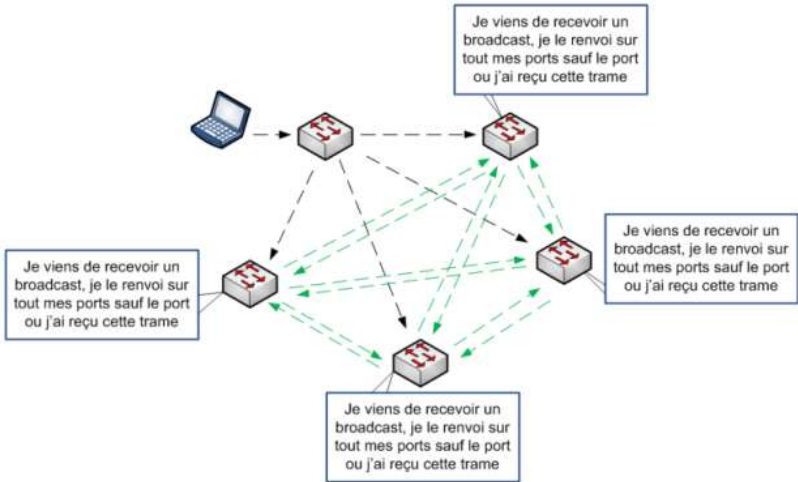


Une formation
Alphorm.com



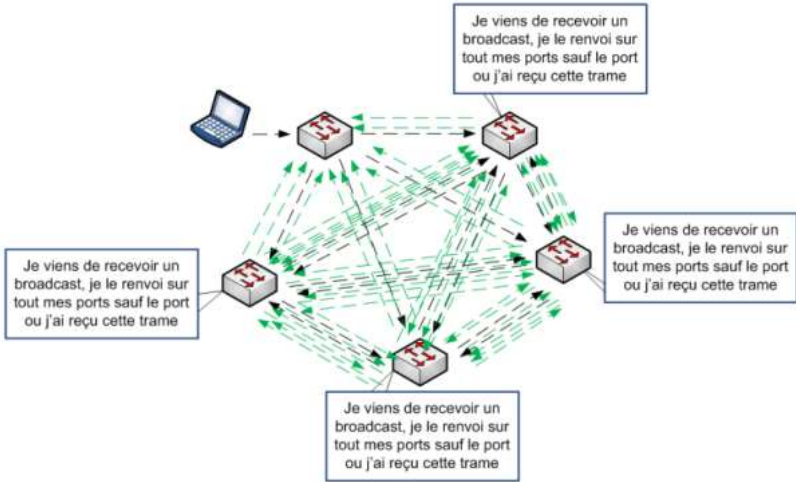
Fonctionnement

ETAPE 2



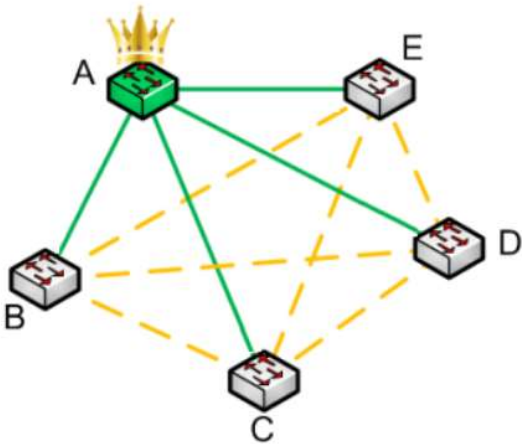
Fonctionnement

ETAPE 3





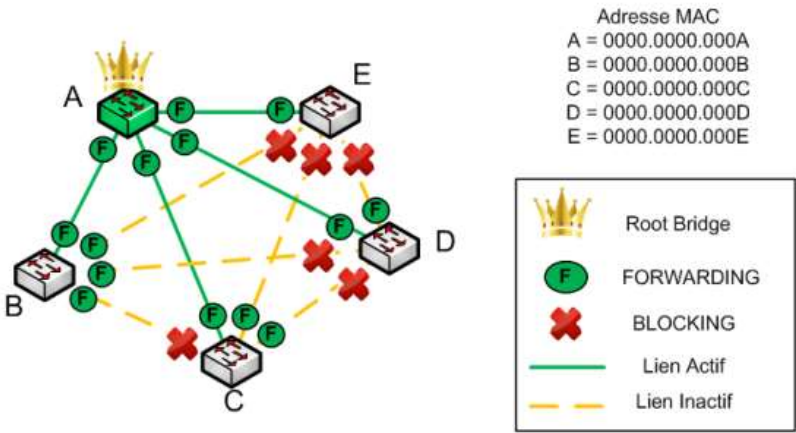
Le protocole STP



Une formation
Alphorm.com



Le protocole STP



Une formation
Alphorm.com



Rôles des ports

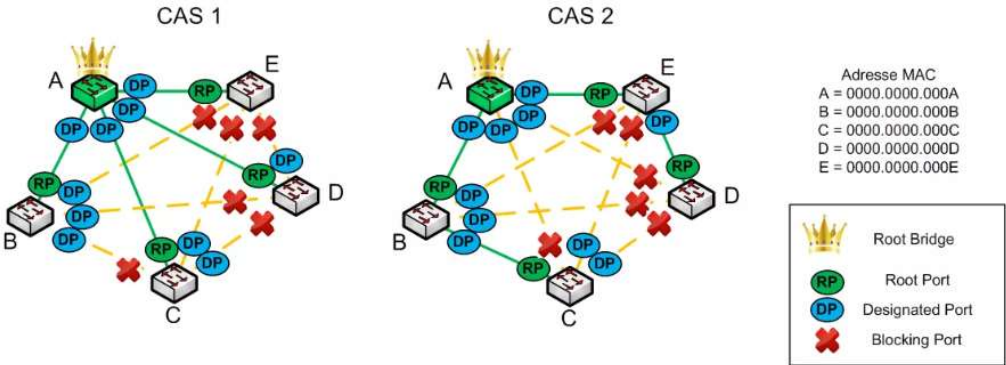
Root Port

Designated Port

Blocking Port

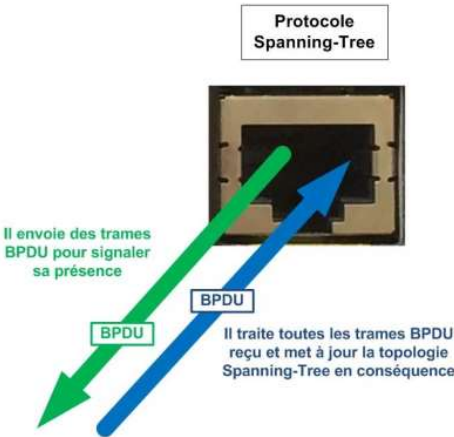


Rôles des ports

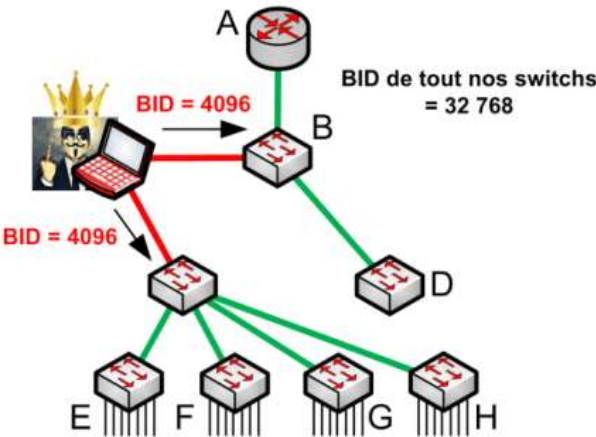




La protection du Spanning Tree

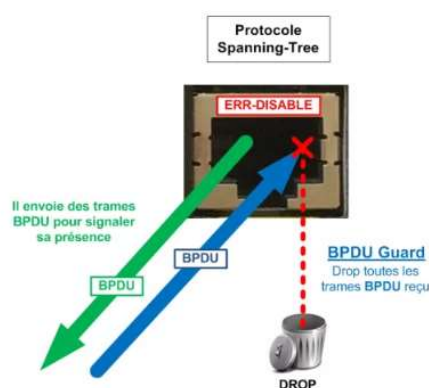


La protection du Spanning Tree





La protection du Spanning Tree



Une formation
Alphorm.com



Attaque & Défense sur le protocole STP



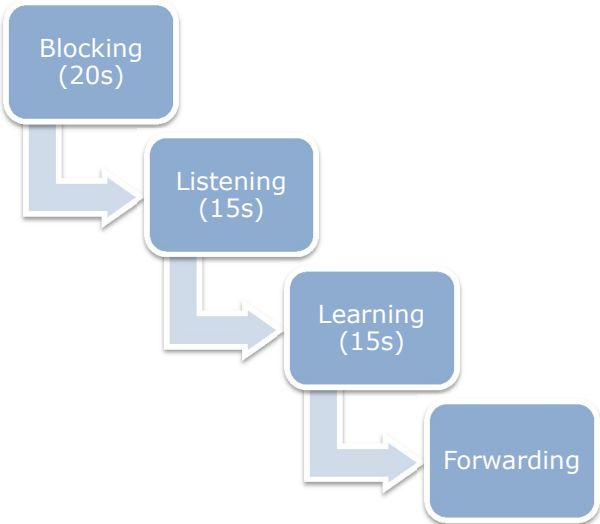
Hamza KONDAH

Une formation
Alphorm.com



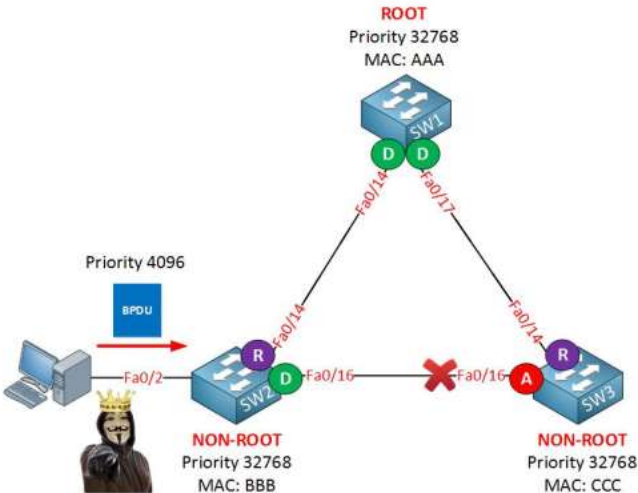
Une formation
Alphorm.com

Etats des ports



Une formation
Alphorm.com

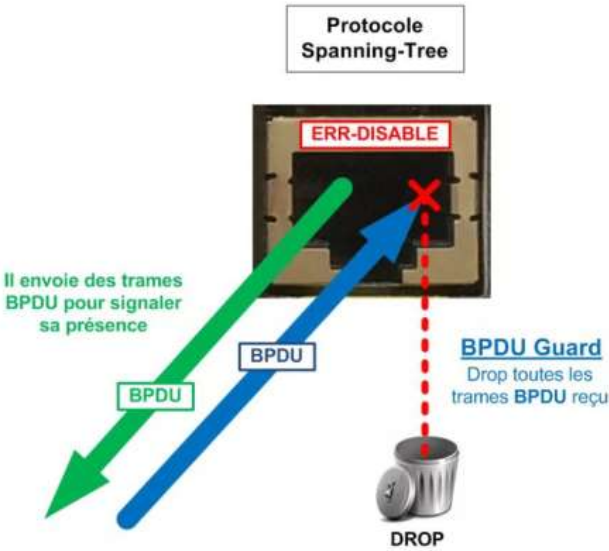
BPDU Guard





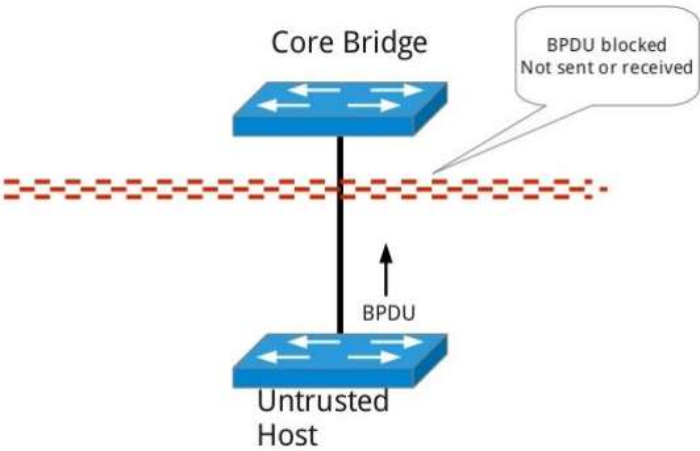
Une formation
Alphorm.com

BPDU Guard



Une formation
Alphorm.com

BPDU Guard





Lab : Protection BPDU

```
Core#
Core#
Core#
Core#show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: default Clients
Extended system ID is enabled
Portfast Default is disabled
Portfast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
EtherChannel misconfig guard is disabled
UplinkFast is disabled
BackboneFast is disabled
Configured Pathcost method used is short
```

Name	Blocking	Listening	Learning	Forwarding	STP Active
VLAN0001	0	0	0	2	2
VLAN0010	0	0	0	2	2
2 vlans	0	0	0	4	4

```
Core#
```



Rappels sur les VPNs



Hamza KONDAH



Plan

IPSEC

Mécanisme SA

AH et ESP

Une formation
Alphorm.com



IPSEC

Protocole fournissant un mécanisme
de sécurisation au niveau IP

RFC 2401 concernant IPSEC

RFC 2402 concernant le mode AH
(authentification)

Une formation
Alphorm.com



IPSEC

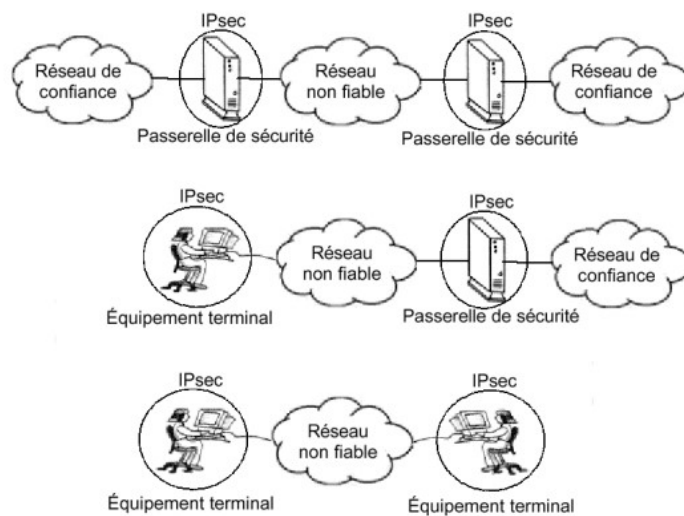
RFC 2406 concernant le mode ESP
(chiffrement)

RFC 2409 concernant IKE (*Internet Key
Exchange*)

Une formation
Alphorm.com



IPSEC



Une formation
Alphorm.com



Fonctions de l'IPSEC

Le chiffrement
L'authentification
La gestion des clés

Une formation
Alphorm.com



Mécanisme SA

Mécanisme des « SA » (*Security Association*) permet une négociation préalable avant toute communication des algorithmes utilisés, au travers d'un protocole distinct (ex: IKE, ISAKMP...)

Une formation
Alphorm.com



AH et ESP

Deux mécanismes de sécurité :

1. **Format AH** (*Authentication Header*) :
Utilisée en cas de besoin
d'authentification et d'intégrité
2. **Format ESP** (*Encapsulation Security
Payload*) : Utilisée en cas de besoin de
chiffrement (confidentialité)

Une formation
Alphorm
com



Fonctionnement

SA = connexion de service, offrant
des fonctionnalités de sécurité au
trafic transporté

Les services fournis par une SA
mettent en œuvre soit le protocole
AH soit **ESP**, mais pas les deux

Une formation
Alphorm
com



Notions mises en jeu

Algorithmes asymétriques

hachage (MD5)

Certificats X509

Infrastructures de gestion de clés...

Une formation
Alphorm.com



Deux solutions

1. **Gestion manuelle** des clés + négociation des SA
2. **Gestion de P.K.I.** (I.C.P) + négociation des SA

Une formation
Alphorm.com



Fonctionnement

Protocole **ISAKMP** (*Internet Security Association and Key Management Protocol*)
transporte UDP port 500 + protocole
IKE (*Internet Key Exchange*)

Une formation
Alphorm.com



Le terme “gestion” englobe

- La génération des clés
- La distribution des clés
- Le stockage des clés
- La révocation des clés
- La destruction des clés

Une formation
Alphorm.com



ISAKMP permet

La négociation

L'établissement

La modification

La suppression des SA et de leurs attributs

Une formation
Alphorm.com



Fonctionnement

La négociation est indépendante du protocole de sécurité utilisé

Les paramètres négociés sont décrits dans un "domain of Interpretation" (DOI)

Une formation
Alphorm.com



ISAKMP procède en 2 étapes

1. Création d'une première SA "ISAKMP" permettant ensuite
2. D'assurer la sécurité des négociations

Une formation
Alphorm.com



Fonctionnement

Création d'une SA pour le compte d'un protocole de sécurité, par exemple IPSec

ISAKMP est en fait un "toolkit" permettant de négocier une SA selon des directives "DOI"

Une formation
Alphorm.com



Une formation
Alphorm.com

Comprendre la PKI (*Public Key Infrastructure*)



Hamza KONDAH



Une formation
Alphorm.com

Plan

Rôle des PKI

Exemples d'utilisation des PKI

Composantes

Cryptage symétrique

Cryptage asymétrique

Comparaison



Rôle des PKI

PKI (*Public Key Infrastructure* ou *Infrastructure de clé publique*)

Technologies de cryptographie pour la sécurisation de votre environnement informatique

Une formation
Alphorm.com



Rôle des PKI

Confidentialité (Chiffrement)

Authentification (Utilisateur, Ordinateur)

Intégrité (Données non modifiées)

Une formation
Alphorm.com



Une formation
Alphorm.com

Exemples d'utilisation des PKI

Fichiers (Efs, Bitlocker)

Pilotes, ActiveX, Macros, Scripts PowerShell

Site Web (SSL)

Connexions réseau (VPN, Wifi...)

Sécurisation de trafic réseau (IpSec...)

Authentification Forte (Cartes à puce)

Mails



Une formation
Alphorm.com

Composantes

Cryptographie

- Algorithmes mathématiques
- Certificats

Autorités de certification (Gestion des certificats)



Cryptage symétrique

Algorithme mathématique + Clé (élément variable de l'algorithme)

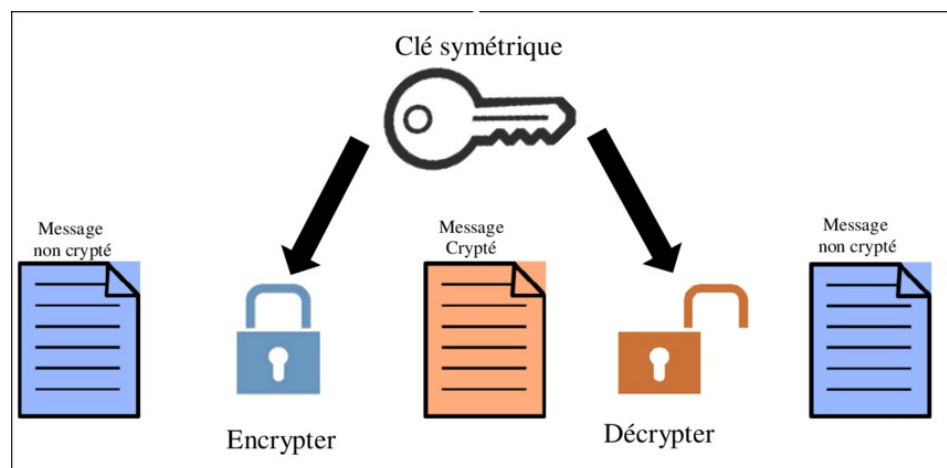
- Algorithmes mathématiques : Des, 3Des ou Aes ...
- Une seule clé (128, 256 bits)

La clé symétrique doit être transmise à l'aide de moyen de communication sécurisé

Une formation
Alphorm.com



Cryptage symétrique



Une formation
Alphorm.com



Certificat

Utilisation des clés, propriétaire,
durée de vie...)

Clé publique

Une formation
Alphorm.com



Clé Privée

Stockée dans un emplacement
protégé sur l'ordinateur

Lien mathématique de 1 à 1 entre la
clé privée et la clé publique

Une formation
Alphorm.com



Cryptage asymétrique

Principe : On génère 2 clés. Ce qui est encodé avec une clé est décodé par l'autre et réciproquement



Cryptage asymétrique

Echange de message sécurisé





Cryptage symétrique

Plus rapide, une seule clé de petite taille (128, 256 bits)

Requiert une communication déjà sécurisée pour l'échange de la clé
Cryptage

Une formation
Alphorm.com



Cryptage Asymétrique

Plus lent (100 fois ou plus...), deux clés (Publique\Privée + un certificat)

Taille des clés plus importante (1024, 2048, 4096 bits)

Totalement sécurisé

Une formation
Alphorm.com



Combinaison

On utilisera toujours une combinaison
de cryptage Symétrique\Asymétrique
Chiffrement du contenu : Symétrique
Plus rapide

Une formation
Alphorm
com



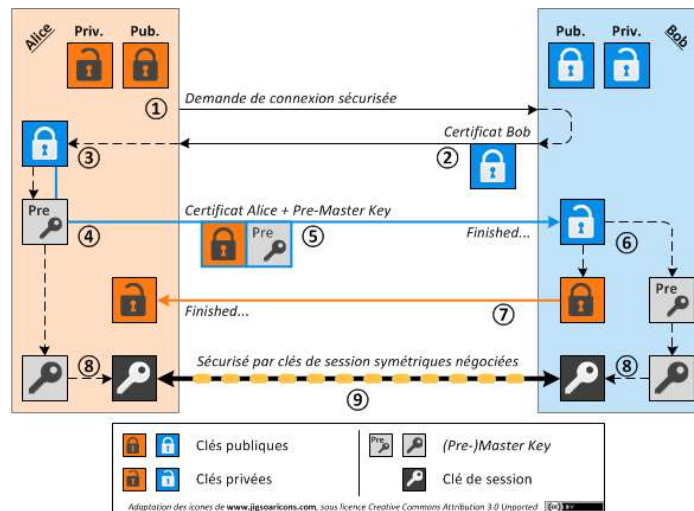
Combinaison

Protection de la clé : Asymétrique
Totalelement sécurisé
Le chiffrement asymétrique
sécurise la clé symétrique !!!

Une formation
Alphorm
com



Combinaison



Une formation
Alphorm.com



Comprendre et configurer un VPN poste à site



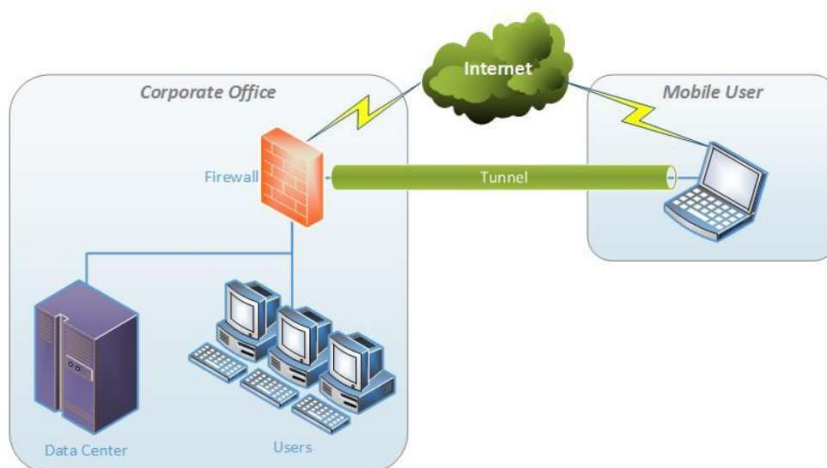
Hamza KONDAH

Une formation
Alphorm.com



Une formation
Alphorm.com

Lab : VPN poste à site



Une formation
Alphorm.com

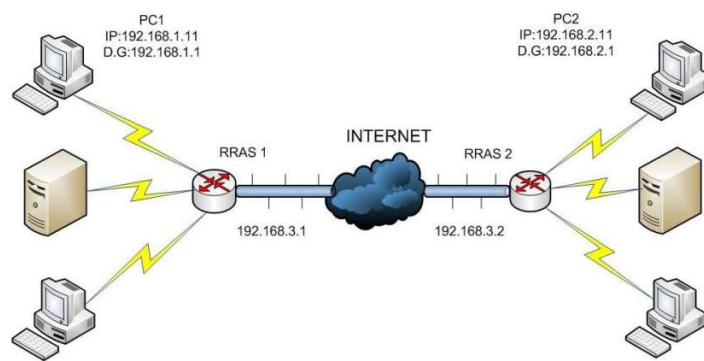
Configurer le VPN Site to Site



Hamza KONDAH



LAB : VPN IPSEC site à site



Une formation
Alphorm.com



Introduction à Cisco ASA



Hamza KONDAH

Une formation
Alphorm.com



Plan

Introduction

Fonctions ASA

Fonctionnalités avancées

Une formation
Alphorm.com



Introduction

Cisco ASA est le firewall Stateful le plus déployée en entreprise

Analyse du flux complet de trafic avec la fonction Cisco AVC (*Application Visibility and Control*)

Une formation
Alphorm.com



Introduction

FirePOWER Next-Generation IPS
(NGIPS)

Filtrage URL par réputation et par
catégorie et fonctionnalités de VPN

Une formation
Alphorm.com

Fonctions ASA

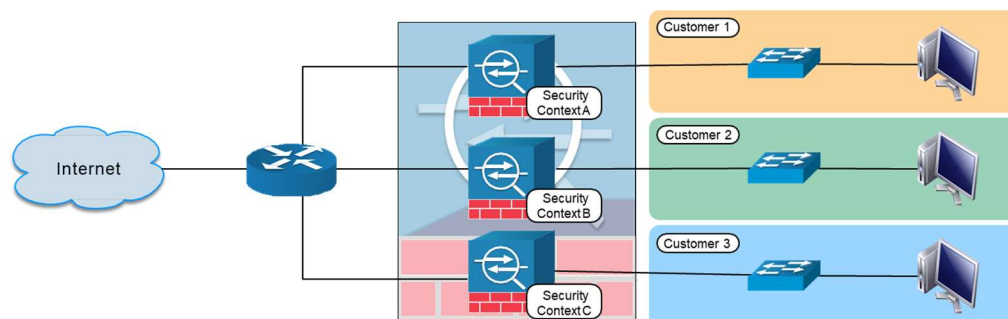
Fonction	Description
<i>Stateful Firewall</i>	◦ L'ASA propose un service de firewall avec gestion des états TCP ou UDP pour les connexions qui transitent par lui ◦ Seuls les paquets qui correspondent à une connexion active sont autorisés par le firewall, les autres sont rejetés
<i>VPN Concentrator</i>	◦ L'ASA supporte les connexions IPsec et SSL en Remote Access et les connexions VPN Site-to-Site
<i>Intrusion Prevention</i>	◦ Tous les modèles ASA supportent des fonctionnalités basiques d'IPS ◦ Des analyses plus détaillées peuvent être implémentées en ajoutant une carte ou un module d'extension Cisco Advanced Inspection and Prevention Security Services Module (AIP-SSM) ou Cisco Advanced Inspection and Prevention Security Services Card (AIP-SSC)

Fonctionnalités avancées

Fonction	Description
Virtualisation	- Une appliance physique peut être partitionnée en plusieurs instances virtuelles appelées contextes de sécurité (Security Contexts) - Chaque contexte est considéré comme un périphérique indépendant, avec ses propres règles, interfaces et administrateurs - La plupart des fonctionnalités IPS sont supportées excepté VPN et les protocoles de routage dynamiques
Haute disponibilité	- Deux ASA peuvent être reliés dans un mode de fonctionnement Active/Standby pour permettre la redondance d'équipements et la tolérance de pannes - Un ASA est promu comme périphérique primaire (Active) tandis que l'autre est mis en mode StandBy - Le software, les licences, la mémoire et les interfaces doivent être identiques sur les deux ASA
Identity Firewall	- L'ASA permet un contrôle d'accès en utilisant les informations d'authentification d'un annuaire Active Directory - Permet de créer des règles permettant des utilisateurs ou groupes d'utilisateurs au lieu de règles traditionnelles basées sur les adresses IP
Threat Control	En plus des fonctions IPS, des outils anti-malware et gestion des risques peuvent être ajoutés via le module Content Security and Control (CSC)

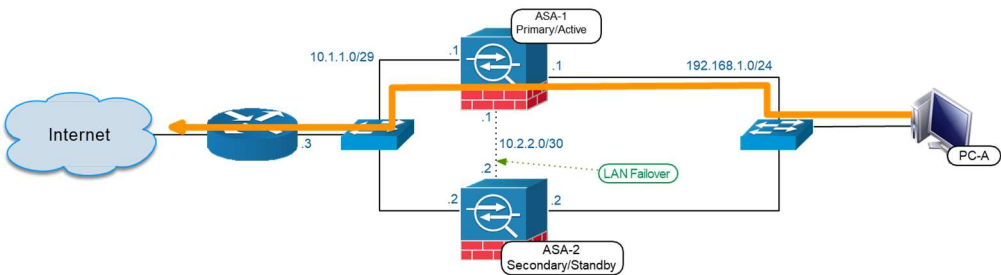


Virtualisation

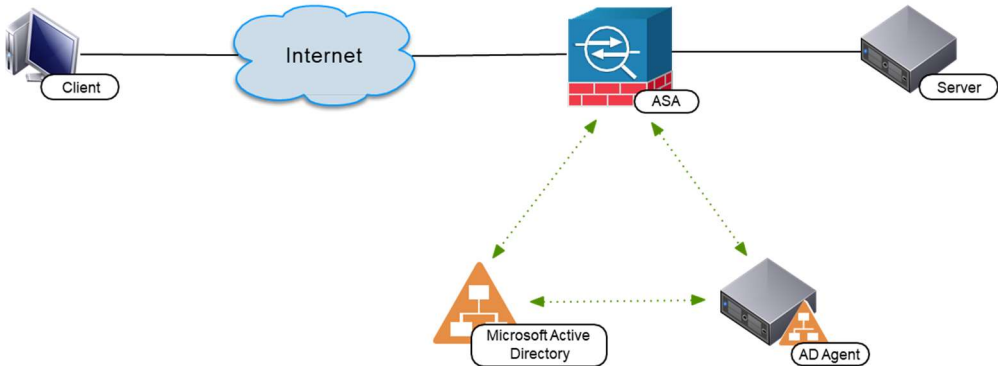




Haute disponibilité

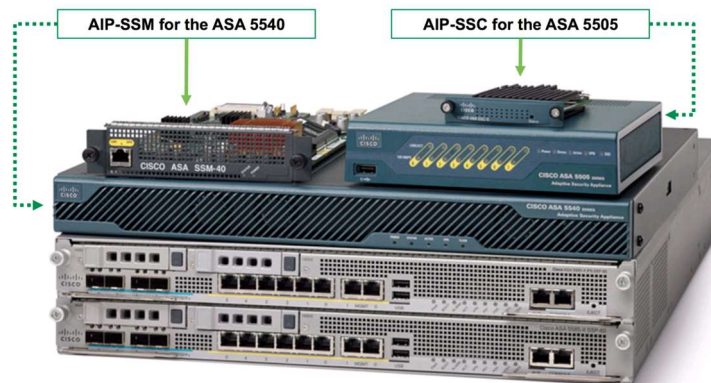


Identity Firewall





IDS/IPS



Une formation
Alphorm.com



Découvrir la terminologie ASA



Hamza KONDAH

Une formation
Alphorm.com



Plan

Niveaux de sécurité ASA

Types d'accès

Terminologie ASA

Lab : Mise en place de l'ASA

Une formation
Alphorm.com



Niveaux de sécurité ASA

Pour distinguer les réseaux internes et externes, l'ASA leur assigne un niveau de sécurité (Security-level)

Le niveau de sécurité définit la confiance accordée à une interface

Une formation
Alphorm.com



Niveaux de sécurité ASA

Plus le niveau est élevé, plus la confiance accordée est importante
Le niveau peut être défini dans un intervalle de 0 (non confiant) à 100 (confiance totale)

Une formation
Alphorm.com



Niveaux de sécurité ASA

Chaque interface opérationnelle doit avoir :

- Un nom
- Un niveau de sécurité entre 0 et 100
- Une adresse IP (si on place l'ASA en mode Routed)

Une formation
Alphorm.com



Niveaux de sécurité ASA

Par défaut :

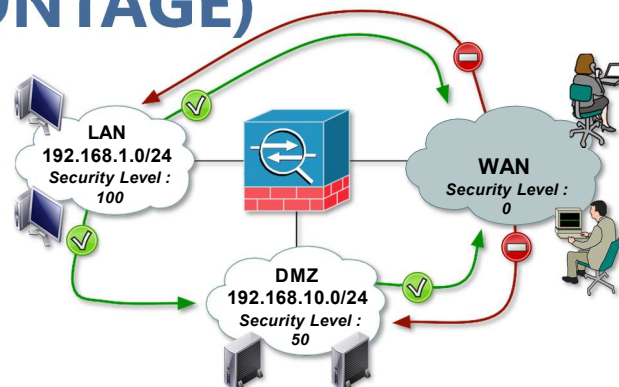
Toute interface nommée inside se verra automatiquement attribuée un niveau de sécurité = 100

Toute interface nommée outside se verra automatiquement attribuée un niveau de sécurité = 0

Une formation
Alphorm.com



Niveaux de sécurité ASA (PAS EGAL DANS MONTAGE)



Une formation
Alphorm.com



Niveaux de sécurité ASA

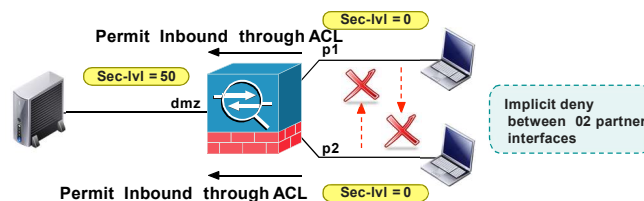
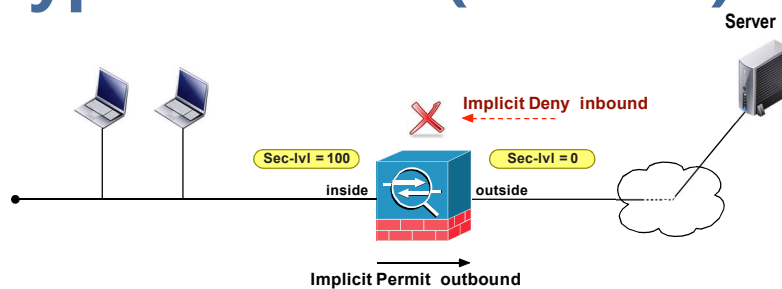
```
ASA2# show nameif
```

Interface	Name	Security
Vlan4	out	0
Vlan7	dmz	50
Vlan100	inside	100

Une formation
Alphorm.com



Types d'accès (a revoir)



Une formation
Alphorm.com



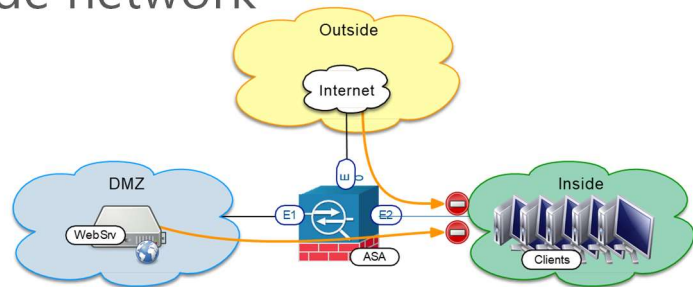
Une formation
Alphorm.com

Terminologie ASA

Inside Network

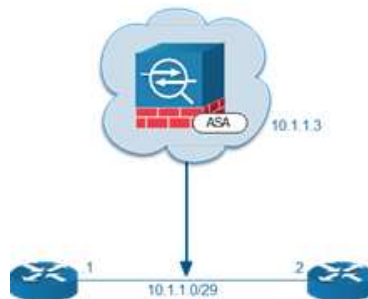
DMZ

Outside network



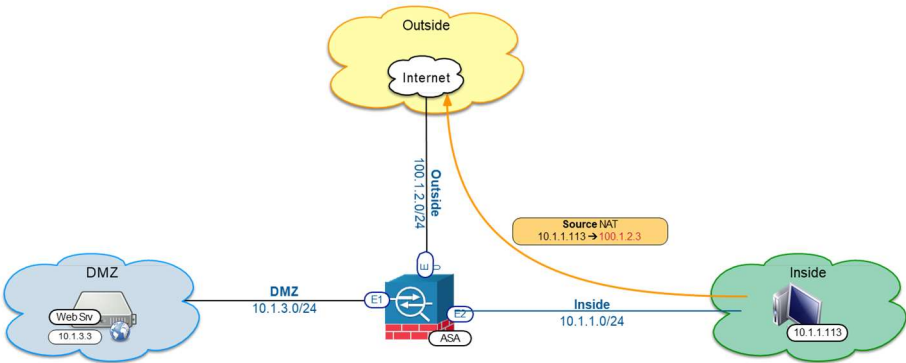
Une formation
Alphorm.com

Mode Routed vs Transparent

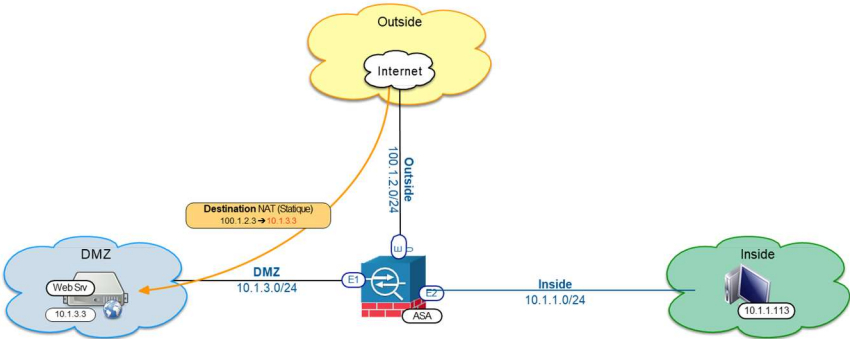




Mode Routed



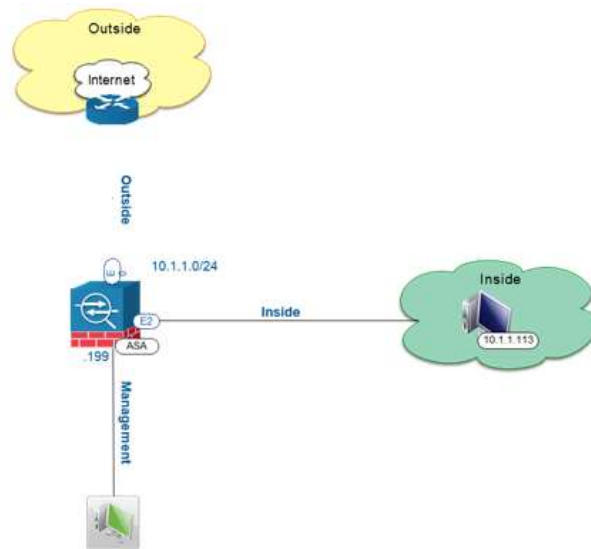
Mode Routed (revoir ce que j'ai dit à la fin)





Une formation
Alphorm.com

Mode Transparent



Une formation
Alphorm.com

Lab : Configuration de base

```
ASA(config)# firewall transparent  
Switched to transparent mode  
  
ASA# show firewall  
Firewall mode : Transparent
```



Une formation
Alphorm.com

Mettre en place une configuration de base



Hamza KONDAH



Une formation
Alphorm.com

Plan

ASA CLI

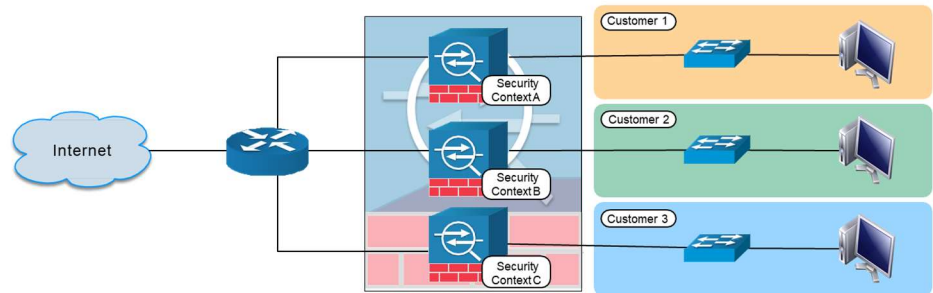
Equivalences des commandes

Modes d'accès

Lab : Configuration de base



Security Context



Une formation
Alphorm.com



Security Context

```
ASA(config)# context customer1
Creating context 'customer1'...Done (4)
ASA(config-ctx)# description customer 1 context
ASA(config-ctx)#
ASA(config-ctx)# allocate-interface gigabitethernet0/1.101
int1 ASA(config-ctx)# allocate-interface
gigabitethernet0/1.102 int2 ASA(config-ctx)#
ASA(config-ctx)# config-url disk0:context1.cfg
INFO: Converting disk0:context1.cfg to disk0/context1.cfg

WARNING: Could not fetch the URL
disk0:/context1.cfg INFO: Creating context with
default config
```

Une formation
Alphorm.com



Une formation
Alphorm.com

Security Context

```
ASA# changeto context customer1
ASA/customer1# show run
: Saved
:
ASA Version 9.1(3) <context>
!
hostname customer1
enable password 8Ry2YjIyt7RRXU24
encrypted names
!
interface int 1
 no nameif
 no security-level
 no ip address
!
interface int2
 no nameif
 no security-level
 no ip address
```



Une formation
Alphorm.com

Use cases des SC

Un Service Provider qui veut proposer des fonctionnalités de sécurité à plusieurs clients

- Coûts réduits, réduction des équipements physiques tout en offrant une séparation de trafic entre clients
- Grande entreprise ou campus qui désire séparer les départements (Segmentation)



Use cases des SC

Toute organisation qui désire que son réseau soit sécurisée par plus d'un ASA

Une formation
Alphorm.com



ASA CLI

Comme les routeurs IOS Cisco, l'ASA reconnaît les éléments suivants :

- Abréviation des commandes et mots-clés
- Utilisation de la touche Tab pour compléter une commande partielle
- Utilisation de la touche (?) pour voir la syntaxe

Une formation
Alphorm.com



ASA CLI

Permet d'exécuter n'importe quelle commande ASA quel que soit le mode de configuration affiché et ne reconnait pas la commande do utilisé en mode de configuration globale sur les routeurs IOS

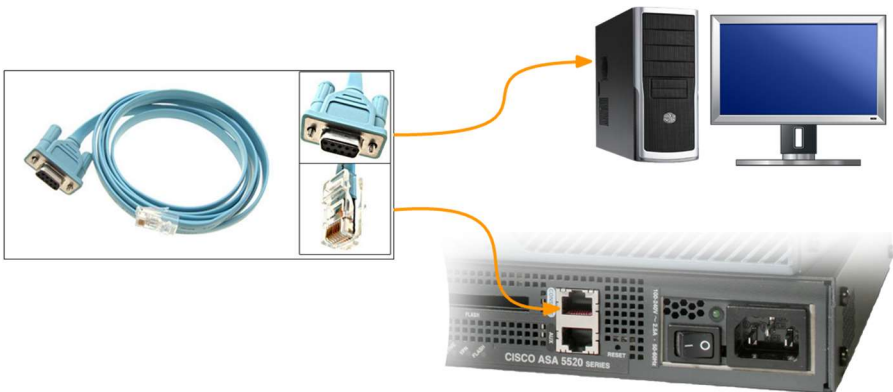


Equivalences des commandes

Commande routeur IOS	Commande ASA
enable secret password	enable password password
line con 0 password password login	passwd password
ip route	route outside
show ip interfaces brief	show interface ip brief
show ip route	show route
show plan	show switch vlan
show ip nat translations	show xlate
copy running-config startup-config	write [memory]
erase startup-config	write erase



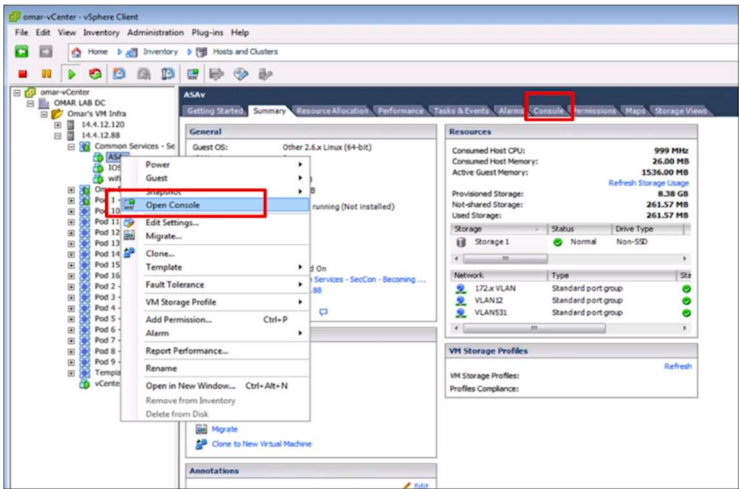
Le mode console



Une formation
Alphorm.com



ASDM



Une formation
Alphorm.com



Telnet

Il est possible de configurer les adresses IP acceptées par l'ASA pour une connexion Telnet

```
ASA(config)# telnet 10.1.1.0 255.255.255.0 inside
```

Telnet est un protocole non sécurisé. Il est recommandé d'utiliser SSH pour gérer le Cisco ASA ou tout autre périphérique



SSH

Etape 1

```
ASA(config)# crypto key generate rsa modulus 1024
```

Etape 2

```
ASA# write mem
```

Etape 3

```
ASA(config)# aaa authentication ssh console LOCAL
```

Etape 4

```
ASA(config)# ssh version 2
```

Etape 5

```
ASA(config)# ssh 10.1.1.0 255.255.255.0 inside
```



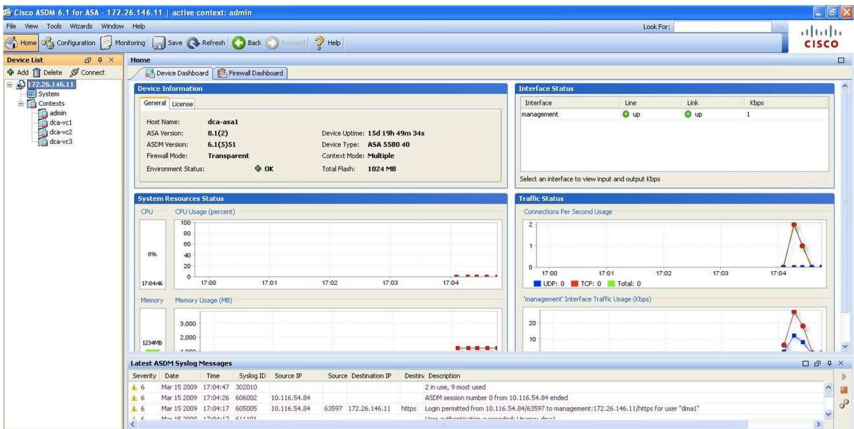
SSH

```
ASA(config)# username admin password class
ASA(config)# aaa authentication ssh console LOCAL
ASA(config)# crypto key generate rsa modulus 1024
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.

Do you really want to replace them? [yes/no]: y
Keypair generation process begin. Please wait...
CCNAS-ASA(config)# ssh 192.168.1.3 255.255.255.255 inside
CCNAS-ASA(config)# ssh timeout 10
CCNAS-ASA(config)# exit
CCNAS-ASA#
CCNAS-ASA# show ssh
Timeout: 5 minutes
Versions allowed: 1 and 2
192.168.1.3 255.255.255.255 inside
CCNAS-ASA#
```



Lab : Configuration ASA





Une formation
Alphorm.com

Comprendre les Objects et Objects Groups



Hamza KONDAH



Une formation
Alphorm.com

Plan

Les objects
Les types d'objects
Objects Groups



Une formation
Alphorm.com

Les Objects

Sur un ASA, l'administrateur effectue les configurations (règles de firewalls, règles VPN, règles NAT, ...) via l'utilisation d'objets (Objects) ou groupes d'objets (Objects Groups)



Une formation
Alphorm.com

Les Objects

Un objet peut être défini par une adresse IP particulière, un sous-réseau ou un protocole (et optionnellement un numéro de port)



Les Objects

L'avantage d'utiliser les objets est que, lorsque l'un des paramètres doit être modifié (adresse IP, port, ...), les changements sont automatiquement appliqués aux règles utilisant cet objet

Une formation
Alphorm.com



Network Object

Contient une adresse IP/Masque de sous-réseau

Peut être défini pour un hôte, un sous-réseau ou un intervalle

Une formation
Alphorm.com



Service Object

Contient un protocole ainsi (optionnel) qu'un port source et/ou destination

Un Network Object est requis pour configurer le NAT

Une formation
Alphorm.com



Objects Groups

Ils sont utilisés pour grouper les objets
Les objets peuvent être rattachés ou détachés de plusieurs Objects Groups
Cela permet d'éviter la duplication d'objets

Une formation
Alphorm.com

Objects Groups

Object-Group	Description
Network	Spécifie une liste d'hôtes IP, sous-réseaux ou intervalles d'IP
Protocol	Combine les protocoles IP (comme TCP, UDP, ICMP) dans un objet Par exemple, pour intégrer TCP et UDP pour le protocole DNS, créer un Object Group et ajouter le protocole TCP et UDP dans ce groupe
ICMP	Le protocole ICMP utilise un type unique pour l'envoi de messages de contrôle (RFC 792) Le groupe d'objets ICMP-type peut grouper les types nécessaires pour des besoins de sécurité
Service	Utilisé pour grouper les ports TCP, UDP, TCP/UDP dans un objet Il peut contenir un mélange de services TCP, services UDP, services ICMP, et tout protocole comme par ex. ESP, GRE, ...



Maitriser les ACL



Hamza KONDAH



Une formation
Alphorm.com

Plan

Introduction
Types ACL
Applications
Access Group
Lab : Les ACL



Une formation
Alphorm.com

Introduction

Les ACL sont composés d'un ensemble de règles ACE

Les ACL sont traitées de manière séquentielle depuis le haut vers le bas

Dès qu'une entrée ACE correspond, on sort de l'ACL sans consulter les règles suivantes



Introduction

Ils possèdent une entrée de refus par défaut à la fin de la liste

Ils respectent la règle suivante : une ACL par interface, par protocole, par sens

Ils peuvent être activés/désactivés selon des plages horaires définies

Une formation
Alphorm.com

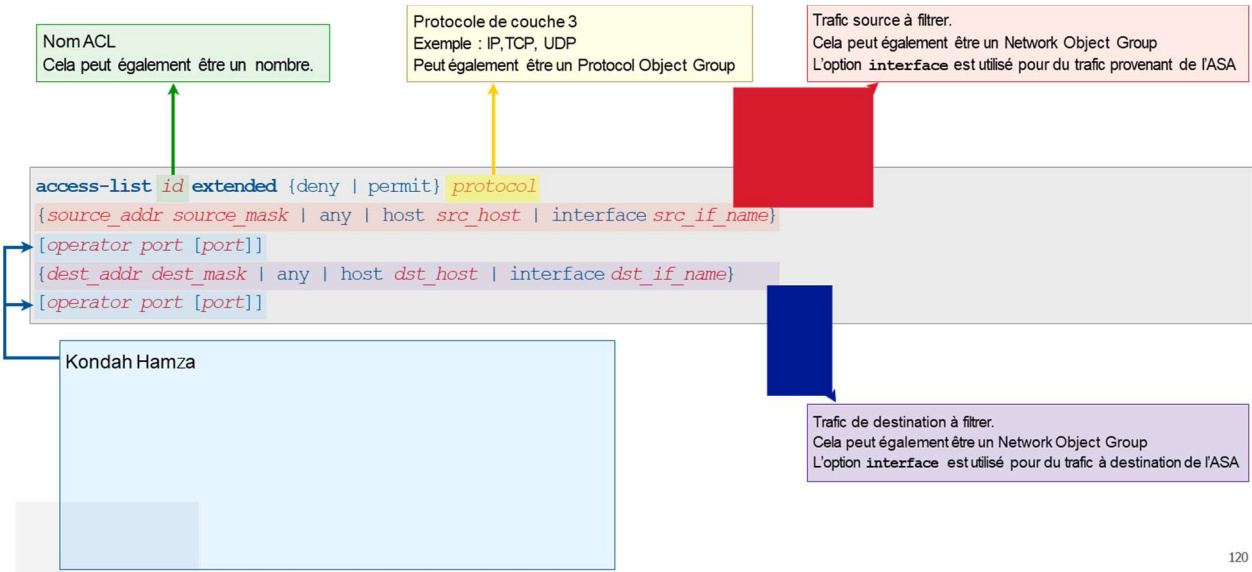
Types ACL

Type d'ACL	Description
<i>Extended</i>	- ACL le plus populaire - Filtrage basé sur le port source/destination et le protocole
<i>Standard</i>	- Utilisé pour les protocoles de routage, pas comme règles de firewall - Ne peut s'appliquer aux interfaces pour contrôler le trafic
<i>IPv6</i>	Utilisé pour supporter l'adressage IPv6
<i>Webtype</i>	Utilisé pour SSL VPN Clientless
<i>Ethertype</i>	- Spécifie le protocole de couche réseau - Utilisé uniquement lorsque l'ASA est en mode transparent

Applications

Utilisation ACL	Type d'ACL	Description
Gérer le trafic inter-réseaux	Extended	Par défaut, l'ASA n'autorise pas le trafic provenant d'un niveau de sécurité plus faible vers une interface ayant un niveau de sécurité plus haut sauf si explicitement autorisé
Identifier le trafic des règles AAA	Extended	Utilisé dans les listes d'accès AAA pour identifier le trafic
Identifier les adresses pour NAT	Extended	Les règles NAT permettent d'identifier le trafic local pour effectuer la translation d'adresses
Etablissement d'un accès VPN	Extended	Utilisé dans les commandes VPN
Identifier le trafic Modular Policy Framework (MPF)	Extended	Utilisé pour identifier le trafic dans une Class Map, qui est utilisé dans les fonctionnalités qui supportent MPF
Identifier la redistribution de route OSPF	Standard	- Les ACL Standards n'incluent que l'adresse de destination - Utilisé pour contrôler la redistribution des routes OSPF
Contrôler l'accès réseau pour les réseaux IPv6	IPv6	Utilisé pour contrôler le trafic sur les réseaux IPv6

Extended ACL



Access Group

Syntaxe	Description
access-group	◦ Mot-clé utilisé pour appliquer une ACL à une interface
acl-id	◦ Nom de l'ACL
in	◦ L'ACL filtre les paquets entrants
out	◦ L'ACL filtre les paquets sortants
interface	◦ Mot-clé utilisé pour spécifier l'interface à appliquer l'ACL
interface_name	◦ Nom de l'interface sur lequel appliquer l'ACL
per-user-override	◦ Option permettant de remplacer toutes les ACL de l'interface par l'ACL
control-plane	◦ Spécifie si la règle est utilisée pour du trafic vers ou provenant de l'ASA

```
access-group acl-id {in | out} interface interface-name  
[per-user-override | control-plane]
```



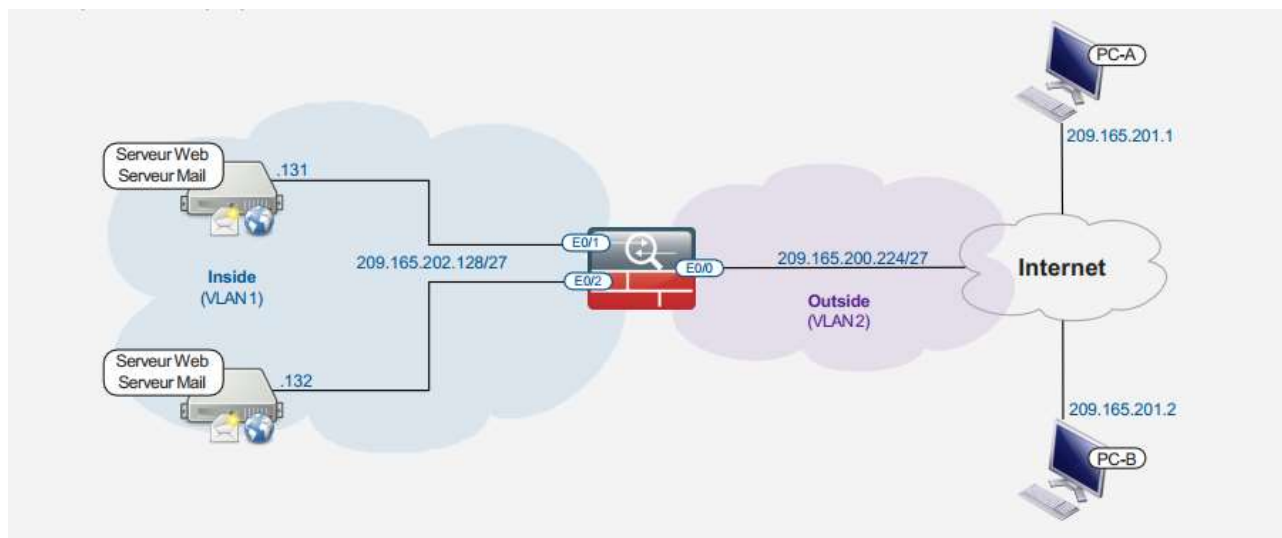
Exemples

```
access-list ACL-IN-1 extended permit ip any any  
access-group ACL-IN-1 in interface inside
```

```
access-list ACL-IN-3 extended permit tcp 192.168.1.0 255.255.255.0 host 209.165.201.228  
access-group ACL-IN-3 in interface inside
```

```
access-list ACL-IN-4 extended deny tcp any host 209.165.201.229 eq www  
access-list ACL-IN-4 extended permit ip any any  
access-group ACL-IN-4 in interface inside
```

```
access-list ACL-IN-2 extended deny tcp 192.168.1.0 255.255.255.0 host 209.165.201.228  
access-list ACL-IN-2 extended permit ip any any  
access-group ACL-IN-2 in interface inside
```



Lab : Les ACL

```
ASA# show run aaa
aaa authentication http console TACACS-SVR LOCAL
aaa authentication ssh console TACACS-SVR LOCAL
aaa authentication telnet console TACACS-SVR LOCAL
aaa authentication enable console TACACS-SVR LOCAL
ASA# disable
ASA> exit
```

```
Username: admin
Password: *****
Type help or '?' for a list of available commands.
ASA>
```



Une formation
Alphorm.com

Découvrir et configurer le Modular Policy Framework (MPF)



Hamza KONDAH



Une formation
Alphorm.com

Plan

Introduction

Politique ASA

Politique par default

Lab : Modular Policy Framework



Introduction

MPF définit un ensemble de règles pour configurer des fonctionnalités comme par exemple inspection de trafic et QoS au trafic qui traverse l'ASA

Permet la classification des flux de trafic et l'application de différentes politiques aux flux

Une formation
Alphorm.com



Introduction

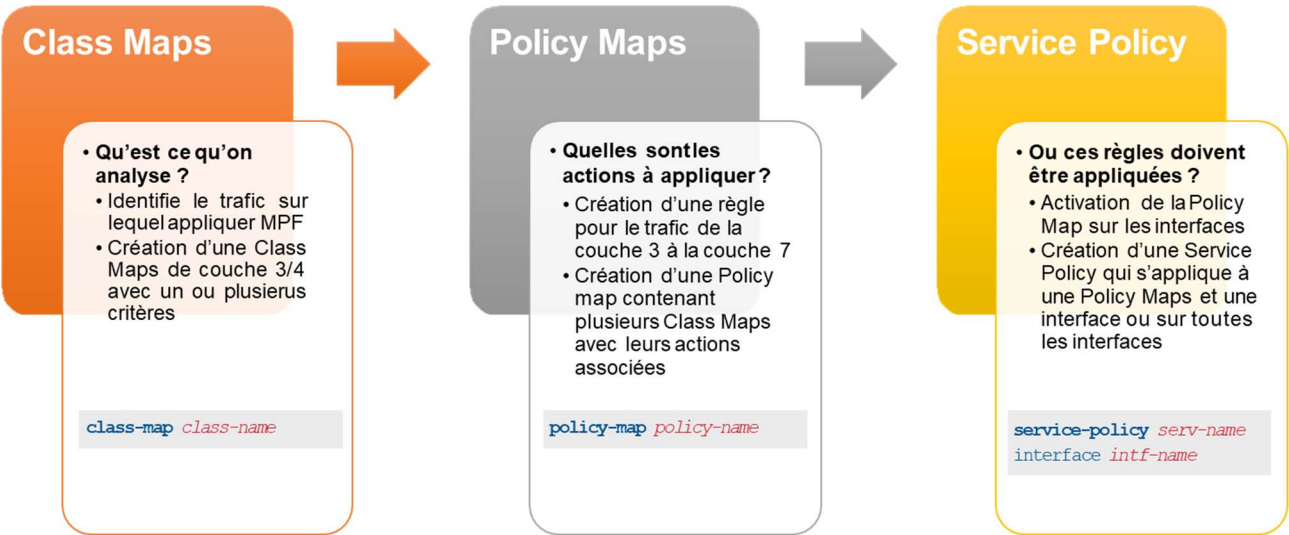
Class Maps

Policy Maps

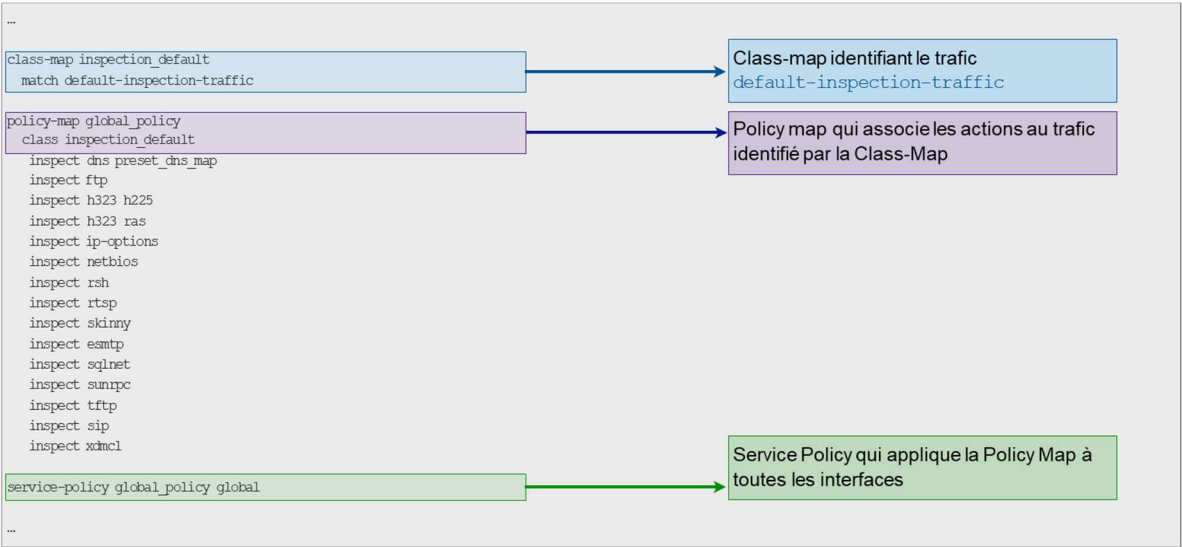
Service Policy

Une formation
Alphorm.com

Politique ASA



Politique par défaut





Lab : Modular Policy Framework

```
CCNAS-ASA(config)# access-list TFTP-TRAFFIC permit udp any any eq 69
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map CLASS-TFTP
CCNAS-ASA(config-cmap)# match access-list TFTP-TRAFFIC
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# policy-map POLICY-TFTP
CCNAS-ASA(config-pmap)# class CLASS-TFTP
CCNAS-ASA(config-pmap-c)# inspect tftp
CCNAS-ASA(config-pmap-c)# exit
CCNAS-ASA(config-pmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# service-policy POLICY-TFTP global
CCNAS-ASA(config)#
```

Une formation
Alphorm
com



Conclusion et Perspectives



Hamza KONDAH

Une formation
Alphorm
com



Bilan

AAA

Sécurité Spanning Tree

La sécurité des protocoles

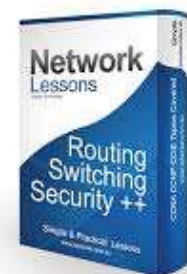
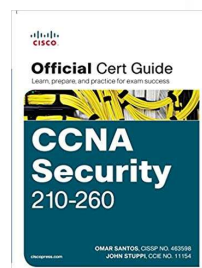
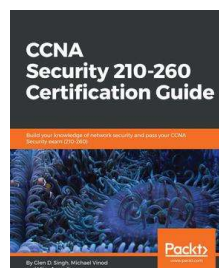
La Sécurité ASA

Durcissement équipements Cisco

Une formation
Alphorm.com



Bibliographie



Une formation
Alphorm.com



Prochainement



Une formation
Alphorm.com



Prochainement



Une formation
Alphorm.com



Prochainement



Une formation
Alphorm.com