



MASTERY TECH CENTER · NETWORK LABS · CAS PRATIQUES

CAS-01 · Lab complet

Segmentation sécurisée avec OSPF multi-area, filtrage avancé et Palo Alto

Manipulation de chemins OSPF (coûts, stub, NSSA, résumés), filtrage par prefix-list / route-map / filter-list, redistribution contrôlée d'un partenaire et segmentation Zero Trust avec un NGFW Palo Alto.

PnetLab · 16 équipements · Cisco IOL L3 / L2 · PAN-OS 10.x (VR legacy) · OSPFv2 · Niveau : intermédiaire · ≈ 4 h

Auteur : Hilaire T. · Mastery Tech Center

Version 1.0 · octobre 2026

Tous les labs : masterytechnologycenter.github.io/network-labs

Licence CC BY-NC-ND 4.0 : partage libre en citant l'auteur, sans usage commercial et sans modification. Les clés et mots de passe du lab sont factices.

MASTERY TECH CENTER



Sommaire

1. Scénario et objectifs

2. Topologie

3. Plan d'adressage

4. Références officielles

5. Tâches

Tâche 1 · Câblage, VLAN, trunks et adressage

Tâche 2 · OSPF multi-area de base (coûts par défaut)

Tâche 3 · Durcissement du plan de contrôle OSPF

Tâche 4 · Manipulation de chemin par le coût OSPF — trafic déterministe et symétrique

Tâche 5 · Area 20 Totally Stubby et manipulation de la route par défaut

Tâche 6 · Résumé inter-zone (area range) et manipulation du coût du résumé

Tâche 7 · Filtrage des LSA type 3 (filter-list) vs filtrage RIB (distribute-list)

Tâche 8 · NSSA + redistribution contrôlée d'un partenaire (route-maps, tags, metric-type)

Tâche 9 · Segmentation Palo Alto : zones, politiques App-ID, Zone Protection, ACL IoT

Tâche 10 · Tests de bascule et validation finale

6. Checklist de validation finale





1. Scénario et objectifs

L'entreprise **NEXA Industries** possède deux sites (A et B), un datacenter (web + base de données) et un partenaire externe qui doit accéder uniquement à l'application web. L'audit sécurité exige une **segmentation de bout en bout** : contrôle du plan de contrôle (qui peut annoncer quoi), maîtrise des chemins (par où passe le trafic) et contrôle d'accès (qui parle à qui).

16 équipements	5 domaines OSPF (areas 0/10/20/30 + process 200)	4 zones Palo Alto	10 tâches progressives	≈ 4 h durée estimée
--------------------------	--	-----------------------------	----------------------------------	-------------------------------

Compétences visées

- Concevoir un OSPF multi-area sécurisé (passive-interface, HMAC-SHA-256, p2p).
- Manipuler les chemins : coût d'interface, area default-cost, area range ... cost, metric-type E1/E2, choix du traducteur NSSA.
- Filtrer avec les outils recommandés : **prefix-list**, **route-map** (match/set/tag), area filter-list, distribute-list, summary-address.
- Segmenter avec un NGFW Palo Alto : zones, App-ID, objets, journalisation des refus, Zone Protection.
- Valider un design en mode nominal **et** dégradé.

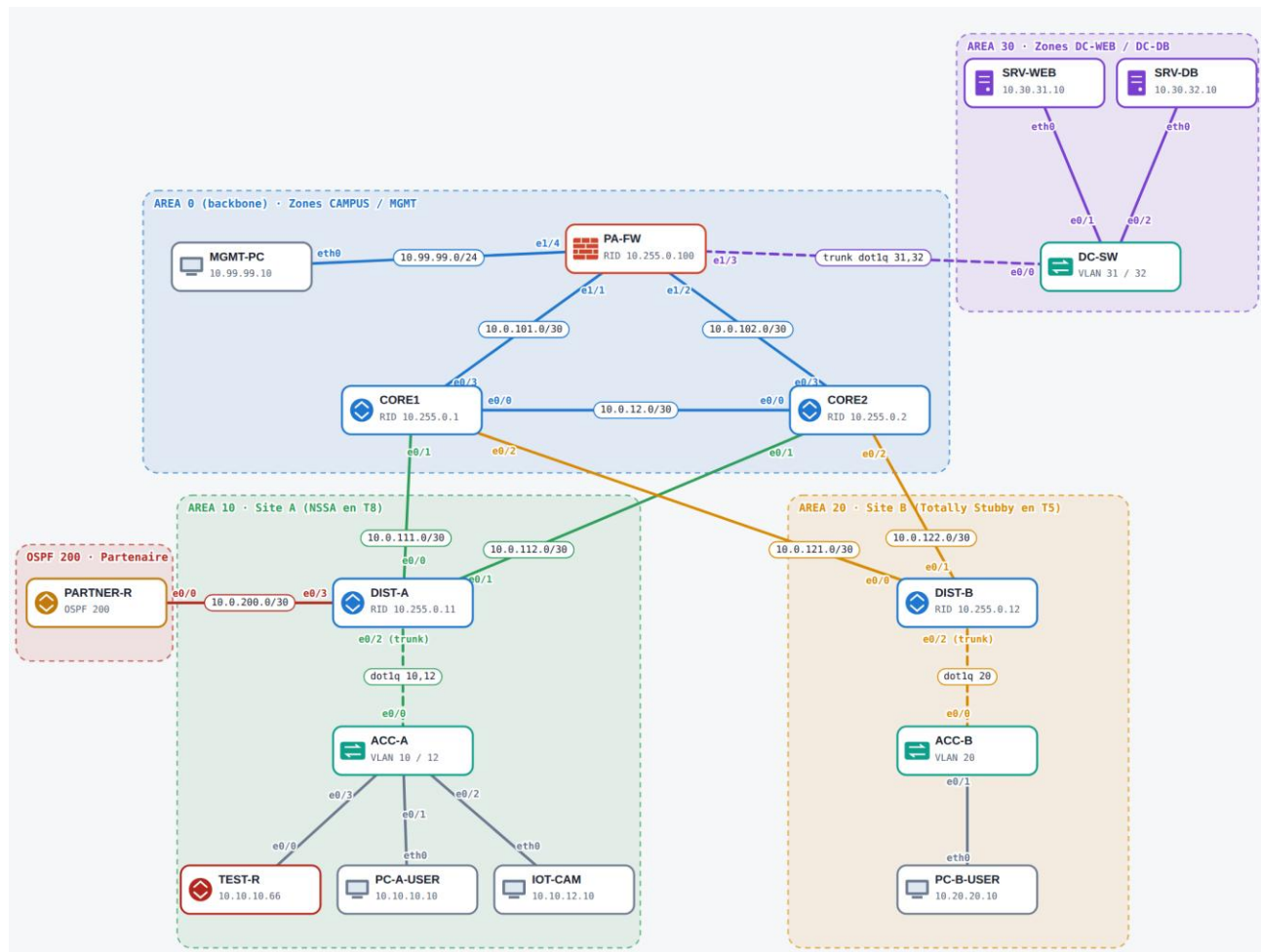
Philosophie du lab

Le routage décide **par où** passe le trafic, le pare-feu décide **s'il** passe. Une segmentation robuste combine les deux : réduction de la surface de routage (need-to-know) + politique de sécurité explicite + intégrité du plan de contrôle.

MASTERY TECH CENTER



2. Topologie



Légende : Area 0 · Area 10 (Site A) · Area 20 (Site B) · Area 30 / DC · OSPF 200 (partenaire) · Accès L2 · Trunk 802.1Q

Chaque lien porte **les interfaces aux deux extrémités** (couleur du domaine) et son sous-réseau. Les liens pointillés sont des trunks 802.1Q. Pour éviter toute confusion au câblage, suis la matrice ci-dessous, pas uniquement le dessin.

Inventaire des équipements

#	Équipement	Rôle	Image PnetLab	RAM conseillée	Interfaces utilisées
1	CORE1	Cœur, ABR area 0/10/20, traducteur NSSA	IOL L3 (i86bi-linux-l3-adventerprisek9 15.x)	512 Mo	e0/0–e0/3
2	CORE2	Cœur, ABR area 0/10/20	IOL L3	512 Mo	e0/0–e0/3
3	DIST-A	Distribution Site A, ASBR (redistribution partenaire)	IOL L3	512 Mo	e0/0–e0/3
4	DIST-B	Distribution Site B	IOL L3	512 Mo	e0/0–e0/2
5	PARTNER-R	Routeur du partenaire (domaine OSPF 200)	IOL L3	512 Mo	e0/0, lo1/2/99
6	TEST-R	Routeur non autorisé (test de validation du durcissement)	IOL L3	512 Mo	e0/0
7	ACC-A	Switch d'accès Site A	IOL L2 (i86bi-linux-l2-adventerprisek9)	512 Mo	e0/0–e0/3
8	ACC-B	Switch d'accès Site B	IOL L2	512 Mo	e0/0–e0/1
9	DC-SW	Switch Datacenter	IOL L2	512 Mo	e0/0–e0/2
10	PA-FW	Pare-feu de segmentation, ABR area 0/30	PA-VM PAN-OS 10.x	2 vCPU / 7 Go	mgmt, e1/1–e1/4
11	MGMT-PC	Poste d'administration	VPCS (ou Linux)	—	eth0
12	PC-A-USER	Utilisateur Site A	VPCS	—	eth0



#	Équipement	Rôle	Image PnetLab	RAM conseillée	Interfaces utilisées
13	IOT-CAM	Caméra IP / objet connecté	VPCS	—	eth0
14	PC-B-USER	Utilisateur Site B	VPCS	—	eth0
15	SRV-WEB	Serveur web / VMS	Linux (Alpine/TinyCore) ou VPCS	256 Mo	eth0
16	SRV-DB	Base de données	Linux ou VPCS	256 Mo	eth0

Matrice de câblage

Lien	Équipement A	Interface A	Équipement B	Interface B	Sous-réseau / VLAN	Domaine
L1	CORE1	e0/0	CORE2	e0/0	10.0.12.0/30 (.1 / .2)	Area 0
L2	CORE1	e0/3	PA-FW	ethernet1/1	10.0.101.0/30 (.1 / .2)	Area 0 · zone CAMPUS
L3	CORE2	e0/3	PA-FW	ethernet1/2	10.0.102.0/30 (.1 / .2)	Area 0 · zone CAMPUS
L4	CORE1	e0/1	DIST-A	e0/0	10.0.111.0/30 (.1 / .2)	Area 10
L5	CORE2	e0/1	DIST-A	e0/1	10.0.112.0/30 (.1 / .2)	Area 10
L6	CORE1	e0/2	DIST-B	e0/0	10.0.121.0/30 (.1 / .2)	Area 20
L7	CORE2	e0/2	DIST-B	e0/1	10.0.122.0/30 (.1 / .2)	Area 20
L8	DIST-A	e0/2 (sous-int.)	ACC-A	e0/0 (trunk)	VLAN 10 + 12	Area 10 (passif)
L9	DIST-A	e0/3	PARTNER-R	e0/0	10.0.200.0/30 (.1 / .2)	OSPF 200
L10	DIST-B	e0/2 (sous-int.)	ACC-B	e0/0 (trunk)	VLAN 20	Area 20 (passif)
L11	PA-FW	ethernet1/3 (sous-int.)	DC-SW	e0/0 (trunk)	VLAN 31 + 32	Area 30 (passif)
L12	PA-FW	ethernet1/4	MGMT-PC	eth0	10.99.99.0/24	Area 0 (passif) · zone MGMT
L13	ACC-A	e0/1	PC-A-USER	eth0	VLAN 10 (access)	—
L14	ACC-A	e0/2	IOT-CAM	eth0	VLAN 12 (access)	—
L15	ACC-A	e0/3	TEST-R	e0/0	VLAN 10 (access)	—
L16	ACC-B	e0/1	PC-B-USER	eth0	VLAN 20 (access)	—
L17	DC-SW	e0/1	SRV-WEB	eth0	VLAN 31 (access)	—
L18	DC-SW	e0/2	SRV-DB	eth0	VLAN 32 (access)	—
MGMT	PA-FW	management	Cloud pnet0	—	IP de ton réseau de gestion	Accès GUI HTTPS

MASTERY TECH CENTER



3. Plan d'adressage

Réseau	Préfixe	Passerelle	Hôtes	Zone PA	Area
Site A – Utilisateurs (VLAN 10)	10.10.10.0/24	10.10.10.1 (DIST-A e0/2.10)	PC-A-USER .10 · TEST-R .66	CAMPUS	10
Site A – IoT (VLAN 12)	10.10.12.0/24	10.10.12.1 (DIST-A e0/2.12)	IOT-CAM .10	CAMPUS	10
Site B – Utilisateurs (VLAN 20)	10.20.20.0/24	10.20.20.1 (DIST-B e0/2.20)	PC-B-USER .10	CAMPUS	20
DC – Web (VLAN 31)	10.30.31.0/24	10.30.31.1 (PA e1/3.31)	SRV-WEB .10	DC-WEB	30
DC – Base de données (VLAN 32)	10.30.32.0/24	10.30.32.1 (PA e1/3.32)	SRV-DB .10	DC-DB	30
Administration	10.99.99.0/24	10.99.99.1 (PA e1/4)	MGMT-PC .10	MGMT	0
Partenaire (contractuel)	172.20.1.0/24, 172.20.2.0/24	—	PARTNER-R lo1 / lo2	CAMPUS (objet PARTNER-NETS)	OSPF 200
Partenaire (NON contractuel)	172.20.99.0/24	—	PARTNER-R lo99	doit être filtré	OSPF 200
Loopbacks / Router-ID	10.255.0.0/24	—	CORE1 .1 · CORE2 .2 · DIST-A .11 · DIST-B .12 · PA .100 (RID) · TEST-R .66	—	selon équipement

1 Choix de design

- Liens de transit en /30 pour la compatibilité PAN-OS / IOL (le /31 est possible côté IOS, RFC 3021).
- Les plages /16 par site (10.10/16, 10.20/16, 10.30/16) sont pensées pour le résumé en T6.
- Mots de passe et clés du lab : valeurs factices — ne publie jamais de vraies clés sur GitHub.

MASTERY TECH CENTER



4. Références officielles

- RFC 2328 — OSPF Version 2 (types de LSA, résumé inter-zone §12.4.3, calcul SPF).
- RFC 3101 — The OSPF Not-So-Stubby Area (NSSA) Option (LSA type 7, traduction 7→5, élection du traducteur).
- RFC 5709 — OSPFv2 HMAC-SHA Cryptographic Authentication.
- Cisco — [OSPFv2 Cryptographic Authentication \(key chain HMAC-SHA\)](#) · IP Routing: OSPF Configuration Guide (IOS / IOS-XE) : area range, filter-list, NSSA, stub.
- Palo Alto Networks — [Configure OSPF](#) · [OSPF Authentication Profile](#) · PAN-OS 10.2 Admin Guide : Security Zones, Zone Protection, Security Policy.
- NIST SP 800-207 (Zero Trust) et CIS Controls v8 (contrôle 12 : gestion de l'infrastructure réseau / segmentation) pour le cadrage sécurité.





5. Tâches

Réalise les tâches dans l'ordre : chacune s'appuie sur la précédente. Essaie d'abord sans ouvrir la solution, puis compare avec les **résultats attendus**.

Tâche 1 · Câblage, VLAN, trunks et adressage

L2 · Hardening L2 · PAN-OS

Objectif : Construire la topologie exactement selon la matrice de câblage, configurer les switches (VLAN, trunks sécurisés), l'adressage IP de tous les routeurs, du Palo Alto et des hôtes.

! Pourquoi ?

- La segmentation commence en couche 2 : VLAN natif « parking » non utilisé, liste de VLAN autorisés explicite, DTP désactivé (switchport nonegotiate), BPDU Guard sur les ports d'accès — recommandations des guides de durcissement Cisco et du CIS Benchmark.
- Le Palo Alto est le **point de contrôle** entre le campus et le DC : chaque segment DC est une sous-interface dans sa propre zone. Pas de routeur entre WEB et DB : tout flux inter-segment passe par la politique de sécurité.

Étapes à réaliser

1. Dans PnetLab, créer les 16 nœuds et les câbler en suivant **strictement** la matrice (interface par interface). Connecter le port *management* du PA à un Cloud (pnet0) pour l'accès GUI.
2. Configurer ACC-A, ACC-B, DC-SW (VLAN, trunks, ports d'accès, ports inutilisés).
3. Configurer les interfaces et sous-interfaces de CORE1, CORE2, DIST-A, DIST-B (pas encore de routage).
4. Configurer sur le PA : profil PING-ONLY, zones, interfaces/sous-interfaces, rattachement au virtual router default. Commit.
5. Configurer les VPCS / serveurs.

Solution

Configurations complètes. Essaie d'abord sans regarder, puis compare.

ACC-A (IOL L2) · IOS

```
hostname ACC-A
no ip domain-lookup
vlan 10
  name SITEA-USERS
vlan 12
  name SITEA-IOT
vlan 999
  name PARKING-NATIVE
!
interface Ethernet0/0
  description TRUNK vers DIST-A e0/2
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 999
  switchport trunk allowed vlan 10,12
  switchport mode trunk
  switchport nonegotiate
!
interface Ethernet0/1
  description PC-A-USER
  switchport mode access
  switchport access vlan 10
  spanning-tree portfast
  spanning-tree bpduguard enable
!
interface Ethernet0/2
  description IOT-CAM
  switchport mode access
  switchport access vlan 12
  spanning-tree portfast
  spanning-tree bpduguard enable
```



```
!  
interface Ethernet0/3  
  description Prise utilisateur (TEST-R branche ici)  
  switchport mode access  
  switchport access vlan 10  
  spanning-tree portfast  
  spanning-tree bpduguard enable  
!  
! Ports non utilises : shutdown + VLAN parking  
interface range Ethernet1/0 - 3  
  switchport mode access  
  switchport access vlan 999  
  shutdown
```

ACC-B (IOL L2) · IOS

```
hostname ACC-B  
vlan 20  
  name SITEB-USERS  
vlan 999  
  name PARKING-NATIVE  
interface Ethernet0/0  
  description TRUNK vers DIST-B e0/2  
  switchport trunk encapsulation dot1q  
  switchport trunk native vlan 999  
  switchport trunk allowed vlan 20  
  switchport mode trunk  
  switchport nonegotiate  
interface Ethernet0/1  
  description PC-B-USER  
  switchport mode access  
  switchport access vlan 20  
  spanning-tree portfast  
  spanning-tree bpduguard enable
```

DC-SW (IOL L2) · IOS

```
hostname DC-SW  
vlan 31  
  name DC-WEB  
vlan 32  
  name DC-DB  
vlan 999  
  name PARKING-NATIVE  
interface Ethernet0/0  
  description TRUNK vers PA-FW ethernet1/3  
  switchport trunk encapsulation dot1q  
  switchport trunk native vlan 999  
  switchport trunk allowed vlan 31,32  
  switchport mode trunk  
  switchport nonegotiate  
interface Ethernet0/1  
  description SRV-WEB  
  switchport mode access  
  switchport access vlan 31  
  spanning-tree portfast  
interface Ethernet0/2  
  description SRV-DB  
  switchport mode access  
  switchport access vlan 32  
  spanning-tree portfast
```

CORE1 · IOS

```
hostname CORE1  
no ip domain-lookup  
interface Loopback0  
  ip address 10.255.0.1 255.255.255.255  
interface Ethernet0/0  
  description L1 vers CORE2 e0/0  
  ip address 10.0.12.1 255.255.255.252  
  no shutdown
```



```
interface Ethernet0/1
  description L4 vers DIST-A e0/0
  ip address 10.0.111.1 255.255.255.252
  no shutdown
interface Ethernet0/2
  description L6 vers DIST-B e0/0
  ip address 10.0.121.1 255.255.255.252
  no shutdown
interface Ethernet0/3
  description L2 vers PA-FW ethernet1/1
  ip address 10.0.101.1 255.255.255.252
  no shutdown
```

CORE2 · IOS

```
hostname CORE2
no ip domain-lookup
interface Loopback0
  ip address 10.255.0.2 255.255.255.255
interface Ethernet0/0
  description L1 vers CORE1 e0/0
  ip address 10.0.12.2 255.255.255.252
  no shutdown
interface Ethernet0/1
  description L5 vers DIST-A e0/1
  ip address 10.0.112.1 255.255.255.252
  no shutdown
interface Ethernet0/2
  description L7 vers DIST-B e0/1
  ip address 10.0.122.1 255.255.255.252
  no shutdown
interface Ethernet0/3
  description L3 vers PA-FW ethernet1/2
  ip address 10.0.102.1 255.255.255.252
  no shutdown
```

DIST-A · IOS

```
hostname DIST-A
no ip domain-lookup
interface Loopback0
  ip address 10.255.0.11 255.255.255.255
interface Ethernet0/0
  description L4 vers CORE1 e0/1
  ip address 10.0.111.2 255.255.255.252
  no shutdown
interface Ethernet0/1
  description L5 vers CORE2 e0/1
  ip address 10.0.112.2 255.255.255.252
  no shutdown
interface Ethernet0/2
  description L8 TRUNK vers ACC-A
  no ip address
  no shutdown
interface Ethernet0/2.10
  description GW SITEA-USERS
  encapsulation dot1Q 10
  ip address 10.10.10.1 255.255.255.0
interface Ethernet0/2.12
  description GW SITEA-IOT
  encapsulation dot1Q 12
  ip address 10.10.12.1 255.255.255.0
interface Ethernet0/3
  description L9 vers PARTNER-R (domaine OSPF 200)
  ip address 10.0.200.1 255.255.255.252
  no shutdown
```

DIST-B · IOS

```
hostname DIST-B
no ip domain-lookup
interface Loopback0
```



```

ip address 10.255.0.12 255.255.255.255
interface Ethernet0/0
description L6 vers CORE1 e0/2
ip address 10.0.121.2 255.255.255.252
no shutdown
interface Ethernet0/1
description L7 vers CORE2 e0/2
ip address 10.0.122.2 255.255.255.252
no shutdown
interface Ethernet0/2
no ip address
no shutdown
interface Ethernet0/2.20
description GW SITEB-USERS
encapsulation dot1Q 20
ip address 10.20.20.1 255.255.255.0

```

PA-FW — GUI (PAN-OS 10.x) · GUI

```

# 1) Network > Network Profiles > Interface Mgmt > Add : PING-ONLY (cocher Ping)
# 2) Network > Zones > Add : CAMPUS, DC-WEB, DC-DB, MGMT (type Layer3)
# 3) Network > Interfaces > Ethernet
#   ethernet1/1 : Layer3, VR default, zone CAMPUS, 10.0.101.2/30, Mgmt profile PING-ONLY
#   ethernet1/2 : Layer3, VR default, zone CAMPUS, 10.0.102.2/30, PING-ONLY
#   ethernet1/3 : Layer3 sans IP, VR default (parent du trunk)
#     ethernet1/3.31 : tag 31, zone DC-WEB, 10.30.31.1/24, PING-ONLY
#     ethernet1/3.32 : tag 32, zone DC-DB, 10.30.32.1/24, PING-ONLY
#   ethernet1/4 : Layer3, VR default, zone MGMT, 10.99.99.1/24, PING-ONLY
# 4) Commit

```

PA-FW — CLI équivalente (mode configure, syntaxe indicative : valider avec TAB) · PAN-OS CLI

```

set network profiles interface-management-profile PING-ONLY ping yes
set network interface ethernet ethernet1/1 layer3 ip 10.0.101.2/30
set network interface ethernet ethernet1/1 layer3 interface-management-profile PING-ONLY
set network interface ethernet ethernet1/2 layer3 ip 10.0.102.2/30
set network interface ethernet ethernet1/2 layer3 interface-management-profile PING-ONLY
set network interface ethernet ethernet1/3 layer3 units ethernet1/3.31 tag 31 ip 10.30.31.1/24
set network interface ethernet ethernet1/3 layer3 units ethernet1/3.31 interface-management-profile PING-ONLY
set network interface ethernet ethernet1/3 layer3 units ethernet1/3.32 tag 32 ip 10.30.32.1/24
set network interface ethernet ethernet1/3 layer3 units ethernet1/3.32 interface-management-profile PING-ONLY
set network interface ethernet ethernet1/4 layer3 ip 10.99.99.1/24
set network interface ethernet ethernet1/4 layer3 interface-management-profile PING-ONLY
set zone CAMPUS network layer3 [ ethernet1/1 ethernet1/2 ]
set zone DC-WEB network layer3 ethernet1/3.31
set zone DC-DB network layer3 ethernet1/3.32
set zone MGMT network layer3 ethernet1/4
set network virtual-router default interface [ ethernet1/1 ethernet1/2 ethernet1/3 ethernet1/3.31
ethernet1/3.32 ethernet1/4 ]
commit

```

VPCS / Linux · hosts

```

PC-A-USER> ip 10.10.10.10/24 10.10.10.1
IOT-CAM> ip 10.10.12.10/24 10.10.12.1
PC-B-USER> ip 10.20.20.10/24 10.20.20.1
MGMT-PC> ip 10.99.99.10/24 10.99.99.1
# (save sur chaque VPCS)
# SRV-WEB (Linux) : ip addr add 10.30.31.10/24 dev eth0 ; ip link set eth0 up ; ip route add default via 10.30.31.1
# SRV-DB (Linux) : ip addr add 10.30.32.10/24 dev eth0 ; ip link set eth0 up ; ip route add default via 10.30.32.1
# Option : SRV-WEB -> python3 -m http.server 80 | SRV-DB -> nc -lk -p 3306

```

Vérification

Vérifications · show



```
ACC-A# show interfaces trunk
ACC-A# show vlan brief
DIST-A# show ip interface brief
DIST-A# ping 10.10.10.10
CORE1# ping 10.0.101.2
PA> show interface all
PA> show interface ethernet1/3.31
```

✓Résultat attendu

- `show interfaces trunk` sur ACC-A : Et0/0 en mode *on*, encapsulation 802.1q, native VLAN 999, VLAN autorisés **10,12** uniquement.
- Tous les liens point-à-point répondent au ping du voisin direct (ex. CORE1 → 10.0.101.2 = PA e1/1 grâce au profil PING-ONLY).
- DIST-A ping 10.10.10.10 et 10.10.12.10 OK ; PC-A-USER ne joint encore **rien** hors de son sous-réseau (aucun routage dynamique).
- PA : `show interface all` liste e1/1, e1/2, e1/3.31, e1/3.32, e1/4 *up*, avec la bonne zone et le VR default.

⚠Pièges / points d'attention

- Dans PnetLab, la 1^{re} interface du PA-VM est le **management** ; ethernet1/1 est la 2^e interface du nœud. Vérifie l'ordre avant de câbler.
- Le PA-VM met plusieurs minutes à démarrer : attendre le prompt `login:` puis encore 2–3 min avant que le GUI réponde.
- Sans profil de gestion d'interface, le PA ne répond pas au ping sur ses interfaces data : ce n'est pas une panne.



MASTERY TECH CENTER



Tâche 2 · OSPF multi-area de base (coûts par défaut)

OSPF · Multi-area · PAN-OS

Objectif : Monter OSPF sur tout le domaine (areas 0, 10, 20, 30) avec le PA comme ABR de l'area 30, puis observer le comportement « par défaut » : ECMP, asymétrie, types de LSA.

i Pourquoi ?

- Liens routeur-routeur en point-to-point : pas d'élection DR/BDR, pas de LSA type 2, convergence plus rapide (recommandation de design pour les liens /30-/31).
- OSPF configuré en mode interface (`ip ospf 1 area X`) : plus lisible, évite les erreurs de wildcard des commandes `network`.
- Les coûts restent par défaut pour **constater** l'ECMP et l'asymétrie, corrigés en tâche 4. Sur IOL, une interface Ethernet est vue à 10 Mb/s : coût par défaut = 10 (référence 100 Mb/s).

Étapes à réaliser

1. Configurer OSPF processus 1 sur CORE1, CORE2, DIST-A, DIST-B (router-id = Loopback0).
2. Configurer OSPF sur le PA (RID 10.255.0.100, area 0 et area 30).
3. Vérifier les adjacences, la LSDB, puis les tables de routage.
4. Depuis DIST-A, afficher la route vers 10.30.31.0/24 et noter le nombre de next-hops.

Solution

Configurations complètes. Essaie d'abord sans regarder, puis compare.

CORE1 · IOS

```
router ospf 1
  router-id 10.255.0.1
  log-adjacency-changes detail
!
interface Loopback0
  ip ospf 1 area 0
interface Ethernet0/0
  ip ospf network point-to-point
  ip ospf 1 area 0
interface Ethernet0/3
  ip ospf network point-to-point
  ip ospf 1 area 0
interface Ethernet0/1
  ip ospf network point-to-point
  ip ospf 1 area 10
interface Ethernet0/2
  ip ospf network point-to-point
  ip ospf 1 area 20
```

CORE2 · IOS

```
router ospf 1
  router-id 10.255.0.2
  log-adjacency-changes detail
interface Loopback0
  ip ospf 1 area 0
interface Ethernet0/0
  ip ospf network point-to-point
  ip ospf 1 area 0
interface Ethernet0/3
  ip ospf network point-to-point
  ip ospf 1 area 0
interface Ethernet0/1
  ip ospf network point-to-point
  ip ospf 1 area 10
interface Ethernet0/2
  ip ospf network point-to-point
  ip ospf 1 area 20
```

**DIST-A · IOS**

```
router ospf 1
  router-id 10.255.0.11
  log-adjacency-changes detail
interface Loopback0
  ip ospf 1 area 10
interface Ethernet0/0
  ip ospf network point-to-point
  ip ospf 1 area 10
interface Ethernet0/1
  ip ospf network point-to-point
  ip ospf 1 area 10
interface Ethernet0/2.10
  ip ospf 1 area 10
interface Ethernet0/2.12
  ip ospf 1 area 10
! Volontairement PAS de passive-interface ici : on corrigera en tache 3
```

DIST-B · IOS

```
router ospf 1
  router-id 10.255.0.12
  log-adjacency-changes detail
interface Loopback0
  ip ospf 1 area 20
interface Ethernet0/0
  ip ospf network point-to-point
  ip ospf 1 area 20
interface Ethernet0/1
  ip ospf network point-to-point
  ip ospf 1 area 20
interface Ethernet0/2.20
  ip ospf 1 area 20
```

PA-FW — GUI · GUI

```
# Network > Virtual Routers > default > OSPF
# [x] Enable Router ID : 10.255.0.100
# Areas > Add 0.0.0.0 (Type : Normal)
#   Interface ethernet1/1 : Enable, Link Type p2p, Metric 10, Passive NON
#   Interface ethernet1/2 : Enable, Link Type p2p, Metric 10, Passive NON
#   Interface ethernet1/4 : Enable, Passive OUI (reseau MGMT annonce, aucune adjacence)
# Areas > Add 0.0.0.30 (Type : Normal)
#   Interface ethernet1/3.31 : Enable, Passive OUI
#   Interface ethernet1/3.32 : Enable, Passive OUI
# Commit -> le PA devient ABR area 0 / area 30
```

PA-FW — CLI indicative · PAN-OS CLI

```
set network virtual-router default protocol ospf enable yes
set network virtual-router default protocol ospf router-id 10.255.0.100
set network virtual-router default protocol ospf area 0.0.0.0 type normal
set network virtual-router default protocol ospf area 0.0.0.0 interface ethernet1/1 enable yes passive no
link-type p2p metric 10
set network virtual-router default protocol ospf area 0.0.0.0 interface ethernet1/2 enable yes passive no
link-type p2p metric 10
set network virtual-router default protocol ospf area 0.0.0.0 interface ethernet1/4 enable yes passive yes
set network virtual-router default protocol ospf area 0.0.0.30 type normal
set network virtual-router default protocol ospf area 0.0.0.30 interface ethernet1/3.31 enable yes passive
yes
set network virtual-router default protocol ospf area 0.0.0.30 interface ethernet1/3.32 enable yes passive
yes
commit
```

Vérification**Vérifications · show**

```
CORE1# show ip ospf neighbor
CORE1# show ip ospf database
```



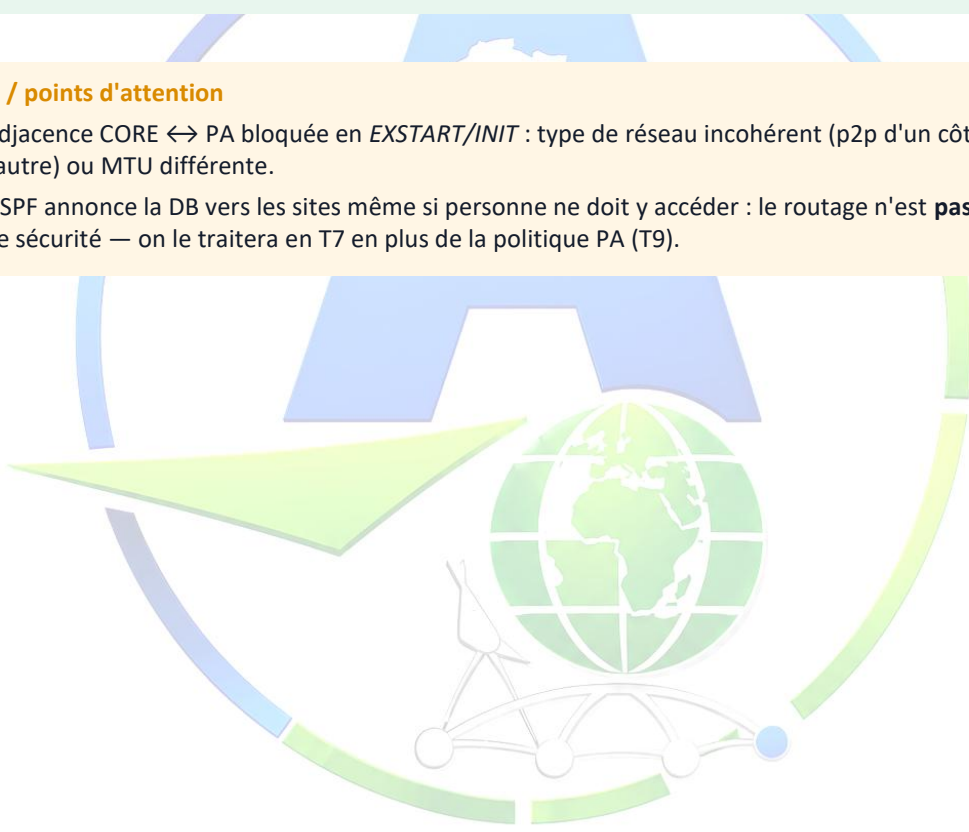
```
CORE1# show ip route ospf
DIST-A# show ip route 10.30.31.0
DIST-A# traceroute 10.30.31.10 source 10.10.10.1
PA> show routing protocol ospf neighbor
PA> show routing route type ospf
```

✓Résultat attendu

- CORE1 : 4 voisins en FULL/ - (CORE2, PA 10.255.0.100, DIST-A, DIST-B) — pas de DR en point-à-point.
- PA : 2 voisins FULL (10.255.0.1 et 10.255.0.2) ; aucune adjacence sur e1/3.x et e1/4 (passives).
- `show ip ospf database` sur CORE1 : LSA Router (type 1) pour chaque area, LSA Summary Net (type 3) pour 10.30.31.0/24 et 10.30.32.0/24 (ADV router 10.255.0.100). **Aucune** LSA type 2.
- DIST-A : 10.30.31.0/24 en **O IA** avec **2 next-hops** (10.0.111.1 et 10.0.112.1) → ECMP.
- PC-A-USER ping 10.20.20.10 OK : le trafic inter-sites ne traverse **pas** le PA. Le ping vers le DC échoue (aucune règle, interzone-default = deny).

⚠Pièges / points d'attention

- Adjacence CORE ↔ PA bloquée en *EXSTART/INIT* : type de réseau incohérent (p2p d'un côté, broadcast de l'autre) ou MTU différente.
- OSPF annonce la DB vers les sites même si personne ne doit y accéder : le routage n'est **pas** une politique de sécurité — on le traitera en T7 en plus de la politique PA (T9).



MASTERY TECH CENTER



Tâche 3 · Durcissement du plan de contrôle OSPF

Sécurité · OSPF · Hardening

Objectif : Garantir qu'aucun équipement non autorisé branché sur une prise utilisateur ne peut former d'adjacence OSPF, et authentifier cryptographiquement toutes les adjacences légitimes.

i Pourquoi ?

- Tant qu'OSPF est actif sur un segment utilisateur, n'importe quel routeur qui y envoie des Hello avec les bons paramètres devient voisin et peut influencer la LSDB : c'est un risque d'intégrité du routage.
- `passive-interface default` + exceptions explicites est la pratique recommandée (approche « deny by default »).
- HMAC-SHA-256 (RFC 5709) remplace MD5, considéré comme faible. Le VR legacy de PAN-OS ne propose que Simple/MD5 : on utilise donc MD5 uniquement sur les liens vers le pare-feu — c'est un compromis à documenter dans ton LLD.

Étapes à réaliser

1. Configurer TEST-R (simple témoin) et constater que DIST-A forme une adjacence avec lui : c'est l'exposition à corriger.
2. Appliquer `passive-interface default` sur DIST-A, DIST-B, CORE1, CORE2 avec les exceptions nécessaires.
3. Configurer la key chain HMAC-SHA-256 sur les liens Cisco ↔ Cisco, MD5 sur CORE ↔ PA (et le profil d'auth côté PA).
4. Vérifier que TEST-R n'a plus aucun voisin et que toutes les adjacences légitimes sont revenues FULL.

Solution

Configurations complètes. Essaie d'abord sans regarder, puis compare.

TEST-R (équipement non autorisé, sert uniquement de témoin) · IOS

```
hostname TEST-R
interface Ethernet0/0
 ip address 10.10.10.66 255.255.255.0
 no shutdown
router ospf 1
 router-id 10.255.0.66
interface Ethernet0/0
 ip ospf 1 area 10
```

DIST-A — durcissement · IOS

```
! 1) Aucune adjacence possible sur les reseaux utilisateurs / IoT
router ospf 1
 passive-interface default
 no passive-interface Ethernet0/0
 no passive-interface Ethernet0/1
!
! 2) Authentification HMAC-SHA-256 (RFC 5709) sur les liens Cisco-Cisco
key chain KC-OSPF
 key 1
  key-string L@b-0spf-2026
  cryptographic-algorithm hmac-sha-256
interface Ethernet0/0
 ip ospf authentication key-chain KC-OSPF
interface Ethernet0/1
 ip ospf authentication key-chain KC-OSPF
```

DIST-B — durcissement · IOS

```
router ospf 1
 passive-interface default
 no passive-interface Ethernet0/0
 no passive-interface Ethernet0/1
key chain KC-OSPF
```



```
key 1
key-string L@b-0spf-2026
cryptographic-algorithm hmac-sha-256
interface Ethernet0/0
ip ospf authentication key-chain KC-OSPF
interface Ethernet0/1
ip ospf authentication key-chain KC-OSPF
```

CORE1 et CORE2 (identique) · IOS

```
router ospf 1
passive-interface default
no passive-interface Ethernet0/0
no passive-interface Ethernet0/1
no passive-interface Ethernet0/2
no passive-interface Ethernet0/3
key chain KC-OSPF
key 1
key-string L@b-0spf-2026
cryptographic-algorithm hmac-sha-256
! Liens Cisco <-> Cisco : HMAC-SHA-256
interface range Ethernet0/0 - 2
ip ospf authentication key-chain KC-OSPF
! Lien vers le Palo Alto : le VR legacy PAN-OS supporte Simple ou MD5 -> MD5
interface Ethernet0/3
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 L@b-PA-Md5
```

PA-FW — GUI · GUI

```
# Network > Virtual Routers > default > OSPF > Auth Profiles > Add
# Name : OSPF-MD5 Password Type : MD5 Key-ID : 1 Key : L@b-PA-Md5 [x] Preferred
# Areas > 0.0.0.0 > ethernet1/1 > Auth Profile : OSPF-MD5
# Areas > 0.0.0.0 > ethernet1/2 > Auth Profile : OSPF-MD5
# Commit
```

Fallback si ton image IOL ne connaît pas 'cryptographic-algorithm' · IOS

```
interface Ethernet0/0
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 L@b-0spf-2026
```

Vérification

Vérifications · show

```
! Avant durcissement
DIST-A# show ip ospf neighbor          ! 10.255.0.66 apparait -> exposition
! Apres durcissement
DIST-A# show ip ospf interface brief
DIST-A# show ip ospf interface Ethernet0/0 | include auth|Cryptographic
TEST-R# show ip ospf neighbor          ! vide
CORE1# show ip ospf neighbor
CORE1# debug ip ospf adj                ! en cas d'echec : "Mismatched authentication"
PA> show routing protocol ospf neighbor
```

✓Résultat attendu

- Avant : show ip ospf neighbor sur DIST-A liste 10.255.0.66 via Et0/2.10 — preuve qu'un segment utilisateur non passif est un point d'entrée sur le plan de contrôle.
- Après : TEST-R n'a **aucun** voisin ; show ip ospf interface brief sur DIST-A montre Et0/2.10 et Et0/2.12 en état passif (0 voisin).
- show ip ospf interface Et0/0 : « Cryptographic authentication enabled » / key chain KC-OSPF avec algorithme HMAC-SHA-256.
- Toutes les adjacences légitimes sont de nouveau FULL (CORE1 : 4 voisins, PA : 2 voisins).



- Les réseaux utilisateurs (10.10.10.0/24, 10.10.12.0/24) restent annoncés : passif ≠ non annoncé.

⚠ Pièges / points d'attention

- Appliquer l'authentification lien par lien des deux côtés en même temps, sinon l'adjacence tombe (« Mismatched authentication type/key »).
- La clé du PA est stockée chiffrée avec la master key ; documente-la dans ton coffre de secrets, pas dans le repo GitHub public (utilise des valeurs factices dans les fichiers publiés).





Tâche 4 · Manipulation de chemin par le coût OSPF — trafic déterministe et symétrique

Path manipulation · OSPF cost

Objectif : Forcer le Site A à utiliser CORE1 et le Site B à utiliser CORE2, dans les deux sens, pour obtenir des flux symétriques à travers le pare-feu.

i Pourquoi ?

- Un pare-feu stateful a besoin de voir l'aller **et** le retour d'une session. Ici, CORE1 et CORE2 arrivent tous deux dans la même zone CAMPUS, mais dans une architecture HA ou multi-zones l'asymétrie casse les sessions et la vérification anti-spoofing.
- Le coût OSPF est appliqué **en sortie** d'interface : pour maîtriser le retour, il faut agir aussi côté CORE (sortie vers DIST).
- Un chemin déterministe facilite le troubleshooting et la lecture des logs.

Étapes à réaliser

1. Relever les chemins actuels (ECMP) depuis DIST-A, DIST-B et le PA.
2. Appliquer les coûts sur DIST-A, DIST-B, CORE1, CORE2 selon le tableau ci-dessous.
3. Vérifier aller et retour par traceroute et par la table de routage du PA.
4. Calculer à la main le coût total DIST-A → 10.30.31.0/24 et le comparer à la sortie IOS.

Solution

Configurations complètes. Essaie d'abord sans regarder, puis compare.

Lien	Coût sortie côté DIST	Coût sortie côté CORE	Rôle
DIST-A ↔ CORE1	10	10	Primaire Site A
DIST-A ↔ CORE2	100	100	Secours Site A
DIST-B ↔ CORE2	10	10	Primaire Site B
DIST-B ↔ CORE1	100	100	Secours Site B

DIST-A · IOS

```
! Site A : chemin primaire via CORE1, secours via CORE2
interface Ethernet0/0
 ip ospf cost 10
interface Ethernet0/1
 ip ospf cost 100
```

DIST-B · IOS

```
! Site B : chemin primaire via CORE2, secours via CORE1
interface Ethernet0/0
 ip ospf cost 100
interface Ethernet0/1
 ip ospf cost 10
```

CORE1 · IOS

```
! Symetrie du trafic retour : le cout est applique en SORTIE d'interface
interface Ethernet0/1
 ip ospf cost 10
interface Ethernet0/2
 ip ospf cost 100
```

CORE2 · IOS

```
interface Ethernet0/1
 ip ospf cost 100
interface Ethernet0/2
```



```
ip ospf cost 10
```

Bonne pratique production (pour info) · IOS

! Sur TOUS les routeurs du domaine, valeur identique (ex. reference 100 Gb/s) :

```
router ospf 1
```

```
auto-cost reference-bandwidth 100000
```

! Dans ce lab IOL (interfaces a 10 Mb/s), on prefere des couts explicites.

Vérification

Vérifications · show

```
DIST-A# show ip route 10.30.31.0
```

```
DIST-A# show ip ospf interface brief
```

```
DIST-B# show ip route 10.30.31.0
```

```
PA> show routing route destination 10.10.10.0/24
```

```
PA> show routing route destination 10.20.20.0/24
```

```
PC-A-USER> trace 10.30.31.10
```

✓Résultat attendu

- DIST-A : 10.30.31.0/24 via **10.0.111.1 uniquement** (Et0/0), métrique 30 = 10 (DIST-A→CORE1) + 10 (CORE1→PA) + 10 (coût passif PA e1/3.31).
- DIST-B : 10.30.31.0/24 via **10.0.122.1 uniquement** (Et0/1), métrique 30.
- PA : 10.10.10.0/24 via 10.0.101.1 (CORE1) ; 10.20.20.0/24 via 10.0.102.1 (CORE2) → retour symétrique.
- Traceroute PC-A-USER → SRV-WEB (une fois la règle T9 en place) : 10.10.10.1 → 10.0.111.1 → 10.0.101.2 → 10.30.31.10.
- Le lien de secours n'apparaît plus dans la RIB mais l'adjacence reste FULL (prête pour la bascule en T10).

⚠Pièges / points d'attention

- Oublier le côté CORE = aller déterministe mais retour en ECMP : symptôme typique, sessions « incomplete » ou « aged-out » dans les logs du PA.
- Si tu modifies `auto-cost reference-bandwidth`, fais-le sur **tous** les routeurs : sinon les coûts deviennent incohérents (IOS l'avertit à la saisie).

MASTERY TECH CENTER



Tâche 5 · Area 20 Totally Stubby et manipulation de la route par défaut

OSPF · Stub · default-cost

Objectif : Réduire la LSDB du Site B à une seule route par défaut, puis choisir quel ABR la fournit en priorité grâce à `area default-cost`.

i Pourquoi ?

- Un site d'extrémité n'a pas besoin de connaître toute la topologie : moins de LSA = moins de CPU, convergence plus rapide, **surface d'information réduite** (le site ne « voit » plus le plan d'adressage du DC).
- Totally Stubby (propriétaire Cisco, `no-summary` sur les ABR) bloque les LSA 3, 4 et 5 et injecte une LSA 3 0.0.0.0/0.
- `default-cost` est un outil de manipulation de chemin : la LSA par défaut porte ce coût, chaque ABR peut annoncer une valeur différente.

Étapes à réaliser

1. Déclarer l'area 20 stub sur DIST-B et stub no-summary sur les deux ABR (le flag stub doit être identique sur tous les routeurs de l'area).
2. Configurer `default-cost 10` sur CORE2 et `100` sur CORE1.
3. Comparer la LSDB et la RIB de DIST-B avant/après.
4. Test : remettre temporairement les coûts d'interface DIST-B à 10/10 et vérifier que `default-cost` suffit à départager.

Solution

Configurations complètes. Essaie d'abord sans regarder, puis compare.

CORE1 · IOS

```
router ospf 1
 area 20 stub no-summary
 area 20 default-cost 100
```

CORE2 · IOS

```
router ospf 1
 area 20 stub no-summary
 area 20 default-cost 10
```

DIST-B · IOS

```
router ospf 1
 area 20 stub
```

Vérification

Vérifications · show

```
DIST-B# show ip route ospf
DIST-B# show ip ospf database summary 0.0.0.0
DIST-B# show ip ospf database | include Summary|External
CORE2# show ip ospf | section Area 20
```

✓Résultat attendu

- DIST-B : la table OSPF ne contient plus que 0*IA 0.0.0.0/0 (plus les routes intra-area 20).
- La LSDB de DIST-B contient 2 LSA Summary 0.0.0.0 : une de 10.255.0.2 (metric 10) et une de 10.255.0.1 (metric 100). Aucune LSA External.
- Route par défaut via 10.0.122.1 (CORE2), métrique 20 (10 interface + 10 default-cost).



- Avec coûts d'interface 10/10 : la route reste via CORE2 (20 contre 110) → default-cost a bien départagé.
- PC-B-USER joint toujours le DC et le Site A (via la route par défaut).

⚠ Pièges / points d'attention

- Si l'adjacence DIST-B ↔ CORE tombe après la commande : le flag stub (bit E dans les Hello) ne correspond pas des deux côtés.
- Une area stub ne peut contenir ni ASBR ni lien virtuel.





Tâche 6 · Résumé inter-zone (area range) et manipulation du coût du résumé

OSPF · Summarization

Objectif : Résumer chaque site en un seul préfixe vers le backbone et rendre CORE1 préférentiel pour le résumé du Site A grâce au paramètre `cost` de `area range`.

i Pourquoi ?

- Le résumé stabilise le backbone (une instabilité d'un /24 du site ne déclenche plus de recalcul dans les autres areas) et réduit la taille des tables.
- Le coût d'un résumé est dérivé des coûts des composants (RFC 2328 §12.4.3 : coût le plus élevé ; certaines implémentations en compatibilité RFC 1583 prennent le plus faible). Le fixer explicitement avec `cost` rend le comportement prévisible et devient un outil de manipulation de chemin.
- IOS installe automatiquement une route **discard** (Null0) pour le résumé sur l'ABR : protection anti-boucle pour les sous-réseaux non utilisés du /16.

Étapes à réaliser

1. Relever sur le PA les routes 10.10.x et 10.20.x (plusieurs /24).
2. Configurer les `area range` sur CORE1 et CORE2 (avec `cost 500` sur CORE2 pour l'area 10).
3. Vérifier la LSDB du PA, sa table de routage, et la route Null0 sur les ABR.
4. Tester un ping vers une adresse non utilisée, 10.10.50.1, depuis MGMT-PC (après T9) : observer où le paquet est détruit.

Solution

Configurations complètes. Essaie d'abord sans regarder, puis compare.

CORE1 · IOS

```
router ospf 1
 area 10 range 10.10.0.0 255.255.0.0
 area 20 range 10.20.0.0 255.255.0.0
```

CORE2 (summary dissuasif) · IOS

```
router ospf 1
 area 10 range 10.10.0.0 255.255.0.0 cost 500
 area 20 range 10.20.0.0 255.255.0.0
```

PA-FW — GUI (optionnel : résumé de l'area 30) · GUI

```
# Network > Virtual Routers > default > OSPF > Areas > 0.0.0.30 > Range
# Add : 10.30.0.0/16 Action : Advertise
# (Ne le fais qu'APRES la tâche 7, voir le piège ci-dessous)
```

Vérification

Vérifications · show

```
CORE1# show ip route 10.10.0.0 255.255.0.0
CORE1# show ip ospf database summary 10.10.0.0
PA> show routing route type ospf
PA> show routing protocol ospf dump lsdb
```

✓Résultat attendu

- PA : un seul préfixe 10.10.0.0/16 (au lieu de 10.10.10.0/24 + 10.10.12.0/24) et un seul 10.20.0.0/16.
- PA : 10.10.0.0/16 via **10.0.101.1 (CORE1)**, métrique ≈ 10 + coût du résumé CORE1 ; la LSA de CORE2 annonce metric 500 → non retenue.



- CORE1 : 0 10.10.0.0/16 is a summary, ... Null0 (route discard locale).
- Ping vers 10.10.50.1 : le paquet est jeté sur CORE1 (Null0), aucune boucle entre CORE et PA.

⚠ Pièges / points d'attention

- Si tu ajoutes le résumé 10.30.0.0/16 sur le PA, le préfixe DB disparaît dans le résumé : le filtrage par préfixe de la tâche 7 ne pourrait plus le cibler. Choisis l'un ou l'autre selon ton design (ici : pas de résumé area 30).
- Les liens de transit 10.0.111.0/30 et 10.0.112.0/30 n'entrent pas dans 10.10.0.0/16 : ils restent annoncés individuellement — normal.





Tâche 7 · Filtrage des LSA type 3 (filter-list) vs filtrage RIB (distribute-list)

Filtrage · prefix-list · Need-to-know routing

Objectif : Appliquer le principe de « need-to-know » au routage : le Site A ne reçoit pas de route vers la DB, et aucun préfixe du DC ne peut être annoncé depuis l'area 10. Puis comprendre la différence fondamentale avec distribute-list.

i Pourquoi ?

- area X filter-list prefix ... in|out agit sur l'ABR et filtre la **génération des LSA type 3** : la LSDB de l'area est réellement modifiée.
- distribute-list ... in sous OSPF ne filtre que l'installation dans la **RIB locale** : la LSA reste dans la LSDB et continue d'être inondée aux voisins (OSPF est link-state, tous les routeurs d'une area doivent avoir la même LSDB).
- Les prefix-lists sont l'outil recommandé pour filtrer des préfixes (plus lisibles et plus efficaces que les ACL, gestion précise de la longueur avec ge/le).
- Le filtre out est une garde-fou : même par erreur de configuration, un routeur du Site A ne pourra pas propager de préfixe 10.30.x.x vers le backbone.

Étapes à réaliser

1. Créer les prefix-lists et appliquer les filter-list in/out sur les deux ABR.
2. Vérifier sur DIST-A que 10.30.32.0/24 a disparu de la LSDB **et** de la RIB, alors que 10.30.31.0/24 est toujours présent.
3. Sur DIST-A, appliquer la distribute-list de comparaison : constater que 10.99.99.0/24 quitte la RIB mais reste dans la LSDB. Puis la retirer.
4. Expliquer pourquoi PC-B-USER (Site B) atteint quand même la DB au niveau routage (route par défaut) — et pourquoi ce n'est pas grave grâce au PA (T9).

Solution

Configurations complètes. Essaie d'abord sans regarder, puis compare.

CORE1 et CORE2 (identique) · IOS

```
! (a) Ce qui ENTRE dans l'area 10 : pas de route vers la DB pour le Site A
ip prefix-list PL-AREA10-IN seq 5 deny 10.30.32.0/24
ip prefix-list PL-AREA10-IN seq 100 permit 0.0.0.0/0 le 32
!
! (b) Ce qui SORT de l'area 10 : le Site A ne doit jamais annoncer l'espace DC
ip prefix-list PL-AREA10-OUT seq 5 deny 10.30.0.0/16 le 32
ip prefix-list PL-AREA10-OUT seq 100 permit 0.0.0.0/0 le 32
!
router ospf 1
 area 10 filter-list prefix PL-AREA10-IN in
 area 10 filter-list prefix PL-AREA10-OUT out
```

DIST-A — comparaison : distribute-list (filtre RIB local) · IOS

```
ip prefix-list PL-RIB-NO-MGMT seq 5 deny 10.99.99.0/24
ip prefix-list PL-RIB-NO-MGMT seq 100 permit 0.0.0.0/0 le 32
router ospf 1
 distribute-list prefix PL-RIB-NO-MGMT in
! Observer puis RETIRER (le Site A doit pouvoir répondre au MGMT) :
! no distribute-list prefix PL-RIB-NO-MGMT in
```

Vérification

Vérifications · show

```
DIST-A# show ip ospf database summary 10.30.32.0
DIST-A# show ip route 10.30.32.0
DIST-A# show ip route 10.30.31.0
CORE1# show ip prefix-list detail PL-AREA10-IN
! Pendant le test distribute-list :
```



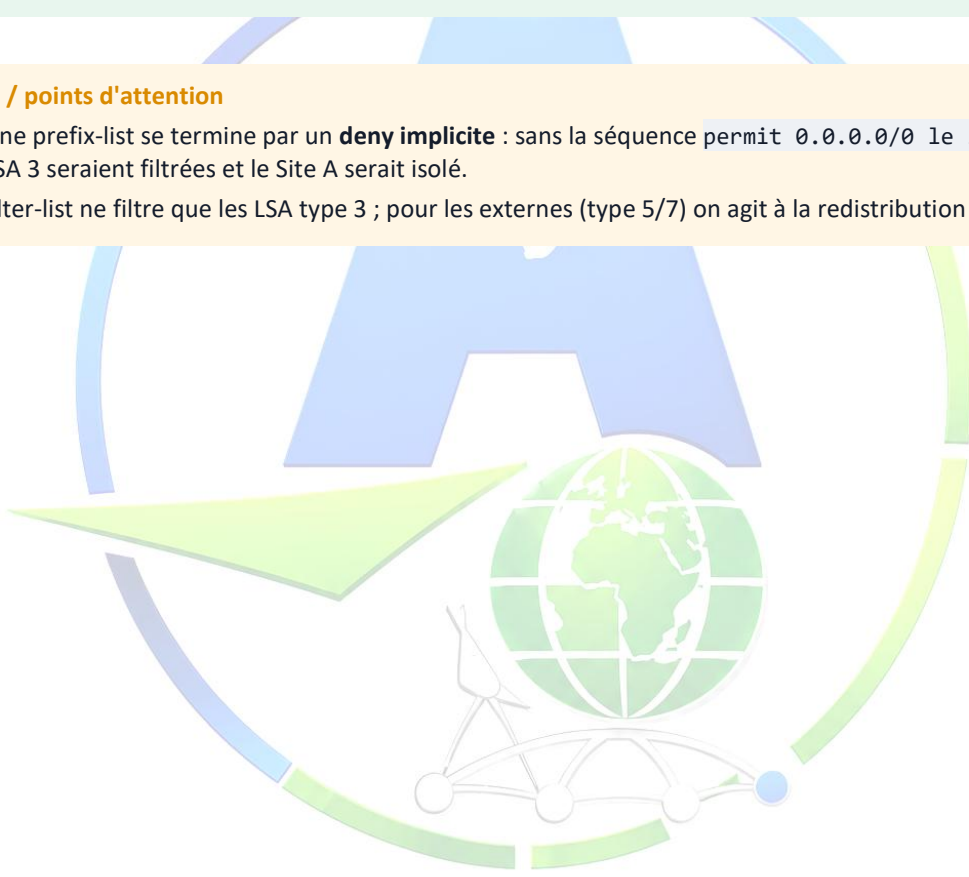
```
DIST-A# show ip route 10.99.99.0
DIST-A# show ip ospf database summary 10.99.99.0
```

✓Résultat attendu

- DIST-A : `show ip ospf database summary 10.30.32.0` → aucune LSA ; `show ip route 10.30.32.0` → « % Subnet not in table ».
- DIST-A : 10.30.31.0/24 toujours présent en O IA via CORE1.
- `show ip prefix-list detail` : compteur *hit count* > 0 sur la séquence 5.
- Test distribute-list : 10.99.99.0/24 absent de la RIB de DIST-A **mais présent** dans sa LSDB → démonstration de la différence.
- PC-B-USER → 10.30.32.10 : le paquet atteint le PA via la route par défaut ; c'est la politique PA (T9) qui le bloquera. Conclusion : filtrage de routage = réduction de surface, pare-feu = contrôle d'accès.

⚠Pièges / points d'attention

- Une prefix-list se termine par un **deny implicite** : sans la séquence `permit 0.0.0.0/0 le 32`, toutes les LSA 3 seraient filtrées et le Site A serait isolé.
- filter-list ne filtre que les LSA type 3 ; pour les externes (type 5/7) on agit à la redistribution (T8).



MASTERY TECH CENTER



Tâche 8 · NSSA + redistribution contrôlée d'un partenaire (route-maps, tags, metric-type)

NSSA · Redistribution · route-map · tags

Objectif : Raccorder le domaine OSPF d'un partenaire en n'acceptant **que** ses préfixes contractuels, sans jamais accepter de route par défaut ni de préfixe chevauchant notre plan d'adressage, et en n'exposant que SRV-WEB.

i Pourquoi ?

- L'area 10 contient désormais un ASBR : elle ne peut pas être stub, mais NSSA permet de garder un périmètre réduit (pas de LSA 5 venant de l'extérieur) tout en autorisant la redistribution locale (LSA type 7, RFC 3101).
- L'ABR NSSA traduit les LSA 7 en LSA 5. Par défaut, c'est l'ABR au plus grand router-id (CORE2) ; `translate type7` `always` rend CORE1 traducteur de manière déterministe.
- Trois couches de contrôle : **distribute-list** (ce qui entre dans la RIB), **route-map de redistribution** (ce qui est exporté, avec tag/metric-type), **tags** (anti-boucle si un 2^e point de redistribution est ajouté un jour).
- Metric-type E1 : le coût interne jusqu'à l'ASBR s'ajoute → meilleur choix si plusieurs points de sortie existent. Une redistribution ne propage jamais la route par défaut sans `default-information originate` explicite.
- Bonne pratique : avec une organisation tierce, préférer eBGP (frontière de politique claire). OSPF est utilisé ici pour maîtriser les outils de redistribution.

Étapes à réaliser

1. Configurer PARTNER-R tel que fourni (il annonce volontairement des éléments indésirables : 0.0.0.0/0, 172.20.99.0/24, 10.30.32.0/24).
2. Passer l'area 10 en NSSA sur CORE1, CORE2, DIST-A (CORE1 traducteur forcé).
3. Monter l'adjacence OSPF 200 DIST-A ↔ PARTNER-R (router-id distinct pour le process 200).
4. Appliquer la `distribute-list`, puis les deux `route-maps` de redistribution, puis le `summary-address`.
5. Vérifier la LSDB (type 7 sur DIST-A, type 5 sur CORE1/PA), les tags, et l'absence de tout préfixe non désiré.
6. Vérifier que PARTNER-R ne reçoit que 10.30.31.0/24.

Solution

Configurations complètes. Essaie d'abord sans regarder, puis compare.

PARTNER-R (configuration du partenaire, imposée) · IOS

```
hostname PARTNER-R
interface Loopback1
  description Reseau contractuel 1
  ip address 172.20.1.1 255.255.255.0
  ip ospf network point-to-point
interface Loopback2
  description Reseau contractuel 2
  ip address 172.20.2.1 255.255.255.0
  ip ospf network point-to-point
interface Loopback99
  description Reseau de test NON contractuel
  ip address 172.20.99.1 255.255.255.0
  ip ospf network point-to-point
interface Ethernet0/0
  ip address 10.0.200.2 255.255.255.252
  ip ospf network point-to-point
  no shutdown
! Erreur de configuration du partenaire : une route statique qui chevauche notre DB
ip route 10.30.32.0 255.255.255.0 Null0
router ospf 200
  router-id 172.20.255.1
  network 10.0.200.0 0.0.0.3 area 0
  network 172.20.0.0 0.0.255.255 area 0
  redistribute static subnets
  default-information originate always
```

**CORE1 (traducteur NSSA forcé) · IOS**

```
router ospf 1
 area 10 nssa translate type7 always
```

CORE2 · IOS

```
router ospf 1
 area 10 nssa
```

DIST-A — process 200 + redistribution sécurisée · IOS

```
router ospf 1
 area 10 nssa
!
interface Ethernet0/3
 ip ospf network point-to-point
 ip ospf 200 area 0
!
! ----- Couche 1 : filtre RIB sur ce qui vient du partenaire
ip prefix-list PL-FROM-PARTNER seq 5 deny 172.20.99.0/24
ip prefix-list PL-FROM-PARTNER seq 10 permit 172.20.0.0/16 ge 24 le 24
! (tout le reste - 0.0.0.0/0, 10.30.32.0/24 ... - est refuse par le deny implicite)
router ospf 200
 router-id 10.255.200.11
 distribute-list prefix PL-FROM-PARTNER in
!
! ----- Couche 2 : partenaire -> notre domaine (tag 200, E1, metrique fixe)
route-map RM-P200-TO-P1 permit 10
 match ip address prefix-list PL-FROM-PARTNER
 set metric 20
 set metric-type type-1
 set tag 200
route-map RM-P200-TO-P1 deny 100
!
! ----- Couche 3 : notre domaine -> partenaire (seulement SRV-WEB, anti-boucle par tag)
ip prefix-list PL-TO-PARTNER seq 10 permit 10.30.31.0/24
route-map RM-P1-TO-P200 deny 5
 match tag 200
route-map RM-P1-TO-P200 permit 10
 match ip address prefix-list PL-TO-PARTNER
 set tag 1
route-map RM-P1-TO-P200 deny 100
!
router ospf 1
 redistribute ospf 200 subnets route-map RM-P200-TO-P1
 summary-address 172.20.0.0 255.255.0.0
router ospf 200
 redistribute ospf 1 subnets route-map RM-P1-TO-P200
```

Vérification**Vérifications · show**

```
DIST-A# show ip ospf 200 neighbor
DIST-A# show ip route ospf 200
DIST-A# show ip ospf database nssa-external
DIST-A# show route-map RM-P200-TO-P1
CORE1# show ip ospf | include translation|Translator
CORE1# show ip ospf database external 172.20.0.0
PA> show routing route destination 172.20.0.0/16
PARTNER-R# show ip route ospf
PARTNER-R# ping 10.30.31.10 source 172.20.1.1
```

✓Résultat attendu

- show ip route ospf 200 sur DIST-A : uniquement 172.20.1.0/24 et 172.20.2.0/24. **Absents** : 0.0.0.0/0, 172.20.99.0/24, 10.30.32.0/24.



- DIST-A : `show ip ospf database nssa-external` → une LSA type 7 **172.20.0.0/16** (summary-address), Metric Type 1, metric 20, **Tag 200**.
- CORE1 : « Perform type-7/type-5 LSA translation » ; `database external 172.20.0.0` → Advertising Router **10.255.0.1** (CORE1 = traducteur).
- PA : 172.20.0.0/16 en route OSPF externe type 1 via 10.0.101.1.
- PARTNER-R : seule route reçue de notre domaine = 0 E2 10.30.31.0/24 ; aucune visibilité sur 10.10.x, 10.20.x, 10.30.32.x, 10.99.x.
- `show route-map` : compteurs de correspondance qui augmentent sur les séquences permit/deny attendues.

⚠ Pièges / points d'attention

- Deux processus OSPF sur le même routeur ne doivent pas avoir le même router-id : fixe-le explicitement pour le process 200.
- Oublier subnets sur IOS 15.x = seules les routes classful sont redistribuées (sur IOS-XE 17, subnets est implicite).
- Le summary-address 172.20.0.0/16 couvre aussi 172.20.99.0/24 : le trafic vers ce réseau sera jeté sur DIST-A (route Null0 du résumé), ce qui est le comportement souhaité.
- L'adresse de transfert (Forwarding Address) des LSA traduites doit être joignable en intra/inter-area depuis le PA ; sinon la route externe n'est pas installée.





Tâche 9 · Segmentation Palo Alto : zones, politiques App-ID, Zone Protection, ACL IoT

PAN-OS · Zero Trust · Segmentation

Objectif : Mettre en œuvre une matrice de flux « moindre privilège » entre CAMPUS, DC-WEB, DC-DB et MGMT, journaliser les refus, protéger la zone CAMPUS et contraindre l'IoT dès la passerelle.

i Pourquoi ?

- La zone est liée à l'interface : partenaire et utilisateurs arrivent tous par la zone CAMPUS → on différencie par **objets d'adresse**. C'est pourquoi la cohérence du routage (T4–T8) conditionne la sécurité.
- App-ID + application-default : l'application doit utiliser son port standard (bonne pratique PAN-OS de la Policy Optimizer / Best Practice Assessment).
- La règle par défaut interzone est deny mais **ne journalise pas** : on la surcharge pour avoir la visibilité.
- Le contrôle « Spoofed IP address » de la Zone Protection s'appuie sur la table de routage : une route manquante ou asymétrique peut faire jeter du trafic légitime.
- Le trafic Site A ↔ Site B ne traverse pas le PA : l'ACL sur la passerelle IoT est un contrôle complémentaire. Le Lab 2 montre la solution complète (VRF-lite + firewall).

Étapes à réaliser

1. Créer les objets d'adresse.
2. Créer les règles R01 → R90 dans cet ordre, puis surcharger interzone-default (Deny + log).
3. Créer et appliquer le profil de Zone Protection sur CAMPUS.
4. Appliquer l'ACL IoT sur DIST-A.
5. Valider chaque flux avec `test security-policy-match` puis par des tests réels.

Solution

Configurations complètes. Essaie d'abord sans regarder, puis compare.

PA-FW — objets · GUI

```
# Objects > Addresses
# SITE-A-USERS    10.10.10.0/24
# SITE-A-IOT      10.10.12.0/24
# SITE-B-USERS    10.20.20.0/24
# PARTNER-NETS    172.20.0.0/16
# SRV-WEB         10.30.31.10/32
# SRV-DB          10.30.32.10/32
# MGMT-NET        10.99.99.0/24
```

Règle	Zone src	Source	Zone dst	Destination	Application	Service	Action
R01-MGMT-ADMIN	MGMT	MGMT-NET	CAMPUS, DC-WEB, DC-DB	any	ssh, ping, traceroute, snmp	application-default	Allow
R10-USERS-TO-WEB	CAMPUS	SITE-A-USERS, SITE-B-USERS	DC-WEB	SRV-WEB	web-browsing, ssl, ping	application-default	Allow
R15-IOT-TO-VMS	CAMPUS	SITE-A-IOT	DC-WEB	SRV-WEB	ssl	application-default	Allow
R20-PARTNER-TO-WEB	CAMPUS	PARTNER-NETS	DC-WEB	SRV-WEB	ssl, ping	application-default	Allow
R30-WEB-TO-DB	DC-WEB	SRV-WEB	DC-DB	SRV-DB	mysql	application-default	Allow
R90-DENY-TO-DB	any	any	DC-DB	any	any	any	Deny + log
interzone-default (override)	—	—	—	—	—	—	Deny + Log at Session End

PA-FW — CLI indicative (extrait) · PAN-OS CLI



```

set rulebase security rules R10-USERS-TO-WEB from CAMPUS to DC-WEB source [ SITE-A-USERS SITE-B-USERS ]
destination SRV-WEB application [ web-browsing ssl ping ] service application-default action allow log-end
yes
set rulebase security rules R30-WEB-TO-DB from DC-WEB to DC-DB source SRV-WEB destination SRV-DB
application mysql service application-default action allow log-end yes
set rulebase security rules R90-DENY-TO-DB from any to DC-DB source any destination any application any
service any action deny log-end yes
set rulebase default-security-rules rules interzone-default action deny log-end yes

```

PA-FW — Zone Protection (GUI) · GUI

```

# Network > Network Profiles > Zone Protection > Add : ZP-INTERNAL
# Flood Protection : SYN (SYN Cookies), ICMP, UDP -> seuils adaptes au lab
# Reconnaissance Protection : TCP Port Scan, Host Sweep -> action block-ip (Track By: source)
# Packet Based Attack Protection > IP Drop :
# [x] Spoofed IP address [x] Strict IP Address Check [x] Unknown / Malformed option
# Network > Zones > CAMPUS > Zone Protection Profile : ZP-INTERNAL
# Commit

```

DIST-A — ACL de bordure pour l'IoT (contrôle au plus près de la source) · IOS

```

ip access-list extended ACL-IOT-IN
remark IoT : uniquement le VMS (SRV-WEB) en HTTPS + ping de la passerelle
permit icmp 10.10.12.0 0.0.0.255 host 10.10.12.1 echo
permit tcp 10.10.12.0 0.0.0.255 host 10.30.31.10 eq 443
deny ip any any log
interface Ethernet0/2.12
ip access-group ACL-IOT-IN in

```

Vérification

Vérifications · show

```

PA> test security-policy-match from CAMPUS to DC-WEB source 10.10.10.10 destination 10.30.31.10 protocol 6
destination-port 443 application ssl
PA> test security-policy-match from CAMPUS to DC-DB source 10.10.10.10 destination 10.30.32.10 protocol 6
destination-port 3306
PA> test security-policy-match from DC-WEB to DC-DB source 10.30.31.10 destination 10.30.32.10 protocol 6
destination-port 3306 application mysql
PA> test security-policy-match from CAMPUS to DC-WEB source 172.20.1.1 destination 10.30.31.10 protocol 1
PA> show session all filter destination 10.30.31.10
# GUI : Monitor > Traffic, filtre ( action eq deny )
DIST-A# show ip access-lists ACL-IOT-IN
PC-A-USER> ping 10.30.31.10
PC-A-USER> ping 10.30.32.10
IOT-CAM> ping 10.20.20.10
MGMT-PC> ping 10.30.32.10

```

✓Résultat attendu

- test-match : utilisateur → WEB ssl = **R10-USERS-TO-WEB** ; utilisateur → DB 3306 = **R90-DENY-TO-DB** ; WEB → DB mysql = **R30-WEB-TO-DB** ; partenaire ping WEB = **R20-PARTNER-TO-WEB**.
- PC-A-USER → 10.30.31.10 : ping OK. PC-A-USER → 10.30.32.10 : échec (déjà sans route depuis T7) ; PC-B-USER → 10.30.32.10 : échec avec log deny R90 dans Monitor > Traffic.
- MGMT-PC → 10.30.32.10 : ping OK (R01).
- IOT-CAM → 10.20.20.10 : échec, compteur de la ligne deny ip any any log de ACL-IOT-IN incrémenté.
- PARTNER-R ping 10.30.31.10 source 172.20.1.1 : OK, session visible avec la règle R20.
- Aucun flux inattendu « allow » dans les logs : chaque session autorisée correspond à une règle nommée de la matrice.

⚠Pièges / points d'attention



- Avec VPCS, seul ICMP est testable : utilise `test security-policy-match` pour les applications, ou des hôtes Linux (curl, nc) pour un test App-ID réel.
- Un serveur HTTP en clair sur le port 443 sera identifié *web-browsing* sur un port non standard → refusé avec application-default : comportement attendu, pas un bug.
- Ordre des règles : R90 doit rester sous R30, sinon WEB → DB est bloqué.



MASTERY TECH CENTER



Tâche 10 · Tests de bascule et validation finale

Résilience · Validation

Objectif : Vérifier que la manipulation de chemin reste cohérente en cas de panne et que les contrôles de sécurité restent actifs pendant et après la bascule.

i Pourquoi ?

- Un design de segmentation n'est valide que s'il reste correct en mode dégradé : une bascule ne doit ni ouvrir de flux ni créer d'asymétrie durable.

Étapes à réaliser

1. Lancer un ping -t (ou VPCS ping 10.30.31.10 -t) depuis PC-A-USER vers SRV-WEB.
2. Couper le lien primaire du Site A : CORE1(config)# interface e0/1 → shutdown. Mesurer les pertes, vérifier le nouveau chemin aller et retour. Rétablir.
3. Arrêter complètement CORE1 (stop du nœud) : vérifier que CORE2 devient traducteur NSSA et que 172.20.0.0/16 reste joignable depuis le PA.
4. Option : activer BFD sur les liens CORE ↔ DIST (bfd interval 300 min_rx 300 multiplier 3 + ip ospf bfd) et comparer le temps de convergence.
5. Rejouer la checklist de validation en bas de page.

Vérification

Vérifications · show

```
DIST-A# show ip route 10.30.31.0
PA> show routing route destination 10.10.0.0/16
CORE2# show ip ospf | include translation
CORE2# show ip ospf database external 172.20.0.0
PA> show routing route destination 172.20.0.0/16
DIST-A# show bfd neighbors
```

✓Résultat attendu

- Lien CORE1–DIST-A coupé : DIST-A bascule vers 10.0.112.1 (métrique 120 = 100 + 10 + 10) ; le PA reçoit le résumé 10.10.0.0/16 uniquement de CORE2 (coût 500) et l'utilise → retour symétrique via CORE2.
- Pertes ≈ temps de détection (dead-interval 40 s par défaut sur p2p si la panne n'est pas vue en couche 1, ~1 s avec BFD).
- CORE1 arrêté : CORE2 « Perform type-7/type-5 LSA translation », LSA 5 172.20.0.0 annoncée par 10.255.0.2.
- Pendant toute la bascule, PC-A-USER → SRV-DB reste refusé et les logs R90 continuent d'apparaître.
- Après rétablissement, retour au chemin nominal (CORE1) sans intervention.

⚠Pièges / points d'attention

- Si le ping reprend mais que les sessions TCP existantes cassent après bascule, vérifie que les deux interfaces du PA vers les CORE sont bien dans la **même zone** (CAMPUS).



6. Checklist de validation finale

- ☐ Tous les nœuds câblés selon la matrice ; trunks limités aux VLAN nécessaires, VLAN natif 999
- ☐ Adjacences OSPF : CORE1 = 4, CORE2 = 4, PA = 2, DIST-A = 2 (+1 en process 200), DIST-B = 2
- ☐ Aucune adjacence possible depuis un port utilisateur (TEST-R sans voisin)
- ☐ Authentification HMAC-SHA-256 entre Cisco, MD5 vers le PA
- ☐ Site A via CORE1, Site B via CORE2, aller ET retour
- ☐ DIST-B ne voit qu'une route par défaut, fournie par CORE2
- ☐ PA voit 10.10.0.0/16 et 10.20.0.0/16 (résumés), préférence CORE1 pour 10.10.0.0/16
- ☐ 10.30.32.0/24 absent de la LSDB de l'area 10
- ☐ Seuls 172.20.1.0/24 et 172.20.2.0/24 importés (résumés en 172.20.0.0/16, tag 200, E1)
- ☐ PARTNER-R ne voit que 10.30.31.0/24
- ☐ Matrice de flux PA validée par test security-policy-match + logs deny
- ☐ IoT limité au VMS en HTTPS (ACL + règle R15)
- ☐ Bascules testées, sécurité inchangée en mode dégradé

🍷 Ce lab t'a été utile ?

Tous les labs Mastery Tech Center sont gratuits, solutions comprises. Tu peux soutenir la création des prochains en offrant un café :

ko-fi.com/masterytechcenter

MASTERY TECH CENTER