Workbook: LAB_Integrazione_Brownfield-Greenfield_con_DCI_VXLAN

1. 🎯 Obiettivo del Laboratorio

Questo workbook descrive i passaggi per costruire un'architettura di rete ibrida complessa. L'obiettivo è espandere un sito "Brownfield" esistente (un campus OSPF multi-area) e collegarlo a un nuovo Datacenter "Greenfield" costruito con una moderna fabric L3 Spine-Leaf.

La connettività tra i due siti è assicurata da un tunnel VPN IPsec. L'obiettivo finale è implementare un Data Center Interconnect (DCI) utilizzando VXLAN per estendere un dominio L2 (VLAN 100) attraverso l'infrastruttura L3 e il tunnel VPN, permettendo la comunicazione L2 tra host in siti fisici separati.

2. 🛠️ Prerequisiti (Immagini PNetLab)

- **Router Cisco (IOL L3):** Per i router del Building A (R1-R9) e la fabric Spine-Leaf del Building B (SPINE-1, LEAF-1, ecc.).
- **Firewall (FortiGate VM):** 2x (FGT-A, FGT-B) per il perimetro e la VPN.
- **Switch VTEP (Arista vEOS):** 2x (VTEP-DC1, VTEP-DC2) per la gestione dell'overlay VXLAN.
- **Host (Docker):** 2x (Host-A, Host-B) per i test L2.

3. 🗺️ Piano di Indirizzamento IP

Building A (Brownfield) - Principali Link OSPF

Dispositivo	Interfaccia	Indirizzo IP	Area OSPF
R1	Loopback0	192.168.0.1/32	Area 0
	Ethernet0/0	10.255.0.1/24	Area 0 (a FGT-A)
R2 (ABR)	Loopback0	192.168.0.2/32	Area 0
	Ethernet0/0	10.2.27.2/24	Area 2
	Ethernet0/3	10.1.24.2/24	Area 1
R8	Loopback0	192.168.0.8/32	Area 2
	Ethernet0/0	10.2.8.1/30	Area 2 (a VTEP-DC1)
R9	Loopback0	192.168.0.9/32	Area 2
	Ethernet0/0	10.2.9.1/30	Area 2 (a VTEP-DC1)

Zona WAN e Perimetro

Dispositivo	Interfaccia	Indirizzo IP	Note
R-ISP	Ethernet0/0	100.64.1.1/24	Link a FGT-A
	Ethernet0/1	DHCP	Internet (NAT Outside)
	Ethernet0/2	100.64.2.1/24	Link a FGT-B
FGT-A	port2 (WAN)	100.64.1.2/24	GW: 100.64.1.1
	port1 (LAN)	10.255.0.254/24	Link a R1
FGT-B	port2 (WAN)	100.64.2.2/24	GW: 100.64.2.1
	port1 (LAN)	10.100.0.254/24	Link a SPINE-1
	port3 (LAN)	10.100.1.254/24	Link a SPINE-2

Building B (Greenfield) - Fabric L3 (OSPF Area 0)

Dispositivo	Interfaccia	Indirizzo IP	Note
SPINE-1	Loopback0	169.254.2.2/32	Router-ID
	Ethernet0/0	10.100.0.1/24	Link a FGT-B (port1)
	Ethernet1/0	10.254.11.1/30	Link a LEAF-1 (e1/0)
	Ethernet1/1	10.254.12.1/30	Link a LEAF-2 (e1/1)
SPINE-2	Loopback0	169.254.2.3/32	Router-ID
	Ethernet0/0	10.100.1.2/24	Link a FGT-B (port3)
	Ethernet1/0	10.254.22.1/30	Link a LEAF-2 (e1/0)
	Ethernet1/1	10.254.21.1/30	Link a LEAF-1 (e1/1)
LEAF-1	Loopback0	169.254.2.4/32	Router-ID
	Ethernet1/0	10.254.11.2/30	Link a SPINE-1 (e1/0)
	Ethernet1/1	10.254.21.2/30	Link a SPINE-2 (e1/1)
	Ethernet0/1	10.254.1.1/30	Link a VTEP-DC2 (Eth1)
LEAF-2	Loopback0	169.254.2.5/32	Router-ID

	Ethernet1/0	10.254.22.2/30	Link a SPINE-2 (e1/0)
	Ethernet1/1	10.254.12.2/30	Link a SPINE-1 (e1/1)
	Ethernet0/2	10.254.2.1/30	Link a VTEP-DC2 (Eth2)

Overlay DCI (VXLAN VNI 10100)

Dispositivo	Interfaccia	Indirizzo IP	Note
VTEP-DC1	Loopback1	192.168.110.1/32	VTEP Source (DC-1)
	Ethernet1	10.2.9.2/30	Link a R9 (e0/0)
	Ethernet2	10.2.8.2/30	Link a R8 (e0/0)
	Vlan100	192.168.100.1/24	**Anycast Gateway**
	Ethernet3	VLAN 100 Access	Link a Host-A
VTEP-DC2	Loopback1	192.168.110.2/32	VTEP Source (DC-2)
	Ethernet1	10.254.1.2/30	Link a LEAF-1 (e0/1)
	Ethernet2	10.254.2.2/30	Link a LEAF-2 (e0/2)
	Vlan100	192.168.100.1/24	**Anycast Gateway**
	Ethernet3	VLAN 100 Access	Link a Host-B
Host-A	eth0	192.168.100.101/24	GW: 192.168.100.1
Host-B	eth0	192.168.100.102/24	GW: 192.168.100.1

4. 🔬 Fasi di Configurazione

Fase 1: Configurazione WAN (R-ISP e Firewall)

Obiettivo: Stabilire la connettività WAN di base e il NAT.

1. **Configurare R-ISP:**
   - Assegnare IP a Ethernet0/0 (a FGT-A) e Ethernet0/2 (a FGT-B).
   - Configurare Ethernet0/1 come ip address dhcp (simula Internet).
   - Configurare il NAT: ip nat inside sulle interfacce LAN (e0/0, e0/2) e ip nat outside su Ethernet0/1.
   - Creare una ACL (es. access-list 10) per permettere alle reti WAN 100.64.1.0/24 e 100.64.2.0/24 di essere NATtate.
   - Applicare il NAT: ip nat inside source list 10 interface Ethernet0/1 overload.
2. **Configurare FGT-A e FGT-B (Interfacce Base):**
   - Assegnare gli IP alle interfacce port2 (WAN) e alle interfacce LAN (port1 per FGT-A; port1 e port3 per FGT-B).
   - Abilitare il ping sulle interfacce WAN per i test.
3. **Configurare FGT-A e FGT-B (Routing Base):**
   - Su entrambi i firewall, creare una rotta di default (0.0.0.0/0) che punta al rispettivo IP di R-ISP.

Fase 2: Configurazione OSPF (Firewall e Router)

Obiettivo: Far girare OSPF tra i Firewall e le reti interne per lo scambio di rotte L3.

1. **Configurare OSPF su FGT-A:**
   - Abilitare OSPF, impostare un Router ID (es. 192.168.0.10).
   - Creare Area 0.0.0.0.
   - Aggiungere l'interfaccia port1 (LAN) all'Area 0.
   - Configurare default-information-originate always per fornire una rotta di default al Building A.
2. **Configurare OSPF su FGT-B:**
   - Abilitare OSPF, impostare un Router ID (es. 169.254.2.1).

- Creare Area 0.0.0.0.
- Aggiungere le interfacce port1 (a SPINE-1) e port3 (a SPINE-2) all'Area 0.
- Configurare default-information-originate always.

3. **Verificare OSPF su R1 (Building A):**
   - R1 ha già OSPF attivo dalle configurazioni del Lab 1.
   - Aggiungere l'interfaccia Ethernet0/0 (a FGT-A) in ip ospf 1 area 0.
   - R1 non ha più bisogno della rotta statica, ma la manterrà per ridondanza (ip route 0.0.0.0 0.0.0.0 10.255.0.254). OSPF (via default-information originate da FGT-A) sarà preferito.
4. **Verificare OSPF su SPINE-1 e SPINE-2 (Building B):**
   - Abilitare OSPF sulle interfacce Ethernet0/0 (verso FGT-B) e su tutte le interfacce Spine-Leaf.

Fase 3: Configurazione Tunnel VPN S2S (Route-Based)

Obiettivo: Creare il tunnel L3 sicuro tra FGT-A e FGT-B.

1. **Configurare Fase 1 (IKE) su entrambi i FortiGate:**
   - Creare una phase1-interface (es. "VPN-to-FGTB").
   - Impostare l'interfaccia (port2), remote-gw (l'IP WAN del peer) e la psksecret (chiave).
2. **Configurare Fase 2 (IPsec):**
   - Creare una phase2-interface.
   - Impostare i selettori (src-subnet e dst-subnet) a 0.0.0.0/0 (modalità route-based).
3. **Configurare Interfaccia Tunnel:**
   - Creare l'interfaccia tunnel virtuale (es. "VPN-to-FGTB").
   - Assegnare gli IP del tunnel (es. 169.254.10.1/30 su FGT-A e 169.254.10.2/30 su FGT-B).
   - Abilitare il ping sull'interfaccia tunnel per i test.
4. **Verifica:** Eseguire execute ping 169.254.10.2 da FGT-A per testare il tunnel.

Fase 4: Configurazione Fabric L3 (Building B)

Obiettivo: Costruire la fabric L3 Spine-Leaf (Underlay) nel DC-2.

1. **Configurare SPINE-1 e SPINE-2:**
   - Abilitare OSPF sulle interfacce Ethernet1/0 e Ethernet1/1 (link ai Leaf) in Area 0.
2. **Configurare LEAF-1 e LEAF-2:**
   - Configurare le interfacce Ethernet1/0 e Ethernet1/1 (link agli Spine) in Area 0.
   - Configurare OSPF e redistribute connected subnets per annunciare le future LAN.

3. **Verifica:** Da LEAF-1, verificare di avere due rotte OSPF a costo uguale (ECMP) per la rotta di default originata da FGT-B.

Fase 5: Configurazione Underlay DCI (VTEP)

Obiettivo: Collegare i VTEP Arista alla rete L3 e garantire la raggiungibilità degli IP sorgente del tunnel.

1. **Configurare VTEP-DC1 (in DC-1):**
   - Abilitare ip routing.
   - Configurare Ethernet1 (a R9) e Ethernet2 (a R8) con gli IP corretti.
   - Configurare Loopback1 con l'IP sorgente VTEP (192.168.110.1/32).
   - Configurare OSPF, impostare il router-id (es. 192.168.110.1) e aggiungere tutte le interfacce (Eth1, Eth2, Lo1) in area 0.0.0.2.
2. **Configurare VTEP-DC2 (in DC-2):**
   - Abilitare ip routing.
   - Configurare Ethernet1 (a LEAF-1) e Ethernet2 (a LEAF-2) con gli IP corretti.
   - Configurare Loopback1 con l'IP sorgente VTEP (192.168.110.2/32).
   - Configurare OSPF, impostare il router-id (es. 192.168.110.2) e aggiungere tutte le interfacce (Eth1, Eth2, Lo1) in area 0.0.0.0.
3. **Aggiornare Firewall (Routing VTEP):**
   - Poiché i VTEP si trovano *dietro* i firewall, dobbiamo aggiornare le rotte statiche e le policy VPN per permettere la comunicazione tra 192.168.110.1 e 192.168.110.2.
   - **Su FGT-A:** Aggiungere una rotta statica per 192.168.110.2/32 via VPN-to-FGTB.
   - **Su FGT-B:** Aggiungere una rotta statica per 192.168.110.1/32 via VPN-to-FGTA.
4. **Verifica:** Da VTEP-DC1, eseguire ping 192.168.110.2 source 192.168.110.1. Questo deve funzionare.

Fase 6: Configurazione Overlay DCI (VXLAN)

Obiettivo: Creare il tunnel L2 (VNI 10100) sopra l'Underlay L3.

1. **Configurare VTEP-DC1 (Arista):**
   - Creare vlan 100 e interface Vlan100.
   - Assegnare l'IP Anycast Gateway: ip address 192.168.100.1/24.
   - Configurare interface Vxlan1:
     - vxlan source-interface Loopback1
     - vxlan vlan 100 vni 10100

        - vxlan vlan 100 flood vtep 192.168.110.2 (IP del peer)
    - Configurare la porta di accesso: interface Ethernet3 -> switchport access vlan 100.
2. **Configurare VTEP-DC2 (Arista):**
    - Creare vlan 100 e interface Vlan100.
    - Assegnare lo **stesso** IP Anycast Gateway: ip address 192.168.100.1/24.
    - Configurare interface Vxlan1:
        - vxlan source-interface Loopback1
        - vxlan vlan 100 vni 10100
        - vxlan vlan 100 flood vtep 192.168.110.1 (IP del peer)
    - Configurare la porta di accesso: interface Ethernet3 -> switchport access vlan 100.
3. **Aggiornare Policy Firewall (Traffico VXLAN):**
    - I firewall devono permettere il traffico VXLAN (UDP 4789) tra i VTEP.
    - Creare un servizio custom per UDP_4789.
    - Creare una nuova policy (es. policy 12) su FGT-A e FGT-B per permettere il traffico UDP_4789 tra 192.168.110.1 e 192.168.110.2 attraverso il tunnel VPN.

Fase 7: Configurazione Host e Verifica Finale

Obiettivo: Testare la connettività L2 end-to-end.

1. **Configurare Host-A (Docker):**
    - Collegare a VTEP-DC1 (Eth3).
    - IP: 192.168.100.101/24, GW: 192.168.100.1.
2. **Configurare Host-B (Docker):**
    - Collegare a VTEP-DC2 (Eth3).
    - IP: 192.168.100.102/24, GW: 192.168.100.1.
3. **Test Finale:**
    - Da Host-A, eseguire ping 192.168.100.102.
    - Da Host-B, eseguire ping 192.168.100.101.
4. **Verifica VTEP:**
    - Su entrambi i VTEP, eseguire show vxlan address-table. Dovresti vedere il MAC address dell'host remoto imparato attraverso l'interfaccia Vxlan1.

5. 🗺️ Diagramma di Rete