NETWORK SECURITY PROJECT

FortiGate 80F Multi-VDOM Deployment

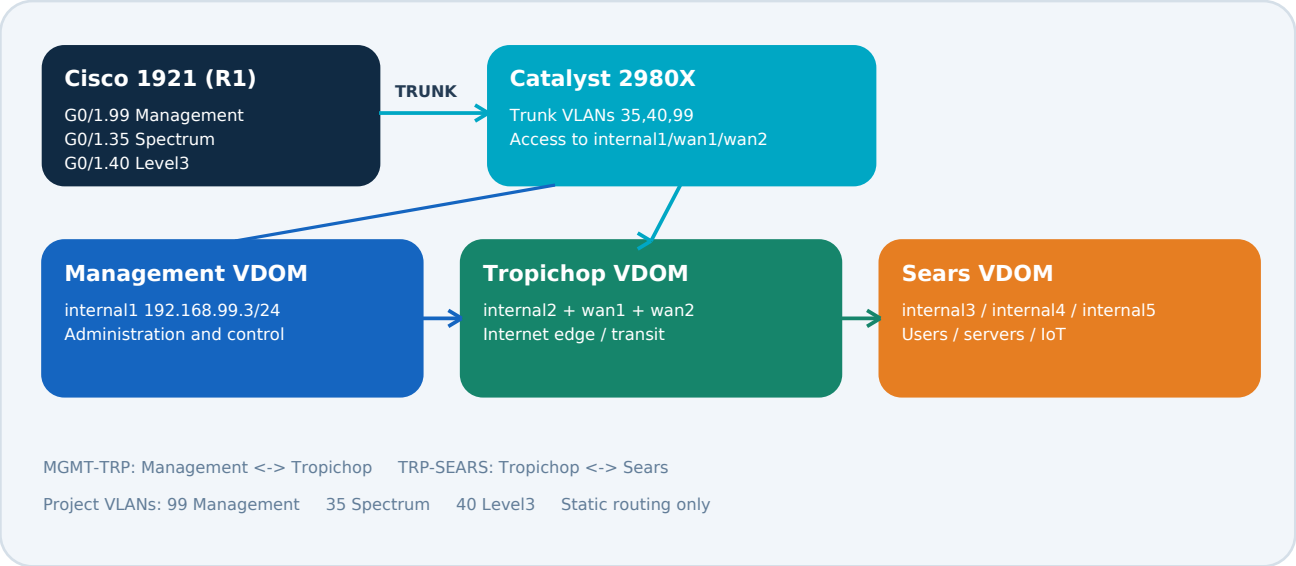
Management, Tropichop, and Sears VDOMs with controlled inter-VDOM routing and Cisco WAN infrastructure.

Prepared by

Clovis Capellan

31 August 2026 | Version 2.3

1. Architecture and Addressing



Cisco 1921 R1 uses Gi0/0 as a DHCP/NAT outside interface and Gi0/1 as an 802.1Q trunk to the Catalyst. The project uses VLAN 99 for Management, VLAN 35 for Spectrum, and VLAN 40 for Level3. The Catalyst presents VLAN 99 to FortiGate internal1 in the Management VDOM, while Tropichop owns wan1 and wan2.

Key interfaces

INTERFACE	VDOM	PURPOSE	ADDRESS
internal1	Management	Management / VLAN 99	192.168.99.3/24
internal2	Tropichop	Client LAN	10.20.20.1/24
wan1	Tropichop	Spectrum / VLAN 35	66.31.1.3/24
wan2	Tropichop	Level3 / VLAN 40	TBD; GW 43.64.1.254
internal3	Sears	Users	10.30.10.1/24
internal4	Sears	Servers	10.30.20.1/24
internal5	Sears	IoT / Voice	10.30.30.1/24
MGMT-TRP0/1	Mgmt / Tropichop	Transit	10.255.0.1/30 - .2/30
TRP-SEARS0/1	Tropichop / Sears	Transit	10.255.0.5/30 - .6/30

Confirmed from R1: Management gateway 192.168.99.254, Spectrum gateway 66.31.1.254, and Level3 gateway 43.64.1.254. FortiGate wan2 address remains TBD.

2. Essential FortiGate Configuration

The following is the minimum project configuration. Validate interface membership and remove internal1-internal5 from the default internal switch before moving them between VDOMs.

```
# GLOBAL: enable VDOMs and set management role
config system global
 set vdom-mode multi-vdom
 set management-vdom "Management"
end
config vdom
 edit "Management"
 next
 edit "Tropichop"
 next
 edit "Sears"
 next
end

# GLOBAL: create paired VDOM links
config system vdom-link
 edit "MGMT-TRP"
  set type ethernet
 next
 edit "TRP-SEARS"
  set type ethernet
 next
end

# GLOBAL: confirmed management and Spectrum interfaces
config system interface
 edit "internal1"
  set vdom "Management"
  set ip 192.168.99.3 255.255.255.0
  set allowaccess ping https ssh
 next
 edit "internal2"
  set vdom "Tropichop"
  set ip 10.20.20.1 255.255.255.0
 next
 edit "wan1"
  set vdom "Tropichop"
  set alias "Spectrum"
  set ip 66.31.1.3 255.255.255.0
  set allowaccess ping
 next
end

# GLOBAL: routed VDOM-link endpoints
config system interface
 edit "MGMT-TRP0"
  set vdom "Management"
  set ip 10.255.0.1 255.255.255.252
 next
 edit "MGMT-TRP1"
  set vdom "Tropichop"
  set ip 10.255.0.2 255.255.255.252
 next
 edit "TRP-SEARS0"
  set vdom "Tropichop"
  set ip 10.255.0.5 255.255.255.252
 next
 edit "TRP-SEARS1"
  set vdom "Sears"
  set ip 10.255.0.6 255.255.255.252
 next
end

# Assign internal2, wan2, and internal3-internal5 to their
# documented VDOMs and addresses from the page 2 table.
```

Essential routes

VDOM	DESTINATION	NEXT HOP	DEVICE
Management	0.0.0.0/0	10.255.0.2	MGMT-TRP0
Sears	0.0.0.0/0	10.255.0.5	TRP-SEARS1
Tropichop	192.168.99.0/24	10.255.0.1	MGMT-TRP1
Tropichop	10.30.10/20/30.0/24	10.255.0.6	TRP-SEARS0
Tropichop	0.0.0.0/0	66.31.1.254	wan1

3. Cisco WAN and Firewall Policies

Cisco 1921 R1 connects to the Catalyst 2980X using an 802.1Q trunk on Gi0/1. The switch delivers Management, Spectrum, and Level3 to the FortiGate as separate access VLANs.

```
! Cisco 1921 R1 - sanitized project-relevant configuration
interface GigabitEthernet0/0
 ip address dhcp
 ip nat outside
 ip nat enable
interface GigabitEthernet0/1
 no ip address
interface GigabitEthernet0/1.99
 encapsulation dot1Q 99
 ip address 192.168.99.254 255.255.255.0
interface GigabitEthernet0/1.35
 description Spectrum
 encapsulation dot1Q 35
 ip address 66.31.1.254 255.255.255.0
 ip nat inside
interface GigabitEthernet0/1.40
 description Level3
 encapsulation dot1Q 40
 ip address 43.64.1.254 255.255.255.0
 ip nat inside
ip nat inside source list 1 interface GigabitEthernet0/0 overload
ip route 0.0.0.0 0.0.0.0 10.0.0.1

! Catalyst 2980X WAN switch
vlan 99
 name MANAGEMENT
vlan 35
 name SPECTRUM
vlan 40
 name LEVEL3
interface GigabitEthernet1/0/1
 description TRUNK_TO_CISCO_1921
 switchport mode trunk
 switchport trunk allowed vlan 35,40,99
interface GigabitEthernet1/0/2
 description FORTIGATE_WAN1_SPECTRUM
 switchport mode access
 switchport access vlan 35
 spanning-tree portfast
interface GigabitEthernet1/0/3
 description FORTIGATE_WAN2_LEVEL3
 switchport mode access
 switchport access vlan 40
 spanning-tree portfast
interface GigabitEthernet1/0/4
 description FORTIGATE_INTERNAL1_MANAGEMENT
 switchport mode access
 switchport access vlan 99
 spanning-tree portfast
```

Required policy flow

VDOM	FROM	TO	SERVICE	ACTION	NAT
Management	internal1	MGMT-TRP0	Admin host	Allow / log	No
Sears	internal3/4/5	TRP-SEARS1	Approved services	Allow / log	No
Tropichop	internal2	wan1	Standard Internet	Allow + UTM	Yes
Tropichop	MGMT-TRP1	wan1	Management egress	Allow + UTM	Yes
Tropichop	TRP-SEARS0	wan1	Sears egress	Allow + UTM	Yes
Tropichop	TRP-SEARS0	internal2	Any	Deny / log	No

Apply antivirus, IPS, application control, web/DNS filtering, certificate inspection, and full traffic logging on Internet-edge allow policies.

4. Security, Validation, and Document Control

Priority security controls

CONTROL	REQUIREMENT
Management plane	Use internal1 only; HTTPS/SSH from trusted hosts; named admins with MFA; no HTTPS/SSH on WAN interfaces.
Tenant isolation	No Sears-to-Tropichop client access. Add shared-service exceptions only with documented business approval.
Logging	Send traffic, security, system, and administrator logs to FortiAnalyzer or protected syslog.
Operations	Encrypted backups, supported FortiOS, current FortiGuard packages, NTP, quarterly policy review.

Acceptance tests

TEST	PASS CONDITION
Interfaces	Each physical and VDOM-link interface belongs to the documented VDOM.
Routing	Management and Sears default to Tropichop; Tropichop has return routes and Spectrum default.
Internet	Approved clients reach DNS/HTTPS through wan1; NAT and UTM logs are visible.
Isolation	Sears cannot reach Tropichop internal2; the deny is logged.
VLAN separation	internal1 is in VLAN 99; wan1 is in VLAN 35; wan2 is in VLAN 40.
Administration	internal1 at 192.168.99.3 is assigned to Management VDOM and reachable only from approved sources.

Open item: provide the FortiGate Level3 wan2 IP address and approve its static-route preference. Credentials, password hashes, and the router serial number are intentionally excluded.

Document control

FIELD	VALUE
Version	2.3
Date	31 August 2026
Prepared by	Clovis Capellan
Approval status	Project Based
Scope	FortiGate 80F multi-VDOM project summary

Reference basis: Fortinet FortiOS VDOM and inter-VDOM routing guidance. Validate commands against the installed FortiOS and Cisco IOS versions before deployment.