

CCNA 200-301 v1.1

MODULE 5 — Security Fundamentals

Complete Hands-on Training Labs

Topology • Sequential Device Configuration • Verification Output • Troubleshooting

NETWORK GUIDE ACADEMY

Instructor / Student Lab Guide

Scope: This workbook follows a single forward configuration sequence. Each device is configured once for the base lab. Later commands are only verification, controlled attack/failure tests, or deliberate security-policy changes.

Module 5 lab map

Lesson	Lab focus	Hands-on outcome
5.1	Security concepts: threats, vulnerabilities, exploits and mitigation	Guided security assessment
5.2	Security program elements: awareness, training and physical access	Security-control audit
5.3	Device access control using local passwords	Router + switch hardening
5.4	Password policy, complexity and alternatives	Policy + login lockout
5.5	IPsec remote access and site-to-site VPNs	Site-to-site IPsec demonstration
5.6	Access control lists	Standard + extended IPv4 ACLs
5.7	Layer 2 security	Port security + DHCP snooping + DAI
5.8	Authentication, authorization and accounting	TACACS+ with local fallback
5.9	Wireless security protocols	WPA/WPA2/WPA3 interpretation
5.10	WLAN with WPA2 PSK	WLC GUI + client verification

How to use this workbook

1. Build the topology exactly as shown and apply the addressing plan.
2. Configure devices in the order presented. Do not repeat an earlier configuration block.
3. Run each verification command immediately after its related configuration.
4. Compare your output with the sample output and read the “What to verify” bullets.
5. Run the end-to-end test, then perform the controlled security/failure exercise where provided.

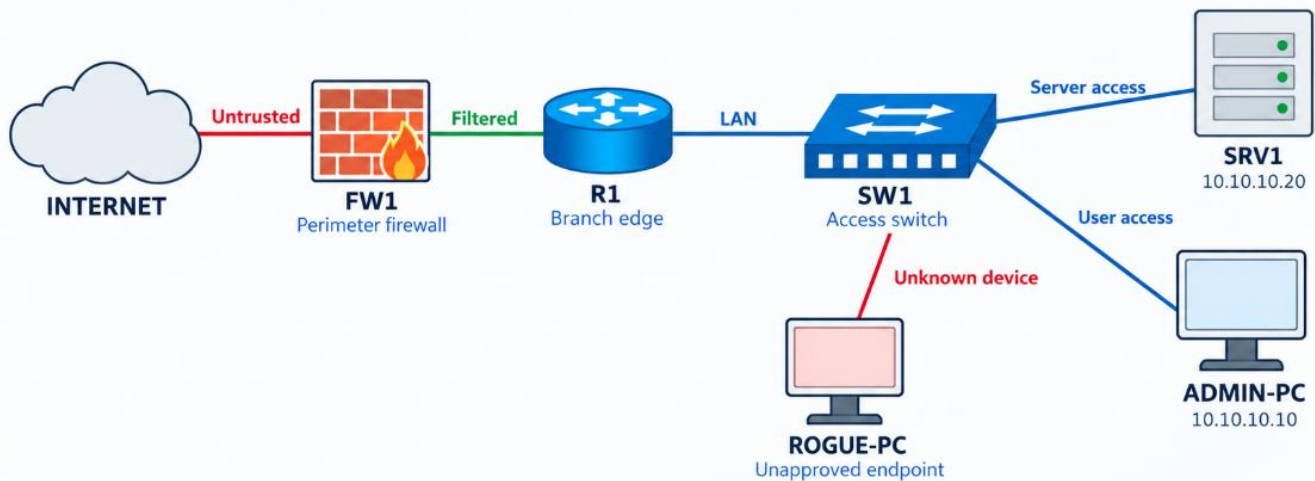
Exam alignment: Cisco CCNA 200-301 v1.1 lists Security Fundamentals objectives 5.1 through 5.10. Concept-only objectives are implemented as guided scenario/interpretation labs; configuration objectives include full device-by-device CLI or GUI steps.

Lab 5.1 — Security Concepts: Threat, Vulnerability, Exploit and Mitigation

Perform a security assessment of an intentionally weak branch network. The goal is to distinguish a threat from a vulnerability and an exploit, then select a realistic mitigation.

Lab topology

Lab 5.1 — Security Concepts: Threat, Vulnerability, Exploit & Mitigation | IP Connectivity



Lab goal: collect evidence, classify the issue, and map each finding to an appropriate mitigation.

Addressing / device plan

Device	Interface / role	Address / state
R1	LAN gateway	10.10.10.1/24
SW1	Access switch	10.10.10.2/24 management
ADMIN-PC	Approved endpoint	10.10.10.10/24
SRV1	Application server	10.10.10.20/24
ROGUE-PC	Unapproved endpoint	10.10.10.99/24

Lab objectives

- Collect evidence without changing the network.
- Classify findings as threat, vulnerability, exploit or mitigation.
- Identify weak management access, unused-access-port exposure and unauthorized endpoints.
- Create a mitigation plan that will be implemented in later Module 5 labs.

Step 1 — Inspect R1 without making changes

```
R1# show ip interface brief
Interface      IP-Address    OK? Method Status      Protocol
GigabitEthernet0/0  10.10.10.1   YES manual up          up

R1# show running-config | section line vty
line vty 0 4
 password cisco
 login
 transport input telnet ssh

R1# show running-config | include enable password|enable secret|username|service password
enable password cisco
service password-encryption

R1# show logging | include LOGIN|SECURITY
<no security-login messages>
```

What to verify

- VTY access accepts Telnet, which exposes credentials and management traffic in clear text.
- The router uses a weak enable password rather than an enable secret.
- No named local administrator is present.
- The absence of security-login events does not prove the device is secure; it only shows that no login-control feature is generating those events.

Step 2 — Inspect SW1

```
SW1# show interfaces status
Port    Name      Status      Vlan
Gi0/1    connected 10
Gi0/2    connected 10
Gi0/3    notconnect 1
Gi0/4    notconnect 1

SW1# show mac address-table dynamic
Vlan    Mac Address      Type      Ports
----    -
10      00aa.aaaa.0010   DYNAMIC   Gi0/1
10      00bb.bbbb.0099   DYNAMIC   Gi0/2

SW1# show running-config | include port-security|bpduguard|shutdown
<no matching lines>
```

What to verify

- An unexpected MAC address is learned on an access port, representing an unauthorized endpoint threat.
- Unused ports are in VLAN 1 and are not administratively shut down.
- No port-security or BPDU Guard control is present on access interfaces.

Step 3 — Classify the findings

Observation	Classification	Why it matters	Recommended mitigation
Telnet permitted on VTY	Vulnerability	Credentials can be captured in transit	SSH only; local/AAA authentication

Weak enable password	Vulnerability	Easy credential guessing / offline recovery	Use enable secret and strong password policy
Rogue endpoint attached	Threat / possible exploit path	Unauthorized host can probe the LAN	Port security, 802.1X where available, shut unused ports
Unused access ports active	Vulnerability	Provides physical entry point	Move to unused VLAN and shutdown
ARP/DHCP protections absent	Vulnerability	Enables spoofing or rogue DHCP attacks	DHCP snooping + DAI

End-of-lab verification

What to verify

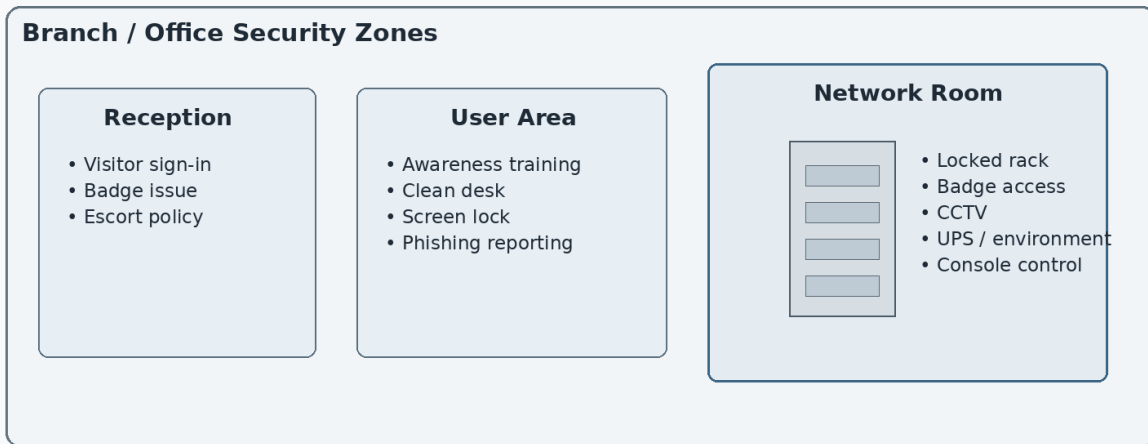
- You can explain the difference between a threat (potential cause of harm), vulnerability (weakness), exploit (method used to abuse the weakness), and mitigation (control that reduces likelihood or impact).
- Every observed weakness has a specific mitigation that can be validated in a later lab.

Lab 5.2 Optional — Security Program Elements: Awareness, Training and Physical Access

Audit a small branch from the perspective of people, process and physical controls. This lab intentionally has no IOS configuration because the objective is to validate the security program around the network.

Lab topology / facility view

Lab 5.2 — Security Program Elements and Physical Access Control



Lab goal: verify that people, process, and physical controls reinforce technical controls.

Lab objectives

- Verify user-awareness and recurring training controls.
- Verify visitor, badge and restricted-room controls.
- Verify physical safeguards for network equipment and console access.
- Document evidence rather than relying on assumed policy.

Step 1 — User awareness and training audit

Control	Evidence to collect	Pass condition
Security awareness	Training completion report	All in-scope users completed required training
Phishing awareness	Simulation/reporting record	Users know how and where to report suspicious messages
Password/MFA guidance	Published standard	Users receive current password and MFA guidance
Incident reporting	Help desk / SOC process	Users can identify the correct reporting channel

Step 2 — Physical access audit

Control	Verification action	Expected result
Visitor management	Attempt entry without sign-in	Visitor is stopped and registered

Network-room access	Review badge group membership	Only authorized operations staff have access
Rack security	Inspect rack doors and keys	Racks are locked; keys are controlled
Console access	Inspect console cables / terminal server	Access is restricted and auditable
Environmental resilience	Inspect UPS / temperature monitoring	Power and environmental controls are operational

Step 3 — Record findings

SECURITY PROGRAM AUDIT RESULT

User awareness training: PASS / FAIL

Phishing reporting process: PASS / FAIL

Visitor sign-in / escort: PASS / FAIL

Network-room badge control: PASS / FAIL

Rack locking: PASS / FAIL

Console access control: PASS / FAIL

UPS/environment monitoring: PASS / FAIL

Open findings:

1. _____
2. _____
3. _____

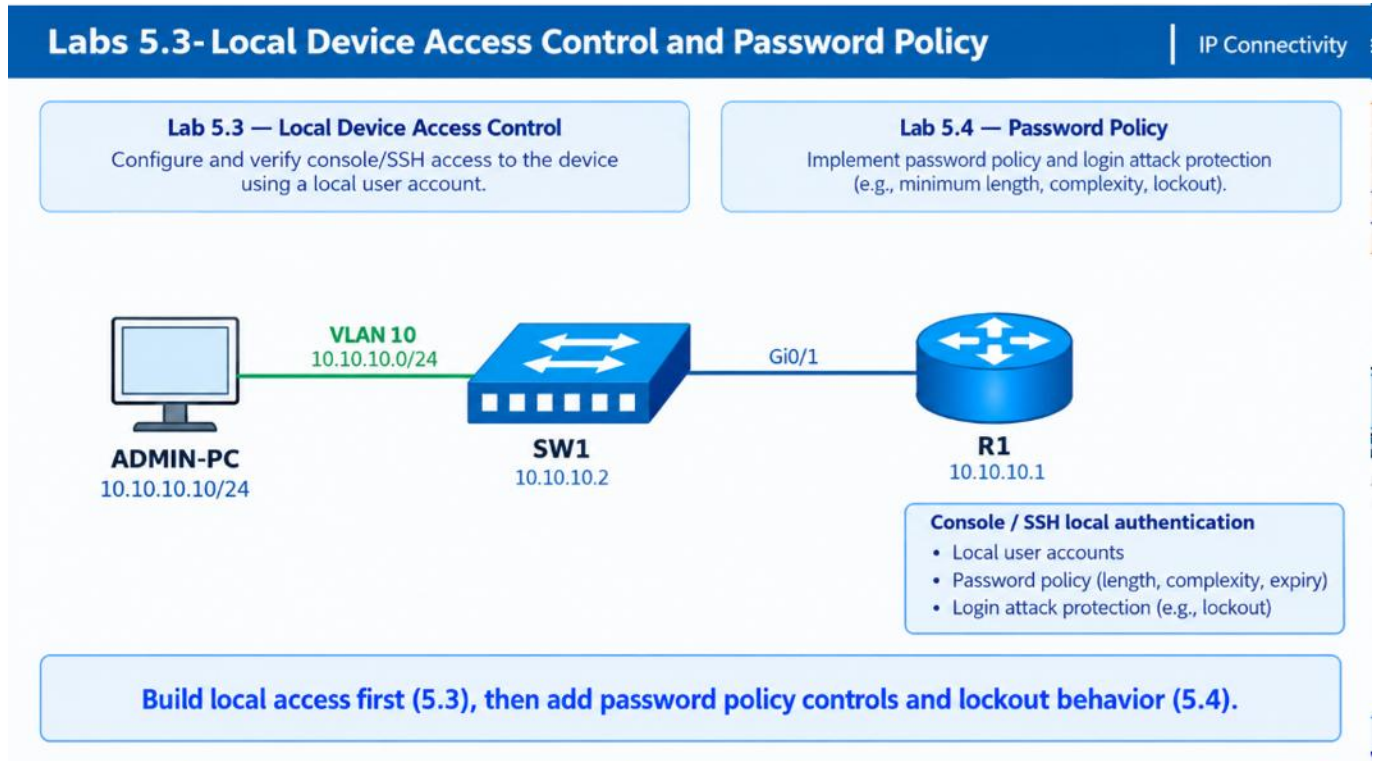
What to verify

- Each control has evidence, an owner and a pass/fail decision.
- Physical controls protect the devices that logical controls depend on.
- Security awareness and training are treated as recurring controls, not one-time events.

Lab 5.3 — Configure and Verify Local Device Access Control

Harden one router and one switch with local named accounts, enable secret, console authentication and SSH-only VTY access.

Lab topology



Addressing / device plan

Device	Interface	IPv4
R1	Gi0/0	10.10.10.1/24
SW1	SVI VLAN 10	10.10.10.2/24
ADMIN-PC	NIC	10.10.10.10/24; GW 10.10.10.1

Step 1 — Configure SW1 Layer 2 and management access

```
enable
configure terminal
hostname SW1
!
vlan 10
 name MANAGEMENT
!
interface GigabitEthernet0/1
 description TO_R1
 switchport mode access
 switchport access vlan 10
 no shutdown
!
interface GigabitEthernet0/2
 description ADMIN_PC
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
 no shutdown
!
interface Vlan10
 ip address 10.10.10.2 255.255.255.0
 no shutdown
!
ip default-gateway 10.10.10.1
!
enable secret CcnaEnable!2026
username netadmin privilege 15 secret LocalAdmin!2026
service password-encryption
ip domain-name nga.lab
crypto key generate rsa modulus 2048
ip ssh version 2
!
line console 0
 login local
 exec-timeout 5 0
!
line vty 0 4
 login local
 transport input ssh
 exec-timeout 10 0
end
write memory
```

SW1 verification

```
SW1# show ip interface brief | include Vlan10
Vlan10          10.10.10.2    YES manual up          up

SW1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3

SW1# show running-config | include enable secret|username netadmin|service password
enable secret 9 <hash>
username netadmin privilege 15 secret 9 <hash>
service password-encryption
```

What to verify

- SVI VLAN 10 is up/up and reachable from ADMIN-PC.
- SSH version 2 is enabled.
- Secrets are stored as hashes rather than visible plaintext.
- Console and VTY lines authenticate against the local username database.

Step 2 — Configure R1 local access control

```
enable
configure terminal
hostname R1
!
interface GigabitEthernet0/0
description TO_SW1
ip address 10.10.10.1 255.255.255.0
no shutdown
!
enable secret CcnaEnable!2026
username netadmin privilege 15 secret LocalAdmin!2026
service password-encryption
ip domain-name nga.lab
crypto key generate rsa modulus 2048
ip ssh version 2
!
line console 0
login local
exec-timeout 5 0
!
line vty 0 4
login local
transport input ssh
exec-timeout 10 0
end
write memory
```

R1 verification

```
R1# show ip ssh
SSH Enabled - version 2.0

R1# show running-config | section line vty
line vty 0 4
login local
transport input ssh
exec-timeout 10 0

R1# show users
  Line      User      Host(s)      Idle      Location
*  0 con 0   netadmin   idle        00:00:00
```