Author: Mohammad Sotoudeh

Captive Portal Implementation Playbook

FortiGate + Active Directory LDAP Authentication

FortiOS v7.4.1 · Windows Server 2019 · Domain: lab.local

PLATFORM

FortiGate VM64-KVM v7.4.1

AUTH METHOD

Active Directory LDAP :389

LAB ENV

PNetLab / VMware Workstation

Mohammad Sotoudeh

Domain: lab.local · Difficulty: Advanced · Est. Time: 3 hours · © 2026

FortiOS v7.4.1 Build 2463

Table of Contents

Step-by-step implementation roadmap

01 Introduction & How It Works

What we are building and why

1

What is a Captive Portal?

A captive portal is a network access control mechanism used in enterprises, hotels, airports, universities, and offices. It forces users to authenticate before accessing the internet. The firewall intercepts all HTTP traffic, redirects the browser to a login page, validates credentials against a directory service (Active Directory), and grants or denies internet access based on group membership.

Lab Components

Component	Version	IP Address	Role in This Setup
FortiGate VM64-KVM	FortiOS v7.4.1	10.1 / 20.1 / 145.220	Firewall + Portal Engine + LDAP Client
Windows Server 2019	Build 17763	192.168.20.2	Domain Controller + DNS + IIS Web Server
Windows Client	Any Windows	192.168.10.2	End-user workstation (unauthenticated)
VMware NAT	—	192.168.145.2	Internet gateway for the PNetLab lab
Active Directory	Domain: lab.local	192.168.20.2:389	Identity provider — stores users/groups

Authentication Sequence — Full Flow

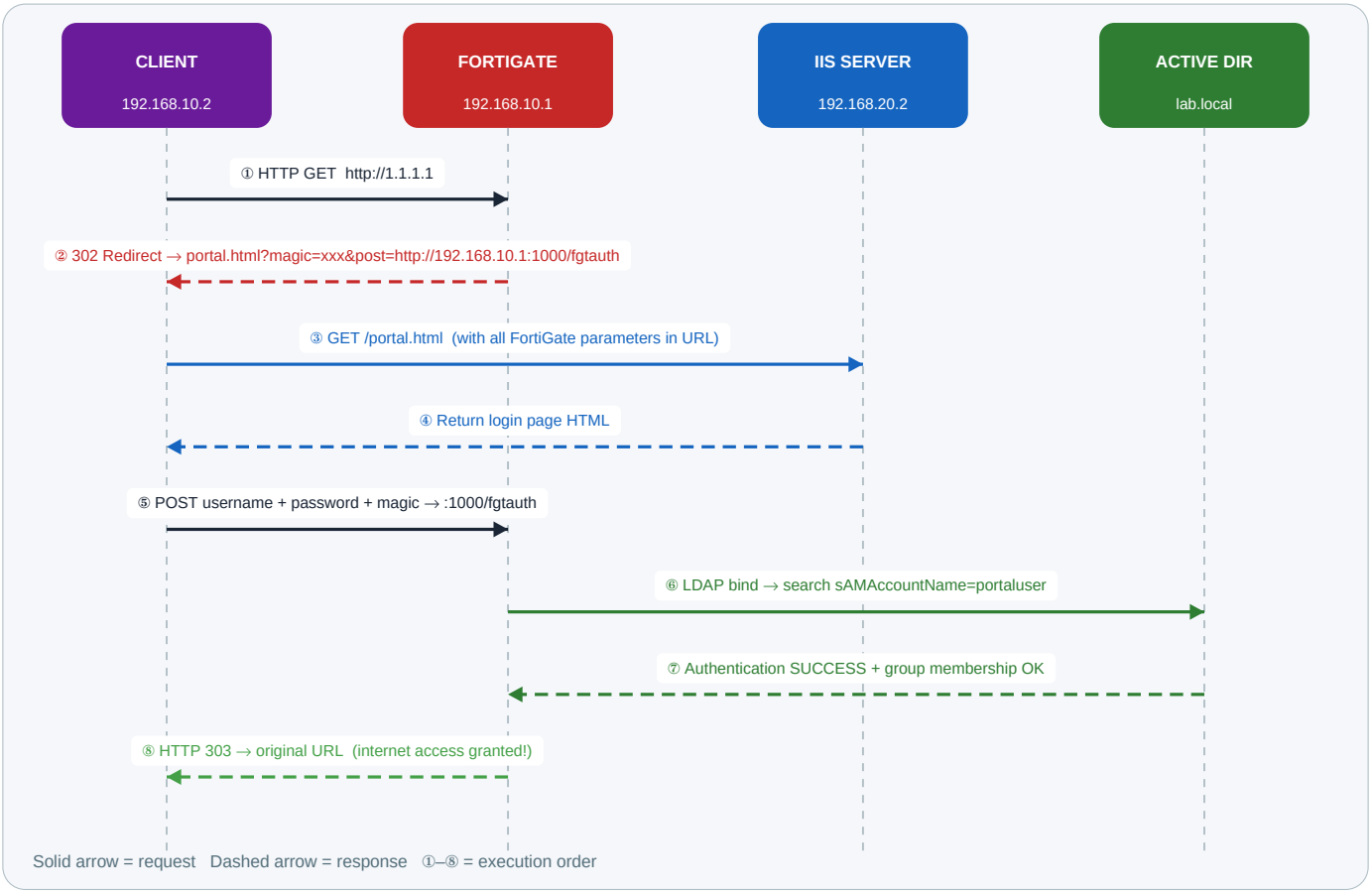

Figure 1.1 — Every step from client browser to internet access granted

02 Lab Topology & IP Schema

Network diagram and addressing

2

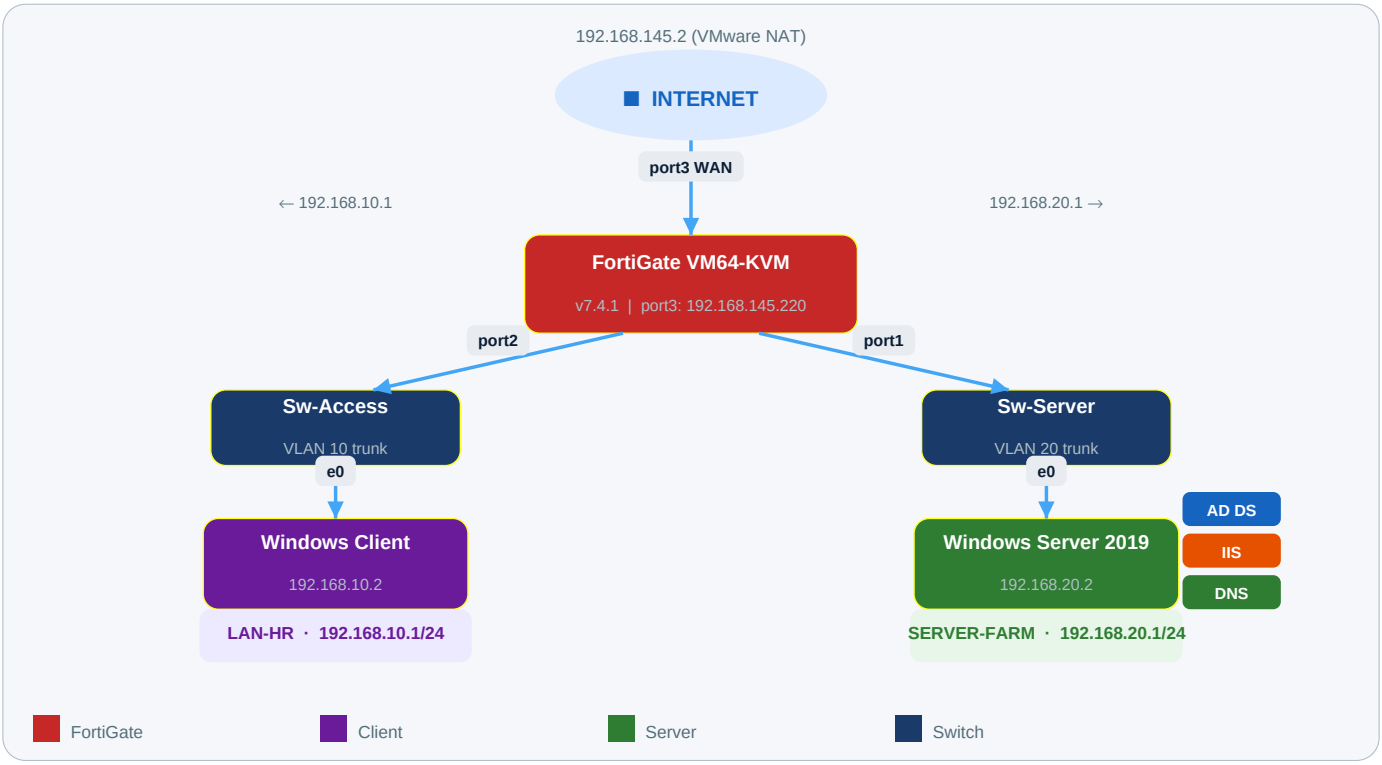

Figure 2.1 — Lab topology running on PNetLab inside VMware Workstation

Interface Assignments

FortiGate Port	VLAN / Sub-Interface	IP Address	Connects To
port1	SERVER-FARM (VLAN 20)	192.168.20.1/24	Sw-Server → Windows Server 2019
port2	LAN-HR (VLAN 10)	192.168.10.1/24	Sw-Access → Windows Client
port3	WAN (no VLAN)	192.168.145.220/24	VMware NAT gateway 192.168.145.2

Default Route — Required for Internet

Default Route

```
# FortiGate CLI
config router static
    edit 1
        set dst 0.0.0.0 0.0.0.0
        set gateway 192.168.145.2
        set device "port3"
    next
end

# Verify:
get router info routing-table all
# Expected: S*  0.0.0.0/0 [10/0] via 192.168.145.2, port3
```

Pre-flight Checklist — Verify These Before Starting

- ✓ FortiGate pings 192.168.145.2 and has internet access on port3
- ✓ Windows Client (192.168.10.2) pings FortiGate gateway 192.168.10.1
- ✓ Windows Server (192.168.20.2) pings FortiGate gateway 192.168.20.1
- ✓ Windows Server has internet access (needed for Windows Updates)
- ✓ AD DS and IIS roles are installed on Windows Server (not yet configured)

03 Phase 1 — Active Directory Setup

Promote server to Domain Controller, create users and groups

3

✕ CRITICAL
CRITICAL ORDER: Never install AD CS (Certificate Authority) before promoting to Domain Controller. Correct order: Install AD DS → Promote to DC → Reboot → then optionally install AD CS. Installing AD CS first causes a fatal prerequisites error that blocks DC promotion completely.

■ STEP 1 — Set Static IP on Windows Server

The server must have a static IP. The DNS field must point to **127.0.0.1** (itself) because Active Directory is completely dependent on DNS. Go to: Control Panel → Network and Sharing Center → Change adapter settings → Right-click NIC → Properties → IPv4

Static IP Settings

```
IP Address:       192.168.20.2
Subnet Mask:      255.255.255.0
Default Gateway:  192.168.20.1       # FortiGate SERVER-FARM interface
DNS (Primary):    127.0.0.1           # Must point to ITSELF - critical!
DNS (Alternate):  8.8.8.8             # Fallback for external resolution
```

■ STEP 2 — Promote Server to Domain Controller

Open **Server Manager**. You will see a yellow flag ■ at the top right. Click it → "Promote this server to a domain controller". This launches the AD DS Configuration Wizard. Use these exact settings:

AD DS Configuration Wizard

```
# PAGE 1: Deployment Configuration
Select:               Add a new forest
Root domain name:     lab.local

# PAGE 2: Domain Controller Options
Forest functional level:  Windows Server 2016
Domain functional level:  Windows Server 2016
[x] Domain Name System (DNS) server   <- keep checked
[x] Global Catalog (GC)               <- keep checked
[ ] Read-only domain controller       <- leave unchecked
DSRM Password:        Admin@1234       <- disaster recovery password

# PAGE 3: DNS Options
# You will see a yellow warning about DNS delegation -> IGNORE and click Next

# PAGE 4: Additional Options
NetBIOS domain name:  LAB              <- auto-filled, leave as-is

# PAGES 5, 6, 7: Paths and Review
# Leave all paths as default -> click Next through all of them

# PAGE 8: Prerequisites Check
# Yellow warnings are normal. Look for green:
# "All prerequisite checks passed successfully" -> click INSTALL
# Server will automatically reboot after installation completes
```

✓ STEP 3 — Verify Domain Controller After Reboot

After the reboot, log in as **LAB\Administrator**. Then verify:

RUN THIS COMMAND

```
echo %USERDOMAIN%
```

Note: Must show domain name, not computer name

EXPECTED OUTPUT

```
LAB
```

RUN THIS COMMAND

```
nslookup lab.local
```

Note: Server resolves its own domain

EXPECTED OUTPUT

```
Address: 192.168.20.2
```

■ STEP 4 — Create Portal User and Security Group

Open **Server Manager** → **Tools** → **Active Directory Users and Computers**. This user represents an employee who will log in through the captive portal:

Create User and Group

```
# === CREATE THE USER ===
Right-click "Users" folder -> New -> User
  First name:       Portal
  Last name:        User
  User logon name:  portaluser@lab.local
  -> click Next
  Password:         Portal@1234
  [x] Password never expires    <- check this
  [ ] User must change password <- UNCHECK this
  -> click Finish

# === CREATE THE SECURITY GROUP ===
Right-click "Users" folder -> New -> Group
  Group name:   CaptivePortalUsers
  Group scope:  Global
  Group type:   Security
  -> click OK

# === ADD USER TO GROUP ===
Double-click "CaptivePortalUsers" -> Members tab -> Add
Type "portaluser" -> Check Names -> OK -> Apply -> OK
```

04

Phase 2 — IIS Captive Portal Page

Host the login page and understand FortiGate magic parameters

4

Why Use IIS Instead of FortiGate Built-in Portal?

FortiGate has a built-in portal (Local mode), but using an External IIS-hosted page gives complete control over the design and company branding — exactly how real enterprises do it. IIS serves the HTML file only. It plays zero role in the actual authentication. Credentials go directly from the browser to FortiGate.

■ STEP 1 — Verify IIS and Open Port 80

Check IIS Service

```
# Run in PowerShell as Administrator on Windows Server

Get-Service W3SVC
# Expected: Status = Running

# If it shows Stopped, start it:
Start-Service W3SVC

# Open Windows Firewall for HTTP port 80:
New-NetFirewallRule -DisplayName "Allow HTTP Portal" `
    -Direction Inbound -Protocol TCP -LocalPort 80 -Action Allow
```

■ UNDERSTANDING — The FortiGate Magic Parameters

This is the most important concept in this guide. When FortiGate redirects a client to the portal page it appends special session parameters to the URL. These are mandatory. Without them, authentication is impossible. If you navigate directly to portal.html yourself (without being redirected by FortiGate), the parameters are missing and auth always fails.

FortiGate URL Parameters — Explained

```
# What FortiGate sends to the client browser (full redirect URL):
http://192.168.20.2/portal.html
    ?login
    &post=http://192.168.10.1:1000/fgtauth
#    ^ This is WHERE to POST the credentials.
#      It points to FortiGate authd daemon on port 1000.
#      NOT back to IIS.
    &magic=03040f829d85ed66
#    ^ One-time session token. Ties this browser session
#      to the specific client IP + MAC address.
#      FortiGate rejects any POST with missing/wrong magic.
    &usermac=50:5c:49:00:69:00   # Client MAC address
    &apip=192.168.10.1           # FortiGate LAN interface IP
    &userip=192.168.10.2         # Client IP address
    &ssid=LAN-HR                 # VLAN interface the client is on

# The HTML JavaScript reads all these and sets the form action:
document.getElementById("loginForm").action = postUrl;
# Form then submits directly to FortiGate, bypassing IIS completely.
```

■ WARNING

Never navigate directly to portal.html to test it. You must trigger it by opening Chrome and visiting any plain HTTP site like http://neverssl.com or http://1.1.1.1. FortiGate intercepts that request, injects the parameters, and then redirects you to portal.html. Only then does authentication work.

■ STEP 2 — Create the Portal HTML File

Run this entire PowerShell block on Windows Server as Administrator. Note the **https → http replacement** in JavaScript — this fixes a FortiOS v7.4 specific bug where the post URL uses https:// but FortiGate authd only listens on plain HTTP port 1000, causing a 405 error.

portal.html — PowerShell Creation Script

```
# Run this entire block in PowerShell (Administrator) on Windows Server
$html = @'
<!DOCTYPE html>
<html><head>
  <title>Network Access Portal</title>
  <style>
    body{font-family:Arial,sans-serif;text-align:center;
         padding:50px;background:#0B1D35;}
    h2{color:#fff;margin-bottom:5px;}
    p{color:#90A4AE;font-size:13px;}
    form{max-width:320px;margin:20px auto;background:#fff;
         padding:30px;border-radius:10px;
         box-shadow:0 8px 32px rgba(0,0,0,0.5);}
    input{width:100%;padding:12px;margin:8px 0;
          box-sizing:border-box;border:1px solid #ddd;
          border-radius:6px;font-size:14px;}
    button{width:100%;padding:12px;background:#1565C0;
           color:#fff;border:none;font-size:16px;
           border-radius:6px;cursor:pointer;}
    button:hover{background:#0D47A1;}
    .footer{margin-top:20px;font-size:11px;color:#546E7A;}
  </style>
</head><body>
  <h2>Enterprise Network Portal</h2>
  <p>Sign in with your domain credentials to access the internet</p>
  <form id="loginForm" method="POST">
    <input type="text"     name="username" placeholder="Username" required/>
    <input type="password" name="password" placeholder="Password" required/>
    <input type="hidden"   id="magic"   name="magic"   value=""/>
    <input type="hidden"   id="4Tredir" name="4Tredir" value=""/>
    <button type="submit">Connect to Network</button>
  </form>
  <div class="footer">lab.local — Unauthorized access is prohibited</div>
  <script>
    function getParam(n){
      return new URLSearchParams(window.location.search).get(n)||"";
    }
    var magic=getParam("magic");
    var post=getParam("post");
    var redir=getParam("4Tredir");
    if(magic) document.getElementById("magic").value=magic;
    if(redir) document.getElementById("4Tredir").value=redir;
    if(post){
      // FortiOS v7.4 bug: post uses https:// but authd is HTTP only
      // Fix: force http:// to avoid 405 Method Not Allowed error
      document.getElementById("loginForm").action=
```

… 7 more lines

RUN THIS COMMAND

```
Invoke-WebRequest http://192.168.20.2/po
rtal.html -UseBasicParsing
```

EXPECTED OUTPUT

```
StatusCode : 200
```

05

Phase 3 — FortiGate LDAP Connector

Connect FortiGate to Active Directory for credential validation

5

■ STEP 1 — Create LDAP Server Object

GUI path: User & Authentication → LDAP Servers → Create New
This object tells FortiGate the address and query method for your AD server. **sAMAccountName** is the AD attribute for short usernames (e.g. "portaluser" rather than "portaluser@lab.local").

LDAP Server Object

```
# GUI Field              Value
Name:                    AD-LAB
Server IP/Name:          192.168.20.2
Server Port:             389
Common Name Identifier: sAMAccountName
Distinguished Name:      DC=lab,DC=local
Bind Type:               Regular
Username:                CN=Administrator,CN=Users,DC=lab,DC=local
Password:                (your domain admin password)
Secure Connection:       OFF   # No AD CS = no LDAPS, use plain LDAP

# After saving:
# 1. Click "Test Connectivity" -> Expected: Connection Successful
# 2. Click "Test User Credentials":
#    Username: portaluser
#    Password: Portal@1234
#    Expected: Authentication Successful

# Equivalent CLI:
config user ldap
    edit "AD-LAB"
        set server "192.168.20.2"
        set cnid "sAMAccountName"
        set dn "DC=lab,DC=local"
        set type regular
        set username "CN=Administrator,CN=Users,DC=lab,DC=local"
        set password ENC <password>
    next
end
```

■ STEP 2 — Create User Group Linked to AD Group

GUI path: User & Authentication → User Groups → Create New

User Group — Linked to AD Group

```
# GUI Fields:
Name:            CaptivePortal-Group
Type:            Firewall

# Remote Groups section -> Add:
Remote Server:   AD-LAB
Groups:          CN=CaptivePortalUsers,CN=Users,DC=lab,DC=local

# CLI equivalent:
config user group
    edit "CaptivePortal-Group"
        config match
            edit 1
                set server-name "AD-LAB"
                set group-name "CN=CaptivePortalUsers,CN=Users,DC=lab,DC=local"
            next
        end
    next
end
```

✓ STEP 3 — Verify LDAP via CLI

RUN THIS COMMAND

```
diagnose test authserver ldap AD-LAB por
taluser Portal@1234
```

EXPECTED OUTPUT

```
authenticate 'portaluser' against 'AD-
LAB' succeeded!
```

06

Phase 4 — Captive Portal Interface Config

Enable captive portal on LAN-HR and set global auth settings

6

■ STEP 1 — Global Authentication Settings

GUI path: User & Authentication → Authentication Settings

Global Auth Settings

```
# GUI Settings:
Captive Portal Type:  IP   (select IP, not FQDN)
Captive Portal:       ON   (enable the toggle)
IP Address:           192.168.20.2
HTTP redirect:        ON   (enable the toggle)
Certificate:          Fortinet_Factory

# CLI (more reliable — always apply via CLI too):
config user setting
    set auth-type http
    set auth-secure-http disable
    set auth-http-basic disable
    set auth-src-mac enable
    set auth-cert "Fortinet_Factory"
end
```

■ STEP 2 — Configure LAN-HR Interface

GUI path: Network → Interfaces → LAN-HR → Edit → scroll down to the "Network" / "Admission Control" section:

LAN-HR Captive Portal Settings

```
# GUI fields on LAN-HR interface:
Security Mode:              Captive Portal
Authentication Portal:      External   <- MUST select External, not Local!
External URL:               http://192.168.20.2/portal.html
User Access:                Restricted to Groups
User Groups:                CaptivePortal-Group
Redirect after portal:      Original Request

# CLI equivalent:
config system interface
    edit "LAN-HR"
        set allowaccess ping http
        set security-mode captive-portal
        set security-external-web "http://192.168.20.2/portal.html"
        set security-groups "CaptivePortal-Group"
    next
end
```

■ **WARNING**

Adding "http" to allowaccess is what lets FortiGate intercept HTTP traffic on this interface and redirect it to the portal. Without this, FortiGate drops packets silently instead of redirecting. In FortiOS v7.4, adding http automatically adds https due to admin-https-redirect — this causes the 405 error. Fix this in Step 3.

■ STEP 3 — Fix the FortiOS v7.4 HTTPS Redirect Bug

FortiOS v7.4.1 has **admin-https-redirect enabled by default**. This forces the **post** parameter in the redirect URL to use https://, but FortiGate authd only listens on HTTP port 1000. Result: 405 Method Not Allowed when the login form submits. This must be disabled:

Disable HTTPS Redirect — FortiOS v7.4 Fix

```
config system global
    set admin-https-redirect disable
end

# Verify it worked:
get system global | grep redirect
# Expected output: admin-https-redirect: disable

# Clear any existing sessions to start fresh:
diagnose firewall auth clear
```

07 Phase 5 — Firewall Policies

Four policies required — order is critical

7

INFO

You need exactly four policies. Three allow pre-authentication traffic (before the user logs in), and one allows post-authentication internet access. The order matters — FortiGate matches policies top to bottom. Pre-auth policies must be ABOVE the internet policy.

Required Policies — Must Be In This Exact Order

Order	Policy Name	From	To	Service	NAT	Why It Is Needed
1	PreAuth-DNS	LAN-HR	SERVER-FARM	DNS	OFF	Client must resolve DNS names before logging in
2	PreAuth-HTTP-Portal	LAN-HR	SERVER-FARM	HTTP	OFF	Client fetches portal.html from IIS before auth
3	LDAP-to-AD	LAN-HR	SERVER-FARM	LDAP	OFF	FortiGate queries AD to validate credentials
4	CaptivePortal-Internet	LAN-HR	port3	ALL	ON	Post-auth internet — NAT must be ON for internet

CLI — Create All Four Policies

```
# Allow DNS before authentication
config firewall policy
    edit 0
        set name "PreAuth-DNS"
        set srcintf "LAN-HR"
        set dstintf "SERVER-FARM"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "DNS"
        set nat disable
    next
end
```

```
# Allow portal page fetch before auth
config firewall policy
    edit 0
        set name "PreAuth-HTTP-Portal"
        set srcintf "LAN-HR"
        set dstintf "SERVER-FARM"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "HTTP"
        set nat disable
    next
end
```

```
# Allow FortiGate to query Active Directory
config firewall policy
    edit 0
        set name "LDAP-to-AD"
        set srcintf "LAN-HR"
        set dstintf "SERVER-FARM"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "LDAP"
        set nat disable
    next
end
```

```
# Post-auth internet (NAT must be ON)
config firewall policy
    edit 0
        set name "CaptivePortal-Internet"
        set srcintf "LAN-HR"
        set dstintf "port3"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

08

Deep Dive — The Magic Parameters

Why direct access fails, what 405 means, and how auth really works

8

Why Direct URL Access Always Fails

Direct Access vs FortiGate Redirect

```
# WRONG — navigating directly to the portal page:
URL:   http://192.168.20.2/portal.html
magic  = ""  (empty — no FortiGate session)
post   = ""  (empty — no endpoint to submit to)

# JavaScript: form.action = ""
# Form POSTs back to IIS itself
# IIS is a static file server — it rejects POST requests
# Result: 405 Method Not Allowed. Auth FAILS.

# CORRECT — triggered by FortiGate redirect:
You open: http://neverssl.com
FortiGate intercepts and redirects to:
URL:   http://192.168.20.2/portal.html?login
         &post=http://192.168.10.1:1000/fgtauth   <- FortiGate authd
         &magic=03040f829d85ed66                  <- session token
         &userip=192.168.10.2 &ssid=LAN-HR

# JavaScript: form.action = "http://192.168.10.1:1000/fgtauth"
# Form POSTs credentials to FortiGate authd directly (bypasses IIS)
# FortiGate validates via LDAP -> grants access. Auth SUCCEEDS.
```

Component Roles Explained

FortiGate authd (port 1000)

The authentication daemon generates the magic token, intercepts HTTP traffic on LAN-HR, handles the redirect, receives the credential POST, validates against LDAP, and updates the firewall session table to allow traffic from authenticated clients.

The magic token

A cryptographic one-time session ID. It binds the browser session to a specific client IP and MAC address. FortiGate rejects any auth request with a missing or invalid magic token. It expires after auth-portal-timeout (default 3 minutes).

IIS role (Windows Server)

Acts as a plain static file server only. Serves the HTML file and nothing else. IIS plays zero role in authentication. Credentials POST directly to FortiGate authd, completely bypassing IIS.

The 405 error (FortiOS v7.4)

The post parameter contains https:// but authd only listens on HTTP port 1000. Fix 1: set admin-https-redirect disable in config system global. Fix 2: JavaScript replace("https://","http://") in portal.html. Both are needed.

09

End-to-End Testing

Verify every layer from network to authentication

9

Test 1 — Client pings FortiGate

RUN THIS COMMAND

```
ping 192.168.10.1
```

Note: Basic connectivity check

EXPECTED OUTPUT

```
Reply from 192.168.10.1
```

Test 2 — Client pings WinServer

RUN THIS COMMAND

```
ping 192.168.20.2
```

Note: Inter-VLAN routing working

EXPECTED OUTPUT

```
Reply from 192.168.20.2
```

Test 3 — Portal page loads

RUN THIS COMMAND

```
Chrome: http://192.168.20.2/portal.html
```

Note: IIS serving files

EXPECTED OUTPUT

```
Login form displayed
```

Test 4 — HTTP triggers redirect

RUN THIS COMMAND

```
Chrome: http://neverssl.com
```

Note: Captive portal intercepting

EXPECTED OUTPUT

```
Browser redirects to portal.html?magic
=...
```

Test 5 — Parameters in URL

RUN THIS COMMAND

```
Check address bar after redirect
```

Note: FortiGate injecting params

EXPECTED OUTPUT

```
URL contains &magic=xxx &post=http://.
..
```

Test 6 — Login works

RUN THIS COMMAND

```
Enter portaluser / Portal@1234 -> Connec
t
```

Note: LDAP auth successful

EXPECTED OUTPUT

```
Browser redirects to original URL
```

Test 7 — Internet works

RUN THIS COMMAND

```
Chrome: http://google.com
```

Note: Post-auth policy working

EXPECTED OUTPUT

```
Page loads
```

Test 8 — Auth monitor

RUN THIS COMMAND

```
Monitor -> Firewall User Monitor
```

Note: Full confirmation

EXPECTED OUTPUT

```
portaluser listed as Authenticated
```

Check Authenticated Sessions

```
# After successful login, check FortiGate CLI:
diagnose firewall auth list

# Expected output:
ip: 192.168.10.2, mac: 50:5c:49:00:69:00
user: portaluser
group: CaptivePortal-Group
duration: 45
----- 1 listed, 0 filtered ------
```

10 Troubleshooting Guide

Every common failure, cause, and exact fix

10

■ WARNING
Portal never appears — browser says "site unreachable" Fix: FortiGate is not intercepting HTTP traffic on LAN-HR. Check: show system interface LAN-HR — verify security-mode captive-portal is set. Verify allowaccess includes http. Check PreAuth-DNS and PreAuth-HTTP-Portal policies exist with correct interfaces. Always use http:// not https:// when testing.

✕ CRITICAL
405 Method Not Allowed after submitting credentials Fix: Form is POSTing to wrong endpoint. Run: get system global | grep redirect. If admin-https-redirect is enable, run: config system global / set admin-https-redirect disable / end. Also verify the JavaScript in portal.html replaces https:// with http:// in the post URL.

■ WARNING
Login page is blank or keeps refreshing Fix: Client navigated directly to portal.html URL without FortiGate redirect. Magic and post parameters are empty. Open http://neverssl.com or http://1.1.1.1 instead — FortiGate must be the one redirecting you to portal.html.

■ WARNING
Credentials rejected even though they are correct Fix: LDAP connectivity issue. Test directly from FortiGate CLI: diagnose test authserver ldap AD-LAB portaluser Portal@1234. If it fails, check the DN is exactly DC=lab,DC=local. Verify portaluser is member of CaptivePortalUsers in AD Users and Computers.

■ INFO
Authenticated but still no internet access Fix: Post-authentication policy is missing or wrong. Verify CaptivePortal-Internet policy exists going from LAN-HR to port3 with NAT enabled. Verify default route: get router info routing-table all — must show S* 0.0.0.0/0 via 192.168.145.2, port3.

■ FortiGate Debug Commands Reference

All Debug Commands

```
# Live authentication daemon debug — most useful tool
diagnose debug reset
diagnose debug application authd 255
diagnose debug enable
# Now trigger auth from the client browser
# Watch the output — you will see every step
diagnose debug disable
diagnose debug reset

# Packet trace for specific client IP
diagnose debug flow filter addr 192.168.10.2
diagnose debug flow trace start 20
diagnose debug enable
# Trigger traffic from client
diagnose debug flow trace stop
diagnose debug disable

# Test LDAP credential check directly
diagnose test authserver ldap AD-LAB portaluser Portal@1234

# View all currently authenticated users
diagnose firewall auth list

# Force all users to re-authenticate
diagnose firewall auth clear
```

11 Full HTML Source Code

Complete portal.html — save to C:\inetpub\wwwroot\portal.html

11

✓ SUCCESS
This is the complete working portal.html. The critical part is the JavaScript that reads FortiGate URL parameters and forces HTTP (replacing https://) to avoid the 405 error specific to FortiOS v7.4.

portal.html

```
<!DOCTYPE html>
<html>
<head>
  <title>Network Access Portal</title>
  <style>
    body { font-family: Arial, sans-serif; text-align: center;
           padding: 50px; background: #0B1D35; margin: 0; }
    h2   { color: #ffffff; font-size: 24px; margin-bottom: 5px; }
    p    { color: #90A4AE; font-size: 13px; margin-bottom: 20px; }
    form { max-width: 320px; margin: 0 auto; background: #ffffff;
           padding: 30px; border-radius: 10px;
           box-shadow: 0 8px 32px rgba(0,0,0,0.5); }
    input { width: 100%; padding: 12px; margin: 8px 0;
            box-sizing: border-box; border: 1px solid #ddd;
            border-radius: 6px; font-size: 14px; }
    button { width: 100%; padding: 12px; background: #1565C0;
             color: white; border: none; font-size: 16px;
             border-radius: 6px; cursor: pointer; margin-top: 10px; }
    button:hover { background: #0D47A1; }
    .footer { margin-top: 20px; font-size: 11px; color: #546E7A; }
  </style>
</head>
<body>
  <h2>Enterprise Network Portal</h2>
  <p>Sign in with your domain credentials to access the internet</p>
  <form id="loginForm" method="POST">
    <input type="text"
           name="username"
           placeholder="Username (e.g. portaluser)"
           required/>
```

```
    <input type="password"
           name="password"
           placeholder="Password"
           required/>
    <!-- Session token injected by FortiGate — do not change -->
    <input type="hidden" id="magic"   name="magic"   value=""/>
    <!-- Redirect URL after auth — do not change -->
    <input type="hidden" id="4Tredir" name="4Tredir" value=""/>
    <button type="submit">Connect to Network</button>
  </form>
  <div class="footer">lab.local Network — Unauthorized access is prohibited</div>

  <script>
    // Read all parameters FortiGate injected into the URL
    function getParam(name) {
      return new URLSearchParams(window.location.search).get(name) || "";
    }

    var magic   = getParam("magic");     // One-time session token
    var postUrl = getParam("post");       // FortiGate auth endpoint
    var redir   = getParam("4Tredir");    // Redirect URL after login

    // Populate hidden form fields with FortiGate session data
    if (magic)   document.getElementById("magic").value   = magic;
    if (redir)   document.getElementById("4Tredir").value = redir;

    if (postUrl) {
      // FortiOS v7.4 HTTPS redirect bug fix:
      // post parameter comes as https:// but authd listens on HTTP :1000
      // Forcing http:// here prevents the 405 Method Not Allowed error
```

```
      var httpPost = postUrl.replace("https://", "http://");
      document.getElementById("loginForm").action = httpPost;
    }
  </script>
</body>
</html>
```

12

Quick Reference Card

All IPs, credentials, paths, and commands on one page

12

IP Address & Credentials Reference

Item	Value
Domain name	lab.local (NetBIOS: LAB)
FortiGate LAN-HR gateway (port2 VLAN 10)	192.168.10.1/24
FortiGate SERVER-FARM gateway (port1 VLAN 20)	192.168.20.1/24
FortiGate WAN (port3)	192.168.145.220/24
Windows Server 2019 (DC + IIS + DNS)	192.168.20.2
Windows Client	192.168.10.2
VMware NAT internet gateway	192.168.145.2
Portal login page URL	http://192.168.20.2/portal.html
FortiGate auth endpoint (authd)	http://192.168.10.1:1000/fgtauth
LDAP port	389 plain text (636 SSL if AD CS installed)
Test AD user credentials	portaluser / Portal@1234
AD security group	CaptivePortalUsers
FortiGate user group	CaptivePortal-Group
FortiGate LDAP server object	AD-LAB
Portal file location on server	C:\inetpub\wwwroot\portal.html

■ All Critical CLI Commands

Complete CLI Reference

```
# Show FortiGate firmware version
get system status

# Show captive portal interface config
show system interface LAN-HR

# Show authentication settings
show user setting

# Check HTTPS redirect status (v7.4 fix)
get system global | grep redirect
# Must show: admin-https-redirect: disable

# Test LDAP authentication
diagnose test authserver ldap AD-LAB portaluser Portal@1234

# View authenticated users
diagnose firewall auth list

# Force re-authentication (clear all sessions)
diagnose firewall auth clear

# Live auth debug
diagnose debug application authd 255
diagnose debug enable
# ... trigger auth from client ...
diagnose debug disable

# Show routing table
get router info routing-table all

# Show all firewall policies
show firewall policy
```

■ INFO

This playbook was authored by Mohammad Sotoudeh. It covers FortiOS v7.4.1 build 2463. Some CLI commands and GUI paths may differ on other firmware versions. For production environments: install AD CS to enable LDAPS (port 636) with encrypted credential transmission, and sign the portal page with a trusted certificate to avoid browser security warnings. Test thoroughly in lab before deploying to production networks.