# FCP_FGT_AD-7.4 Training Course

## FCP - FortiGate 7.4 Administrator

Structured Learning & Certification Preparation

# Table of Contents

# Introduction

The FCP_FGT_AD-7.4 certification, aligned with the FortiGate 7.4 Administrator track, validates a professional's ability to deploy, configure, and manage FortiGate devices within a network security environment. It reflects practical knowledge of firewall operations, secure connectivity, and traffic inspection. In modern IT infrastructures where integrated security platforms are essential, this certification demonstrates the capability to maintain and enforce network protection mechanisms effectively.

# About This Training / Certification

This certification assesses competencies in administering FortiGate systems, including deployment, policy configuration, and secure network design. It is typically positioned at an intermediate level, requiring prior understanding of networking fundamentals and basic security principles. The certification forms part of a broader professional development path in network security, supporting progression toward more advanced roles in security architecture and threat management.

# What We Offer (AAAdemy)

AAAdemy provides structured training resources designed to support certification preparation and skill development across a wide range of IT domains. Our learning materials are built around clear knowledge structures, practical study guidance, and exam-oriented practice to help learners progress with confidence.

We offer well-organized knowledge explanations that break down complex topics into clear, understandable sections aligned with official exam objectives and real-world skill requirements. Each topic is designed to support both conceptual understanding and practical application.

Our study plans and learning guidance help learners follow a logical progression, focusing on key concepts, common pitfalls, and effective preparation strategies. This approach enables learners to study efficiently while maintaining a clear view of their learning goals.

To reinforce understanding, AAAdemy also provides practice questions and exam-focused insights that reflect typical certification scenarios. These resources are intended to help learners evaluate their readiness and strengthen their confidence before taking an exam.

All content is designed for flexible, self-paced learning, allowing individuals to study independently or alongside their existing professional or academic commitments.

# Knowledge Overview

The certification blueprint is structured around key functional domains that reflect real-world administrative responsibilities:

Deployment and System Configuration Area focuses on initial device setup, interface configuration, and system-level settings. Candidates are expected to understand how FortiGate devices are introduced into a network and prepared for operation.

Firewall Policies and Authentication Area emphasizes how traffic control rules are defined and enforced. This includes understanding policy structure, user authentication methods, and how identity-based access is applied within security policies.

Content Inspection Area covers the mechanisms used to analyze and filter network traffic. Candidates should understand how inspection techniques are applied to detect threats, enforce compliance, and control application usage.

Routing Area addresses how traffic is directed across networks. This includes conceptual knowledge of static and dynamic routing, as well as how routing integrates with firewall policies.

VPN Area focuses on secure connectivity between networks and remote users. Candidates are expected to understand the principles behind VPN technologies and how encrypted communication is established and maintained.

# Detailed Knowledge Explanation

## 1. FCP_FGT_AD-7.4 Deployment and System Configuration

As a Senior Architect, I view the initial deployment not as a series of checkboxes, but as the creation of a "Root of Trust." A standardized deployment ensures that the security posture is predictable and resilient. If the bedrock—interface roles, management restrictions, and system synchronization—is flawed, every subsequent security layer is compromised. Foundational settings dictate how the FortiGate interacts with the threat landscape and the internal fabric, making initial precision a non-negotiable requirement for enterprise integrity.

### 1.1 Initial Deployment of FortiGate

Standard access to a factory-default FortiGate occurs via the management port using the default IP **192.168.1.99**. For initial configuration, administrators must connect a PC on the same subnet and use the default credentials: **Username: admin / Password: (blank)**. Access is available through the GUI (HTTPS) or CLI (Console/SSH).

**Architectural Risk Mitigation:** Restricting administrative access is the first line of defense. By specifying trusted source IPs in the interface configuration, we neutralize unauthorized management attempts.

- **CLI Best Practice:**

## 1.2 FortiGate Basic Features

DNS and NTP are often overlooked but are operationally critical. DNS allows the FortiGate to resolve FortiGuard services, while NTP ensures synchronization.

- **The "So What?" Layer:** Inaccurate time synchronization is a silent killer for security. It invalidates certificate chains during SSL inspection and renders logs useless for forensic audits or legal compliance. Without precise NTP, the security fabric loses its chronological integrity.

## 1.3 High Availability (HA) Deployment

FortiGate supports **Active-Passive** (failover) and **Active-Active** (load balancing) modes.

- **Architect's Warning:** Firmware parity and identical hardware configurations are non-negotiable prerequisites for HA synchronization.
- **Heartbeat Connections:** Dedicated interfaces monitor cluster health. In a failover scenario, the cluster ensures sub-second transition to maintain service continuity, preventing a single point of failure from paralyzing the network.

## 1.4 System Upgrades and Backups

Firmware upgrades in an HA environment must be performed sequentially to maintain availability. Always source firmware from the Fortinet support portal.

- **Configuration Lifecycle:** Use `execute backup config` to maintain version control. A backup is not just a recovery tool; it is a point-in-time reference for configuration audits.

## 1.5 System Monitoring and Diagnostics

Effective monitoring reduces the **Mean-Time-To-Resolution (MTTR)**. While the Dashboard provides high-level resource views (CPU/Memory), deep-dive diagnostics require the CLI:

- **Flow Analysis:** `diagnose debug flow` allows an architect to see exactly how the FortiGate "thinks"—identifying which policy is matching or why a packet is being dropped.
- **Performance Tracking:** `diagnose sys top` identifies resource-heavy processes in real-time.

## 1.6 Virtual Domains (VDOMs)

VDOMs allow a single physical unit to be partitioned into multiple independent virtual firewalls. Enable this via: `config system global` -> `set vdom-admin enable`.

- **Evaluation:** While VDOMs are excellent for multi-tenancy and department isolation (HR vs. Finance), architects must account for the **increased CPU/Memory overhead** and the added complexity of inter-VDOM routing and management.

## 1.7 Interface Role Assignment

Assigning roles (**LAN, WAN, DMZ**) is more than cosmetic; it influences default security behaviors and simplifies policy creation. For example, a WAN role typically expects NAT, while a DMZ role implies strict incoming traffic controls for public-facing servers.

## 1.8 Factory Reset and Basic Licensing

An `execute factoryreset` wipes all configurations, including policies and local licenses. Post-reset, registration at `support.fortinet.com` is required to re-activate FortiGuard subscriptions. Features like Web Filtering and IPS are fundamentally crippled without an active license to receive real-time signature updates.

## 1.9 Deployment and system configuration Practice Question

Q1: What is the default management IP address of a newly deployed FortiGate device?
A. 192.168.1.99
B. 10.0.0.1
C. 192.168.0.1
D. 192.168.100.1

Q2: Which CLI command sets the IP address of port1 to 192.168.10.1/24?
A. `edit system interface; set port1 ip 192.168.10.1/24; end`
B. `config port1; set ip 192.168.10.1/24; end`
C. `config system interface; edit port1; set ip 192.168.10.1/24; end`
D. `set interface port1 ip 192.168.10.1/24; exit`

Q3: Which setting restricts administrative access to FortiGate from a specific IP subnet?
A. set allow https
B. set trustedhosts 192.168.10.0 255.255.255.0
C. set access-type admin-only
D. set access-restriction enable

Q4: What type of interface allows traffic segmentation over a single physical interface?
A. Physical Interface
B. Software Switch
C. VLAN Interface
D. Loopback Interface

Q5: Which feature allows combining multiple physical interfaces into a logical unit in FortiGate?
A. Link Aggregation Control Protocol (LACP)
B. Software Switch

C. Interface Grouping
D. Redundant Interfaces

Q6: Which CLI commands configure FortiGate to use Google's public DNS servers?
A. config system dns; set primary 8.8.8.8; set secondary 8.8.4.4; end
B. set dns server1 8.8.8.8; server2 8.8.4.4
C. config network dns; set server 8.8.8.8 8.8.4.4; end
D. dns set primary 8.8.8.8 secondary 8.8.4.4

Q7: Why is it important to configure an NTP server on FortiGate?
A. It speeds up network throughput.
B. It enables firmware updates.
C. It improves DNS resolution.
D. It ensures accurate log and event time tracking.

Q8: What are valid modes for High Availability (HA) in FortiGate? (Choose two)
A. Active-Passive
B. Load-Balance
C. Active-Active
D. Monitor-only

Q9: What is required for two FortiGate devices to join the same HA cluster?
A. Same hostname and serial number
B. Same admin password
C. Same firmware version and configuration compatibility
D. Identical interface IP addresses

Q10: Which command enables HA in active-passive mode and sets port3 as the heartbeat interface?
A. set ha-mode active-passive; heartbeat port3; end
B. config system ha; set mode a-p; set hbdev port3 50; end
C. ha configure active-passive; set link port3; end
D. config ha; mode passive-active; link port3 enable; end

Q11: How can you back up FortiGate configuration to a TFTP server?
A. execute backup tftp config
B. backup config via tftp <IP>
C. export system config tftp
D. execute backup config tftp <IP> <filename>

Q12: Which dashboard component displays real-time CPU and memory usage?
A. System Resources
B. Traffic Shaper
C. Session Monitor
D. Interface View

Q13: What is the function of the CLI command diag debug flow?
A. Show interface statistics

B. Display CPU and memory usage
C. Troubleshoot traffic flow
D. Run system self-test

Q14: Which of the following commands helps monitor FortiGate CPU load in real time?
A. diag debug flow
B. diag sys top
C. get system status
D. exec show cpu-status

---

# 2. FCP_FGT_AD-7.4 Firewall Policies and Authentication

The firewall policy is the primary decision engine of the FortiGate. Every packet is evaluated against a sequential set of rules to determine its fate, effectively translating corporate security policy into technical enforcement.

## 2.1 Firewall Policy Configuration

The workflow involves matching Source/Destination objects, Service Protocols (HTTPS, DNS), and an Action (Accept/Deny).

- **Least Privilege:** Utilizing **Schedules** (e.g., restricting access to office hours) ensures a granular access model, reducing the window of opportunity for attackers.

## 2.2 Policy Matching and Implicit Deny

FortiGate uses **top-down evaluation**. The first rule that matches all criteria is applied.

- **Critical Architect's Tip:** If no match is found, traffic hits the **Implicit Deny**. Be aware that **Implicit Deny is not logged by default**. To gain visibility into blocked "unknown" traffic, you must explicitly configure a manual "Deny All" rule with logging enabled at the bottom of your policy list.

## 2.3 Policy ID vs. Sequence Number

- **Policy ID:** A system-assigned unique ID used for database referencing; it **does not** affect the order of evaluation.
- **Sequence Number:** The actual position in the list, which dictates the matching order. Use the GUI or the `move` command in the CLI to reorder policies.

## 2.4 Firewall Policy Types: Proxy vs. Flow

- **Flow-based:** Optimized for speed using single-pass processing.
- **Proxy-based:** Buffers traffic for deep inspection. This mode is **required** for advanced features like **Full Content Caching and Data Loss Prevention (DLP)**.

## 2.5 NAT Configuration

- **Source NAT (SNAT):** Translates internal IPs to an external interface IP or an **Address Pool** for outbound traffic.
- **Destination NAT (DNAT):** Uses **Virtual IPs (VIPs)** to map external requests to internal resources (e.g., mapping port 443 on a public IP to an internal web server).

## 2.6 User Authentication

Centralized management via **LDAP, RADIUS, or TACACS+** is preferred over local accounts for enterprise scale. **Fortinet Single Sign-On (FSSO)** is the strategic choice for identity-based policy enforcement, as it synchronizes with Active Directory login events to provide seamless access without redundant login prompts.

### 2.7 Firewall policies and authentication Practice Question

Q1: In which order does FortiGate evaluate firewall policies?
A. Based on policy ID, ascending
B. Top to bottom in the GUI list
C. Random based on source address
D. Based on destination port priority

Q2: What happens if no firewall policy matches a traffic session in FortiGate?
A. It is allowed with default settings
B. It is redirected to a captive portal
C. It is denied due to the implicit deny policy
D. It is forwarded to the WAN by default

Q3: Which CLI command enables NAT in a firewall policy using the outgoing interface IP address?
A. `set srcnat enable`
B. `set nat-ip dynamic`
C. `set nat enable`
D. `set snat using-interface`

Q4: What is the main function of an IP pool in Source NAT (SNAT)?
A. To dynamically assign internal IPs to LAN devices
B. To assign external IPs to internal traffic from a defined range
C. To limit the number of users accessing the WAN
D. To isolate DNS queries from VPN traffic

Q5: Which FortiGate object is used to perform Destination NAT (DNAT) for incoming services?
A. Address Group
B. Virtual IP (VIP)

C. Static Route
D. Address Pool

Q6: In a VIP configuration, which setting ensures that only HTTP traffic is forwarded to the internal server?
A. `set type static-nat`
B. `set extport 443`
C. `set portforward enable`
D. `set mappedip auto`

Q7: Which option correctly associates a VIP with a firewall policy?
A. Add VIP to the service field
B. Use VIP as the source address
C. Use VIP as the destination address
D. Assign VIP under advanced NAT settings

Q8: Which option allows firewall policies to be active only during specific time periods?
A. User group schedules
B. Administrative time settings
C. Policy schedule
D. Log retention rules

Q9: Which command enables logging for all sessions that match a firewall policy?
A. `set logging enable`
B. `set log all`
C. `set logtraffic all`
D. `set syslog forward enable`

Q10: What is the purpose of identity-based policies in FortiGate?
A. To filter traffic based on MAC addresses
B. To allow policies to match based on user credentials
C. To route traffic through dedicated VPN tunnels
D. To assign different IP addresses to each user

Q11: Which authentication method does NOT require external servers?
A. LDAP
B. RADIUS
C. Local user accounts
D. TACACS+

Q12: Which field must be defined when configuring an LDAP server on FortiGate?
A. Radius secret
B. CNID (Common Name Identifier)
C. DNS Domain
D. Port forwarding object

Q13: Which protocol supports both user authentication and accounting on FortiGate?
A. LDAP
B. RADIUS
C. TACACS+
D. FSSO

Q14: What is the role of Fortinet Single Sign-On (FSSO) integration?
A. To allow FortiGate to function as a domain controller
B. To eliminate the need for firewall policies
C. To track user logins and associate them with IPs
D. To assign licenses to user accounts

Q15: Which component is installed on the AD server to support FSSO?
A. FortiAnalyzer agent
B. LDAP Proxy
C. FSSO Agent
D. Radius Collector

---

# 3. FCP_FGT_AD-7.4 Content Inspection

In the era of ubiquitous encryption, port-blocking is obsolete. Content inspection provides the visibility required to identify threats—like malware or SQL injections—hidden within encrypted payloads.

## 3.1 HTTPS Traffic Encryption Inspection

- **Certificate Inspection:** Only verifies metadata (validity/issuer). Fast, but blind to the payload.
- **Deep Inspection:** Acts as a **Man-in-the-Middle (MITM)**. It decrypts traffic, scans it, and re-encrypts it. This requires installing the FortiGate CA certificate on all client devices to maintain trust.

## 3.2 SSL Inspection Exceptions

Sensitive sites (Banking, Healthcare) often fail under MITM inspection due to certificate pinning or privacy regulations.

- **CLI Configuration:**

## 3.3 Web Filtering

Web filtering utilizes the FortiGuard dynamic database to categorize URLs. Security leads can block specific categories (e.g., Category 4 for Gambling, Category 5 for Malicious Sites) to reduce risk.

## 3.4 FortiGuard Rating Service Availability

If FortiGuard servers are unreachable, the fallback action takes effect: **Allow, Block, or Monitor**.

- **Recommendation:** For high-security environments, **Block** is the only safe choice. For standard business environments, **Monitor** balances security with usability by allowing access while logging the event for review.

## 3.5 Application Control

Using the FortiGuard signature database, Application Control identifies traffic regardless of port. This allows for sub-feature control, such as permitting YouTube browsing while blocking video uploads via the `youtube_upload` signature restriction.

## 3.6 Antivirus and IPS

- **Antivirus:** Scans HTTP, FTP, and SMTP in real-time. Integration with **FortiSandbox** provides protection against unknown "zero-day" threats.
- **IPS:** Protects against known exploits (SQL injection, buffer overflows). Applying an IPS profile to a policy effectively shields unpatched internal systems from external attack.

### 3.7 Content inspection Practice Question

Q1: Which SSL inspection mode in FortiGate examines only the SSL handshake and certificate without decrypting the content?
A. Deep Inspection
B. Certificate Inspection
C. Full Proxy Inspection
D. Bypass Mode

Q2: What is required for FortiGate to perform Deep Inspection on HTTPS traffic?
A. A static route to the server
B. DNS filtering enabled
C. FortiGate CA certificate installed on client devices
D. A NAT policy on the SSL port

Q3: What is a key advantage of using Certificate Inspection instead of Deep Inspection?
A. Provides malware scanning
B. Allows for URL filtering
C. Requires no certificate installation on clients
D. Enforces application control

Q4: Which FortiGate profile is applied to inspect HTTPS traffic in firewall policies?
A. Web Filter
B. SSL/SSH Inspection

C. Application Control
D. IPS Sensor

Q5: What is the function of FortiGuard in Web Filtering?
A. It scans emails for spam
B. It assigns IP addresses to URLs
C. It categorizes websites based on content
D. It updates firmware remotely

Q6: How can you block websites under the “Gambling” and “Malicious Websites” categories using CLI?
A. By blocking specific IP addresses
B. By disabling DNS forwarding
C. By setting category IDs to "block" in the Web Filter profile
D. By enabling SSL Inspection

Q7: Which type of Web Filtering is used to explicitly allow or block access to specific domains?
A. Category-based Filtering
B. DNS Filtering
C. URL-based Filtering
D. Certificate-based Filtering

Q8: Which FortiGate feature uses application signatures to detect and control traffic like YouTube or Skype?
A. Web Filter
B. Application Control
C. Antivirus
D. SSL Certificate Inspection

Q9: What can Application Control do besides blocking an entire application?
A. Rate limit the application
B. Restrict specific functions within an application
C. Enable DNS caching
D. Scan files for viruses

Q10: Which protocols can be scanned by FortiGate’s Antivirus engine?
A. Only HTTP and FTP
B. HTTP, HTTPS, FTP, SMTP
C. Only SMTP and POP3
D. SSH and Telnet

Q11: What is FortiSandbox used for in Antivirus configuration?
A. It replaces antivirus scanning
B. It scans DNS requests
C. It detects zero-day threats
D. It monitors CPU usage

Q12: What is the purpose of the Intrusion Prevention System (IPS) in FortiGate?
A. To encrypt VPN tunnels

B. To filter spam emails
C. To block known vulnerability exploits
D. To manage DNS resolution

Q13: Which of the following actions can be taken by an IPS sensor?
A. Bypass
B. Deny routing
C. Block or Monitor
D. Forward to DNS

Q14: Which configuration is needed to activate a custom IPS signature in FortiGate?
A. DNS entry creation
B. IP pool binding
C. Add the signature to an IPS sensor and apply it in a firewall policy
D. Apply antivirus scan to the same policy

Q15: What is required to bypass HTTPS inspection for specific domains like banking sites?
A. Disable firewall policy
B. Add the domain to SSL Exempt list in SSL/SSH profile
C. Create a static route for the domain
D. Turn off Web Filter temporarily

---

# 4. FCP_FGT_AD-7.4 Routing

Routing is the network's nervous system. Efficient path selection and link redundancy are fundamental to a high-availability architecture.

## 4.1 Static Routing

Manual routes are defined by **Administrative Distance (AD)** and **Priority**. A lower AD indicates a more reliable route source, while Priority breaks ties between routes with the same AD.

## 4.2 Blackhole Routes and Route Monitoring

- **Blackhole Routes:** Used to silently drop traffic to malicious ranges or prevent loops during failover.
- **Route Monitoring:** Link health checks (Ping Servers) allow the FortiGate to monitor gateway responsiveness. If a target (e.g., 8.8.8.8) fails to respond, the FortiGate automatically withdraws the failed static route from the table.

## 4.3 SD-WAN

SD-WAN optimizes bandwidth by grouping WAN links. It utilizes **SLA Rules** to monitor latency, jitter, and packet loss, dynamically steering critical traffic (like VoIP) to the healthiest link.

## 4.4 SD-WAN Rule Matching Order

SD-WAN rules are processed **top-down**. Specific business-critical rules must be placed above general internet rules to ensure they receive priority link selection.

## 4.5 Dynamic Routing Protocols (OSPF and BGP)

- **OSPF:** An interior protocol using areas to manage local topology.
- **BGP:** An Inter-AS protocol operating over **TCP port 179**. It is the de facto protocol for ISP peering.
- **Architectural Distinction:** Use **Prefix Lists** to filter *which* routes are accepted, and **Route Maps** to modify *attributes* (like Local Preference or Metric) to influence traffic engineering.

### 4.6 Routing Practice Question

Q1: Which of the following values determines the preferred static route when multiple routes exist for the same destination?
A. IP address of the gateway
B. Interface name
C. Administrative Distance
D. Metric

Q2: Which command sets a static route to the 192.168.10.0/24 network via gateway 10.0.0.1 on port1?
A. `set route 192.168.10.0/24 via 10.0.0.1 port1`
B. `config router static; edit 1; set dst 192.168.10.0/24; set gateway 10.0.0.1; set device "port1"; end`
C. `config system route; edit 1; set next-hop 10.0.0.1; set subnet 192.168.10.0/24; end`
D. `config router static; set route 192.168.10.0 next-hop 10.0.0.1 via port1`

Q3: In SD-WAN, what is the purpose of configuring SLA (Service Level Agreement) targets?
A. To define static routes
B. To allocate bandwidth per user
C. To monitor link performance and trigger failover
D. To block high-latency protocols

Q4: Which metrics are typically used in SD-WAN to evaluate link performance? (Choose two)
A. CPU usage
B. Latency
C. Jitter
D. Interface bandwidth

Q5: What does SD-WAN do when one of the WAN links exceeds its configured SLA thresholds?
A. Blocks all traffic

B. Switches the traffic to a better-performing link
C. Restarts the interface
D. Disables web filtering

Q6: What is the minimum required component to configure a functional SD-WAN setup?
A. A dynamic routing protocol
B. Two or more WAN interfaces as SD-WAN members
C. A BGP neighbor configuration
D. A DNS forwarding rule

Q7: Which OSPF area type is required for all OSPF deployments to function correctly?
A. Area 1
B. NSSA Area
C. Area 0
D. Stub Area

Q8: What is the function of the Router ID in OSPF?
A. Identifies the static route
B. Defines the routing table size
C. Uniquely identifies each OSPF router
D. Specifies the next-hop IP

Q9: Which of the following is used to influence OSPF Designated Router (DR) election on a broadcast network?
A. Route priority
B. Administrative distance
C. OSPF interface priority
D. Next-hop IP address

Q10: What must be true about BGP peers before they can exchange routes?
A. They must have matching interface names
B. They must belong to the same subnet
C. They must have established a TCP session on port 179
D. They must use the same administrative distance

Q11: Which BGP command configures the FortiGate device to use AS number 65001?
A. `set as 65001`
B. `set remote-as 65001`
C. `config router ospf; set as 65001`
D. `router bgp enable 65001`

Q12: What is the purpose of a prefix list in BGP routing?
A. To set bandwidth limits
B. To monitor link usage
C. To filter advertised or received routes
D. To control DNS queries

Q13: Which command denies all BGP prefixes in the 192.168.0.0/16 network?

A. `set route deny 192.168.0.0/16`

B. `block prefix 192.168.0.0/16`

C. `set access-list deny 192.168.0.0/16`

D. `config router prefix-list; edit "block_private"; config rule; edit 1; set prefix 192.168.0.0/16; set action deny; end; end`

Q14: Which of the following statements is true about administrative distance in FortiGate?

A. It applies only to BGP routes

B. Lower values mean less preference

C. Higher values are more trusted

D. It is used to choose between routes from different sources

Q15: When configuring SD-WAN rules in the GUI, which section is used to define the type of traffic the rule applies to?

A. Performance SLA

B. Interface Members

C. SD-WAN Service

D. Matching Criteria or Source/Destination fields

---

# 5. FCP_FGT_AD-7.4 VPN

VPNs extend the corporate security perimeter to remote sites and mobile users via encrypted tunnels.

## 5.1 SSL VPN

- **Web Mode:** Browser-based, clientless access.
- **Tunnel Mode:** Full network access via **FortiClient**.
- **Architectural Warning:** The **`ssl.root`** virtual interface **must** be used as the source interface in firewall policies for VPN traffic. Using a physical interface like `wan1` in the policy is a common configuration error that prevents traffic flow.

## 5.2 IPsec VPN

IPsec is the standard for Site-to-Site and high-performance remote access.

- **Phase 1:** Tunnel establishment and peer authentication.
- **Phase 2:** Negotiation of data encryption proposals.

## 5.3 Mode-cfg for Remote IPsec VPN

The `mode-cfg` feature allows the FortiGate to act as a **DHCP-like service**. It dynamically assigns internal IP addresses from a configured pool to remote FortiClient users, ensuring they receive valid internal identities for policy enforcement.

## 5.4 IKEv1 vs. IKEv2

- **IKEv1:** Supports Main and Aggressive modes; slower and less efficient.
- **IKEv2:** The modern recommendation. It offers faster negotiation, better error handling, and **MOBIKE** support for mobile users switching between networks (e.g., Wi-Fi to LTE).

## 5.5 Common VPN Troubleshooting Tips

If Phase 1 is established but Phase 2 fails, the issue is typically a mismatch in encryption proposals or source/destination subnets.

- **Diagnostic Toolkit:**
  - `get vpn ipsec tunnel summary` (Quick status check).
  - `diagnose vpn ike gateway list` (Phase 1 details).
  - `diagnose sniffer packet any 'port 500 or 4500' 4` (Monitor IKE traffic).

**Summary:** A comprehensive FortiGate solution integrates these five domains into a unified defense. **Deployment** creates the foundation; **Firewall Policies** and **Content Inspection** provide the security logic and visibility; **Routing** ensures efficient data delivery; and **VPN** technologies securely extend the perimeter. Mastering these core areas ensures a resilient, enterprise-grade security posture.

### 5.6 VPN Practice Question

Q1: Which SSL VPN mode allows access to internal web applications through a browser without installing any software?
A. Tunnel Mode
B. Web Mode
C. IPsec Mode
D. Transparent Mode

Q2: What is required on the client side to use SSL VPN Tunnel Mode?
A. A web browser
B. A firewall policy on FortiGate
C. The FortiClient VPN software
D. An active DNS filter

Q3: In an SSL VPN configuration, which FortiGate interface is typically used as the source interface in firewall policies?
A. port1
B. ssl.root

C. wan1
D. internal

Q4: Which of the following statements about SSL VPN Web Mode is true?
A. It supports all protocols including FTP and SSH
B. It requires the FortiClient app
C. It is limited to web-based services like HTTP and HTTPS
D. It offers full network access

Q5: In IPsec VPN configuration, what is the primary purpose of Phase 1?
A. To exchange data packets
B. To establish a secure tunnel and authenticate peers
C. To encrypt application traffic
D. To apply antivirus filters

Q6: What parameter must match on both sides of an IPsec VPN tunnel for Phase 1 to succeed?
A. NAT type
B. Service port
C. Pre-shared key (PSK)
D. Address range

Q7: In IPsec Phase 2 configuration, what is the purpose of `src-subnet` and `dst-subnet`?
A. To define the tunnel endpoints
B. To specify peer identities
C. To define which traffic is encrypted through the tunnel
D. To assign client IP addresses

Q8: Which IPsec VPN mode is most suitable for secure connectivity between two branch offices with static IPs?
A. Aggressive Mode
B. Site-to-Site VPN
C. Remote Access VPN
D. Transparent VPN

Q9: When configuring a Remote Access IPsec VPN, which mode is often used for dynamic client IPs?
A. Main Mode
B. Manual Mode
C. Aggressive Mode
D. Peerless Mode

Q10: What is the function of Dead Peer Detection (DPD) in IPsec VPNs?
A. It distributes bandwidth evenly
B. It blocks unauthorized users
C. It monitors peer availability and clears stale sessions
D. It optimizes routing paths

Q11: What does the command `set dpd enable` do in a VPN configuration?
A. Disables NAT traversal

B. Enables backup tunnel monitoring
C. Activates Dead Peer Detection
D. Resets tunnel state

Q12: Which of the following is required to successfully connect an SSL VPN user to internal network resources?
A. A static route to the WAN
B. A firewall policy from `ssl.root` to the destination network
C. DNS forwarding enabled
D. NAT policy for port 443

Q13: What is the purpose of configuring multiple IPsec VPN tunnels between two sites?
A. To share IP addresses
B. For URL filtering
C. To provide redundancy and failover
D. To support multiple VLANs

Q14: Which FortiGate configuration sets the SSL VPN to listen on port 443 and use a specific IP pool?
A. `set interface port 443; set address-pool SSLPool`
B. `config firewall interface; set https-port 443; set pool SSLPool`
C. `config vpn ssl settings; set port 443; set tunnel-ip-pools "SSLPool"`
D. `set vpn-port 443; set pool SSLPool`

Q15: In a site-to-site IPsec VPN setup, which phase handles encryption of the actual data traffic?
A. Phase 1
B. Phase 2
C. Authentication phase
D. Pre-connection phase

# Learning Path & Study Advice

A progressive learning approach is recommended, beginning with core networking concepts such as IP addressing, subnetting, and routing behavior. Building on this foundation, candidates should focus on how FortiGate implements these concepts through configuration and policy enforcement. It is important to understand how different domains—such as firewall policies, routing, and VPN—interact within a unified system. Emphasis should be placed on conceptual clarity and practical reasoning, particularly when analyzing traffic flow and security decisions. Hands-on practice with configuration scenarios can reinforce understanding of how system components operate together.

# Who This PDF Is For

This document is intended for network and security professionals responsible for configuring and managing firewall solutions in enterprise environments. It is suitable for individuals with a foundational understanding of networking who are advancing toward more specialized security roles. Network administrators, system engineers, and security analysts will benefit from this material, especially those seeking to strengthen their ability to manage integrated security platforms such as FortiGate.

# Call To Action

This document provides an overview of structured learning and certification preparation approaches. For learners seeking clear knowledge organization, guided study planning, and exam-focused practice resources, AAAdemy offers a comprehensive platform to support independent and effective learning.

Explore additional training materials, study guidance, and practice resources at:

https://www.aaademy.com/FCP-in-Network-Security/FCP_FGT_AD-7.4.html

Online Flashcards (Quizlet):

https://quizlet.com/user/AAAdemy/folders/fcp_fgt_ad-74-fortigate-74-administrator-flashcards?i=6zfa5t&x=1xqt

## Attachment : Answers by Knowledge Point

Deployment and system configuration Practice Question
A1: Answer: A
Explanation: By default, FortiGate devices are configured with the IP address 192.168.1.99 on the management interface for initial access.

A2: Answer: C
Explanation: Option C contains the correct sequence for editing port1 and assigning the IP address in CLI.

A3: Answer: B
Explanation: The trustedhosts setting allows you to define source IPs or subnets that are permitted administrative access.

A4: Answer: C
Explanation: VLAN interfaces allow you to assign multiple logical networks to one physical port, each identified by a unique VLAN ID.

A5: Answer: B
Explanation: Software Switch is used to aggregate multiple interfaces into one logical switch interface.

A6: Answer: A
Explanation: This command block correctly configures primary and secondary DNS servers in FortiGate using CLI.

A7: Answer: D
Explanation: Correct time synchronization is crucial for accurate log timestamps, certificate validation, and cluster coordination.

A8: Answer: A, C
Explanation: FortiGate supports both Active-Passive and Active-Active HA modes. Load-Balance and Monitor-only are not valid HA modes.

A9: Answer: C
Explanation: Firmware version and system configurations (such as VDOMs and interfaces) must be synchronized before enabling HA.

A10: Answer: B
Explanation: The given CLI commands properly configure HA with port3 as heartbeat and mode as active-passive.

A11: Answer: D
Explanation: The execute backup config tftp command is used for backing up configuration files via TFTP.

A12: Answer: A
Explanation: The System Resources widget on the dashboard allows monitoring of CPU, memory, and session counts.

A13: Answer: C
Explanation: diag debug flow is used for detailed traffic-level debugging and flow analysis in FortiGate.

A14: Answer: B
Explanation: diag sys top is used to display real-time system performance, including CPU usage.

Firewall policies and authentication Practice Question
A1: Answer: B
Explanation: Firewall policies in FortiGate are evaluated sequentially from top to bottom as shown in the GUI. The first matching policy is applied.

A2: Answer: C
Explanation: FortiGate includes an implicit deny at the end of the policy list. If no rule matches, the traffic is automatically denied.

A3: Answer: C
Explanation: The `set nat enable` command in a firewall policy tells FortiGate to use Source NAT with the interface's IP address.

A4: Answer: B
Explanation: An IP pool allows FortiGate to dynamically map internal IP addresses to a range of external IPs when performing SNAT.

A5: Answer: B
Explanation: A Virtual IP (VIP) object maps external IPs and ports to internal IPs and ports, enabling DNAT.

A6: Answer: C
Explanation: `set portforward enable` is required to specify port-based mapping in a VIP, such as forwarding only port 80 for HTTP.

A7: Answer: C
Explanation: In firewall policies, the VIP object is applied in the destination address field to match incoming traffic.

A8: Answer: C
Explanation: A schedule can be assigned to a policy to control when it is active. This is configured under the policy's "Schedule" setting.

A9: Answer: C
Explanation: The `set logtraffic all` command enables logging for all sessions that match the firewall policy, not just the start or end.

A10: Answer: B
Explanation: Identity-based policies allow FortiGate to make decisions based on the user's identity (local or external authentication).

A11: Answer: C
Explanation: Local user accounts are created and stored directly on the FortiGate and do not rely on any external servers.

A12: Answer: B
Explanation: CNID defines which LDAP attribute will be used for identifying users. Common values include sAMAccountName for AD.

A13: Answer: B
Explanation: RADIUS provides both authentication and accounting functionalities, making it suitable for network access control.

A14: Answer: C
Explanation: FSSO monitors AD login events and maps users to IP addresses, enabling identity-based policy enforcement without re-authentication.

A15: Answer: C
Explanation: The FSSO Agent is installed on the Active Directory server to track login events and send them to the FortiGate.

Content inspection Practice Question
A1: Answer: B
Explanation: Certificate Inspection only analyzes the SSL/TLS handshake and certificate fields without decrypting the actual content.

A2: Answer: C
Explanation: For Deep Inspection to work, client devices must trust the FortiGate CA certificate to avoid certificate errors.

A3: Answer: C
Explanation: Certificate Inspection does not decrypt traffic and therefore does not require installing any trusted CA on client devices.

A4: Answer: B
Explanation: The SSL/SSH Inspection profile determines how FortiGate handles encrypted traffic in firewall policies.

A5: Answer: C
Explanation: FortiGuard classifies websites into categories like Gambling, Social Media, etc., which are used for filtering policies.

A6: Answer: C
Explanation: FortiGate uses category IDs in web filter profiles to block or allow content types defined by FortiGuard.

A7: Answer: C
Explanation: URL-based filtering allows the admin to manually define domains or patterns for allow/block actions.

A8: Answer: B
Explanation: Application Control uses a signature database to identify and take action on specific applications regardless of port.

A9: Answer: B
Explanation: Application Control can limit specific behaviors within an app, like allowing YouTube browsing but blocking uploads.

A10: Answer: B
Explanation: FortiGate’s Antivirus can inspect HTTP, HTTPS, FTP, and SMTP traffic for malware and viruses.

A11: Answer: C
Explanation: FortiSandbox provides behavior-based analysis to detect unknown or zero-day threats not yet identified by traditional signatures.

A12: Answer: C
Explanation: IPS scans network traffic and blocks attempts to exploit known vulnerabilities such as buffer overflows or SQL injection.

A13: Answer: C
Explanation: IPS sensors can be configured to block or monitor specific signatures or traffic patterns.

A14: Answer: C
Explanation: Custom IPS signatures must be part of a sensor profile, which is then linked to a firewall policy to take effect.

A15: Answer: B
Explanation: The SSL/SSH profile allows the administrator to configure SSL inspection exceptions for trusted or sensitive domains.

Routing Practice Question
A1: Answer: C
Explanation: Administrative Distance (AD) determines the trust level of a route; lower AD values are preferred when multiple routes exist for the same destination.

A2: Answer: B
Explanation: This is the correct CLI sequence for adding a static route in FortiGate.

A3: Answer: C
Explanation: SLA targets allow FortiGate to monitor metrics such as latency, jitter, and packet loss and switch traffic to better-performing links.

A4: Answer: B, C
Explanation: SD-WAN performance evaluation relies on latency and jitter to ensure quality of service.

A5: Answer: B
Explanation: SD-WAN automatically reroutes traffic to another member link that meets the SLA requirements.

A6: Answer: B
Explanation: SD-WAN requires at least two WAN interfaces added as members to perform link monitoring and traffic balancing.

A7: Answer: C
Explanation: Area 0, the backbone area, is mandatory in OSPF for inter-area communication.

A8: Answer: C
Explanation: The Router ID is a unique identifier for the OSPF router, often chosen automatically or set manually.

A9: Answer: C
Explanation: OSPF interface priority determines the DR/BDR election; higher values are preferred.

A10: Answer: C
Explanation: BGP peers communicate using a TCP session established on port 179.

A11: Answer: A
Explanation: In BGP configuration, `set as` sets the local AS number used by FortiGate.

A12: Answer: C
Explanation: Prefix lists define which IP prefixes should be accepted or denied during BGP route exchange.

A13: Answer: D
Explanation: This command block creates a prefix list that denies the specified IP range from being accepted in BGP routing.

A14: Answer: D
Explanation: Administrative distance is used to select the best route when multiple protocols offer routes to the same destination; lower values are preferred.

A15: Answer: D
Explanation: Matching Criteria (such as source, destination, application, or service) define the type of traffic the SD-WAN rule applies to.

VPN Practice Question
A1: Answer: B
Explanation: Web Mode enables browser-based access to internal web resources without requiring a VPN client like FortiClient.

A2: Answer: C
Explanation: SSL VPN Tunnel Mode requires FortiClient software to establish a full tunnel between the client and internal network.

A3: Answer: B
Explanation: The `ssl.root` interface is the virtual interface created by FortiGate for SSL VPN traffic, and is used in related firewall policies.

A4: Answer: C
Explanation: Web Mode supports browser-based access only and is limited to HTTP/HTTPS applications.

A5: Answer: B
Explanation: Phase 1 negotiates and establishes the secure tunnel, including authentication and encryption parameters.

A6: Answer: C
Explanation: The pre-shared key must be identical on both peers for Phase 1 negotiation to complete successfully.

A7: Answer: C
Explanation: The `src-subnet` and `dst-subnet` parameters define which subnets are permitted to send/receive encrypted traffic.

A8: Answer: B
Explanation: Site-to-Site VPNs are designed for permanent connections between fixed locations with static IPs.

A9: Answer: C
Explanation: Aggressive Mode is used when the peer IP is unknown or dynamic, as in remote access scenarios.

A10: Answer: C
Explanation: DPD ensures tunnel stability by detecting unreachable peers and terminating stale or dead connections.

A11: Answer: C
Explanation: This command activates DPD, allowing FortiGate to detect when a peer becomes unresponsive.

A12: Answer: B
Explanation: A firewall policy must be created to allow traffic from the `ssl.root` interface to the internal destination.

A13: Answer: C
Explanation: Configuring redundant IPsec tunnels ensures continuous connectivity in case the primary tunnel fails.

A14: Answer: C
Explanation: These are the correct SSL VPN settings to configure listening port and tunnel IP pool via CLI.

A15: Answer: B
Explanation: Phase 2 defines the encryption and encapsulation of the actual user data within the tunnel.