NSE7_SDW-7.2 Training Course

Fortinet NSE 7 - SD-WAN 7.2

Structured Learning & Certification Preparation

Table of Contents

Introduction

The NSE7_SDW-7.2 certification, part of the Fortinet NSE 7 track, focuses on advanced knowledge of secure SD-WAN deployment using FortiGate devices. It validates a candidate’s ability to design, configure, manage, and troubleshoot SD-WAN solutions in enterprise environments. This certification is relevant for network and security professionals working with modern distributed networks where performance, reliability, and centralized control are critical.

About This Training / Certification

This certification assesses intermediate to advanced competencies in implementing and operating Fortinet Secure SD-WAN solutions. It emphasizes practical understanding of traffic steering, application-aware routing, centralized orchestration, and network optimization. Typically positioned at an advanced level, it builds upon foundational networking and security knowledge and fits into a broader learning path focused on enterprise network architecture, secure connectivity, and performance-driven WAN design.

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

Area: SD-WAN Configuration
Candidates are expected to understand how to configure SD-WAN interfaces, define performance SLAs, and integrate WAN links into a logical SD-WAN construct. This includes knowledge of interface roles, health checks, and basic policy setup.

Area: Rules and Routing
This area covers the logic behind traffic steering decisions, including policy-based routing, application-aware routing, and dynamic path selection. Candidates should understand how routing decisions are influenced by performance metrics and business policies.

Area: Centralized Management
Focuses on managing SD-WAN deployments through centralized tools such as Fortinet management platforms. Candidates should understand device provisioning, policy deployment, and monitoring across multiple sites.

Area: SD-WAN Overlay Design and Best Practices
This domain emphasizes architectural considerations, including overlay network design, redundancy strategies, scalability, and best practices for resilient and efficient WAN connectivity.

Area: SD-WAN Troubleshooting
Candidates are expected to diagnose and resolve common SD-WAN issues. This includes interpreting logs, analyzing performance metrics, identifying misconfigurations, and applying systematic troubleshooting methodologies.

Detailed Knowledge Explanation

1. NSE7_SDW-7.2 Centralized management

Centralized management serves as the strategic foundation for large-scale SD-WAN deployments, effectively reducing the operational complexity inherent in managing numerous distributed nodes. By providing a unified platform, administrators can ensure configuration consistency across geographically dispersed sites, which is essential for maintaining enterprise-wide security and performance standards. This centralized approach allows for the efficient orchestration of devices, transitioning from manual, per-site management to a streamlined, holistic administrative model that ensures every branch adheres to corporate compliance and security requirements.

1. FortiManager

FortiManager functions as the primary orchestration tool within the Fortinet ecosystem, enabling unified control over multiple FortiGate and SD-WAN devices. Its core utility lies in configuration templates and version control, which work in tandem to prevent configuration drift and maintain regulatory compliance. Configuration templates

allow for the creation of standardized rules, interfaces, and policies that can be pushed to multiple branches simultaneously. Version control tracks every change made, providing a safety net for rolling back configurations if issues arise and documenting all modifications for auditing purposes. The technical workflow begins by registering all SD-WAN devices within the FortiManager and ensuring they are reachable over the network. Administrators then navigate to Policy and Objects and select Templates to define SD-WAN rules, SLA settings, and interfaces. Once saved, these templates are distributed by selecting specific device groups and pushing the configuration from FortiManager to the devices, followed by a synchronization verification to ensure uniformity across the fabric.

2. FortiAnalyzer

FortiAnalyzer acts as the central intelligence hub, specialized in logging, reporting, and deep data analysis. Strategically, it provides critical visibility into link utilization and SLA compliance by aggregating logs from all connected SD-WAN devices. This centralized log collection captures bandwidth usage, application traffic, and security events, transforming raw data into actionable performance insights. To implement this, administrators must enable log forwarding on individual FortiGate devices by navigating to Log Settings and then Remote Logging to specify the FortiAnalyzer IP address. Once the data is aggregated, administrators use the Reports and Custom Reports sections on FortiAnalyzer to create specialized views focusing on link utilization or application performance. These reports can be scheduled for automated delivery, providing long-term capacity planning data and rapid troubleshooting evidence.

3. Centralized Monitoring

Centralized monitoring synthesizes real-time network health data into a single-pane-of-glass view. This functionality is driven by continuous health checks and real-time alerts that notify administrators of link failures, SLA breaches, or performance drops via email, SMS, or the management dashboard. The strategic impact of this feature is the transition from reactive to proactive network maintenance; by defining thresholds, such as an alert for latency exceeding 100ms, administrators identify issues like link degradation as they occur rather than after users report a failure. Achieving this integration requires registering all devices within the management interface and customizing dashboards to display critical real-time metrics, including active SD-WAN links, current SLA performance, and device uptime.

4. FortiManager Enhancements

Advanced management features within FortiManager, specifically Role-Based Access Control (RBAC) and Device Groups, further refine administrative control. RBAC enforces security best practices by limiting administrative scope through specific roles where a Super Admin holds full system control, a Global Manager oversees multiple regional instances, and a Device Manager is restricted to specific device groups. Device Groups allow for the application of bulk policy updates to similar sites, ensuring that all branch offices maintain identical configurations. This structure reduces the administrative workload during rapid network expansion and ensures that security policies are applied consistently across the entire enterprise.

Zero-Touch Provisioning (ZTP)

Zero-Touch Provisioning (ZTP) is a transformative workflow for large-scale deployments that eliminates the need for manual on-site technical intervention. The ZTP process begins when a new device connects to the network

and automatically contacts FortiManager via a cloud discovery service or a predefined URL. To enable this, administrators configure the FortiGate using the `config system auto-install` command and ensure `set auto-install-config enable` is active. FortiManager then automatically pushes the necessary configurations and policies to the new device. This automation significantly reduces deployment timelines and ensures that every new branch is onboarded with a standardized, enterprise-approved configuration without requiring a technician to be present on-site.

5. FortiAnalyzer Enhancements

The integration of FortiAnalyzer with the Fortinet Security Fabric provides a holistic view of the network by correlating SD-WAN traffic data with security events. This synergy enhances visibility, allowing for automated response actions based on detected threats across multiple Fortinet devices. By viewing security and network performance through a single lens, organizations can better understand how security incidents impact application delivery and overall WAN performance, effectively serving as an SD-WAN-focused Security Operations Center (SOC).

Anomaly Detection and Incident Response

FortiAnalyzer utilizes machine learning (ML) algorithms for anomaly detection and behavioral analysis, which are vital for identifying DDoS attacks, compromised devices, or data exfiltration attempts. For incident response, administrators can use drill-down analysis to investigate top talkers, blocked security events, or geolocation-based attack sources. This provides the strategic value of multi-layered forensic analysis, helping to optimize traffic based on historical trends and remediate security threats by correlating global threat intelligence with local network behavior.

6. Centralized Monitoring and AI/ML Enhancements

Advanced troubleshooting and optimization are supported by tools such as packet capture, log replay, and path tracing. Packet capture allows for in-depth analysis of real-time traffic to identify dropped packets or unexpected patterns, while log replay enables historical analysis to find the root cause of intermittent issues by reviewing past network events. Path tracing, or traceroute analysis, is further used to identify inefficient routing across multiple WAN links, ensuring that the traffic follows the most logical and high-performance path.

AI/ML-Powered Network Optimization

AI/ML models enhance network efficiency by predicting bandwidth consumption patterns and suggesting optimal WAN paths based on real-time and historical SLA data. These automated SLA evaluations continuously monitor compliance and trigger alerts if a link degrades beyond acceptable levels. By leveraging these predictive capabilities, FortiManager can suggest smart routing optimizations that prevent network congestion and performance degradation before they impact the end-user experience. These centralized management tools collectively drive massive efficiency gains, providing the necessary oversight to transition to the granular control mechanisms of rules and routing.

7. Centralized management Practice Question

Q1: What is the primary function of FortiManager in an SD-WAN deployment?

A. To replace FortiAnalyzer for log collection and reporting.

B. To centralize configuration management and policy enforcement across multiple SD-WAN devices.

C. To provide real-time SD-WAN traffic visualization without any configuration capabilities.

D. To dynamically adjust BGP routing policies based on network conditions.

Q2: In FortiManager, which feature allows administrators to apply uniform configurations to multiple SD-WAN devices?

A. Device Groups

B. FortiAnalyzer Log Templates

C. SD-WAN Load Balancing

D. Dynamic Routing Protocols

Q3: Which of the following best describes the role of FortiAnalyzer in an SD-WAN environment?

A. It manages SD-WAN configuration policies.

B. It provides centralized log collection and analysis for network and security events.

C. It replaces FortiManager for centralized monitoring.

D. It is used only for real-time monitoring and cannot store historical data.

Q4: What is the benefit of using configuration templates in FortiManager?

A. They allow administrators to configure each SD-WAN device manually.

B. They enable standardized policy enforcement across multiple SD-WAN devices.

C. They replace the need for SD-WAN rules.

D. They function only in standalone FortiGate deployments.

Q5: How does FortiAnalyzer improve network troubleshooting in SD-WAN environments?

A. It allows administrators to configure SD-WAN rules dynamically.

B. It provides real-time and historical log analysis for detecting network and security anomalies.

C. It automatically blocks malicious traffic on all SD-WAN links.

D. It replaces the need for FortiManager in managing SD-WAN policies.

Q6: In a FortiManager deployment, what is the purpose of Zero-Touch Provisioning (ZTP)?

A. To automatically configure new SD-WAN devices upon connection without manual intervention.

B. To dynamically adjust SD-WAN link performance based on SLA metrics.

C. To centralize log collection from all FortiGate devices.

D. To create a direct VPN connection between FortiManager and SD-WAN devices.

Q7: Which FortiGate CLI command is used to check the connectivity between FortiManager and an SD-WAN device?

A. `get router info routing-table all`

B. `execute ping <FortiManager_IP>`

C. `diagnose sys sdwan health-check`

D. `show firewall policy`

Q8: In FortiAnalyzer, what type of data can administrators analyze?

A. SD-WAN traffic statistics, security logs, and SLA compliance reports.

B. Only real-time security events, without historical records.

C. Only routing updates from OSPF and BGP.

D. Only bandwidth utilization metrics, without security-related logs.

Q9: Which feature of FortiManager allows administrators to track and revert configuration changes?

A. Routing Policy Management

B. Version Control

C. SLA Monitoring

D. Dynamic SD-WAN Rules

Q10: How does centralized monitoring benefit SD-WAN operations?

A. It provides a single-pane-of-glass view for real-time network health and performance monitoring.

B. It forces all traffic through a single WAN link for better visibility.

C. It eliminates the need for SD-WAN rules.

D. It only applies to FortiGate devices operating in standalone mode.

2. NSE7_SDW-7.2 Rules and Routing

Rules and routing serve as the "brain" of the SD-WAN architecture, facilitating the dynamic direction of traffic based on real-time network conditions. Unlike traditional static networking, SD-WAN routing decisions are performance-aware, ensuring that traffic is steered toward the most suitable path based on application requirements, priority, and current link health.

1. SD-WAN Rules

SD-WAN rules are the policies used to determine the best path for traffic based on specific conditions such as source and destination IP addresses, application categories, and services. These rules are matched sequentially, starting from the highest priority, meaning their order is critical for effective traffic steering. High-priority rules are typically reserved for business-critical traffic like voice and video conferencing to ensure they are routed over low-latency links. For example, a rule might be defined to route all traffic matching the Video Conferencing application category through a high-performance fiber link while a lower-priority rule sends social media traffic to a backup broadband connection.

2. Static Routing

Static routing provides a foundational layer of predictable traffic flows by manually directing traffic to specific next-hop addresses. This involves defining a destination network and assigning it to a specific gateway or ISP. A common implementation is the configuration of a default route, or 0.0.0.0/0, directed toward an ISP gateway or an SD-WAN member. While static routing is simple and reliable for stable environments, its manual nature makes it rigid in dynamic environments where link availability and performance fluctuate constantly.

3. Dynamic Routing Protocols

Dynamic routing protocols like OSPF and BGP are synthesized into SD-WAN to provide the scalability and resiliency needed for complex environments. OSPF is often preferred for medium-sized networks due to its fast convergence speeds, allowing the network to adjust automatically if a WAN link fails. In contrast, BGP is the standard for global, multi-domain deployments where scalability is paramount, as it allows for the management of traffic across multiple ISPs and continents. These protocols ensure that branch offices can automatically learn and update paths to one another without constant manual intervention, providing the necessary resiliency for the SD-WAN overlay.

4. Route Tables and Route Priority

The FortiGate routing hierarchy is essential for correct traffic steering and troubleshooting, as the system evaluates routes in a specific order: Connected routes have the highest priority, followed by Static routes, Policy-Based Routing (PBR), Dynamic Routing Protocols (OSPF, BGP), and finally SD-WAN Rules. Understanding this hierarchy is strategically important because a static route or a PBR entry might override an intended SD-WAN rule. Administrators verify active routes using the `get router info routing-table all` command, which displays all active routes along with their priority, cost, and next-hop decisions.

5. Policy-Based Routing (PBR)

Policy-Based Routing (PBR) acts as a mechanism to override standard routing behavior by enforcing specific traffic requirements before SD-WAN rules are processed. PBR is often used to force specific traffic types, such as VoIP using UDP port 5060, through a dedicated WAN link regardless of the default routing table entries. This is configured by defining the source, destination, and protocol within the PBR settings and specifying the outgoing interface. This capability is critical for meeting specific ISP requirements or ensuring mission-critical applications bypass standard load-balancing logic to maintain performance integrity.

6. Equal-Cost Multi-Path (ECMP) Routing

ECMP routing allows the SD-WAN to balance traffic across multiple WAN links that share the same cost metric. In FortiOS, administrators configure this using the `set v4-ecmp-mode` command, and the system supports a maximum of 4 equal-cost paths. Traffic is distributed using hashing algorithms based on source-destination pairs, which increases overall bandwidth availability and provides redundancy. If one path in the ECMP group degrades or fails, the traffic is redistributed across the remaining active paths, improving load distribution efficiency in dynamic routing environments.

7. Advanced BGP Features in SD-WAN

Advanced BGP features like Local Preference and Multi-Exit Discriminator (MED) are used to influence traffic flow between Autonomous Systems. Local Preference is used internally within an AS to prefer a specific outbound route, where higher values are preferred. Conversely, MED is used to influence how external traffic enters the network, where lower values are preferred. Integration of BGP with SD-WAN allows for dynamic ISP selection and ensures fast convergence during link failures, optimizing WAN performance by dynamically adjusting paths based on learned routing information. This robust routing logic is the necessary precursor to configuring the foundational interfaces and health settings of the SD-WAN fabric.

8. Rules and Routing Practice Question

Q1: In FortiGate SD-WAN, what is the primary function of an SD-WAN rule?

A. To configure a default static route for all network traffic.

B. To define specific routing policies for traffic based on conditions like application, source, and destination.

C. To replace dynamic routing protocols such as OSPF and BGP.

D. To prevent traffic from using multiple WAN links.

Q2: When configuring SD-WAN rules in FortiGate, which factor takes precedence in determining traffic routing?

A. The lowest priority number assigned to a rule.

B. The highest priority number assigned to a rule.

C. The link with the highest bandwidth.

D. The link with the lowest packet loss.

Q3: Which of the following statements about static routing in FortiGate SD-WAN is TRUE?

A. Static routes automatically update when a WAN link fails.

B. Static routes require manual configuration and do not change dynamically.

C. Static routes are always preferred over dynamic routes.

D. Static routes are only used in SD-WAN environments with a single WAN link.

Q4: What is the main advantage of using dynamic routing protocols such as OSPF in an SD-WAN deployment?

A. They allow administrators to manually configure every route.

B. They provide automatic route adjustments based on network topology changes.

C. They prevent SD-WAN rules from being applied.

D. They eliminate the need for a default route.

Q5: Which routing protocol is commonly used in SD-WAN deployments that involve multiple ISPs and require global scalability?

A. OSPF

B. RIP

C. BGP

D. EIGRP

Q6: In a dual-WAN SD-WAN setup, which feature allows multiple equal-cost paths to be used for load balancing?

A. SD-WAN failover

B. OSPF link-state advertisements

C. Equal-Cost Multi-Path (ECMP)

D. Static routes with different administrative distances

Q7: Which of the following is a key difference between SD-WAN rules and Policy-Based Routing (PBR)?

A. SD-WAN rules operate before PBR in the routing decision process.

B. PBR rules override SD-WAN rules.

C. PBR is used only for static routing, while SD-WAN rules are dynamic.

D. SD-WAN rules only work with BGP, while PBR supports OSPF.

Q8: What happens when a WAN link used by an SD-WAN rule exceeds its SLA threshold for latency and jitter?

A. Traffic continues using the same link regardless of the performance.

B. The SD-WAN rule automatically switches traffic to another available WAN link.

C. The administrator must manually change the WAN link.

D. The firewall drops all packets from the affected link.

Q9: When using BGP in an SD-WAN environment, what is the purpose of MED (Multi-Exit Discriminator)?

A. It allows the local router to determine the best path based on the lowest MED value.

B. It forces all traffic to use a single WAN link.

C. It controls bandwidth allocation between different VPN tunnels.

D. It replaces the need for SD-WAN rules.

Q10: Which FortiGate command allows an administrator to view all current SD-WAN routes?

A. `get router info routing-table all`

B. `show system interface`

C. `diagnose sys sdwan health-check`

D. `execute ping`

3. NSE7_SDW-7.2 SD-WAN configuration

SD-WAN configuration is the backbone of the deployment, where physical and virtual links are transformed into a cohesive, performance-aware logical network. This process involves defining the participants in the SD-WAN, establishing the criteria for performance, and setting the rules for how traffic is distributed across available resources to maximize reliability.

1. SD-WAN Interfaces and Members

The configuration begins with the identification and definition of SD-WAN members, which can be physical ethernet ports or virtual interfaces like VLANs. In the Network menu under Interfaces, administrators add members and assign IP addresses provided by the ISP. Configuring these interfaces involves setting roles, such as primary or backup, and establishing load-balancing weights. For example, if WAN1 has a weight of 80 and WAN2 has a weight of 20, the system will direct 80% of the traffic to the more robust WAN1 link, ensuring efficient utilization of high-speed fiber versus secondary broadband.

2. Service Level Agreement (SLA)

SLA benchmarks ensure application quality by defining acceptable thresholds for performance. Administrators navigate to the Performance SLA section to define maximum acceptable values for latency, such as 50ms, jitter at 10ms, and packet loss at less than 1%. If a link exceeds these thresholds, SD-WAN can take automated

actions like rerouting traffic to a better link or sending alerts. These benchmarks ensure that latency-sensitive applications like video calls always traverse the highest-quality path.

3. Load Balancing and Path Selection

Load balancing intelligently distributes traffic across WAN links to prevent congestion. Volume-based load balancing distributes traffic proportionally based on bandwidth, while session-based balancing assigns new sessions to interfaces in a round-robin fashion. Application-based balancing is more granular, routing specific traffic types to dedicated links based on their needs. Failover rules complement this by designating a preferred link for important traffic and configuring an automatic switchover if that link fails or violates SLA benchmarks.

4. Application Awareness

Application awareness utilizes Deep Packet Inspection (DPI) to identify over thousands of different application types, moving beyond simple port and protocol matching. This allows the SD-WAN to prioritize business-critical applications like Microsoft Teams while throttling non-essential traffic like social media. By recognizing the application itself, the system prevents non-critical traffic from contending for resources required by essential business operations, ensuring a consistent user experience.

5. SD-WAN Health Monitoring

Health monitoring relies on three primary probing mechanisms: ICMP (Ping) for basic connectivity, HTTP probes for application-level connectivity, and TCP probes for verifying specific service availability and ensuring firewall traversal. These probes track real-time link performance metrics, which can be visualized through FortiView or the CLI using the `diagnose sys sdwan health-check` command. Visualizing this data is essential for validating policy effectiveness and identifying performance degradation before a total link failure occurs.

6. Redundancy and Failover

Redundancy is managed through Active-Active or Active-Standby modes. In Active-Active mode, all WAN links are simultaneously used for load balancing. In Active-Standby mode, a primary link handles traffic while the backup link remains idle. Failover is triggered by SLA violations, such as latency exceeding 100ms or packet loss exceeding 5%. These mechanisms ensure network resilience and session persistence, automatically switching traffic to the best available path without manual intervention when a link degrades.

7. SD-WAN VPN Integration

The integration of Site-to-Site and Remote Access VPNs with SD-WAN provides secure connectivity across the public internet. By using IPsec encryption with AES-256 and Multi-Factor Authentication (MFA), the SD-WAN ensures data confidentiality. A strategic advantage is that SD-WAN can dynamically select the best VPN tunnel based on real-time SLA metrics. If a primary IPsec tunnel over a fiber link experiences high jitter, SD-WAN automatically reroutes the VPN traffic through a backup tunnel, ensuring secure and stable communication. These interface and health settings create the reliable fabric required for a high-level overlay design.

8. SD-WAN configuration Practice Question

Q1: Which of the following statements about SD-WAN interfaces in FortiGate is TRUE?

A. Only physical interfaces can be added as SD-WAN members.

B. WAN interfaces in SD-WAN must have static IP addresses.

C. SD-WAN members can include both physical and virtual interfaces.

D. Only one WAN interface can be configured as a primary link.

Q2: What is the purpose of setting up an SLA (Service Level Agreement) in SD-WAN?

A. To manually assign bandwidth quotas to users.

B. To ensure that all traffic is always routed through the primary WAN link.

C. To define performance thresholds for WAN links and trigger failover when necessary.

D. To prevent SD-WAN from switching links dynamically.

Q3: In FortiGate SD-WAN, which of the following metrics can be used to define an SLA policy?

A. Bandwidth utilization

B. Latency

C. Jitter

D. Packet loss

E. Number of concurrent connections

Q4: Which of the following best describes the function of SD-WAN Load Balancing in FortiGate?

A. It prioritizes specific traffic types and ignores SLA performance metrics.

B. It dynamically distributes network traffic across multiple WAN links based on policies.

C. It forces all traffic through a single WAN link to ensure stability.

D. It only works with static routes and cannot be adjusted dynamically.

Q5: In FortiGate SD-WAN, how can application-aware routing be configured?

A. By defining SD-WAN rules that prioritize specific applications based on their performance needs.

B. By setting up NAT policies to redirect application traffic.

C. By allowing only HTTP and HTTPS traffic through SD-WAN.

D. By using static routing instead of SD-WAN dynamic policies.

Q6: When configuring SD-WAN, what is the benefit of configuring a secondary (backup) WAN link?

A. It ensures that SD-WAN always uses the slowest link first.

B. It provides redundancy in case the primary WAN link fails or degrades.

C. It blocks traffic on the secondary link unless the administrator manually switches it.

D. It prevents failover by always keeping traffic on the primary WAN link.

Q7: Which of the following commands in FortiGate can be used to monitor SD-WAN health checks?

A. `diagnose sys sdwan health-check`

B. `show system interface`

C. `get router info routing-table`

D. `execute ping`

Q8: Which SD-WAN feature helps in automatically rerouting traffic when a link exceeds SLA thresholds?

A. Manual link selection

B. Static routing

C. Dynamic path selection

D. NAT policies

Q9: How does FortiGate SD-WAN integrate with VPNs?

A. It allows SD-WAN rules to select the best VPN tunnel dynamically.

B. It disables SD-WAN functionality when VPN tunnels are active.

C. It forces all VPN traffic through a single static WAN interface.

D. It only supports VPN integration for IPsec tunnels, not SSL VPNs.

Q10: What happens if an SD-WAN link exceeds its SLA limits for latency and packet loss?

A. The link continues to be used regardless of SLA violations.

B. The SD-WAN policy automatically switches traffic to another WAN link.

C. The administrator must manually disable the link.

D. The FortiGate firewall blocks all outbound traffic.

4. NSE7_SDW-7.2 SD-WAN overlay design and best practices

Overlay design is strategically important for structuring how various sites in an SD-WAN environment communicate, balancing the trade-offs between management simplicity and the performance requirements of various applications to ensure the network topology supports the organization's specific communication patterns.

1. Topology Design

Topology design primarily involves choosing between Hub-and-Spoke and Full-Mesh configurations. Hub-and-Spoke is simpler to manage and ideal for centralized traffic but can introduce latency for branch-to-branch communication as all data must pass through the hub. Full-Mesh topology allows sites to communicate directly, providing the lowest possible latency and high redundancy, though it is more complex to manage and consumes more system resources in large-scale environments due to the number of direct connections.

2. Tunnel Configuration

Secure communication in the overlay is achieved through IPsec tunnels and Auto-Discovery VPN (ADVPN). Static IPsec tunnels are reliable for predictable communication, but ADVPN significantly reduces complexity by dynamically establishing on-demand tunnels directly between spoke sites. In an ADVPN environment, the system creates a shortcut tunnel for a specific session, such as a video call, and then tears down the tunnel once the

session is complete. This combines the management simplicity of a hub-based design with the low-latency performance of a mesh.

3. Hybrid Topology

A hybrid topology combines the benefits of both architectures by using Hub-and-Spoke for general traffic and Full-Mesh ADVPN for high-priority traffic. In this design, general traffic such as ERP access is routed through the central hub for policy enforcement, while latency-sensitive traffic like voice and video is handled via direct dynamic tunnels between branches. This optimization ensures that bandwidth is used efficiently while maintaining centralized security control over the majority of the network traffic.

4. SD-WAN Overlay Security Considerations

Security within the overlay is maintained through Zero Trust Network Access (ZTNA) and data encryption. ZTNA enforces strict identity-based access control, preventing lateral movement within the network. Data confidentiality is ensured through IPsec encryption for all tunnels and TLS for control traffic. To ensure ADVPN performance monitoring does not compromise security, administrators use `set monitor enable` on the VPN settings. Additionally, FortiAnalyzer monitors abnormal traffic patterns to detect DDoS attacks, allowing the FortiGate to apply rate limiting at the SD-WAN edge.

5. WAN Edge High Availability (HA)

To prevent downtime at the WAN edge, organizations implement redundancy solutions such as Dual FortiGate HA and the Virtual Router Redundancy Protocol (VRRP). Dual FortiGate HA configurations, which can be Active-Passive or Active-Active, ensure that a hardware failure does not interrupt services. VRRP allows two SD-WAN edge devices to act as a single virtual router, providing seamless failover if one device fails. These configurations, managed via the `config system vrrp` command, ensure that both hardware and ISP failures are mitigated effectively.

6. WAN Optimization Strategies

WAN optimization techniques like Forward Error Correction (FEC) and TCP/UDP acceleration enhance performance over lossy links such as LTE or satellite. FEC adds redundant data packets to reconstruct lost data, reducing retransmissions. Furthermore, Cloud OnRamp optimizes SaaS performance by providing direct connectivity to applications like Office 365, reducing the number of intermediate hops and decreasing overall latency. Sound design principles ensure a future-proof network, transitioning the focus to the diagnostic methodologies required for maintaining these systems.

7. SD-WAN overlay design and best practices Practice Question

Q1: In a Hub-and-Spoke SD-WAN topology, where does branch traffic typically flow?

A. Directly between branch sites without using a central hub.

B. From branch sites to a central hub before reaching its destination.

C. Randomly through multiple available paths.

D. Only through a single WAN link at all times.

Q2: Which SD-WAN topology is best suited for organizations where branch sites frequently communicate with each other?

A. Hub-and-Spoke

B. Full-Mesh

C. Star Topology

D. Ring Topology

Q3: Which tunneling method in SD-WAN allows branch sites to establish direct VPN connections dynamically without predefined tunnels?

A. Static IPsec VPN

B. ADVPN (Auto-Discovery VPN)

C. GRE Tunnel

D. MPLS VPN

Q4: What is a primary advantage of using IPsec tunnels in an SD-WAN deployment?

A. They allow unencrypted traffic to pass between sites.

B. They improve security by encrypting and authenticating traffic between SD-WAN endpoints.

C. They dynamically optimize application traffic across multiple paths.

D. They eliminate the need for any SD-WAN rules.

Q5: Which method can be used in SD-WAN to ensure that critical applications, such as video conferencing, receive the best network performance?

A. Load balancing based on bandwidth usage only

B. Static routing with no SLA monitoring

C. Traffic classification with SLA-based path selection

D. Always routing all traffic through a single WAN link

Q6: What is the primary benefit of using a Hybrid SD-WAN topology?

A. It enforces centralized traffic routing through a single data center.

B. It optimizes both branch-to-branch and branch-to-hub communication.

C. It eliminates the need for multiple WAN links.

D. It prevents SD-WAN from dynamically adjusting traffic paths.

Q7: What is the primary function of Equal-Cost Multi-Path (ECMP) in SD-WAN?

A. To route all traffic through a single static link

B. To distribute traffic evenly across multiple WAN links with the same cost metric

C. To block non-business applications on SD-WAN links

D. To enforce policy-based routing rules without failover

Q8: Which security best practice should be implemented in an SD-WAN overlay network to protect against unauthorized access?

A. Disable encryption to improve performance

B. Implement Zero Trust Network Access (ZTNA) for SD-WAN devices

C. Allow all traffic between SD-WAN sites without restrictions

D. Disable firewall policies on SD-WAN links

Q9: How can an SD-WAN deployment ensure WAN link redundancy?

A. By using a single ISP for all connections

B. By configuring Active-Active or Active-Standby WAN links

C. By relying only on static routes without failover

D. By disabling SLA monitoring to keep all links active

Q10: What SD-WAN optimization technique helps improve performance over high-latency networks such as LTE or satellite connections?

A. Forward Error Correction (FEC)

B. Disabling encryption

C. Routing all traffic through a single link

D. Increasing the packet loss rate to balance traffic

5. NSE7_SDW-7.2 SD-WAN troubleshooting

Troubleshooting is a systematic discipline essential for maintaining the stability and uptime of an SD-WAN infrastructure. It involves a structured approach to diagnosing physical connectivity issues, performance degradations, and logical configuration errors to ensure consistent network service delivery across all branch locations.

1. Common Issues

The most frequent failure points in an SD-WAN environment include rule misconfigurations, SLA violations, and routing anomalies. Rule misconfigurations result in traffic being steered toward incorrect paths, often requiring a check of matching conditions and rule priority. SLA violations occur when links fail to meet performance thresholds, and routing anomalies like OSPF or BGP adjacency failures can lead to unreachable destinations. Troubleshooting these issues involves identifying missing or incorrect routes and looking for mismatched network advertisements between SD-WAN nodes.

2. Diagnostic Tools

The CLI provides the most critical tools for real-time diagnostic analysis. The command `diagnose sys sdwan service` is used to verify SD-WAN rule matching, revealing exactly which rule is being applied to specific traffic. The command `diagnose sys sdwan health-check` displays the status of WAN links, including real-time latency, jitter, and packet loss metrics. For traffic distribution insights, administrators use `diagnose debug application sdwan`, which provides real-time information on how rules are being applied to active sessions.

3. Troubleshooting Workflow

A systematic three-step troubleshooting workflow involves scoping the issue, applying temporary mitigation, and identifying the root cause. Scoping determines if the problem is rooted in rules, link performance, or hardware. Temporary mitigation might involve manually rerouting traffic to a backup link or adjusting rule priorities. Finally, the root cause is identified, which may involve correcting misconfigured rules or working with ISPs to resolve faulty hardware, ensuring a permanent resolution to the problem.

4. Physical and WAN Link-Level Troubleshooting

Before addressing complex policies, administrators must verify underlying link stability. This includes checking interface status using `get system interface` to ensure they are up and have the correct IP. Indicators of WAN issues include packet loss exceeding 5% or high latency spikes. If fragmentation is suspected, administrators check MTU values and adjust them using `set mtu-override`. For VPN tunnels, performance is often improved by setting MSS clamping via `set tcp-mss-sender` to avoid packet fragmentation across the WAN.

5. Advanced SD-WAN Troubleshooting

Advanced scenarios often involve cases where SLA failovers do not trigger or load balancing fails. If a failover does not occur despite link degradation, the SLA thresholds may be set too high and require reduction to ensure failover happens sooner. If load balancing is not distributing traffic, administrators must verify that ECMP is enabled and that multiple equal-cost routes exist. Using the `diagnose debug flow filter addr` command helps determine if traffic is being dropped or misrouted due to firewall rule conflicts.

6. SD-WAN VPN and ADVPN Troubleshooting

Troubleshooting VPN and ADVPN failures requires debugging IKE negotiations and verifying routing advertisements. If an IPsec tunnel fails to establish, administrators check for configuration mismatches using `diagnose vpn tunnel list` and debug IKE negotiation with `diagnose debug application ike -1`. For ADVPN issues, the focus shifts to verifying that OSPF or BGP are advertising the correct routes between hubs and spokes, as routing failures often prevent the dynamic discovery of shortcut paths.

7. FortiAnalyzer for Deep Analysis

FortiAnalyzer plays a critical role in troubleshooting intermittent issues by providing long-term log correlation and analysis. The log replay feature allows administrators to view past traffic flows to identify when and why a specific routing decision was made. By correlating logs from multiple sites, administrators can identify ISP-specific failures that affect an entire region. This historical perspective is vital for identifying trends in SLA violations and optimizing SD-WAN policies to avoid recurring bottlenecks, representing the hallmark of an SD-WAN expert.

8. SD-WAN troubleshooting Practice Question

Q1: If SD-WAN traffic is not following the expected path, which of the following should be checked first?

A. The firewall’s default deny policy.

B. The SD-WAN rule priority order.

C. The power supply of the FortiGate device.

D. The admin login attempts.

Q2: An administrator is troubleshooting SD-WAN failover issues. Which of the following is the most likely cause of failure?

A. The primary WAN link is not exceeding SLA thresholds.

B. The backup WAN link is in active mode.

C. The administrator has changed the FortiGate hostname.

D. The FortiGate is operating in transparent mode.

Q3: A remote branch is experiencing frequent disconnections over SD-WAN. What should the administrator check first?

A. The number of firewall rules applied to the branch.

B. FortiAnalyzer logs for historical SLA violations.

C. The time synchronization settings.

D. The admin user password policy.

Q4: A branch office reports that some applications are performing poorly over SD-WAN, even though bandwidth is sufficient. What could be the cause?

A. The FortiGate device is running in standalone mode.

B. High jitter and packet loss on the WAN link.

C. A missing administrative password change policy.

D. Incorrectly configured firewall policies.

Q5: An administrator needs to verify which SD-WAN rule is applied to a specific traffic flow. Which command should be used?

A. `execute traceroute`

B. `diagnose sys sdwan service`

C. `show firewall policy`

D. `get router info ospf neighbor`

Q6: A company is experiencing intermittent performance issues with their cloud-based applications over SD-WAN. What is the best approach to diagnose the problem?

A. Change the IP addressing scheme of the internal network.

B. Delete all SD-WAN rules and reconfigure from scratch.

C. Use `diagnose sys sdwan health-check` to monitor link SLA metrics.

D. Disable all firewall policies temporarily.

Q7: A company using ADVPN notices that some branch sites cannot dynamically establish direct tunnels. What is the most likely cause?

A. The VPN tunnel encryption settings are incorrect.

B. The FortiAnalyzer logging service is disabled.

C. The SD-WAN feature is not supported on the FortiGate device.

D. Misconfigured dynamic routing protocols such as OSPF or BGP.

Q8: A branch office cannot access the internet through SD-WAN, but internal branch-to-branch communication works fine. What should the administrator check first?

A. The default user login history.

B. The FortiGate power supply.

C. SD-WAN rules for local internet breakout configuration.

D. The firewall's SNMP monitoring settings.

Q9: A company is experiencing slow performance on a secondary SD-WAN link, but there are no SLA violations. What could be the cause?

A. The firewall is blocking all incoming traffic.

B. The WAN link has a high congestion level but is not exceeding SLA limits.

C. The administrator is using an outdated login credential.

D. The FortiGate’s system clock is not synchronized.

Q10: An administrator wants to analyze SD-WAN performance trends over the past month. Which tool should be used?

A. SNMP-based alerting system

B. CLI-based real-time monitoring

C. FortiGate built-in syslog viewer

D. FortiAnalyzer

Learning Path & Study Advice

A structured approach should begin with strengthening core networking concepts such as routing, VPNs, and firewall policies. From there, learners should progress to understanding SD-WAN fundamentals, including how traffic steering and performance SLAs function. Practical exposure to configuration and monitoring is important to reinforce theoretical knowledge. As understanding deepens, focus should shift to design considerations and troubleshooting techniques, ensuring the ability to analyze real-world scenarios and apply appropriate solutions. Emphasis should remain on conceptual clarity and practical comprehension rather than memorization.

Who This PDF Is For

This document is intended for network engineers, security professionals, and IT specialists who are involved in designing, deploying, or managing WAN infrastructures. It is suitable for individuals with prior experience in networking and firewall technologies who are seeking to deepen their understanding of SD-WAN concepts. Those working in enterprise environments or managed services roles will benefit most from this material, particularly if they are responsible for optimizing network performance and reliability.

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/NSE-7-Network-Security-Architect/NSE7_SDW-7.2.html

Online Flashcards (Quizlet):

https://quizlet.com/user/AAAdemy/folders/nse7_sdw-72-fortinet-nse7-sd-wan-72-flashcards-aaademy?i=6zfa5t&x=1xqt

Attachment : Answers by Knowledge Point

SD-WAN configuration Practice Question
A1: Answer: C. SD-WAN members can include both physical and virtual interfaces.
Explanation: SD-WAN in FortiGate supports both physical interfaces (e.g., ethernet ports) and virtual interfaces (e.g., VLANs, tunnels) as SD-WAN members. Options A, B, and D are incorrect because SD-WAN supports both dynamic and static IPs, and multiple WAN interfaces can act as primary or backup links.
A2: Answer: C. To define performance thresholds for WAN links and trigger failover when necessary.
Explanation: SLAs in SD-WAN monitor key network parameters such as latency, jitter, and packet loss. If a WAN link fails to meet SLA thresholds, SD-WAN can dynamically reroute traffic to a better-performing link.
A3: Answer: B. Latency, C. Jitter, D. Packet loss.
Explanation: SLA policies in FortiGate SD-WAN typically measure latency (delay in ms), jitter (variation in delay), and packet loss (%) to assess WAN link performance. Bandwidth utilization and concurrent connections are not SLA parameters but may be used for monitoring network load.
A4: Answer: B. It dynamically distributes network traffic across multiple WAN links based on policies.
Explanation: SD-WAN load balancing optimizes network performance by distributing traffic across available WAN links based on bandwidth utilization, application type, and SLA performance metrics. Options A, C, and D are incorrect as SD-WAN does not force traffic through a single link and does support dynamic routing.
A5: Answer: A. By defining SD-WAN rules that prioritize specific applications based on their performance needs.
Explanation: Application-aware routing allows FortiGate SD-WAN to identify traffic types (e.g., VoIP, video streaming) and direct them to the most optimal WAN link. NAT and static routing are unrelated to application-based routing.
A6: Answer: B. It provides redundancy in case the primary WAN link fails or degrades.
Explanation: A backup WAN link ensures high availability in SD-WAN. If the primary WAN fails or performs poorly, SD-WAN can automatically switch to the secondary WAN based on SLA thresholds.
A7: Answer: A. `diagnose sys sdwan health-check`.

Explanation: This command provides detailed real-time diagnostics on SD-WAN link health, showing latency, jitter, and packet loss. The other commands serve different functions:

- B. `show system interface` - Displays general interface settings.
- C. `get router info routing-table` - Shows the current routing table.
- D. `execute ping` - Only checks connectivity but does not provide detailed SD-WAN health metrics.

A8: Answer: C. Dynamic path selection.
Explanation: Dynamic path selection allows FortiGate SD-WAN to continuously monitor WAN link performance and reroute traffic automatically when a link fails to meet SLA standards.
A9: Answer: A. It allows SD-WAN rules to select the best VPN tunnel dynamically.
Explanation: FortiGate SD-WAN integrates with VPNs by dynamically selecting the best VPN tunnel based on latency, jitter, and packet loss metrics.
A10: Answer: B. The SD-WAN policy automatically switches traffic to another WAN link.
Explanation: SD-WAN automatically reroutes traffic if a WAN link exceeds SLA thresholds, ensuring optimal performance.

Rules and Routing Practice Question
A1: Answer: B. To define specific routing policies for traffic based on conditions like application, source, and destination.
Explanation: SD-WAN rules are used to prioritize and control how traffic flows through available WAN links, based on conditions such as IP address, application type, and service type. They do not replace dynamic routing protocols but work alongside them.
A2: Answer: B. The highest priority number assigned to a rule.
Explanation: SD-WAN rules are evaluated in descending order of priority, meaning that higher-priority rules are matched first. If no rule matches, traffic is routed based on the default SD-WAN strategy.
A3: Answer: B. Static routes require manual configuration and do not change dynamically.
Explanation: Static routes must be manually configured and do not automatically update in response to network changes. Dynamic routing protocols (such as OSPF and BGP) are used when automatic adjustments are needed.
A4: Answer: B. They provide automatic route adjustments based on network topology changes.
Explanation: OSPF dynamically learns and updates routes based on real-time network conditions, making it useful in SD-WAN environments where link failures or performance changes may require automatic rerouting.
A5: Answer: C. BGP
Explanation: BGP (Border Gateway Protocol) is ideal for large-scale SD-WAN deployments involving multiple ISPs because it supports global scalability and advanced route selection mechanisms. OSPF is typically used for internal networks, while RIP and EIGRP are less common in modern SD-WAN solutions.
A6: Answer: C. Equal-Cost Multi-Path (ECMP)
Explanation: ECMP enables FortiGate SD-WAN to distribute traffic across multiple WAN links that have the same cost metric, improving network performance and resilience.
A7: Answer: B. PBR rules override SD-WAN rules.
Explanation: Policy-Based Routing (PBR) operates before SD-WAN rules and allows manual traffic routing based on specific conditions, which can override SD-WAN's default path selection.
A8: Answer: B. The SD-WAN rule automatically switches traffic to another available WAN link.

Explanation: SD-WAN continuously monitors WAN links using SLA performance metrics (latency, jitter, packet loss) and dynamically shifts traffic to a better-performing link if the active link degrades.
A9: Answer: A. It allows the local router to determine the best path based on the lowest MED value.
Explanation: MED (Multi-Exit Discriminator) is a BGP attribute used to indicate the preferred path into an AS (Autonomous System). The lowest MED value is preferred by other BGP peers.
A10: Answer: A. `get router info routing-table all`
Explanation: This command displays all active static and dynamic routes used by FortiGate, including SD-WAN routes. The other commands serve different purposes:

- `show system interface` - Displays interface configurations.
- `diagnose sys sdwan health-check` - Shows SD-WAN link health status.
- `execute ping` - Tests connectivity but does not display routing information.

Centralized management Practice Question
A1: Answer: B. To centralize configuration management and policy enforcement across multiple SD-WAN devices.
Explanation: FortiManager is a centralized management platform that simplifies the configuration, deployment, and monitoring of multiple SD-WAN devices. It does not replace FortiAnalyzer (Option A) and does not function primarily as a real-time traffic visualization tool (Option C).
A2: Answer: A. Device Groups
Explanation: Device Groups in FortiManager allow administrators to apply the same configurations to multiple SD-WAN devices, ensuring consistency across all managed devices. FortiAnalyzer (Option B) is used for logging, and SD-WAN Load Balancing (Option C) and Dynamic Routing (Option D) are not related to centralized configuration management.
A3: Answer: B. It provides centralized log collection and analysis for network and security events.
Explanation: FortiAnalyzer is designed for centralized log collection, forensic analysis, and security event reporting in SD-WAN environments. It does not manage configurations (Option A) and does not replace FortiManager (Option C).
A4: Answer: B. They enable standardized policy enforcement across multiple SD-WAN devices.
Explanation: Configuration templates in FortiManager allow administrators to define uniform policies and configurations, which can be applied to multiple SD-WAN devices, reducing manual effort and ensuring consistency.
A5: Answer: B. It provides real-time and historical log analysis for detecting network and security anomalies.
Explanation: FortiAnalyzer centralizes log data, allowing administrators to detect trends, investigate anomalies, and improve network troubleshooting. It does not configure SD-WAN rules (Option A) or replace FortiManager (Option D).
A6: Answer: A. To automatically configure new SD-WAN devices upon connection without manual intervention.
Explanation: Zero-Touch Provisioning (ZTP) enables newly deployed SD-WAN devices to automatically receive configurations from FortiManager, reducing manual setup time and ensuring consistent configurations.
A7: Answer: B. `execute ping <FortiManager_IP>`
Explanation: To verify connectivity between FortiManager and an SD-WAN device, administrators can use the ping command. Other commands are used for different purposes, such as viewing routing tables (Option A) or firewall policies (Option D).
A8: Answer: A. SD-WAN traffic statistics, security logs, and SLA compliance reports.

Explanation: FortiAnalyzer provides comprehensive logging and reporting, including SD-WAN traffic trends, security events, and SLA compliance analysis. It is not limited to real-time logs or only routing updates.
A9: Answer: B. Version Control
Explanation: FortiManager provides version control, allowing administrators to track changes, roll back configurations, and ensure compliance in SD-WAN deployments.
A10: Answer: A. It provides a single-pane-of-glass view for real-time network health and performance monitoring.
Explanation: Centralized monitoring in FortiManager and FortiAnalyzer gives administrators complete visibility into SD-WAN performance, link health, and security events.

SD-WAN overlay design and best practices Practice Question
A1: Answer: B. From branch sites to a central hub before reaching its destination.
Explanation: In a Hub-and-Spoke topology, branch sites send their traffic to a central hub (such as a data center or headquarters) before it is forwarded to other locations. This ensures centralized security enforcement and simplified management, but can introduce latency for branch-to-branch communication.
A2: Answer: B. Full-Mesh
Explanation: In a Full-Mesh SD-WAN topology, branch sites establish direct connections with each other, reducing latency and improving performance for applications like VoIP and video conferencing. In contrast, Hub-and-Spoke requires traffic to flow through a central hub, which may introduce delays.
A3: Answer: B. ADVPN (Auto-Discovery VPN)
Explanation: ADVPN enables branch-to-branch VPN tunnels to be created dynamically on demand, reducing the need for preconfigured static tunnels and improving network efficiency. This is useful in Full-Mesh or Hybrid SD-WAN topologies.
A4: Answer: B. They improve security by encrypting and authenticating traffic between SD-WAN endpoints.
Explanation: IPsec tunnels provide secure, encrypted communication between SD-WAN sites, ensuring confidentiality, integrity, and authentication of transmitted data.
A5: Answer: C. Traffic classification with SLA-based path selection
Explanation: SD-WAN can classify traffic based on application type (e.g., video conferencing, VoIP, file transfers) and dynamically route it through the best available WAN link based on SLA metrics such as latency, jitter, and packet loss.
A6: Answer: B. It optimizes both branch-to-branch and branch-to-hub communication.
Explanation: Hybrid SD-WAN combines Hub-and-Spoke and Full-Mesh designs, allowing branch sites to use direct communication when needed while still utilizing a hub for centralized applications.
A7: Answer: B. To distribute traffic evenly across multiple WAN links with the same cost metric
Explanation: ECMP enables SD-WAN to load balance traffic across multiple WAN links that have equal cost, improving network redundancy and performance.
A8: Answer: B. Implement Zero Trust Network Access (ZTNA) for SD-WAN devices
Explanation: ZTNA ensures that all SD-WAN connections are authenticated and authorized before granting access, enhancing security by minimizing attack surfaces and preventing lateral movement in case of a breach.
A9: Answer: B. By configuring Active-Active or Active-Standby WAN links
Explanation: SD-WAN can be configured with multiple WAN links in either Active-Active (both links used simultaneously) or Active-Standby (secondary link activates only upon failure) to provide redundancy and high availability.
A10: Answer: A. Forward Error Correction (FEC)

Explanation: FEC is an SD-WAN optimization technique that adds redundant data to transmissions, allowing the receiving end to recover lost packets, which is especially useful for high-latency, high-packet-loss networks like LTE and satellite connections.

SD-WAN troubleshooting Practice Question

A1: Answer: B. The SD-WAN rule priority order.

Explanation: SD-WAN rules are processed in order of priority. If a lower-priority rule is incorrectly applied, it may override a higher-priority rule, leading to unexpected routing behavior.

A2: Answer: A. The primary WAN link is not exceeding SLA thresholds.

Explanation: If SD-WAN failover is not occurring, it is likely because the primary link has not exceeded the predefined SLA violation thresholds. FortiGate will not switch to a backup link unless performance degrades beyond the configured limits.

A3: Answer: B. FortiAnalyzer logs for historical SLA violations.

Explanation: FortiAnalyzer can provide insights into repeated SLA violations (latency, jitter, packet loss), helping diagnose whether the issue is caused by poor link quality.

A4: Answer: B. High jitter and packet loss on the WAN link.

Explanation: Jitter and packet loss can severely impact real-time applications such as VoIP and video conferencing. Checking SD-WAN SLA monitoring can help identify and mitigate poor link performance.

A5: Answer: B. `diagnose sys sdwan service`

Explanation: This command displays SD-WAN rule matching details, allowing administrators to confirm whether traffic is following the expected policy-based path.

A6: Answer: C. Use `diagnose sys sdwan health-check` to monitor link SLA metrics.

Explanation: Checking SLA metrics such as latency, jitter, and packet loss can help diagnose whether the issue is related to poor WAN link performance affecting cloud applications.

A7: Answer: D. Misconfigured dynamic routing protocols such as OSPF or BGP.

Explanation: ADVPN relies on dynamic routing to establish on-demand VPN tunnels. If OSPF or BGP settings are incorrect, tunnels will not form properly.

A8: Answer: C. SD-WAN rules for local internet breakout configuration.

Explanation: If branch-to-branch communication works but internet traffic fails, it is likely due to misconfigured SD-WAN rules preventing direct internet breakout.

A9: Answer: B. The WAN link has a high congestion level but is not exceeding SLA limits.

Explanation: SLA thresholds may not capture all performance issues. If a WAN link is experiencing congestion but remains below SLA violation thresholds, traffic may still suffer from slow speeds.

A10: Answer: D. FortiAnalyzer

Explanation: FortiAnalyzer provides historical data analysis for SD-WAN performance trends, allowing administrators to identify recurring issues and optimize configurations.