Identity & Certificates

Fortinet NSE 7 - LAN Edge 7.0

KNOWLEDGE CHEATSHEET

IDENTITY TO ENFORCEMENT

Identify LDAP / RADIUS → **Validate** Credentials / PKI → **Map** User group → **Enforce** Access policy

01 Identity, authentication and certificates

LDAP identity and group matching

- **LDAP authentication** proves credentials; a **remote group match** restricts authorization. Match the required AD group distinguished name in the FortiGate user group, then reference that group in SSL VPN rules and firewall policies.
- **Base DN** sets the search scope. **Bind DN** identifies the search account. **Common Name Identifier** selects the login attribute; AD commonly uses **sAMAccountName**. A display name and an LDAP distinguished name serve different purposes.
- **diagnose test authserver ldap** tests the configured directory with supplied credentials. Use the result and authentication debug to distinguish connectivity, bind, search, user-password and group-matching failures.
- **LDAPS** needs a trusted server certificate and matching server identity. Check DNS, time, the certificate chain, bind permissions and whether the search base contains the intended users.

RADIUS requests and authentication methods

- **RADIUS** separates access requests from accounting. **Access-Accept**, **Access-Reject** and **Access-Challenge** describe different authentication outcomes; **Accounting-Start**, updates and **Stop** describe session activity.
- Check the **RADIUS client source IP**, shared secret, routing and server-side client definition. Authentication commonly uses UDP **1812**; accounting uses **1813**. A NAS identifier or NAS IP is distinct from the packet source address.
- **PAP** supplies a password that a proxy can validate through an LDAP bind. **MSCHAPv2** uses challenge-response and needs a compatible backend; success with PAP does not prove MSCHAPv2 will work.
- **FortiAuthenticator AD domain authentication** establishes domain integration for supported Windows authentication methods. An ordinary LDAP lookup configuration alone does not provide every AD authentication protocol.
- **RADIUS attributes** can carry group membership, vendor-specific information and VLAN assignment. Authentication success must be followed by matching the returned identity or group to the intended access policy.

Identity & Certificates

Fortinet NSE 7 - LAN Edge 7.0

KNOWLEDGE CHEATSHEET

IDENTITY TO ENFORCEMENT

Identify (LDAP / RADIUS) → **Validate** (Credentials / PKI) → **Map** (User group) → **Enforce** (Access policy)

RSSO and enforcement

- **RADIUS single sign-on (RSSO)** learns user-to-IP associations from accounting messages. Verify the accounting sender, listening interface, secret, user/IP attributes and the configured attribute used for group matching.
- An **RSSO group mapping** identifies a session; it does not itself limit traffic. Reference the group in the allow policy and check policy order for an earlier rule that admits everyone.
- Use **diagnose firewall auth list** and the firewall user monitor to inspect learned sessions. Correlate the user, IP address, group and accounting lifecycle before investigating policy matching.

EAP and certificate trust

- **802.1X** has a supplicant, an authenticator such as a switch or AP, and an authentication server. The authenticator carries EAP between the endpoint and server; it need not terminate the inner authentication method.
- **EAP-TLS** uses certificates on both client and server. **PEAP** and **EAP-TTLS** establish a TLS tunnel using a server certificate and support inner authentication methods. Clients must validate the server identity.
- A **root CA** is a trust anchor, normally self-signed. **Intermediate CAs** can issue further certificates when their constraints permit it. Validate signatures, validity periods, key usage and the complete chain.
- **OCSP** reports certificate status such as good, revoked or unknown. Responder selection, response verification and behavior when the responder is unreachable depend on configuration; unknown status is not proof of validity.

Certificate-based IPsec

- For **signature authentication**, FortiGate needs its own local certificate and private key, plus the CA chain used to trust the remote peer. The peer also needs a suitable certificate and its private key.
- Use a **PKI peer/user** and certificate identity constraints to restrict accepted peers, then associate the peer or peer group with the IPsec configuration. Trusting a CA alone may admit a wider set of certificates than intended.
- Check **IKE identity**, certificate validity, trust chain and revocation separately from proposals and traffic selectors. **XAuth** is an additional authentication mechanism; certificate authentication does not inherently require it.

FortiSwitch Access

Fortinet NSE 7 - LAN Edge 7.0

KNOWLEDGE CHEATSHEET

WIRED ACCESS LIFECYCLE

Connect FortiLink / VLAN → **Authenticate** 802.1X / MAB → **Classify** NAC policy → **Enforce** Segment / quarantine

02 FortiSwitch access and segmentation

FortiLink and VLAN foundations

- **FortiLink** lets FortiGate discover, authorize, configure and monitor managed FortiSwitch devices. Discovery, authorization, online status and configuration synchronization are separate stages.
- FortiLink **DHCP VCI matching** uses the client vendor-class identifier, not the hostname. A restricted scope can limit leases to matching FortiSwitch or FortiExtender clients; it is not an address reservation.
- Managed-switch onboarding creates **system VLANs** for functions such as quarantine, mirroring, voice/video and NAC. Inspect their actual interface names and purpose before reusing VLAN IDs.
- **Native VLAN** classifies untagged ingress traffic. **Allowed VLANs** determine permitted tagged traffic. Carry the required VLANs consistently across access ports, inter-switch links and FortiLink.

802.1X port security and MAB

- **Port-based 802.1X** authorizes at port scope. **MAC-based 802.1X** authenticates individual attached devices and can apply different access to each device behind the same physical port.
- **MAC authentication bypass (MAB)** provides an authentication path for devices without an 802.1X supplicant. The MAC address is commonly sent as the RADIUS username and password; it is a device identifier that can be spoofed.
- **MAC-based 802.1X** and **MAB** are different mechanisms. The first describes authorization granularity; the second describes an alternative way to authenticate a device.
- Inspect the assigned **security policy** for MAB, guest/unauthenticated VLANs, failure behavior and reauthentication. A silent supplicant, rejected credentials and a quarantined device are different states; none implies a universal port action.

FortiSwitch Access

Fortinet NSE 7 - LAN Edge 7.0

KNOWLEDGE CHEATSHEET

WIRED ACCESS LIFECYCLE

Connect FortiLink / VLAN → **Authenticate** 802.1X / MAB → **Classify** NAC policy → **Enforce** Segment / quarantine

NAC classification and onboarding

- **NAC policies** classify devices using available attributes such as MAC address and detected operating system, then assign access or a target VLAN. Unmatched devices can remain in the **onboarding VLAN**.
- For a missed match, verify the applied port policy, device-detection settings, observed MAC and OS, and the actual rule criteria. Generate representative traffic so classification has evidence to evaluate.
- Validate **management connectivity** and target-VLAN availability as well as classification. A policy can match correctly while VLAN delivery or switch configuration synchronization still fails.

Trunks, isolation and local forwarding

- A FortiSwitch **trunk** is a **link aggregation group**. It can carry tagged VLAN traffic and can use **LACP**. Supported managed-switch topologies can create inter-switch trunks automatically.
- **Access VLAN** isolation can block host-to-host traffic within a VLAN while allowing traffic toward FortiGate. If gateway and inter-VLAN connectivity work but same-VLAN peers fail, inspect isolation settings.
- Use the **MAC table** for Layer 2 forwarding and the **ARP table** for IP-to-MAC resolution. Check port VLAN membership and isolation before treating an intra-VLAN failure as a routing problem.

Quarantine and Security Fabric automation

- **Quarantine by VLAN** sends affected device traffic toward FortiGate on a separate quarantine VLAN. **Quarantine by redirect** retains the received VLAN and redirects affected traffic to FortiGate for enforcement.
- With redirect quarantine, inspect the configured firewall address group, commonly **QuarantinedDevices**, and the matching firewall rules. MAC identification and a quarantine record must lead to an actual enforcement action.
- An **IOC automation stitch** links detection to quarantine. Verify FortiAnalyzer integration, applicable threat-detection entitlement, IOC classification, event delivery and the configured FortiGate action; a web-filter log alone does not prove an IOC event occurred.
- For **wireless quarantine**, ensure the selected SSID mode and traffic path support the intended enforcement. A **tunnel SSID** brings client traffic to FortiGate; bridge-mode traffic exits locally and has a different enforcement path.

Wireless LAN

Fortinet NSE 7 - LAN Edge 7.0

KNOWLEDGE CHEATSHEET

WIRELESS DELIVERY

- **VAP** — SSID and security
- **AP profile** — Radios and assignment
- **Traffic mode** — Tunnel or bridge
- **RF** — Airtime and coverage

03 FortiAP deployment and radio performance

SSID provisioning and CAPWAP

- A **VAP** defines the wireless network; a **WTP/AP profile** supplies radio settings and SSID assignments. An online, authorized AP cannot advertise an SSID that has not been assigned to an active radio.
- For a missing SSID, check the **broadcast setting**, AP profile or group assignment, radio band, enabled channels and provisioning status. Explicitly assign bridge SSIDs where the profile requires manual VAP selection.
- **CAPWAP** carries AP control and, for tunnel SSIDs, client data. Discovery and authorization do not prove that both tunnels are healthy. Check permitted CAPWAP access on the interface receiving AP management traffic.
- For remote APs across **IPsec**, verify routing and return paths, interface access, firmware compatibility and tunnel MTU. Investigate fragmentation when control connectivity works but encapsulated traffic fails.

Tunnel, bridge and local resources

- **Tunnel mode** carries wireless client traffic to FortiGate for central policy enforcement. **Bridge mode** exits traffic at the AP onto the local LAN or VLAN, which must be available on the AP uplink.
- **SSID split tunneling** allows selected destinations to use the remote local network while other traffic returns through the controller. Define the intended local subnets and validate routes and local access to services such as printers.
- **Block Intra-SSID Traffic** isolates wireless clients on the same SSID. It addresses peer communication, while split tunneling addresses the traffic exit path; inspect the actual path to the destination.

RF capacity, power and roaming

- **Channel utilization** measures airtime occupancy, not just associated-client count. Sustained busy airtime, retries, interference and low-rate clients can reduce throughput even when the signal is strong.
- For **2.4 GHz**, use a coordinated non-overlapping channel plan, commonly **1, 6 and 11** with 20 MHz channels where permitted. Select channels using survey evidence and local regulatory limits.
- Compare **RSSI**, signal-to-noise ratio, retry rate, utilization and neighboring APs before changing channels or power. A less negative RSSI is stronger, but stronger signal alone does not establish the best association.

Wireless LAN / Guest Access & Operations

Fortinet NSE 7 - LAN Edge 7.0

KNOWLEDGE CHEATSHEET

GUEST LOGIN PATH

Pre-login DNS and portal access → **Portal** Trusted HTTPS → **Identity** Authentication result → **Post-login** Group policy

- **Automatic TX power control** adjusts power within configured bounds to manage coverage and overlap. Excessive power can create interference and asymmetric links; verify coverage from the client as well as the AP.
- **AP handoff/load balancing** and client limits address uneven association load. **Frequency handoff/band steering** favors another supported band; it cannot move a 2.4 GHz-only client onto 5 GHz.
- **Roaming** depends on client behavior, coverage overlap, compatible SSID/security settings and authentication delay. Interpret any predicted AP or band selection against the actual handoff thresholds and radio configuration.

04 Guest access, management and diagnostics

External guest portal flow

- An **external captive portal** needs a preauthentication path to DNS, the portal and required supporting services. Use narrowly scoped destination/service exemptions or **captive-portal-exempt** policies for that path.
- Exempting the entire **guest source subnet** can bypass the intended authentication requirement. After login, enforce access through the correct authenticated user group and firewall policy.
- **FortiAuthenticator guest portals** support services before and after login, self-registration and sponsored workflows. Activation, approval and expiration depend on the configured portal policy.
- **Portal mapping rules** use request context, such as incoming parameters and the RADIUS client configuration, to select the portal. Preserve required redirect and POST parameters throughout the login exchange.

HTTPS portal trust

- Use **HTTPS** consistently for the external portal and FortiGate authentication callback. Configure authentication redirection settings and the portal URLs together; changing administrative HTTP access does not secure the guest login flow.
- Validate both HTTPS endpoints: the **portal hostname** and the **FortiGate callback hostname** must resolve for guests and match their certificates. Clients need the appropriate root and intermediate trust chain.
- Check **subject alternative names**, validity periods, client time and browser trust when the portal reports a certificate error. A secure portal page can still fail when it submits to an untrusted callback endpoint.

Guest Access & Operations

Fortinet NSE 7 - LAN Edge 7.0

KNOWLEDGE CHEATSHEET

GUEST LOGIN PATH

Pre-login DNS and portal access → **Portal** Trusted HTTPS → **Identity** Authentication result → **Post-login** Group policy

FortiManager and switch administration

- **FortiSwitch Manager** supports per-device and central management workflows. Verify the selected mode, managed FortiGate, switch authorization and live connection status rather than inferring one state from another.
- FortiManager changes must be **installed on FortiGate** to reach the managed switches. Check the device database, installation result and FortiGate-to-FortiSwitch synchronization when intended settings are missing.
- **Local-access profiles** control services exposed by managed switches. Match **internal-allowaccess** and **mgmt-allowaccess** to the interface being used; prefer SSH over Telnet for administrative sessions.
- For **zero-touch provisioning**, verify the FortiGate serial/model entry, assigned configuration, enabled provisioning workflow and manager reachability. DHCP options **240/241** can supply FortiManager discovery information; discovery alone does not prove installation completed.

Focused authentication and switch diagnostics

- Use **diagnose test authserver radius** to test a named RADIUS server with an explicit method and test credentials. Compare the method with the real client exchange; a synthetic test is only one part of the end-to-end check.
- **diagnose debug application fnbamd -1** exposes backend authentication and certificate-validation activity. **diagnose debug application authd -1** helps trace authentication control and RSSO processing.
- For managed-switch configuration push problems, use **diagnose debug application flcfgd -1**. Distinguish a failed manager installation from a FortiGate-to-switch synchronization failure.
- Run **diagnose debug reset**, select the relevant application, then **diagnose debug enable** and reproduce one failure. Finish with **diagnose debug disable** and **diagnose debug reset**; correlate debug with logs, sessions and packet captures.