Security Concepts

Implementing and Operating Cisco Security Core Technologies

KNOWLEDGE CHEATSHEET

LAYERED RISK REDUCTION

Weakness Vulnerability → **Technique** Exploit → **Protection** Layer controls → **Evidence** Investigate

01 Security concepts 25%

Threats, vulnerabilities and social engineering

- A **vulnerability** is a weakness; an **exploit** uses it. A threat is a potential cause of harm. Reduce risk through patching, least privilege, segmentation and layered controls.
- **Phishing** impersonates a trusted source to induce disclosure or action. **Spear phishing** targets selected victims; **whaling** targets senior executives. Awareness training, email filtering, DNS protection and MFA address different stages.
- A **Trojan** masquerades as legitimate software; a **worm** self-propagates. **Ransomware** denies access, often by encryption. **Rootkits** hide privileged persistence in user space, the kernel or the boot chain.
- A **man-in-the-middle** attack intercepts or alters communication. Authenticate peers, validate certificates and encrypt transport. MFA reduces reliance on stolen passwords but does not make every phishing or relay attack impossible.

Availability and covert channels

- **DoS** disrupts availability; **DDoS** distributes the attack across many sources, often a botnet. Distinguish bandwidth exhaustion, protocol-state exhaustion and application-layer resource exhaustion.
- **SYN floods** consume half-open connection state. **Slowloris** keeps HTTP connections incomplete. Reflection and amplification abuse third-party services; source validation and upstream mitigation complement local rate limits.
- **Ping of death** exploits malformed oversized IP reassembly. **Teardrop** abuses fragment reassembly. These are implementation attacks, distinct from a simple high-volume ICMP flood.
- **DNS tunneling** hides data or command traffic in queries and responses, including encoded query labels. Look for unusually long names, high entropy, abnormal query volume and rare destinations; constrain clients to approved resolvers.
- **ICMP payloads**, HTTPS uploads and messaging APIs can carry exfiltrated data. Encryption can hide content, so combine destination controls, DNS inspection, DLP and behavior analytics instead of relying on port numbers alone.

Security Concepts

Implementing and Operating Cisco Security Core Technologies

KNOWLEDGE CHEATSHEET

LAYERED RISK REDUCTION

Weakness Vulnerability → **Technique** Exploit → **Protection** Layer controls → **Evidence** Investigate

Application attack distinctions

- **SQL injection** changes database query meaning through untrusted input. Prefer parameterized queries, server-side type validation and least-privileged database accounts; a WAF adds protection while application defects are fixed.
- **Cross-site scripting (XSS)** executes attacker-controlled script in a victim's browser. Apply context-specific output encoding and sanitize permitted HTML. Content Security Policy and secure cookie attributes add defense in depth.
- **Path traversal** escapes an intended filesystem directory. Canonicalize paths, restrict access to an allowed root and avoid directly mapping untrusted names to filesystem paths.
- **Command injection** reaches an operating-system interpreter. Avoid shell concatenation and validate structured arguments. **XXE** abuses unsafe XML external-entity processing; disable unnecessary external entities and DTDs.
- **Buffer overflows** exceed memory bounds, particularly in memory-unsafe code. Bounds checking, safe libraries, patching, ASLR and non-executable memory reduce exposure. TLS alone does not correct application input-handling flaws.

Cryptography and secure transport

- **Symmetric encryption** uses a shared secret for efficient bulk protection. **AES** has a 128-bit block and 128-, 192- or 256-bit keys. DES, 3DES and RC4 are legacy choices to avoid in new designs.
- **Asymmetric cryptography** uses a public/private key pair. RSA supports suitable encryption or signature schemes; **Diffie-Hellman/ECDH** establishes shared key material. Authenticate the exchange to prevent interception.
- **Hashes** summarize content; **HMAC** adds a secret for integrity and origin authentication. Prefer SHA-2 over legacy MD5 or SHA-1 for new security designs. A plain hash does not provide confidentiality.
- **AES-GCM** provides authenticated encryption. **AES-CBC** requires separate integrity protection. **Perfect forward secrecy** uses fresh key agreement so later compromise of a long-term key does not expose earlier session keys.
- **TLS 1.3** removes obsolete negotiation choices and uses authenticated encryption. Verify certificate trust and names. **DTLS** protects datagram transport and can avoid TCP-over-TCP behavior for remote-access VPN traffic.
- Store passwords with a **salted, deliberately expensive password hash**. A unique salt defeats shared precomputed tables; it does not stop all guessing. Keep secrets out of source code and avoid treating reversible obfuscation as secure storage.

Security Concepts / Network Security

Implementing and Operating Cisco Security Core Technologies

KNOWLEDGE CHEATSHEET

PROTECT THE TRAFFIC PATH

- **Firewall** — Access policy
- **IPS** — Deep inspection
- **VPN** — Secure transport
- **Telemetry** — Observe flows

PKI and threat intelligence

- A **certificate authority (CA)** signs certificates that bind an identity to a public key and manages revocation. A **registration authority (RA)** validates enrollment requests; it does not replace the CA's signing role.
- **Enrollment** requests a certificate. A **CSR** carries subject information and a public key, signed with the matching private key. Keep that private key confidential; **SCEP** automates supported enrollment workflows.
- Validate the **trust chain**, validity interval, intended use and peer name. **CRLs** and **OCSP** provide revocation information. Reachability and synchronized time matter; a self-signed certificate needs an explicit trust decision.
- **STIX** represents threat intelligence such as indicators, observables and relationships. **TAXII** transports threat intelligence through defined services. An **IoC** is evidence that can support detection, not proof in isolation.
- **Talos** supplies threat research and reputation intelligence. **PSIRT** handles product vulnerability response. **CVE** identifies publicly disclosed vulnerabilities; severity scoring and real exposure together guide remediation priorities.

02 Network security 20%

Firewall roles and deployment modes

- A **stateful firewall** tracks connection state. An **NGFW** adds application awareness and integrated inspection; **Secure Firewall Threat Defense (FTD)** combines firewalling with Snort-based IPS, file control and URL filtering.
- **Routed mode** places the firewall in the Layer 3 path. **Transparent mode** bridges Layer 2 segments and can inspect traffic between hosts in the same IP subnet without renumbering them.
- A **bridge group** joins selected interfaces and uses a **BVI** for its IP presence. Forwarding still depends on access policy. **Multiple contexts** separate virtual firewall configurations and administration on one ASA.
- **Stateful failover** replicates supported connection state to preserve sessions. Stateless failover generally requires session reestablishment. Match supported hardware, software and configuration, and provide reliable failover/state links.
- **ASA/ASAv** provides stateful firewalling and VPN services. **FTD/FTDv** adds integrated next-generation inspection. Appliance form factor alone does not determine throughput, feature support or cloud availability.

Network Security

Implementing and Operating Cisco Security Core Technologies

KNOWLEDGE CHEATSHEET

PROTECT THE TRAFFIC PATH

- **Firewall** — Access policy
- **IPS** — Deep inspection
- **VPN** — Secure transport
- **Telemetry** — Observe flows

Policy actions and inspection

- An **FTD access control policy** evaluates ordered rules and then its default action. Match zones, networks, users, applications and URLs as needed; associate intrusion and file policies with traffic requiring inspection.
- **Allow** permits traffic subject to configured inspection. **Trust** bypasses further deep inspection. **Monitor** records a match and lets rule evaluation continue; it is not a final permit decision.
- **Block** denies traffic; **block with reset** also terminates supported sessions. **Interactive block** can present a user bypass warning for supported web traffic. Configure the action required by the policy intent.
- **Security Intelligence** uses reputation and configured IP, domain or URL lists for early filtering. **URL categories** describe content; **reputation** describes assessed risk. Category selection and reputation thresholds are separate conditions.
- A **file policy** can detect files, block selected types or block files convicted as malware. **Block Malware** differs from blocking every file of a type; unknown disposition is not automatically proof of malware.

Intrusion prevention and management

- **Passive IDS** sees copied traffic and alerts without directly blocking the original stream. **Inline IPS** sits in the path and can drop traffic; inline interface pairs and fail-open/fail-closed behavior affect availability.
- **Network analysis policies** control decoding and preprocessing; **intrusion policies** control detection rules. Protocol-aware inspection can examine SIP, Modbus, DNP3 and CIP semantics instead of only port numbers.
- **Network discovery** builds host, operating-system and application context. Vulnerability context helps assess intrusion impact; third-party host information can supplement passive discovery through supported integrations.
- **FMC** centrally manages supported FTD devices, policies and events. **FDM** manages a device locally; **ASDM** manages ASA. Cloud orchestration provides a different deployment and management model from local appliance administration.
- For **FTD registration**, configure the manager address and matching registration key; use a NAT identifier when required. Verify management reachability, DNS and time, then deploy the intended policies and licenses.
- **Platform settings** group common device settings such as NTP, DNS, SNMP and logging. **Threat Intelligence Director** ingests external intelligence and distributes relevant observables to supported managed sensors.

Network Security

Implementing and Operating Cisco Security Core Technologies

KNOWLEDGE CHEATSHEET

PROTECT THE TRAFFIC PATH

- **Firewall** — Access policy
- **IPS** — Deep inspection
- **VPN** — Secure transport
- **Telemetry** — Observe flows

Layer 2 attack controls

- **DHCP snooping** blocks unauthorized server messages on untrusted ports and builds IP/MAC/VLAN/port bindings. Enable it globally and on relevant VLANs; trust only paths toward legitimate DHCP servers or relays.
- **Dynamic ARP Inspection (DAI)** validates ARP on untrusted ports using bindings or configured ARP ACLs. Trusted ports bypass validation. Static-address hosts need a valid alternative binding strategy.
- **IP Source Guard** uses bindings to restrict source addresses. **Port security** limits allowed MAC addresses: static entries are explicit, dynamic entries are learned, and sticky learning places learned addresses into configuration.
- **Storm control** limits selected broadcast, multicast or unknown-unicast traffic against thresholds. Recovery from an err-disabled port requires fixing the cause plus manual recovery or configured automatic recovery.
- Reduce **VLAN hopping** by explicitly configuring access/trunk roles, disabling unwanted DTP negotiation, limiting allowed VLANs and using an unused native VLAN. Shut unused ports and place them in an unused VLAN.
- **Private VLANs** separate hosts within a subnet: isolated ports reach promiscuous ports; community ports also reach their own community. **BPDU Guard** protects edge ports against unexpected BPDUs.

Device hardening and zone policies

- Restrict management to trusted networks and use **SSHv2**, HTTPS and centralized AAA. Generate supported SSH host keys, restrict VTY transport and disable unused services such as clear-text HTTP or unnecessary discovery on exposed links.
- **CDP** and **LLDP** reveal directly connected neighbors; `show cdp neighbors detail` supplies Cisco neighbor detail. Limit discovery where exposure outweighs operational value; these protocols do not enumerate every routed device.
- **login block-for** enters a quiet period after a configured failure count within a time window. Use supported strong secret hashes; **service password-encryption** alone provides weak protection for legacy configuration passwords.
- A **zone-based firewall** assigns an interface to one security zone and applies directional zone-pair policy. **Inspect** creates state for return traffic; **pass** does not. Plan interzone default drops and self-zone policy explicitly.
- **Class maps**, **policy maps** and service-policy attachment form the policy framework. ASA ACLs use subnet masks; IOS ACLs commonly use wildcard masks. Define protocol and destination service precisely, then attach the ACL to the correct interface/direction.

Network Security

Implementing and Operating Cisco Security Core Technologies

KNOWLEDGE CHEATSHEET

PROTECT THE TRAFFIC PATH

- **Firewall** — Access policy
- **IPS** — Deep inspection
- **VPN** — Secure transport
- **Telemetry** — Observe flows

IPsec and IKE fundamentals

- **IKE** authenticates peers and negotiates security associations; **IPsec** protects data traffic. **ESP** supports confidentiality and integrity/authentication; **AH** provides integrity/authentication without encryption and is unsuitable across ordinary NAT.
- **Tunnel mode** protects the original IP packet under a new outer header. **Transport mode** protects the payload while retaining the original IP header. GRE and L2TP provide encapsulation, not their own equivalent encryption.
- **IKEv1 Phase 1** establishes the IKE SA; **Phase 2/Quick Mode** negotiates IPsec SAs. Main and aggressive modes belong to IKEv1; aggressive mode exposes identities and has weaker protection against password attacks.
- **IKEv2** uses IKE_SA_INIT and IKE_AUTH, then supports additional/rekeyed CHILD_SAs. It provides explicit request/response sequencing, supports EAP authentication and integrates NAT traversal. IKE commonly uses UDP 500; NAT-T uses UDP 4500.
- An IKE proposal defines compatible encryption, integrity/PRF and DH choices. Peer authentication, traffic selectors, lifetimes and PFS must also align as applicable. A lower policy number generally represents higher Cisco IKE policy priority.

VPN designs and remote access

- **DMVPN** combines multipoint GRE, NHRP and IPsec for scalable hub/spoke and dynamic spoke connectivity. **NHRP** resolves overlay tunnel addresses to underlay NBMA addresses. DMVPN can use IKEv1 or IKEv2.
- **FlexVPN** is an IKEv2-based framework using virtual tunnel interfaces for site-to-site and remote access. **Static VTI** suits fixed peers; **dynamic VTI** creates interfaces for negotiated sessions.
- **GET VPN** uses group key management and group security associations for private routed WANs. It preserves the original routing header and avoids a per-peer tunnel mesh; it complements rather than replaces IPsec protection.
- **GRE over IPsec** carries multicast and routing protocols while IPsec secures the encapsulated traffic. GRE is IP protocol 47, not TCP port 47. **L2TP** commonly uses UDP 1701 and also needs IPsec for secure transport.
- **Secure Client/AnyConnect** provides individual remote-access VPN sessions with identity-based policy. Deploy through endpoint management or a supported web-deployment process; configure authentication, group policy and optional certificate plus AAA requirements.
- **Split tunneling** sends selected routes through the VPN and other traffic locally. **Dynamic split tunneling** adds domain-based decisions. Pair offloaded traffic with appropriate local or cloud protection and verify DNS behavior.

Network Security / Cloud Security

Implementing and Operating Cisco Security Core Technologies

KNOWLEDGE CHEATSHEET

PROTECT THE TRAFFIC PATH

- **Firewall** — Access policy
- **IPS** — Deep inspection
- **VPN** — Secure transport
- **Telemetry** — Observe flows

VPN troubleshooting and telemetry

- A **pre-shared key** authenticates a peer; it does not select protected traffic. In IKEv1 `crypto isakmp key` configuration, an address/mask scopes peer matching. Broad wildcard matching eases dynamic peers but broadens trust.
- For dynamic peers, distinguish **DNS reachability**, the peer's configured **IKE identity** and key lookup. A configured hostname is not a substitute for matching authentication identities or certificates.
- Check VPNs in layers: peer reachability, IKE version/proposals and authentication, then IPsec proposals/selectors, routing, NAT exemption and access policy. An established IKE SA does not prove that application traffic is protected.
- **show crypto ipsec sa** exposes encapsulation/decapsulation counters. Generate matching traffic and verify both directions. Use IKE SA displays and narrowly scoped debugging to distinguish negotiation failure from data-path failure.
- **ASA NSEL** exports significant flow events such as creation, denial and teardown using NetFlow v9 templates. Configure a collector with **flow-export destination** and select events under a class in an applied policy map.
- **NSEL** is event-oriented rather than a packet capture or continuous per-packet feed. Ensure collector reachability and template delivery; use traffic classification and event selection to control export volume.

03 Securing the cloud 15%

Cloud models and shared responsibility

- **IaaS** supplies infrastructure; the customer manages guest operating systems, applications and data. The provider manages physical facilities and the virtualization layer. Patch customer-managed virtual routers and firewalls as well as servers.
- **PaaS** adds a managed operating system and runtime. Customers still secure their application code, data, identities and configuration. **SaaS** delivers a managed application; customers retain access governance and data-use responsibilities.
- **Public cloud** serves multiple consumers; **private cloud** is exclusive to one organization. **Community cloud** serves a defined community of organizations. **Hybrid cloud** combines distinct environments with integration between them.
- Compare operating responsibility, data residency, isolation, elasticity and connectivity. No deployment label makes a system automatically secure; misconfigured access, insecure APIs and unpatched components remain material risks.

Cloud Security

Implementing and Operating Cisco Security Core Technologies

KNOWLEDGE CHEATSHEET

SHARED RESPONSIBILITY

IaaS	PaaS	SaaS	All models
Guest OS and apps	Apps and data	Access and usage	Identity policy

Cloud data and workload protection

- A **CASB** adds visibility and policy over cloud applications. **Cloudlock** uses cloud APIs for data discovery, DLP and activity analysis; sanctioned-app access does not mean all sharing or OAuth grants are safe.
- **Cloudlock Apps Firewall** discovers and controls connected cloud apps and their permissions. Review third-party OAuth access and revoke risky integrations rather than relying solely on a network perimeter.
- **Cloud DLP** identifies sensitive information and triggers supported actions such as quarantining, restricting sharing or transferring ownership. API connectors need explicit authorization and appropriate scopes in each cloud service.
- **Microsegmentation** defines least-privileged application/workload communication, including workloads on the same subnet or host. Discover dependencies, model policy, validate intended flows and then enforce default-deny boundaries.
- **Secure Workload (Tetration)** combines workload flow/process telemetry, software inventory, vulnerability context and segmentation policy. Baselines help identify abnormal logins, privilege changes and unexpected file or process activity.

Cloud visibility and orchestration

- **Secure Cloud Analytics** uses cloud telemetry such as AWS **VPC Flow Logs** for behavior-based detection. These logs describe network flows, not complete packet payloads; enable collection and authorize the analytics integration.
- A **private network monitoring sensor** supplies on-premises visibility to cloud analytics. Deploy it where it sees relevant traffic and associate it with the correct service account; metadata analysis can avoid exporting full payloads.
- **Secure Workload connectors** integrate inventory and context from external systems. A supported **reverse tunnel** can provide connectivity initiated from a site that blocks inbound connections; NAT alone does not establish that integration.
- **AppDynamics** observes application transactions and performance dependencies. **Workload Optimization Manager** analyzes demand and can recommend or automate resource resizing; performance management and threat detection serve different purposes.
- Virtual security appliances require supported **cloud networking**, routes, interfaces, management reachability and sizing. Cloud management can be remote; physical-appliance transparent-mode or HA behavior must not be assumed for every virtual deployment.

Cloud Security / Content Security

Implementing and Operating Cisco Security Core Technologies

KNOWLEDGE CHEATSHEET

SHARED RESPONSIBILITY

- **IaaS** — Guest OS and apps
- **PaaS** — Apps and data
- **SaaS** — Access and usage
- **All models** — Identity policy

DevSecOps and container security

- **Continuous integration (CI)** merges changes into a shared repository and runs automated builds/tests. **Continuous delivery** keeps validated releases deployable; continuous deployment automatically releases changes that pass the gates.
- **DevSecOps** embeds security throughout development and operations: review code, scan dependencies and images, test configuration and secrets, and enforce release gates. CI/CD tools orchestrate these repeatable activities.
- **Containers** package applications; orchestration such as **Kubernetes** coordinates deployment, scheduling and recovery. Secure images, registries, workload identities, secrets and network policies; containers share underlying host risk.
- **Serverless functions** run on provider-managed infrastructure in response to events. Design for short-lived execution and external state; validate triggers, constrain permissions and protect dependencies even when no guest OS is managed.
- **ACI** uses endpoint groups and contracts for policy. **Intra-EPG isolation** can restrict peers within an endpoint group. Workload microsegmentation and container networking also need enforcement support at the actual traffic path.

04 Content security 15%

DNS-layer protection with Umbrella

- **Umbrella** can block resolution of malicious destinations before an application connects. Register the public egress network identity and direct approved DNS queries to the service; use its diagnostic welcome page to verify the path.
- **Virtual appliances** retain internal client identity for subnet-based policy behind shared public NAT. Directory integration adds user/group context; a public-IP network identity alone does not identify every internal endpoint.
- **Roaming protection** extends DNS-layer policy off the corporate network, including when the VPN is disconnected. It complements endpoint antimalware rather than replacing file scanning or providing a VPN by itself.
- **Security categories** address threats such as malware, phishing and command-and-control. **Content categories** address acceptable use. **Destination lists** apply custom allow/block choices; review policy order when identities match multiple rules.
- **DNSSEC** validates signed DNS data authenticity and integrity; it does not encrypt DNS or stop every malicious domain. Monitor tunneling patterns and control alternate resolution paths as part of DNS security.

Content Security

Implementing and Operating Cisco Security Core Technologies

KNOWLEDGE CHEATSHEET

CONTENT PROTECTION LAYERS

- **DNS** — Destination risk
- **Web** — Requests and files
- **Email** — Messages and links
- **DLP** — Sensitive content

Proxy inspection and cloud logging

- **Intelligent Proxy** selectively examines web requests to risky domains that may host both safe and malicious content. A full secure web gateway provides broader proxy enforcement; DNS-only visibility is different from full URL/content visibility.
- **HTTPS inspection** terminates and re-establishes TLS so supported content can be inspected. Deploy the inspection CA to clients, validate upstream certificates and define decryption exceptions for privacy and application compatibility.
- **Umbrella Investigate** relates domains, IP addresses, autonomous systems and files to support infrastructure investigation. Reputation is a useful risk signal, not an absolute guarantee of safety.
- **Policy logging** controls recorded activity. Export to an authorized **Amazon S3 bucket** for retention and SIEM ingestion; protect bucket access and plan retention and storage charges independently of dashboard visibility.

Secure Web Appliance traffic and identity

- An **explicit proxy** is selected by browser settings or a **PAC** file; the client connects to the proxy. A PAC function decides between proxy and direct access for each URL and host.
- A **transparent proxy** receives traffic redirected by infrastructure, commonly **WCCP** or policy-based routing. Clients initially address the origin server; no explicit browser proxy setting is required.
- **WCCP** coordinates redirection between network devices and caches/proxies using Here-I-Am and I-See-You messages. Verify service groups, redirect interfaces and bypass/failure behavior as well as basic reachability.
- **Identification profiles** determine how users and requests are identified. Access policies apply URL, application and other controls; unmatched requests fall through to the applicable global policy. Test authenticated, guest and failed-authentication paths.
- **NTLM**, **Kerberos** and supported LDAP realms supply authentication or directory context. **Context Directory Agent** maps AD logon events to IP/user identities; cached mappings and group information can delay policy changes.

Web inspection and operations

- **Web usage controls** apply URL-category policy. **Application Visibility and Control (AVC)** recognizes applications and can restrict supported application activities; port-based rules alone cannot reliably distinguish all applications.
- Enable the **HTTPS proxy** and configure decryption policy, trusted signing material and invalid-certificate handling. Certificate errors require an explicit policy decision; bypassing warnings on clients undermines the trust model.
- **File reputation** uses hashes to identify known content. **File analysis/sandboxing** examines suspicious files in isolation. Results can be shared across supported appliance groups; an unknown verdict is not the same as a clean verdict.

Content Security

Implementing and Operating Cisco Security Core Technologies

KNOWLEDGE CHEATSHEET

CONTENT PROTECTION LAYERS

- **DNS** — Destination risk
- **Web** — Requests and files
- **Email** — Messages and links
- **DLP** — Sensitive content

- Monitor **access logs**, capacity and export health. Size log retention and rotate/export before storage exhaustion; retain enough URI and identity context for investigation while limiting sensitive data collection.
- On-premises web security provides local control; cloud-delivered web inspection can reduce remote-worker backhaul. Standard, hybrid and connector deployments place scanning and enforcement in different locations; check required local features before choosing.

Email flow, reputation and anti-phishing

- **Secure Email Gateway** acts as an **SMTP mail transfer agent**. **MX records** direct inbound mail toward the gateway. Separate inbound acceptance from outbound relay and prevent unauthenticated open relay.
- **Listeners** receive SMTP connections. The **Host Access Table (HAT)** maps sender groups to mail-flow behavior; the **Recipient Access Table (RAT)** controls accepted recipients. LDAP recipient validation reduces invalid delivery attempts.
- **Directory Harvest Attack Prevention** limits attempts to enumerate valid recipients. Sender reputation can reject or throttle bad sources before full message processing; this differs from accepting a message and later quarantining it.
- Layer **anti-spam**, antivirus, outbreak filters, URL reputation and attachment analysis. **Graymail** is bulk mail such as marketing or social notifications; manage it separately from malware and credential theft.
- **SPF** authorizes sending hosts, **DKIM** signs selected message content, and **DMARC** uses alignment with the visible From domain plus policy/reporting. Behavioral phishing detection adds impersonation and relationship signals.

Email DLP, investigation and deployment

- **DLP** inspects outbound content for sensitive data and applies message actions such as quarantine, encryption, notification or a disclaimer. **Matched content logging** preserves evidence of a match and needs tightly controlled access.
- **TLS** protects an SMTP hop; message encryption protects content through its supported delivery workflow. Encryption and DLP solve different problems, and neither substitutes for validating the intended recipient.
- Investigate blocked mail with **message tracking**, filter verdicts, mail logs and quarantine. Choose the narrowest matching policy and preserve suspect messages for analysis; quarantine does not itself establish that a file is harmless.
- **URL defanging** renders links inactive; rewriting and time-of-click checks provide different controls. Keep antispam, antivirus and outbreak rules current, and define behavior for unknown attachments and unavailable analysis services.

Content Security / Endpoint Security

Implementing and Operating Cisco Security Core Technologies

KNOWLEDGE CHEATSHEET

ENDPOINT DEFENSE CYCLE

Prevent EPP controls → **Observe** Endpoint telemetry → **Investigate** EDR context → **Contain** Isolate and remediate

- Physical/virtual gateways retain customer operational control; a **cloud gateway** reduces appliance hosting work. Hybrid designs split processing according to data and control requirements. Virtual resource allocation still needs capacity planning.
- Use protected log delivery such as **SCP over SSHv2** when required. Configure trusted authentication and host keys, verify export success, and use supported RADIUS MFA and cluster-join workflows for administrative access.

05 Endpoint protection and detection 10%

Prevention, detection and response

- **EPP** emphasizes prevention through antimalware, exploit defenses and policy. **EDR** collects endpoint telemetry for detection, investigation and response after suspicious activity occurs. Modern products overlap and often combine both.
- **Secure Endpoint (AMP for Endpoints)** combines file reputation, behavioral detection, cloud intelligence and response. It protects host activity that perimeter controls may miss, including remote and intermittently connected devices.
- **Sandboxing** combines static examination with controlled execution to identify malicious behavior. **Fuzzy fingerprinting** finds related malware variants; machine-learning classifications add signals rather than replacing all other engines.
- Keep the connector, policies and signatures healthy. Endpoint security, host firewalling, least privilege, patching and tested backups provide complementary protection against phishing, malware and ransomware.

Outbreak control and containment

- **Simple custom detections** use **SHA-256** hashes to identify specified files for supported detection/quarantine behavior. A SHA-256 value is 64 hexadecimal characters; an MD5 value is 32 and cannot be substituted.
- **Application blocking** uses file hashes to prevent execution without requiring the file to be quarantined. **IP Block & Allow** lists govern supported network destinations; file hashes and IP addresses belong in different controls.
- **Advanced custom detections** support more complex detection signatures. Verify the required signature format and endpoint-platform support instead of assuming every list accepts raw files or the same hash type.

Endpoint Security

Implementing and Operating Cisco Security Core Technologies

KNOWLEDGE CHEATSHEET

ENDPOINT DEFENSE CYCLE

Prevent — EPP controls → **Observe** — Endpoint telemetry → **Investigate** — EDR context → **Contain** — Isolate and remediate

- Attach the intended detection list to the effective **endpoint policy** and verify policy receipt before testing. Hash matching identifies exact content; a modified file has a different cryptographic hash.
- **Endpoint isolation** contains spread and command traffic while preserving supported management communication. Investigate, remediate and validate the host before removing isolation; changing a password alone does not remove malware.

Retrospective investigation

- **Retrospective detection** revisits previously observed files when intelligence or disposition changes. A file allowed at one point can later generate a security event; point-in-time scanning alone lacks that history.
- **Device trajectory** shows endpoint activity over time; **file trajectory** traces a file's movement and relationships. **File prevalence** indicates how broadly a file has been observed across managed systems.
- Correlate **IoCs**, process ancestry, file activity, connections and intrusion events to assess compromise. An indicator needs context; validate scope before applying widespread containment or exclusions.
- **Secure Client Network Visibility** supplies endpoint/application flow telemetry to supported analytics integrations. Its purpose differs from the VPN, ISE Posture and Umbrella roaming modules.

Patching and mobile device management

- Maintain a **patch inventory**, prioritize exploitable weaknesses, test updates and track successful installation. A defined patch cycle reduces known vulnerabilities; posture checks can restrict access until requirements are met.
- **MDM** inventories devices and enforces supported settings such as encryption, passcodes and application controls. It can distribute configuration and perform remote wipe on lost or stolen devices according to enrollment and platform capabilities.
- **ISE-MDM integration** uses device registration and compliance signals in network authorization. The MDM manages the device; ISE uses those signals to determine allowed network access.
- Reduce ransomware spread through segmentation, host firewall policy and timely patching, including relevant SMB fixes. Restrict noncompliant endpoints to remediation access instead of treating successful authentication as proof of health.

Access & Visibility

Implementing and Operating Cisco Security Core Technologies

KNOWLEDGE CHEATSHEET

ACCESS AND REASSESSMENT

Identity Authenticate → **Health** Assess posture → **Policy** Authorize → **Change** CoA and recheck

06 Secure network access, visibility and enforcement 15%

AAA and access protocols

- **Authentication** establishes identity; **authorization** determines permitted actions; **accounting** records activity. Centralize policy while preserving a controlled local recovery method for server outages.
- **RADIUS** commonly handles network access using UDP 1812/1813. **TACACS+** uses TCP 49, separates AAA functions and supports detailed device command authorization. Match shared secrets and the device source IP registered on the server.
- **AAA method lists** define ordered methods. A server timeout/error can trigger a later method; an explicit authentication rejection normally does not. Enable **aaa new-model** and attach the intended list to the applicable service or lines.
- For **ISE and AD**, verify DNS resolution, clock synchronization, domain-controller reachability and permissions to join. ISE node registration also depends on correct FQDN records and certificate trust, not simply sharing a subnet.

802.1X, MAB and guest access

- **802.1X** uses a supplicant, an authenticator such as a switch/WLC, and an authentication server such as ISE. **EAPOL** runs between endpoint and authenticator; the authenticator relays EAP through RADIUS.
- **EAP-TLS** uses client/server certificates. Validate trust and server names and provision the endpoint identity. Supplicant deployment and certificate enrollment are separate from posture assessment.
- On supported switches, enable **dot1x system-auth-control**, configure AAA/RADIUS, enable port control and the authenticator role. Use **show authentication sessions** or supported access-session displays and **ISE RADIUS Live Logs** to trace failures.
- **MAC Authentication Bypass (MAB)** uses the endpoint MAC identity for devices without supplicants. Because MAC addresses can be spoofed, combine MAB with profiling and restricted authorization instead of granting broad trust.
- **Central Web Authentication** uses a redirect ACL and portal reference returned by ISE; the network device enforces redirection. **Local WebAuth** handles the web exchange locally. Guest authorization must allow DNS, portal and required onboarding traffic.

Access & Visibility

Implementing and Operating Cisco Security Core Technologies

KNOWLEDGE CHEATSHEET

ACCESS AND REASSESSMENT

Identity Authenticate → **Health** Assess posture → **Policy** Authorize → **Change** CoA and recheck

Profiling, posture and BYOD

- **Profiling** classifies what an endpoint appears to be from attributes such as OUI, DHCP, RADIUS, SNMP, HTTP, CDP or LLDP. **Probes** collect those attributes; device-sensor exports can enrich RADIUS accounting with observed device information.
- **Posture** evaluates endpoint health such as OS/patch level, antivirus, firewall, services and registry values. It requires appropriate collection support and policy. Profiling alone does not prove that a required patch is installed.
- A posture flow discovers the service, assesses requirements, provides remediation when configured, and reassesses. Use compliant, noncompliant and unknown results in authorization; keep remediation destinations reachable before full access is granted.
- **BYOD onboarding** registers personally owned devices and can provision supplicant settings and certificates. Single-SSID and dual-SSID designs differ in how onboarding and secure access WLANs are arranged; **My Devices** supports user device registration/management.
- **ISE personas** separate administration (PAN), policy services (PSN), and monitoring/troubleshooting (MnT). Plan availability and scale for each role; adding a node is not the same operation as changing an endpoint authorization policy.

CoA, TrustSec and adaptive authentication

- **RADIUS Change of Authorization (CoA)** updates an existing session's authorization or requests reauthentication/disconnection. **CoA-ACK** signals success; **CoA-NAK** signals failure. Identify the correct session and trust the authorized policy server.
- **CoA reauthentication** reevaluates policy without deliberately bouncing the physical link. **Port bounce** cycles the access port and can affect attached devices; termination ends a session. Select the least disruptive supported action.
- Enable dynamic authorization on the network device and align server addresses, shared secrets and ports. Cisco deployments commonly use **UDP 1700**; standards-based dynamic authorization can use **UDP 3799**. Match both ends and firewall rules.
- **TrustSec** assigns **Security Group Tags (SGTs)** and enforces group policy with SGACLs. **Easy Connect/PassiveID** can map AD-authenticated users to security groups without requiring endpoint 802.1X for that identity source.
- **pxGrid** shares contextual information among ISE and integrated security products. It supports coordinated visibility and response; it is distinct from RADIUS authentication and from a threat-intelligence file format.
- **MFA** combines independent knowledge, possession or inherence factors. **Adaptive MFA** considers context such as device, location and risk. Duo can integrate through supported proxies or application connectors; prefer phishing-resistant methods where available.

Access & Visibility

Implementing and Operating Cisco Security Core Technologies

KNOWLEDGE CHEATSHEET

ACCESS AND REASSESSMENT

Identity Authenticate → **Health** Assess posture → **Policy** Authorize → **Change** CoA and recheck

Network visibility and trustworthy time

- **NetFlow/IPFIX** describes traffic flows using addresses, ports, protocol and additional fields. Flexible NetFlow uses a **record** for key/nonkey fields, an **exporter** for delivery, and an attached **monitor** with a flow cache.
- **NetFlow v9 templates** define the layout of data records. Match collector protocol/port, source addressing, route and template refresh; a collector cannot decode arbitrary records correctly without the corresponding template.
- **Secure Network Analytics (Stealthwatch)** analyzes flow behavior. **Encrypted Traffic Analytics** uses supported metadata to identify threats without decrypting payloads; it does not expose the clear-text contents of encrypted sessions.
- **NBAR2/AVC** recognizes applications; performance monitors collect measures such as TCP performance or RTP loss/jitter. Exporting metrics enables analysis; it does not itself drop an attack or apply QoS policy.
- **SPAN** copies local switch traffic; **RSPAN** carries mirrored traffic over a dedicated VLAN; **ERSPAN** transports mirrored traffic over GRE. Place capture points to observe both directions and protect access to copied data.
- **NTP** aligns event timestamps and certificate checks. Configure a reachable server, authentication key, trusted key and authenticated association as supported; stratum **16** means unsynchronized. Prefer a source explicitly without turning a client into a peer.

Monitoring protocols, SDN and APIs

- **SNMPv3** levels: **noAuthNoPriv** has neither authentication nor encryption; **authNoPriv** authenticates; **authPriv** adds encryption. Groups and views scope users' MIB access. Choose supported strong algorithms.
- **Polling** requests information; **traps** are unsolicited notifications; **informs** receive acknowledgments. Configure the destination and security user consistently. **Model-driven telemetry** streams subscribed structured data for timely, scalable monitoring.
- **Northbound APIs** connect an SDN controller to applications and management systems. **Southbound APIs** connect it to network elements; examples include OpenFlow, NETCONF and device-specific interfaces. Interface direction describes roles, not one mandatory protocol.
- **REST** uses resources and HTTP methods: GET reads, POST creates or invokes, PUT replaces and DELETE removes. Authenticate, validate TLS, inspect status codes and parse response data. Tokens and API keys need scoped access and secure storage.
- **DNA Center** provides design, provisioning, automation and assurance. Intent APIs express network operations; integration APIs connect workflows such as ITSM. Device inventory, plug-and-play onboarding and configuration templates are different resources and workflows.
- **NETCONF** exchanges structured XML RPCs, commonly over SSH; use supported filters to retrieve configuration. **RESTCONF** exposes modeled resources through HTTP. API automation still needs authorization, input validation, error handling and deployment verification.