About the Exam

The CompTIA CloudNetX certification exam will certify the successful candidate has the knowledge and skills required to:

- Analyze business requirements to design and configure secure network architecture for on-premises and cloud environments.
- Analyze requirements to design for network security, availability, Zero Trust, and identity and access management technologies.
- Apply and configure concepts and tools related to network monitoring and performance, automation, and scripting.
- Troubleshoot network issues related to connectivity, performance, access, and security.
- Perform network operation and maintenance.

EXAM DEVELOPMENT
CompTIA exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an IT professional.

CompTIA AUTHORIZED MATERIALS USE POLICY
CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse, or condone utilizing any content provided by unauthorized third-party training sites (aka “brain dumps”). Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA’s exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the CompTIA Certification Exam Policies. Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to abide by the CompTIA Candidate Agreement. If a candidate has a question as to whether study materials are considered unauthorized (aka “brain dumps”), they should contact CompTIA at examsecurity@comptia.org to confirm.

PLEASE NOTE
The lists of examples provided in bulleted format are not exhaustive lists. Other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam, although not listed or covered in this objectives document. CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current, and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid.
TEST DETAILS

Required exam: CNX-001
Number of questions: Maximum of 90
Types of questions: Multiple-choice and performance-based
Length of test:
Recommended experience: A minimum of ten years of experience in the IT field and five years of experience in a network architect role, with experience in the hybrid cloud environment. Network+, Security+, and Cloud+ or equivalent experience.
Passing Score: Pass/fail only; no scaled score

EXAM OBJECTIVES (DOMAINS)

The table below lists the domains measured by this examination and the extent to which they are represented.

<table>
<thead>
<tr>
<th>DOMAIN</th>
<th>PERCENTAGE OF EXAMINATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Network Architecture Design</td>
<td>31%</td>
</tr>
<tr>
<td>2.0 Network Security</td>
<td>28%</td>
</tr>
<tr>
<td>3.0 Network Operations, Monitoring, and Performance</td>
<td>16%</td>
</tr>
<tr>
<td>4.0 Network Troubleshooting</td>
<td>25%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>
1.0 Network Architecture Design

1.1 Given a scenario, analyze business requirements to apply core networking concepts to a network design.

- Open Systems Interconnection (OSI) model
- Internet Protocol (IP) addressing
  - IPv4
  - IPv6
  - IP subnetworking
  - Classless Inter-domain Routing (CIDR) notation
  - Variable Length Subnet Mask (VLSM)
  - Public vs. private
  - Static vs. dynamic
- Network address translation (NAT)
  - Port forwarding
  - Port address translation (PAT)
  - NAT64
- Networking protocols
  - Transmission Control Protocol (TCP)/User Datagram Protocol (UDP)
  - Authentication protocols
    - Power and cooling
    - 802.1X
    - Remote Authentication Dial-in User Service (RADIUS)
    - Terminal Access Controller Access Control System Plus (TACACS+)
    - Lightweight Directory Access Protocol (LDAP)
- Routing protocols
  - Dynamic
    - Open Shortest Path First (OSPF)
    - Border Gateway Protocol (BGP)
  - Static
    - Routing tables
- Network virtual interfaces
  - Dynamic Host Configuration Protocol (DHCP)

1.2 Given a scenario, analyze business requirements to select and implement the appropriate network architectures and topologies.

- Topology types
  - Mesh
  - Star
  - Hub-and-spoke
  - Spine-and-leaf
  - Point-to-point
- Zones
  - Trusted
  - Untrusted
  - Screened subnet
- Traffic flows
  - North/south
  - East/west
- Segmentation
  - Virtual local area network (VLAN)
  - Virtual extensible LAN (VXLAN)
  - Generic Network Virtualization Encapsulation (GENEVE)
- Environments
  - Production
  - Non-production
1.3 Given a scenario, analyze requirements to select appropriate connectivity solutions in a hybrid environment.

- Multi-protocol Label Switching (MPLS)
- Software-defined wide area network (SD-WAN)
- Cellular
- Satellite
- Dark fiber
- Direct internet access
- Metro network
- Public cloud connectivity
  - ExpressRoute
  - Direct Connect
  - Software-defined cloud interconnect (SDCI)
- Remote access
  - Bastion host
  - Secure Shell (SSH)
  - Remote Desktop Protocol (RDP)
- Application gateways
- Private Platform as a Service (PaaS) connectivity
  - Service endpoints
  - Transit gateways
  - Virtual private cloud (VPC) peering
  - Private link
- Virtual private network (VPN)
  - Site-to-site
  - Point-to-site
  - Remote access
  - Split tunneling
  - WireGuard

1.4 Given a scenario, analyze availability requirements to recommend technologies that meet business needs.

- Load balancing
  - Global
  - Local
  - Virtual IP (VIP)
  - Methods
    - Round robin
    - Load-based
    - Least connections
    - Weighted
- High availability
  - Active-active
  - Active-passive
- Link aggregation
- Autoscaling
- Regions and availability zones
- Content delivery network (CDN)
- Fault domains
- Update domains
- Redundancy
  - Devices
  - Paths

1.5 Given a scenario, evaluate business requirements to make recommendations for physical campus installations.

- Power considerations
  - Voltage
  - Wattage
  - Amperage
  - Power distribution unit (PDU)
  - Uninterruptible power supply (UPS)
  - Utility power
  - Emergency power off (EPO)
  - Backup power generators
- Power disruption
  - Blackout
  - Brownout
  - Surge
  - Spike
- Environmental factors
  - Temperature
  - Humidity
  - British thermal units (BTUs)
- Fire suppression
- Physical access controls
  - Video surveillance
  - Biometrics
  - Proximity readers
  - Locks and keys
  - Near-field communication (NFC)
  - Door sensors
1.6 Given a scenario, analyze business requirements to select the appropriate campus wired network components.

- Layer 2 vs. Layer 3
  - Switch
  - Router
- Power over Ethernet (PoE)
- Three-tier hierarchy
  - Core
  - Distribution
  - Access
- Collapsed core
- Intermediate distribution frame (IDF)
- Main distribution frame (MDF)
- Cable management
- Spanning Tree Protocol (STP)
- Tagging/trunking
- Bonding
- Voice and video
- Session Initiation Protocol (SIP)
- WebRTC
- Real-time Streaming Protocol (RTSP)
- H.323
- Customer premises equipment (CPE)
- Power management

1.7 Given a scenario, analyze business requirements to select the appropriate campus wireless network components.

- Wi-Fi
  - Wireless access points
    - Antenna types
      » Omni-directional
      » Directional
    - Placement
    - Enclosure
    - Power considerations
  - Controllers
  - Standards and protocols
    - 802.11
    - Frequencies
      » 2.4GHz
      » 5GHz
      » 6GHz
    - Channels
  - Authentication
  - Data encryption
  - Authentication
- Bluetooth Low Energy (BLE)
- NFC
- Long-range wide area network (LoRaWAN)

1.8 Given a scenario, analyze requirements to select the appropriate artifacts for architecture documentation.

- Requirements analysis
  - Business
  - Technical
  - Regulatory compliance
  - Statement of work (SOW)
- Network diagramming
  - Physical vs. logical
  - High-level vs. low-level designs
  - Flow diagrams
- Verification and validation
- Runbooks
- Work breakdown structure (WBS)
- Knowledge base articles
- Baselines
- Reference architectures
  - External
  - Internal
- Configuration management database (CMDB)
2.0 Network Security

2.1 Explain common cloud and network threats, vulnerabilities, and mitigations.

- **Threats**
  - Distributed denial-of-service (DDoS) attack
  - Data exfiltration
  - On-path attack
  - Credential reuse
  - Brute-force attack
  - Out-of-band (OOB) attack
  - IP spoofing
  - Buffer overflow
  - Privilege escalation
  - Insider threat
  - Evil twin
  - Rogue access point
  - Initialization vector attack
  - BGP hijacking
  - Social engineering attack

- **Vulnerabilities**
  - Zero-day
  - Open Worldwide Application Security Project (OWASP) top 10
  - Overly permissive rules
  - IP reuse
  - Legacy access control lists (ACLs)
  - Insecure protocols
  - Unpatched devices
  - Misconfigurations

- **Mitigations**
  - Input sanitization
  - Data loss prevention (DLP) controls
  - IP address management (IPAM)
  - MITRE ATT&CK Framework
  - Cyber Kill Chain
  - Cloud Controls Matrix (CCM)
  - Patch management
  - Vulnerability management
  - Center for Internet Security (CIS) benchmarks
  - Configuration reviews
  - Null routing

2.2 Given a scenario, analyze requirements to select the appropriate technology to secure a network.

- **Firewalls**
  - Next-generation firewall (NGFW)
  - Cloud-native firewall
  - Web application firewall (WAF)
  - Intrusion prevention system (IPS)/intrusion detection system (IDS)
  - Encryption
  - Protocol types
  - Secure sockets layer (SSL)/TLS inspection
  - Cipher suites
  - Algorithms
  - Asymmetric
  - Symmetric

- **Application gateway**
- **Secure web gateway**
- **Network access control (NAC)**
  - Posture assessment
  - Dynamic list

2.3 Given a scenario, configure the appropriate access controls to secure a network.

- **Firewall rules**
  - Decryption rules
  - Application aware
  - Source and destination
  - Allow list
  - Block list
  - Network access control lists (NACLs)

- **Network security groups**
  - Inbound rules
  - Outbound rules
  - IPS/IDS signature rules
  - Geolocation rules
  - Content/Uniform Resource Locator (URL) filtering
  - Categories

- **Applications**
  - DLP controls
  - Port security
2.4 Given a scenario, analyze requirements to apply the appropriate Zero Trust architecture (ZTA) principles to secure a network.

- Microsegmentation
- Secure Access Service Edge (SASE)
- Secure Service Edge (SSE)
- Cloud Access Security Broker (CASB)
- Identity as the perimeter
- Device trust
- Principle of least privilege
- Zero Trust network access

2.5 Given a scenario, apply identity and access management to secure a network environment.

- Single sign-on (SSO)
  - Federation
  - Security Assertion Markup Language (SAML)
  - OAuth 2.0
  - OpenID Connect (OIDC)
  - Passwordless
- Multifactor authentication (MFA)
- Conditional access
- Geofencing
- Privileged access management (PAM)
- Risk-based authentication
- Role-based access control
- Attribute-based access control (ABAC)
- Endpoint trust
- User and entity behavior analytics (UEBA)
- Public key infrastructure (PKI)
  - Certificate-based authentication
  - Key management system (KMS)
- Session-based tokens
- Just-in-time (JIT) provisioning
- System for Cross-domain Identity Management (SCIM)
- Cloud Infrastructure Entitlement Management (CIEM)

2.6 Given a scenario, use the appropriate wireless security method or configuration.

- Encryption
  - Advanced Encryption Standard (AES)
  - Wi-Fi Protected Access 2 (WPA2)
  - Wi-Fi Protected Access 3 (WPA3)
- Authentication
  - Temporal Key Integrity Protocol (TKIP)
  - Preshared key (PSK)
  - PSK enterprise
- Guest access
- Captive portal
- Layer 2 client isolation
- Media access control (MAC) address filtering

2.7 Given a scenario, implement the appropriate appliance-hardening technique.

- Patch management
  - Delivery channels
  - Verification
- Default credential management
- Disabling unneeded services
- Local password management
  - Password complexity
  - Password length
  - Password rotation
- Protocol configuration
  - Disabling insecure protocols
- Restricting access to administrative interfaces
- Disabling unused physical ports
- Log management
  - Log rotation
  - Remote logging
3.0 Network Operations, Monitoring, and Performance

3.1 Explain concepts related to operating and maintaining a network environment.

- Risk management
  - Risk acceptance
    - Waivers and exceptions
  - Risk avoidance
  - Risk transference
  - Risk mitigation
  - Risk register
- Business continuity
  - Mean time to recovery (MTTR)
  - Mean time between failures (MTBF)
  - Mean time to detect (MTTD)
  - Mean time to investigate (MTTI)
  - Recovery point objective (RPO)/recovery time objective (RTO)
- Disaster recovery
- Service management
- Auditing
- Failure rate
- Contracts, agreements, and terms
  - Interconnection Security Agreement (ISA)
  - Memorandum of understanding (MOU)
  - Master service agreement (MSA)
  - Service-level indicator (SLI)/key performance indicator (KPI)
  - Service-level objective (SLO)
  - Operational-level agreement (OLA)
  - Non-disclosure agreement (NDA)
  - Licensing agreements
  - End-of-life (EOL)/end-of-support (EOS)
- Network function virtualization (NFV)
  - Firewall as a service
  - Reverse proxy
  - Forward proxy
  - NAT gateways
- OOB management
- Network cost management
  - Operating expenditure (OpEx)
  - Capital expenditure (CapEx)
  - Cost optimization
  - Chargeback model
  - Orphaned resources
- Service delivery
  - Self-service
  - Cross-connect
  - Time to market

3.2 Given a scenario, use tools and techniques related to monitoring and performance.

- Traffic analysis
  - Traffic mirroring
  - Throughput
  - Latency
  - Loss
  - Jitter
  - Network flows
  - Reachability
- Log collection
  - Centralized logging
- Security information and event management (SIEM)
- Syslog
- JavaScript Object Notation (JSON)
- Data lake
- Simple Network Management Protocol (SNMP)
- Quality of service (QoS)
- Alerting
- Telemetry
- Dashboards
  - Status pages
- Metrics
- Continuous monitoring
  - Resource utilization
  - Bandwidth utilization
  - Reactive vs. proactive monitoring
Given a scenario, apply automation and scripting to administer a hybrid cloud environment.

<table>
<thead>
<tr>
<th><strong>3.3</strong></th>
<th><strong>Network Operations, Monitoring, and Performance</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Given a scenario, apply automation and scripting to administer a hybrid cloud environment.</strong></td>
<td></td>
</tr>
</tbody>
</table>

- **Infrastructure as code (IaC)**
  - Resource provisioning
  - Resource configuration
  - Yet Another Markup Language (YAML)
  - JSON
  - Linters
- **Life cycle management**
  - Mutable infrastructure
  - Immutable infrastructure
  - Patch management
- **Version control**
  - Desired state
    - Configuration reviews
    - Baselines/benchmarks
    - Configuration backup and restore
  - Change management
- **Public vs. private repositories**
- **Secrets management**
- **DevOps**
  - Continuous integration and continuous delivery (CI/CD) pipeline management
  - GitOps
- **Generative artificial intelligence (AI)**
- **Application programming interface (API)**
- **Software development kit (SDK)**
- **Command-line interface (CLI)**
4.0 Network Troubleshooting

4.1 Explain the troubleshooting methodology.

- Identify the problem
  - Gather information
  - Question users
  - Identify symptoms
  - Determine if anything has changed
  - Duplicate the problem, if possible
  - Approach multiple problems individually
- Test the theory to determine cause
  - If the theory is confirmed, determine the next steps to resolve the problem
  - If the theory is not confirmed, re-establish a new theory or escalate
- Establish a theory of probable cause
  - Question the obvious
- Consider multiple approaches
  - Top-to-bottom/bottom-to-top OSI model
  - Divide and conquer
- Establish a plan of action to resolve the problem and identify potential effects
- Implement the solution or escalate as necessary
- Verify full system functionality and if applicable implement preventive measures
- Document findings, actions, outcomes, and lessons learned throughout the process

4.2 Given a scenario, use the appropriate tool or command.

- Tools
  - Wireshark
  - Netcat
  - Nmap
  - Iperf
  - radclient
  - OpenSSL
  - Postman
- Commands
  - tcpdump
  - dig
  - mtr
  - arp
  - netstat
  - curl
  - ping
  - nslookup
  - tracert
  - ip
  - ipconfig
  - flushdns
  - ifconfig
  - route
  - ss
  - dhclient
  - top
  - snmpwalk
  - nfdump

4.3 Given a scenario, analyze output from network tools and commands to resolve issues.

- Tools
  - Wireshark
  - Netcat
  - Nmap
  - Iperf
  - radclient
  - OpenSSL
  - Postman
  - Spectrum analyzer
  - Heat map
  - SIEM
- Commands
  - tcpdump
  - dig
  - mtr
  - arp
  - netstat
  - curl
  - ping
  - nslookup
  - tracert
  - ip
  - ipconfig
  - ifconfig
  - route
  - ss
  - dhclient
  - top
  - snmpwalk
  - nfdump

• Performance issues
• Connectivity issues
• Access and security issues
4.4 Given a scenario, troubleshoot connectivity issues.

- Intermittent connectivity
- DNS issues
- Asymmetric routing
- Port exhaustion
- Port misconfiguration
  - VLAN assignment
- Duplicated IP addresses
- Duplicated MAC addresses
- IP address exhaustion
- NAT table exhaustion
- DHCP issues
- Request timeouts
- IPv6 router advertisements
- Physical layer disruptions
- Stale cache
- IPSec issues
- BGP issues
- Routing loops
- Single point of failure

4.5 Given a scenario, troubleshoot network performance issues.

- Latency issues
- Packet loss
- Maximum transmission unit (MTU) issues
  - Misconfigured jumbo frames
  - Fragmentation
- Hairpinning
- Broadcast storm
- Resource exhaustion
- Bandwidth issues
  - Overutilization
  - Bottleneck
  - Throttling
- Network scanning issues

4.6 Given a scenario, troubleshoot Wi-Fi performance issues.

- Signal interference
- Signal loss
- Signal degradation
- Low signal strength
- Band steering issues
- Channel overlap
- Incorrect channel width
- Client disassociation
- Roaming issues
  - Sticky clients
- Transmitter/receiver incompatibility

4.7 Given a scenario, troubleshoot access and security issues.

- Rule and policy issues
  - Incorrect security group
  - Missing rules
  - Misconfigured rules
  - Overly permissive rules
  - URL/web content filtering
  - Geo-restriction
  - ACL issues
- DoS issues
  - DDoS
  - SYN floods
- Authentication and authorization failures
  - Password issues
  - Incorrect group membership
  - Mismatched secrets
- Certificate issues
  - Mismatch
  - Expired certificates
  - Revoked certificates
  - Trust issues
  - Hash incompatibility
  - TLS issues
- Blocked or dropped traffic
CompTIA CloudNetX CNX-001 Acronym List

The following is a list of acronyms that appears on the CompTIA CloudNetX CNX-001 exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as part of a comprehensive exam preparation program.

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Spelled Out</th>
<th>Acronym</th>
<th>Spelled Out</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Authentication, Authorization, and Accounting</td>
<td>EDR</td>
<td>Endpoint Detection and Response</td>
</tr>
<tr>
<td>ABAC</td>
<td>Attribute-based Access Control</td>
<td>EOL</td>
<td>End-of-life</td>
</tr>
<tr>
<td>ACL</td>
<td>Access Control List</td>
<td>EOS</td>
<td>End-of-support</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
<td>GENEVE</td>
<td>Generic Network Virtualization Encapsulation</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
<td>HCL</td>
<td>HashiCorp Configuration Language</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>BIA</td>
<td>Business Impact Analysis</td>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure</td>
</tr>
<tr>
<td>BGP</td>
<td>Border Gateway Protocol</td>
<td>iAC</td>
<td>Infrastructure as Code</td>
</tr>
<tr>
<td>BLE</td>
<td>Bluetooth Low Energy</td>
<td>IAM</td>
<td>Identity and Access Management</td>
</tr>
<tr>
<td>BPDU</td>
<td>Bridge Protocol Data Units</td>
<td>IDF</td>
<td>Intermediate Distribution Frame</td>
</tr>
<tr>
<td>BPF</td>
<td>Berkeley Packet Filter</td>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>BTU</td>
<td>British Thermal Unit</td>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>BYOD</td>
<td>Bring Your Own Device</td>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>CASB</td>
<td>Cloud Access Security Broker</td>
<td>IPAM</td>
<td>IP Address Management</td>
</tr>
<tr>
<td>CCM</td>
<td>Cloud Controls Matrix</td>
<td>IPS</td>
<td>Intrusion Prevention System</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed-circuit TV</td>
<td>ISA</td>
<td>Interconnection Security Agreement</td>
</tr>
<tr>
<td>CDN</td>
<td>Content Delivery Network</td>
<td>ISO</td>
<td>Industry Standards Organization</td>
</tr>
<tr>
<td>CI/CD</td>
<td>Continuous Integration and Continuous Deployment</td>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>CICD</td>
<td>Continuous Integration and Continuous Deployment</td>
<td>JSON</td>
<td>JavaScript Object Notation</td>
</tr>
<tr>
<td>CIDR</td>
<td>Classless Inter-domain Routing</td>
<td>KMS</td>
<td>Key Management System</td>
</tr>
<tr>
<td>CIEM</td>
<td>Cloud Identity Entitlement Management</td>
<td>KPI</td>
<td>Key Performance Indicator</td>
</tr>
<tr>
<td>CIS</td>
<td>Center for Internet Security</td>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>CLI</td>
<td>Command-line Interface</td>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>CMDB</td>
<td>Configuration Management Database</td>
<td>LoRaWAN</td>
<td>Long-range Wide Area Network</td>
</tr>
<tr>
<td>CPE</td>
<td>Customer Premises Equipment</td>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
<td>MDF</td>
<td>Main Distribution Frame</td>
</tr>
<tr>
<td>CSP</td>
<td>Cloud Service Provider</td>
<td>MIB</td>
<td>Management Information Base</td>
</tr>
<tr>
<td>DAC</td>
<td>Discretionary Access Control</td>
<td>MFA</td>
<td>Multifactor Authentication</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed Denial of Service</td>
<td>MOU</td>
<td>Memorandum of Understanding</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
<td>MPLS</td>
<td>Multi-protocol Label Switching</td>
</tr>
<tr>
<td>DLP</td>
<td>Data Loss Prevention</td>
<td>MSA</td>
<td>Master Service Agreement</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
<td>MSP</td>
<td>Managed Service Provider</td>
</tr>
<tr>
<td>DNSSEC</td>
<td>Domain Name System Security Extensions</td>
<td>MTBF</td>
<td>Mean Time Between Failures</td>
</tr>
<tr>
<td>DoH</td>
<td>DNS over HTTPS</td>
<td>MTTD</td>
<td>Mean Time To Detect</td>
</tr>
<tr>
<td>DoT</td>
<td>DNS over TLS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acronym</td>
<td>Spelled Out</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MTTI</td>
<td>Mean Time To Investigate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MTTR</td>
<td>Mean Time To Recovery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum Transmission Unit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MX</td>
<td>Mail Exchange</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAC</td>
<td>Network Access Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NACL</td>
<td>Network Access Control List</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAS</td>
<td>Network Attached Storage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NDA</td>
<td>Non-disclosure Agreement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NFC</td>
<td>Near-field Communication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NFV</td>
<td>Network Function Virtualization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NGFW</td>
<td>Next-generation Firewall</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NOC</td>
<td>Network Operations Center</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NSG</td>
<td>Network Security Group</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OIDC</td>
<td>OpenID Connect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OLA</td>
<td>Operational-level Agreement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OOB</td>
<td>Out-of-band</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OSPF</td>
<td>Open Shortest Path First</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OTP</td>
<td>One-time Password</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OWASP</td>
<td>Open Worldwide Application Security Project</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PaaS</td>
<td>Platform as a Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAM</td>
<td>Privileged Access Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAT</td>
<td>Port Address Translation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCAP</td>
<td>Packet Capture</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PDU</td>
<td>Power Distribution Unit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PII</td>
<td>Personally Identifiable Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PoE</td>
<td>Power over Ethernet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSK</td>
<td>Pre-shared Key</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QR</td>
<td>Quick Response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-in User Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RAID</td>
<td>Redundant Array of Independent Disks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RDP</td>
<td>Remote Desktop Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>REST</td>
<td>Representational State Transfer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RPO</td>
<td>Recovery Point Objective</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RTMP</td>
<td>Real-time Messaging Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RTO</td>
<td>Real Time Objective</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RTSP</td>
<td>Real-time Streaming Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAE</td>
<td>Simultaneous Authentication of Equals</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAML</td>
<td>Security Assertion Markup Language</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SASE</td>
<td>Secure Access Service Edge</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SCIM</td>
<td>System for Cross-interdomain Identity Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SDCI</td>
<td>Software-defined Cloud Interconnect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SDK</td>
<td>Software Development Kit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SD-WAN</td>
<td>Software-defined Wide Area Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SFP</td>
<td>Small Form-factor Pluggable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIEM</td>
<td>Security Information and Event Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SLA</td>
<td>Service-level Agreement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SLI</td>
<td>Service-level Indicator</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SLO</td>
<td>Service-level Objective</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SOW</td>
<td>Statement of Work</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSE</td>
<td>Secure Service Edge</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSID</td>
<td>Service Set Identifier</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSO</td>
<td>Single Sign-on</td>
<td></td>
<td></td>
</tr>
<tr>
<td>STP</td>
<td>Spanning Tree Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TACACS+</td>
<td>Terminal Access Controller Access Control System Plus</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TKIP</td>
<td>Temporal Key Integrity Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UEA</td>
<td>User Entity Behavior Analytics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UPS</td>
<td>Uninterruptible Power Supply</td>
<td></td>
<td></td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VIP</td>
<td>Virtual IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLSM</td>
<td>Variable Length Subnet Mask</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice Over Internet Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPC</td>
<td>Virtual Private Cloud</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VXLAN</td>
<td>Virtual Extensible LAN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAF</td>
<td>Web Application Firewall</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAP</td>
<td>Wireless Access Point</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WBS</td>
<td>Work Breakdown Structure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WPA2</td>
<td>Wi-Fi Protected Access 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WPA3</td>
<td>Wi-Fi Protected Access 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
<td></td>
<td></td>
</tr>
<tr>
<td>XXS</td>
<td>Cross-site Scripting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>YAMAL</td>
<td>Yet Another Markup Language</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ZTA</td>
<td>Zero Trust Architecture</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CloudNetX Proposed Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the CloudNetX exam. This list may also be helpful for training companies who wish to create a lab component to their training offering. The bulleted lists below each topic are a sample list and not exhaustive.

**Hardware**
- NGFWs
- Routers
- Switches
- Wireless access points
- Wireless controllers
- Cables
- Spectrum analyzer
- Cable tester

**Software**
- Device enumeration software
- Protocol analyzer
- Cisco packet tracer
- Load balancer
- CLI
- Wireshark
- Nmap
- Sample packet capture (pcap) files
- Diagramming software
- Access to Linux and Windows operating systems
- Postman
- Terraform
- IPS/IDS
- Git client
- Python/Bash/PowerShell
- Log samples
- Integrated development environment

**Other**
- Whiteboard
- Access to a cloud provider
- OWASP Top Ten
- MITRE ATT&CK Framework
- Cloud Security Alliance Cloud Controls Matrix (CCM)
- CIS benchmarks