Website: https://vceplus.com
VCE to PDF Converter: https://vceplus.com/vce-to-pdf/
Facebook: https://www.facebook.com/VCE.For.All.VN/
Twitter : https://twitter.com/VCE_Plus

700-765

Cisco Security Architecture for System Engineers

Version 1.0

Exam A

QUESTION 1 What are two reasons why perimeter-based network security is no longer sufficient?
(Choose two.)

A. More users
B. More devices
C. More networks
D. More IT professionals
E. More vulnerabilities

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2 Which two Cisco products help manage data access policy consistently?
(Choose two.)

A. Stealthwatch
B. pxGrid
C. Duo
D. AMP for Endpoints
E. Cloudlock

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3

How does SD-WAN protect network traffic from end-to-end?

A. Management
B. Automation
C. Segmentation
D. Analyzation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4

Which two IoT environment layers are protected by Stealthwatch? (Choose two.)

A. Access Points B.
Endpoints
C. Internet/Cloud

D. Control Layer
E. Things

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5 What are two key Cisco IoT use cases?
(Choose two.)

A. Industrial Security
B. Parks and Recreation
C. Connected Health
D. Financial Institutions
E. Mobile Utilities

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6 What are the main features of Umbrella for Cloud-Delivered Security?

A. Protect users against DDOS attacks
B. Handles 130B+ DNS requests daily with 99% uptime
C. Runs suspicious cloud applications in a sandbox environment
D. Blocks malware, C2 callbacks, & phishing over any port/protocol

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7 What are two core functionalities of DNS-layer security?
(Choose two.)

A. Live threat intelligence
B. Proxy and file inspection
C. URL filtering
D. Real-time sandboxing
E. Data analytics and monitoring

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Which two attack vectors are protected by Cyber Threat Defense & Network Analytics? (Choose two.)

A. Web
B. Cloud
C. Data Center
D. Email
E. Endpoints

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9 What are two ways that Cisco helps customers secure IoT deployments?
(Choose two.)

A. limited access points
B. segmentation & visibility
C. cross-architecture automation
D. secure remote access
E. network analysis

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10 Which two security risks are created by legacy approaches to networking?
(Choose two.)

A. network downtime
B. user vulnerability
C. slow containment
D. access points
E. large attack surface

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11 What are three security blind spots that must be addressed?
(Choose three.)

A. Workloads
B. Data
C. Networks
D. IT
E. Applications
F. Email

Correct Answer: BCE
Section: (none)

Explanation

Explanation/Reference:

QUESTION 12 Which two IoT environment layers are protected by ISE?
(Choose two.)

A. Endpoints
B. Access Points
C. Control Layer
D. Things
E. Internet/Cloud

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13 Which Cisco NGIPS capability provides control over users, applications, devices, threats, and provides insights to network vulnerabilities?

A. global threat intelligence
B. security automation
C. advanced threat protection and rapid remediation
D. contextual awareness

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14 What does ThreatGrid integrate?

A. File reputation and behavioral indications of compromise
B. Malware analysis and threat intelligence
C. Threat intelligence and access control
D. File trajectory and time signatures

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15 What are two steps customers can take to evolve to a trust-centric security philosophy?
(Choose two.)

A. Block BYOD devices
B. Always verify and never trust everything inside and outside the perimeter.
C. Limit internal access to networks.
D. Only grant access to authorized users and devices.

E. Require and install agents on mobile devices.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16 Which feature of ISE provides role-based access control and command level authorization with logging
for auditing?

A. Platform exchange grid
B. TACACS+ Device Administration
C. Context-aware access
D. Centralized policy management

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17 What are two result of utilizing a fragmented security model?
(Choose two.)

A. Reduced malicious file risk through additional segmentation.
B. Decreased network accessibility through multiple applications.
C. Decreased visibility and limited understand of security coverage.
D. Increased identity controls
E. Individual components pieced together to meet requirements.

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18 Which feature of AnyConnect provides better access security across wired and wireless connections
with 802.1X?

A. Flexible AAA Options
B. Trusted Network Detection
C. Secure Layer 2 Network Access
D. AnyConnect with AMP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which two products are involved in granting safe access to apps? (Choose two.)
A. ISE

B. ACI
C. TrustSec
D. Duo
E. SD-Access

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20 What are two solutions Cisco offers for email security?
(Choose two.)

A. Tetration
B. Meraki
C. Cloudlock
D. Umbrella
E. AMP for Email Security

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21 Which two Cisco products remediate network, cloud, and endpoint threats?
(Choose two.)

A. AMP for Endpoints
B. Duo
C. Cisco Security Connector
D. pxGrid
E. Stealthwatch

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22 Which two products empower customers to create secure next-gen networks?
(Choose two.)

A. AMP
B. SD-Access
C. MFA
D. ISEE. ACI

Correct Answer: BE
Section: (none)
Explanation
Explanation/Reference:

QUESTION 23 What are two critical networking challenges?
(Choose two.)

A. Threat protection
B. Orchestration
C. Automation
D. Access
E. Visibility

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24 What percent of threats did ASA with FilePOWER block that earned AMP the highest security effectiveness scores in third-party testing?

A. 98.5% B.
95.6%
C. 99.2%
D. 100%

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25 Which two areas require secure access?
(Choose two.)

A. Worktable
B. Workspace
C. Workloads
D. Workforce
E. Workflow

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26 Which two attack vectors are protected by Web Security?
(Choose two.)

A. Web
B. Cloud
C. Voicemail
D. Data Center
E. Email

Correct Answer: AB

Section: (none)
Explanation

Explanation/Reference:

QUESTION 27 What are two key capabilities of Meraki?
(Choose two.)

A. identity-based and device-aware security
B. application visibility and control
C. device profiling
D. contextual awareness
E. security automation

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28 What is a key
feature of Duo?

A. Provides SSL VPN
B. Supports pxGrid
C. Authenticates user identity for remote access
D. Automates policy creation for IT staff

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29 Which feature of AnyConnect provides customers the ability to monitor endpoint application usage to uncover potential behavior anomalies?

A. Differentiated Mobile Access
B. Secure Layer 2 Network Access
C. Trusted Network Detection
D. Network Visibility Module

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which feature of StealthWatch aggregates and normalizes NetFlow data?
A. Netflow analytics
B. Forensic investigation
C. Advanced malware protection

D. FlowCollector

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31 What does remote access use to
verify identity?

A. Agents
B. MFA
C. Remote Access VPN
D. AMP for Endpoints

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32 What are two common seller obstacles?
(Choose two.)

A. Seller competition
B. Overcrowded portfolios
C. Fragmented solutions
D. Unresponsive potential customers
E. Complexity of solution components

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33 What is one of the key features of Cognitive
Intelligence?

A. Allows visibility into anonymous and encrypted communications
B. It enables greater threat intelligence with entity modeling
C. It enables safe email usage with event analytics
D. It enhances anonymity with URL filtering

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 34 Which two attack vectors are protected by Malware Protection?
(Choose two.)

A. Voicemail
B. Web

C. Mobile
D. Email
E. Data Center

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35 What are three key benefits of Cisco NGFW?
(Choose three.)

A. Reduces throughput
B. Increases traffic latency
C. Detects and remediates threats faster
D. Identifies anomalous traffic
E. Prepares defenses
F. Reduces complexity

Correct Answer: CDF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36 What are two features of Advanced Malware Protection (AMP)?
(Choose two.)

A. File Retrospection and Trajectory
B. Dynamic Malware Analysis
C. Local Threat Intelligence
D. Automated Policy Management
E. Automatic Behavioral Authorization

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37 What is a continuous protection feature of Advanced Malware Protection?

A. File Reputation
B. Behavioral Indicators of Compromise
C. Global Threat Intelligence
D. Sandboxing File Analysis
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38 Which feature of ISE has the capability to encounter a device new on the market, and correctly profile it to onboard it quickly and easily?

A. Device profiling
B. Centralized policy management
C. Context-aware access
D. Platform exchange grid

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39 What are two features provided by ISE?
(Choose two.)

A. Device Firewalling
B. Guest Management
C. DDOS attack prevention
D. Centralized policy management
E. Network visibility

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40 What are two solutions Cisco offers for web security?
(Choose two.)

A. Cloudlock
B. AMP for Web Security
C. Cognitive Intelligence
D. CRES
E. NGFW

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
What do customers receive when implementing TrustSec?

A. Context-aware access enhancing the forensic capabilities available to their IT team
B. SSL decryption enabling secure communications on and off company networks
C. Dynamic role-based access control that enables them to enforce business role policies across all network services
D. Dynamic profiling and onboarding, enabling businesses to control company role policies across all network services

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 42 Which two IoT environment layers are protected by AMP for Endpoints?
(Choose two.)

A. Control Layer
B. Internet/Cloud
C. Data Center
D. Things
E. Access Points

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43 What does Cisco provide via Firepower's simplified, consistent
management?

A. Higher value
B. Reduced complexity
C. Improved speed to security
D. Reduced down time

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44 What are three major features of StealthWatch?
(Choose three.)

A. Real-time sandboxing
B. Forensic investigation
C. Threat-based anomaly detection
D. Data Loss Prevention
E. Netflow monitoringF. Malware clustering

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
QUESTION 45 What are two key advantages of Cisco's Security Solutions Portfolio?
(Choose two.)

A. An effective security solution portfolio can help customers overcome ever-growing security challenges
B. Cisco Security provides direct, simple, and balanced detection by driving customer outcomes
C. Cisco Security provides flexible, simple, and integrated advanced threat detection, through a multilayered approach.

D. The Cisco Security Portfolio offers realtime access control and event monitoring to drive business outcomes.
E. The Cisco Security Portfolio provides security across the entire business environment.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46 Which statement best embodies trust-
centric security?

A. Verify before granting access via identity-based policies for users, devices, apps, and locations
B. Prevent attacks via an intelligence-based policy, then detect, investigate, and remediate.
C. Verify before granting access via MDM software.
D. Protect users from attacks by enabling strict security policies.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47 What are two tenants of establishing an SD-perimeter?
(Choose two.)

A. Securing device access
B. Securing network access
C. Securing user-device trust
D. Securing app access
E. Securing endpoints

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48 Which three customer business objectives does Cisco's Advanced Threat solutions address?
(Choose three.)

A. Visibility and control with a managed environment
B. Secure communications with advanced access
C. Lower TCO through intelligent API management
D. Comprehensive support with flexible solutions
E. Complete protection with holistic defense
F. Accelerated firewall implementation
Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
What do Cisco NGFW fully integrated platforms offer that allow other security components to participate to achieve pervasive and consistent enforcement?

A. Telemetry, shared intelligence, and profiling sources
B. Context, telemetry and intelligence sources
C. Intelligence sources, telemetry, and shared intelligence
D. Context, telemetry, and profiling sources

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50 Which two attack vendors are protected by Visibility and Enforcement?
(Choose two.)

A. Web
B. Cloud
C. Endpoints
D. Email
E. Mobile

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51 What are two steps organizations must take to secure IoT?
(Choose two.)

A. block contractors
B. prevent blackouts
C. acquire subscription solutions
D. remediate malfunctions
E. update equipment

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Which feature of Cognitive intelligence can separate statistically normal traffic from anomalous traffic?
A. Anomaly modeling
B. Anomaly detection
C. Event classification
D. Trust modeling

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
In the Campus NGFW use case, which capability is provided by NGFW & NGIPS?

A. Flexible AAA Options
B. Differentiated Mobile Access
C. High throughput maintained while still protecting domains against threats
D. Identity Service Engine

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54 What are three main areas of the Cisco Security Portfolio?
(Choose three.)

A. IoT Security
B. Roaming Security
C. Advanced Threat
D. Cloud Security
E. Voice & Collaboration
F. Firewalls

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
What are two common customer obstacles? (Choose two.)

A. Compliance regulations
B. Security system blackouts
C. High turnover of IT professionals
D. Limited resources
E. Lack of solution integration

Correct Answer: AE
Section: (none)
Explanation
Explanation/Reference:

QUESTION 56 In which two ways has digitization transformed today's security threat landscape?
(Choose two.)

A. Decreasing endpoint ecosystem
B. Increasing access points
C. Expanding complexity
D. Decreasing 3rd party applications

E. Growing ecosystem

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57 In which two ways should companies modernize their security philosophies?
(Choose two.)

A. Rebuild their security portfolios with new solutions
B. Complement threat-centric tactics with trust-centric methods
C. Expand their IT departments
D. Decrease internal access and reporting
E. Reinforce their threat-centric security tactics

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58 Which two elements does Advanced Malware Protection provide?
(Choose two.)

A. dynamic data analysis
B. intrusion analysis
C. dynamic URL filtering
D. reputation analytics
E. advanced analytics

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59 How do AMP's device trajectory capabilities help address customers' breach
remediation issues?

A. It analyzes the data from suspicious files to provide a new level of threat intelligence
B. It searches for potential threats based on identified activities and behaviors.
C. It determines the scope and cause of an outbreak and tracks suspicious files
D. It tracks file behavior across the network to see which devices it enters and exits

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60 Which two attack vectors are protected by MFA?
(Choose two.)

A. Mobile
B. Cloud
C. Data center
D. Web
E. Endpoints

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61 Where do you start to achieve true
network visibility?

A. OT
B. Branches
C. IT
D. Fabric Level

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62 What are two capabilities of Cisco's NGFW Identity Based Policy Control feature?
(Choose two.)

A. access to multiple data layers
B. threats stopped from getting in and spreading
C. see and share malware details
D. access to Trojan downloader

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
What are three benefits that Cisco Umbrella brings to DNS-Layer Security? (Choose three.)
A. Reputation filtering
B. Malware scanning
C. Predictive intelligence
D. Breach mitigation
E. Off-network security
F. Recursive DNS

Correct Answer: CEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64 What is an attribute
of Cisco Talos?

A. Blocks threats in real time
B. Real-time threat information
C. 3rd party applications integrated through comprehensive APIs
D. Detection of threats communicated within 48 hours of occurrence

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65 What does TrustSec assign to the user or device traffic at ingress that enforces the access policy based on the tag in the
infrastructure?

A. VXLAN
B. Ingress VLAN
C. Security Group Tag
D. Access Control List

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66 How does AnyConnect provide highly secure access for select enterprise
mobile apps?

A. Per application VPN
B. Secure Layer 2 Network Access
C. Application Visibility & control
D. Identity Service Engine

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 67 What are the competing IT and Operation Technology (OT) priorities that make securing
IoT difficult?

A. Innovation vs. manufacturing
B. Hackers vs. safety
C. Malfunctions vs. output
D. Security vs. availability

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68 Which two features are part of Cisco Web security?
(Choose two.)

A. user authentication
B. device profiling and onboarding
C. URL filtering & dynamic content analysis
D. intrusion prevention
E. user identity tracking

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69 Which two products are involved in discovering, classifying, and verifying profiles?
(Choose two.)

A. Duo
B. Cisco Security Connector
C. Industrial Network Director
D. Identity Services Engine
E. Advanced Malware Protection

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70 What are two solutions for Cisco Cloud Security?
(Choose two.)

A. cloud data security
B. intrusion prevention
C. advanced network security
D. cloud-delivered security
E. cloud security

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71 How does AMP's file reputation feature
help customers?

A. It enables secure web browsing with cognitive threat analytics B.
It enables point in time detection through a one-to-one engine
C. It increases the accuracy of threat detection with Big Data analytics
D. It increases the protection to systems with exact fingerprinting

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 72 Which two attack vectors are protected by NGFW?
(Choose two.)

A. Mobile
B. Data Center
C. Cloud
D. Web
E. Email

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73 What are three main solutions areas for Advanced Threat?
(Choose three.)

A. NGFW
B. Network Analytics
C. Intrusion Analytics
D. Threat Analytics
E. Malware ProtectionF. Threat Defense

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
What is a key feature of Application Visibility and Control?
A. Retrospective security
B. Control of protocol-hopping apps that evade traditional firewalls
C. Scalable policy inheritance
D. Automated remediation APIs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75 Which two security areas are part of Cisco's campus & branch solutions?
(Choose two.)

A. Network Analytics
B. Behavioral Indication of Compromise

C. Remote Access VPN
D. File Retrospection and Trajectory
E. Mobile Access

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76 On average, how many days elapse before businesses discover that they have
been hacked?

A. 50
B. 30
C. 10
D. 70

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77 What is one of the reasons that customers need a Visibility &
Enforcement solution?

A. Storage is moving from on-premises to cloud-based
B. Network traffic is growing at an exponential rate
C. Organizations need the ability to block high-risk websites
D. Businesses can't see or protect devices on their network

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 78 Which two attack vectors are protected by Cloud Security?
(Choose two.)

A. Web
B. Cloud
C. Endpoints
D. Data Center
E. Email

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79 What is used to reduce
attack surfaces?

A. Device trust
B. Remediation
C. Segmentation
D. Access

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80 What are two areas present a security challenge for customers?
(Choose two.)

A. Email
B. Corporate priorities
C. IoT devices
D. IT departments
E. OT environments

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference: