

**Boost up Your Certification Score**

# **Huawei**

## **H35-664**

### **HCIA-5G-Security Solution**



**For More Information – Visit link below:**

**<https://www.examsboost.com/>**

### **Product Version**

- ✓ Up to Date products, reliable and verified.
- ✓ Questions and Answers in PDF Format.

# Latest Version: 6.0

## Question: 1

An operator's gNBs at cell sites connect to its core data center over leased backhaul that the operator does not control. All core functions, including the SMF and the UPF, sit in that data center. Neighboring gNBs also exchange traffic with each other over the same backhaul.

Which traffic could an attacker with access to that backhaul observe or alter if it is left unprotected? (Choose two.)

- A. N4 session rules sent from the SMF down to the UPF.
- B. The subscriber's long-term key, sent to the gNB during registration.
- C. N2 signaling to the AMF and N3 user data to the UPF.
- D. Over-the-air traffic between UEs and their serving gNB.
- E. Xn signaling exchanged between neighboring gNBs.

**Answer: C,E**

## Question: 2

A defense contractor's policy states that its production traffic must never run on equipment that also carries other organizations' traffic. An operator offers the contractor a slice with dedicated core NFs, reserved radio resources and its own transport VPN.

Does the offer satisfy the policy?

- A. No, since only a network on dedicated equipment meets that policy.
- B. Yes, since dedicated core NFs, reserved radio resources and a transport VPN make the slice physically separate.
- C. Yes, provided the slice's traffic is also encrypted end to end, since encryption removes the need for separate equipment.
- D. No, since a slice can have dedicated core NFs only when it also has dedicated cell sites, which this offer lacks.

**Answer: A**

## Question: 3

A vendor has completed the process assessment part of NESAS and now needs its new gNB release evaluated. Its product manager asks who performs the evaluation and what the product is evaluated against.

Which statement is correct?

- A. An accredited test laboratory evaluates the gNB against the vendor's own security target.
- B. An accredited test laboratory evaluates the gNB against the operator's acceptance criteria.
- C. An accredited test laboratory evaluates the gNB against ISO/IEC 27001 controls.
- D. An accredited test laboratory evaluates the gNB using the applicable 3GPP SCAS as the test basis.

**Answer: D**

### Question: 4

An operator is splitting its gNBs into a CU and DUs. The DUs will sit in street cabinets beside the antennas, and the planners must decide where the CUs go. The security team wants the point where user data leaves radio-interface protection to be in a physically secured site. Which placement decision meets this requirement?

- A. Place the DUs in a secured site, because radio protection terminates in the physical layer that they host.
- B. Place the CUs in a secured site, because PDCP runs there and radio protection terminates in it.
- C. Place the CUs beside the DUs to shorten the midhaul, simplify cabling and reduce latency.
- D. Place the CUs in the cabinets too, because the transport link to the core is where radio protection ends.

**Answer: B**

### Question: 5

At 02:10 an edge site raises a cabinet-door-open alarm, although no maintenance visit is scheduled. At 02:25 the edge UPF at that site restarts without any planned change, comes back up and starts carrying traffic again. What should the security O&M engineer do?

- A. Treat it as possible tampering and verify the node's software integrity before it carries traffic.
- B. Clear both alarms once the UPF has recovered and traffic is flowing normally.
- C. Raise a transport ticket for the N4 link between the UPF and the SMF.
- D. Record both alarms in the shift log and review them at the next scheduled security audit of the site.

**Answer: A**

### Question: 6

A hospital buys a slice for remote patient monitoring on an operator's shared infrastructure. Its risk assessment lists one concern: during a major public event, consumer traffic on the operator's

broadband slice could consume capacity that the monitoring devices need. A reviewer states that slice isolation is a confidentiality control and so does not address this concern. How should the reviewer's statement be evaluated?

- A. It is correct, since isolation exists to stop one slice's traffic being read by another slice's tenant.
- B. It is correct, since capacity during public events is set by the radio scheduler, which slicing cannot influence.
- C. It is wrong, since isolation encrypts each slice's traffic so the broadband slice cannot see monitoring data.
- D. It is wrong, since resource isolation also protects availability.

**Answer: D**

### Question: 7

An operator downloads CNF images from a vendor's repository. Today its deployment pipeline compares each image with a checksum file published in the same repository. A review warns that an attacker who gains write access to the repository could replace an image with a modified one. Which change to the pipeline defends against that attack?

- A. Download the image and its checksum file over an encrypted connection.
- B. Verify the vendor's signature on each image before deployment.
- C. Compare the checksum twice, once at download and again just before deployment.
- D. Scan each running container for known vulnerabilities once it is deployed.

**Answer: B**

### Question: 8

Security monitoring shows that a small number of UEs each day report an authentication synchronization failure, after which authentication succeeds on the next attempt. A new analyst proposes opening a security incident for every such event. What is the correct view of these events?

- A. Each shows that a false base station has captured the UE.
- B. They reveal that the UDM holds a corrupted long-term key.
- C. On its own, this is routine resynchronization.
- D. They prove an attacker has de-concealed the UE's SUCI.

**Answer: C**

### Question: 9

An attacker gains full read access to an AMF in a visited network, including the security contexts it holds for roaming subscribers. The home operator is assessing what the breach exposes. Which of those subscribers' keys can the attacker still not obtain from this breach?

- A. The long-term key held in the USIM and the ARPF.
- B. The anchor key the serving network received once primary authentication completed.
- C. The NAS keys that protect signaling between these subscribers' UEs and the AMF.
- D. The key the AMF passed to the gNB, from which the radio-link keys are derived.

**Answer: A**

### Question: 10

A regional operator buys a core network product that has a NESAS evaluation report. A manager proposes closing the network's security review because "the product is already NESAS-evaluated". Which two responsibilities does the operator still own after the purchase? (Choose two.)

- A. The accredited laboratory's evaluation of the product's own security functions.
- B. The audit of the vendor's development and product lifecycle processes.
- C. Fixing design flaws in the product's software, which the operator patches into the source code itself.
- D. Operation, patching and monitoring of the product.
- E. Secure configuration of the product and its integration into the network.

**Answer: D,E**

# Thank You for Trying Our Product

For More Information – **Visit link below:**

**<https://www.examsboost.com/>**

15 USD Discount Coupon Code:

**G74JA8UF**

## FEATURES

- ✓ **90 Days Free Updates**
- ✓ **Money Back Pass Guarantee**
- ✓ **Instant Download or Email Attachment**
- ✓ **24/7 Live Chat Support**
- ✓ **PDF file could be used at any Platform**
- ✓ **50,000 Happy Customer**



Visit us at: <https://www.examsboost.com/test/h35-664>