NSE2

2022/08/02 - 04:33:10 PM - Tuesday

Certification Name: NSE 2 The Evolution of Cybersecurity
URL: https://training.fortinet.com/local/staticpage/view.php?page=nse_2

NSE2_Course_Description.pdf

NSE2_Lesson_Scripts_22.01.pdf

> Description

In NSE 1, you learned about the threat landscape and the security problems facing organizations and individuals.
In NSE 2 The Evolution of Cybersecurity course, you will learn about the types of security products that security vendors created to address those problems.

> Who Should Attend

This course is open to anyone who wants to learn about about cybersecurity and security products.
All Fortinet employees and partners are required to obtain NSE 1, NSE 2, and NSE 3 certifications.

> Program Requirements

You must successfully complete all lessons and quizzes within the The Evolution of Cybersecurity course.

> How to Enroll in NSE 2 Training

The NSE 2 course is available on the Fortinet Training Institute.

- If you are a customer or a public user, you must first

create an account on the Fortinet Training Institute. You must use your company email address to register.
◇ If you are a partner, you must first create an account on the Partner Portal. You must use your company email address to register.
◇
https://training.fortinet.com/

After you log in in the Fortinet Training Institute, click the following link to enroll in this course: NSE 2 The Evolution of Cybersecurity.

If you have questions, contact your regional training team:

the Americas - training@fortinet.com
Asia, Pacific, India - apactraining@fortinet.com
Europe, Middle East, Africa - emeatraining@fortinet.com

The Evolution of Cybersecurity

In NSE 1 you learned about the threat landscape and the problems facing organizations and individuals. In this course, *The Evolution of Cybersecurity*, you will learn about the types of security products that have been created by security vendors to address those problems.
The completion of all lessons and associated quizzes in this course completes the requirement to obtain the NSE 2 level certification.
Course duration (estimated): 2 hours

ZTNA

2022/08/02 - 04:42:11 PM - Tuesday

ZTNA - Zero Trust Network Access

In this lesson, we will explore secure remote access and why it's important.

Secure Remote Access ⇒ It is a combination of security methods and technologies that allow outside end entities to connect to networks, without compromising digital assets or exposing networks to unauthorized parties.

Remote Access is secured using the following features ⇒

Data Privacy: A state in which information is concealed from the public and privy only to select people.
Data Integrity: The accuracy and consistency of data over its life cycle.

AAA ⇒ Authentication, Authorization, Accounting

Authentication: The process of verifying the identity of a person or thing.
Authorization: The function of specifying access rights to resources.
Accounting: The record keeping and tracking of agent activities on a computer network.

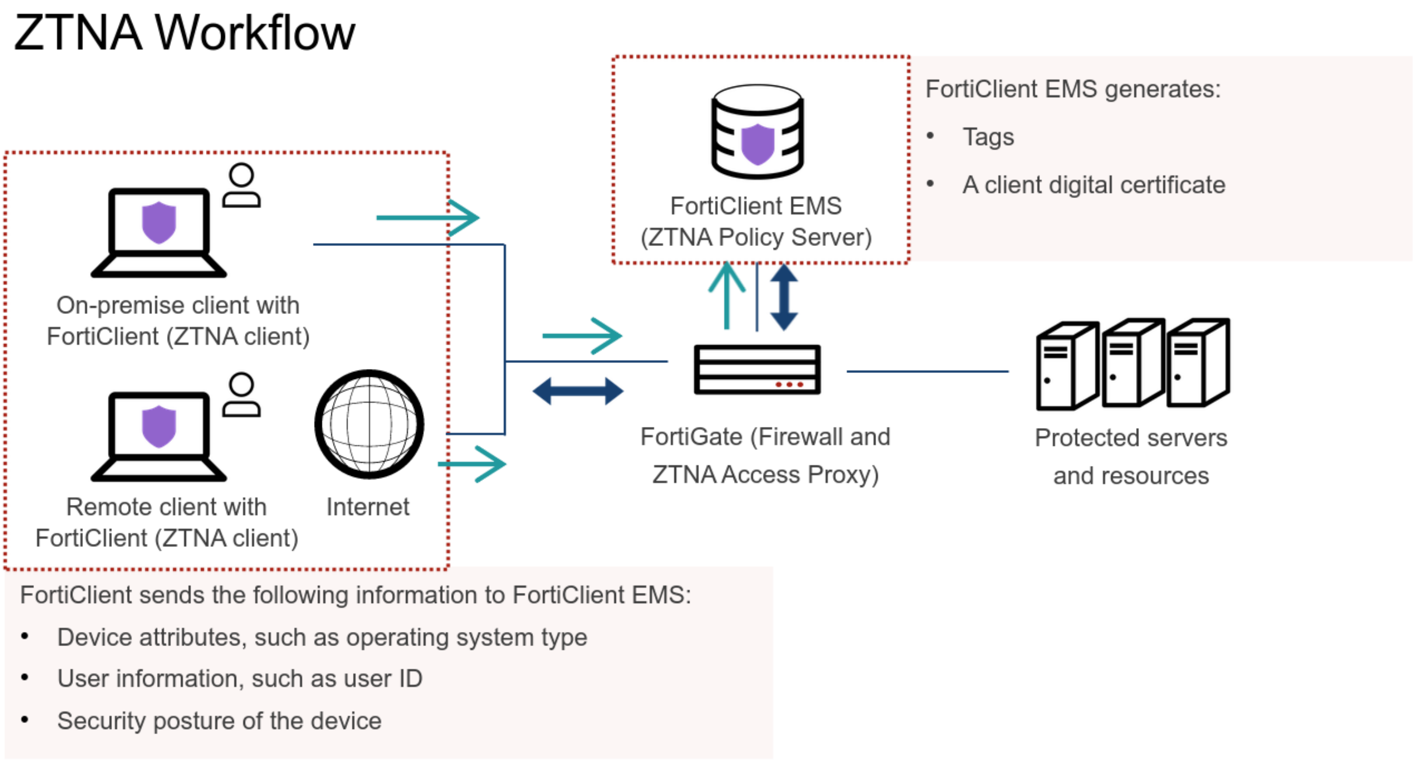
Most Common Secure Access Methods ⇒

IPsec VPN: Internet protocol security virtual private network
SSL VPN: Secure Socket Layer Virtual Private Network
ZTNA: Zero trust network access (which incorporates the principle of zero trust)

Comparing ZTNA to VPN ⇒

VPN: A VPN is a private connection across a public network that enables a user to exchange data safely with a private network as if the computing device was directly connected to the private network. Main components: client, server and protocols. Use cases: secure remote access and site-to-site.

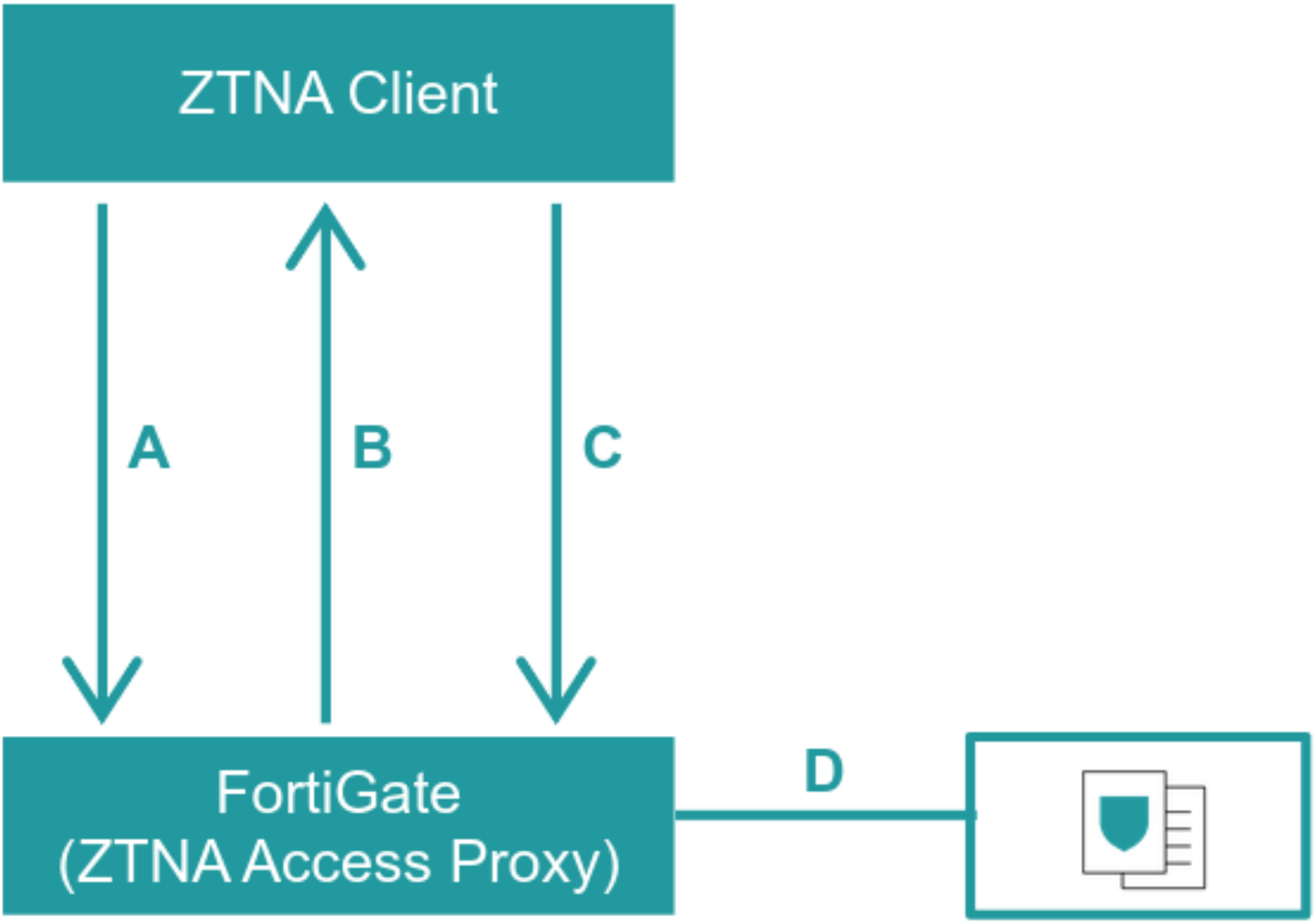
ZTNA: It applies the Zero Trust principal which is no user or device whether it is inside or outside of a network is trusted. It has enhanced security.


ZTNA Workflow
FortiClient EMS (ZTNA Policy Server)
FortiClient EMS generates:
• Tags
• A client digital certificate
On-premise client with FortiClient (ZTNA client)
Remote client with FortiClient (ZTNA client)
Internet
FortiGate (Firewall and ZTNA Access Proxy)
Protected servers and resources
FortiClient sends the following information to FortiClient EMS:
• Device attributes, such as operating system type
• User information, such as user ID
• Security posture of the device

How Does Fortinet ZTNA Work?

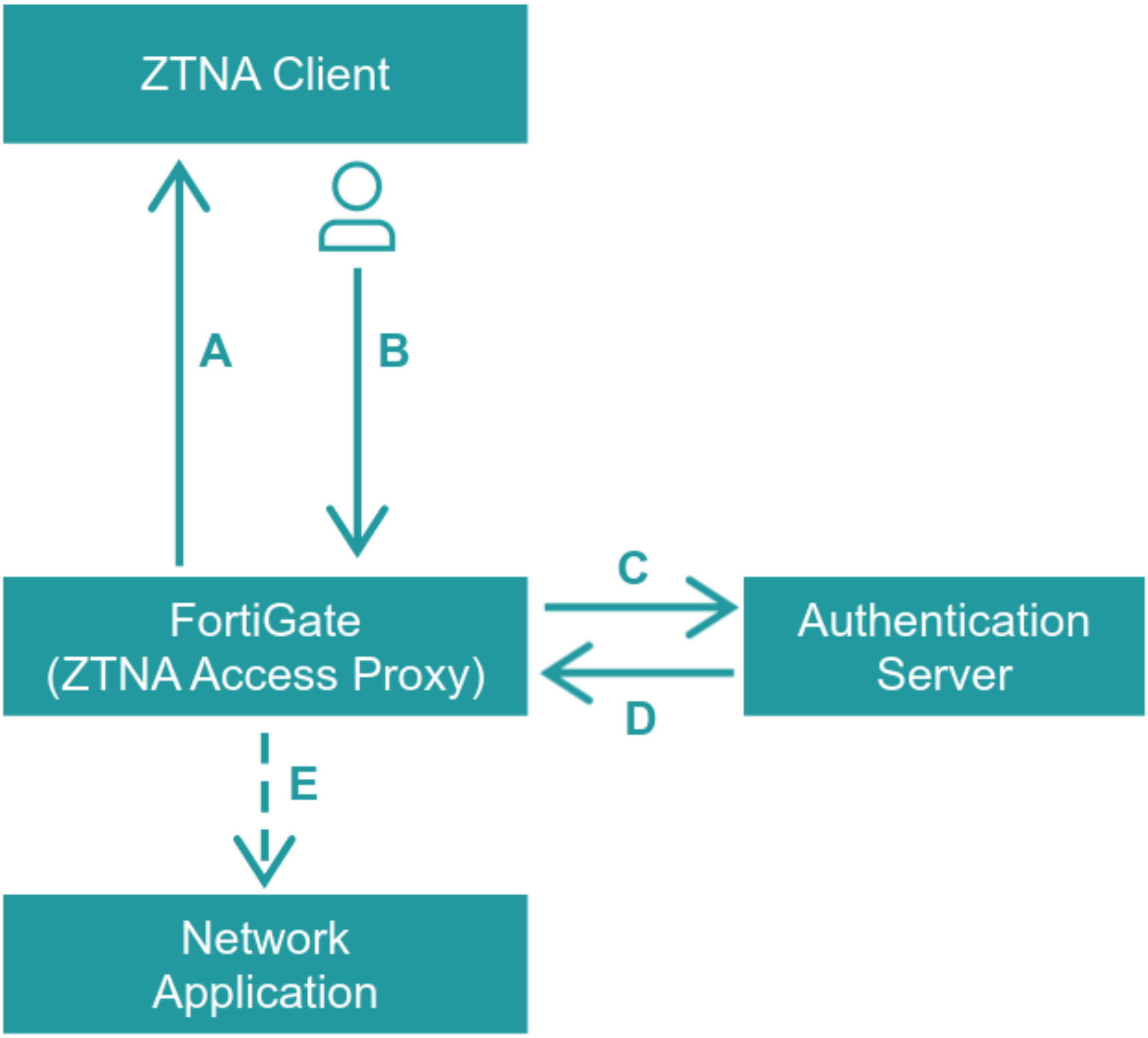
Step 1 → Device Identity Validation

a. The Endpoint connects to the ZTNA access proxy
b. FortiGate challenges the endpoint foe device identification
c. Endpoint sends its certificates to FortiGate, which was previously issues by FortiClient EMS
d. FortiGate applier the tags and rules associated with the device.

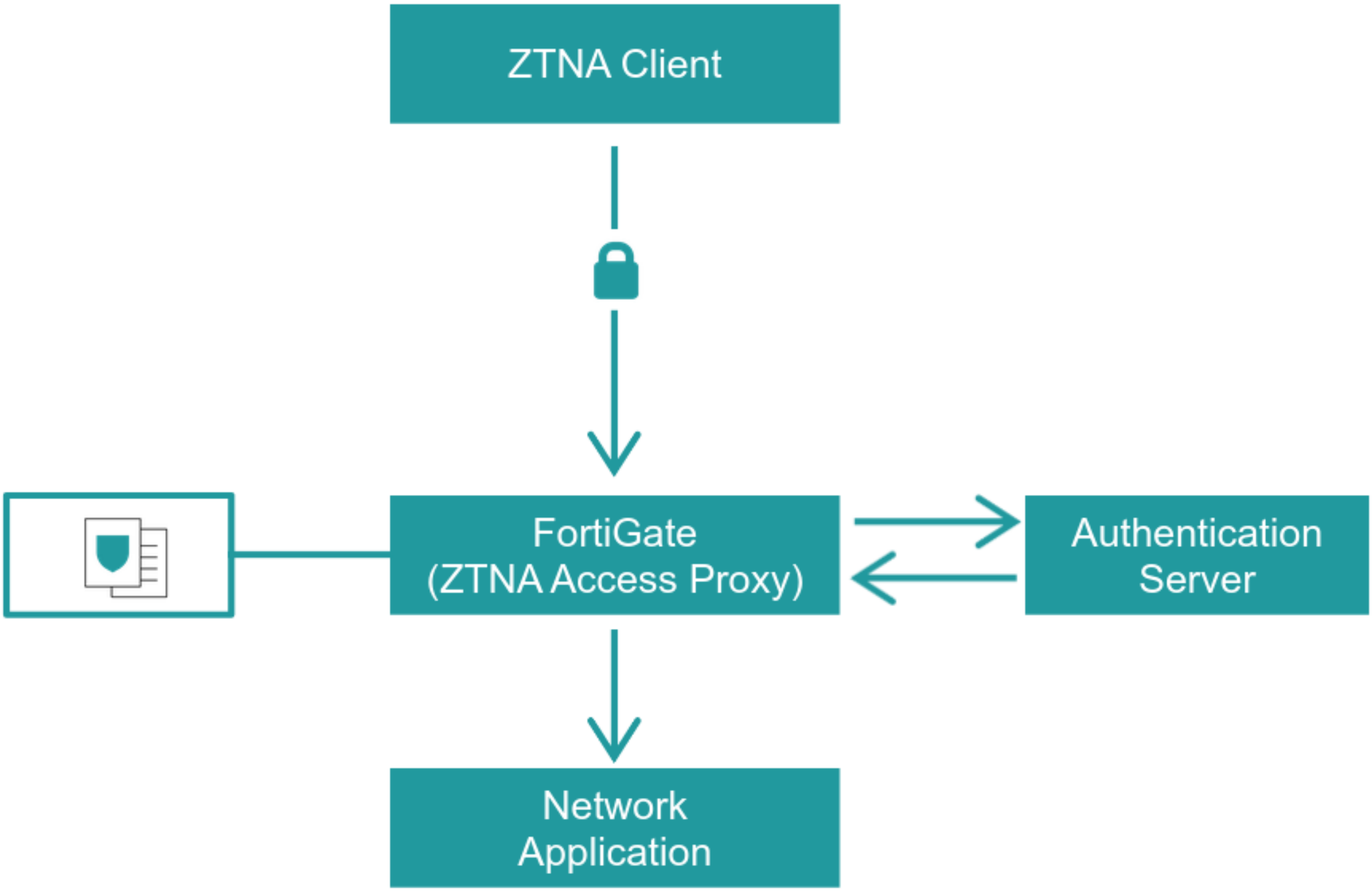


Step 2 → User authentication

    a. FortiGate asks endpoint for user authentication
    b. User sends their credentials on the endpoint
    c. FortGate forwards the creds to the authentication server (could be an AD, LDAP directory, a database or IDaaS)
    d. The user's identity is validated and its roles are retrieved from the authentication server
    e. The roles are used by FortiGate to determine access to the network application



Step 3 → Encrypted Session is established



Firewall

2022/08/02 - 05:26:59 PM - Tuesday
Firewall

Packet Filter Firewall ⇒
1. Examines the packets based on source+destination network addresses, protocols and port numbers.
2. Could be bypassed by bad actors.

2nd Generation Fireawall ⇒
1. aka Stateful firewall
2. They observe new connections and continuously monitor their conversation
3. Then drop packet if a connection behaved improperly

4. Drawback: Could not detect rouge packets if they were an acceptable protocol such as HTTP

3rd Generation Firewall ⇒
1. Still Stateful
2. understands higher level protocols (application layer filtering)
3. Can differentiate between HTTP, FTP or DNS

Next Generation Firewall ⇒
1. Has multiple security checkpoints
2. Has rule based filtering
3. Performs deep packet inspection (IPS) on malicious packets
4. uses sandboxed environments to inspect malicious packets
5. Can control application based on the user type/role
6. Segregates users, devices and application.
7. Delivers high performance inspection

FortiGate is the next-generation firewall of Fortinet.

Wi-Fi

2022/08/02 - 06:10:44 PM - Tuesday
Wi-Fi

It is a technology for wireless, local area networking based on the IEEE 802.11 standards.

Originally the authentication and privacy mechanisms for wifi were very weak. WEP (wired equivalent privacy) used a key to encrypt traffic using the RC4 keystream. But it could be compromised.

Then IEEE and the wifi alliance produced WPA (Wi-Fi Protected Access). It added extra security but still used RC4.

Based on AES (Advanced Encryption Standard) from the NIST (National Institute of Standards and Technology) a new standard was introduced named WPA2 (Wi-Fi Protected Access 2).

This was a lot more secure than WEP. WPA2 had 2 flavors. The personal level of security used a shared passphrase for network authentication and key exchange. The enterprise level security used 802.1x authentication mechanisms.

WPA3 (Wi-Fi Protected Access 3) was introduced in 2018. It introduced a new, more secure handshake for making connections, an easier method for adding devices to the network, increased key sizes, and other security features.

Fortinet offers a wireless product named FortiAP which intregates with and is managed by FortiGate, a NGFW.

Threat Intelligence Services

2022/08/02 - 06:21:08 PM - Tuesday

Threat Intelligence Services

In the early days of endpoint antivirus products, vendors kept a catalog of each known virus using their signatures and detected malware based on that catalog.

But with time malware developers gained expertise and their malware became more sophisticated. They evaded classic signature based scanning by being able to change their file content at will. There were known as polymorphic malware.

To detect complete unknown malware, vendorr created products that took a suspect file and released it in a sandbox and analyzed its behaviors closely. They used proprietary heuristic algorithms.

IoC = Indicators of Compromise

Fortinets Threat Intelligence Service is known as FortiGuard Labs.

SOAR

2022/08/05 - 08:09:32 AM - Friday

SOAR
Security Orchestration Automation and Response

SIM = Security Information Management System

What is SOAR?
SOAR connects all of the other tools in the security stack together into defined workflows, which can be run automatically, reducing alert fatigue and repetitive manual processes.

Alert Fatigue: More alerts to respond to each day means that you have less time to spend on each alert. Performance degradation in the face of a flood of alerts is called alert fatigue.

Phishing investigations are one of the most common use cases for SOAR implementation by customers.

The fortinet SOAR product is named FortiSOAR.

Network Access Control

2022/08/05 - 08:26:40 AM - Friday
Network Access Control (NAC)

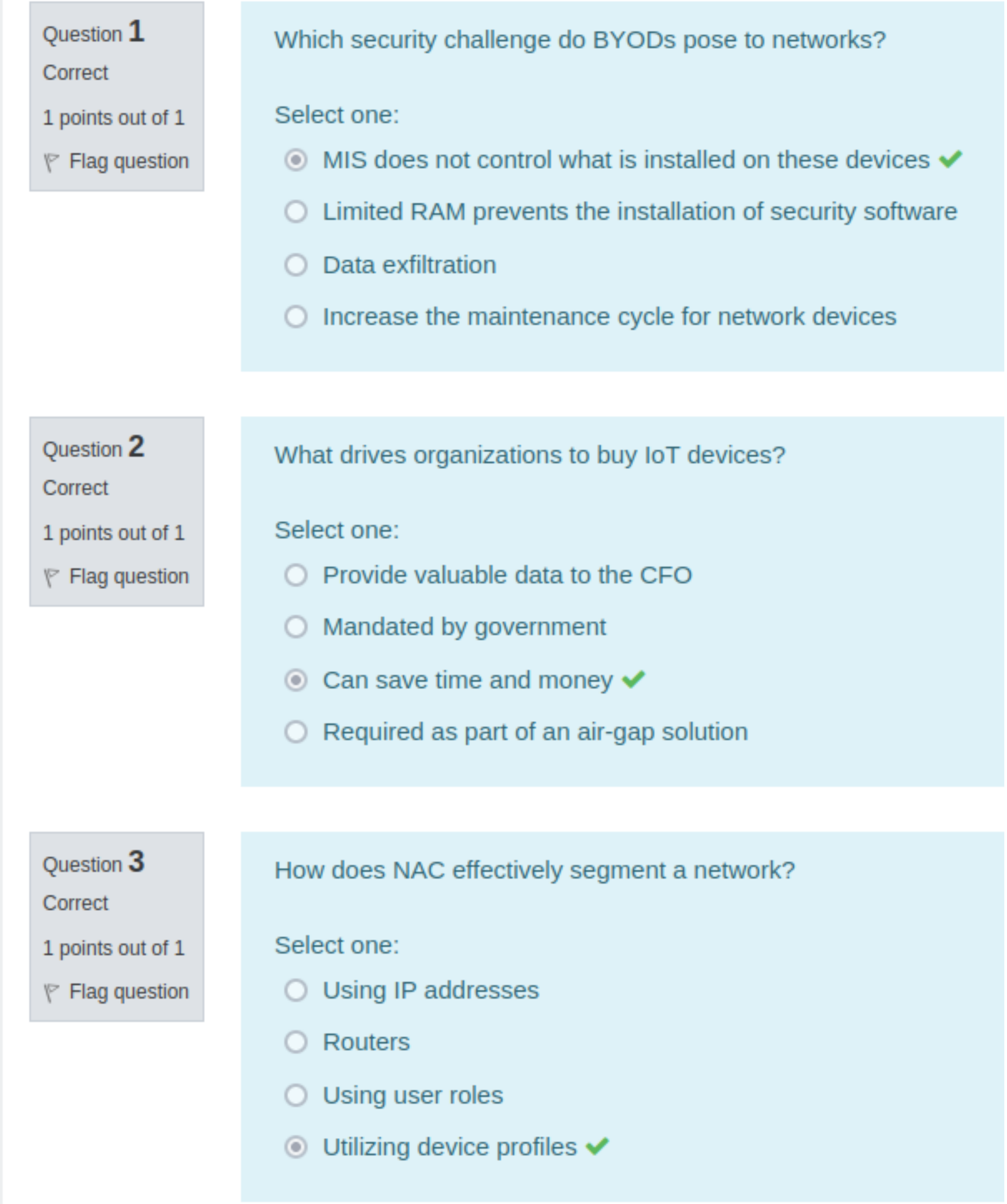
NAC is an appliance or virtual machine that controls device access to the network. It began as a network authentication and authorization method for devices joining the network, which follows the IEEE 802.1X standards.
The authentication method involves 3 parties:
1. The client device
2. The authenticator

3. The authentication server

NVR = Network Video Recorder

NAC grants access to devices for specific services based on the device profiles. For example: an IP camera will be given access to a NVR server, but will not be given access to a finance server.

Fortinet NAC product is FortiNAC.



Question **1**

Correct

1 points out of 1

Flag question

Which security challenge do BYODs pose to networks?

Select one:

● MIS does not control what is installed on these devices ✓

○ Limited RAM prevents the installation of security software

○ Data exfiltration

○ Increase the maintenance cycle for network devices

Question **2**

Correct

1 points out of 1

Flag question

What drives organizations to buy IoT devices?

Select one:

○ Provide valuable data to the CFO

○ Mandated by government

● Can save time and money ✓

○ Required as part of an air-gap solution

Question **3**

Correct

1 points out of 1

Flag question

How does NAC effectively segment a network?

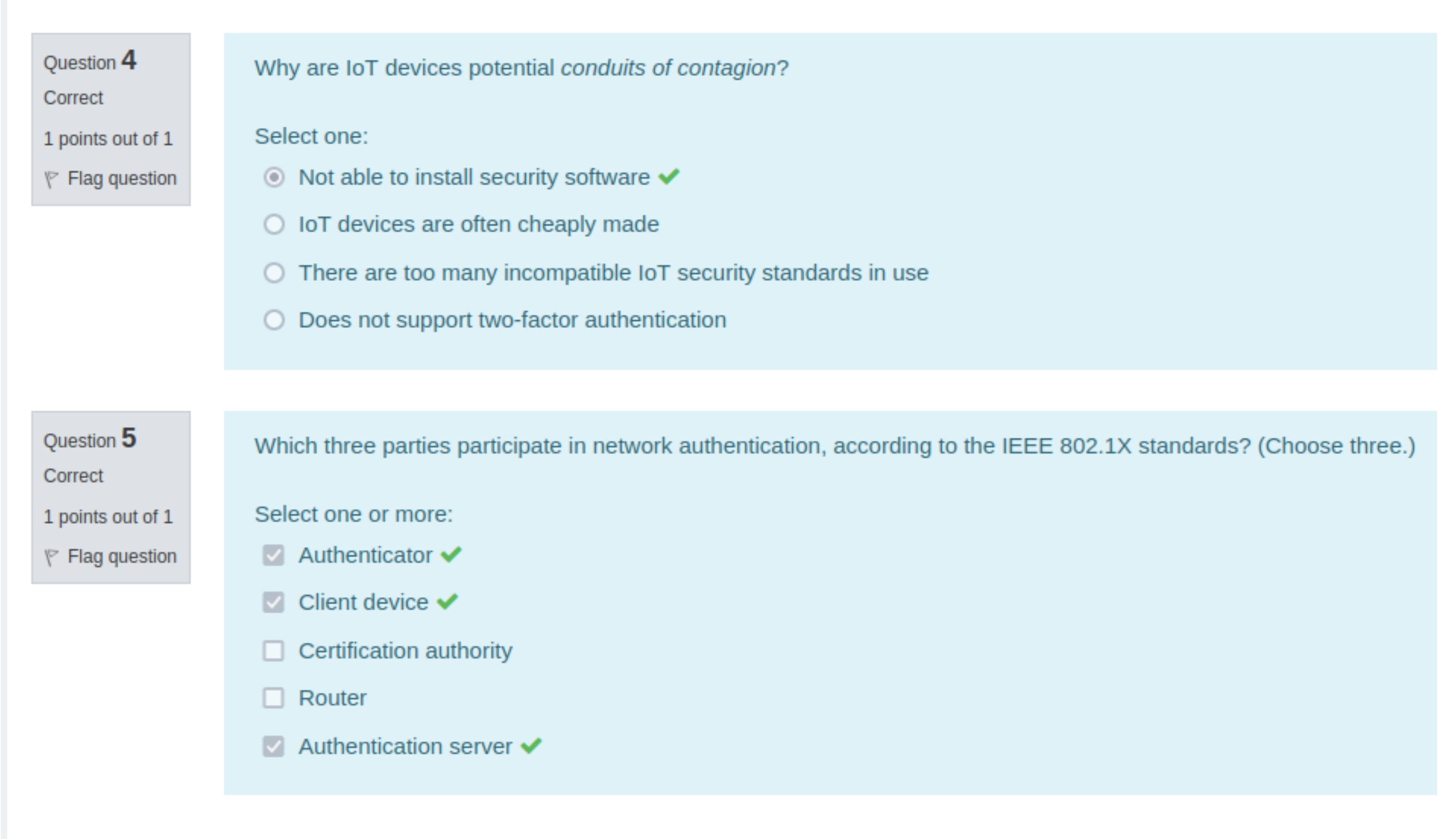
Select one:

○ Using IP addresses

○ Routers

○ Using user roles

● Utilizing device profiles ✓



Question **4**

Correct

1 points out of 1

Flag question

Why are IoT devices potential *conduits of contagion*?

Select one:

● Not able to install security software ✓

○ IoT devices are often cheaply made

○ There are too many incompatible IoT security standards in use

○ Does not support two-factor authentication

Question **5**

Correct

1 points out of 1

Flag question

Which three parties participate in network authentication, according to the IEEE 802.1X standards? (Choose three.)

Select one or more:

☑ Authenticator ✓

☑ Client device ✓

□ Certification authority

□ Router

☑ Authentication server ✓

Sandbox

```
2022/08/05 - 08:42:34 AM - Friday
Sandbox
```

Question **1**

Correct

1 points out of 1

Flag question

Which new development in malware caused sandbox technology to automate and introduce artificial intelligence learning?

Select one:

◉ AI-driven attacks ✓

○ Polymorphic viruses

○ Ransomware

○ Trojan horse

Question **2**

Correct

1 points out of 1

Flag question

Which feature characterizes third-generation sandbox technology?

Select one:

◉ Automation and artificial intelligence ✓

○ Faster network speeds

○ Scanning of encrypted data streams

○ Streamlines manual testing

Question **3**

Correct

1 points out of 1

Flag question

What was a benefit of second generation sandbox technology?

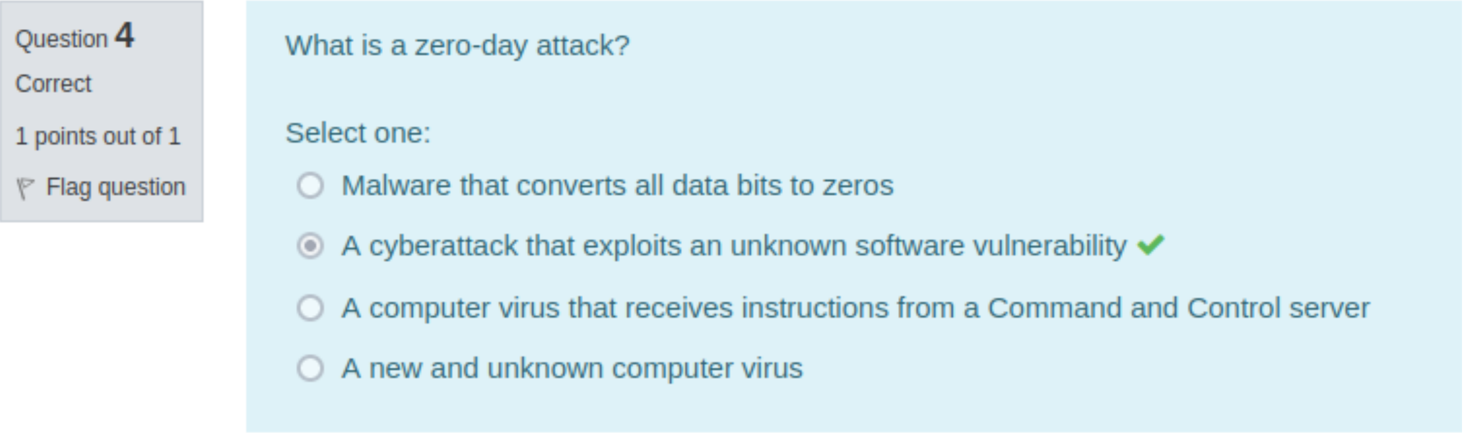
Select one:

◉ Timely sharing of threat intelligence ✓

○ Automation and artificial intelligence (AI)

○ Faster network speeds

○ Scanning of encrypted data streams



Question 4

Correct

1 points out of 1

Flag question

What is a zero-day attack?

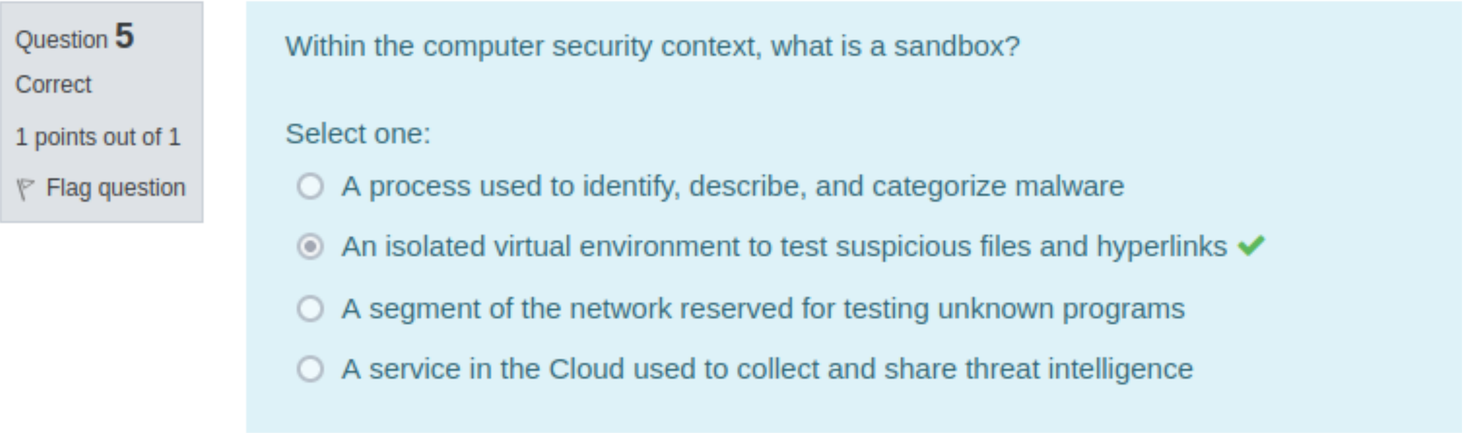
Select one:

○ Malware that converts all data bits to zeros

● A cyberattack that exploits an unknown software vulnerability ✓

○ A computer virus that receives instructions from a Command and Control server

○ A new and unknown computer virus



Question 5

Correct

1 points out of 1

Flag question

Within the computer security context, what is a sandbox?

Select one:

○ A process used to identify, describe, and categorize malware

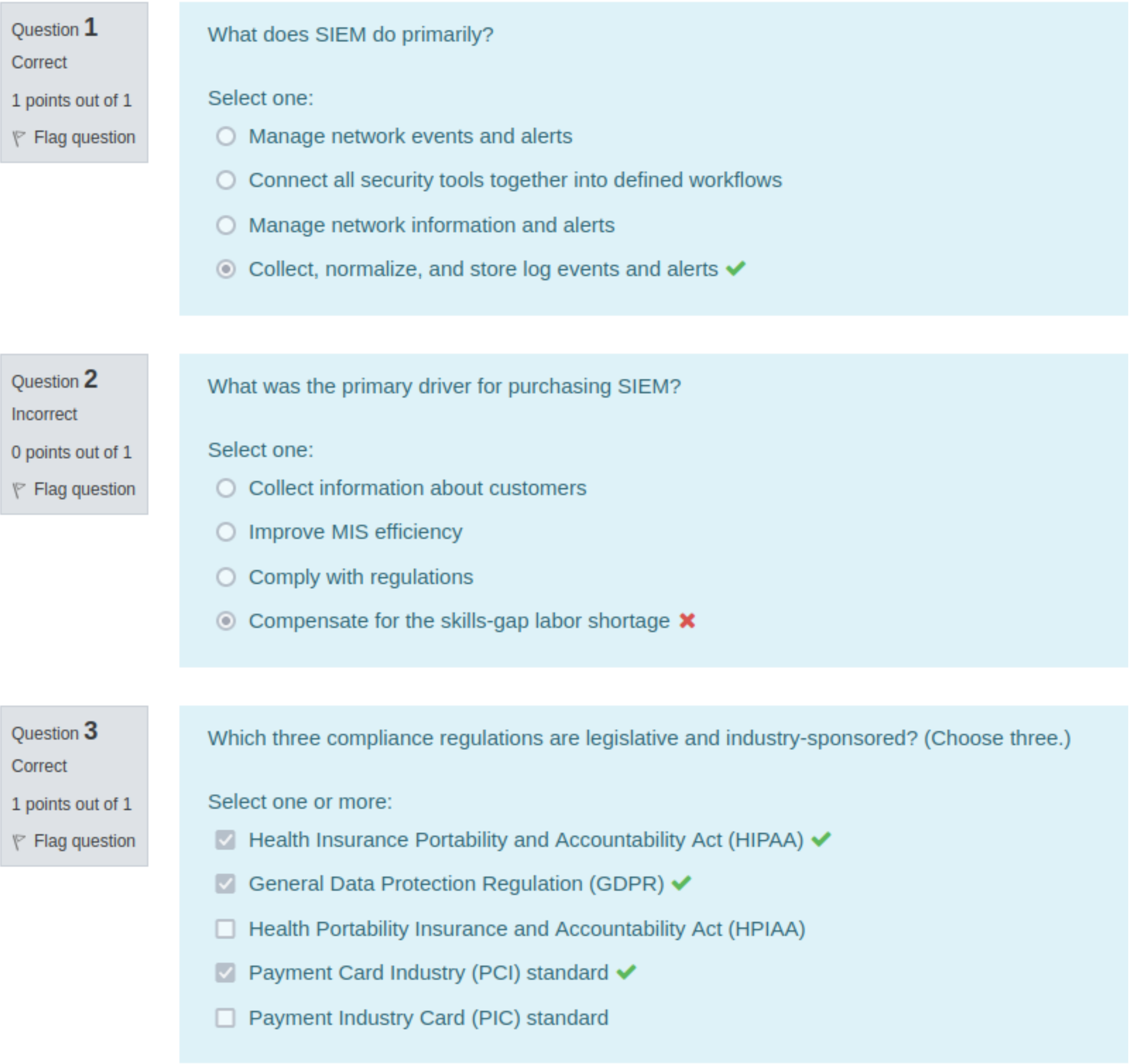
● An isolated virtual environment to test suspicious files and hyperlinks ✓

○ A segment of the network reserved for testing unknown programs

○ A service in the Cloud used to collect and share threat intelligence

Security Information & Event Management

2022/08/05 - 08:52:13 AM - Friday
Security Information & Event Management - SIEM



Question **1**

Correct

1 points out of 1

Flag question

What does SIEM do primarily?

Select one:

○ Manage network events and alerts

○ Connect all security tools together into defined workflows

○ Manage network information and alerts

● Collect, normalize, and store log events and alerts ✓

Question **2**

Incorrect

0 points out of 1

Flag question

What was the primary driver for purchasing SIEM?

Select one:

○ Collect information about customers

○ Improve MIS efficiency

○ Comply with regulations

● Compensate for the skills-gap labor shortage ✗

Question **3**

Correct

1 points out of 1

Flag question

Which three compliance regulations are legislative and industry-sponsored? (Choose three.)

Select one or more:

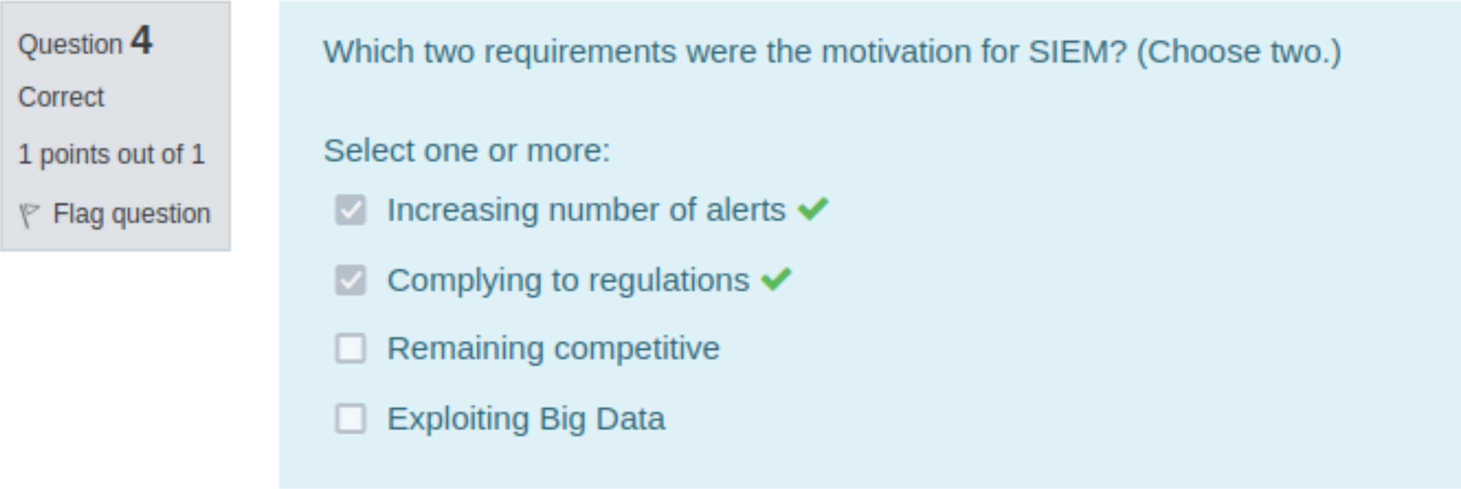
☑ Health Insurance Portability and Accountability Act (HIPAA) ✓

☑ General Data Protection Regulation (GDPR) ✓

□ Health Portability Insurance and Accountability Act (HPIAA)

☑ Payment Card Industry (PCI) standard ✓

□ Payment Industry Card (PIC) standard



Question **4**

Correct

1 points out of 1

Flag question

Which two requirements were the motivation for SIEM? (Choose two.)

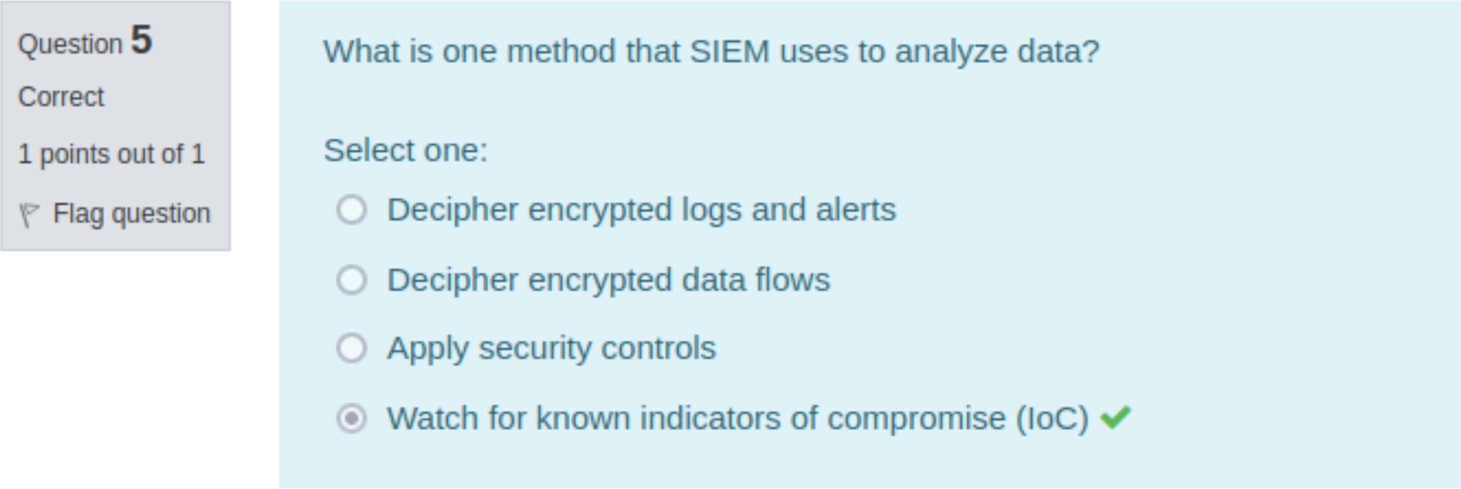
Select one or more:

☑ Increasing number of alerts ✓

☑ Complying to regulations ✓

□ Remaining competitive

□ Exploiting Big Data



Question **5**

Correct

1 points out of 1

Flag question

What is one method that SIEM uses to analyze data?

Select one:

○ Decipher encrypted logs and alerts

○ Decipher encrypted data flows

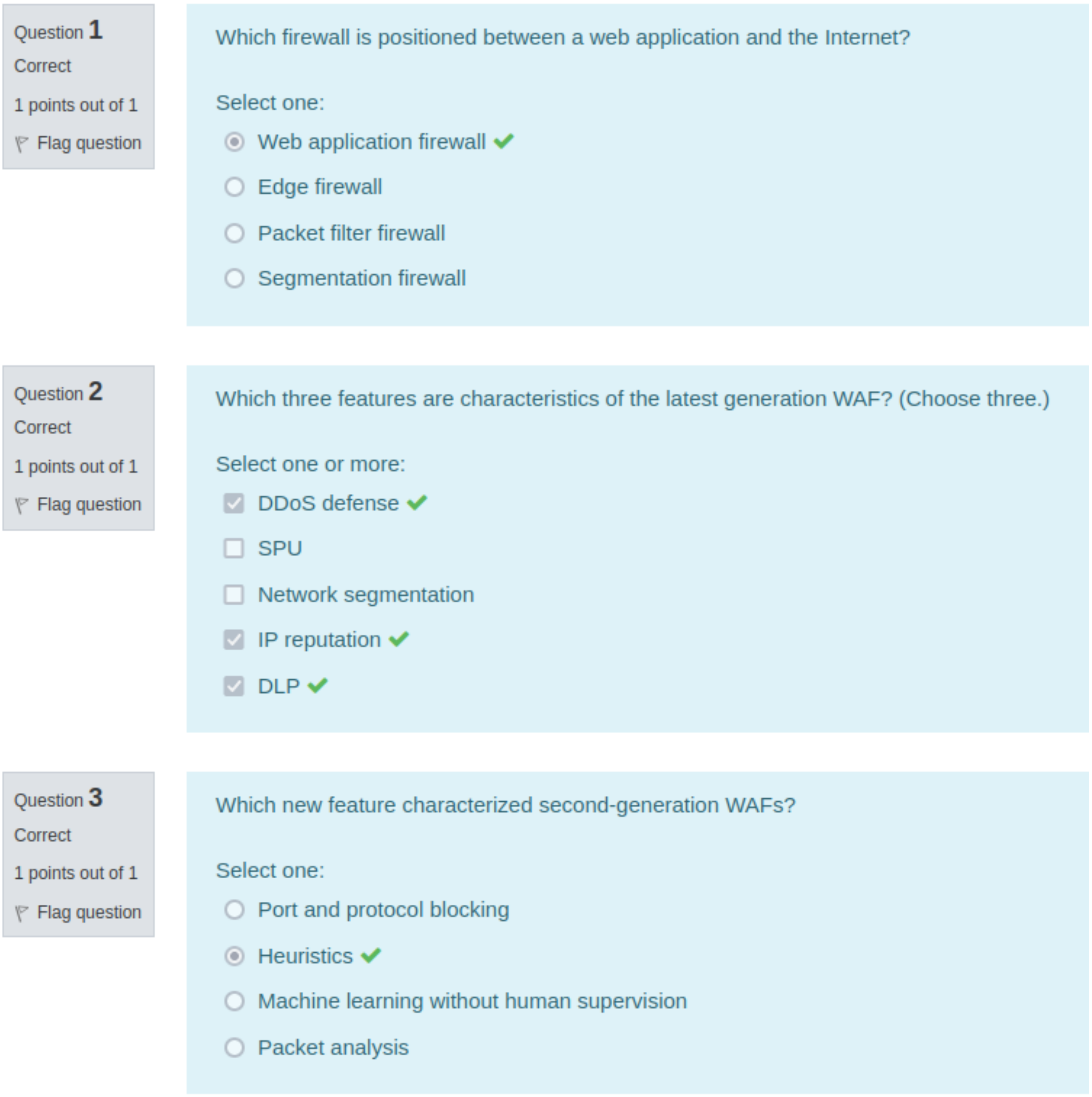
○ Apply security controls

● Watch for known indicators of compromise (IoC) ✓

Web Application Firewall

2022/08/05 - 09:03:33 AM - Friday

Web Application Firewall



Question **1**

Correct

1 points out of 1

Flag question

Which firewall is positioned between a web application and the Internet?

Select one:

● Web application firewall ✓

○ Edge firewall

○ Packet filter firewall

○ Segmentation firewall

Question **2**

Correct

1 points out of 1

Flag question

Which three features are characteristics of the latest generation WAF? (Choose three.)

Select one or more:

☑ DDoS defense ✓

□ SPU

□ Network segmentation

☑ IP reputation ✓

☑ DLP ✓

Question **3**

Correct

1 points out of 1

Flag question

Which new feature characterized second-generation WAFs?

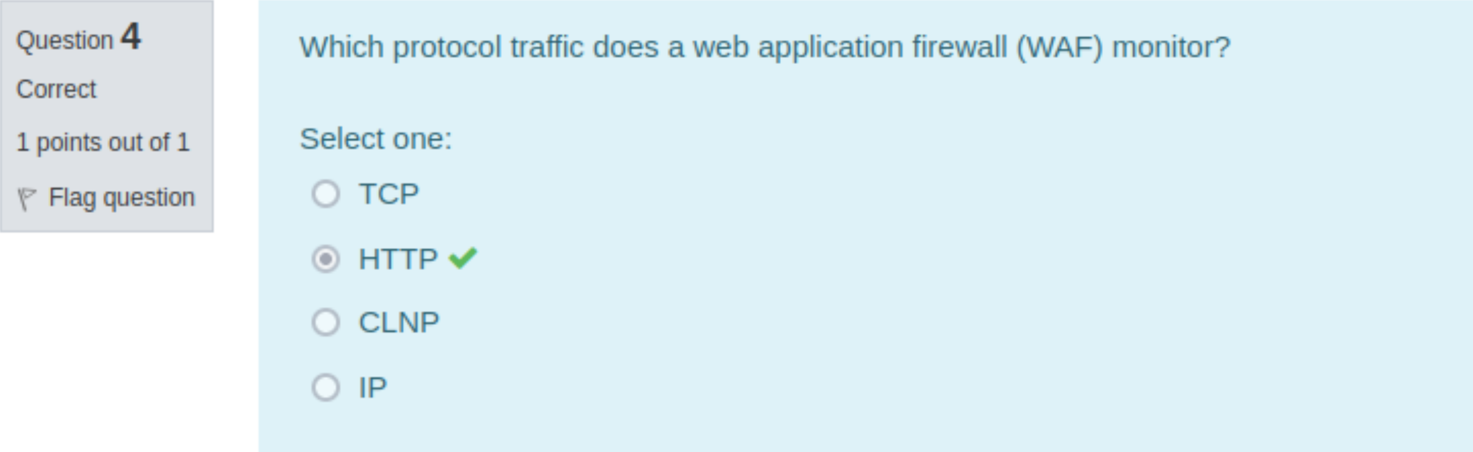
Select one:

○ Port and protocol blocking

● Heuristics ✓

○ Machine learning without human supervision

○ Packet analysis



Question 4

Correct

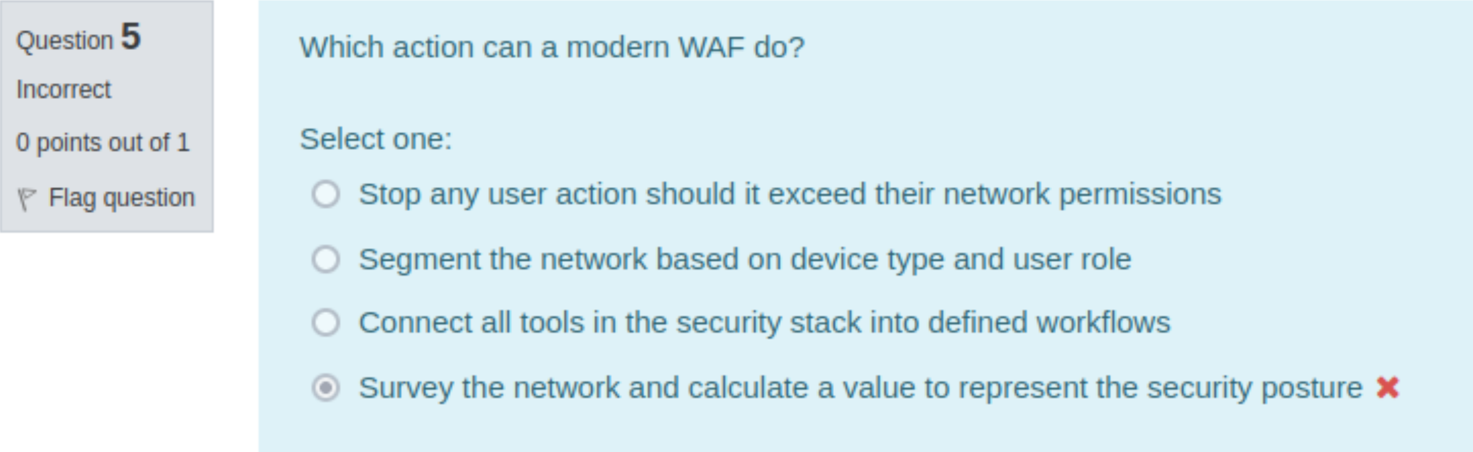
1 points out of 1

Flag question

Which protocol traffic does a web application firewall (WAF) monitor?

Select one:

- ○ TCP
- ● HTTP ✓
- ○ CLNP
- ○ IP



Question 5

Incorrect

0 points out of 1

Flag question

Which action can a modern WAF do?

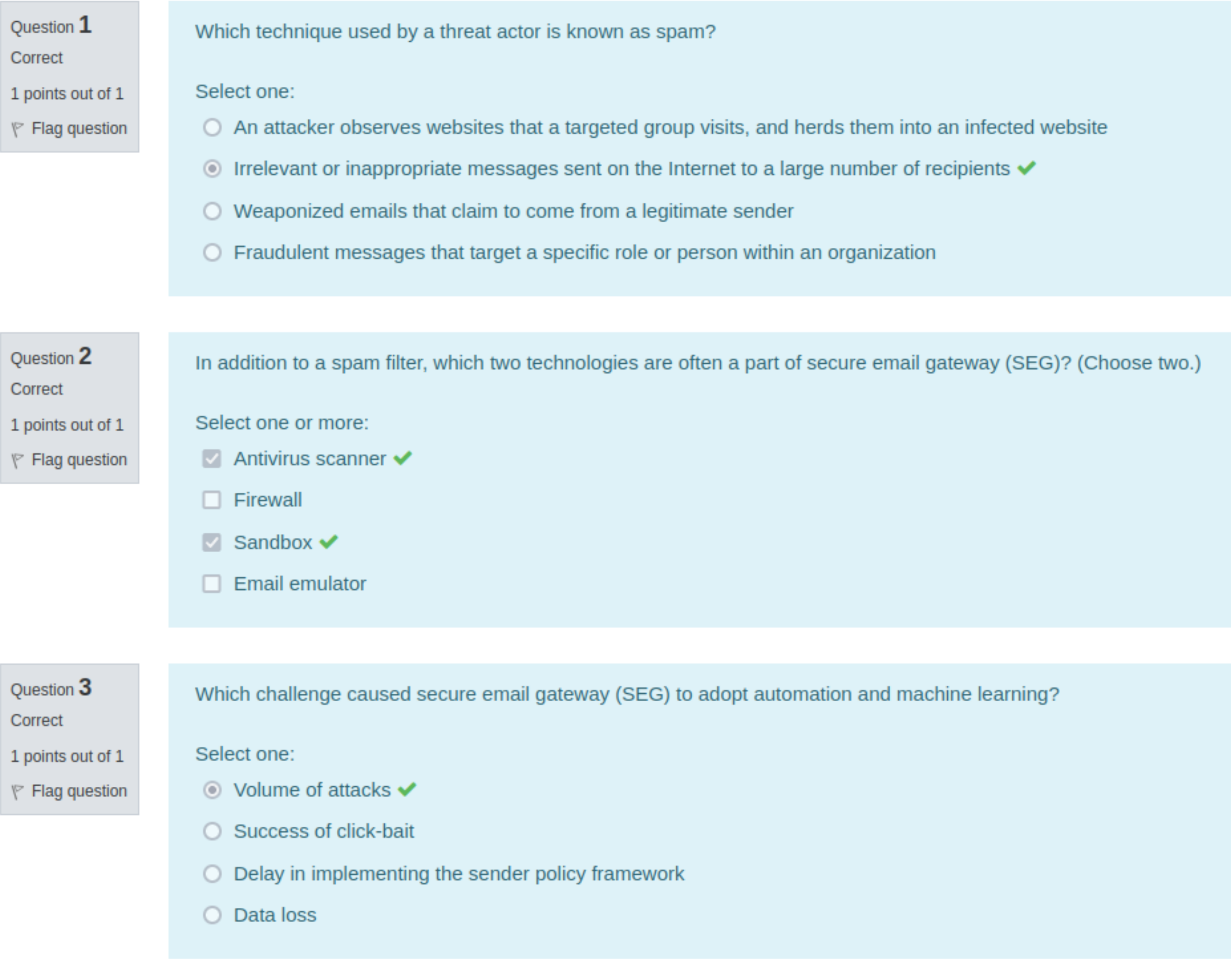
Select one:

- ○ Stop any user action should it exceed their network permissions
- ○ Segment the network based on device type and user role
- ○ Connect all tools in the security stack into defined workflows
- ● Survey the network and calculate a value to represent the security posture ✗

Secure Email Gateway

2022/08/05 - 11:40:33 AM - Friday

Secure Email Gateway



Question **1**
Correct
1 points out of 1
Flag question

Which technique used by a threat actor is known as spam?

Select one:

○ An attacker observes websites that a targeted group visits, and herds them into an infected website
● Irrelevant or inappropriate messages sent on the Internet to a large number of recipients ✓
○ Weaponized emails that claim to come from a legitimate sender
○ Fraudulent messages that target a specific role or person within an organization

Question **2**
Correct
1 points out of 1
Flag question

In addition to a spam filter, which two technologies are often a part of secure email gateway (SEG)? (Choose two.)

Select one or more:

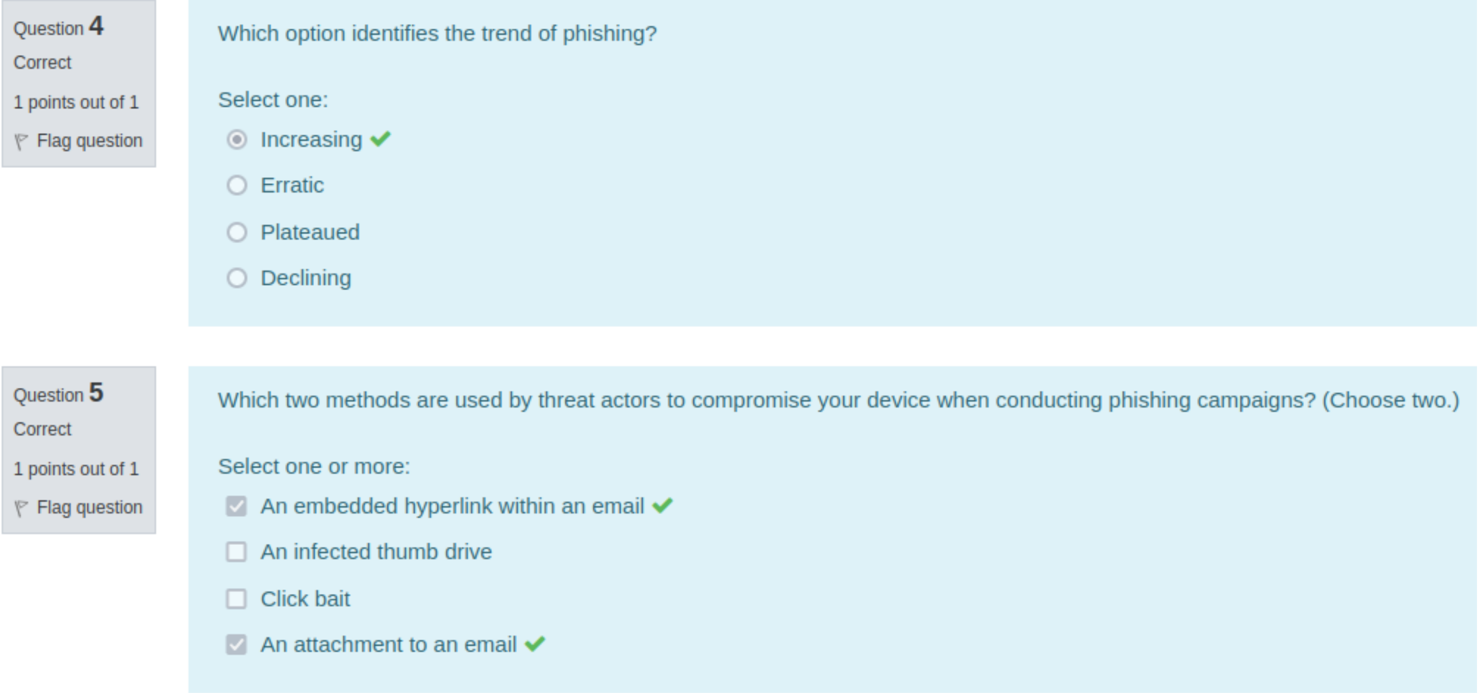
☑ Antivirus scanner ✓
□ Firewall
☑ Sandbox ✓
□ Email emulator

Question **3**
Correct
1 points out of 1
Flag question

Which challenge caused secure email gateway (SEG) to adopt automation and machine learning?

Select one:

● Volume of attacks ✓
○ Success of click-bait
○ Delay in implementing the sender policy framework
○ Data loss



Question **4**
Correct
1 points out of 1
Flag question

Which option identifies the trend of phishing?

Select one:

● Increasing ✓
○ Erratic
○ Plateaued
○ Declining

Question **5**
Correct
1 points out of 1
Flag question

Which two methods are used by threat actors to compromise your device when conducting phishing campaigns? (Choose two.)

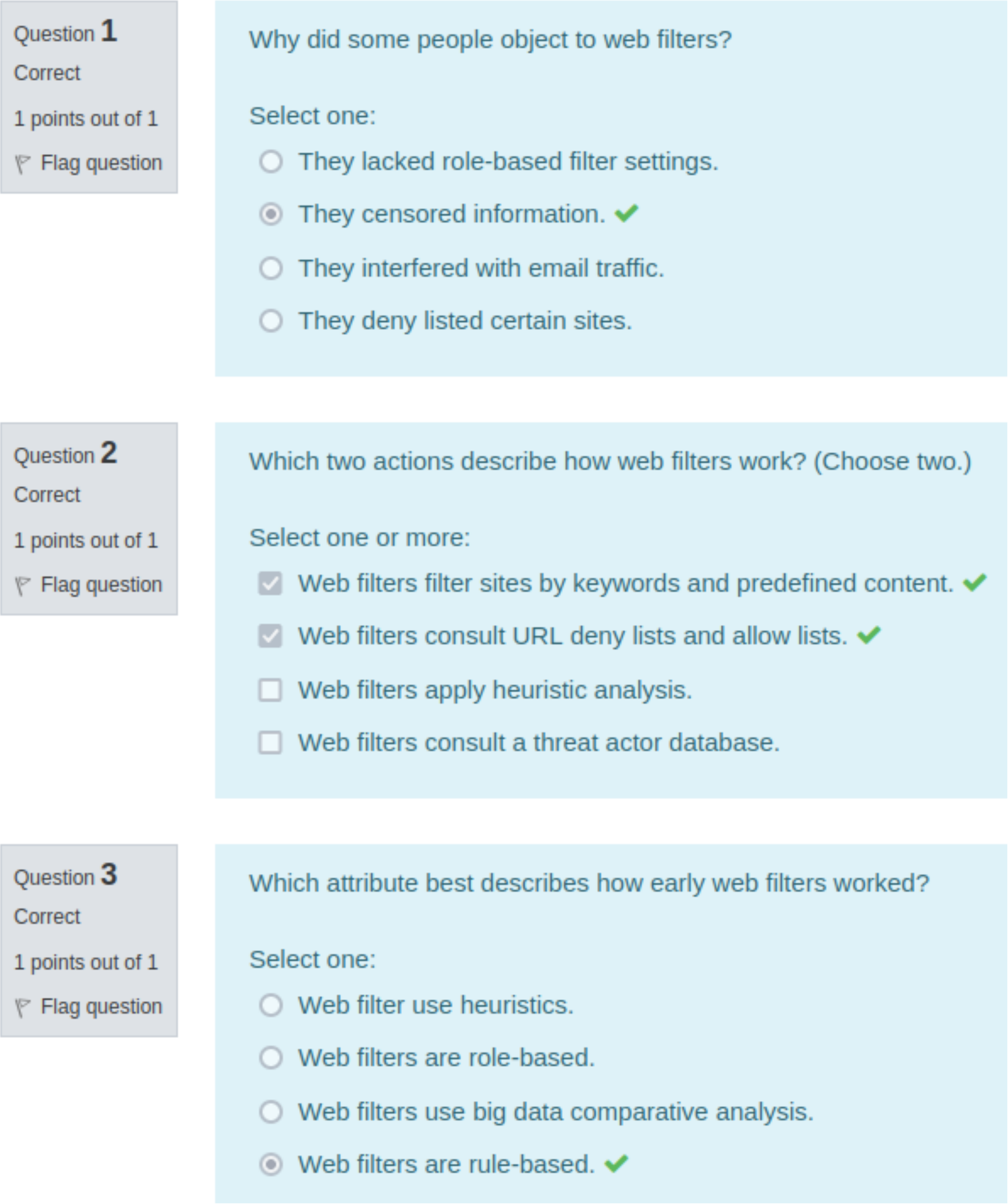
Select one or more:

☑ An embedded hyperlink within an email ✓
□ An infected thumb drive
□ Click bait
☑ An attachment to an email ✓

Web Filter

2022/08/05 - 11:49:22 AM - Friday

Web Filter



Question **1**

Correct

1 points out of 1

Flag question

Why did some people object to web filters?

Select one:

○ They lacked role-based filter settings.

● They censored information. ✓

○ They interfered with email traffic.

○ They deny listed certain sites.

Question **2**

Correct

1 points out of 1

Flag question

Which two actions describe how web filters work? (Choose two.)

Select one or more:

☑ Web filters filter sites by keywords and predefined content. ✓

☑ Web filters consult URL deny lists and allow lists. ✓

□ Web filters apply heuristic analysis.

□ Web filters consult a threat actor database.

Question **3**

Correct

1 points out of 1

Flag question

Which attribute best describes how early web filters worked?

Select one:

○ Web filter use heuristics.

○ Web filters are role-based.

○ Web filters use big data comparative analysis.

● Web filters are rule-based. ✓

Question **4**

Correct

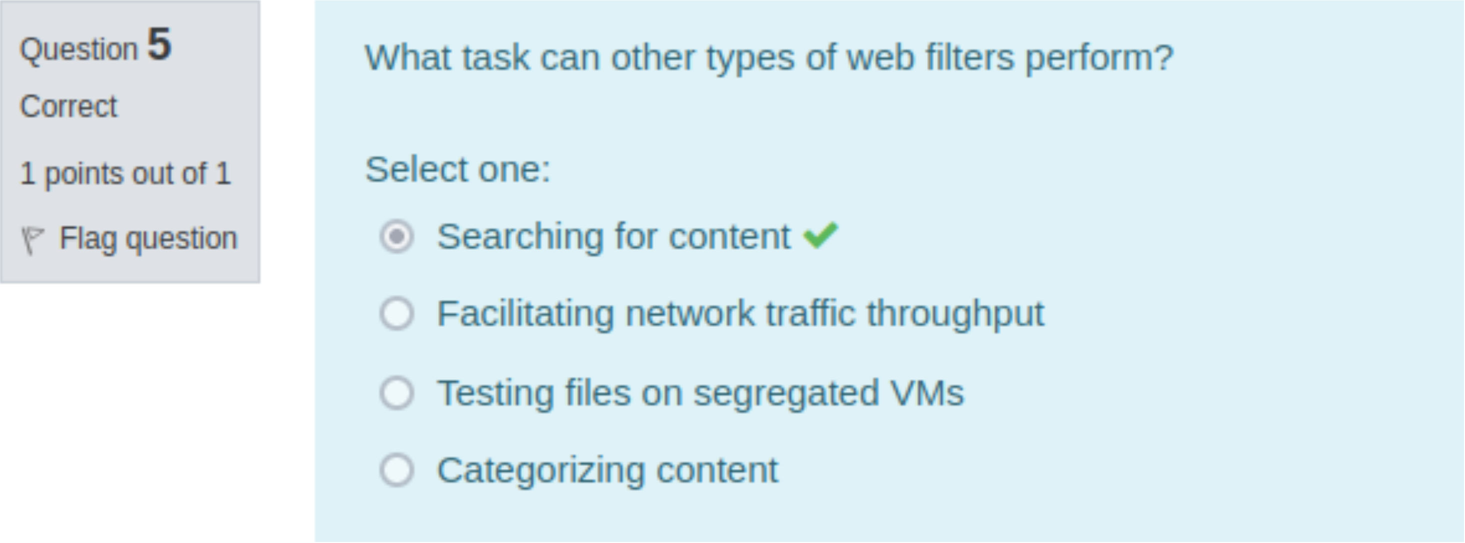
1 points out of 1

Flag question

Which two reasons gave rise to web filters? (Choose two.)

Select one or more:

- ☑ Web filters improve security. ✓
- □ Web filters reduce network traffic.
- ☑ Web filters stop objectionable content. ✓
- □ Web filters promote education.



Question **5**

Correct

1 points out of 1

Flag question

What task can other types of web filters perform?

Select one:

- ● Searching for content ✓
- ○ Facilitating network traffic throughput
- ○ Testing files on segregated VMs
- ○ Categorizing content

Certificate

2022/08/05 - 11:58:41 AM - Friday

Course_Completion_Certificate.pdf

NSE_2_Certification.pdf

NSE2 Logo: