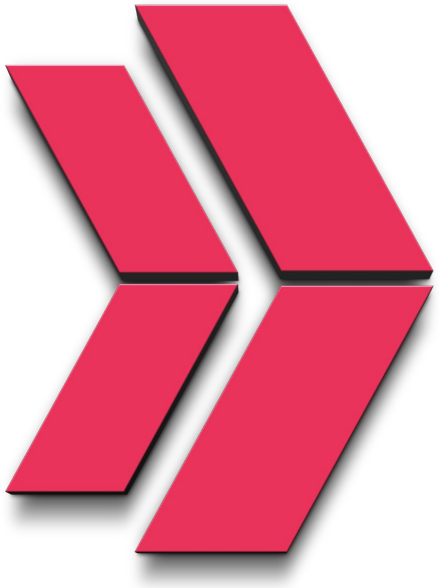


CLARUSWAY

WAY TO REINVENT YOURSELF

CompTIA (5A-5B-5C) Secure Enterprise Network Architecture

AGENDA

- 5A - Enterprise Network Architecture (6)
- 5B - Network Security Appliances (12)
- 5C - Secure Communications (4)
- TOTAL: 22

5A - Enterprise Network Architecture

5A - Enterprise Network Architecture

NO.1 A business received a small grant to migrate its infrastructure to an off-premises solution.
Which of the following should be considered first?

(A). Security of cloud providers
(B). Cost of implementation
(C). Ability of engineers
(D). Security of architecture

5A - Enterprise Network Architecture

NO.1 A business received a **small grant** to migrate its infrastructure to an **off-premises** solution.
Which of the following should be considered first?

(A). Security of cloud providers
(B). Cost of implementation
(C). Ability of engineers
(D). Security of architecture

5A - Enterprise Network Architecture

NO.2 Which of the following security concepts is accomplished with the installation of a RADIUS server?

A. CIA
B. AAA
C. ACL
D. PEM

5A - Enterprise Network Architecture

NO.2 Which of the following security concepts is accomplished with the installation of a **RADIUS server?**

A. CIA
B. AAA
C. ACL
D. PEM

5A - Enterprise Network Architecture

NO.3 A company would like to provide employees with computers that do not have access to the internet in order to prevent information from being leaked to an online forum.

Which of the following would be best for the systems administrator to implement?

A. Air gap
B. Jump server
C. Logical segmentation
D. Virtualization

5A - Enterprise Network Architecture

NO.3 A company would like to provide employees with computers that do not have access to the internet in order to **prevent information from being leaked** to an online forum.

Which of the following would be best for the systems administrator to implement?

A. Air gap
B. Jump server
C. Logical segmentation
D. Virtualization

5A - Enterprise Network Architecture

NO.4 A visitor plugs a laptop into a network jack in the lobby and is able to connect to the company's network.

Which of the following should be configured on the existing network infrastructure to best prevent this activity?

A. Port security

B. Web application firewall

C. Transport layer security

D. Virtual private network

5A - Enterprise Network Architecture

NO.4 A visitor **plugs a laptop into a network jack** in the lobby and is able to connect to the company's network.

Which of the following should be configured on the existing network infrastructure to best prevent this activity?

A. Port security

B. Web application firewall

C. Transport layer security

D. Virtual private network

5A - Enterprise Network Architecture

NO.5 A recent penetration test identified that an attacker could flood the MAC address table of network switches.

Which of the following would best mitigate this type of attack?

A. Load balancer

B. Port security

C. IPS

D. NGFW

5A - Enterprise Network Architecture

NO.5 A recent penetration test identified that an attacker could **flood the MAC address table of network switches.**

Which of the following would best mitigate this type of attack?

A. Load balancer

B. Port security

C. IPS

D. NGFW

5A - Enterprise Network Architecture

NO.6 A security analyst finds a rogue device during a monthly audit of current endpoint assets that are connected to the network. The corporate network utilizes 802.1x for access control. To be allowed on the network, a device must have a known hardware address, and a valid user name and password must be entered in a captive portal. The following is the audit report:

IP address	MAC	Host	Account
10.18.04.42	BE-AC-11-F1-E4-44	PC-NY	user1
10.18.04.38	EB-AC-11-82-42-F3	PC-CA	user3
10.18.04.59	28-BB-5A-11-52-29	PC-PA	user2
10.18.04.58	28-BB-5A-F0-E9-D1	PC-TX	user4
10.18.04.22	EB-AC-11-82-42-F3	WIN10	user3
10.18.04.26	BB-28-11-21-A2-73	PC-NJ	admin

Which of the following is the most likely way a rogue device was allowed to connect?
A. A user performed a MAC cloning attack with a personal device.
B. A DMCP failure caused an incorrect IP address to be distributed
C. An administrator bypassed the security controls for testing.
D. DNS hijacking let an attacker intercept the captive portal traffic.

5A - Enterprise Network Architecture

NO.6 A security analyst **finds a rogue device** during a monthly audit of current endpoint assets that are connected to the network. The corporate network utilizes 802.1x for access control. To be allowed on the network, a device must have a known hardware address, and a valid user name and password must be entered in a captive portal. The following is the audit report:

IP address	MAC	Host	Account
10.18.04.42	BE-AC-11-F1-E4-44	PC-NY	user1
10.18.04.30	EB-AC-11-82-42-F3	PC-CA	user3
10.18.04.59	28-BB-5A-11-52-29	PC-PA	user2
10.18.04.58	28-BB-5A-F0-E9-D1	PC-TX	user4
10.18.04.22	EB-AC-11-82-42-F3	WIN10	user3
10.18.04.26	BB-28-11-21-A2-73	PC-NJ	admin

Which of the following is the most likely way a rogue device was allowed to connect?

A. A user performed a MAC cloning attack with a personal device.

B. A DMCP failure caused an incorrect IP address to be distributed

C. An administrator bypassed the security controls for testing.

D. DNS hijacking let an attacker intercept the captive portal traffic.

5B - Network Security Appliances

5B - Network Security Appliances

NO.1 Security controls in a data center are being reviewed to ensure data is properly protected and that human life considerations are included.
Which of the following best describes how the controls should be set up?

A. Remote access points should fail closed.
B. Logging controls should fail open.
C. Safety controls should fail open.
D. Logical security controls should fail closed.

5B - Network Security Appliances

NO.1 Security controls in a data center are being reviewed to ensure data is properly protected and that human life considerations are included.
Which of the following best describes how the controls should be set up?

A. Remote access points should fail closed.
B. Logging controls should fail open.
C. Safety controls should fail open.
D. Logical security controls should fail closed.

5B - Network Security Appliances

NO.2 A hacker gained access to a system via a phishing attempt that was a direct result of a user clicking a suspicious link. The link laterally deployed ransomware which laid dormant for multiple weeks across the network.
Which of the following would have mitigated the spread?

A. IPS
B. IDS
C. WAF
D. UAT

5B - Network Security Appliances

NO.2 A hacker gained access to a system via a phishing attempt that was a direct result of a user clicking a suspicious link. The link laterally deployed ransomware which laid dormant for multiple weeks across the network.
Which of the following would have mitigated the spread?

A. IPS
B. IDS
C. WAF
D. UAT

5B - Network Security Appliances

NO.3 An enterprise has been experiencing attacks focused on exploiting vulnerabilities in older browser versions with well-known exploits.
Which of the following security solutions should be configured to best provide the ability to monitor and block these known signature-based attacks?

A. ACL
B. DLP
C. IDS
D. IPS

5B - Network Security Appliances

NO.3 An enterprise has been experiencing attacks focused on exploiting vulnerabilities in older browser versions with well-known exploits.
Which of the following security solutions should be configured to best provide the ability to monitor and block these known signature-based attacks?

A. ACL
B. DLP
C. IDS
D. IPS

5B - Network Security Appliances

NO.4 An organization's internet-facing website was compromised when an attacker exploited a buffer overflow.
Which of the following should the organization deploy to best protect against similar attacks in the future?

A. NGFW
B. WAF
C. TLS
D. SD-WAN

5B - Network Security Appliances

NO.4 An organization's internet-facing website was compromised when an attacker exploited a buffer overflow.
Which of the following should the organization deploy to best protect against similar attacks in the future?

A. NGFW
B. WAF
C. TLS
D. SD-WAN

5B - Network Security Appliances

NO.5 A company tested and validated the effectiveness of network security appliances within the corporate network. The IDS detected a high rate of SQL injection attacks against the company's servers, and the company's perimeter firewall is at capacity.

Which of the following would be the best action to maintain security and reduce the traffic to the perimeter firewall?

A. Set the appliance to IPS mode and place it in front of the company firewall.
B. Convert the firewall to a WAF and use IPSec tunnels to increase throughput.
C. Set the firewall to fail open if it is overloaded with traffic and send alerts to the SIEM.
D. Configure the firewall to perform deep packet inspection and monitor TLS traffic.

5B - Network Security Appliances

NO.5 A company tested and validated the effectiveness of network security appliances within the corporate network. The IDS detected a high rate of **SQL injection attacks** against the company's servers, and the company's perimeter firewall is at capacity.

Which of the following would be the best action to maintain security and reduce the traffic to the perimeter firewall?

A. Set the appliance to IPS mode and place it in front of the company firewall.
B. Convert the firewall to a WAF and use IPSec tunnels to increase throughput.
C. Set the firewall to fail open if it is overloaded with traffic and send alerts to the SIEM.
D. Configure the firewall to perform deep packet inspection and monitor TLS traffic.

5B - Network Security Appliances

NO.6 The CIRT is reviewing an incident that involved a human resources recruiter exfiltration sensitive company data. The CIRT found that the recruiter was able to use HTTP over port 53 to upload documents to a web server.

Which of the following security infrastructure devices could have identified and blocked this activity?

A. WAF utilizing SSL decryption
B. NGFW utilizing application inspection
C. UTM utilizing a threat feed
D. SD-WAN utilizing IPSec

5B - Network Security Appliances

NO.6 The CIRT is reviewing an incident that involved a human resources recruiter exfiltration sensitive company data. The CIRT found that the recruiter was able to use HTTP over port 53 to **upload documents to a web server.**

Which of the following security infrastructure devices could have identified and blocked this activity?

A. WAF utilizing SSL decryption
B. NGFW utilizing application inspection
C. UTM utilizing a threat feed
D. SD-WAN utilizing IPSec

5B - Network Security Appliances

NO.7 A security engineer needs to configure an NGFW to minimize the impact of the increasing number of various traffic types during attacks.

Which of the following types of rules is the engineer the most likely to configure?

A. Signature-based
B. Behavioral-based
C. URL-based
D. Agent-based

5B - Network Security Appliances

NO.7 A security engineer needs to configure an NGFW to minimize the impact of the increasing number of various traffic types during attacks.

Which of the following types of rules is the engineer the most likely to configure?

A. Signature-based
B. Behavioral-based
C. URL-based
D. Agent-based

5B - Network Security Appliances

NO.8 A security engineer is installing an IPS to block signature-based attacks in the environment.

Which of the following modes will best accomplish this task?

A. Monitor

B. Sensor

C. Audit

D. Active

5B - Network Security Appliances

NO.8 A security engineer is **installing an IPS to block signature-based attacks** in the environment.

Which of the following modes will best accomplish this task?

A. Monitor

B. Sensor

C. Audit

D. Active

5B - Network Security Appliances

NO.9 A security analyst is investigating a workstation that is suspected of outbound communication to a command- and-control server. During the investigation, the analyst discovered that logs on the endpoint were deleted.

Which of the following logs would the analyst most likely look at next?

A. IPS

B. Firewall

C. ACL

D. Windows security

5B - Network Security Appliances

NO.9 A security analyst is investigating a workstation that is suspected of outbound communication to a command- and-control server. During the investigation, the analyst discovered that **logs on the endpoint were deleted.**

Which of the following logs would the analyst most likely look at next?

A. IPS

B. Firewall

C. ACL

D. Windows security

5B - Network Security Appliances

NO.10 A new vulnerability enables a type of malware that allows the unauthorized movement of data from a system.

Which of the following would detect this behavior?

A. Implementing encryption

B. Monitoring outbound traffic

C. Using default settings

D. Closing all open ports

5B - Network Security Appliances

NO.10 A new vulnerability enables a type of malware that allows the **unauthorized movement** of data from a system.

Which of the following would detect this behavior?

A. Implementing encryption

B. Monitoring outbound traffic

C. Using default settings

D. Closing all open ports

5B - Network Security Appliances

NO.11 A security analyst is assessing several company firewalls.

Which of the following tools would the analyst most likely use to generate custom packets to use during the assessment?

A. hping
B. Wireshark
C. PowerShell
D. netstat

5B - Network Security Appliances

NO.11 A security analyst is assessing several company firewalls.

Which of the following tools would the analyst most likely use to **generate custom packets** to use during the assessment?

A. hping
B. Wireshark
C. PowerShell
D. netstat

5B - Network Security Appliances

NO.12 An organization recently started hosting a new service that customers access through a **web portal**. A security engineer needs to add to the existing security devices a new solution to protect this new service.

Which of the following is the engineer most likely to deploy?

A. Layer 4 firewall

B. NGFW

C. WAF

D. UTM

5C - Secure Communications

5C - Secure Communications

NO.1 A security analyst scans a company's public network and discovers a host is running a remote desktop that can be used to access the production network. Which of the following changes should the security analyst recommend?

A. Changing the remote desktop port to a non-standard number
B. Setting up a VPN and placing the jump server inside the firewall
C. Using a proxy for web connections from the remote desktop server
D. Connecting the remote server to the domain and increasing the password length

5C - Secure Communications

NO.1 A security analyst scans a company's public network and discovers a host is running a remote desktop that can be used to access the production network. Which of the following changes should the security analyst recommend?

A. Changing the remote desktop port to a non-standard number
B. Setting up a VPN and placing the jump server inside the firewall
C. Using a proxy for web connections from the remote desktop server
D. Connecting the remote server to the domain and increasing the password length

5C - Secure Communications

NO.2 A company prevented direct access from the database administrators' workstations to the network segment that contains database servers.
Which of the following should a database administrator use to access the database servers?

A. Jump server
B. RADIUS
C. HSM
D. Load balancer

5C - Secure Communications

NO.2 A company prevented direct access from the database administrators' workstations to the network segment that contains database servers.
Which of the following should a database administrator use to access the database servers?

A. Jump server
B. RADIUS
C. HSM
D. Load balancer

5C - Secure Communications

NO.3 An engineer needs to find a solution that creates an added layer of security by preventing unauthorized access to internal company resources. Which of the following would be the best solution?

A. RDP server
B. Jump server
C. Proxy server
D. Hypervisor

5C - Secure Communications

NO.3 An engineer needs to find a solution that creates an added layer of security by preventing unauthorized access to internal company resources. Which of the following would be the best solution?

A. RDP server
B. Jump server
C. Proxy server
D. Hypervisor

5C - Secure Communications

NO.4 A vendor needs to remotely and securely transfer files from one server to another using the command line.

Which of the following protocols should be Implemented to allow for this type of access? (Select two).

A. SSH
B. SNMP
C. RDP
D. S/MIME
E. SMTP
F. SFTP

5C - Secure Communications

NO.4 A vendor needs to remotely and **securely transfer files** from one server to another using the command line.

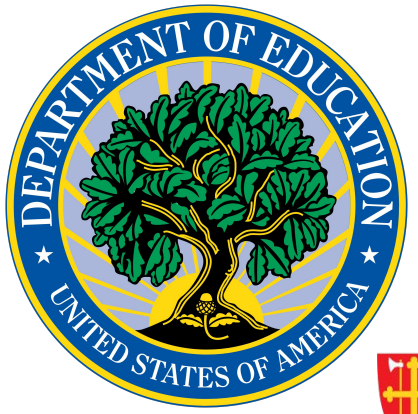
Which of the following protocols should be Implemented to allow for this type of access? (Select two).

A. SSH
B. SNMP
C. RDP
D. S/MIME
E. SMTP
F. SFTP

THANKS!

Any questions?

Our Graduates are Hired By



Google

Deloitte.

AT&T

ally
do it right.

DEN NORSKE KIRKE
Kirkepartner

Robinhood

VIZNET

COMCAST

INSPARK

ING BANK

proValus

SOCRadar®
Extension to Your SOC Team!

AGILIS
TECHNOLOGIES

Humana
Wellness

EQUANS

BBS

BGA
SECURITY

gravity
IT RESOURCES

GetMoneyGlobal

proximus

northramp

ease
LEARNING