

Lab Assignment & Solution



Cybersecurity Professional Program
Cyber Infrastructure and
Technology

Secure Network Architecture

CIT-10-LS2

Drawing a Secure Topology

Copyright © 1996-2020 HackerU Ltd.
All Rights Reserved.

Note: Solutions for the instructor are shown inside the green box.

Lab Objective

Acquire a better understanding of secure network architecture.

Lab Mission

Draw a diagram of a secure architecture for an organization.

Lab Duration

25–30 minutes

Requirements

- Basic understanding of secure network architecture.

Resources

- Environment & Tools
Web browser
- Links
<https://diagrams.net>

Textbook References

- Chapter 10: Secure Network Architecture
Section 1: Security Considerations
Section 2: Concepts & Technologies

Lab Task

Go to the diagrams.net website and create a drawing of a topology consisting of the following components:

- 1** Two firewalls (DMZ)
- 2** Three routers
- 3** Two switches
- 4** 20 workstations in four departments
- 5** Public web application server
- 6** Mail relay server
- 7** WAF – Web Application Firewall protects your web apps by enforcing a policy to filter, monitor, and block any HTTPS traffic to and from the web application.
- 8** SIEM server
- 9** Web server database
- 10** Honeypot
- 11** DLP

Compare your diagram with the rest of the class and discuss the considerations behind your architecture.

A router is placed at the intersection of each network to route packets to their destination.

A firewall is placed immediately after the router to inspect packets and filter incoming and outgoing traffic.

Since we cannot connect all workstations and servers directly to the router because of security reasons and since most routers do not have enough physical ports for the machine, we use switches to accomplish this task.

The workstations are placed in the LAN network behind all the security mechanisms, since they are meant to be part of the internal network.

The web application server is placed in the DMZ, since it needs to be accessed from the outside. A WAF is placed before it for added protection.

The mail relay is also placed in the DMZ since it also requires access from the outside.

The SIEM server will be the LAN network, segmented into separate subnets to be used by servers.

Honeypots are placed in strategic locations in the environment to create traps in places that hackers will often try to access.

