

EX 7: Secure Network Architecture

Aim:-

To understand the principles of secure network architecture design, learn and implement common network security concepts and protocols, understand a network's environment and potential threats.

PROBLEMS:-

Room completed (100%)

<name>.<vlan/sub-interface id>

Below is an example of adding a new virtual sub-interface and configuring its corresponding addressing.

In this example, we will use the open-source router: [VyOS](#)

```
vyos@vyos-rt1# set interfaces ethernet eth0 vif 10 description 'VLAN 10'
vyos@vyos-rt1# set interfaces ethernet eth0 vif 10 address '192.168.100.1/24'
```

If all went well and was appropriately configured, we should be able to route traffic between VLANs while keeping traffic tagged and isolated!

But are they really isolated? Physically, they are isolated, but because routes exist between them, there is no security boundary, and they are not necessarily isolated. As long as a route exists between two VLANs, any device can communicate between the two.

This brings us to our following two tasks, where we will discuss designing secure VLANs and introduce the concept of zoning.

Analyzing a VLAN Configuration

Apply what you learned to analyze a VLAN configuration given the output below.

▶ [Interface Configuration Snippet \(Click to view\)](#)

Answer the questions below

How many trunks are present in this configuration?

✓ Correct Answer

🔍 Hint


What is the VLAN tag ID for interface eth12?

✓ Correct Answer

🔍 Hint

Room completed (100%)

Restricted Zone



Security zones and access controls will physically direct how and where traffic goes. But how is it decided what resources users or devices have access to? Traffic rules are often governed by company security policy or compliance as equally as security controls that determine access permissions.

We've now established a system to approach designing VLANs, but how can we practically implement and enforce them? In the next task, we will cover several protocols and applications that can be used to implement and enforce VLANs.

Answer the questions below

From the above table, what zone would a user connecting to a public web server be in?

External

✓ Correct Answer

🔍 Hint

From the above table, what zone would a public web server be in?

DMZ

✓ Correct Answer

🔍 Hint

From the above table, what zone would a core domain controller be placed in?

Restricted

✓ Correct Answer

🔍 Hint

Room completed (100%)

In the next task, we will continue answering this question and look at how we may approach solutions for this problem.

Analyzing Packets and ACLs

Now that we understand the structure of an ACL and what it will look for in a packet, let's analyze a few packets and ACL policies to determine if they will be accepted or dropped.

Below is each packet and ACL policy required; answer the questions using the resources below.

▶ Packet #1 (Click to view)

▶ ACL Policy #1 (Click to view)

▶ Packet #2 (Click to view)

▶ ACL Policy #2 (Click to view)

Answer the questions below

According to the corresponding ACL policy, will the first packet result in a drop or accept?

accept

✓ Correct Answer

According to the corresponding ACL policy, will the second packet result in a drop or accept?

drop

✓ Correct Answer

Room completed (100%)

1. set zone-policy zone LAN from WAN firewall name lan-wan

2. set zone-policy zone WAN from LAN firewall name wan-lan

We should have our first zone-pairs defined and enforced now. To test our new configuration, we can attempt to send a `ping` command in both directions to ensure the `firewall` is dropping or accepting our ICMP packets.

Creating a Zone-Pair from Scratch

Now that you have an understanding of how to create a basic zone-pair policy, launch the static site attached to this task by pressing the green View **Site** button. Use the table below to fill in the blanks provided in the static site.

Source	Destination	Protocol	Action	Default Action
DMZ	LAN	HTTP	Accept	Drop
DMZ	WAN	-	-	Drop
LAN	DMZ	ICMP	Accept	Drop
WAN	DMZ	-	-	Drop

Common Name	Interface	Default Action
DMZ	eth0.10	Drop
LAN	eth0.20	Drop
WAN	eth0.30	Drop

Answer the questions below

What is the flag found after filling in all blanks on the static site?

THM{Mostly_53cure}

✓ Correct Answer

Room completed (100%)

Task 6 Validating Network Traffic

To begin this task, let's first start with a scenario. Your organization has proper zoning and routes in place. A zone-pair between the DMZ and LAN allows an HTTPS connection. Of course, the `firewall` should accept these connections... How else is Susie supposed to watch Facebook or your azure updates install?

In this scenario, let's say there is a threat actor that has landed an implant through phishing on a LAN machine. Assuming host defense mechanisms have failed, how can the implant be detected and monitored? If their beacon is using HTTPS through the DMZ. That will look like primarily legitimate traffic to your `firewall` and analysts.

To solve this issue, we must use SSL/TLS inspection to intercept HTTPS connections.

SSL/TLS Inspection

SSL/TLS inspection uses an **SSL proxy** to intercept protocols, including HTTP, POP3, SMTP, or other SSL/TLS encrypted traffic. Once intercepted, the `proxy` will decrypt the traffic and send it to be processed by a **UTM** (Unified Threat Management) platform. UTM solutions will employ deep SSL inspection, feeding the decrypted traffic from the `proxy` into other UTM services, including but not limited to web filters or **IPS** (Intrusion Prevention System), to process the information.

This solution may seem ideal, but what are the downsides? Some of you may have already noted that this requires an SSL proxy or **MITM** (Man-in-the-Middle). Even if a `firewall` or vendor has already implemented the solution, it will still act as a MITM between your devices and the outside world; what if it intercepts potentially plain-text passwords? A corporation must assess the pros and cons of this solution, dependent on its calculated risk. You could allow all applications that you know are safer to prevent potential cons, but this solution will still have disadvantages. For example, an advanced threat actor could route their traffic through a cloud provider or a trusted domain.

Answer the questions below

Does SSL inspection require a man-in-the-middle proxy? (Y/N)

Y

✓ Correct Answer

What platform processes data sent from an SSL proxy?

Unified Threat Management

✓ Correct Answer

Room completed (100%)

Answer the questions below

Where does DHCP snooping store leased IP addresses from untrusted hosts?

DHCP Binding Database

✓ Correct Answer

Will a switch drop or accept a DHCPRELEASE packet?

Drop

✓ Correct Answer

Does dynamic ARP inspection use the DHCP binding database? (Y/N)

Y

✓ Correct Answer

Dynamic ARP inspection will match an IP address and what other packet detail?

MAC Address

✓ Correct Answer

Task 8 ✓ Conclusion

Result: Hence the experiment was done successfully