|  |  |
| --- | --- |
| **Student Number:** | **Seat Number:** |
| **Student Name:** | **Module Group:** |



**Network Security**

Year 3 (2019/20), Semester 5

**SCHOOL OF INFOCOMM TECHNOLOGY**

Diploma in Information Security & Forensics

COMMON TEST

Date: 04 Jun 2019 (Tuesday)

Time: 1:30 pm - 3:00 pm

INSTRUCTIONS TO CANDIDATES:

1. Check carefully to ensure you are sitting for the correct paper.
2. Write your Student Number, Name, Module Group and Seat Number CLEARLY in the boxes provided above.
3. This paper consists of 13 pages including this cover page. Check carefully to make sure your set is complete.
4. There are FOUR questions. Answer ALL questions.

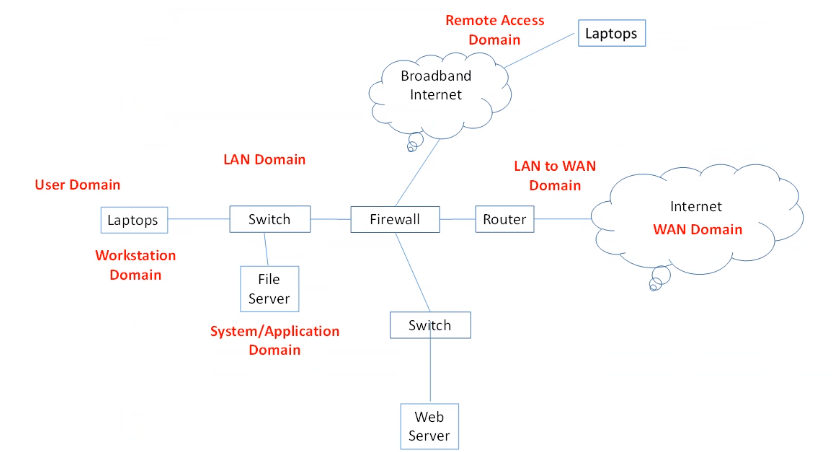
**GRADE**

**QUESTION 1** (25 marks)

TBG is a Singapore based tour agency and it has a LAN with Internet connection. The LAN consists of 20 laptops and a file server running Windows Server 2013. On the DMZ there is a web server. The LAN is protected by a firewall and remote access to the LAN is allowed.

1. Draw a well-labelled network diagram to illustrate the 7 domains of TBG’s IT Infrastructure.

(8 marks)



1. Briefly describe the security concerns in any THREE domains of TBG’s IT infrastructure and how network security can play a part in protecting these domains.

(6 marks)

User Domain: Actual Users like employees can be protected by segregating the network into different zones/subnets. Separate user domain from DMZ and Internet. Firewall policies can incorporate User IDs in allow/deny rules. Usage of access control to limit user access to the network.

Workstation Domain: Workstations can be assigned IP addresses on different subnets to limit their access to specific networks. Workstations contains sensitive user data.

System/Application Domain: File servers, AD servers, application servers contain organisational level data which are important to the organisation. Servers in this domain can be protected by network security measures like securing the access through active directory.

1. Network based firewalls may not be effective deterrents against insider threats. Explain how other forms of network security can be used to prevent insider threats.

(3 marks)

lDS/IPS can be deployed to detect insider attacks. An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Insider attacks within the LAN cannot be detected by firewall.

1. TBG is currently using Packet Filtering firewall to protect its network. Briefly describe ONE advantage and ONE disadvantage of Packet Filtering firewall.

(4 marks)

Advantage: It is cheap and easy to implement.

Disadvantage: Firewall rules are too simple and not able to protect against advanced attacks. Block packets based on port numbers where some evasive applications might use commonly open ports such 80 to avoid being detected.

1. You are a network administrator of TBG and you proposed to replace the Packet Filtering firewall with Next Generation Firewall. State TWO reasons to support your proposal.

(4 marks)

NGFW can block against advanced attacks. NGFW can be deployed to inspect and allow/deny packets based on the application that is transmitted.

NGFW also has capabilities to perform content inspection such as antivirus, file blocking.

A Palo Alto firewall has been set up with two zones: Trust-L3 and Untrust-L3 as shown in Figure 2. It is connected to the Internet via a router.

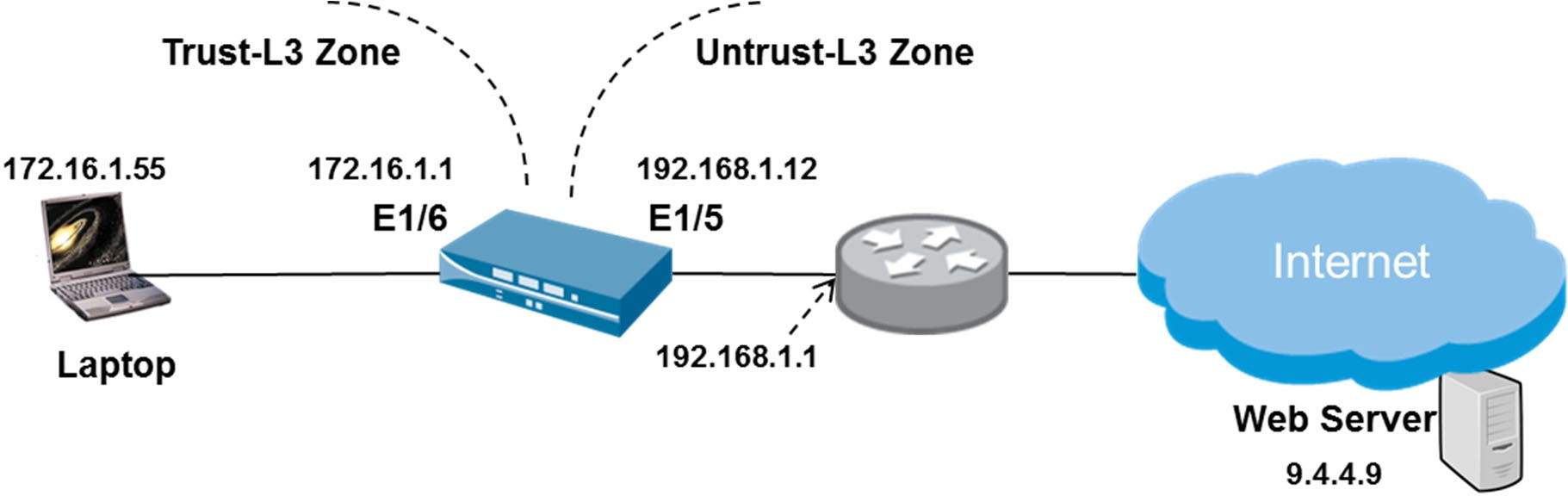


Figure 2: Palo Alto Firewall with Two Zones

1. Explain the concept of zones which is implemented in the above firewall configuration.

(2 marks)

Palo Alto Firewall separates network segments using zones. Firewall policies are configured based on zones. Interfaces are assigned to zones, and inspection policy is applied to traffic moving between the zones.

1. The firewall interfaces and NAT policies had been configured. The administrator has yet to configure any firewall policy, but implicit firewall rules already exist. Explain what happens if the end user tries to access the Web Server from the Laptop.

(3 marks)

The Laptop would not be able to access the Web server (1 mark)

The implicit policy denies inter-zone traffic. The Laptop is in the Trust-L3 zone but the Web Server is at the Untrust—L3 zone.

1. The layer 3 interfaces: E1/5 and E1/6, in Untrust-L3 zone and Trust-L3 zone respectively, were configured to respond to pings.

Explain the TWO configurations required on the firewall so that the Laptop is able to ping interface E1/5.

(4 marks)

Create a virtual router is to enable routing between the two interfaces: E1/5 and E1/6.

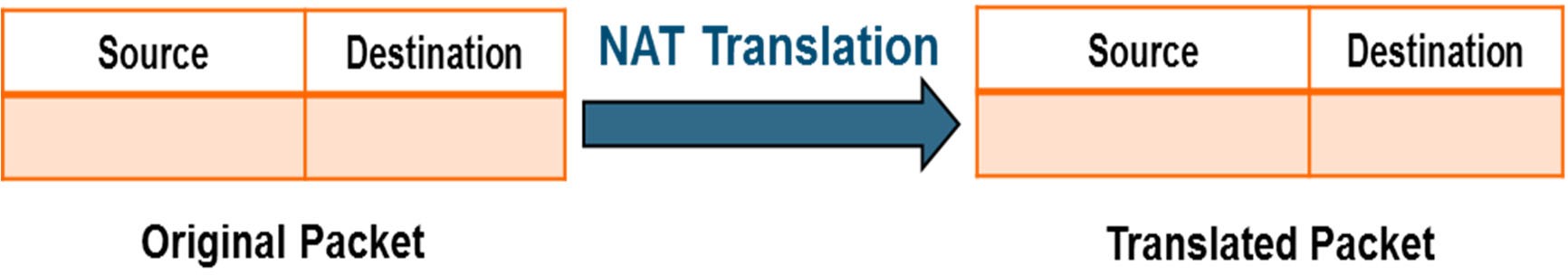
Security policy created to allow traffic from Trust-L3 Security Zone to Untrust—L3 Security Zone.

1. A Source NAT policy is created using “Dynamic IP and Port” type. A packet is sent from the Laptop to the Web Server.

Fill in the source and destination information for the original packet and the translated packet in Figure 2(d).

* + Local port number used by the browser on Laptop is 3333
  + Dynamic port number assigned by the NAT is 2222

(4 marks)



9.4.4.9:

80/443

192.168.1.12:

2222

172.16.55:

3333

9.4.4.9:

80/443

Figure 2(d): NAT Translation

1. The above policy is a Source NAT. What is Destination NAT meant for? Highlight how you would configure Destination NAT on the firewall.

(4 marks)

Destination NAT is used when an internal host needs to be accessible from the internet. Destination NAT translates a public IP address into a private IP address. For example, a web server in the DMZ with a private IP address, needs to be mapped to a public IP.

1. A firewall security policy configuration in Table 2(f) is applied to allow general Internet access.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Source** | | **Destination** | |  | | |
| **Name** | **Zone** | **Address** | **Zone** | **Address** | **Application** | **Service** | **Action** |
| General Internet | Trust-L3 | Any | Untrust- L3 | Any | DNS  Ping SSL  Web-browsing | Application  -default | Allow |
| Deny Outbound | Trust-L3 | Any | Untrust- L3 | Any | Any | Any | Deny |
| Deny  Inbound | Untrust-  L3 | Any | Trust-L3 | Any | Any | Any | Deny |

Table 2(f): Security Policy Configuration

1. Explain the purpose of “application-default” setting configured in the Service field.

(2 marks)

The service application—default option will set the security policy to allow the application on the standard/default ports associated with the application eg. for DNS, only port 53 is allowed.

[i.e. policy is configured to only match if applications with well-known port numbers are found on the expected port.]

1. For each of the network traffic listed in Table 2(f)(ii), fill in the actions taken by the firewall (Allow / Deny) and provide the corresponding explanation:

(6 marks)

|  |  |  |
| --- | --- | --- |
| **Network Traffic** | **Action** | **Explanation** |
| http://www.microsoft.com:8080 | Deny | Web-browsing is allowed on default port (port 80). Access to Microsoft’s homepage is using port 8080 which is not the default port of http. |
| https://www.google.com:443 | Allow | Google’s homepage is using https with default port 443 (ssl) |
| https://www.facebook.com:443 | Deny | Facebook base is recognized as App ID and it is not in the General Internet policy |

Table 2(f)(ii): Actions taken and Security Profile checked by firewall

You are the network security engineer of a small company and your task is to configure the firewall policy according to the following requirements:

* Deny the access to https://[www.instagram.com](http://www.instagram.com/) using App ID “Instagram”
* Allow the access to https:[//www.linkedin.com](http://www.linkedin.com/) using App ID “LinkedIn”
* Deny the posting function on LinkedIn website using App ID “LinkedIn-posting”
* Complete “Deny All Outbound” policy to deny all outgoing traffic

1. Complete Table 3(a) below to show the firewall security policy configuration.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Source** | | **Destination** | |  |  |
| **Name** | **Zone** | **Address** | **Zone** | **Address** | **Application** | **Action** |
| Deny-LinkedIn-Posting | Trust-L3 | Any | Untrust-L3 | Any | LinkedIn-Posting | Deny |
| Deny-Instagram | Trust-L3 | Any | Untrust-L3 | Any | Instagram | Deny |
| Allow-LinkedIn | Trust-L3 | Any | Untrust-L3 | Any | LinkedIn | Allow |
| Basic Access | Trust-L3 | Any | Untrust-L3 | Any | DNS  Ping SSL  Web-browsing | Allow |
| **Deny All Outbound** | Trust-L3 | Any | Untrust-L3 | Any | Any | Deny |

Table 3(a): Security Policy Configuration

(8 marks)

1. After the configuration and the changes are committed, you noticed that the posting function on LinkedIn is still allowed. Briefly explain why LinkedIn-posting cannot be denied. Explain what needs to be configured so that LinkedIn-posting can be denied.

(4 marks)

Decryption policy is required. LinkedIn uses protocol HTTPS, which is encrypted. The firewall, without the decryption policy is not able to decrypt the traffic, hence not able to have visibility to view the application shift from LinkedIn to LinkedIn-Posting.

1. If the order of “Basic Access” policy and “Deny All Outbound” policy is swapped, would you be able to access https:[//w](http://www.np.edu.sg/)w[w.n](http://www.np.edu.sg/)p[.edu.sg?](http://www.np.edu.sg/) Briefly explain the reason.

(3 marks)

https://www.np.edu.sg would not be able to access if the policy is swapped. Policies are evaluated from top down. If the Deny AII Outbound policy is on top, all outbound traffic would be denied.

1. Figure 3(d) shows one entry of a firewall Threat Report. The threat named “Win32.Conficker.C p2p” is logged 2125 times within one week.

Figure 3(d): Firewall Threat Report

Briefly describe how the security policy can be configured to block this threat.

(3 marks)

Configure anti-spyware security profile in Basic Access policy and select Action “Block”.

1. Figure 3(e) shows a File Blocking Profile configuration page on the firewall. Briefly explain the meaning of the actions by filling up Table 3(e) below.

(6 marks)

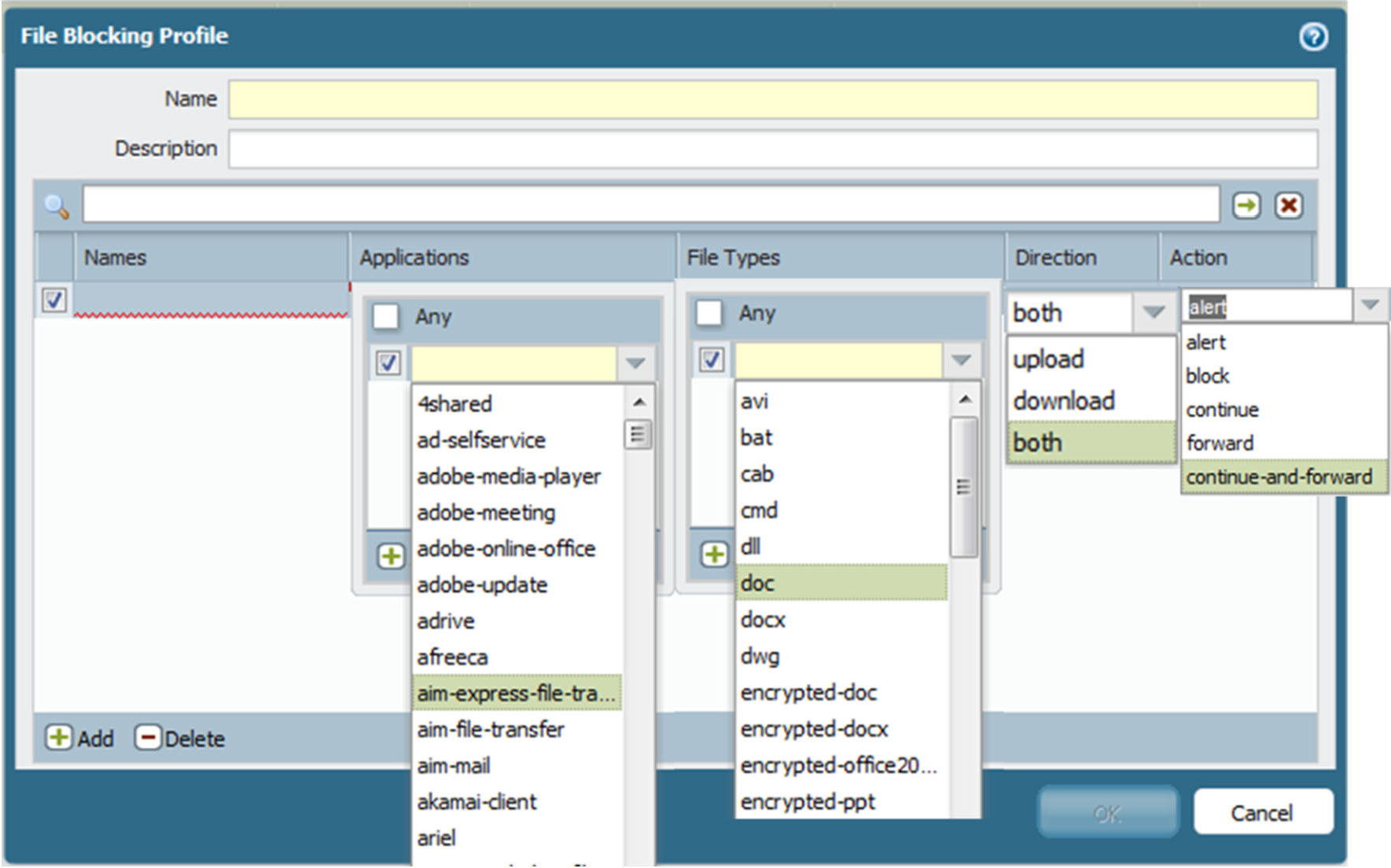


Figure 3(e): File Blocking Profile configuration

|  |  |
| --- | --- |
| **Actions** | **Explanation** |
| Alert | Allow the user to access the file but add an alert to the URL log |
| Block | Traffic is blocked, a Block log entry is generated, and a Response page is sent to the user’s browser if the traffic is  web-based |
| Continue – and  - Forward | Send a response page requiring the user to click Continue to  proceed and log the action. If the user continues, forward the  file to the WildFire cloud and log the action. |

Table 3(e): File Blocking Profile Actions

1. Company TWG’s existing network diagram is shown in Figure 4(a). Firewall 1 is a stateless packet filtering firewall deployed into the network 3 years ago.

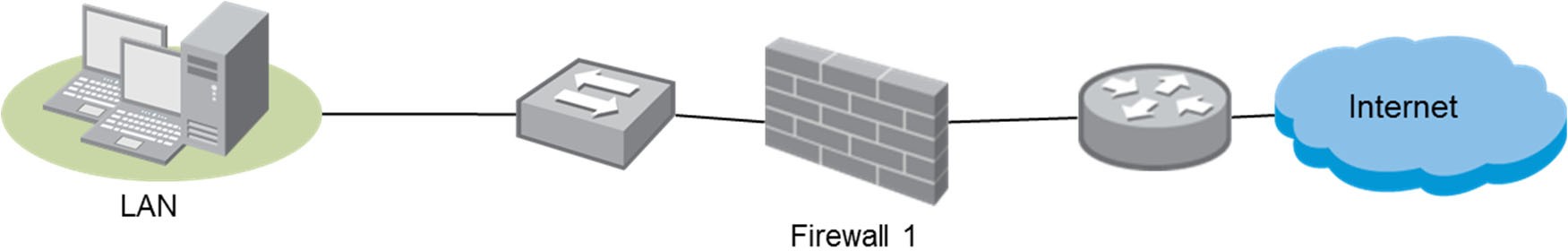


Figure 4(a): Network Diagram for TWG

* 1. Briefly explain Application ID, Content ID and User ID capabilities of Palo Alto Firewalls.

(4 marks)

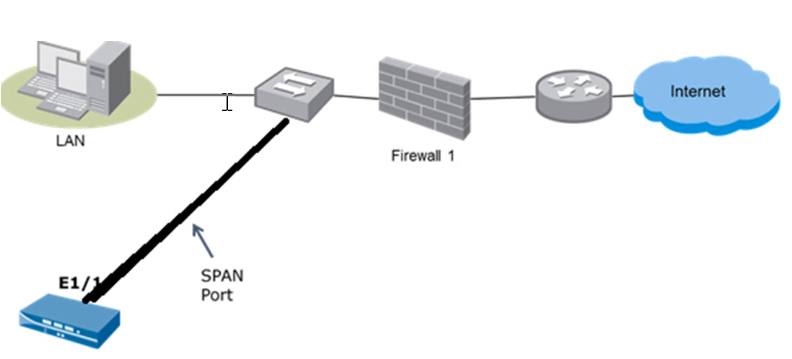
Application ID: Allow/Deny packets based on identifying the unique application header of each packet.

Content ID: Analysing the content of the packet eg an SMTP email, firewall is able to view the attachment in the email and block the attachment if the attachment is infected with virus.

User ID: Integration with Microsoft active directory so that security policies can allow/deny traffic based on specific users on the AD.

* 1. A firewall vendor provided Company TWG with a NGFW, Palo Alto Firewall for testing. The network security team decided to evaluate this new firewall before making a purchase to upgrade the existing firewall. Draw an updated network diagram to suggest a suitable placement of the firewall WITHOUT **inline** deployment.

(3 marks)



* 1. Refer to the connection suggested in **Q4(a)(ii)**, state ONE advantage and ONE disadvantage of this deployment mode.

(4 marks)

Advantage: No change required on current network topology.

Disadvantage: Firewall is not able to block any traffic.

* 1. Before replacing the packet filtering firewall, the network security team decided to do further evaluation by deploying the new firewall **inline** into its network without redesigning the current topology.

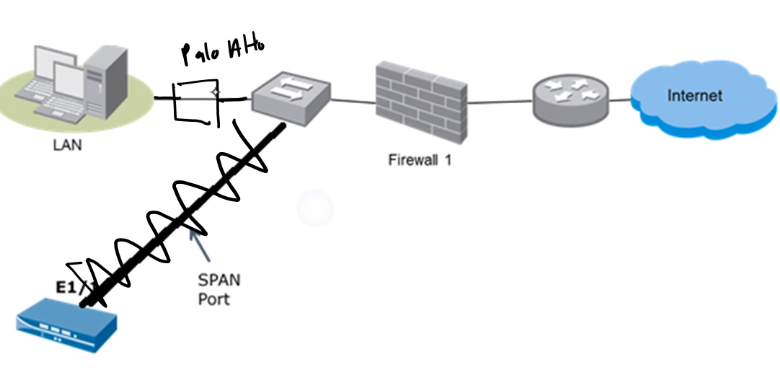
State the suitable deployment mode to meet this requirement.

(2 marks)

VirtualWire

* 1. Draw an updated network diagram to suggest a suitable placement of the firewall with **inline** deployment.

(3 marks)



1. You are setting up security profiles in your firewall policies. The following URL filtering profile is implemented on the firewall. Fill up Table 4(b)-2 below to indicate the expected results based on the information provided in Figure 4(b) and Table 4(b)-1. Provide explanation for the results indicated.

(10 marks)

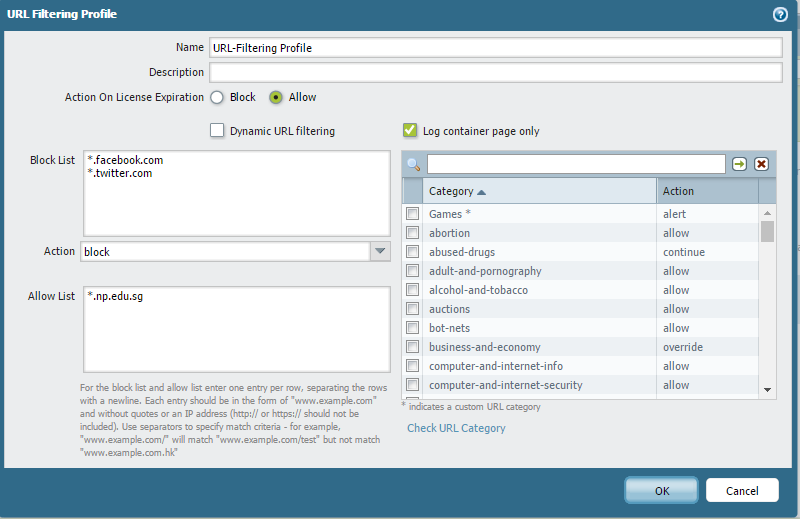


Figure 4(b): URL Filtering Profile

|  |  |
| --- | --- |
| **URL Categories** | **URLs** |
| Games\* | \*.maplestory.com  \*.dota.com |
| Abused-drugs | Pre-defined by Palo Alto |
| Business-and-economy | Pre-defined by Palo Alto |

Table 4(b)-1: URL categories

|  |  |  |
| --- | --- | --- |
| **Access to the following websites** | **Result (Allow or**  **Deny)** | **Explanation** |
| [www.facebook.com](http://www.facebook.com/) | Deny | Facebook is listed in block list, hence deny. |
| [www.np.edu.sg](http://www.np.edu.sg/) | Allow | NP website is listed in allow list,  hence allow. |
| [www.cheapdrugs.com](http://www.cheapdrugs.com/) | Allow | Action chosen is continue. User will  be directed to response page to click continue to proceed. |
| [www.dota.com](http://www.dota.com/) | Allow | User will be allowed to access website but an alert will be created to the URL log. |
| [www.businesstimes.com.sg](http://www.businesstimes.com.sg/) | Depends on user action | User will be directed to a response page and If user key in correct password, allow user to access and log will be created. |

Table 4(b)-2: Results for URL Filtering Profile

# \*\* End of Paper \*\*