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



**Network Security**

Year 2 (2017/18), Semester 4

# SCHOOL OF INFOCOMM TECHNOLOGY

Diploma in Information Technology Diploma in Information Security & Forensics

COMMON TEST

Date: 15 Dec 2017

Time: 8:30 am - 10:00 am

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 14 pages including this cover page. Check carefully to make sure your set is complete.
4. There are FIVE questions. Answer ALL questions.

**GRADE**

NS 2017/18 Semester 4 Page 1

There are FIVE questions. Answer **ALL** questions.

**QUESTION 1** – Multiple-Choice Questions (20 marks)

Indicate the correct answer in the box provided.

* 1. A border firewall cannot protect against which of the following?
     1. Flooding attacks.
     2. Insider attacking another internal target.
     3. Port scans.
     4. Unauthorized inbound service requests.
  2. Which of the following is NOT a traditional zone of risk in a common network?
     1. Department subnets
     2. A DMZ
     3. The Internet
     4. An extranet
  3. Based on the Seven Domains of a Typical IT Infrastructure, which location is completely NOT an appropriate location for firewall deployment?
     1. Between a LAN and a WAN.
     2. Between application servers and a WAN.
     3. Between workstations and users.
     4. Between remote access and a LAN.
  4. Which of the following is FALSE regarding firewall implicit and explicit rules?
     1. When traffic does not matched any user-defined policy, firewall will enforce implicit rules.
     2. Implicit rules do not generate traffic log entries.
     3. An explicit rule at the end of the user-defined policies will be processed after the implicit rules.
     4. None of the above.
  5. Which of the following is TRUE regarding Secure Socket Layer (SSL)?
     1. A client can use a server’s private key to encrypt the session key and then send the encrypted session key back to the server.
     2. The only usage of the Asymmetric encryption is to exchange the symmetric key.
     3. The session key is used by both the client and the server for bulk data encryption.
     4. All of the above.
  6. Which of the following is NOT a component of APP ID?
     1. Heuristics
     2. Application Signatures
     3. Protocol Decoders
     4. Encryption
  7. Which of the following is FALSE regarding APP ID filtering?
     1. It is application signature based.
     2. Multiple applications can be run from one web page.
     3. It manages HTTP and HTTPS traffic only.
     4. It is configured in security policies.
  8. Which of the following is NOT part of Content ID?
     1. Anti-virus
     2. Anti-spyware
     3. Application filtering
     4. Vulnerability
  9. Traffic going to a public IP address is being translated by Palo Alto firewall to an internal server’s private IP address. Which IP address should the security policy use as the Destination IP address in order to allow traffic to the server?
     1. The server’s private IP
     2. The server’s public IP
     3. The firewall’s gateway IP
     4. The firewall’s MGT IP
  10. In order to route traffic between layer 3 interfaces on the Palo Alto firewall, you need a:
      1. Virtual router
      2. VLAN
      3. Virtual wire
      4. Security profile

Company XYZ is considering of replacing its existing Stateless Packet Filtering Firewall with a Next Generation Firewall.

1. Briefly describe how Stateless Packet Filtering Firewall makes allow/deny decisions on incoming traffic.

(3 marks)

The allow/deny decisions are taken on packet by packet basis and there are not related to the previous allowed/denied packets

1. Briefly describe TWO disadvantages of Stateless Packet Filtering Firewall.

(4 marks)

* Packet Filtering Firewalls can work only on the Network Layer
* It does not support complex rule based models
* It’s also vulnerable to Spoofing in some cases

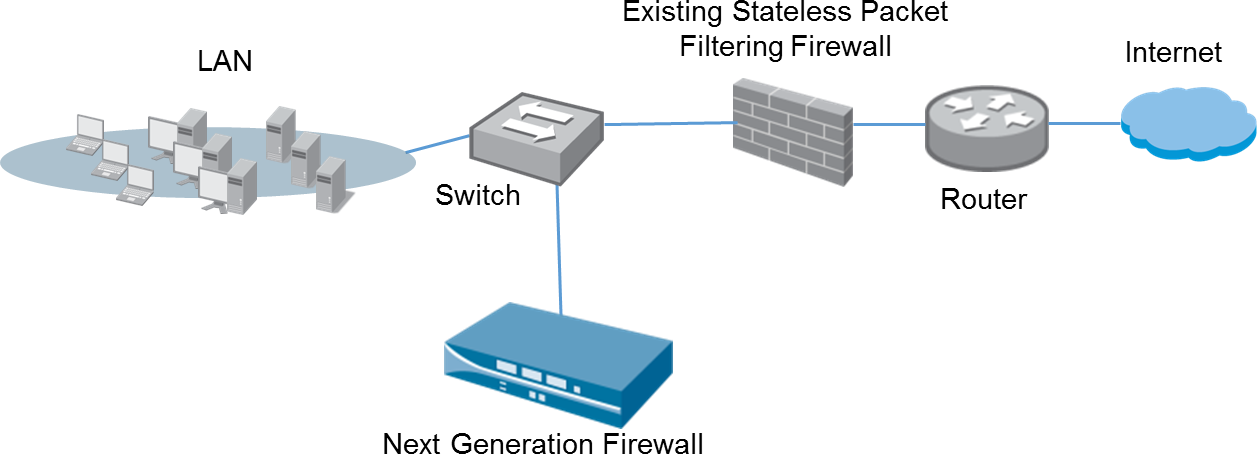
1. The Sales team of the Next Generation Firewall suggests to Company XYZ that the initial deployment option should follow the connection as shown in Figure 2(c).

Figure 2(c): Initial Deployment Option

* 1. Identify the deployment option and the capabilities of the Next Generation Firewall.

(3 marks)

Tap mode deployment.

Connect in this way is for the new firewall to identify applications running on the network for evaluation purpose

* 1. State ONE limitation of this connection.

(2 marks)

The firewall cannot block any traffic

1. You are the network security administrator of company XYZ and you want to deploy the Next Generation Firewall into the network as shown in Figure 2(d). You also need to ensure that the Head Quarter and Branch Office are able to communicate with each other, and they should both be able to access internet.

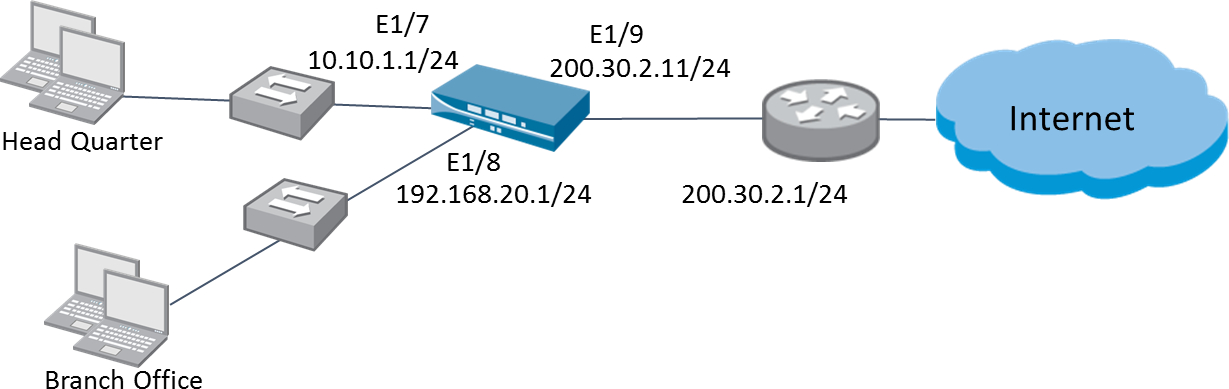


Figure 2(d): Firewall Deployment

* 1. Fill the table below to complete your configuration of a virtual router.

(4 marks)

|  |  |
| --- | --- |
| **Virtual Router -1** | |
| Interfaces | E1/7  E1/8  E1/9 |
| **Static Route** | |
| Destination | 0.0.0.0/0 |
| Next Hop | IP Address |
| Next Hop IP Address | 200.30.2.1/24 |

* 1. Briefly describe the steps required to allow computers from Head Quarter to ping the firewall interface E1/7. State the benefit of allowing this ping traffic.

(4 marks)

Configure interface Management Profile for interface E1/7 to allow ping.

Allowing ping to E1/7 is for troubleshooting purpose, user can test the

connectivity from their computer to the firewall interface.

**QUESTION 3** (20 marks)

You are a firewall administrator for GDT Pte Ltd. Your IT manager has requested you to implement firewall policies with the following requirements:

* Allow web access to [http://www.np.edu.sg](http://www.np.edu.sg/) and [https://www.google.com](https://www.google.com/)
* Deny all other outbound traffic
* Deny all inbound traffic

You may assume the following zone names:

* Trust Zone: GDT\_LAN
* Untrust Zone: Internet

1. Fill in the firewall policies below to fulfil the requirements:

(7 marks)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Source** | | **Destination** | |  | | |
| **Name** | **Zone** | **Address** | **Zone** | **Address** | **Application** | **Service** | **Action** |
| Allow web access | GDT\_LAN | Any | Internet | Any | DNS  SSL  Web-Browsing | Application  Default | Allow |
| Deny Outbound | GDT\_LAN | Any | Internet | Any | Any | Any | Deny |
| Deny Inbound | Internet | Any | GDT\_LAN | Any | Any | Any | Deny |

Table 3(a): Firewall Policies of GDT Pte Ltd.

1. Based on the policies implemented above, indicate and explain if the following user actions is/are allowed/denied when he performs the following at his desktop:

(6 marks)

|  |  |  |
| --- | --- | --- |
| **User action** | **(Allow/Deny)** | **Explanation** |
| (i) https:/[/www.d](http://www.dbs.com.sg/)b[s.com.sg](http://www.dbs.com.sg/) | Allow | Access to a normal website  is allowed. |
| (ii) https://map.google.com | Deny | App ID google-map need to  be allowed in the policy. |
| (iii) https:/[/www.t](http://www.twitter.com/)w[itter.com](http://www.twitter.com/) | Deny | App ID twitter need to be allowed in the policy. |

Table 3(b): Actions Taken and Security Profile Checked by Firewall

1. Give TWO examples of evasive application and describe their characteristics.

(4 marks)

Yahoo messenger, Bit torrent or any other valid applications.

(2 marks, 1 mark for each example)

Evasive applications can bypass a traditional stateful inspection firewall.

Evasive applications use tactics such as port hopping, non-standard ports,

SSL encryption and emulation to evade the firewall.

(2 marks)

1. Based on the policies applied in Q3(a), would GDT Pte Ltd be protected against evasive applications? Explain your answer.

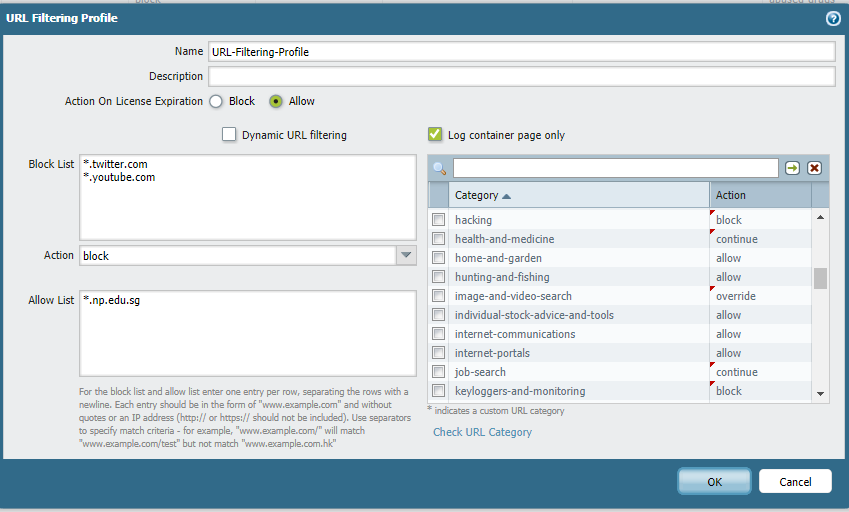
(3 marks)

Yes

(1 mark)

This is because Palo Alto firewall block by allowing/disallowing specific applications, not by the port number. Hence, evasive applications are not able to use tactics such as port hopping to bypass the firewall.

(2 marks)



**\*.hacking-lab.com**

1. The following URL filtering profile is implemented on the APP Pte Ltd’s firewall as indicated in Figure 4(a) and Table 4(a)-1.

(12 marks)

Figure 4(a): URL Filtering Profile

|  |  |
| --- | --- |
| **URL Categories** | **URLs** |
| Hacking | [www.hacking-lab.com](http://www.hacking-lab.com/) |
| Image-and-video-search | [www.findimage.com](http://www.findimage.com/) |
| Job-search | [www.jobstreet.com](http://www.jobstreet.com/) |
| Keyloggers-and-monitoring | [www.key-logger.com](http://www.key-logger.com/) |

Table 4(a)-1: URL categories

Fill up Table 4(a)-2 to indicate the expected results. Provide explanations for the results.

|  |  |  |
| --- | --- | --- |
| **Access to the**  **following websites** | **Result (Allow or Deny)** | **Explanation**  **(Write down the expected outcome which user will be prompted, if applicable)** |
| [www.youtube.com](http://www.youtube.com/) | Deny | Website is in the block list, hence deny |
| [www.np.edu.sg](http://www.np.edu.sg/) | Allow | Website is in the allow list, hence allow |
| [www.hacking-lab.com](http://www.hacking-lab.com/) | Allow | Website is in the allow list, hence allow |
| [www.key-logger.com](http://www.key-logger.com/) | Deny | Website is in the Keyloggers-and-monitoring URL Categories list that is block, hence deny |
| [www.findimage.com](http://www.findimage.com/) | Depend on user action | Website is in the Image-and-video-search URL Categories list that is on override, hence deny unless user know the password |
| [www.jobstreet.com](http://www.jobstreet.com/) | Allow | Website is in the Job-search URL Categories list that is on continue, hence allow when click continue |

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

1. After implementing the profile in Q4(a), you discovered that a particular hacking website [www.hacklah.com](http://www.hacklah.com/) is accessible by users in the LAN. Explain what you can do to block the website.

(2 marks)

Put www.hacklah.com in the block list

or

Create a custom URL category and place www.hacklah.com in the category and block the category.

1. You implemented the following file blocking profile on APP’s Palo Alto firewall:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name | | File-Blocking-Profile | | | |
| **Rule Name** | **Applications** | | **File Types** | **Direction** | **Action** |
| type-1 | any | | docx | upload | Continue- and-forward |
| type-2 | any | | xls | download | Alert |
| type-3 | any | | exe | both | Block |

Table 4(c)-1: File Blocking Profile

(6 marks)

Answer the following questions based on the file blocking profile implemented:

|  |  |  |
| --- | --- | --- |
| **User Action** | **Result (Allow or Block)** | **Explanation**  **(Write down the expected outcome which user will be prompted or log created if applicable)** |
| Goes to [http://tinyupload.com](http://tinyupload.com/) to download a file named customerinfo.xls | Allow | Allow the user to access the file but  add an alert to the URL log |
| Goes to [http://tinyupload.com](http://tinyupload.com/) to upload a file named customerdata.docx | Allow | 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. |
| Goes to [http://tinyupload.com](http://tinyupload.com/) to download a file named installFTP.exe | Block | Traffic is blocked. a Block log entry is  generated, and a Response page is  sent to the user's browser if the traffic  ls web-based |

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

1. Company ABC has a web server hosted in the DMZ zone providing HTTPS service to the clients. The network security team of the company has set up an inbound SSL inspection policy in their firewall in order to monitor the encrypted network traffic of this server.
   1. Briefly explain the process of the firewall’s inbound SSL inspection process when an external user is trying to request an SSL connection to the internal web server.

(6 marks)

* 1. When the firewall is performing SSL inspection, will the original packet data from the external user be changed when it reaches the internal server? Briefly explain your answer.

(3 marks)

1. A self-signed certificate can be created when a firewall is required to perform outbound SSL inspection.
   1. State TWO differences between self-signed certificates and Certificate Authority certificates.

(4 marks)

* 1. When configuring a self-signed certificate, the “Forward Trust Certificate” option must be selected as shown in Figure 5(b)(ii) below. Briefly explain why there is a need to include this option.

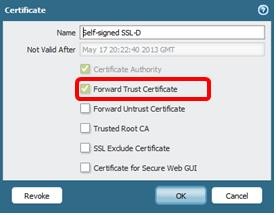


Figure 5(b)(ii): Self-signed Certificate

(3 marks)

1. “*Palo Alto firewall acts as a Forward Proxy (a “Man in the Middle” like approach) when performing outbound SSL decryption.”* Is this statement TRUE or FALSE? Briefly justify you answer.

(4 marks)

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