|  |  |
| --- | --- |
| **Network Security**  Diploma in CSF  Year 3 (2020/21) Semester 5 | Week 3 |
| Tutorial |
| **Firewall Technologies** | |

**Objectives**

At the end of this lesson, students should be able to understand functions of firewalls, types of filtering, and security zones.

**Activities**

1. Explain why firewall could not protect against insider attacks. List other threats that firewall could not protect against.

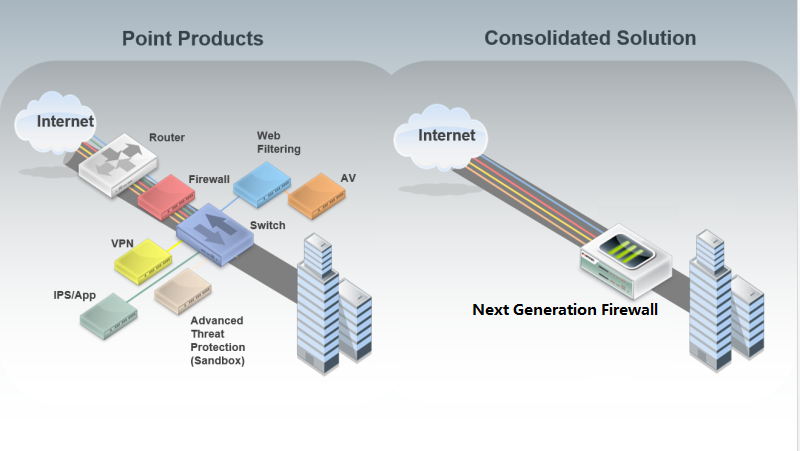
|  |
| --- |
| Firewall are placed at the border and it cannot view interior traffic, hence it would not be able to protect against insider attacks.  Other threats that firewall could not protect:  - Removable media  - Social engineering attack  - Physical attack  - Intrusion attack |

1. List some typical implicit security rules regarding intra-zone and inter-zone traffic found in most firewalls.

|  |
| --- |
| Typical security rules in most firewalls:  - Intra-zone traffic is usually allowed by default,  - Inter-zone traffic is usually denied by default, |

**Reflection**

Refer to the below diagram, discuss the disadvantages of the traditional security solutions in an organization.



|  |
| --- |
| • Traditional security solution in an organization consisted of all the point products.  • Stand-alone, non-integrated security appliances created gaps in security strategy.  • The mix of off-the-shelf systems and applications were difficult to deploy, manage and use.  • There was also high cost of ownership. |