# Assessment Task 3 – Performance Task

|  |  |  |  |
| --- | --- | --- | --- |
| **Student Name** |  | **Date** |  |
| **Unit being assessed** | VU23218 - Implement network security infrastructure for an organisation |
| **Instructions for Assessment Task 3** | Performance Tasks – Site-to-Site VPN and IDS.This assessment comprises one (1) scenario. This scenario provides an opportunity for the student to demonstrate the skills required for competence in this unit. The assessment task will include background information and all required resources.Your Assessor will use the “Assessor Checklist” to ensure all aspects of **Task 3: Performance Project** have been completed and mark the relevant rubric in the [Canvas](https://canvas.tastafe.tas.edu.au/) LMS.The completed Evidence Portfolio file required as part of **Task 3: Performance Project** must be submitted in the relevant submission area of the [Canvas](https://canvas.tastafe.tas.edu.au/) LMS. |

**Task 3.1: Practical**

Use the “Background” information and the step-by-step “Task Guide” (provided below) to complete this activity and ensure all the items listed in the “Assessor Checklist” have been completed.

**Background:**

As the new ICT Manager for the College of Art, Technology and Science (CATS), your role involves designing and preparing the network infrastructure. A key focus on the project is implementing Site-to-Site connection between Hobart and Launceston Campuses and increasing security features and threat visibility through IDS/IPS implementation.

Before committing to and implementing a new Gateway Security Devices (Netgate), you have decided to use Virtual Machines to test configuration and deployment of the required features.

Templates of the Virtual Machines[[1]](#footnote-2) have been supplied to you with basic installation and configurations already undertaken, including static IPs and hotsnames. There are 5 VMs in total:

* HBT\_FW
* HBT\_Deb
* LAU\_FW
* LAU\_Deb
* KALI

**Network Diagram:**



**IPs & VM Network Adapters**

|  |  |  |
| --- | --- | --- |
| **Hostname** | **Adapter Connected** | **IP Address** |
| **HBT\_FW** (pfSene) | NAT | 10.10.10.10/24 |
| BLUE (Custom) | 192.168.1.1/24 |
| **HBT\_Deb** (Debian) | BLUE(Custom) | 192.168.1.101/24 |
| **LAU\_FW** (pfSene) | NAT | 10.10.10.11/24 |
| RED (Custom) | 192.168.0.1/24 |
| **LAU\_Deb** (Debian) | RED (Custom) | 192.168.0.101/24 |
| **KALI** (Kali Linux) | NAT | 10.10.10.130 |

**Collecting evidence:**

Throughout this task the student will be required to take screenshots showcasing successful configuration and implementation of the required features. These screenshots will be compiled into an evidence portfolio (Task 3.2) that will be submitted.

Each screenshot the student takes, MUST contain a visible text file hosted on the Virtual Machine that you are being used, showcasing both the student’s name and the student number. The example image below showcases the requirements that must be included for a screenshot to be accepted:



1. Text editor application used clearly visible in taskbar/toolbar.
2. Text file location and name clearly visible in text editor.
3. Student first and last name and student ID clearly legible.

Screenshots that do not meet these requirements will not be accepted.

Using the supplied background information, as well as the network diagram and IP & VM Adapters table, complete all tasks in the task guide.

**Task guide:**

**NOTE:** Steps requiring screenshot/s to be taken will start with [3.2.x – Task name] in the task guide. The 3.2.x indicates where in Task 3.2 the screenshot will be used.

[ ]  Import both **HBT\_Deb** and **LAU\_Deb** Virtual Machines from Provided OVA files. Ensure that both VMs are connected to the appropriate adapters as shown in the Network Topology.

[ ]  Import both **HBT\_FW** and **LAU\_FW** Virtual Machines from provided OVA files. Ensure that both VMs are connected to the appropriate adapters as show in the Network Topology.

[ ]  Power on all Virtual Machines

[ ]  Configure IPsec Site-to-Site VPN between **HBT\_FW** and **LAU\_FW**. Use the following configurations

|  |  |  |
| --- | --- | --- |
| **Configuration** | **HBT\_FW** | **LAU\_FW** |
| **PHASE 1** |
| Description: | HBT to LAU VPN | LAU to HBT VPN |
| Key Exchange version | IKEv2 | IKEv2 |
| Internet Protocol: | IPv4 | IPv4 |
| Interface: | WAN | WAN |
| Remote Gateway: | 10.10.10.11 | 10.10.10.10 |
| Authentication Method: | Mutual PSK | Mutual PSK |
| My identifier: | My IP Address | My IP Address |
| Peer identifier: | Peer IP Address | Peer IP Address |
| Pre-Shared-Key:  | CATSVPNCreds | CATSVPNCreds |
| NOTE\*All unspecified options can be left as their default values |
| **PHASE 2** |
| Description:  | Phase 2 Tunnel | Phase 2 Tunnel |
| Local Network: | LAN Subnet | LAN Subnet |
| NAT/BINAT translation: | None | None  |
| Remote network:  | Network - 192.168.0.0/24 | Network - 192.168.1.0/24 |
| \*All unspecified options can be left as their default values |

[ ]  [ 3.2.1 – IPsec configuration] Take screenshot of the IPsec Phase 1 and Phase 2 tunnel on both **HBT\_FW** and **LAU\_FW**. See Evidence portfolio for example.

[ ]  For each pfSense Firewall, configure an IPsec firewall rule to allow the two sites to communicate with each other. Use the below configuration:

|  |  |  |
| --- | --- | --- |
| **Configuration** | **HBT\_FW** | **LAU\_FW** |
| **Action:**  | Pass | Pass |
| **Interface:**  | IPsec | IPsec |
| **Address Family:**  | IPv4 | IPv4 |
| **Protocol:**  | Any | Any |
| **Source:**  | Network – 192.168.1.0/24 | Network – 192.168.0.0/24 |
| **Destination:**  | Network – 192.168.0.0/24 | Network – 192.168.1.0/24 |
| **Log:**  | Checked | Checked |

Give your Firewall Rule a sensible description.

[ ]  [ 3.2.2 – Firewall rule] Take screenshot of the IPsec Firewall rule for both **HBT\_FW** and **LAU\_FW**. See Evidence portfolio for example.

[ ]  Ping from **HBT\_Deb** to **LAU-Deb** to confirm Site-to-Site VPN is functional

[ ]  [ 3.2.3 – Site-to-Site Ping] Take a screenshot of the ping command and results. See Evidence portfolio for example.

[ ]  [3.2.4 – IPsec Status] Take screenshots of the IPsec status showcasing active IPsec tunnels on both **HBT\_FW** and **LAU\_FW**. See Evidence portfolio for example.

**NOTE**: Once Site-To-Site VPN has been configured and tested, and all required screenshots have been gathered, **LAU\_FW** and **LAU\_Deb** VMs can be shut down.

[ ]  Install **Snort** on **HBT\_FW** using the Package Manager

[ ]  Configure **Snort** Global settings as follows:

* Enable Snort GPLv2: **Checked**
* Enable ET Open: **Checked**
* Enable OpenAppID: **Checked**
* Enable AppID Open Text Rules: **Checked**
* Enable FEODO Tracker Botnet C2 IP Rules: **Checked**
* Update Interval: **12 hours**
* Update Start Time: **00:00**
* Hide Deprecated Rules Categories: **Checked**
* Remove Blocked Hosts Interval: **1 DAY**
* Keep Snort Settings After Deinstall: Checked
* Startup/Shutdown Logging

[ ]  Update Snort Rule Sets

[ ]  Create Snort interface where the traffic on the WAN interface will be inspected. Enable the Snort Interface

[ ]  Enable all WAN categories on the Snort interface:

[ ]  Import **Kali** Virtual Machine from provided OVA file. Ensure that **Kali** VM is connected to NAT adapter. Power on Kali **VM**.

[ ]  From **Kali**, initiate a nmap scan targeting the WAN interface of the **HBT\_FW** VM. Use the following parameters:

 Nmap -sV-sC -Pn 10.10.10.10

[ ]  [3.2.5 – Nmap scan] Take a screenshot of the Nmap command and the results. See Evidence portfolio for example.

[ ]  On **HBT\_FW**, view Snort alerts.

[ ]  [3.2.6 – IDS alerts] Take a screenshot of the Snort alerts that have been generated. See Evidence portfolio 3.2.6 for example.

Once all tasks have been completed correctly, the student notifies their Assessor, ready to be assessed.

**Assessor Checklist (Task 3: Performance Project)**

TasTAFE Assessor will verify the student has completed all required tasks and their submitted evidence portfolio indicates successful configuration of the required features and the following have been completed.

|  |  |
| --- | --- |
| [ ]  | 1. IPsec tunnels configured to enable Site-to-Site VPN connection. IPsec tunnel utilises encryption to ensure data confidentiality, and is authenticated using a Pre-shared Key
 |
| [ ]  | 1. Zone based configuration is employed to create a firewall rule that only applies to IPsec zone. Firewall rule allows only required or approved traffic to pass between Hobart and Launceston over VPN tunnel. All other traffic is dropped to secure internal network.
 |
| [ ]  | 1. Site-to-Site VPN tunnel is tested and proven to be functional. ICMP packet can be sent by one client located in one site and received by a client located in the other site.
 |
| [ ]  | 1. Status of VPN tunnels shown to be “Connected” indicating that both IPsec Phase 1 and IPsec Phase 2 and their corresponding configuration was successful.
 |
| [ ]  | 1. Nmap scan is initiated using the correct parameters. Nmap scan is targeting external interface of HBT\_FW.
 |
|  | 1. Snort has been implemented and configured to monitor WAN interface for malicious traffic based on signatures. Alerts are created as a result of Nmap scan targeting WAN interface of HBT\_FW.
 |

***Note:***

*Should an* **Incomplete** *result be recorded for this task; details of the areas that require rectification (or a re-submission plan) will be entered in the Comments section in the submission area of the* [*Canvas*](https://canvas.tastafe.tas.edu.au/) *LMS.*

**Task 3.2 Evidence Portfolio**

Use the following section as a template for to create your Evidence Portfolio.

Replace the sample images with the screenshots you have captured throughout the task. Descriptions (Text in blue) need to be given for some images as well.

# Task 3.2: Evidence Portfolio

* + 1. **– IPsec Configuration**

HBT\_FW

Description: Give a brief description of what the parameters used to configure the IPsec tunnels

LAU\_FW

Description: Give a brief description of what the parameters used to configure the IPsec tunnels

* + 1. **– IPsec Firewall Rule**

HBT\_FW

Description: Give a brief description outlining the function of the firewall rule created for the IPsec tunnel

LAU\_FW

Description: Give a brief description outlining the function of the firewall rule created for the IPsec tunnel

* + 1. **Site-to-Site Ping**

HBT\_FW

LAU\_FW

Description: Give a brief description demonstrating Site-to-Site Ping

* + 1. **IPsec Status**

HBT\_FW

LAU\_FW

Description: Give a brief description outlining the IPsec tunnel Status

* + 1. **Nmap Scan**

Kali

Description: Give a brief description outlining the Nmap Scan

* + 1. IDS alerts

HBT\_FW

Description: Give a brief description outlining the IDS Alerts

Upload the completed Evidence Portfolio file in the relevant submission area of the [Canvas](https://canvas.tastafe.tas.edu.au/)

1. All VMs can be downloaded from either Teams or Network file share. [↑](#footnote-ref-2)