|  |
| --- |
|  |
| Helpyou Mortgage Company |
|  |

|  |
| --- |
| Thong Thao  Student ID: 474587265 |

**Content**

[Part 1: Remote access via a secure Site-to-Site VPN tunnel 2](#_Toc167704210)

[Part 2: Implement DHCP services on the LANs of Brisbane and Cairns 9](#_Toc167704211)

[Part 3: Implement integrated ADDS services and DNS services on the LANs of Brisbane and Cairns 13](#_Toc167704212)

[Part 4: Implement DFS, FSRM, Desktop Management, Anti-Virus Software Deployment on the LANs of Brisbane and Cairns 21](#_Toc167704213)

[Part 5: Install a WSUS server and Implement interoperability between Linux and Windows 31](#_Toc167704214)

[Part 6: Install and Configure VoIP services on the LANs of Brisbane and Cairns 37](#_Toc167704215)

[Part 7: Implement Videoconferencing services on the LANs of Brisbane and Cairns 40](#_Toc167704216)

[Part 8: Install and configure a network management software on the LANs of Brisbane and Cairns 43](#_Toc167704217)

[Part 9: Implement Ongoing Monitoring of Network security 48](#_Toc167704218)

[Part 10: Troubleshooting report 53](#_Toc167704219)

[Reference 60](#_Toc167704220)

# Part 1: Remote access via a secure Site-to-Site VPN tunnel

1. Prepare the work site as per legislative and WHS requirements.

Preparing the work site as per legislative and WHS requirements involves the following:

* Privacy Act 1988: Protect the personal information of employees and clients by implementing appropriate security measures and obtaining consent for data collection and use.
* Copyright Act 1968: Respect intellectual property rights and obtain necessary licenses for using copyrighted materials, such as software or media files.
* Workplace Bullying and Harassment Policy: Maintain a respectful and professional environment by preventing and addressing any instances of harassment or bullying.
* Electrical Safety Regulation 2013: Ensure electrical equipment is properly installed, maintained, and used safely to prevent electrical hazards.
* Ergonomic Principles: Arrange workstations, equipment, and furniture to minimise physical strain and promote good posture.

1. Summarise a table of IP addresses, netmasks and default gateways (where applicable)

|  |  |  |  |
| --- | --- | --- | --- |
| **Device** | **IP Address** | **Netmask** | **Default Gateway** |
| Helpyou-bne-fw (Firewall) | 10.0.0.254 | 255.255.255.0 |  |
| Brisbane WAN | 172.101.10.135 | 255.255.255.0 |  |
| Helpyou-cns-fw (Firewall) | 192.168.0.254 | 255.255.255.0 |  |
| Cairns WAN | 172.101.10.136 | 255.255.255.0 |  |

1. Install and configure servers, routers, switches or other devices to provide Site-to-Site VPN service.

* VPN Brisbane to Cairns

A screenshot of a computer

Description automatically generated

Figure 1 VPN Configuration of Brisbane Firewall

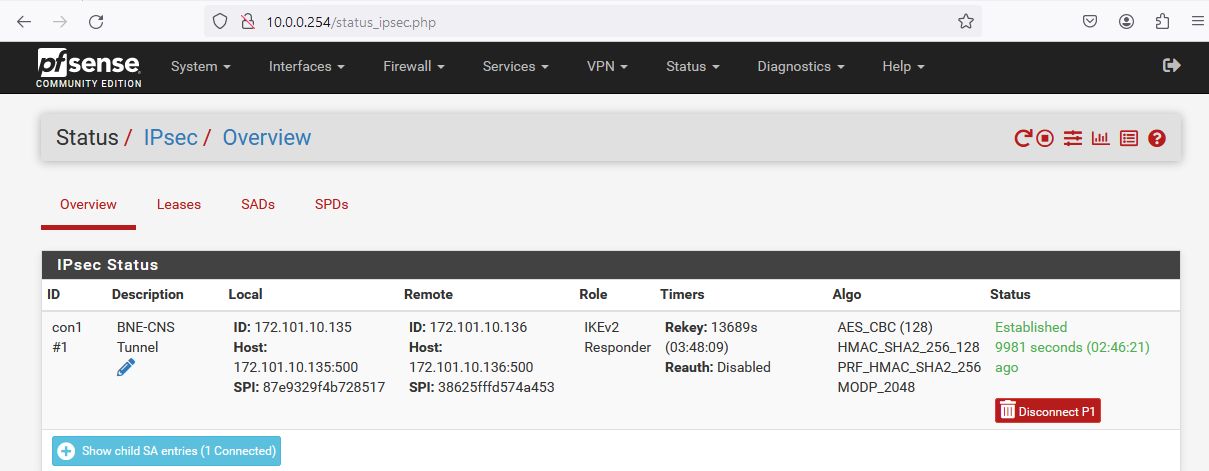


Figure 2 VPN Connection Status of Brisbane Firewall

* VPN Cairns to Brisbane

A screenshot of a computer

Description automatically generated

Figure 3 VPN Configuration of Cairns Firewall

A screenshot of a computer

Description automatically generated

Figure 4 VPN Connection Status of Cairns Firewall

1. Implement NAT functionality in your LAN’s connection to the ISP

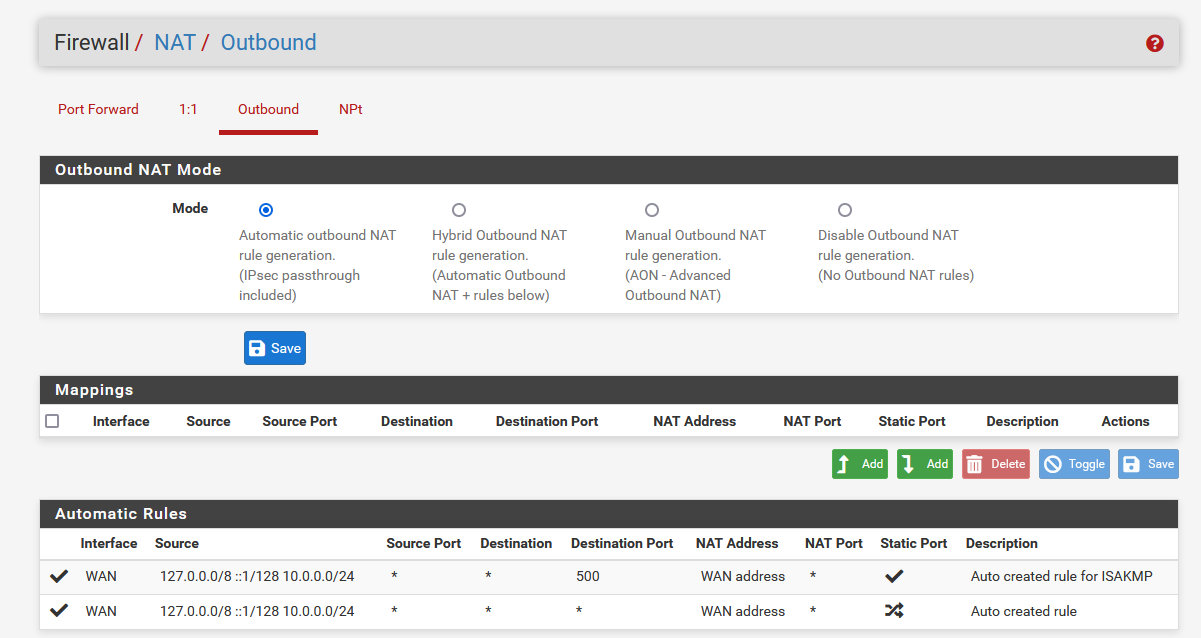


Figure 5 Default NAT Outbound

1. Implement a Firewall between your LAN and the ISP on both Brisbane LAN and Cairns LAN

* Brisbane Firewall

A screenshot of a computer

Description automatically generated

Figure 6 Brisbane Firewall (pfSense)

* Cairns Firewall

A screenshot of a computer

Description automatically generated

Figure 7 Cairns Firewall (pfSense)

1. Configure security policies on the firewall to protect the LAN from the ISP side

A screenshot of a computer

Description automatically generated

Figure 8 WAN Rules of the Firewall

1. Troubleshoot and verify that the network is working as expected

* Brisbane Client ping to Cairns DC Server

A screenshot of a computer

Description automatically generated

Figure 9 Test ping from Brisbane Client to Cairns Server IP

* Cairns Client ping to Brisbane DC Server

A screenshot of a computer

Description automatically generated

Figure 10 Test ping from Cairns Client to Brisbane Server IP

1. Demonstrate to the teacher that you can configure a proxy server and take screenshots of the proxy server configuration and screenshots of proxy client configuration. Briefly describe what is proxy in writing format.

pfSense Firewall Proxy Server

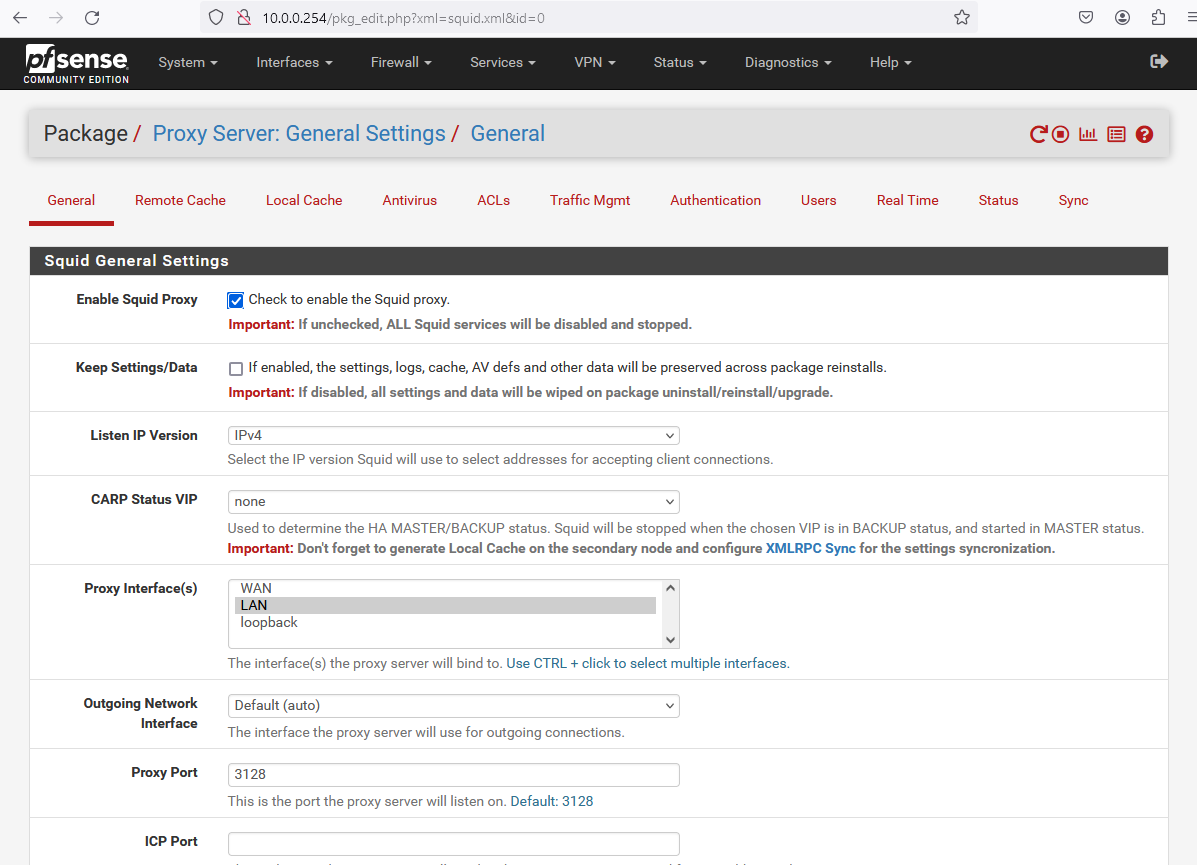


Figure 11 Brisbane pfSense Proxy

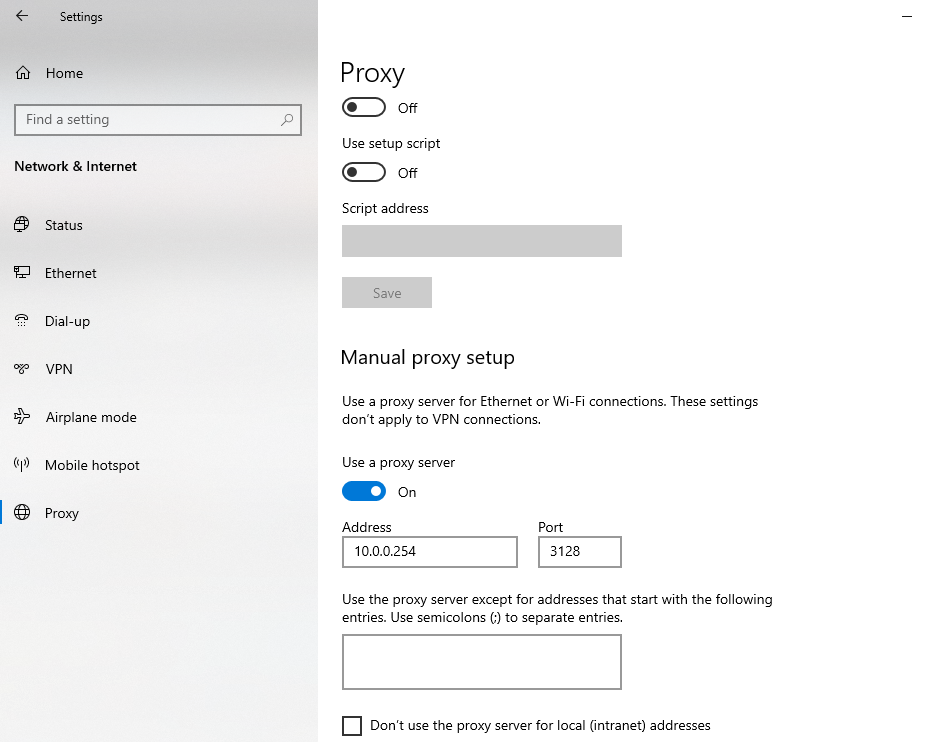


Figure 12 Client Proxy Setup

A **proxy** server is a gateway that anonymously passes data between users and the internet. The proxy itself could be a computer system or a router. All devices connected to the internet have an internet protocol (IP) address. This address is how a device is recognized on the internet, and it plays a role in how proxy servers work.

1. Briefly describe in writing what are the steps to configure this firewall. Briefly describe what firewall applications are.

To install and configure the firewall to provide a Site-to-Site VPN service between the Brisbane and Cairns LANs using pfSense firewall, follow these steps:

* Enabling VPN capabilities on the pfSense firewalls
* Configuring VPN parameters like encryption, authentication, and key exchange protocols (IPsec)
* Defining the remote VPN peer (other site's public IP)
* Setting up interesting traffic to be encrypted and sent over the VPN tunnel
* Allow Firewall Rule to IPsec and WAN to both Brisbane and Cairns.

**Firewall** applications are software solutions designed to monitor and control incoming and outgoing network traffic based on predefined security rules. They act as a barrier between trusted and untrusted networks, protecting internal resources from unauthorized access and potential threats.

1. Briefly describe what VPN is in writing format.

A Virtual Private Network (VPN) is a secure and encrypted connection that extends a private network across a public network, such as the internet. It creates a secure tunnel between two or more devices or networks, allowing them to communicate as if they were directly connected to the same private network.

1. You need to demonstrate that the part is successfully completed to your instructor. Obtain a written sign-off.

Date: 21/05/2024

Prepared by: Thong Thao – Senior System Administrator

**Subject**: Sign-off for Implementing a Site-to-Site VPN Tunnel between Brisbane and Cairns

Dear Frans De Fong,

I have successfully implemented a Site-to-Site VPN tunnel between the Brisbane and Cairns LANs using pfSense firewalls, allowing secure communication between the two sites over the internet. The key steps involved were:

**Preparing the Work Environment**

I ensured compliance with relevant legislative requirements like the Privacy Act 1988, Copyright Act 1968, Workplace Bullying and Harassment Policy, Electrical Safety Regulation 2013, and Ergonomic Principles by implementing appropriate security measures, respecting intellectual property rights, maintaining a respectful work environment, ensuring electrical safety, and promoting good ergonomics.

**Configuring Network Devices**

I configured the pfSense firewalls at both Brisbane and Cairns sites to establish the VPN tunnel over the internet connections provided by the ISPs. This included enabling VPN capabilities, setting up encryption (IPsec) and authentication protocols, defining the remote VPN peer, and specifying the interesting traffic (internal network ranges) to be encrypted and sent over the VPN tunnel.

**Implementing NAT and Firewall**

I implemented NAT (Network Address Translation) functionality on the LAN connections to the ISPs at both sites, allowing internal devices to access the internet while hiding their private IP addresses behind the firewall's public IP. I also implemented firewalls between the LANs and ISPs using pfSense, configuring security policies to protect the LANs from the ISP side.

**Testing and Verification**

To verify the network's functionality, I performed successful ping tests from clients in the Brisbane LAN to servers in the Cairns data centre, and vice versa, confirming that the Site-to-Site VPN tunnel was operational and allowing secure communication between the two sites.

Sign-off.

Signed: Date:

# Part 2: Implement DHCP services on the LANs of Brisbane and Cairns

1. Summarise a table of IP addresses, netmasks and default gateways (where applicable) for the DHCP servers

|  |  |  |  |
| --- | --- | --- | --- |
| **Device** | **IP Address** | **Netmask** | **Default Gateway** |
| Helpyou-bne-fw (Firewall) | 10.0.0.254 | 255.255.255.0 |  |
| Brisbane LAN Devices | 10.0.0.10-10.0.0.100 | 255.255.255.0 | 10.0.0.254 |
| Helpyou-cns-fw (Firewall) | 192.168.0.254 | 255.255.255.0 |  |
| Cairns LAN Devices | 192.168.0.10-192.168.0.100 | 255.255.255.0 | 192.168.0.254 |

1. Install and configure DHCP servers to provide the DHCP services for Brisbane and Cairns LANs.

* Brisbane DHCP Servers

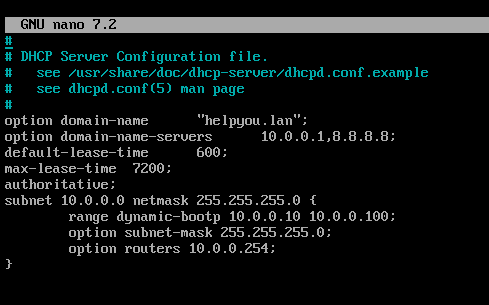


Figure 13 Brisbane DHCP Server Configuration

A screenshot of a computer

Description automatically generated

Figure 14 Brisbane DHCP Server is active

* Cairns DHCP Server

A screenshot of a computer

Description automatically generated

Figure 15 Cairns DHCP Server Configuration

A screenshot of a computer

Description automatically generated

Figure 16 Cairns DHCP Server is active

1. Confirm that the end devices in each LAN successfully obtain IP addresses from the corresponding DHCP server automatically

* Brisbane Client

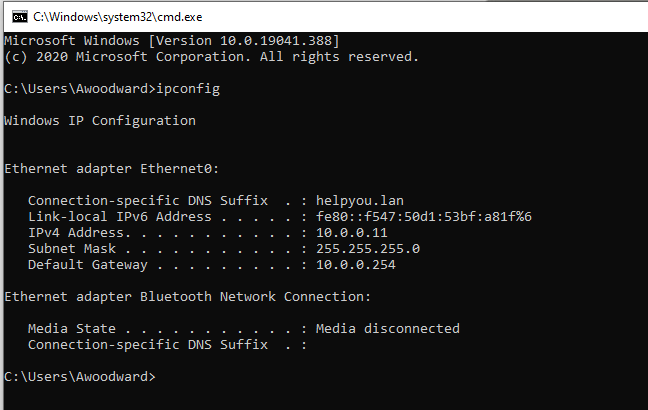


Figure 17 Brisbane Client PC has successfully obtained IP from the DCHP Server

* Cairns Client

A computer screen shot of a black screen

Description automatically generated

Figure 18 Cairns Client PC has successfully obtained IP from the DCHP Server

1. You need to demonstrate that the part is successfully completed to your instructor. Describe orally what this part is and how you implement it. Obtain a written sign-off.

Date: 21/05/2024

Prepared by: Thong Thao – Senior System Administrator

**Subject**: Sign-off for Implementing DHCP Services Brisbane and Cairns

Dear Frans De Oude,

I have implemented DHCP (Dynamic Host Configuration Protocol) services on the LANs of Brisbane and Cairns offices. DHCP automatically assigns IP addresses, subnet masks, and default gateways to devices on a network, eliminating the need for manual configuration.

**Brisbane DHCP Server**

For the Brisbane LAN, I configured a DHCP server to assign IP addresses in the range of 10.0.0.10 to 10.0.0.100, with a subnet mask of 255.255.255.0 and a default gateway of 10.0.0.254 (the firewall IP). The DHCP server is active and running, as shown in Figures 13 and 14 of the report.

I confirmed that a client device on the Brisbane LAN successfully obtained an IP address from the DHCP server, as demonstrated in Figure 17.

**Cairns DHCP Server**

Similarly, for the Cairns LAN, I configured a DHCP server to assign IP addresses in the range of 192.168.0.10 to 192.168.0.100, with a subnet mask of 255.255.255.0 and a default gateway of 192.168.0.254 (the firewall IP). The DHCP server is active, as shown in Figures 15 and 16.

I verified that a client device on the Cairns LAN successfully obtained an IP address from the DHCP server, as illustrated in Figure 18.

Sign-off.

Signed: Date:

# Part 3: Implement integrated ADDS services and DNS services on the LANs of Brisbane and Cairns

1. Summarise a table of IP addresses, netmasks and default gateways (where applicable) for the DC servers

|  |  |  |  |
| --- | --- | --- | --- |
| **Server** | **IP Address** | **Netmask** | **Default Gateway** |
| helpyou-bne-dc | 10.0.0.1 | 255.255.255.0 | 10.0.0.254 |
| helpyou-cns-dc | 192.168.0.1 | 255.255.255.0 | 192.168.0.254 |

1. Install and configure Domain Controller servers to provide the ADDS services for Brisbane and Cairns LANs. Compare and keep the time zone settings on the two DCs to be consistent with each other to make sure NTP is used for time synchronisation. Please describe what is NTP.

* Brisbane Domain Controller

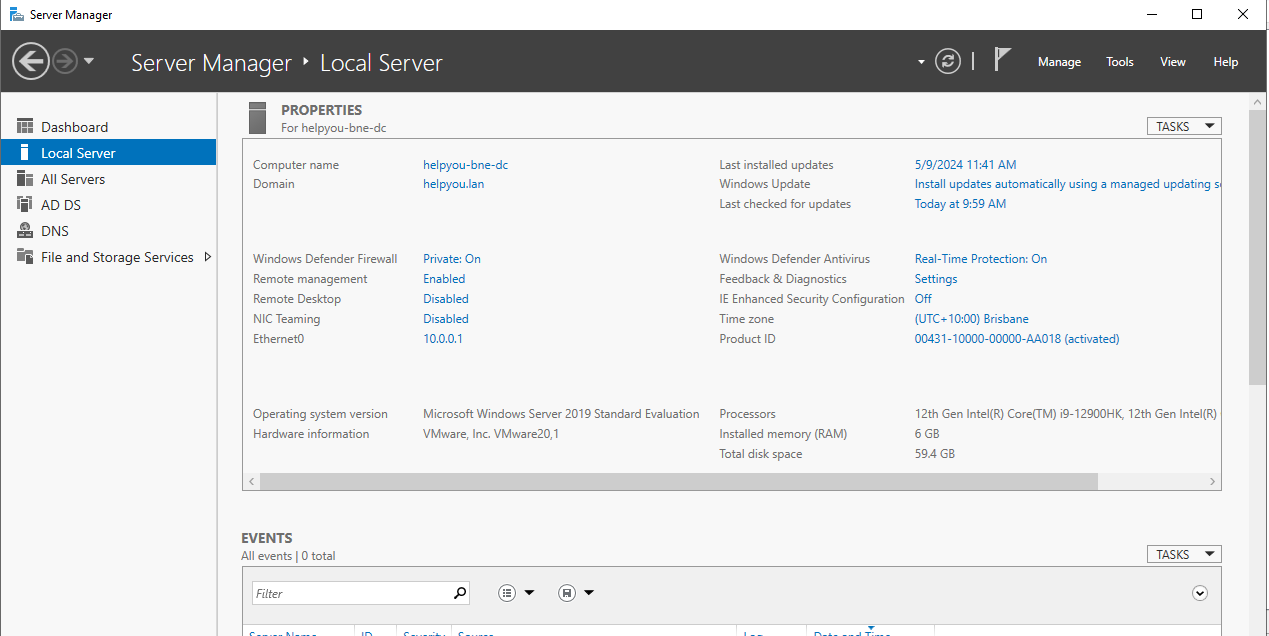


Figure 19 Brisbane Domain Controller

* Cairns Domain Controller

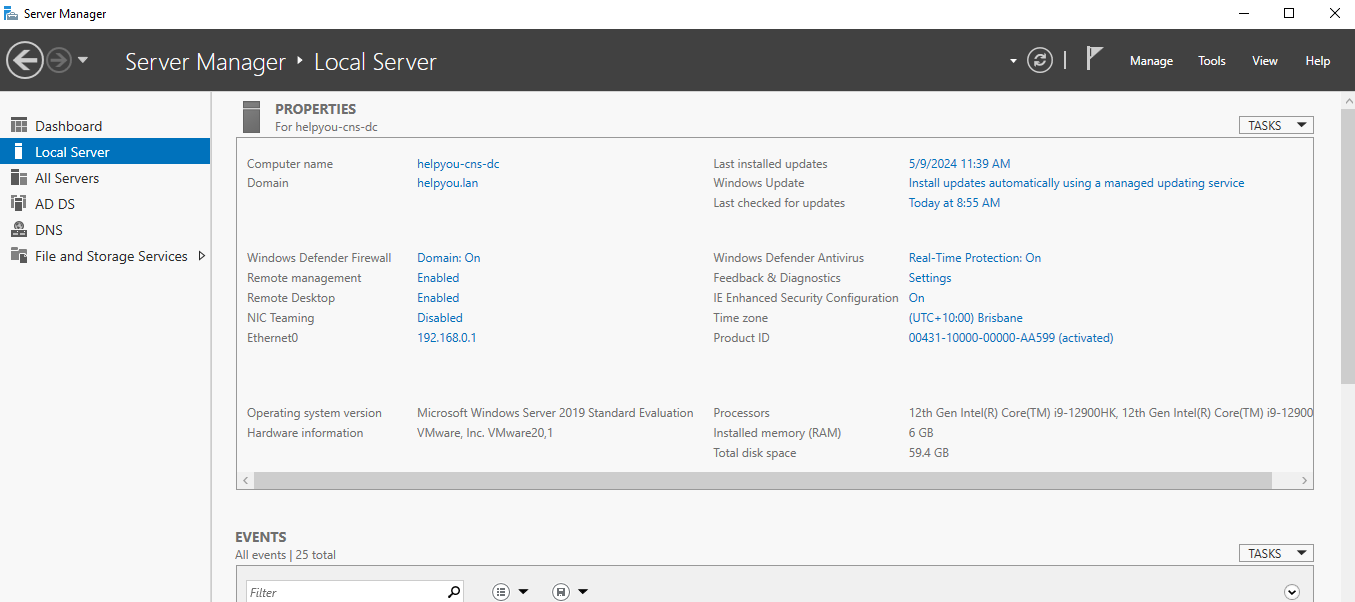


Figure 20 Cairns Domain Controller

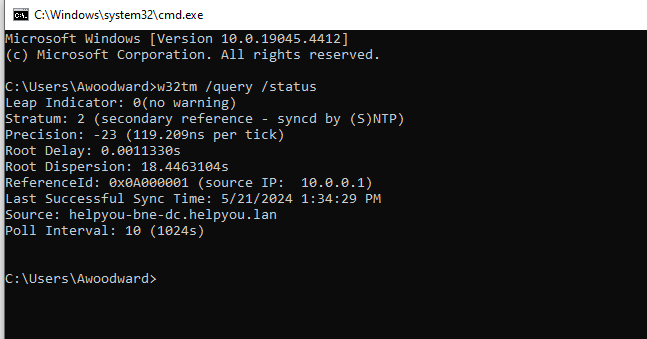


Figure 21 Checking NTP

**Network Time Protocol (NTP)** is an internet protocol used to synchronize with computer clock time sources in a network.

1. Install and configure DNS (Domain Name Service) service on the Domain Controller servers in Brisbane and Cairns LANs.

* Brisbane DNS

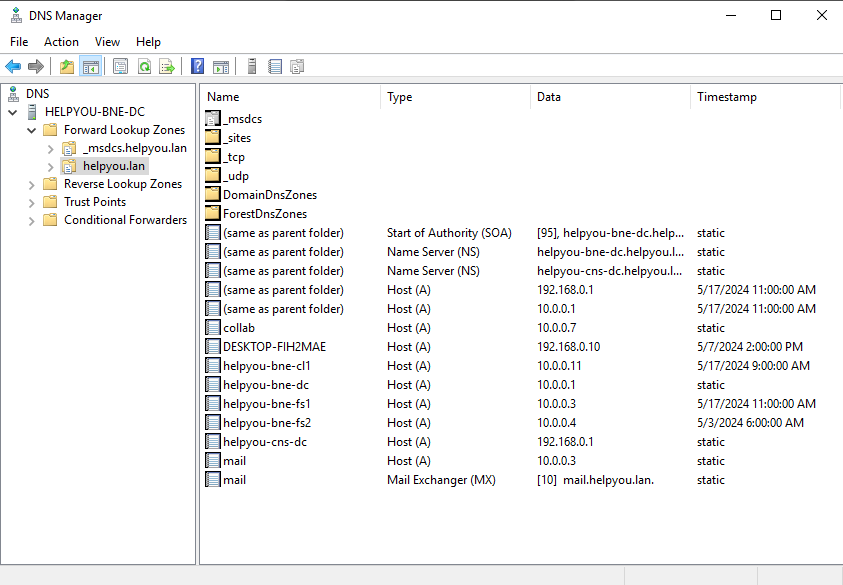


Figure 22 DNS Manager of Brisbane Domain Controller

* Cairns DNS

A screenshot of a computer

Description automatically generated

Figure 23 DNS Manager of Cairns Domain Controller

1. Confirm that the end devices in each LAN successfully join the Domain servers correspondently
2. Brisbane Client

A screenshot of a computer

Description automatically generated

Figure 24 Brisbane Client PC has successfully joined the Domain

1. Cairns Client

A screenshot of a computer

Description automatically generated

Figure 25 Cairns Client PC has successfully joined the Domain

1. Create Site Brisbane and Site Cairns in the Active Directory as these two sites connected with a WAN link are two networks located separately in Brisbane and Cairns. Please describe in writing how ADDS Sites implement load balancing across DCs to share with the client AD requests.

* Brisbane and Cairns Site

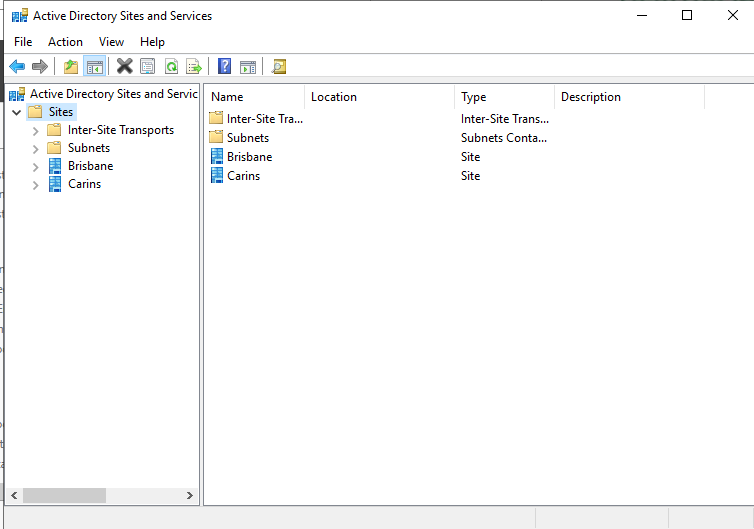


Figure 26 Brisbane and Cairns Site in Active Directory

**Active Directory Domain Services (ADDS)** logically groups domain controllers (DCs) into sites based on their physical network proximity and connection speed. When a client (user or computer) needs to authenticate or query ADDS, it first locates the closest site by referencing its configured site information. The client then randomly selects a DC from the list of DCs in that site to handle the request. This random selection of DCs within the same site automatically distributes the load across multiple DCs, providing load balancing.

1. Create subnets for the two sites according to the IP address tables you designed for this project

A screenshot of a computer

Description automatically generated

Figure 27 Create subnets for two sites

1. Move the domain controllers to the corresponding sites. DC-1 under Brisbane Site and DC-2 under Cairns Site.

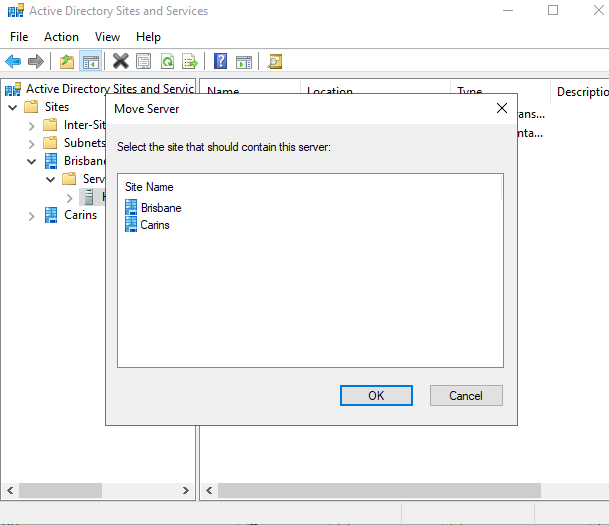


Figure 28 Brisbane and Cairns Sites

1. Configure the IP site link schedules to replicate the Active Directory data between DC-1 and DC-2 during the off peak hours.

A screenshot of a computer

Description automatically generated

Figure 29 Setting Schedule for Brisbane and Cairns Site

1. Modify the firewall policies on the LAN border in both sites to allow the communication between DC-1 and DC-2.

A screenshot of a computer

Description automatically generated

Figure 30 VPN Configuration of pfSense firewall of Cairns and Brisbane

1. Create OUs on one DC and force replication between two DCs to verify the synchronisation between the two sites.

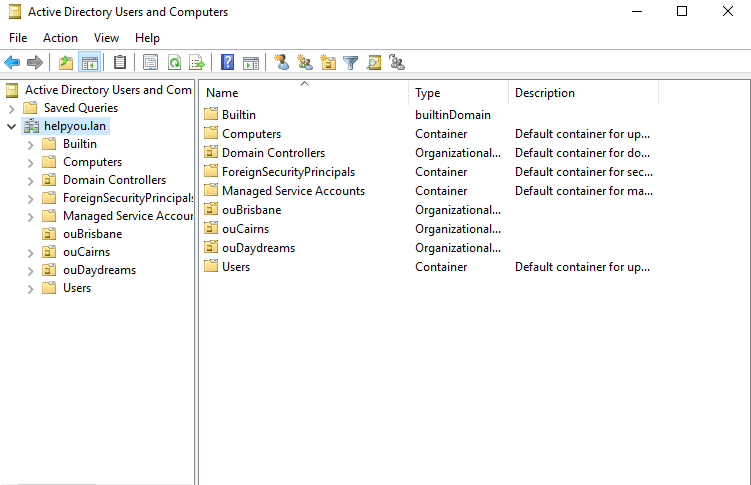


Figure 31 Creation of OUs for Brisbane DC

A screenshot of a computer

Description automatically generated

Figure 32 Cairns DC successfully has synced from Brisbane DC

1. Briefly describe what user authentication is in writing format. Briefly describe what Active Directory is in writing format.

**User Authentication** is the process of verifying the identity of a user attempting to access a system, application, or network resource. It typically involves providing valid credentials, such as a username and password, to prove the user's identity.

**Active Directory (AD)** is a directory service developed by Microsoft for Windows domain networks. It is a centralized and standardized system that authenticates and authorizes users and computers in a Windows domain network environment. AD stores information about user accounts, and computer accounts, and provides a way to manage them in an organized and hierarchical manner. It enables administrators to manage access to network resources, enforce security policies, and provide a single sign-on experience for users across the domain.

1. You need to demonstrate that the part is successfully completed to your instructor. Describe orally what this part is and how you implement it. Obtain a written sign-off.

Date: 24/05/2024

Prepared by: Thong Thao

Subject: Sign-off for Implementing ADDS and DNS - Brisbane and Cairns

Dear Frans De Oude,

I implemented integrated Active Directory Domain Services (ADDS) and Domain Name System (DNS) services across two separate local area networks (LANs) in Brisbane and Cairns, connected via a wide area network (WAN) link.

**The key steps involved:**

* Configured IP addressing, netmasks, and default gateways for the domain controller (DC) servers in each LAN.
* Installed and configured the ADDS role on the DC servers, enabling them to act as domain controllers for their respective LANs. Ensured time synchronization using Network Time Protocol (NTP).
* Installed and configured the DNS role on the DC servers to provide name resolution services within each LAN.
* Verified that client machines in each LAN successfully joined their respective domain.
* Created Active Directory sites for Brisbane and Cairns to logically group the DCs based on network proximity. This enables load balancing of authentication requests across DCs within each site.
* Configured site links and schedules to replicate Active Directory data between the Brisbane and Cairns DCs during off-peak hours over the WAN link.
* Modified firewall policies to allow communication between the Brisbane and Cairns DCs over the WAN link.
* Created organisational units (OUs) on one DC and forced replication to verify synchronisation between the two sites.

Sign-off.

Signed: Date:

# Part 4: Implement DFS, FSRM, Desktop Management, Anti-Virus Software Deployment on the LANs of Brisbane and Cairns

1. Write out a table of IP addresses, netmasks and default gateways (where applicable) for the File servers according to the instructions provided by your instructor.

|  |  |  |  |
| --- | --- | --- | --- |
| **Server** | **IP Address** | **Netmask** | **Default Gateway** |
| helpyou-bne-fs1 | 10.0.0.3 | 255.255.255.0 | 10.0.0.254 |
| helpyou-bne-fs2 | 10.0.0.4 | 255.255.255.0 | 10.0.0.254 |

1. Add two file servers to the Brisbane LAN using the IP addresses in step 2.

* Helpyou-bne-fs1

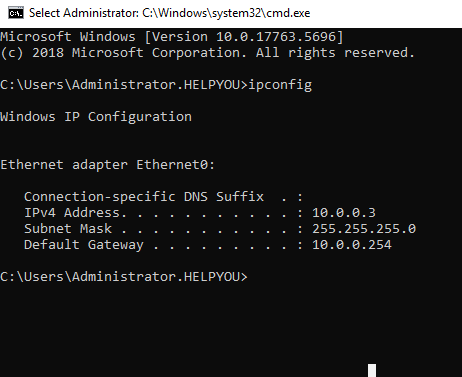


Figure 33 IP of File Server 1

* Helpyou-bne-fs2

A screenshot of a computer

Description automatically generated

Figure 34 IP of File Server 2

1. Install and configure Distributed File System (DFS) on FS-1 and FS-2 to (based on detailed instructions from your instructor)
   1. Allow distributed shares on multiple servers.

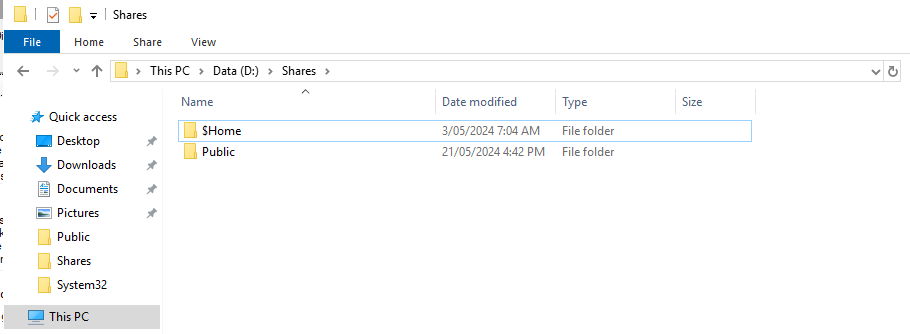


Figure 35 Home and Public Share

* 1. Configure DFS Namespace to allow easier management of the distributed shares created in 4.a.

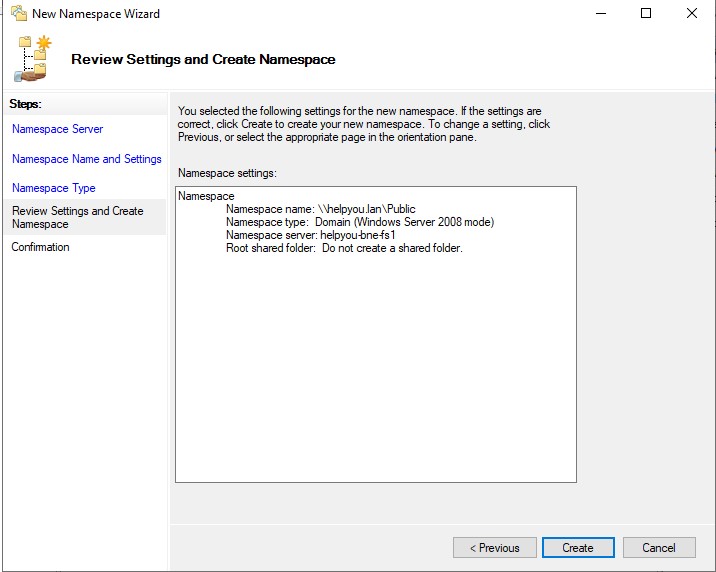


Figure 36 DFS Namespace Creation

* 1. Configure DFS replication between shares created in 4.a.

A screenshot of a computer

Description automatically generated

Figure 37 DFS Replication Between Two File Servers (FS1 and FS2)

1. Install and configure File Server Resource Manager on FS-1 and FS-2 to (based on detailed instructions from your instructor)
   1. Configure storage quotas based on users’ needs.

A screenshot of a computer

Description automatically generated

Figure 38 Quote Configuration for Public Share

* 1. Configure file screening to prevent movies from being stored to a folder based on the filename extension.

A screenshot of a computer screen

Description automatically generated

Figure 39 Block Audio and Video Files Configuration

* 1. Generate storage reports that show the state of file server volumes and anyone who exceeds the quota or users files that aren’t allowed.

A screenshot of a computer

Description automatically generated

Figure 40 Test Copy MP3 file to Public Share Folder

1. Deploy desktop management via Group Policy Object (GPO) on DC-1 (based on detailed instructions from your instructor).
   1. Share a desktop background wallpaper jpeg image to everyone in the domain.

A screenshot of a computer

Description automatically generated

Figure 41 Share Desktop Background Wallpaper

* 1. Deploy a GPO on DC-1 to force all the end devices in the domain to use the jpeg image as its background wallpaper.

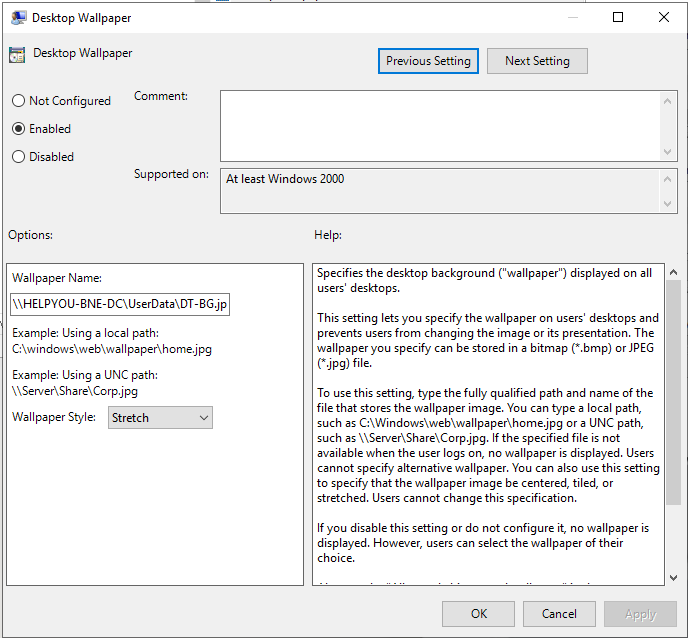


Figure 42 Create Policy for Desktop Wallpaper

* 1. Disallow changes to the items on the desktop.

A screenshot of a computer

Description automatically generated

Figure 43 Enable Policy to Prohibit change

A key to a house

Description automatically generated

Figure 44 The policy is applied to the Client successfully

* 1. Force active directory replication to synchronize this policy to DC-2.

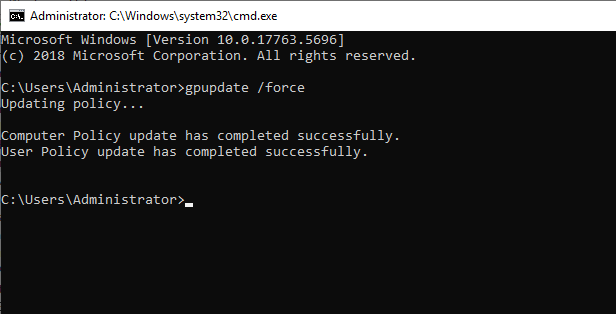


Figure 45 Force Update Policy Command

1. Configure anti-virus software deployment via Group Policy Object (GPO) on DC-1(based on detailed instructions from your instructor).
   1. Share an anti-virus software MSI package to all the computers in the domain.

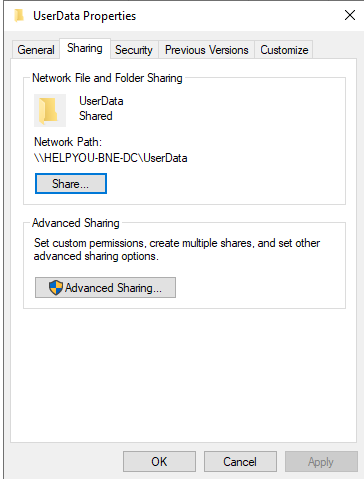


Figure 46 Share Anti-Virus software MSI Package Folder

* 1. Deploy a GPO on DC-1 to force all the end devices in the domain to install the anti-virus software automatically.

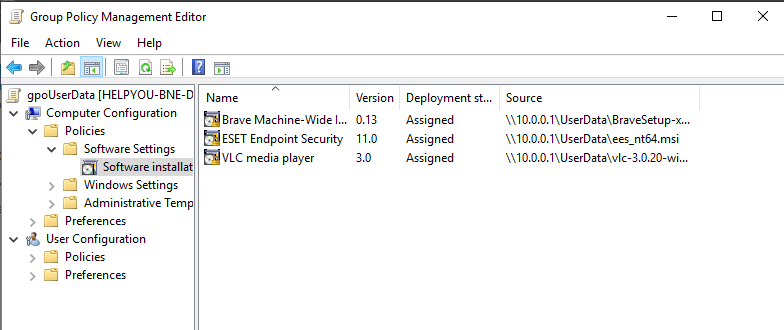


Figure 47 Create a new package ESET Endpoint Security to the Policy

* 1. Test it on the end devices to verify the GPO effects.

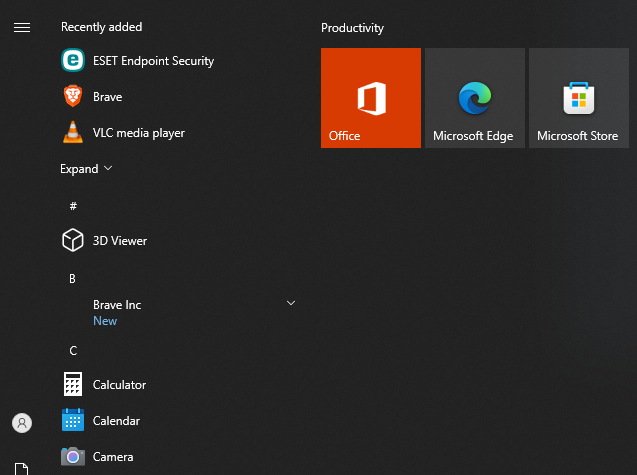


Figure 48 ESET Endpoint Security and other Applications successfully installed

1. Install a simple FTP server and demonstrate the FTP services running. Briefly describe in writing what is FTP protocol.

A screenshot of a computer program

Description automatically generated

Figure 49 FTP Services Running

**FTP** stands for File Transfer Protocol, a standard network protocol that enables the transfer of files between computers over the internet. It allows users to upload, download, and manage files on remote servers

1. You need to demonstrate that the part is successfully completed to your instructor. Describe orally what this part is and how you implement it. Obtain a written sign-off.

Date: 24/05/2024

Prepared by: Thong Thao

Subject: Sign-off for Implement DFS, FSRM, Desktop Management, Anti-Virus Software Deployment on the LANs of Brisbane and Cairns

Dear Frans De Oude,

I am writing to formally notify you of completing the implementation of DFS, FSRM, Desktop Management, Anti-Virus Software Deployment on the LANs of Brisbane and Cairns.

**The following key objectives were successfully achieved:**

* File Server Deployment: Two file servers (Helpyou-bne-fs1, Helpyou-bne-fs2) were integrated into the Brisbane LAN, with appropriate IP configurations.
* Distributed File System (DFS): DFS was implemented to enable distributed file shares, namespace consolidation, and replication between the file servers.
* File Server Resource Manager (FSRM): FSRM was configured to enforce user storage quotas, implement file screening based on extensions, and generate comprehensive storage reports.
* Group Policy Object (GPO) Management: GPO was utilised to centrally manage desktop configurations, including enforcing a standardised wallpaper and restricting desktop modifications. Active Directory replication was implemented to ensure policy consistency.
* Anti-Virus Deployment via GPO: Anti-virus software was automatically deployed across domain devices using GPO, enhancing network security.
* FTP Server Demonstration: A functional FTP server was established, and a demonstration of its operation was provided, along with an explanation of the File Transfer Protocol (FTP).

Thorough testing has confirmed the successful operation of all implemented services. I am prepared to provide a detailed demonstration and address any questions you may have regarding the implementation.

Sign-off.

Signed: Date:

# Part 5: Install a WSUS server and Implement interoperability between Linux and Windows

1. Write out a table of IP addresses, netmasks and default gateways (where applicable) for the WSUS server and the Linux server according to the instructions provided by your instructor.

|  |  |  |  |
| --- | --- | --- | --- |
| **Server** | **IP Address** | **Netmask** | **Default Gateway** |
| Helpyou-bne-fs1 | 10.0.0.3 | 255.255.255.0 | 10.0.0.254 |

1. Install and configure a WSUS server service role on FS-1 server as described below:
   1. Install and configure Windows Server Update Services role on the FS-1 server according to the instructions given by your instructor. FS-1 will become WSUS-1 server as well.
   2. Download and approve the windows updates as instructed by your instructor.

A screenshot of a computer

Description automatically generated

Figure 50 Windows Server Update Service

* 1. Create and configure a computer-based domain Group policy named “Auto Windows Update” to allow the domain computers to detect and pull the windows updates from the WSUS-1 server. A screenshot of a computer program

     Description automatically generated

Figure 51 Enable Automatic Update Policies

* 1. Reboot FS-2 to verify that the Auto Windows Update policy is effective.

A blue screen with white text

Description automatically generated

Figure 52 Updating

1. Describe briefly what is web services and take screenshots of the IIS Web server has been installed on the WSUS server to confirm that the WSUS server is acting as a web server as well.

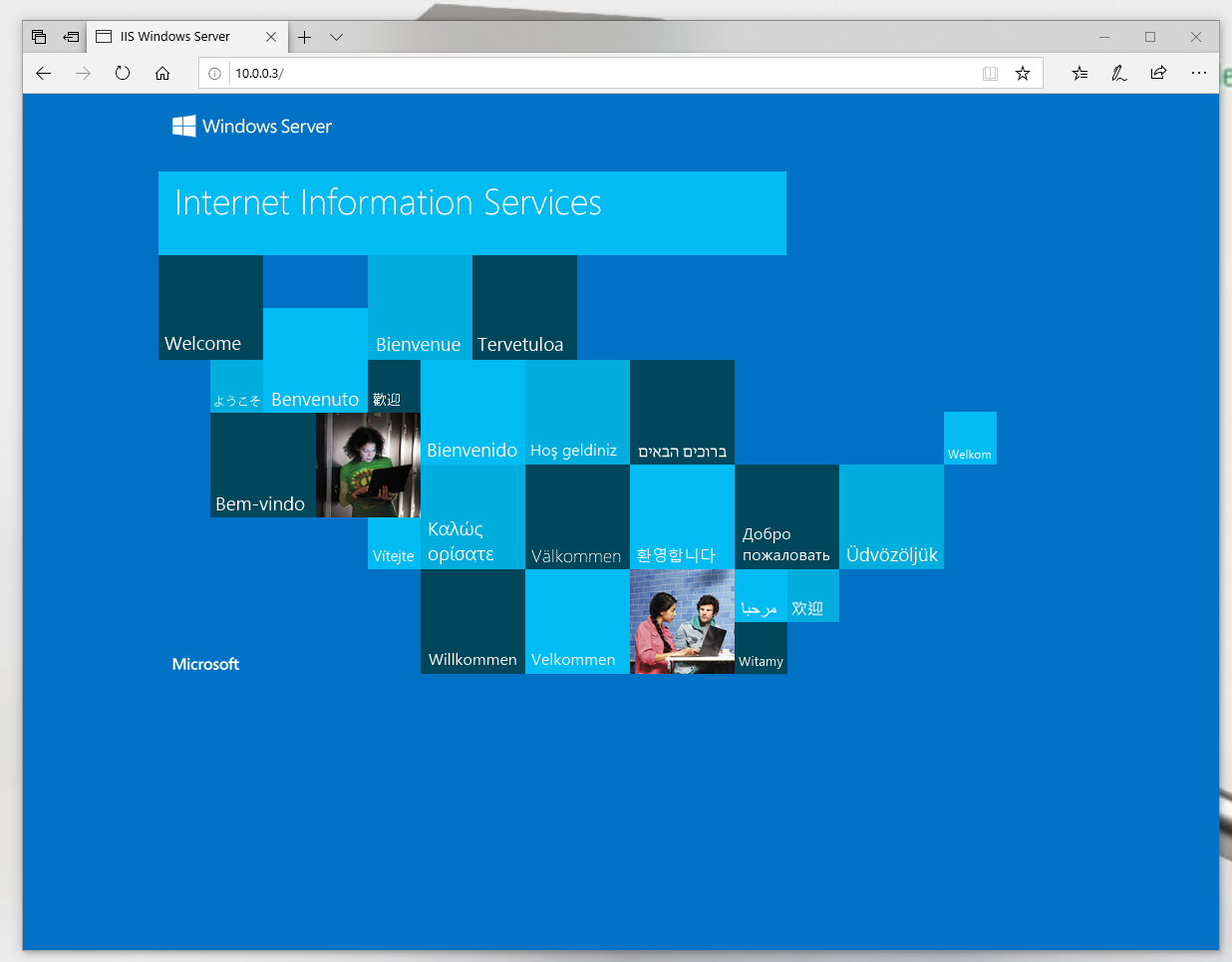


Figure 53 The IIS Web Server

1. Join a Linux server to the existing ADDS domain and enable file sharing between the Linux Server and FS-2. (Note: if the DHCP server implemented previously is a Linux server, adding a new Linux server is not necessary.)

A screenshot of a computer program

Description automatically generated

Figure 54 Brisbane Linux Server Join Domain

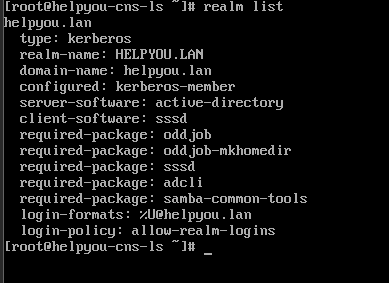


Figure 55 Cairns Linux Server Join Domain

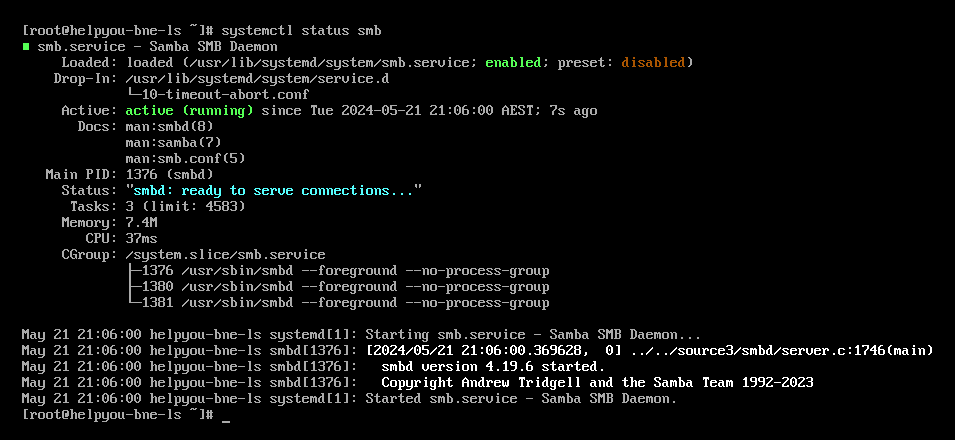


Figure 56 SMB is active (running)

1. Install a simple eMail server on either the Brisbane site.

A screenshot of a computer

Description automatically generated

Figure 57 Mail Server Configuration

1. You need to demonstrate that the part is successfully completed to your instructor. Describe orally what this part is and how you implement it. Obtain a written sign-off.

Date: 24/05/2024

Prepared by: Thong Thao

Subject: Sign-off for a WSUS server and Implement interoperability between Linux and Windows

Dear Frans De Oude,

I am writing to formally notify you to confirm the successful completion of the WSUS server and implement interoperability between Linux and Windows.

**The Summary of Completed Tasks:**

* **WSUS Server Configuration:**
  + Installed and configured the Windows Server Update Services role on the FS-1 server (now known as WSUS-1 server).
  + Downloaded and approved Windows updates as instructed.
  + Created and configured a computer-based domain Group Policy named "Auto Windows Update" to enable domain computers to receive updates from the WSUS-1 server.
  + Verified the policy's effectiveness by rebooting FS-2.
* **Web Services Confirmation:**
  + Briefly described web services.
  + Provided screenshots of the IIS Web server installed on the WSUS server, confirming its role as a web server.
* **Linux Server Integration:**
  + Successfully joined a Linux server (Brisbane or Cairns) to the existing ADDS domain.
  + Enabled file sharing between the Linux server and FS-2.
* **Email Server Installation:**
  + Installed a simple email server on the Brisbane site.

**Sign-off.**

Signed: Date:

# Part 6: Install and Configure VoIP services on the LANs of Brisbane and Cairns

1. Write out a table of IP addresses, netmasks and default gateways (where applicable) for the Call Manager-1, Call-Manager-2, and the VLAN VoIP according to the instructions provided by your instructor.

|  |  |  |  |
| --- | --- | --- | --- |
| **Server** | **IP Address** | **Netmask** | **Default Gateway** |
| Helpyou-bne-voip | 10.0.0.9 | 255.255.255.0 | 10.0.0.254 |

1. Install and configure two Call-Manager servers with selected voice codec according to your instructor’s instructions.

A screenshot of a computer error

Description automatically generated

Figure 58 VoIP Server (FreePBX)

1. Install and configure IP Phone-1 and IP Phone-2 and make sure these two IP phones can communicate with each other across the Site-To-Site VPN Tunnel.

A screenshot of a computer

Description automatically generated

Figure 59 Test Call from Brisbane IP Phone 100 to Cairns IP Phone 101

A screenshot of a computer

Description automatically generated

Figure 60 Test Call from Cairns IP Phone 101 to Brisbane IP Phone 100

1. Describe what VoIP is in writing format.

**Voice over Internet Protocol (VoIP)** is a technology that enables voice calls over the Internet instead of traditional phone lines. It converts voice signals into digital data packets, which are then transmitted over the internet. This allows for cheaper calls, especially for long-distance or international calls.

1. You need to demonstrate that the part is successfully completed to your instructor. Describe orally what this part is and how you implement it. Obtain a written sign-off.

Date: 24/05/2024

Prepared by: Thong Thao

Subject: Sign-off for a WSUS server and Implement interoperability between Linux and Windows

Dear Frans De Oude,

The VoIP (Voice over Internet Protocol) services were installed and configured on the LANs of Brisbane and Cairns. Two Call Manager servers were set up, and IP phones were configured to communicate with each other through a Site-to-Site VPN tunnel. The successful completion of calls between the IP phones in Brisbane and Cairns was verified.

**The Summary of Completed Tasks:**

**VoIP Server Configuration:**

* Installed and configured two Call Manager servers (FreePBX) with the specified voice codec as instructed.
* Provided IP addresses, netmasks, and default gateways for FreePBX servers and the VLAN VoIP.

**IP Phone Configuration:**

* Successfully installed and configured IP Phone-1 and IP Phone-2.
* Confirmed communication between IP phones across the Site-to-Site VPN Tunnel through successful test calls.

**Sign-off.**

Signed: Date:

# Part 7: Implement Videoconferencing services on the LANs of Brisbane and Cairns

1. Write out a table of IP addresses, netmasks and default gateways (where applicable) for the Comm-1 server, which is the communication server for a selected videoconferencing product of your instructor’s choice. For example, the Comm-1 server could be a Skype for Business Front End Server if chosen. Request more detailed instructions from your instructor.

|  |  |  |  |
| --- | --- | --- | --- |
| **Server** | **IP Address** | **Netmask** | **Default Gateway** |
| Daydream-collab | 10.0.0.7 | 255.255.255.0 | 10.0.0.254 |

1. Install and configure videoconferencing services on Comm-1.

A screenshot of a computer

Description automatically generated

Figure 61 Installed Talk App in NextCloud

1. Verify that a video meeting can be started on a client workstation from Brisbane site and communicated through to the other site with another client on Cairns via audio and video. It should work in both directions.

A screenshot of a computer

Description automatically generated

Figure 62 Test video call from Brisbane to Cairns

1. Research for what codecs you can choose from for the videoconferencing software of your selection. Record what you have found in your portfolio.

**Nextcloud Talk** primarily uses the VP8 codec for video conferencing. There is an optional setting to use H.264, but it doesn't work with the High-performance backend. VP8 is the default and required codec due to WebRTC specifications, ensuring compatibility across different devices. VP9 is also mentioned but requires more CPU power and is less commonly used.

1. You need to demonstrate that the part is successfully completed to your instructor. Describe orally what this part is and how you implement it. Obtain a written sign-off.

Date: 24/05/2024

Prepared by: Thong Thao

Subject: Sign-off for a WSUS server and Implement interoperability between Linux and Windows

Dear Frans De Oude,

I am writing to inform you of the successful implementation and configuration of videoconferencing services on the Comm-1 server, utilising NextCloud Talk.

**Key Achievements:**

* Successfully installed and configured NextCloud Talk on the Comm-1 server.
* Verified seamless audio and video communication between client workstations in Brisbane and Cairns.
* Confirmed using the VP8 codec as the primary codec for video conferencing, ensuring compatibility across devices.

This implementation enables efficient and effective communication between our Brisbane and Cairns offices, enhancing collaboration and productivity.

**Sign-off.**

Signed: Date:

# Part 8: Install and configure a network management software on the LANs of Brisbane and Cairns

1. Write out a table of IP addresses, netmasks and default gateways (where applicable) for the NMS-1 server, which is the network management server for a selected network management product of your instructor’s choice. For example, the NMS-1 server could be a PRTG Server if chosen. Request more detailed instructions from your instructor.

|  |  |  |  |
| --- | --- | --- | --- |
| **Server** | **IP Address** | **Netmask** | **Default Gateway** |
| helpyou-bne-nms | 10.0.0.6 | 255.255.255.0 | 10.0.0.254 |

1. Install and configure the NMS-1 to collect Syslog and SNMP messages from servers and/or network devices.

A screenshot of a computer

Description automatically generated

Figure 63 NetCrunch is installed on the helpyou-bne-snm server

1. Set and monitor alerts and logs on the monitored devices and reflect it on the NMS-1 to supervise the network performance in real time.

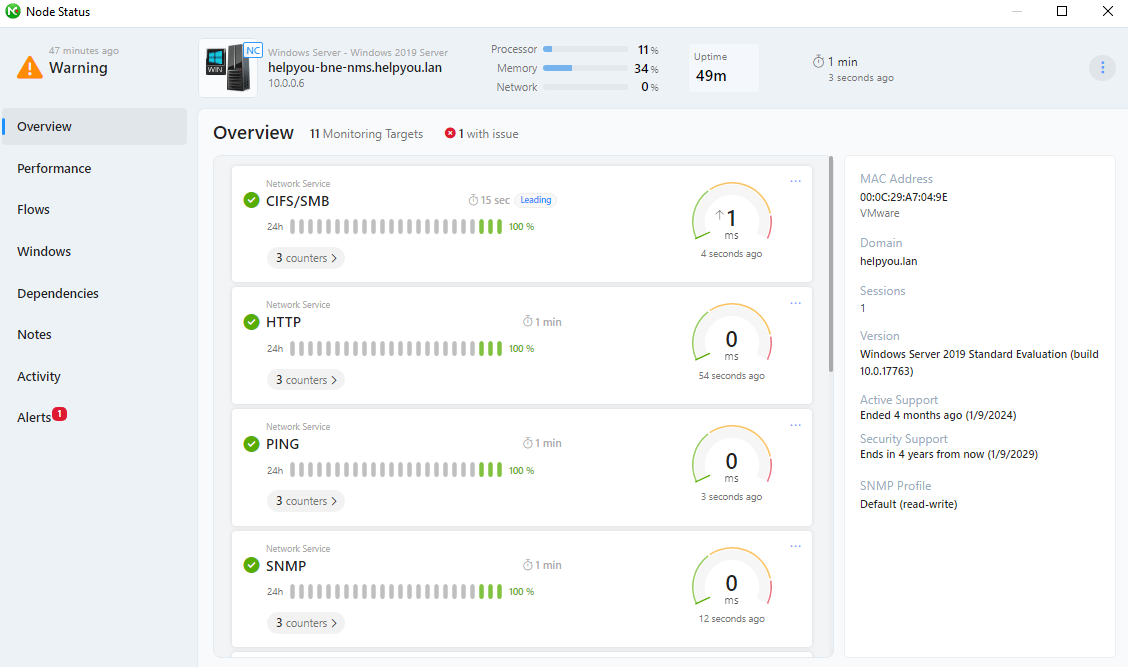


Figure 64 Status of the server (helpyou-bne-nms)



Figure 65 Status of Linux Server (helpyou-bne-ls)

1. Generate traffic or create alerts on the monitored devices purposely. Verify the generated traffic or created alerts can be captured on the NMS-1 in real time. Briefly analyze the captured performance data on your portfolio with sample pictures and compose a short paragraph of analysis.

A screenshot of a computer

Description automatically generated

Figure 66 The Alert on Monitored (NetCruch) is created

**Node Down (10.0.0.2).** This alert notification means that the Linux Server is down or cannot connect to NetCrunch. See ***Figure 67*** below.

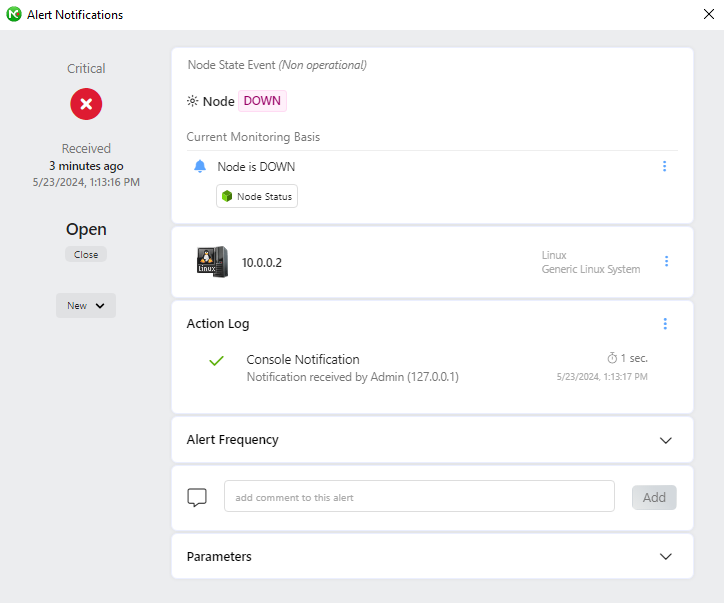


Figure 67 Alert Notifications that Node Down

1. Obtain instructions from your instructor orally and enable SNMP on monitored devices.

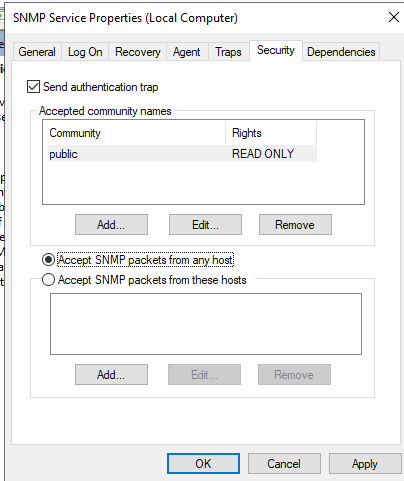


Figure 68 Enable SNMP Service in Windows

A screenshot of a computer

Description automatically generated

Figure 69 Enable SNMP Service is active (running) in Linux

1. Modify security policies on the company’s firewalls and the firewall policies on the monitored devices to specifically allow NMS-1 to remotely manage the monitored devices via SNMP.

Create two new rules to allow SNMP TCP and UDP port 161-162

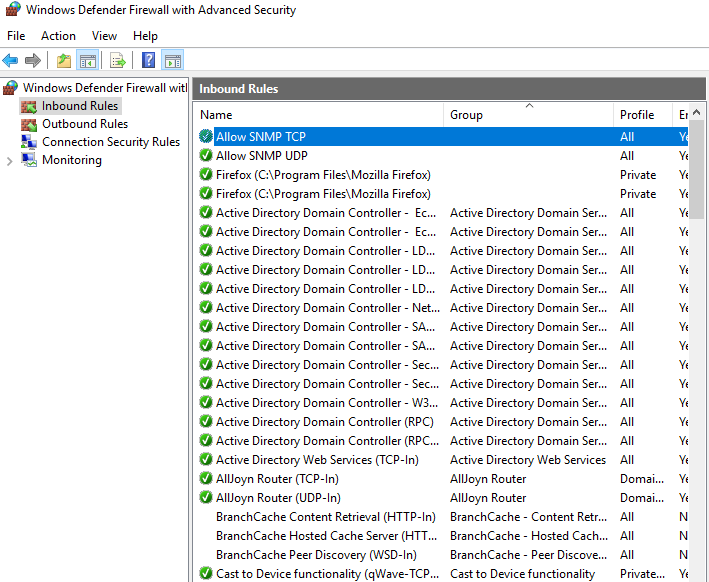


Figure 70 Two new rules for allowing SNMP

1. Briefly describe what SNMP is in writing format.

**Simple Network Management Protocol (SNMP)** is an Internet Standard protocol for collecting and organising information about managed devices on IP networks and for modifying that information to change device behaviour.

1. You need to demonstrate that the part is successfully completed to your instructor. Describe orally what this part is and how you implement it. Obtain a written sign-off.

Date: 24/05/2024

Prepared by: Thong Thao

Subject: Sign-off for Install and configure a network management software on the LANs of Brisbane and Cairns Windows

Dear Frans De Oude,

I have successfully installed and configured network management software (NMS) on the LANs of Brisbane and Cairns. Here's a summary of the tasks accomplished:

**Network Management Server Setup**

* Configured the helpyou-bne-nms server with IP address 10.0.0.6, netmask 255.255.255.0, and default gateway 10.0.0.254.
* Installed NetCrunch as the NMS and configured it to collect Syslog and SNMP messages from servers and network devices.

**Monitoring and Alerts**

* Set up monitoring and alerts on the NMS to supervise network performance in real-time.
* Generated traffic and created alerts on monitored devices to verify their capture on the NMS.
* Analysed the captured performance data, including a "Node Down" alert indicating the Linux server (10.0.0.2) was unreachable.

**SNMP Configuration**

* Enabled SNMP service on monitored Windows and Linux devices.
* Modified firewall policies to allow the NMS to remotely manage devices via SNMP on TCP/UDP ports 161-162.

**Sign-off.**

Signed: Date:

# Part 9: Implement Ongoing Monitoring of Network security

1. Write out a table of IP addresses, netmasks and default gateways (where applicable) for the Nmap scanning PC, and the IDS-1 server, which is the Intrusion Detection Server for a selected IDS software product of your instructor’s choice. For example, the NMS-1 server could be a Secure Onion Server if chosen. Request more detailed instructions from your instructor.

|  |  |  |  |
| --- | --- | --- | --- |
| **Device** | **IP Address** | **Netmask** | **Default Gateway** |
| helpyou-bne-fw | 10.0.0.254 | 255.255.255.0 |  |
| Kali Linux | 172.101.10.130 | 255.255.255.0 | 172.101.10.1 |

1. Install and configure the IDS-1 to analyze network traffic, respectively, and provide log and alert data for detected anomalous events and activity.

* Install the snort package in pfSense firewall

A screenshot of a computer

Description automatically generated

Figure 71 Install the snort package sucessful

* Enable Snort in the Global Settings tab and save.

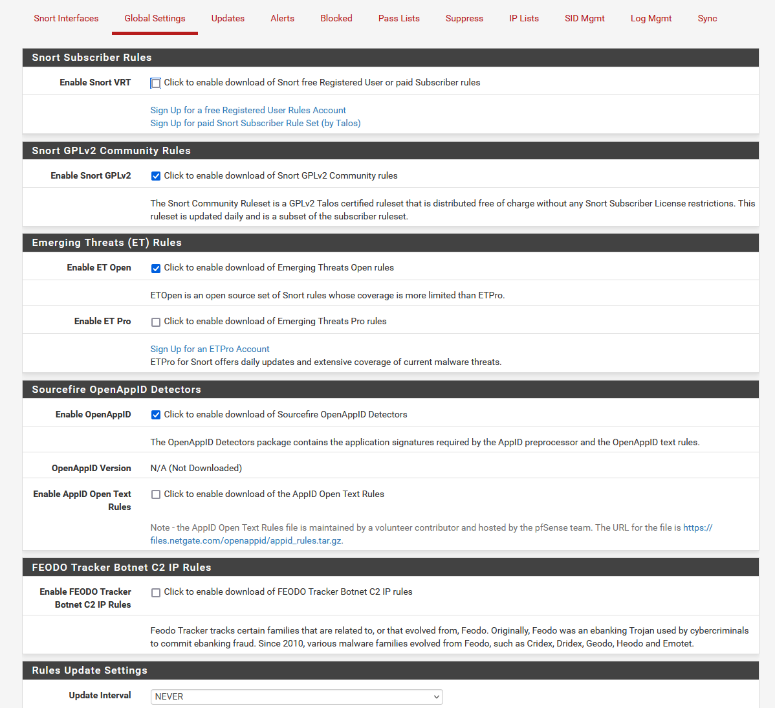


Figure 72 Enable the snort package

* Update rules in the Updates tab

A screenshot of a website

Description automatically generated

Figure 73 Update Rules Success

* Finally, enable the Snort Interface

A screenshot of a computer

Description automatically generated

Figure 74 The Snort Interface is enabled

1. Install a Nmap scanning PC at the edge of the Brisbane LAN.

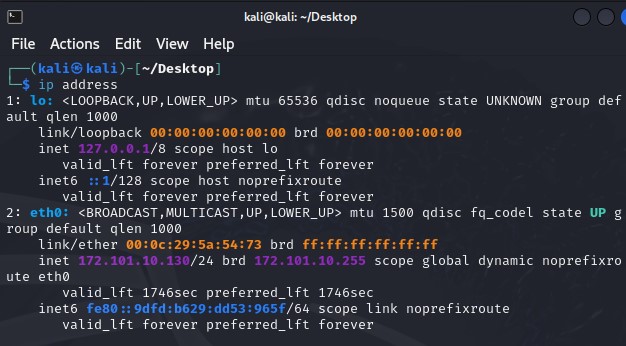


Figure 75 PC (Kali Linux) for test Nmap Scan

A screenshot of a computer program

Description automatically generated

Figure 76 Nmap scan the Brisbane Network

1. Launch a Nmap scanning from the Nmap scanning PC against the Brisbane LAN and verify that IDS-1 can pick up this suspicious event and generate alert on it.

A screenshot of a computer

Description automatically generated

Figure 77 Alert Log in the pfSense Firewall

1. You need to demonstrate that the part is successfully completed to your instructor. Describe orally what this part is and how you implement it. Obtain a written sign-off.

Date: 24/05/2024

Prepared by: Thong Thao

Subject: Sign-off for a WSUS server and Implement interoperability between Linux and Windows

Dear Frans De Oude,

I have completed the implementation of ongoing network security monitoring for the Helpyou Mortgage Company's Brisbane LAN. Here are the key steps I followed:

**Network Configuration**

* Configured IP addresses, netmasks, and default gateways for the Nmap scanning PC (Kali Linux) and the Intrusion Detection Server (IDS-1) as per the provided table.

**IDS Implementation**

* Installed and configured the Snort package on the pfSense firewall to analyse network traffic and generate logs/alerts for anomalous events.
* Enabled Snort in the Global Settings, updated rules, and enabled the Snort interface.

**Nmap Scanning**

* Installed a Kali Linux system as the Nmap scanning PC at the edge of the Brisbane LAN.
* Performed an Nmap scan against the Brisbane LAN from the scanning PC.

**IDS Alert Verification**

* The Snort IDS successfully detected the Nmap scan as a suspicious event and generated an alert in the pfSense firewall logs, demonstrating effective ongoing monitoring.

I have implemented the required network security monitoring solution as per the instructions. Please provide your written sign-off to confirm the successful completion of this task.

**Sign-off.**

Signed: Date:

# Part 10: Troubleshooting report

1. Write a troubleshooting report about the following aspects:
   1. Describe network symptoms came across to you.
   2. Describe what troubleshooting tools and techniques, including any network diagnostic utilities you use to find out what is the cause to the network issues.
   3. Describe how you resolve the issues.

**Network Symptoms**

1. The VPN Tunnel Connectivity Issue

Unable to ping between two networks Cairns and Brisbane, this symptom indicates a network connectivity problem between the two locations, which could be caused by various factors such as routing issues, firewall configurations, or physical network problems.

A computer screen shot of a black screen

Description automatically generated

Figure 78 Test ping from Brisbane Client to Cairns Server

After I tested ping from the Brisbane Client to the Cairns Server, the issue occurred from the VPN IPsec connection between Cairns and Brisbane in the pfSense firewall was disabled on the Brisbane site.

1. The DHCP Server Issue

Clients of Brisbane are unable to obtain IP addresses from the DHCP Server, this symptom indicates that the problem is from the DHCP Server.

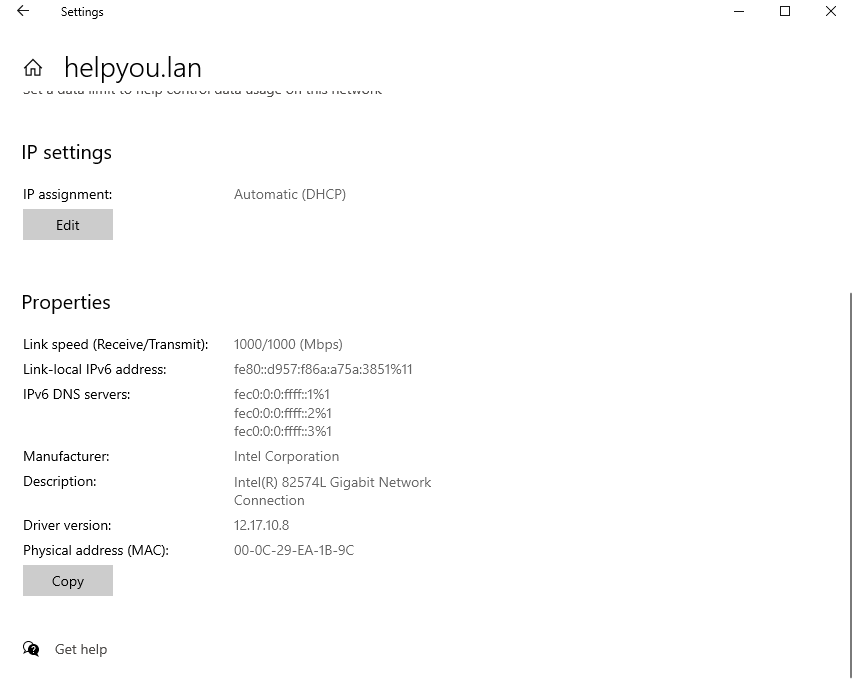


Figure 79 The Client unable to obtain the IP address from the DHCP Server

The overall issue is that the DHCP server which is the Linux Server of Brisbane is disabled and the firewall is blocking the DHCP (67/UDP).

1. The VoIP Phone Setup Failure in Cairns

The VoIP phone cannot register the VoIP on the Cairns site, this symptom indicates the configuration of FreePBX is missing configuration.

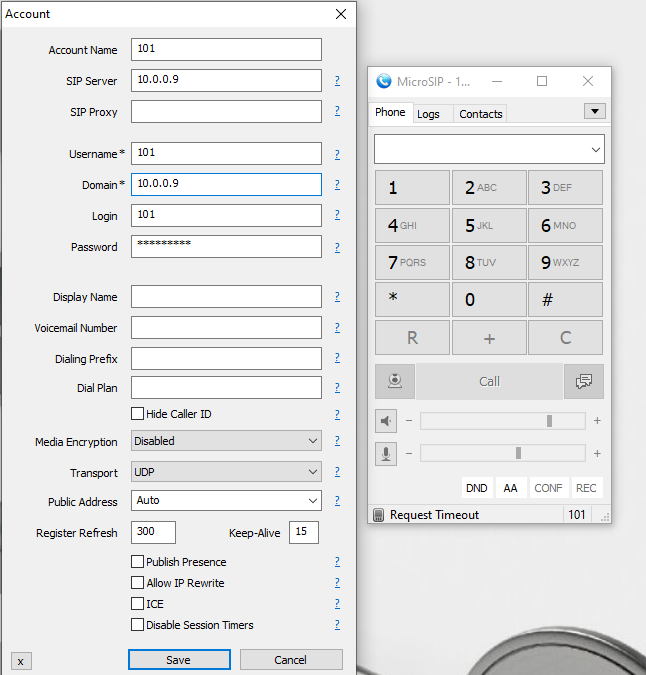


Figure 80 Request Timeout

Firstly, checked the VPN connection between Brisbane and Cairns Sites and it is working fine. Therefore, the issue of not being able to set up the VoIP phones in Cairns due to missing the firewall and fail2bane being enabled in FreePBX.

**Troubleshooting Tools and Techniques**

* Ping: Used to test connectivity between two devices or networks by sending ICMP echo request packets and measuring the response time.
* Traceroute(Linux) Tracert (Windows): Traces the path that packets take from the source to the destination, helping to identify routing issues or network bottlenecks.
* IP config /release: This command is executed to force the client to immediately give up its lease by sending the server a DHCP release notification which updates the server’s status information and marks the old client’s IP address available.
* IP config /renew: This command is executed to request a new IP address from the DHCP Server.
* Advanced IP Scanner: This tool identifies rouge DHCP Servers.

**Resolution Steps**

1. The VPN Tunnel connectivity Issue.

Access to pfSense firewall and enabling the pfSense IPsec connection resolved the connectivity issue between the two sites Brisbane and Cairns.

A screenshot of a computer

Description automatically generated

Figure 81 The VPN IPsec is disabled

**A screenshot of a computer

Description automatically generated**

Figure 82 Enable the VPN

After enabling the VPN and ensuring the connectivity of Cairns and Brisbane working properly, I can be able to successfully ping and tracert to the server of Cairns. See **Figure 83**

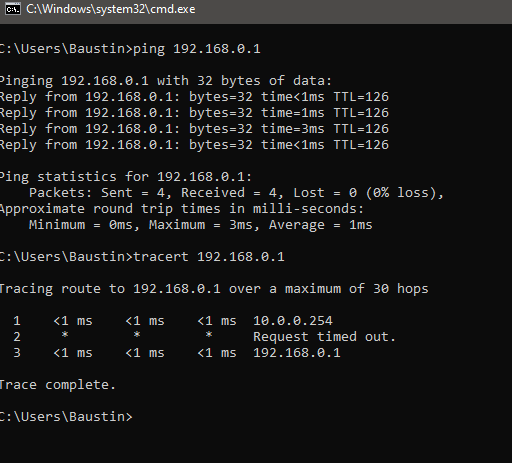


Figure 83 Ping and Tracert to Cairns Server

1. The DHCP Server Issue

Access to the Linux Server. Firstly, check the status of the DHCP Server ( the DHCP service is disabled in **Figure 84**) and then enable the DHCP Server and recheck the status (The DHCP service is enabled and running in **Figure 85**)

A screenshot of a computer program

Description automatically generated

Figure 84 The DHCP service status (Disabled)

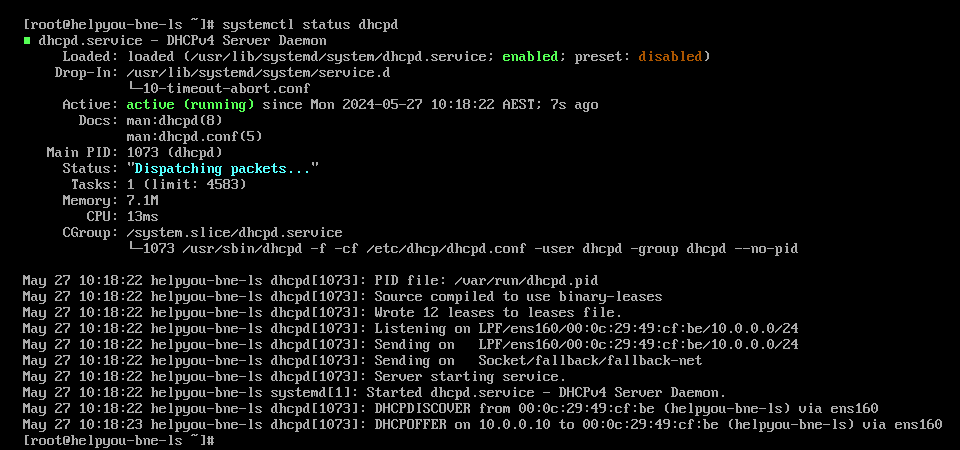


Figure 85 The DHCP service status (Enabled)

The next step is to allow the DHCP service (**Figure 86**)

A screenshot of a computer program

Description automatically generated

Figure 86 Add the DHCP service to the firewall

After implementing by enabling the DHCP service and allowing the DHCP service to the Linux Server and test release and renew the IP in the client PC. (**Figure 87**)

A screenshot of a computer

Description automatically generated

Figure 87 The client able to obtain the IP address from the DHCP Server

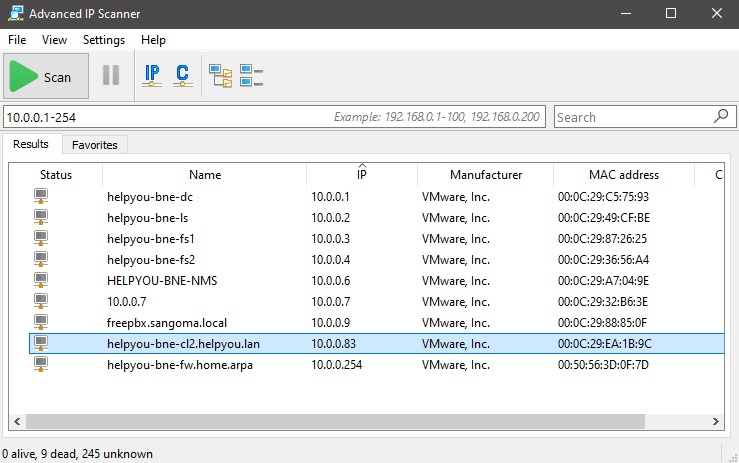


Figure 88 Identifying DHCP service by Advanced IP Scanner

1. The VoIP Phone Setup Failure in Cairns

Firstly, ping test from the Cairns site to the Brisbane firewall to make sure that the VPN connectivity is working fine (**Figure 89**).

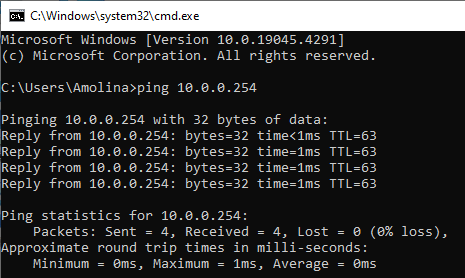


Figure 89 Ping from Cairns to the Brisbane Firewall

After checking the connection, the next step is to focus on the FreePBX firewall configuration.

* Disable and stop fail2ban in FreePBX

To disable and stop use the FreePBX command: *systemctl disable fail2ban* and *systemctl stop fail2ban*

A screenshot of a computer

Description automatically generated

Figure 90 The fail2ban is disabled

* Add known Network (Cairns) to FreePBX server
* A screenshot of a computer

  Description automatically generated

Figure 91 Add Cairns Network to FreePBX Server

After disabled and stopped fail2ban and adding known network (Cairns) to FreePBX server

A screenshot of a computer

Description automatically generated

Figure 92 Register Successful (Online)

# Reference

AVI Networks (2017). *Load Balancing 101 - Learn All About Load Balancers*. [online] Avi Networks. Available at: https://avinetworks.com/what-is-load-balancing/.

builtin.com. (n.d.). *What Is File Transfer Protocol? How Does FTP Work? | Built In*. [online] Available at: https://builtin.com/software-engineering-perspectives/file-transfer-protocol.

Federal Communications Commission (2010). *Voice Over Internet Protocol (VoIP)*. [online] Federal Communications Commission. Available at: https://www.fcc.gov/general/voice-over-internet-protocol-voip.

Nextcloud community. (2020). *What codec is used and how change it*. [online] Available at: https://help.nextcloud.com/t/what-codec-is-used-and-how-change-it/87037.

SearchNetworking. (n.d.). *What is Network Time Protocol (NTP)? - Definition from WhatIs.com*. [online] Available at: https://www.techtarget.com/searchnetworking/definition/Network-Time-Protocol.

Wikipedia Contributors (2019). *Simple Network Management Protocol*. [online] Wikipedia. Available at: https://en.wikipedia.org/wiki/Simple\_Network\_Management\_Protocol.

Digital Guardian. (n.d.). *What is a Proxy Server? Definition, How It Works & More*. [online] Available at: https://www.digitalguardian.com/blog/what-proxy-server-definition-how-it-works-more.