A screenshot of a computer

Description automatically generated

Windows Server 2019 installed with IP address highlighted from the firewall.

A screenshot of a computer

Description automatically generated

DNS active.

A screenshot of a computer

Description automatically generated

Windows Server 2019 with a static IP address of 192.168.1.10 and DNS server IP address of 192.168.1.1 which is also the default gateway from the pfSense firewall.

A computer screen shot of a computer screen

Description automatically generated

Windows 10 installed with its IP address highlighted from the firewall.

A computer screen shot of a computer screen

Description automatically generated

Static IP address for Windows 10 VM highlighted.

A screenshot of a computer

Description automatically generated

Windows 10 with the confirmation of DHCP settings working from the domain name (RTX.com) and IP address within the DHCP range.

A screenshot of a computer

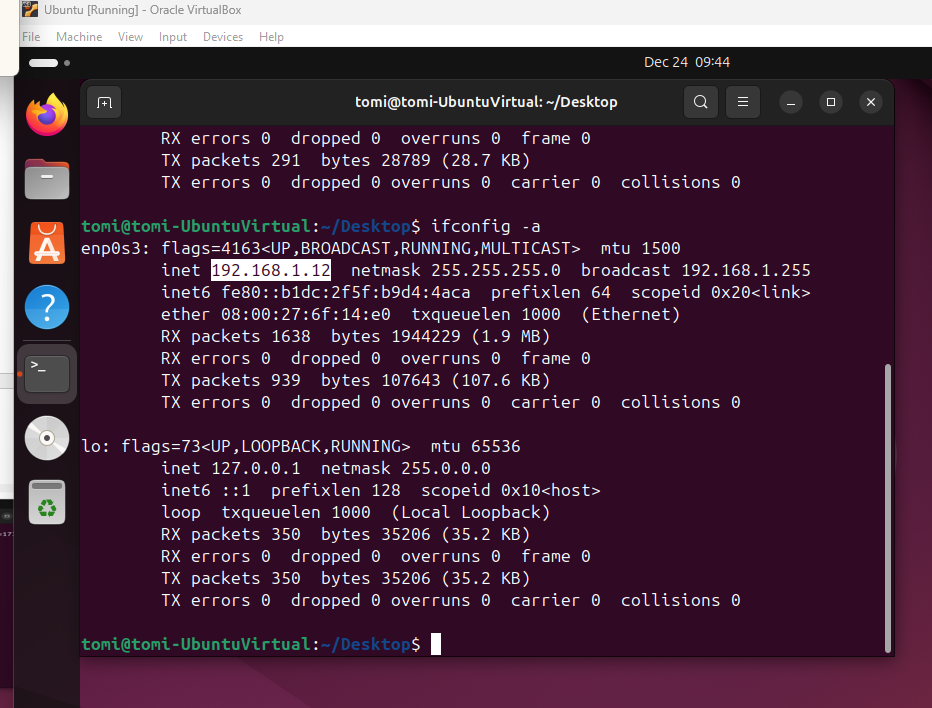
Description automatically generated

Ubuntu VM installed.

A screenshot of a computer

Description automatically generated

The Ubuntu VM IP address as assigned by the firewall.



Static IP address for Ubuntu VM highlighted.

A screenshot of a computer

Description automatically generated

Windows Server 2019 configured with Active Directory, DNS and DHCP server. The server has now been promoted to a domain controller.

A screenshot of a computer

Description automatically generated

Created DHCP settings on Windows Server 2019.

A screenshot of a computer

Description automatically generated

The IP address range for the DHCP.

A screenshot of a computer

Description automatically generated

The address range on the Windows server.

A screenshot of a computer

Description automatically generated

Organizational units created in the domain name RTX.com.

A screenshot of a computer

Description automatically generated

Users created.

A screenshot of a computer

Description automatically generated

The Windows 10 VM and Ubuntu VM were created on the domain controller.

A computer screen shot of a group policy management

Description automatically generated

Group Policy Management indicating the forest and the domain on the domain controller.

A screenshot of a computer

Description automatically generated

The lease duration was set to one day.

A screenshot of a computer

Description automatically generated

Joining Windows 10 to the DHCP server.

A screenshot of a computer

Description automatically generated

Windows 10 domain joined with the DHCP server

A screenshot of a computer

Description automatically generated

Domain joined with DHCP server.

A screenshot of a computer

Description automatically generated

Ubuntu VM discovered domain name RTX.com. Joined with the DHCP server computers are the Windows 10 VM and Ubuntu VM.

A screenshot of a computer

Description automatically generated

User, jtalabi from the DHCP server is authenticated from the Ubuntu VM.

A screenshot of a computer

Description automatically generated

Logon failed from a user.

A screenshot of a computer

Description automatically generated

Logon activities from four different users.

A screenshot of a computer

Description automatically generated

Logoff activities from three different users.

The role of AD in accessing information.

* From a centralized location, AD can allow administrators to manage user accounts and permissions to network resources.
* AD provides directory services, storing information about a network and its users, devices and services.
* AD allows flexible and secure communication between domains and allows for scalability.
* AD allows for group policy management to enforce security settings and configurations across all devices within the network.

Review of security logs in a Security Operations Center.

- Security logs provide detailed records of network activity, thereby the easy detection of unusual behavior or activity is possible.

- Logs can serve as a source of evidence in investigations of activities or security breaches.

- Logs help in incident response because the source of an attack can be seen which can help in understanding the attack’s impact and guidance to the appropriate response.

- Logs monitor the performance of a network which helps in revealing any issues within the network.