Network Access Control for Endpoint Devices

Dipendra Ale, BSc Honours in IT Management
Department of Computer Science,
MTU Cork, May 2023

Introduction

Traditional solutions that operate individually are no longer adequate since attacks continue to grow in complexity, variety, and performance. For us to proactively prevent such threats, we want a more unified security solution that provides an additional security layer to ensure only users and devices that have the appropriate permissions can access the various resources over the network. This project analyses the effectiveness of an open-source NAC solution for endpoint devices and also provides a comparative overview of other vendors solution.

Problem Statement

In order to communicate with servers and other network resources, users can connect their devices to any access point or outlet for connection. Over time, the majority of these endpoint devices may turn out to be prime targets for penetration, endangering the security of the organization if additional security measures such as admission control are not implemented. These dangers can vary from ransomware to DDoS attacks that could possibly bring down the whole network of an organization.

Solution

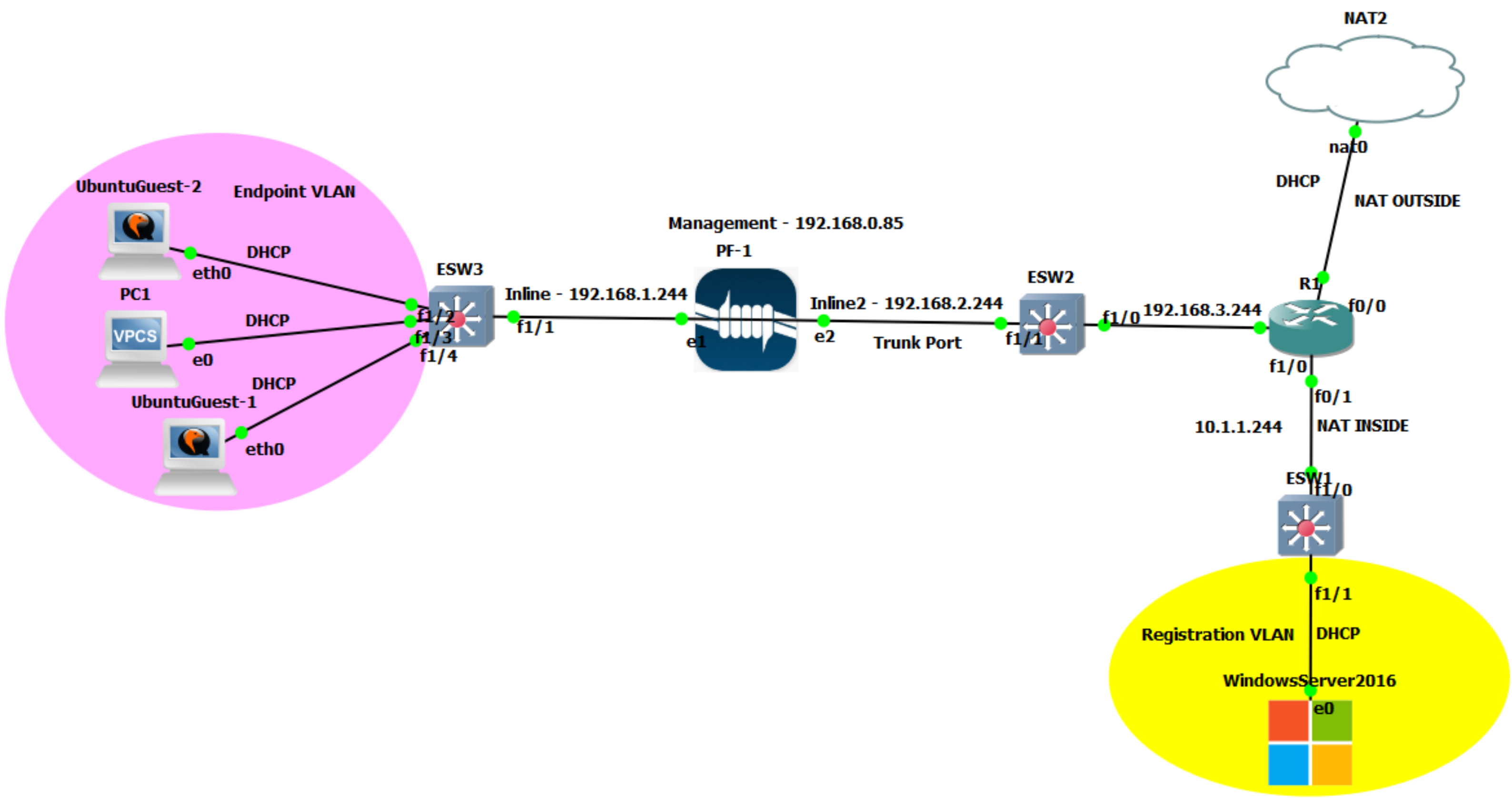
- Integrate and configure PacketFence to enforce Network Access Control for endpoint devices within a network topology in GNS3.
- Define users and groups with specific roles and access polices within PacketFence for access control to imitate university standards.
- Provide technical comparative overview on NAC vendors (PacketFence, Cisco NAC & Microsoft NAP)

Benefits of using NAC solutions

- NAC unifies a variety of network security systems, including Identity Management, Firewalls, IDS, and Anti-Virus software.
- NAC enables administrators to monitor the internal network at any given time including endpoint devices, users, and access requests.
- NAC is a cost-effective network security solution as the detection and remediation of security threats can be automated.

Results

- Restrict network access until users have logged in as a valid user through the captive portal.
- Provide DHCP and DNS IP addresses through PacketFence to endpoint devices.
- Manage Cisco Switches through PacketFence to manually block endpoint device access.



Conclusions

- Integrating PacketFence as NAC solution has improved the security posture in a virtual network environment.
- Our comparative overview of NAC vendors has enabled us to conclude that each solution offer similar functionalities such as improved network security, more visibility and simplified network management. The deciding factors that should be considered are identifying the security requirements, existing infrastructure and budget.

Acknowledgments

I would like to acknowledge my first semester supervisor (Hamdan Awan), second semester supervisor (Roland Katona) and my year co-coordinator Noreen Gubbins for assisting me throughout this project.