Checkpoint Architecture & Design

Purpose:

The purpose of this video is to implement centralized authentication using RADIUS, where Active Directory (on DC1) serves as the authentication server, and the pfSense security appliance (UTM1 VM) acts as the RADIUS client. This scenario focuses on authenticating administrative users managing the pfSense firewall appliance.

Tools Used:

1. Active Directory on DC1 - Serving as the authentication and RADIUS server.
2. pfSense Security Appliance (UTM1 VM) - Configured as a RADIUS client.
3. Network Policy Server (NPS) - Used to configure RADIUS clients and policies.
4. Browser - Accessed to configure the pfSense VM.

Steps to Manage Centralized Authentication:

1. Register RADIUS Client:

- Open Network Policy Server on Server Manager.
- Navigate to RADIUS Clients > New.
- Enter Friendly name (T pfsense.corp.515support.com), Address (10.1.0.254), and generate Shared Secret.
- Copy shared secret.

2. Configure Network Policy:

- Create a new Network Policy named "pfSense Network Security Appliance Administration."
- Add conditions for the LocalAdmin security group.
- Specify Access Permission as Access granted.
- Configure Authentication Methods with MS-CHAPv2.
- Add a Class attribute to transmit LocalAdmin group membership.

3. Configure RADIUS Client on pfSense VM:

- Log in to the pfSense VM.
- Navigate to System > User Manager > Authentication Servers.
- Add a RADIUS server with Descriptive name (AD 515support), Type (RADIUS), Server Settings (IP: 10.1.0.1, Shared Secret: Paste from Clipboard).

4. Configure Role-Based Permissions:

- Create a LocalAdmin group.
- Assign minimal privileges by excluding WebCfg-pfSense wizard subsystem.
- Save settings and logout.

5. Test Credentials:

- Log in with non-administrator credentials (e.g., bobby, PaSSword).
- Verify limited access, demonstrating successful RADIUS authentication.
- Confirm if Bobby's user account is a member of the LocalAdmin group.