Scenariusz testów odbiorczych systemu NAC:

Uwierzytelnianie i dostęp:

1. **Test uwierzytelniania 802.1X (EAP-PEAP / EAP-TLS):** Podłączenie komputera w domenie Windows z poprawnie skonfigurowanym supplicantem – oczekiwane zalogowanie użytkownika i przypisanie VLAN. Próba zalogowania użytkownika z nieprawidłowym certyfikatem – oczekiwane odrzucenie.
2. **Test urządzenia spoza domeny:** Podłączenie komputera, który nie jest członkiem domeny Active Directory – oczekiwane odrzucenie uwierzytelnienia i brak dostępu do sieci przewodowej i/lub bezprzewodowej.
3. **Test dodania urządzenia na podstawie adresu MAC:** Rejestracja urządzenia (np. drukarki lub IoT) w systemie NAC na podstawie adresu MAC – przypisanie do odpowiedniej polityki dostępu i VLAN, zgodnie z konfiguracją administratora.
4. Test Captive Portal: Podłączenie urządzenia BYOD – przekierowanie do portalu, rejestracja użytkownika, potwierdzenie SMS/email i uzyskanie dostępu. Rejestracja użytkownika przez Captive Portal jako „gość" z limitem np. 1 godziny. Weryfikacja czy dostęp wygasa po upływie tego czasu.
5. Test polityki dostępowej (role/VLAN): Sprawdzenie czy użytkownik z określoną rolą trafia do właściwego VLAN. Sprawdzenie przypisywania VLAN po zmianie roli.
6. Test dla urządzeń nieobsługujących 802.1X: Podłączenie drukarki lub urządzenia IoT – przydział VLAN na podstawie adresu MAC (zgodnie z polityką).

Integracja i zgodność z polityką

1. **Test integracji z AD i PKI:** Sprawdzenie poprawnego logowania użytkowników z AD. Weryfikacja ważności certyfikatów X.509, obsługa CRL/OCSP. Użytkownik próbuje się uwierzytelnić z certyfikatem, który stracił ważność. Oczekiwane odrzucenie po stronie NAC. Weryfikacja poprawności logu i alertu.
2. **Test inspekcji i raportowania:** Przejście procesu rejestracji i logowania – weryfikacja czy zdarzenia są zapisywane w logach. Generowanie raportu zgodności z polityką.
3. **Test wsparcia supplicanta:** Weryfikacja poprawnej konfiguracji GPO dla stacji roboczych w domenie.

Środowisko rozproszone i HA

1. **Test działania w środowisku rozproszonym:** Odłączenie jednej lokalizacji od centrali – weryfikacja lokalnej dostępności usług NAC i autoryzacji.
2. **Test autoryzacji przez WiFi w lokalizacjach podległych:** Podłączenie klienta bezprzewodowego (WiFi) w lokalizacji podległej – weryfikacja poprawnej autoryzacji 802.1X (EAP-TLS) oraz przypisania VLAN zgodnie z polityką dostępu. Dodatkowo: test autoryzacji urządzenia infrastrukturalnego (np. AP Aruba) po certyfikacie w lokalizacji podległej.
3. **Test awarii i przywrócenia głównego kontrolera NAC:** Symulacja całkowitej awarii głównego kontrolera (centralnej instancji NAC) – weryfikacja poprawności działania lokalnych instancji w lokalizacjach podległych. Następnie – ponowne uruchomienie głównego kontrolera i sprawdzenie synchronizacji danych, poprawności działania całego systemu oraz braku negatywnego wpływu na trwające sesje i przyszłą autoryzację.

4. **Test mobilności użytkownika między lokalizacjami:** Użytkownik autoryzuje się w jednej lokalizacji, a następnie przenosi do innej (inny NAC w lokalnym HA). Sprawdzenie, czy polityka dostępu i przypisanie VLAN pozostaje zgodne z oczekiwaniami.

Zarządzanie i administracja

1. **Test zarządzania:** Dostęp do panelu administracyjnego przez HTTPS. Sprawdzenie działania ról i ograniczeń uprawnień.
2. **Test awarii:** Symulacja awarii łącza z centralą – weryfikacja czy lokalny dostęp działa zgodnie z założeniami HA.
3. **Test alertów i powiadomień:** Symulacja naruszenia lub błędu systemowego – weryfikacja, czy administrator otrzymuje powiadomienie zgodnie z konfiguracją.

Reakcje bezpieczeństwa i inspekcja

1. **Test wykrycia naruszenia polityki bezpieczeństwa**: Wymuszenie naruszenia (np. prób ataku ARP spoofing z końcówki lub brak aktualizacji antywirusa). Oczekiwane działanie: izolacja stacji do VLAN kwarantanny oraz wygenerowanie logu incydentu.