RADIUS: WPA2-Enterprise With EAP-TLS Using Microsoft NPS

WPA2-Enterprise with 802.1x authentication can be used to authenticate users or computers in an Active Directory domain. The supplicant (wireless client) authenticates against the RADIUS server (authentication server) using an EAP method configured on the RADIUS server. The gateway APs (authenticator) role is to send authentication messages between the supplicant and authentication server. This means the RADIUS server is responsible for authenticating users.

APs perform EAPOL exchanges between the supplicant and convert these to RADIUS Access-requests messages which are sent to the RADIUS servers IP address and UDP port specified in Dashboard. Gateway APs need to receive a RADIUS Access-accept message from the RADIUS server in order to grant the supplicant access to the network. For best performance, it is recommended to have the RADIUS server and gateway APs located within the same layer-2 broadcast domain to avoid firewall, routing, or authentication delays. Keep in mind the AP is not responsible for authenticating wireless clients and acts as an intermediary between clients and the RADIUS server. Below is an EAP-TLS exchange,

EAP-TLS authentication

Wireless, LAN (WLAN), EAP-TLS Deployment Guide for Wireless LAN Networks,

Courtesy of Cisco Systems Inc.
EAP-TLS authentication details

Using EAP-TLS as the EAP method will consistently cause the RADIUS test in Dashboard to fail. When troubleshooting this configuration, please refer to packet captures and logs for specific information.

EAP-TLS is an involved configuration, please refer to your RADIUS vendor documentation for configuration specifics. Once RADIUS has been configured appropriately, please refer to our documentation for instructions on configuring an SSID for WPA2-Enterprise with RADIUS.

Wireless, LAN (WLAN), EAP-TLS Deployment Guide for Wireless LAN Networks,

Courtesy of Cisco Systems Inc.