Schools network security and performance improvements

Background

A school district providing IT services to schools were refreshing all network equipment offering an opportunity to improve on the existing security practice.

Four WLANs were offered in each school:

- CurricISE – WPA2-Enterprise - intended for school owned devices
- CurricMobile – WPA2-Enterprise - Intended for BYOD
- CurricApple – WPA2-Enterprise - Setup for iOS devices but functionally identical to CurricMobile
- Guest – Open - Captive portal restricted guest access

Some schools also had additional local SSIDs for 'special' devices.

Each WLAN statically assigned clients to separate VLANs in one of two Virtual Routing & Forwarding instances (VRF): Curriculum and Public. The Public VRF was intended for BYOD and Guest devices and routed internet bound traffic through a transparent content filtering proxy. The Curriculum VRF was intended for all school owned devices.

The original aim was to ensure separation of traffic for BYOD/Guest providing internet access with no route to central services. The three 'Curric' WLANs used EAP-PEAP for authentication to a central RADIUS server which forwarded requests to the local AD server in the appropriate school based on a Network Access Device (NAD) address group. Users connecting to APs SchoolA would only be authenticated against the SchoolA server. This configuration ensured users could only authenticate when on their home site.

The RADIUS server had no mechanism to determine the type of device so any network security relied entirely on client supplicants being appropriately configured. All school owned iPads and Chromebooks were connecting to either CurricApple or CurricMobile so were placed in the Public VRF preventing access to shared devices in the Curriculum VRF.

This security design didn't anticipate the growth of shared resources e.g. airplay screen sharing. As a result, AppleTVs and Smartboards had been placed in the Public VRF in order to be accessible by iPads and Chromebooks however this meant they couldn't be accessed by the school's Windows laptops or desktop machines in the Curriculum VRF

Having four SSIDs contributed to management traffic overhead, reducing the network capacity. Roaming performance was particularly poor with no handoff enhancements enabled and clients therefore having to go through the full 802.1X authentication for any roaming event.

Implemented changes

Two SSIDs were deployed: an open Guest WLAN, with captive portal, and a WPA2-Enterprise EDU network. All non-guest clients were configured to use the EDU network which used a single VLAN in

the curriculum VRF. Role Based Access Control was employed to limit the access of clients in the EDU WLAN based on the role attribute returned by RADIUS.

The centrally managed RADIUS server was replaced with a more sophisticated policy manager which allowed authentications to be tagged based on AD group membership, client device type and other characteristics such as whether the device has performed a successful machine auth.

School owned iPads and Chromebooks were assigned AD users, placed in a specific AD group and this group was used to identify these devices in order to differentiate school owned and BYOD clients. By placing all devices in the same VRF and using RBAC I could control which clients were able to communicate with the AppleTV or Smartboards.

Clients were assigned one of the following roles

AD-Managed – Windows laptop in AD – assigned to clients after successful machine auth
School-Device – iPad/Chromebook – user is a member of the School-Device AD group
BYOD-Staff – BYOD device – user is a member of staff AD group and device is unknown
BYOD-Student – BYOD device – user is not a member of staff group and device is unknown

An Access Control List (ACL) for each role dictated what a client could do e.g. clients in the AD-Managed role were able to access local and centralized servers. Clients in the BYOD-Student were permitted only internet access with BYOD-Staff and School-Device roles also allowed access to Audio-Visual wired network subnet.

The AD implementation was complex with 80 separate domains, one for each school. I configured the new RADIUS server to authenticate against the appropriate local server based on the user domain. This allowed any client with valid credentials to connect at any site.

Although planned for a future date there was no Mobile Device Management, Public Key Infrastructure or onboarding solution in place. This ruled out the use of EAP-TLS. Manually configured user devices will default to EAP-PEAP so this was used by necessity.

Default settings for EAP-PEAP on most clients results in the real username populating the outer/PEAP-Phase1 credentials, rather than a bogus entry (this credential is not used for user authentication). This is sent in clear text prior to the client validating the authentication server certificate making it trivial to harvest usernames by capturing authentication packets.

Use of EAP-PEAP without MDM or an onboarding process means clients will not be able to validate the RADIUS certificate, requiring users to manually trust this. Such a practice opens an attack surface using a rogue AP and authentication server as the connection process effectively trains users to just accept the RADIUS certificate when challenged. An attacker can harvest usernames and hashed passwords. The preferred use of EAP-TLS would replace user/pass with a client certificate. With this EAP method the client must accept the authentication server certificate before sending its own. Using MDM to deploy certificates and configure the client to fail if it can't validate the RADIUS server certificate, rather than provide an override option to the user, allows for a highly secure authentication solution.

Fast BSS Transition was enabled on the EDU SSID with users immediately providing feedback the roaming experience was significantly improved.

The result was a more flexible network that better met the needs of schools, reduced the likelihood of unmanaged rogue networks being deployed and the ability for users to connect at any site.

Security was improved with BYOD clients recognised as such and assigned a role restricting access to central servers.