Ubiquiti Unifi – eine saubere Netzwerkgeschichte

Lange Zeit war es still in diesem Blog. Dies lag oder liegt vor allem daran, dass ich vermehrt an der Endkunden-Front unterwegs bin und somit weniger Zeit finde zum Schreiben.
Vor gut zwei Wochen verabschiedete sich meine gut siebenjährige ZyWALL in den ewigen Elektronenhimmel und es musste Ersatz her. Ich war mit meinem Heimnetz, welches auch ein Testnetzwerk und Wifi umfasst noch nicht wirklich warm geworden. Ein Arbeitskollege musste wegen eines Brandfalles sein komplettes Netzwerk ersetzen und schwärmte dabei von Ubiquiti. Ubiwas?

Die Firma Ubiquiti Networks wurde 2005 mit lediglich einer Vision und einem Kapital von 30’000USD gegründet. 2010 brachte die Firma die Unifi Serie heraus, mit welcher ich mich nun auch befasst habe. Innerhalb dieser Serie gibt es eine Unmenge an Switches, Access Points und sonstigem Netzwerkkram, was es schon zu Hauf auf dem Markt gibt, notabene auch günstiger.
Was macht diese Unifi Geräte nun so besonders? An der Hardware wird es kaum liegen, denn Design ist Geschmackssache und über Geschmäcker lässt sich streiten. Also muss es an der Software liegen. Verbindet man sich dann aber z.B. mit einem Switch stellt man fest, dass dieser nur über eine CLI Oberfläche verfügt. Warum soll man sich das nun also antun?

Der grösste Vorteil an diesen Geräten ist, dass man dazu gratis eine Controller-Software herunterladen kann. Diese ist für Windows, MAC oder Linux erhältlich. Letztere auch als eigenständiges Produkt, dem Cloud-Key. Dieses USB-Device kann man an einen der PoE Switche anschliessen und die Controller Software läuft dann auf diesem autonom.
Ich habe den Controller aktuell auf einem Windows System installiert. Nach der Konfiguration müsste der

Controller theoretisch nicht mehr laufen, er bietet jedoch ein paar nette Funktionen an wie z.B. ein Gast-WLAN inkl. Anmeldeportal.

Welche Komponenten habe ich nun aus welchem Grund für mein Heimnetz angeschafft, obwohl nur die Firewall zu ersetzen gewesen wäre?

UniFi® Security Gateway (USG)
Wie es der „Gateway“ im Namen schon sagt, ist dies der Zugang ins Internet. Der USG ist einerseits ein Router mit den üblichen Funktionen Routing, DHCP Server, Firewall etc. bildet jedoch auch ein Kern im Aufbau des Unifi Netzwerkes. Das komplizierteste an der Konfiguration war hier, dass ich nicht das Standard Subnetz 192.168.1.0/24 verwenden wollte. In diesem Fall muss der Controller vorher aufgesetzt werden (war meiner bereits) und die USG über CLI mit einer IP im definierten Subnetz konfiguriert werden. Die Beschreibung ist hier zu finden:
https://help.ubnt.com/hc/en-us/articles/236281367-UniFi-How-to-Adopt-a-USG-into-an-Existing-Network
Dies wäre theoretisch das einzige Gerät, welches ich nach dem Ausfall meiner Firewall benötigt hätte. Das Routing etc. macht der USG auch ohne Probleme, jedoch ist im Bereich Firewall noch Entwicklungspotential. Für den Heimbereich und auch in kleineren Firmen absolut brauchbar. Wer jedoch komplexe Firewallregeln, Policy Based Routing, QoS etc. benötigt sollte vorerst ein anderes Gerät wählen.

UniFi® Switch 8-60W
Ich hätte auch meine bisherigen kleinen Netgear Switche im

Einsatz behalten können, jedoch haben mich diese „gemanagten“ Switche in Sachen VLAN entäuscht. Daher habe ich alle für mich relevanten Switche durch das genannte Modell ersetzt. Wegen dem Access Point und dem VoIP Telefon wählte ich ein PoE Modell. Im Büro hätte es auch eines ohne PoE getan, jedoch war der Preisunterschied minimal. Dieser 8-Port-Switch bietet nun 8 verwaltbare Gbit-Ports, wobei vier Ports PoE fähig sind bis zu einer Maximal-Leistung von 60W. Ich habe mir auch den 16-Port Switch angeschaut, jedoch war der teurer wie zwei der kleinen.

UniFi® AP AC PRO
Der Access Point (AP) der PRO Serie sollte meinen kleinen ZyXEL AP ersetzen, welcher wie die ZyWALL schon in die Jahre gekommen ist. Von Ubiquiti gäbe es noch günstigere APs jedoch habe ich mich aus folgenden Gründen für diesen entschieden:
– Dualband (2,4/5GHz) fähig
– VLAN fähig (nicht nur auf dem Papier)
– mehrere unabhängige SSIDs aufschaltbar (max. 4)
– Gäste WLAN fähig
Basierend auf den genannten Punkten sind bei mir nun auch ein produktives WLAN und ein WLAN für Gäste konfiguriert. Zweiteres ist auf einem definierten Gäste-VLAN, welches auch nur den Internet-Zugang zulässt. Als kleines Schmankerl muss ein Benutzer des Gäste-WLANs sich auch mittels separatem Passwort auf einer Portalseite anmelden, wie man es auch aus Hotels kennt.

Anmerkung
Es ist anzumerken, dass jede Geräteklasse für sich angeschafft und betrieben werden kann. Im Verbund jedoch da zeigen sie ihre Stärke. Wenn z.B. ein neues Netzwerk (VLAN) inkl. DHCP Server benötigt wird, wird dieses im Kontroller angelegt, den Switches/Ports und ggf. WLAN zugewiesen und ausgerollt. Anschliessend sind alle Geräte im Verbund fix fertig konfiguriert und es kann gearbeitet werden. Wenn man im Vergleich dazu erst das VLAN erstellen, die einzelnen

Switches/Ports konfigurieren muss, dann hat man je nach Netzwerkgrösse ein arbeitsreiches Wochenende vor sich…

Resumee

Nach nun rund zwei Wochen im Betrieb bin ich noch voll zufrieden. Alles in allem eine vollwertige Lösung, die an der einen oder anderen Ecke noch Verbesserungspotential hat:

+ mehrheitlich intuitive Controller-Software (für IT Leute)
+ einfache Konfiguration
+ auf einander abgestimmte Komponenten
+ Preis/Leistung
– sehr rudimentäre Firewall
– Installation der Controller-Software im Benutzerprofil statt System