Abschlussprüfung Winter 2020/2021

Fachinformatiker für Systemintegration

Dokumentation zur Projektarbeit

Projektdokumentation:

Aufbau eines Heimnetzes

Abgabedatum: [redacted] 02.12.2020

Prüfungsbewerber:

Daniel Daum

[redacted]

Ausbildungsbetrieb:

Externer Prüfling

Inhaltsverzeichnis

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AP ..... Access Point

DAC ..... Direct Attached Copper

DSL ..... Digital Subscriber Line

GUI..... Graphical User Interface

GW..... Gateway

IoT..... Internet of Things

IP ..... Internet Protocol

LAN..... Local Area Network

MIMO ..... Multiple Input Multiple Output

NAS..... Network Attached Storage

NAT..... Network Address Translation

PoE ..... Power over Ethernet

SFP ..... Small Form-factor Pluggable

SSID ..... Service Set Identifier

TAE..... Telekommunikations-Anschluss-Einheit

VLAN..... Virtual Local Area Network

VPN..... Virtual Private Network

WAN ..... Wide Area Network

WLAN..... Wireless Local Area Network

WPA ..... Wi-Fi Protected Access

1 Definitionsphase

1.1 Projektumfeld

Das Projekt habe ich im Privathaus des Kunden durchgeführt. Es handelt sich um ein Reihenhaus mit zwei Etagen sowie einem Keller und ca. 100m^2 Wohnfläche.

Aus Gründen des Datenschutzes habe ich in diesem Dokument IP-Adressen und Passwörter unkenntlich gemacht.

1.2 Zielsetzung

Angesichts der durch die Corona-Pandemie bedingten Verlegung der Arbeit des Kunden in das Homeoffice und der hierdurch gestiegenen Ansprüche an das Heimnetzwerk ist das Ziel dieses Projekts, ein modernes und sicheres Netzwerk aufzubauen sowie eine hausweite Abdeckung mit schnellem und stabilem WLAN zu gewährleisten.

1.3 Ist-Analyse

Das bisherige Netzwerk im Privathaus des Kunden besteht aus einer AVM FritzBox 7490 sowie einem AVM FritzRepeater 1750E, der als WLAN-Brücke eingerichtet ist. Im Netzwerk befinden sich drei Laptops, zwei Smartphones, ein Tablet und IoT-Geräte (z.B. Rolladensteuerung). Zusätzlich wählen sich regelmäßig Gäste mit mobilen Endgeräten in das Netzwerk ein. Der Kunde berichtete im Gespräch, dass die hausweite WLAN-Abdeckung nicht zufriedenstellend sei, da unter anderem in der Küche und im Keller kein ausreichender WLAN-Empfang gewährleistet sei.

2 Planungsphase

2.1 Soll-Konzept

Es soll ein neuer Router installiert werden und die bereits vorhandene FritzBox nur noch als Modem fungieren. Im Wohnzimmer und im Heimbüro des Kunden soll jeweils eine doppelte Netzwerkdose installiert werden. Das WLAN soll über zwei Power over Ethernet (PoE)-fähige Accesspoints realisiert werden. Hierzu wird auch noch ein Switch angeschafft, der PoE unterstützt sowie über ausreichend Ports für zukünftige Erweiterungen wie ein Network Attached Storage (NAS) und/oder IP-Kameras verfügt. Für Besucher soll es ein Gastnetzwerk geben sowie ein VLAN für IoT Geräte. Angesichts der vermehrten Arbeit von zuhause benötigt der Kunde ein stabileres WLAN für Videokonferenzen und Live-Online-Trainings mit bis zu hundert Teilnehmenden. Eine VPN-Verbindung in das Netzwerk soll ebenfalls möglich sein.

2.2 Projektschnittstellen

Da keine anderen Gewerke in der Durchführung des Projekts beteiligt waren, ergaben sich die Schnittstellen nur zwischen dem Kunden und mir sowie den Lieferanten der Hardware und Verbrauchsmaterialien. Da ich durch meine vorherige Ausbildung eine Elektrofachkraft bin, habe ich die benötigten Installationsarbeiten im Haus des Kunden selbst durchgeführt.

2.3 Zeitplanung

Phase	Stunden	Gesamt
Definitionsphase		5
Ist-Analyse	1	
Marktrecherche	2	
Produktvergleich	2	
Planungsphase		5
Soll-Konzept	2	
Hardwareangebote einholen	2	
Angebot erstellen	1	
Durchführungsphase		16
Hardware bestellen	1	
Aufbau der Hardware und Verkabelung	5	
Einrichtung und Konfiguration	8	
◦ Einrichtung des Routers		
◦ Einrichtung der Firewall		
◦ Einrichtung der VLANs		
◦ Einrichtung des VPNs		
◦ Einrichtung des WLANs		
Funktionstest	2	
Abschlussphase		9
Qualitätskontrolle / Fehlerbehebung	3	
Erstellen der Rechnung	0,5	
Gewinn ermitteln	0,5	
Erstellung der Dokumentation (Betriebs- und Kundendokumentation)	5	
GESAMTSTUNDEN		**35**

Tabelle 1 Grobe Zeitplanung

3 Durchführungsphase

3.1 Auswahl der Hardware

3.1.1 Entscheidung Router

In der folgenden Übersicht habe ich zwei Router miteinander verglichen und in einer Entscheidungsmatrix bewertet. Besonderes Augenmerk lag hierbei auf dem Preis und der Leistung. Die Funktionen des Routers sollten des Weiteren nicht an ein Abo-Modell gebunden sein. Zudem sollte der Router sich in einem 19 Zoll Rack verbauen lassen. Ein 19 Zoll Rack wurde gewählt, um alle Hardwarekomponenten platzsparend und ordentlich an einem Ort zu haben. Aufgrund dieser Kriterien kamen die Router UniFi Dream Machine Pro und Netgate XG-7100 1U in die engere Auswahl.

Gewichtung	Features	Unifi Dream Machine Pro	Netgate XG-7100 1U
3	Preis	3	1
1	Open Source	1	3
3	Leistung	2	3
2	GUI	3	2
1	Design	3	1
2	2* 10G SFP+	3	3
Gesamt		**31**	**26**

Tabelle 2 Entscheidungsmatrix Router

Die Entscheidung fiel auf den Router UniFi Dream Machine Pro (ca. 319€), da dieser sich in den geforderten Punkten klar von dem Router Netgate XG-7100 1U (ca. 900€) absetzen konnte.

3.1.2 Entscheidung Access Point

Aufgrund der bereits getroffenen Wahl der UniFi Dream Machine Pro als Router wurde im nächsten Schritt die Entscheidung getroffen, bei dem Switch und den Access Points (APs) auch auf Produkte von Ubiquiti aus der UniFi Serie zu setzen. Dies hat den entscheidenden Vorteil, dass sich alle Geräte von dem UniFi Network Controller managen lassen, welcher bereits in der UDM Pro integriert ist. Hinsichtlich der Access Points habe ich zwei Produkte aus der UniFi Serie miteinander verglichen. Wie aus der nachfolgenden Entscheidungsmatrix ersichtlich wird, lag das Hauptaugenmerk auf den Abmessungen sowie auf der Leistung. Weitere Kriterien waren der Preis, MIMO sowie die Anzahl der maximalen User (‚Max Users'). Weniger wichtig war das Kriterium Ports, weil diese für den Anwendungsfall des Kunden nicht relevant sind.

Gewichtung	Features	UniFi AC Pro	UniFi nanoHD
2	Preis	3	2
3	Abmessungen*	2	3
3	Leistung	2	3
2	MIMO	1	3
2	Max Users	2	3
1	Ports	3	1
Gesamt		**27**	**35**

*kleiner = besser

Tabelle 3 Entscheidungsmatrix APs

Ich habe mich für den UniFi nanoHD entschieden, da er für den gewünschten Anwendungsfall zu einem unwesentlich höheren Preis (von 149€ im Vergleich zu 119€ für den UniFi AC Pro) das bessere Gerät darstellt. Die UniFi nanoHD Access Points unterstützen die aktuellen Sicherheits- und Signalstandards.

3.1.3 Entscheidung Switch

Wie bereits erwähnt, sollte der Switch auch von Ubiquiti aus der UniFi Serie stammen. Die Wahl des Switches fiel auf den UniFi Switch Pro 24 PoE, da dieser über 16 PoE+ und 8 PoE++ Ports mit jeweils 1Gigabit sowie zwei 10G SFP+ Ports verfügt sowie ein Maximum von 400W PoE power zur Verfügung stellen kann. Des Weiteren besitzt er Layer 2 und 3 Features und ist somit insgesamt für mögliche zukünftige Erweiterungen des Netzwerks (IP-Kameras, NAS, APs) des Kunden bestens gerüstet.

3.1.4 DSL Modem

Entgegen des ursprünglichen Projektantrags habe ich mich in der Durchführungsphase für ein dediziertes DSL-Modem entschieden, um doppelte Network Address Translation (NAT) zu vermeiden. Die vorhandene FritzBox ist somit ausschließlich für die DECT Telefonie zuständig. Bei dem ausgewählten Modem handelt es sich um ein DrayTek Vigor165. Bei der Auswahl des DSL-Modems war vor allem die Leistungsfähigkeit ein wichtiges Kriterium, weswegen ich mich für das DrayTek Vigor165 entschieden habe.

3.1.5 UniFi Network Controller

Der UniFi Network Controller ist der zentrale Anlaufpunkt, um die UniFi Geräte zu administrieren. Über ein Webinterface lassen sich Netzwerkstatistiken aufrufen, Softwareupdates einspielen, VLANs anlegen und WLANs erstellen. Zudem kann man Regeln für die Firewall definieren und VPNs erstellen.

3.1.6 Bestellung

Ich habe dem Kunden meine Auswahl der Hardware präsentiert und dabei sowohl die Kosten als auch den Nutzen aufgezeigt. Ich habe meinen Auswahlprozess erklärt und ihm kurz die Funktionen der verschiedenen Geräte erläutert. Zudem legte ich dar, weshalb es meiner Meinung nach sinnvoll ist, komplett auf das UniFi-System zu setzen. Der Kunde teilte meine Auffassung und erteilte mir den Auftrag. Mit Auftragserteilung leitete ich die Bestellung der

entsprechenden Hardwarekomponenten bei diversen Anbietern ein. Tabelle 6 in Kapitel 4 bietet eine detaillierte Darstellung aller bestellten Hardwarekomponenten mit Preisen und Lieferanten.

3.2 Aufbau der Hardware und Verkabelung

3.2.1 Planung

Mit dem Kunden wurde besprochen, wo das Rack mit der Hardware aufgebaut werden soll und wo die APs sowie die Netzwerkdosen angebracht werden sollen. Es wurde sich darauf geeinigt, das Rack im Keller des Wohnhauses aufzubauen. Diese Entscheidung hatte zum einen ästhetische Gründe und zum anderen kann so gewährleistet werden, die Geräuschkulisse im Wohnbereich des Hauses durch die Lüfter des Switches und des Routers nicht negativ zu beeinflussen. Eine TAE-Dose für den DSL-Anschluss ist in dem gewählten Kellerraum vorhanden, sodass ein Aufbau im Keller problemlos möglich war.

Im Wohnzimmer des Kunden sollte eine doppelte Netzwerkdose gesetzt werden und einer der beiden Access Points an die Decke montiert werden. Im Obergeschoss wurde sich darauf verständigt, den zweiten Access Point direkt im Büro zu installieren (ebenfalls Deckenmontage). Auch in diesem Raum soll eine doppelte Netzwerkdose gesetzt werden. Die doppelten Netzwerkdosen werden in beiden Räumen installiert, um dem Kunden bei Bedarf eine Verbindung per Netzwerkkabel zu ermöglichen.

3.2.2 Durchführung

Da im Haus des Kunden bisher noch kein Netzwerkkabel vorhanden war, musste ein solches neu verlegt werden. Hierzu wurden für die Kabeldurchführung zwei Bohrungen durch den Wohnzimmerboden in den Keller vorgenommen. Für die Durchführung der Kabel in das Obergeschoss reichte eine Bohrung durch die Wohnzimmerdecke. Im Anschluss wurde das Kabel durch die Bohrungen gezogen und in Kabelkanälen verlegt. Insgesamt wurden sechs Kabel benötigt, davon drei im Wohnzimmer für den Access Point und die Doppeldose sowie drei weitere im Büro, ebenfalls für den Access Point und die Doppeldose. Bei dem Netzwerkkabel handelt es sich um ein Cat 7A Kabel. Dieses Kabel wurde genommen, um gegebenenfalls zu einem späteren Zeitpunkt auf ein 10G Netzwerk umsteigen zu können. Die Netzwerkdosen, Feldstecke (zum Anschluss der APs) und Keystone Module wurden nach EIA/TIA-568A aufgelegt und die Verbindungen mit einem Netzwerkkabeltester überprüft. Im Anschluss wurde das Rack im Keller aufgebaut und mit dem Router, Switch, Modem und Patchpanel bestückt. Das Patchpanel wurde dann mit den Keystone Modulen bestückt und via Patchkabel mit dem Switch verbunden. Der Switch wurde mit einem DAC-SFP-Kabel über den 10G SFP Port mit dem Router verbunden. Im Anschluss montierte ich die Access Points an der Decke im Wohnzimmer und Büro und schloss diese an.

3.3 Modem: Anschluss und Konfiguration

Das gewählte DrayTek Vigor165 ist von Werk her schon als Modem konfiguriert. Ich habe es dennoch an meinen PC angeschlossen, um dies zu überprüfen und ggf. Updates zu installieren. Wie erwartet war das DrayTek Vigor165 bereits als Modem konfiguriert. Für die weitere Überprüfung vergab ich dem Ethernetadapter meines Laptops die IP 192.168.1.10/24. Das Web-Interface erreicht man unter 192.168.1.1 und die Zugangsdaten lauten:

Username: admin
Passwort: admin

Als erstes habe ich das Standardpasswort geändert und die IP des Modems auf 192.168.1.254 gestellt, damit es nicht zu Konflikten mit dem Router kommt, der standartmäßig auch die IP 192.168.1.1 hat. Im Anschluss habe ich die Firmware des Modems aktualisiert. Danach schloss ich den DSL-Port an die TAE-Dose und schloss LAN1 an den WAN-Port des Routers.

3.4 Router: Anschluss und Konfiguration

Nachdem die Spannungsversorgung für Router und Switch hergestellt war, schloss ich meinen Laptop via LAN an den Router an. Unter der Adresse 192.168.1.1 rief ich das Webinterface des Routers auf. Dort gab ich die Zugangsdaten des DSL-Anschlusses ein (siehe Abbildung 1). Nach Eingabe der DNS-Server (ich habe mich für 1.1.1.1 und 9.9.9.9 entschieden) wurde eine Internetverbindung aufgebaut und ich wurde aufgefordert einen UniFi-Account zu erstellen, welches ich auch tat.

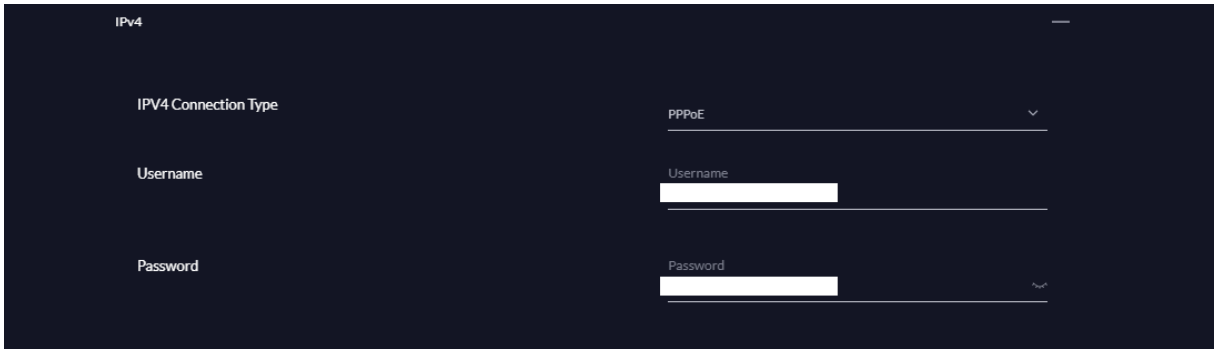

Abbildung 1 WAN Konfig

Danach wurde die aktuelle Firmware geladen und installiert. Nach dem Neustart wurden unter dem Menüpunkt „Devices“ alle UniFi Geräte im Netzwerk angezeigt. Hier musste ich noch die Access Points und den Switch adoptieren und die Firmware der Geräte aktualisieren. Als nächstes habe ich den Access Points einen eindeutigen raumbezogenen Namen gegeben und dem Router, dem Switch und den Access Points feste IPs zugewiesen.

Abbildung 2 Devices

3.5 Einrichtung LAN

Im nächsten Schritt habe ich das Hauptnetzwerk konfiguriert. Hierzu ging ich auf den Menüpunkt `Einstellungen – Netzwerk`. Dort habe ich die standardmäßig vergebene Netzadresse 192.168.1.0/24 auf den von mir gewünschten Netzbereich umgestellt.

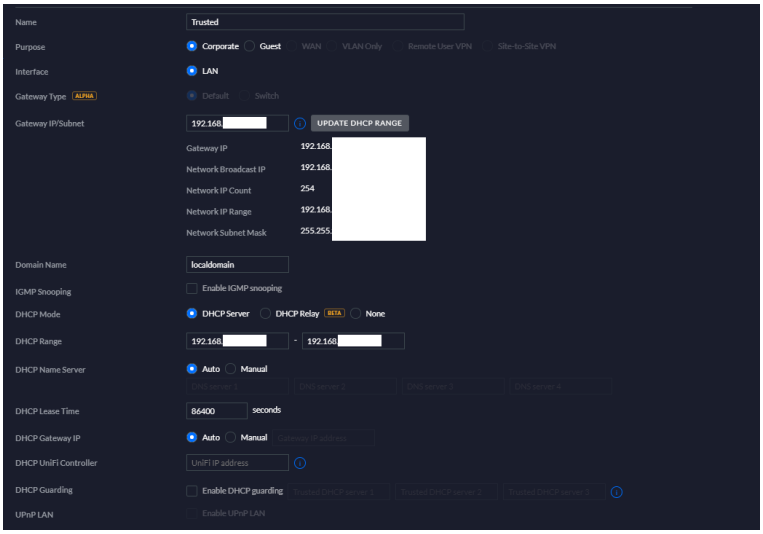

Abbildung 3 Hauptnetzwerk

3.6 Einrichtung VLANs

Nach der Einrichtung des Hauptnetzwerks richtete ich die VLANs „Guest“ und „IoT“ ein. Die Arbeitsschritte hierzu gleichen denen der Einrichtung des LAN mit der Ausnahme, dass ein VLAN Tag vergeben und ein anderer IP-Bereich gewählt wurde.

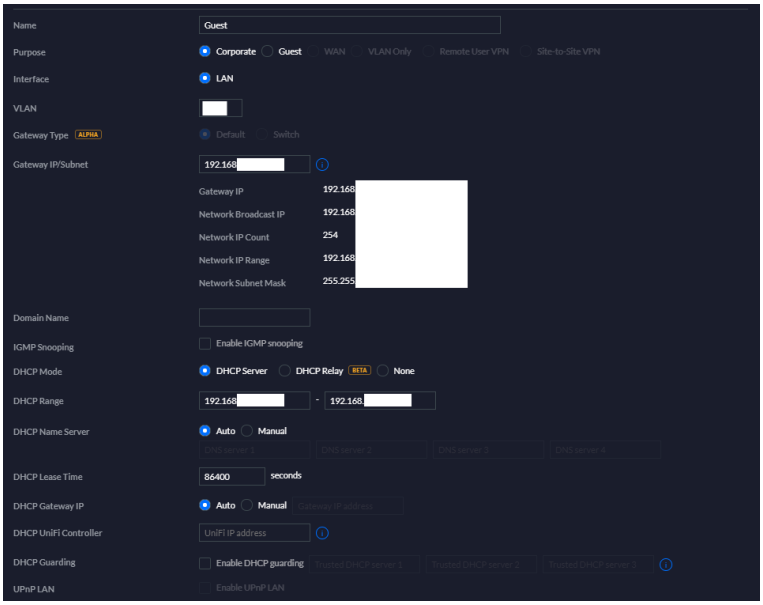

Abbildung 4 Einrichtung VLANs

3.7 Einrichtung WLAN

Um das WLAN nutzen zu können, musste ich im Controller ein oder mehrere WLANs erstellen. Dieses kann man unter `Einstellungen – Wireless Networks` tun. Ich habe für die drei vom Kunden gewünschten Netzwerke (Trusted, IoT, Guest) entsprechend drei WLANs angelegt und die dazugehörigen VLAN-Tags vergeben, damit die Clients IP-Adressen aus dem dazugehörigen Netz erhalten.

Netzwerk	SSID	WPA Personal	VLAN Tag
Trusted	Norwegen	yes	no
IoT	Schweiz	yes	yes
Guest	Finnland	yes	yes

Tabelle 4 WLAN

Das „Guest“ WLAN ist auf 20Mbit/s im Downstream und 5Mbit/s im Upstream begrenzt. Hierzu erstellte ich unter `Einstellungen – User Groups` eine User-Group „Guest“ und stellte die entsprechenden Limits ein. Im Anschluss wählte ich in den Einstellungen des WLANs „Finnland“ diese Gruppe aus.

3.8 Einrichtung Firewall

Im folgenden Schritt richtete ich die Firewall ein (`Einstellungen – Routing & Firewall – Firewall`). Ziel war es, das „IoT“ und „Guest“ Netzwerk voneinander und vom „Trusted“ Netzwerk zu isolieren. Zudem sollte man nicht von „Guest“ und „IoT“ auf das Gateway zugreifen können. Das „Trusted“ Netzwerk hat uneingeschränkten Zugriff auf alle Netze. Das „Guest“ Netzwerk soll zudem auf den Drucker zugreifen können. Um Inter-VLAN-Communication zu unterbinden, erstellte ich eine Gruppe, die den privaten IP-Bereich nach RFC1918 abdeckt. Danach fügte ich eine Regel für LAN IN hinzu, die alle Pakete von und zu diesen Netzen verwirft. Damit das „Trusted“ Netz weiterhin Zugriff auf alle VLANs hat, fügte ich eine Regel hinzu, die alle Pakete erlaubt, die vom „Trusted“ Netzwerk kommend ein Ziel im RFC1918 (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) Adressbereich haben. Damit diese Regel Anwendung findet, musste sie noch über die „Drop-Regel“ geschoben werden, da Firewallregeln in der Liste von oben nach unten abgearbeitet werden.

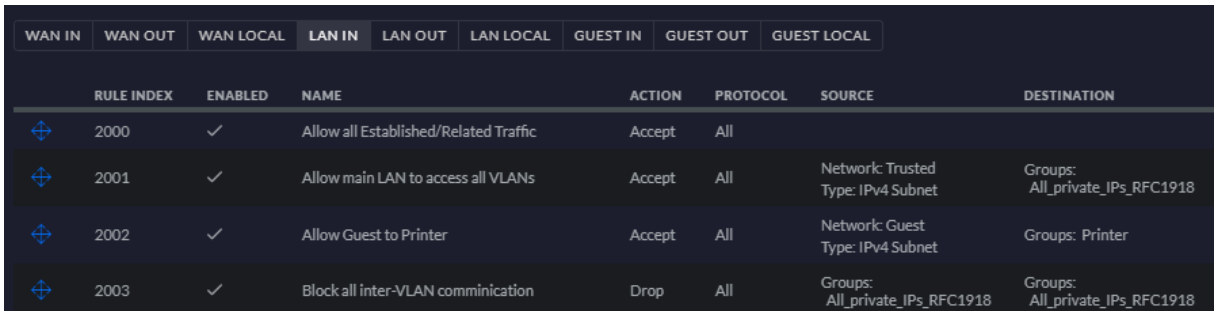

Abbildung 5 Firewallregeln LAN IN

Um den Zugriff der VLANs auf alle Gateways (GWs) außer dem Eigenen zu unterbinden, habe ich unter LAN LOCAL jeweils für „IoT“ und „Guest“ eine Regel erstellt, die alle Pakete aus dem entsprechenden Netz an alle GWs außer dem Eigenen verwirft. Um zu verhindern, dass man sich von den VLANs aus auf dem Router einwählen kann, habe ich http/s (Port 80/443) und ssh (Port 22) für die Adressen der GWs aus dem „IoT“ und „Guest“ Netz blockiert.

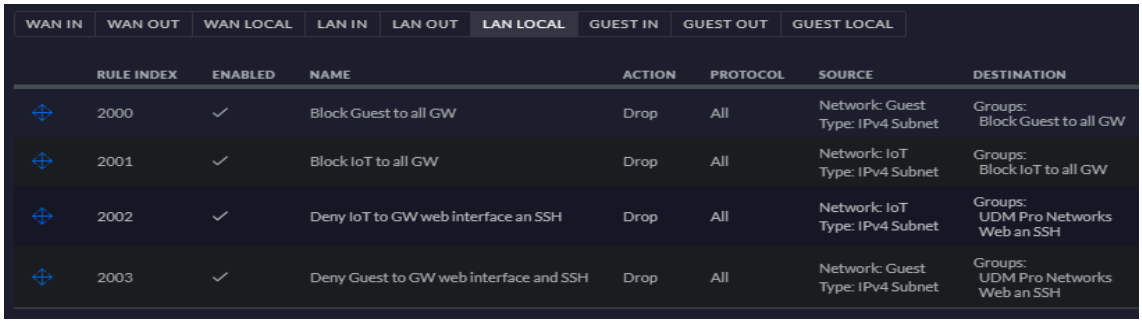

Abbildung 6 Firewallregeln LAN LOCAL

3.9 FritzBox SIP Port forwarding

Da die FritzBox 7490 weiterhin als Telefonanlage genutzt werden soll, musste ich sie für den Betrieb hinter einem Router konfigurieren. Hierfür wählte ich im Menü Internet – Zugangsdaten die Punkte `Anschluss an externes Modem oder Router` und `Vorhandene Internetverbindung mitbenutzen` aus. Danach deaktivierte ich das WLAN der FritzBox. Damit die Telefonie funktioniert, musste ich noch eine Portweiterleitung für den SIP-Traffic auf der UDM Pro einrichten. Hierzu leitete ich den SIP-Port (5060) auf die IP der FritzBox weiter.

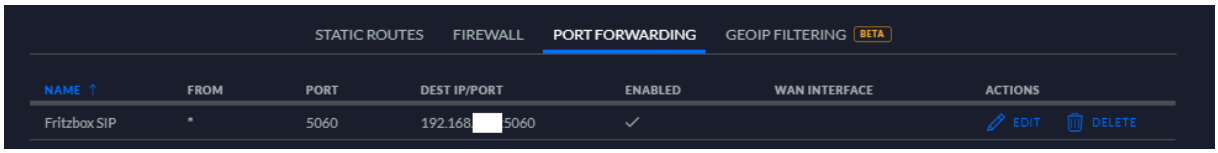

Abbildung 7 Port forwarding

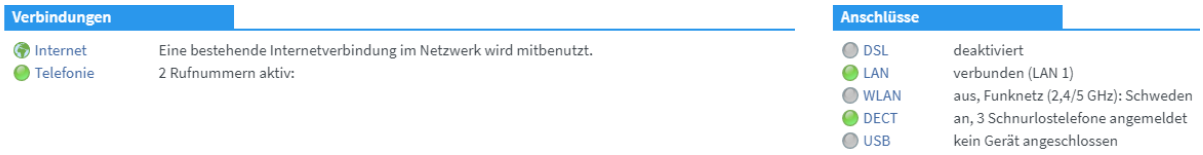

Abbildung 8 FritzBox Übersicht

3.10 Einrichtung VPN

Um auch nach der 24h Zwangstrennung der Internetverbindung durch den Provider und der damit einhergehenden neuen IP des Anschlusses auf das VPN zugreifen zu können, habe ich bei dem Anbieter noip.com eine DynDNS Adresse eingerichtet. Die Zugangsdaten habe ich dann in der UDM Pro eingetragen.

Abbildung 9 DynDNS

Danach habe ich den Radius Server aktiviert und einen User angelegt. Ich vergab ein sicheres Secret für den Radius Server und vergab einen Namen und ein Passwort für den User. Als Tunnel Type stellte ich L2TP ein und Tunnel Medium Type IPv4.

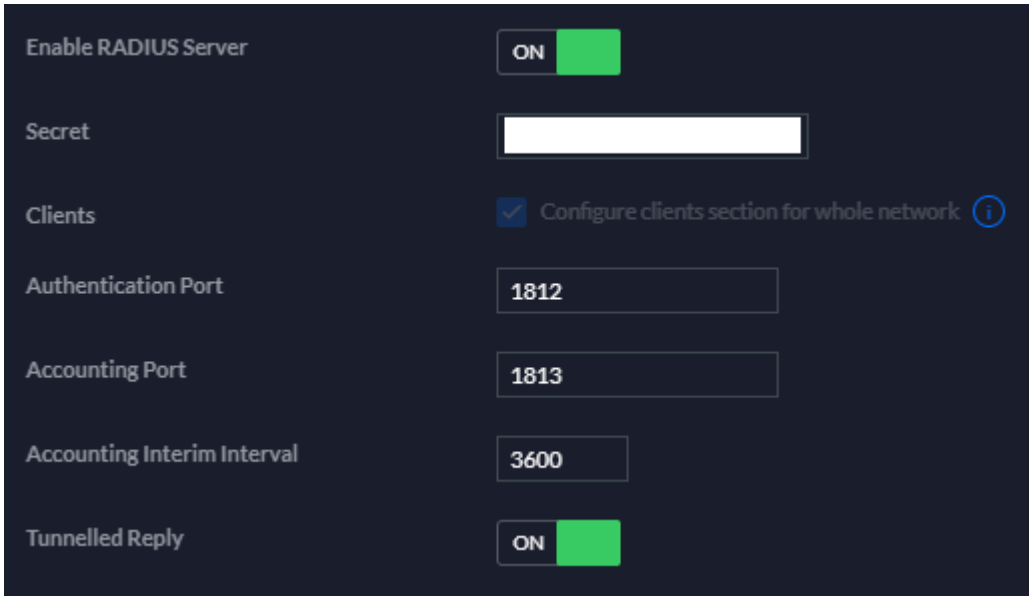

Abbildung 10 Radius Server

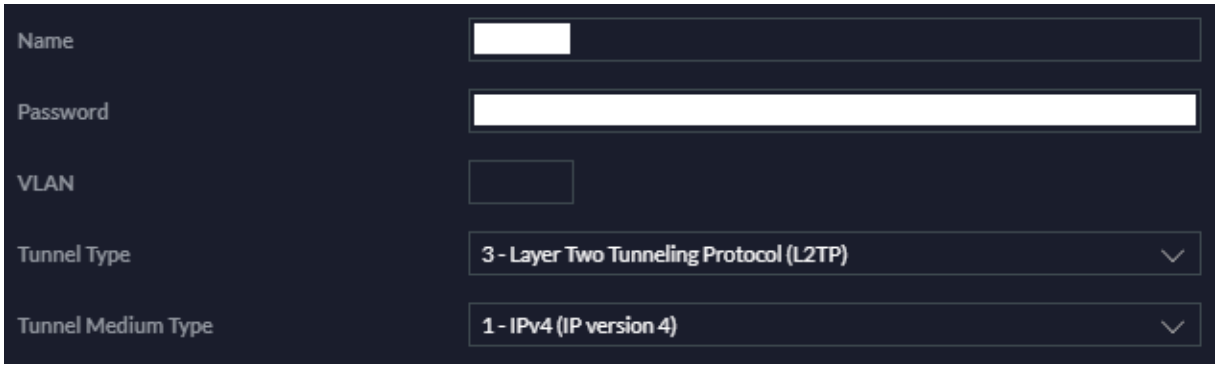

Abbildung 11 Radius User

Im Anschluss habe ich das eigentliche VPN erstellt. Dabei habe ich mich für ein /28 Netz entschieden, da nicht mehr als 14 VPN-Zugänge benötigt werden. Der Pre-Shared Key entspricht dem Secret des Radius Servers und muss auch bei der Einrichtung der VPN-Verbindung auf dem Smartphone und/oder PC zusätzlich zum Userpasswort eingegeben werden.

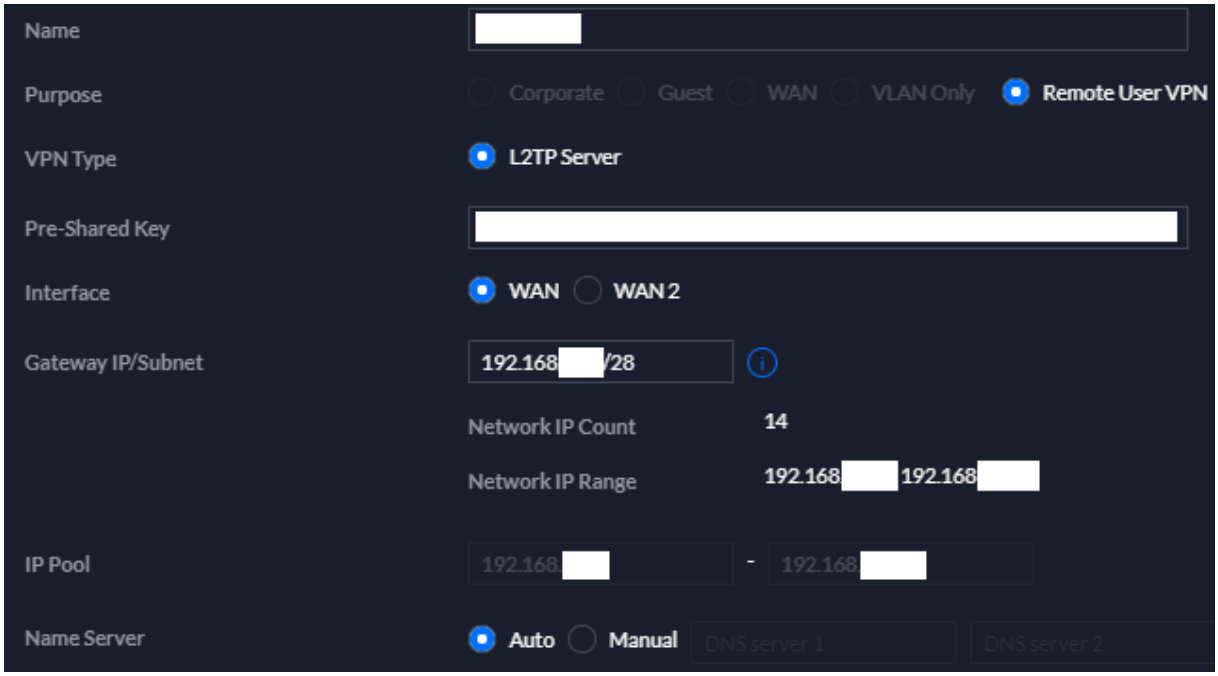

Abbildung 12 VPN Einstellungen

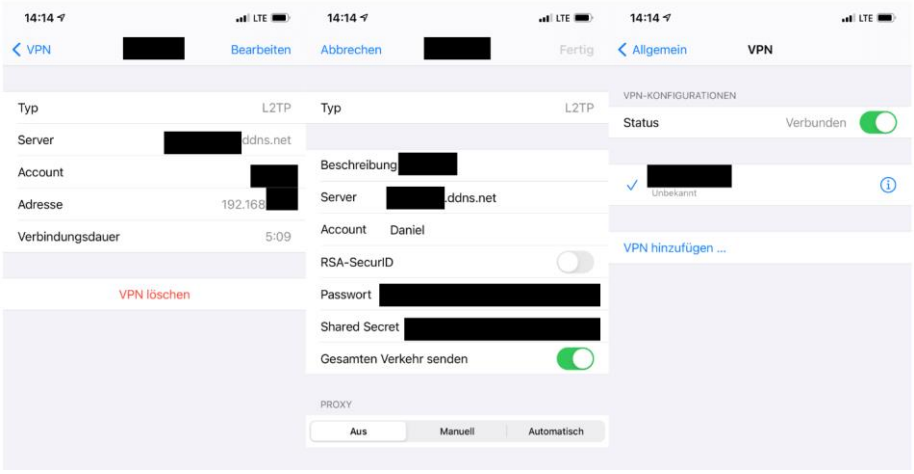

Abbildung 13 VPN Setup iPhone

3.11 Funktionstests

3.11.1 VPN

Um das VPN zu testen gab ich die Zugangsdaten in mein privates iPhone ein und deaktivierte das WLAN. Über LTE erfolgte dann die erfolgreiche Einwahl in das VPN. Des Weiteren habe ich die Verbindungsgeschwindigkeit mit einem Speedtest gemessen und erzielte dabei Geschwindigkeiten von 33,5Mbps im Download und 17,4Mbps im Upload, was der zu erwartenden Geschwindigkeit entsprach.

3.11.2 WLAN

Um die theoretisch mögliche WLAN-Abdeckung zu testen, verwendete ich ein Tool namens UniFi Design Center. In diesem Tool lud ich den Grundriss des Wohnhauses des Kunden hoch

und platzierte die APs an den entsprechenden Stellen im Wohnzimmer und Büro. Im Anschluss teilte ich dem Programm noch die Art des Mauerwerks mit. Daraufhin zeigte das Programm die nachfolgend in Abbildung 14 dargestellte WLAN-Ausleuchtung an.

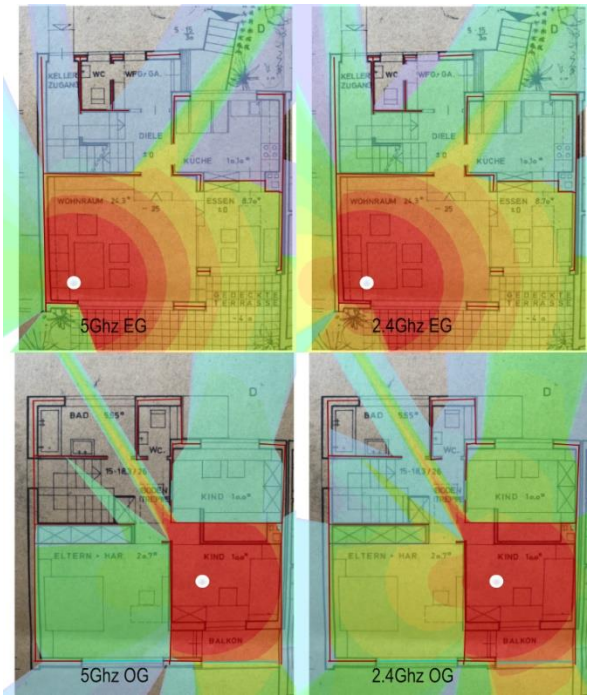

Abbildung 14 WLAN-Abdeckung

Diese Daten überprüfte ich mit dem Tool iperf3, welches ich als Server auf einem Laptop und als Client auf meinem iPhone laufen ließ. Die gemessenen Daten stimmten mit kleineren Ausnahmen mit der Grafik überein. In den Bereichen, die in Abbildung 14 als nicht von dem WLAN abgedeckt angezeigt werden, hatte ich in der Praxis noch Datendurchsatzraten von über 20Mbps. Somit ist das Haus des Kunden auf beiden Etagen sowie im Keller ausreichend mit WLAN abgedeckt.

3.11.3 Firewallregeln

Zum Test der Firewallregeln wählte ich mich in die drei verschiedenen Netze ein und führte in der Kommandozeile den Befehl `ping 192.168.xxx.xxx` aus. Ich versuchte vom „IoT“ und „Guest“ Netzwerk aus, verschiedene Geräte außerhalb des „IoT“ oder „Guest“ Netzes zu erreichen, sowie mich auf dem Webinterface des Gateways einzuwählen. Dies war – den Regeln entsprechend – nicht möglich. Aus dem „Trusted“ Netzwerk konnte ich – wie gewollt – alle Netze erreichen.

3.12 Einweisung

Nach der erfolgreichen Inbetriebnahme erfolgte die Einweisung des Kunden. Ihm wurden die Funktionen der verschiedenen Netzwerke erklärt und die Passwörter für die WLANs übergeben. Ich erklärte außerdem die Funktion des VPNs und konfigurierte das iPhone des Kunden für den VPN-Zugang. Zusätzlich händigte ich dem Kunden meine schriftliche Dokumentation aus, in der die Einweisung noch einmal erläutert wird (siehe A1).

4 Abschlussphase

4.1 Kosten des Projekts

4.1.1 Personalkosten

Die nachfolgende Tabelle gibt Auskunft über die geleisteten Arbeitsstunden, den Stundensatz (netto) sowie die Personalkosten brutto, die im Projekt entstanden sind.

Posten	Faktor	Einzelkosten	Gesamtkosten
Stundensatz	34	30,00 €	1.020,00 €
Mehrwertsteuer	16%	4,80 €	163,20 €
Brutto			1.183,20 €

Tabelle 5 Personalkosten

4.1.2 Hardwarekosten

Die nachfolgende Tabelle stellt detailliert dar, welche Hardwarekomponenten zu welchem Preis bei welchem Lieferanten bestellt und eingekauft wurden. Die Hardwarekosten belaufen sich auf insgesamt 1.805,52 €.

Name	Preis	Menge	Preis Gesamt	Lieferant
DrayTek Vigor 165	105,25 €	1	105,25 €	amazon.de
Cat 7A 100m Verlegekabel	77,17 €	1	77,17 €	amazon.de
12 HE 19 Zoll Open Frame Rack	59,06 €	1	59,06 €	amazon.de
Keystone Modul Cat 6A 8 St. Geschirmt	28,90 €	1	28,90 €	amazon.de
Cat 6A Feldstecker Geschirmt RJ45	8,99 €	3	26,97 €	amazon.de
Cat 6A 2 Port RJ45 Dose	8,91 €	3	26,73 €	amazon.de
Fachboden 19 Zoll	21,99 €	1	21,99 €	amazon.de
Netzwerk Kabeltester	19,85 €	1	19,85 €	amazon.de
Patch Panel 24 Ports	10,98 €	1	10,98 €	amazon.de
Patchkabel Cat.7 0,25 m	1,69 €	10	16,90 €	kabelscheune.de
UniFi Switch PRO 24 PoE	683,24 €	1	683,24 €	Ubiquiti Store Europe
UniFi Dream Machine Pro	370,04 €	1	370,04 €	Ubiquiti Store Europe
UniFi nanoHD Access Point	172,84 €	2	345,68 €	Ubiquiti Store Europe
DAC Cable, SFP+, 10Gbps, 0.5 meter	12,76 €	1	12,76 €	Ubiquiti Store Europe

Tabelle 6 Hardwarekosten

4.1.3 Gesamtkosten

Die Gesamtkosten für den Kunden ergeben sich aus den Personalkosten (brutto) sowie den Hardwarekosten (brutto) und werden in der nachfolgenden Tabelle detailliert ausgewiesen.

Art	Betrag
Stundenlohn 34h Brutto	1.183,20 €
Hardwarekosten Brutto	1.805,52 €
Gesamtkosten	2.988,72 €

Tabelle 7 Gesamtkosten

4.1.4 Gewinnermittlung

Für die Gewinnermittlung gilt Gewinn = Erlös – Kosten. Ich habe die Materialkosten und die Umsatzsteuer von dem Gesamterlös abgezogen, wodurch ein Gewinn von 1.020,00 € bleibt.

4.2 Soll-Ist-Vergleich

Phase	Stunden	Gesamt	Stunden	Gesamt	Differenz
	Geplant		Real		
Definitionsphase		5,0		5,0	0,0
Ist-Analyse	1,0		1,0		0,0
Marktrecherche	2,0		2,0		0,0
Produktvergleich	2,0		2,0		0,0
Planungsphase		5,0		5,0	0,0
Soll-Konzept	2,0		2,0		0,0
Hardwareangebote einholen	2,0		2,0		0,0
Angebot erstellen	1,0		1,0		0,0
Durchführungsphase		16,0		18,0	2,0
Hardware bestellen	1,0		1,0		0,0
Aufbau der Hardware und Verkabelung	5,0		8,0		3,0
Einrichtung und Konfiguration	8,0			7,0	-1,0
◦ Einrichtung des Routers			2,0		
◦ Einrichtung der Firewall			2,0		
◦ Einrichtung der VLANs			1,0		
◦ Einrichtung des VPNs			1,0		
◦ Einrichtung des WLANs			1,0		
Funktionstest	2,0		2,0		0,0
Abschlussphase		9,0		7,0	-2,0
Qualitätskontrolle/ Fehlerbehebung	3,0		2,0		-1,0
Erstellen der Rechnung	0,5		0,5		0,0
Gewinn ermitteln	0,5		0,5		0,0
Erstellung der Dokumentation	5,0		4,0		-1,0
GESAMTSTUNDEN		**35,0**		**35,0**	**0,0**

Tabelle 8 Soll-Ist-Vergleich

Tabelle 8 zeigt den Soll-Ist-Vergleich der geleisteten Arbeitsstunden im Rahmen des Projektes. Dabei ergaben sich an verschiedenen Stellen Abweichungen zur ursprünglichen Planung. Der Aufbau der Hardware und die Verkabelung dauerte in der Durchführungsphase insgesamt acht (statt der geplanten fünf) Stunden, da unter anderem die Bohrungen durch die Decke zwischen Keller und Wohnzimmer sowie Wohnzimmer und Obergeschoss zeitaufwendiger als erwartet waren. Darüber hinaus beanspruchte auch der Aufbau der einzelnen Hardwarekomponenten mehr Zeit als geplant. Dieser Mehraufwand konnte aber durch Einsparungen bei der Einrichtung und Konfiguration sowie bei der Qualitätskontrolle/Fehlerbehebung und Erstellung der Dokumentation ausgeglichen werden, sodass das Projekt insgesamt – wie geplant – 35 Stunden umfasste. Während ich im Projektantrag lediglich pauschal acht Stunden für die Einrichtung und Konfiguration eingeplant habe, habe ich für den Soll-Ist-Vergleich dokumentiert, wie viele Stunden auf die einzelnen Unterschritte entfielen.

4.3 Abweichung vom Projektantrag

Abgesehen von der Verwendung des DSL-Modems (wie in Abschnitt 3.1.4 beschrieben), entspricht dieses Projekt dem Projektantrag.

4.4 Fazit

Wie in Abschnitt 4.2 beschrieben ergaben sich bei der Durchführung des Projekts nur kleinere Abweichungen in der Zeitplanung einzelner Teilaufgaben. Die Gesamtdauer des Projektes wurde hierdurch nicht beeinflusst, sodass dem Kunden keine Mehrkosten entstanden sind. Ziel des Projektes war es, ein modernes und sicheres Netzwerk aufzubauen sowie eine hausweite Abdeckung mit schnellem und stabilem WLAN zu gewährleisten. Der Kunde zeigte sich über das Ergebnis sehr zufrieden. In der täglichen Arbeit des Kunden hat sich das Netzwerk bereits als sehr stabil und schnell erwiesen. Der Kunde berichtete auch, dass sich seine Gäste problemlos in das Gastnetzwerk einwählen können und ist darüber sehr erfreut. Durch den Aufbau dieses Heimnetzes ist der Kunde auch für zukünftige Erweiterungen des Netzwerks bestens aufgestellt.

5 Dokumentation

Für die Betriebs- und Kundendokumentation verweise ich auf die Anlagen A1 und A2.

6 Quellenverzeichnis

Preise und Bezugsquellen

- Amazon.de
- Ubiquiti Store Europe
- KabelScheune

Access Points

- UniFi nanoHD Access Point
- UniFi AC Pro

Router

- Netgate XG-7100 1U
- UniFi Dream Machine Pro

Switch

- UniFi Switch PRO 24 PoE

Anhang

A1 Betriebs- und Kundendokumentation

WLAN-Zugansdaten	
SSID	**Passwort**
Norwegen	SupergeheimesPasswort1234
Schweiz	SupergeheimesPasswort4321
Finnland	SupergeheimesPasswort5678

Tabelle 9 Zugangsdaten WLAN

Ihre eigenen Geräte verbinden Sie bitte mit dem WLAN `Norwegen`. Ihre Gäste verbinden sich mit dem WLAN `Finnland`. Ihre IoT-Geräte verbinden Sie bitte mit dem WLAN `Schweiz`. Die Zugangsdaten entnehmen Sie bitte aus der Tabelle Zugangsdaten WLAN.

VPN Zugangsdaten	
Typ	L2TP
Beschreibung	VPN
Server	superduper.ddns.net
Account	Daniel
Passwort	superduperPasswort
Shared Secret	superduperSecret
Gesamten Verkehr senden	yes

Tabelle 10 VPN Zugangsdaten

Unter iOS gehen Sie bitte in die `Einstellungen` und dort auf den Punkt `Allgemein` und dann auf `VPN – VPN hinzufügen`. Tragen Sie die Daten aus Tabelle 10 ein und speichern Sie. Bei Bedarf können Sie unter `Einstellungen` die Option `VPN` aktivieren.

Unter Windows gehen Sie bitte in die `Einstellungen` und dort auf den Punkt `Netzwerk und Internet`. Wählen Sie dort `VPN – VPN-Verbindung hinzufügen`. Tragen Sie die Daten aus Tabelle 10 ein und speichern Sie. Im Anschluss gehen Sie bitte unter `Systemsteuerung\Alle Systemsteuerungselemente\Netzwerkverbindungen`. Klicken Sie mit der rechten Maustaste auf `VPN` und dann auf `Eigenschaften`. Gehen Sie auf den Reiter `Sicherheit` und aktivieren Sie den Punkt `MS-CHAP v2`. Bestätigen Sie mit OK.

Anhang

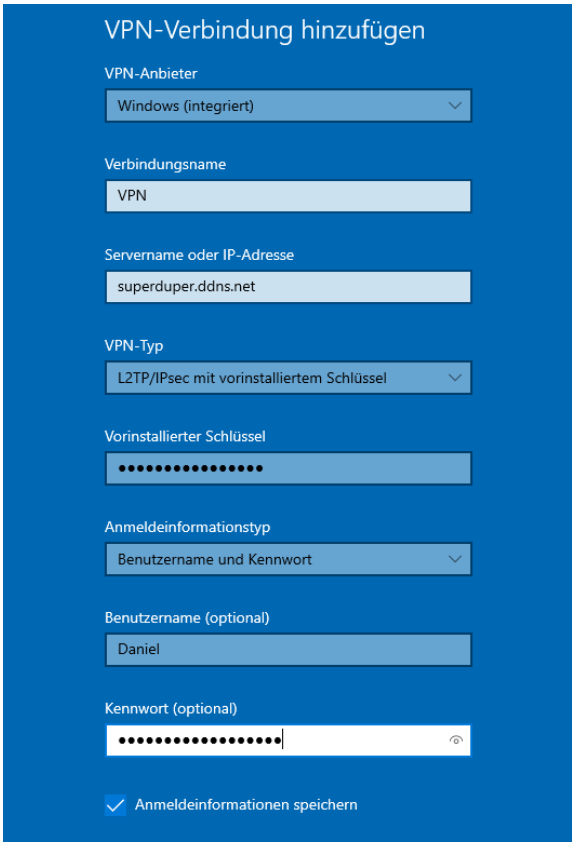

Abbildung 15 VPN Windows

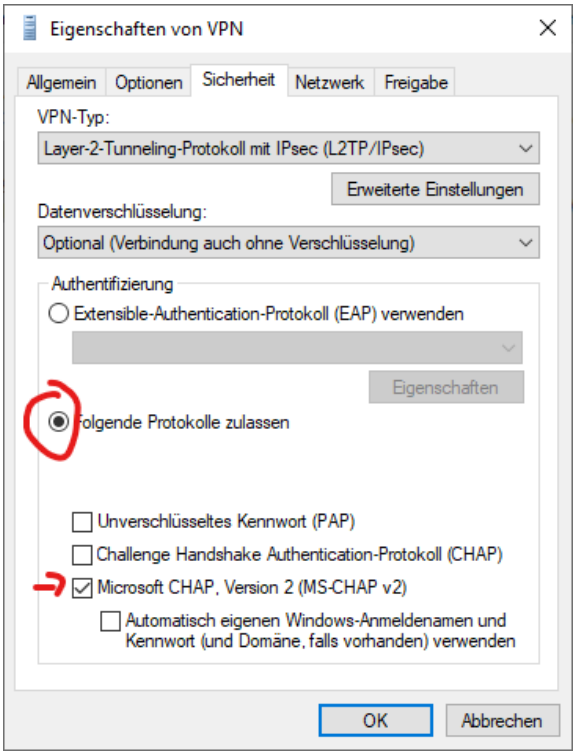

Abbildung 16 Adaptereinstellungen

A2 Netzwerkplan