Projektarbeit Sommer 2021

Fachinformatiker für Systemintegration

Dokumentation zur betrieblichen Projektarbeit

Implementierung eines Edge Routers

Implementieren eines Dual-WAN-Routers mit einer Firewall

Erstellt am: 22.04.2021
Projektzeitraum: 29.03.2021 bis 23.04.2021

Prüfungsbewerber:
Lenard Corsmeier

Prüflingsnummer:
108 70263

Ausbilder:
Philipp Peitz

Ausbildungsbetrieb:
PHP Electronic GmbH
Lange Str. 62
33129 Delbrück

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Abkürzung	Bedeutung
ACL	Access Control List
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarisierte Zone
DNS	Domain Name System
DoS	Denial of Service
DPI	Deep Packet Inspection
DS	Dual Stack
DS-Lite	Dual Stack Lite
DSL	Digital Subscriber Line
ERP	Enterprise Resource Planning
GUI	Graphical User Interface
IPDS	Intrusion Prevention und Detection System
IPS	Intrusion Prevention
ISDN	Integriertes Sprach- und Datennetz
LAN	Local Area Network
NM	Network Monitor
OSPF	Open Shortest Path First
QoS	Quality of Service
RIP	Routing Information Protocol
SPI	Stateful Packet Inspection
TK	Telekommunikation
TSE	Technische Sicherheitseinrichtung
VPN	Virtual Private Network
WAN	Wide Area Network

Tabelle 1: Abkürzungsverzeichnis

Quellenverzeichnis

Information	Quelle
Genehmigter Projektantrag	IHK Ostwestfalen Zweigstelle Paderborn + Höxter
Euronics Logo	Betriebsinterne Grafiksammlung
LANCOM Knowledge Base	https://support.lancom-systems.com/knowledge/
Spiceworks NM	https://www.spiceworks.com/
LANconfig und LANmonitor	https://www.lancom-systems.de/produkte/netzwerk-management/lantools/
Cloudflare DNS	https://www.cloudflare.com/de-de/
Informationen über die FritzBoxen	https://avm.de/produkte/

Tabelle 2: Quellenverzeichnis

1 Einleitung

In Rahmen der Abschlussprüfung zum Fachinformatiker für Systemintegration erläutere ich Lenard Corsmeier, in diesem Dokument als Prüfling bezeichnet, die Handlungsschritte des in den nachfolgenden Punkten definierten Abschlussprojektes.

1.1 Projektumfeld

1.1.1 Organisatorisches Umfeld

Der Auftraggeber und Ausbildungsbetrieb ist die PHP Electronic GmbH.

Die PHP Electronic GmbH ist seit über 20 Jahren ein Einzelhandelsbetrieb für die Bereiche Unterhaltungselektronik, Hausgeräte, Hi-Fi, Telekommunikation, Satellitentechnik und Kaffeevollautomaten. Des Weiteren besitzt die PHP Electronic GmbH eine Reparaturwerkstatt und einen Installations- und Wartungsservice.

1.1.2 Technisches Umfeld

Die PHP Electronic GmbH besitzt zwei Internetanschlüsse. Einen DSL-Anschluss von der Telekom und einen Glasfaseranschluss von der Deutschen Glasfaser.

Im lokalen Firmennetz befinden sich circa 50 Endgeräte.

Von diesen Geräten befindet sich circa die Hälfte im eigentlichen Firmennetzwerk. Die andere Hälfte befindet sich in einen von dem Firmennetzwerk separierten WLAN-Netzwerk. Bei den Geräten im WLAN-Netzwerk handelt es sich um private Endgeräte der Mitarbeiter oder um Kundengeräte.

Außerdem gibt es sowohl einen VPN-Server worüber der Zugriff auf das ERP-System ermöglicht wird und ein TSE-Server, welcher der Überwachung durch das Finanzamt dient.

1.2 Veränderung gegenüber dem Projektantrag

Die Zeitplanung wurde nach der Erstellung des Soll-Konzeptes überarbeitet. Außerdem hat der Auftraggeber entschieden, vorerst kein Failover Cluster zu implementieren. Die Gründe für diese Entscheidung können dem Punkt 2.2 entnommen werden. Wie in der überarbeiteten Zeitplanung unter Punkt 3.3.3 zeigt, behält das Projekt für den Prüfling trotzdem die geplanten 35 Stunden.

1.3 Projektbeschreibung

Momentan wird der Internetzugriff durch zwei FritzBoxen gesteuert. Jeder Internetanschluss hat sein eigenes Subnetz. Jeder Client bekommt vorerst eine IPv4-Adresse mit passendem Standardgateway für das DSL-Subnetz über einen DHCP-Server zugewiesen. Später wird dann für das Glasfasersubnetz und das DSL-Subnetz eine statische IP-Adresskonfiguration vorgenommen. Zusätzlich bekommt jeder Client eine statische Route, welche je nach der Funktion des Gerätes einen der beiden Internetanschlüsse priorisiert.

Hinweis: Das WLAN-Gastnetzwerk besitzt einen separaten DHCP-Server.

Eine logische Topologie des bisherigen Netzwerkes befindet sich im Anhang unter Punkt A.1.

Der Auftraggeber wünscht, dass die FritzBoxen durch einen Dual WAN Router ersetzt werden, welcher eine Lastenverteilung auf die beiden Internetanschlüsse durchführt. Darüber hinaus soll eine bessere Firewall implementiert werden. Damit in Zukunft die Vergabe von statischen IP-Adressen entfällt, werden die beiden Subnetze für eine bessere Übersicht zusammengefasst und ein DHCP-Server konfiguriert. Außerdem soll ein System Monitoring betrieben werden, damit kritische Systemzustände schnellstmöglich erkannt werden.

1.4 Projektziele

Das Hauptziel des Abschlussprojektes ist es der PHP Electronic GmbH einen sichereren Internetzgang bereitzustellen. Dadurch soll die Wahrscheinlichkeit eines erfolgreichen Cyberangriffes über das Internet verringert werden. Außerdem soll der Netzwerkverkehr durch eine Lastenverteilung besser auf die beiden Internetanschlüsse aufgeteilt werden. Damit kritische Systemprozesse schnellstmöglich erkannt werden, wird ebenfalls ein System Monitoring konfiguriert.

Aufgrund des begrenzten Zeitraums liegt das Hauptaugenmerk während des Projektes auf der Konfiguration des Routers. Die Aufspaltung des Firmennetzwerkes in einen sicheren- und halbsicheren-Bereich mithilfe einer DMZ wird also nicht während dieses Projektes durchgeführt.

Alle Arbeiten, welche nicht an dem zu implementierenden System anfallen, werden nicht in diesem Projekt bearbeitet.

Für das Projekt sind folgende Ziele definiert:

Muss-Ziele	Soll-Ziele	Kann-Ziele
IPS-System	DNS-Server	Schulung weiterer Mitarbeiter
SPI-System	ISDN-Port für die TK-Anlage bereitstellen.	Quality of Service
ACL	VLAN für das WLAN-Gastnetzwerk	
DoS-Protection		
Load Balancing zwischen den Internetanschlüssen		
DHCP		
System Monitoring		

Tabelle 3: Muss-, Soll- und Kann-Ziele

Die Muss-Ziele sind für den Projekterfolg entscheidend. Diese müssen implementiert werden, damit das System die vom Auftraggeber gewünschten Aufgaben erfüllen kann.

Soll-Ziele sind ebenfalls sinnvoll, müssen aber nicht zwingend für den Projekterfolg konfiguriert werden.

Die Konfiguration eines **DNS-Server** ist zwar aus verschiedenen Gründen sinnvoll (Bsp.: Cachen und Filtern), muss aber nicht zwingend durchgeführt werden, da ebenfalls ein externer DNS-Server (Bsp.: Google DNS) für die Namensauflösung verwendet werden kann. Bei der Anzahl der im Netzwerk befindlichen Geräten und der zur Verfügung stehenden Bandbreite sollte für den Endnutzer kein Unterschied zu bemerken sein.

Die **ISDN-TK Anlage** soll Ende Juli durch eine Cloudanlage ersetzt werden. Sollte der Punkt nicht umgesetzt werden, kann die TK-Anlage weiterhin über den bisher genutzten VoIP-Endpunkt betrieben werden.

Die Implementierung eines **VLAN für das Gastnetzwerk** ist zwar Sinnvoll, da dadurch ein möglicher Angreifer, welcher bereits den Access-Point korrumpiert hat trotzdem keinen Zugriff auf Unternehmensressourcen bekommt. In absehbarer Zeit soll allerdings eine DMZ implementiert werden, wodurch der Acces Point dann von dem eigentlichen Firmennetzwerk abgeschottet ist.

Eine umfangreiche **Schulung weiterer Mitarbeiter** ist zwar sinnvoll, benötigt allerdings viel Zeit. Wie in weiteren Projektablauf beschrieben ist der leitende Systemadministrator

ebenfalls mit der Konfiguration vertraut. Somit stehen bereits zwei Ansprechpartner zur Verfügung, was bei der Komplexität des Systems ausreichend ist.

Außerdem können **Quality of Service** Richtlinien eingerichtet werden, um den Netzwerktraffic zu steuern. Allerdings steht genug Bandbreite zur Verfügung, damit alle Dienste auch ohne QoS nach den gewünschten Parametern arbeiten können.

1.5 Projektschnittstellen

1.5.1 Organisatorische Schnittstellen

Während des Projektes steht dem Prüfling der leitende Systemadministrator für Rückfragen in Bezug auf die vorhandene IT-Infrastruktur zur Verfügung. Die Anforderungen an das neue System werden durch den Geschäftsführer definiert. Dieser übernimmt ebenfalls die gesamte Kommunikation mit dem Lieferanten. In dem Betrieb befinden sich zwei Server, welche aus dem WAN erreichbar sein müssen. Bei Fragen zu diesen Systemen (z.B.: benötigte Ports) steht eine gebührenfreie Servicehotline zur Verfügung.

1.5.2 Technische Schnittstellen

Auf der Seite des WAN stehen dem Router zwei Internetanschlüsse zur Verfügung. Dazu gehört ein DSL-Anschluss, welcher von der Telekom betrieben wird und ein Glasfaseranschluss, welchen die Deutsche Glasfaser betreibt. Diese beiden Anschlüsse stellen den Internetzugang für die interne IT-Infrastruktur der PHP Electronic GmbH zur Verfügung. In dem LAN befinden sich zwei Server, welche aus dem WAN erreichbar sein müssen. Des Weiteren nutzt der Prüfling ein Notebook zur Konfiguration des Routers.

2 Planung

2.1 Ist-Situation

Im Beisein des Geschäftsführers und des leitenden Systemadministrators erfasst der Prüfling vor Ort die Ist-Situation.

2.1.1 Ist-Zustand

Die lokale IT-Infrastruktur umfasst circa 20 Desktop-Arbeitsplätze für Mitarbeiter, welche über eine Ethernet-Schnittstelle mit dem Firmennetzwerk verbunden sind. Außerdem nutzen durchschnittlich 30 weitere Endgeräte den Internetzugang über ein abgetrenntes WLAN-Netzwerk. Dazu gehören sowohl Reparaturen aus der Werkstatt, als auch die privaten Endgeräte der Mitarbeiter. In dem Firmennetzwerk befindet sich ein VPN-Server, welcher eine Verbindung zu den Servern des ERP-Anbieters ermöglicht, sowie ein TSE-Server, welcher der Kontrolle durch das Finanzamt dient. Darüber hinaus sind keine Systeme in dem Netzwerk vorhanden, welche für das Projekt von Relevanz sind (z.B.: VLAN, Mail- oder Web-Server).

Die PHP Electronic GmbH besitzt einen Glasfaseranschluss von der Deutschen Glasfaser und einen DSL-Anschluss von der Telekom.

Momentan wird der Internetzugriff durch zwei FritzBoxen gesteuert. Jeder Internetanschluss hat sein eigenes Subnetz. Jeder Client bekommt eine IPv4-Adresse für das DSL-Subnetz über einen DHCP-Server zugewiesen, bis ein Administrator die IP-Adresskonfiguration manuell angepasst.

Die IP-Adressvergabe für das WLAN-Gastnetzwerk erfolgt über einen separaten DHCP-Server.

Zusätzlich bekommt jedes Endgerät eine statische Route, welche den Glasfaseranschluss priorisiert.

Der Glasfaseranschluss wir priorisiert, da dieser eine höhere Bandbreite besitzt.

Bei dem VPN- und TSE-Server wird allerdings der DSL-Anschluss priorisiert, um die Last auf beide Leitungen zu verteilen.

Für eine bessere Übersicht befindet sich im Anhang unter Punkt A.1 eine logische Topologie des Netzwerkes.

Der Glasfaseranschluss wird momentan mit einer FritzBox 7590 und der DSL-Anschluss mit einer FritzBox 7490 betrieben. An der 7490 (Telekom-Anschluss) ist ebenfalls eine ISDN TK-Anlage angeschlossen.

2.1.2 Analyse des Ist-Zustandes

2.1.2.1 Verfügbarkeit

Das momentan genutzte System bietet eine hohe Ausfallsicherheit, da bei einem Ausfall von einen der beiden Anschlüsse trotzdem ein weiterer Zugriff auf das Internet möglich ist. Allerdings ist zu beachten, dass bei einem Ausfall der Telekom Fritz Box nur noch interne Telefonie möglich ist.

Da die PHP-Electronic GmbH in ihrer Funktion als Einzelhandelsbetrieb ebenfalls FritzBoxen vertreibt, sind jederzeit mehrere Ersatzgeräte verfügbar.

2.1.2.2 Sicherheit

Da die FritzBoxen nur für den Heimgebrauch konzipiert sind, besitzen diese kein IPS-System oder eine DoS-Protection. Dafür besitzen die Fritz Boxen ein SPI-System.

Eine ACL ist bisher nicht konfiguriert.

2.1.2.3 Skalierbarkeit

Da auch über eine FritzBox mehrere hundert Clients angeschlossen werden können, ist eine ausreichende Skalierbarkeit gegeben (Momentan ist die FritzBox des Glasfaseranschlusses zu 25% ausgelastet).

2.1.2.4 Kosten

Für eine FritzBox fallen keine laufenden Lizenzkosten an. Dadurch sind die laufenden Kosten sehr gering und belaufen sich auf Wartungsarbeiten, die Mietverträge für die beiden Internetanschlüsse, der verwendete Stellplatz für die Hardware, sowie für den verbrauchten Strom.

2.2 Soll-Konzept

Im Anschluss an die Ist-Analyse folgt die gemeinsame Besprechung eines Soll-Konzeptes.

Ein SPI-System alleine bietet heutzutage keinen ausreichenden Schutz mehr. Deshalb soll das neue System zusätzlich zu dem bereits genutzten SPI-System auch mit einer ACL, einem IPS-System und einer DoS-Protection geschützt werden. Darüber hinaus wird eine Passwortrichtlinie und ein Updateplan erstellt. Es wird ein Dual-WAN-Router mit einer Lastenverteilung eingerichtet. Dadurch werden die beiden Internetleitungen bestmöglich genutzt. Darüber hinaus werden Backupverbindungen für die beiden Internetanschlüsse konfiguriert. Sollte also eine von beiden Leitungen ausfallen, übernimmt die andere Leitung innerhalb kürzester Zeit den Datenverkehr der ausgefallenen Leitung. Dadurch bleibt der Internetzugang auch bei dem Ausfall einer Leitung bestehen. Des Weiteren ist die Konfiguration eines ISDN-Mehrgeräteanschlusses wünschenswert. Da in absehbarer Zeit aber eine Cloud TK-Anlage implementiert wird, ist dieser Aspekt nicht als Muss-Ziel definiert. Um kritische Systemprozesse schnellstmöglich ausfindig zu machen, wird ein System-Monitoring eingerichtet. Somit können Fehler schneller behoben und die Ausfallzeit des Systems minimiert werden. Damit bei einen Softwarefehler der Betrieb schnellstmöglich

wieder aufgenommen werden kann, wird immer ein Backup der aktuellen Router Konfiguration gespeichert. Damit das neue System auch in Zukunft genutzt werden kann, benötigt dies Leistungsreserven von mindestens 40%. Bei den heutigen Geräten wird dieser Punkt für ein Netzwerk in dieser Größenordnung von allen Geräten erfüllt. Außerdem wünscht der Auftraggeber ein System mit möglichst geringen laufenden Kosten, weshalb dieser festlegt, dass auf Lizenzmodelle mit fortlaufenden Kosten komplett verzichtet wird. Außerdem sollen die beiden Subnetze zusammengefasst und mithilfe eines DHCP-Servers mit IPv4-Adressen versorgt werden (Weshalb auf ein IPv4-Konzept gesetzt wird, ist dem unter dem Punkt 4.7 beschrieben). Damit sich ein neuer Administrator schnellstmöglich in dem System zurechtfindet, wird ebenfalls Wert auf eine GUI gelegt. Somit kann das System auch von Administratoren ohne Kenntnisse über die Befehlssyntax konfiguriert werden. Darüber hinaus wird eine technische Systemdokumentation angefertigt.

Wie in Punkt 1.2 bereits vorab erwähnt, hat sich der Auftragsgeber aus Kostengründen dazu entschieden, vorerst kein Failover-Cluster zu implementieren. Bei einem unerwarteten Ausfall des Systems, wird dieses voraussichtlich 2 Stunden nicht erreichbar sein. Diese Zeit ergibt sich aus einer Stunde für die Beschaffung eines Ersatzgerätes, welches der Auftraggeber laut eigener Aussage jederzeit bei seinen Lieferanten abholen kann, sowie eine Stunde für das Anschließen der Hardware und Aufspielen des letzten Backups. Der Aspekt, dass kein Failover-Cluster implementiert wird, wirkt sich nachteilig auf die Verfügbarkeit und somit auch auf die Kosten aus, da bei dem Ausfall des Systems der komplette Internetzugang für circa zwei Stunden nicht zur Verfügung steht und somit auch kein Zugriff auf das ERP-System besteht. Außerdem fallen weitere Kosten für die Beschaffung und Installation des Ersatzgerätes an. Allerdings kann so vorerst ein erheblicher Teil der Anschaffungskosten eingespart werden. Außerdem schätzt der Auftragsgeber das Risiko eines Ausfalls als sehr gering ein.

2.3 Ressourcenplanung

In den folgenden Unterpunkten sind alle Ressourcen aufgelistet, die für das Projekt eingesetzt werden. Die Ressourcenplanung wird für eine bessere Übersicht in die Unterpunkte Sachmittel, Personal und Kosten aufgeteilt. Wie in dem Soll-Konzept bereits erwähnt, sollen laufenden Kosten vermieden werden. Das Gerät, welches implementiert werden soll, wurde vom Auftraggeber festgelegt.

2.3.1 Sachmittelplanung

Dazu gehört einmal das vom Auftraggeber gewünschte Gerät (LANCOM 1793VA), diverses Gebrauchsmaterial wie beispielweise Netzwerkkabel zur Konfiguration des Gerätes, etc. Für die Verbindung mit den Internetanschlüssen und für die Verbindung mit dem LAN werden die bereits vorhandenen Kabel genutzt. Darüber hinaus wird ein Arbeitsplatz mit einem Notebook für die Konfiguration benötigt. Ansonsten werden die Programme Microsoft Word, Excel, PowerPoint und Visio für Planungszwecke, das Erstellen der Projektdokumentation und der technischen Systemdokumentation genutzt.

Für die Einrichtung des Gerätes wird die Konfigurationssoftware LANconfig verwendet, welche eine übersichtliche Konfigurationsumgebung bietet.

2.3.1.1 Nutzwertanalyse Monitoring Software

Für die Auswahl der Monitoring Software wurde von dem Prüfling eine Nutzwertanalyse angefertigt.

In der Bewertung stellt die 10 die beste Punktzahl und die 0 die schlechteste Punktzahl da.

	Gewichtung	LANmonitor		Spiceworks NM	
		Bewertung	Wert	Bewertung	Wert
Funktionsumfang	23%	3	0,69	10	2,3
Übersichtlichkeit	20%	10	2	7	1,4
Implementierungsaufwand	13%	10	1,3	8	1,04
Verfügbarkeit	20%	10	2	8	1,6
Support durch LANCOM	7%	10	0,7	0	0
Preis	17%	10	1,7	10	1,7
Ergebnis			**8,39**		**8,04**

Tabelle 4: Nutzwertanalyse Monitoring-Software

Durch die Nutzwertanalyse ist der Prüfling zu der Entscheidung gekommen, dass für den Verwendungszweck der LANmonitor besser geeignet ist.

2.3.2 Personalplanung

Für das Projekt ist ein Zeitraum von insgesamt 47 Arbeitsstunden angesetzt.

Davon leistet der Prüfling 35 Arbeitsstunden und ist von der Definitionsphase bis zum Abschluss an dem Projekt beteiligt.

Für den Geschäftsführer, welcher ausschließlich an der Planung beteiligt ist, fallen insgesamt 5 Stunden an.

Der leitende Systemadministrator ist während der Planungsphase anwesend und führt die Qualitätssicherung durch. Das Projekt gilt erst als erfolgreich, wenn dieser die korrekte Implementierung bestätigt. Dafür sind insgesamt 7 Stunden eingeplant.

2.3.3 Zeitplanung

Für die Umsetzung des Projektes stehen dem Prüfling 35 Stunden zur Verfügung. Diese wurden vor Projektbeginn auf verschiedene Unterpunkte aufgeteilt, welche der Tabelle 5 zu entnehmen sind. Wie bereits in Punkt 1.2 erwähnt, wird die vorherige Zeitplanung, welche dem Projektantrag zu entnehmen ist, nach den Erkenntnissen aus dem Soll-Konzept angepasst.

Vorgang	Mitarbeiter	Zeit (in Stunden)
Besprechung des Ist- und Soll-Zustandes	Geschäftsführer, Leitender Systemadministrator, Auszubildender	4 4 4
Ressourcenplanung	Geschäftsführer, Auszubildender	1 2
Durchführung	Auszubildender	15
Qualitätssicherung & Abschluss	Leitender Systemadministrator, Auszubildender	3 3
Dokumentation	Auszubildender	11

Tabelle 5: Zeitplanung

2.3.4 Kostenplanung

Als letzter Schritt der Ressourcenplanung werden die Gesamtkosten für das Projekt ermittelt.

Bei der Annahme eines Stundenlohns von 7€ pro Stunde für einen Auszubildenden, 30€ für den Systemadministrator und 50€ für den Geschäftsführer, sind der Arbeitgeberanteil bereits

enthalten. Für die Gemeinkosten wird die betriebsinterne Pauschale von 10€ pro Stunde verwendet. Darin enthalten sind unter anderem Abschreibungen für den Arbeitsplatz, aber auch Stromkosten, usw.

Dadurch ergibt sich folgende Formel:

Anzahl der Stunden * (Stundenlohn + Gemeinkosten) = Lohnkosten

2.3.4.1 Kalkulation der einmaligen Kosten

Der geplante Arbeitsaufwand wird wie folgt Aufgeteilt:

Vorgang	Mitarbeiter	Kosten
Planung	Geschäftsführer, Leitender Systemadministrator, Auszubildender	300€ (5 Stunden) 160€ (4 Stunden) 102€ (6 Stunden)
Durchführung	Auszubildender	255€ (15 Stunden)
Qualitätssicherung	Leitender Systemadministrator, Auszubildender	120€ (3 Stunden) 51€ (3 Stunden)
Dokumentation	Auszubildender	187€ (11 Stunden)

Tabelle 6: Kostenkalkulation einmalige Kosten

Für den LANCOM Router 1793VA fallen weitere 529€ an.

Somit ergeben sich einmalige Kosten von insgesamt 1.704,00€.

2.3.4.2 Kalkulation der laufenden Kosten (pro Monat)

Bei den Wartungskosten wird von einem monatlichen Arbeitsaufwand von einer Stunde ausgegangen. Die Betriebskosten ergeben sich aus dem genutzten Platz und den Stromkosten. Es fallen keine wiederkehrenden Lizenzkosten an.

Kostenpunkt	Kosten
Betriebskosten	6€
Wartungskosten	40€ (eine Stunde)
Gesamt:	46€ pro Monat

Tabelle 7: Kostenkalkulation laufenden Kosten

2.4 Qualitätsplan

Da die Migration des Systems den Geschäftsablauf nicht beeinflussen darf, wird das System ausschließlich außerhalb der Geschäftszeiten mit den Internetanschlüssen verbunden.

Damit ein reibungsloser Projektablauf gewährleistet ist, werden während der Realisierungsphase drei White-Box-Tests durch den leitenden Systemadministrator durchgeführt. Einmal nachdem der Router konfiguriert ist und ein weiteres Mal nach der Migration der Firewall. Nachdem alle Muss-Ziele erfüllt sind, implementiert der Prüfling weitere Soll-Ziele. Zum Schluss wird die abschließende Qualitätsprüfung durchgeführt. Hat der leitende Systemadministrator auch diese Konfiguration bestätigt, wird das System dauerhaft als Edge Router betrieben. Damit in Zukunft keine Unklarheiten im Zusammenhang mit der Konfiguration des Gerätes bestehen, wird von dem Prüfling eine technische Systemdokumentation angefertigt und der PHP Electronic GmbH zur Verfügung gestellt.

2.5 Ablaufplan

Tabelle 8 beschreibt die Handlungsschritte in Ihrer geplanten Reihenfolge.

Vorgang Nr.	Bezeichnung	Personal
1	Vorbereitung	Prüfling
2	Grundkonfiguration durchführen	Prüfling
3	Glasfaseranschluss konfigurieren	Prüfling
4	Softwareupdate installieren	Prüfling
5	DSL-Anschluss konfigurieren	Prüfling
6	Implementieren des DHCP-Servers	Prüfling
7	Load Balancing einrichten	Prüfling
8	Routingeintrag hinzufügen (VPN-Server)	Prüfling
9	DHCP-Serverkonfiguration anpassen	Prüfling
10	Konfigurieren des Software Monitoring	Prüfling
11	Durchführen der ersten Qualitätssicherung	Prüfling, Leitender Systemadministrator
12	Konfigurieren der ACL	Prüfling
13	Konfigurieren des SPI-Systems	Prüfling
14	Konfigurieren des IPS-Systems	Prüfling
15	Durchführen der zweiten Qualitätssicherung	Prüfling, Leitender Systemadministrator
16	Soll- und Kann-Ziele implementieren	Prüfling
17	Abschließender Systemtest	Prüfling, Leitender Systemadministrator
18	Schreiben der technischen Systemdokumentation	Prüfling
19	Schreiben der Projektdokumentation	Prüfling

Tabelle 8: Ablaufplan

3 Projektrealisierung

In der Realisierungsphase wird das neue System von dem Prüfling implementiert. Die Phase gilt als abgeschlossen, wenn der leitende Systemadministrator die korrekte Funktionsweise im Rahmen der abschließenden Qualitätssicherung bestätigt hat. Die Realisierungsphase beginnt am 16.04.2021.

3.1 Vorbereitung

Als erstes führt der Prüfling eine Sichtprüfung durch. Dadurch bestätigt dieser, dass das Gerät keine äußeren Mängel besitzt und das Zubehör vollständig vorhanden ist.

Danach installiert der Prüfling die Programme LANconfig und LANmonitor auf dem Notebook. Die Wahl fiel auf diese Produkte, da es sich um intuitiv zu bedienender Freeware handelt, welche extra für die Verwendung mit LANCOM Systemen entwickelt wurde.

Als nächstes wird das Gerät mit Strom versorgt und via Patchkabel mit dem Notebook des Prüflings verbunden. Außerdem wird das Notebook so umkonfiguriert, dass dieses seine IPv4-Adressen von einem DHCP-Server bezieht.

Daraufhin wird ein grundlegender Funktionstest der Hardware durchgeführt, um größere Defekte direkt am Anfang des Projektes auszuschließen. Dafür wird geschaut, ob das Gerät erfolgreich bootet und von der Konfigurationssoftware erkannt wird. In diesem Zusammenhang sind keine Fehler aufgetreten.

3.1.1 Passwortrichtlinie

Für den Sicheren Zugang wird durch den Prüfling eine Passwortrichtlinie erstellt.

Ein Passwort muss folgende Kriterien erfüllen:

- die von dem Router maximal zugelassene Zeichenlänge von 15 Zeichen besitzen.
- Großbuchstaben verwenden
- Kleinbuchstaben verwenden
- Zahlen von 0 bis 9 verwenden
- Sonderzeichen verwenden
- keine Wörter, Datumsangaben, etc. besitzen.
- maximal ein Jahr alt sein.

Beispiel für ein zulässiges Passwort: Q3xY&evT?/70pUh

Beispiel für ein nicht zulässiges Passwort: Julia20!03!15

3.1.2 Updatestrategie

Damit der Geschäftsablauf nicht durch die Installation von neuen Updates gestört wird, entscheidet der Prüfling, dass der Router täglich zwischen 0 Uhr und 1 Uhr nach neuen Updates sucht. Sollten Updates vorhanden sein, hat der Router zwischen 2 Uhr und 4 Uhr Zeit, diese zu installieren. Dadurch besitzt der Router immer die neuste Firmware Version und Sicherheitsupdates.

3.1.3 Backupstrategie

Damit bei einen Softwarefehler (z.B.: Ein Konfigurationsfehler oder ein fehlerhaftes Update) die Ausfallzeit möglichst geringgehalten wird, ist es extrem wichtig, immer die aktuelle Konfiguration des Routers als Backup zu speichern. Deshalb wird die LANconfig so konfiguriert, dass diese nach jeder Konfigurationsänderung ein Backup in einem extra abgesicherten NAS-Ordner ablegt, welchen der leitende Systemadministrator bereits vor dem Projekt erstellt hat. (In dem Ordner werden bereits seit längerer Zeit Backups von anderen Systemen gespeichert.) Dadurch wird verhindert, dass Dritte einfach auf diese Daten zugreifen können. LANconfig erstellt Backups nach jeder Änderung an dem System. Dazu zählen unter anderem Anpassungen an der Konfiguration und das manuelle installieren von Updates.

3.2 Grundkonfiguration

Als nächstes wird mit der Konfiguration des Gerätes begonnen. Dafür wird der Grundkonfigurationsassistent geöffnet.

Im ersten Schritt kann der Gerätename geändert werden. Damit das Gerät im Netzwerk leichter zu identifizieren ist, wird die Bezeichnung „EdgeRouter“ gewählt.

Im zweiten Schritt wird ein Passwort für den root-Benutzer vergeben. Da es sich bei dem root-Benutzer um ein Benutzerkonto mit allumfassenden Rechten handelt, ist dieses besonders schützenswert. Darüber hinaus wird der Zugriff auf den Router nur über das LAN mit den Protokollen HTTPS für die Konfiguration und über SNMPv3 für das Monitoring gestattet. Auf dem Router lässt sich aus dem WAN zwar mithilfe einer Remote Desktop Verbindung trotzdem zugreifen, diese Ports sind allerding durch die ACL gesperrt. (Sollte es ein Angreifer allerdings schaffen, eine End to End VPN Verbindung via HTTPS etablieren, ist auch diese Schutzmaßnahme nicht ausreichend.) Außerdem wird das System so konfiguriert, dass dieses sich nach 5 fehlgeschlagenen Anmeldeversuchen für 5 Minuten sperrt. Aufgrund der Tatsache, dass alle Passwörter jedes Jahr geändert werden, ist die Wahrscheinlichkeit eines erfolgreichen Brute Force Angriffes (Also das ausprobieren aller möglichen Kombinationen) sehr gering.

Als nächstes wird der DHCP-Server aktiviert und dem Router die lokale IPv4-Adresse 192.168.0.1 mit der Subnetzmaske 255.255.255.0 zugewiesen. Mithilfe dieser beiden Werte wird ebenfalls der lokale IPv4-Adressraum spezifiziert. (Anmerkung: Der Adresspool des DHCP-Servers wird unter Punkt 3.10 der Konfiguration des vorherigen Systems angepasst.)

Die darauffolgende Abfrage erfragt die Zeitzone und den gewünschten NTP-Server. Als NTP-Server wird pool.ntp.org gewählt, da es sich hierbei um ein Cluster mehrerer NTP-Server handelt, wodurch eine hohe Verfügbarkeit gewährleistet ist.

Mit dem nächsten Punkt kann die Layer 7-Anwendungskontrolle aktiviert werden. Da diese aber genaue Informationen über den Netzwerkverkehr der einzelnen Arbeitsplätze und somit auch über die einzelnen Mitarbeiter sammelt, bleibt diese aus Datenschutzgründen deaktiviert.

Danach wird die unter Punkt 4.1.2 erläuterte Updatestrategie konfiguriert.

Als nächstes wird die Zusatzfunktion „LANCOM Management Cloud“ deaktiviert. Für diese Funktion wird eine nicht erworbene Lizenz benötigt, wofür laufende Kosten anfallen würden.

Der letzte Schritt beinhaltet das Aktivieren der SPI-Firewall. Außerdem wird für das Gerät der Anti-Ping und Stealth Modus aktiviert. Dadurch wird der Router vor Port Scannern geschützt.

Danach ist die Grundkonfiguration abgeschlossen und es wird mit der eigentlichen Konfiguration begonnen.

3.3 Konfigurieren des Glasfaseranschlusses

Dafür wird ebenfalls der passende Konfigurationsassistent geöffnet.

Da der Glasfaseranschluss ein dediziertes Modem besitzt, wird für diesen Anschluss ein Gigabit Ethernet Port genutzt.

Als nächstes wird konfiguriert, wie der Glasfaseranschluss seine IP-Adressen beziehen soll, die Deutsche Glasfaser betreibt hierfür einen DHCP Server.

Weil der Glasfaseranschluss nur eine native IPv6-Adresse besitzt und sich die öffentliche IPv4-Adresse mit mehreren Anschlüssen teilt (IPv4 über einen Tunnel), wird die Betriebsart DS-Lite gewählt. Das DS-Lite Gateway wird dem Router mithilfe des DHCP-Servers des Providers zugewiesen.

Danach kann eine Backupverbindung eingerichtet werden, sodass der Datenverkehr bei dem Ausfall des DSL-Anschlusses über einen anderen Internetanschluss geleitet wird. Weil bisher kein anderer Internetanschluss eingerichtet ist, wird dieser Schritt zu einem späteren Zeitpunkt unter Nummer 3.6 durchgeführt.

3.4 Softwareupdate

Da nun eine Internetverbindung über den konfigurierten Glasfaseranschluss (welcher via Patchkabel mit dem Firmennetzwerk verbunden ist) besteht, wird bevor mit der Konfiguration vorgefahren wird, die neuste Softwareversion des Betriebssystems LCOS (Version: 10.42.0383RU2) über die Konfigurationssoftware installiert.

3.5 Konfigurieren des DSL-Anschlusses

Da der Router in keinen Hochverfügbarkeitsverbund betrieben wird, kann der DSL-Anschluss direkt mit dem Router verbunden werden. Es wird also kein dediziertes Modem vorgeschaltet.

Um den DSL-Anschluss konfigurieren zu können, wird der passende Konfigurationsassistent gestartet.

Da der DSL-Anschluss sowohl eine nativen IPv4 als auch einen nativen IPv6 Zugang bereitstellt, wird der Betriebsmodus Dual-Stack gewählt.

In dem nächsten Schritt wird der Provider (Telekom) ausgewählt und die passenden Zugangsdaten eingetragen.

Als nächstes wird als Backupleitung der Glasfaseranschluss ausgewählt und die Lastenverteilung für die beiden Anschlüsse aktiviert.

3.6 Load Balancing und Glasfaser-Backupverbindung

Nachdem die Grundkonfiguration der beiden Internetanschlüsse abgeschlossen ist, werden mithilfe des Konfigurationsmenüs manuell ein paar Einstellungen angepasst. Dazu gehört das Konfigurieren des DSL-Anschlusses als Backupverbindung für den Glasfaseranschluss und das Skalieren des Glasfaseranschlusses auf die vom Provider zugelassene Datenrate, da der Load Balancer diese Daten nutzt, um die Internetanschlüsse zu gewichten. Sollte die Datenrate also nicht angepasst werden, dann würde der Load Balancer nicht korrekt arbeiten.

Außerdem ist bei dem Load Balancer zu beachten, dass dieser mit sogenannten Balance-Sekunden (Für eine möglichst schnelle Datenrate werden in diesen Zeitraum beide Internetanschlüsse genutzt) und Binding-Minuten (Nachdem die Balance-Sekunden abgelaufen sind, wird die Verbindung während dieses Zeitraums auf eine der beiden Leitungen gebunden) arbeitet. Da ein Server, welcher eine Authentizitätsprüfung durchführt die Verbindung abbricht, wenn dieser Datenpakete mit zwei verschieden Quell IP-Adressen bekommt, werden die Balance Sekunden auf 0 gestellt. Dadurch besteht zwar eine geringere Datenrate, welche aber bei der Bandbreite der beiden Internetanschlüsse nicht zwingend notwendig ist. Dadurch wird verhindert, dass beispielweise ein Online Shop die Verbindung abbricht, wenn ein Mitarbeiter oder ein Passwortmanager probiert, sich während des Balancing-Zeitraums zu authentifizieren.

3.7 Warum kein IPv6?

Die Vergabe von globalen IPv6-Adressen an Endgeräte ist aufgrund der Nutzung eines Load-Balancers deaktiviert. Es besteht zwar die Möglichkeit, beiden Internetanschlüssen das gleiche statische Präfix zuzuweisen, oder Dienste wie NPTv6 oder NAT66 einzusetzen, die Implementierung ist aber mit zusätzlichen Kosten verbunden und bietet der PHP Electronic GmbH momentan keinen nennenswerten Vorteil, weshalb der Auftraggeber vorerst die Implementierung eines klassischen IPv4 Netzes beauftragt hat.

3.8 Routing Protokoll

In dem Firmennetz sind keine Core Router vorhanden, weshalb die Implementierung eines dynamischen Routingprotokolls nicht notwendig ist. Allerding ist zu erwähnen, dass RIP standardmäßig aktiviert ist. Sollten mehrere Core Router über redundante Verbindungen implementiert werden, empfiehlt sich allerding die Nutzung von Link-State Protokollen wie OSPF.

3.9 Statischen Routingeintrag anlegen

Damit Anfragen, welche für das VPN-Gateway gedacht sind, an dieses weitergeleitet werden, wird eine statische Route in der Routingtabelle eingetragen.

3.10 Anpassungen an dem DHCP-Server

Der IPv4-Adresspool wird so angepasst, dass dieser mit den Adresspool des DHCP-Servers übereinstimmt, welcher die IP-Adressvergabe für den DSL-Anschluss steuert. Dadurch wird verhindert, dass manuell vergebene IP-Adressen ebenfalls durch den DHCP-Server vergeben werden. Des Weiteren wird der zu nutzende DNS-Server eingetragen.

3.11 System Monitoring

Als nächstes wird das System-Monitoring eingerichtet. Dafür wird der von LANCOM angebotene LANmonitor genutzt.

Es besteht die Möglichkeit die Konfigurationssoftware LANconfig zu starten und sich automatisch mit den in dem LANmonitor hinterlegten Zugangsdaten zu authentifizieren.

Da es Personen gibt, welche zwar den LANmonitor nutzen, aber keinesfalls die Konfiguration ändern dürfen, wird hierfür ein extra Benutzerkonto angelegt, welches nur die Berechtigung zum Auslesen der Daten hat.

3.12 Erste Qualitätssicherung

Damit der Systemadministrator eine erste Qualitätsprüfung durchführen kann, verbindet der Prüfling den Router außerhalb der Öffnungszeiten mit den Internetanschlüssen.

Danach prüft der Systemadministrator die einzelnen Konfigurationsschritte auf deren Richtigkeit.

Nachdem der Systemadministrator die richtige Konfiguration des Gerätes bestätigt hat, verbindet der Prüfling die beiden Internetanschlüsse wieder mit den Fritz Boxen und prüft, ob diese einwandfrei arbeiten.

Danach fährt der Prüfling mit der Konfiguration des Gerätes fort.

3.13 Konfigurieren der ACL

In dem nächsten Schritt wird die ACL konfiguriert. Die Konfiguration erfolgt als Whitelist. Somit sind erst einmal alle Ports blockiert, bis eine passende Regel implementiert ist.

Dafür wurden die benötigten Ports für den VPN-Server sowie für den TSE-Server im Vorfeld bei dem passenden Ansprechpartner erfragt. Die Ports für den jeweiligen Server werden auch nur für diesen freigegeben. So bleibt die mögliche Angriffsfläche möglichst gering. Darüber hinaus wird für alle restlichen Clients im Netzwerk der Zugriff auf Webseiten über HTTPS und HTTP sowie das Senden und Empfangen von Mails über SMTP bzw. IMAP erlaubt. Da Windows seine Updates über HTTPS überträgt, werden dafür keine besonderen Ports benötigt.

3.14 Konfigurieren des SPI-Systems

Das SPI-System ist seit Punkt 3.2 aktiviert. Damit der VPN-Server und der TSE-Server ordnungsgemäß funktionieren können, werden Portweiterleitungen auf dem Router eingerichtet. Dadurch werden Anfragen auf diesen Ports nicht durch das SPI-System blockiert.

3.15 DoS-Protection

Um zu verhindern, dass das System durch einen Denial of Service Angriff beeinträchtigt wird, wird eine DoS-Protection eingerichtet. Besitzt eine IP-Adresse über 100 halboffene Verbindungen, so werden diese verworfen und die Absenderadresse für 10 Minuten gesperrt. Außerdem wird der Systemadministrator über diesen Vorfall informiert, wodurch dieser die Möglichkeit hat, geeignete Gegenmaßnahmen zu ergreifen.

3.16 Intrusion Prevention/ Detection System

Das von dem Router genutzte IPDS arbeitet signaturbasiert und ohne Deep Paket Inspection. Es überprüft also nur den IP-Header um Angriffsmuster zu erkennen. Damit Angriffe schnellstmöglich abgewehrt werden können, wird das System als Intrusion Prevention System eingesetzt. Sollte ein Angriff erkannt werden, verwirft das System die Pakete automatisch. Darüber hinaus ist das System so konfiguriert, dass von einer IP-

Adresse höchstens 50 Portanfragen erlaubt sind. Somit wird die Verwendung eines Portscanners unterbunden, sollte dieser mehr als 50 Ports abfragen.

3.17 Zweite Qualitätssicherung

Nachdem alle Muss-Ziele erfüllt sind, schließt der Prüfling den Router ein weiteres Mal außerhalb der Geschäftszeiten an den Internetanschlüssen an. Der Systemadministrator prüft nun ein zweites Mal die Konfiguration des Routers auf Richtigkeit.

Nachdem der Systemadministrator auch dieses Mal die korrekte Konfiguration bestätigt hat, werden die Internetanschlüsse wieder mit den Fritz Boxen verbunden.

Aufgrund der Erfüllung aller Muss-Ziele nutzt der Prüfling nun die verbliebene Zeit, um die in Punkt 1.4 definierten Soll-Ziele umzusetzen.

3.18 TK-Anlage

Als nächsten Schritt ist die Konfiguration des VoIP-Anschlusses vom Auftraggeber gewünscht.

Dafür wird der passende Konfigurationsassistent geöffnet.

Als erstes wählt der Prüfling den passenden Internetanbieter aus und trägt die passenden SIP-Accountdaten ein.

Danach werden die Rufnummern mithilfe von SIP-Benutzern den gewünschten ISDN-Anschluss zugeordnet.

Da das Vorwählen einer Null nicht gewünscht ist, wird die automatische Amtseinholung aktiviert.

Als letztes wird die Landesvorwahl und die Ortsvorwahl eingetragen, sodass der Router nationale und Ortsanrufe erkennen und passend weiterleiten kann.

3.19 DNS-Server

Als letzter Schritt wird der lokale DNS-Server konfiguriert.

Dadurch besteht der Vorteil, dass DNS-Anfragen gecached werden. So können diese Anfragen schneller beantwortet werden. Außerdem besteht somit die Möglichkeit in Zukunft eigene DNS-Filterregeln zu implementieren.

Sollte der DNS-Server eine Anfrage nicht selbst beantworten können, leitet dieser die Anfrage an den Cloudflare DNS weiter (Stichwort: DNS-Forwarding).

Cloudflare DNS-Server wurde aus fünf Gründen gewählt:

1. Bietet eine geringere Latenz als die DNS-Server der Provider.
2. Daten werden für maximal 24 Stunden gespeichert.
3. Bietet einen rudimentären Malwareschutz.
4. Steht kostenfrei zur Verfügung.
5. Eine Nutzung für gewerbliche Zwecke ist in den AGB erlaubt.

4 Projektabschluss

In der letzten Phase des Projektes erstellt der Prüfling im Beisein des leitenden Systemadministrators einen Ist/Soll-Vergleich. Des Weiteren prüft der leitende Systemadministrator die Konfiguration ein letztes Mal auf Richtigkeit. Außerdem erstellt der Prüfling eine Projektdokumentation und eine technische Systemdokumentation.

4.1 Abschließende Qualitätsprüfung

Nachdem der Prüfling die zur Verfügung stehende Zeit für die Realisierungsphase erreicht hat, schließt dieser den Router nach Ladenschluss an die Internetanschlüsse an. Der Systemadministrator prüft nun ein letztes Mal die Konfiguration des Routers auf Richtigkeit.

Auch bei der abschließenden Qualitätsprüfung sind keine Fehler aufgetreten.

Der leitende Systemadministrator bestätigt somit die erfolgreiche Durchführung des Projektes.

4.2 Soll/Ist Vergleich

4.2.1 Soll/Ist Vergleich der Muss- / Soll- und Kann Ziele

Während des Projektes wurden alle Muss- und die meisten Kann-Ziele erfolgreich umgesetzt. Die Tabelle zeigt eine detaillierte Auflistung, welche Ziele umgesetzt wurden:

Muss-Ziele	IPS-System	✔
	SPI-System	✔
	ACL	✔
	DoS-Protection	✔
	Load Balancing	✔
	DHCP-Server	✔
	System Monitoring	✔
Soll-Ziele	DNS-Server	✔
	VoIP	✔
	VLAN	X
Kann-Ziele	Schulung weiterer Mitarbeiter	X
	Quality of Service	X

4.2.2 Soll/Ist Vergleich der Zeitplanung

Während des Projektes sind zwei Differenzen zur Zeitplanung aufgetreten. Die Erstellung der Ist-Analyse und es Soll-Zustandes konnte eine Stunde schneller durchgeführt werden. Diese Stunde wurde von dem Prüfling genutzt, um weitere Soll-Ziele zu erfüllen.

Vorgang	Mitarbeiter	Geplante Zeit (in Std.)	Benötigte Zeit (in Std.)	Differenz (in Std.)
Besprechung des Ist- und Soll-Zustandes	Geschäftsführer, Leitender Systemadministrator, Auszubildender	4 4 4	3 3 3	-1 -1 -1
Ressourcenplanung	Geschäftsführer, Auszubildender	1 2	1 2	
Durchführung	Auszubildender	15	16	+1
Qualitätssicherung & Abschluss	Leitender Systemadministrator, Auszubildender	3 3	3 3	
Dokumentation	Auszubildender	11	11	

Weil die Durchführung eine Stunde schneller absolviert wurde, ergibt sich für den Auftraggeber ein Kostenvorteil von 83€. Dadurch verringern sich die einmaligen Kosten auf 1.621€.

5 Fazit

Nach dem erfolgreichen Abschluss des Projektes zieht der Prüfling ein Fazit.

5.1 Learnd Lessons

Während des Projektes hat der Prüfling neue Erfahrungen gesammelt. Dies bezieht sich sowohl auf das Projektmanagement als auch auf die Fachinhalte. Der Prüfling hat zwar auch in der Vergangenheit viele Projekte eigenständig durchgeführt, allerding nicht von einer solchen Komplexität. Der gesparte Zeitaufwand hat dafür gesorgt, dass das sogar ein Teil des Budgets eingespart wurde, was dem Kundenwunsch einer möglichst preiswerten Umsetzung entgegenkommt.

Wie bereits erwähnt, hat der Prüfling mit der Umsetzung auch neue fachliche Erfahrungen gesammelt. Dazu gehört das Einarbeiten in ein für den Prüfling neues Router-Betriebssystem, aber auch das Implementieren von Techniken, welche dieser bis zur Durchführung des Projektes nur theoretisch kannte. Dadurch war das Projekt während der gesamten Dauer für den Prüfling sehr Interessant.

Außerdem ist die Ausführung der Qualitätssicherung und die Integration in die Durchführungsphase erwähnenswert. Dadurch hätten Fehler in der Konfiguration schnellstmöglich erkannt und behoben werden können. Außerdem ist die Einbindung eines erfahrenden Systemadministrators, welcher die gesamte IT-Infrastruktur der PHP Electronic GmbH aufgebaut hat, von Vorteil. Dadurch konnte der Prüfling sich versichern, dass er alle Konfigurationsschritte richtig durchgeführt hat.

5.2 Ausblick

Die PHP Electronic GmbH ist dank erfolgreicher Projektdurchführung besser gegen Cyberangriffe geschützt. Darüber hinaus ist der Auftraggeber nun in der Lage, durch das Load Balancing und die eingerichteten Backupverbindung seine Internetanschlüsse bestmöglich zu nutzen und kann bei dem Ausfall einer der beiden Leitungen weiterhin das Internet nutzen. Hierbei ist allerding zu beachten, dass die Telefonie nur über das Netz der Telekom betrieben werden kann. Darüber hinaus besitzt das System genug Leistungsreserven, um auch bei einem starken Wachstum der IT-Infrastruktur weiterhin einwandfrei zu funktionieren. Wenn in Zukunft Anpassungen durchgeführt werden müssen, steht ausreichend geschultes Personal zur Verfügung, um diese Anpassungen ohne externe Dienstleister durchzuführen. Darüber hinaus steht eine Systemdokumentation über die aktuelle Konfiguration zur Verfügung. Außerdem wurde wie vom Kunden gewünscht, auf hohe laufende Kosten verzichtet.

Durch diese Unterschrift versichere ich, Lenard Corsmeier, dass ich alle mir zugewiesene Teilaufgaben selbständig durchgeführt und die dazugehörige Dokumentation ebenfalls selbständig erstellt habe. Alle Passagen, welche aus öffentlichen Quellen/Werken entnommen habe, sind entsprechend gekennzeichnet.

Delbrück, 23.04.2021 Corsmeier

6 Genehmigter Projektantrag

IHK Industrie- und Handelskammer Ostwestfalen zu Bielefeld Zweigstelle Paderborn + Höxter

Referat Berufliche Bildung

IHK Ostwestfalen | Zweigstelle Paderborn + Höxter | Postfach 18 07 | 33048 Paderborn

Herrn
Lenard Corsmeier
Holsteiner Weg 18
33129 Delbrück

Ihr Zeichen/Nachricht vom

Ansprechpartner/in
Frank Oppermann
E-Mail
f.oppermann@ostwestfalen.ihk.de
Tel.
05251 1559-26
Fax
0521 554-5626
Datum
12. März 2021

Genehmigung Projektantrag

Sehr geehrter Herr Corsmeier,

der beiliegende Projektantrag hat dem für Sie zuständigen IHK Prüfungsausschuss vorgelegen.
Er wird hiermit unter folgender Auflage genehmigt: Statt einer Betrieblichen Dokumentation soll eine Technische Systemdokumentation erstellt werden. Dies bedeutet: die betriebliche Dokumentation soll ich Form einer Technischen Systemdokumentation angefertigt werden.

Es ist denkbar, dass Sie dies sowieso vorhatten. Dann hat diese Auflage nur hinweisenden Charakter.

Der Zweck dieser Dokumentation (Technische Systemdokumentation) soll sein, dass Kolleginnen und Kollegen sich schneller und zielgerichtet in die von Ihnen konzipierte, designte und implementierte Lösung eindenken können. Dies könnte z.B. notwendig sein, wenn Wartungstätigkeiten notwendig werden oder eine ähnliche Lösung realisiert werden soll. Auf jeden Fall soll sich die ab zu gebende Technische Systemdokumentation an Kolleginnen und Kollegen der ausbildenden Abteilung wenden. Die umfangreiche Dokumentation und Begründung der Konfigurationseinstellungen ist wichtiger Inhalt der Technischen Systemdokumentation.

Beachten Sie bitte: Wenn Sie dieser Auflage nicht nachkommen, so kann sich dies auf die Benotung durch den Prüfungsausschuss auswirken.

Freundliche Grüße

i.A.

Frank Oppermann

#GemeinsamUnternehmen

Industrie- und Handelskammer Ostwestfalen zu Bielefeld
Hausanschrift: IHK Ostwestfalen | Zweigstelle Paderborn + Höxter | Stedener Feld 14 | 33104 Paderborn
Tel. (0 52 51) 15 59-0 | Fax (0 52 51) 15 59-31 | E-Mail: info@ostwestfalen.ihk.de | Internet: www.ostwestfalen.ihk.de

Antrag für die betriebliche Projektarbeit

Berufsbezeichnung/Fachrichtung/Einsatzgebiet/Fachbereich: Fachinformatiker Fachrichtung Systemintegration	
Antragsteller/in: Lenard Corsmeier	Ausbildungsbetrieb: PHP Electronic GmbH Lange Str. 62 33129 Delbrück
Abschlussprüfung: Sommer 2021	Antragsdatum: 04.03.2021

Projektbezeichnung (Auftrag/Teilauftrag):
Implementieren eines neuen Routers und einer neuen Firewall im Failover Cluster.

Kurze Projektbeschreibung:
Aufgrund des schnellen Wachstums der PHP Electronic GmbH hat sich die Führungsebene dafür entschieden, die **IT-Infrastruktur zu modernisieren**, um ihren Mitarbeitern so eine sicherere und flexiblere Netzwerkinfrastruktur bereitzustellen.

Ist-Zustand:
Momentan wird der Internetzugriff durch zwei Fritz!Boxen gesteuert.

Das Unternehmen besitzt sowohl einen Glasfaseranschluss als auch einen DSL-Anschluss. Jeder Internetanschluss hat sein eigenes Subnetz.
Jeder Client bekommt jeweils eine statische IPv4-Adresse mit passendem Gateway für beide Subnetze zugewiesen. Zusätzlich bekommt jeder Client eine Route, welche den Glasfaseranschluss priorisiert.

Soll-Zustand:
Die Fritz!Boxen sollen durch einen **dual WAN Router** ersetzt werden. Darüber hinaus soll eine **Firewall** implementiert werden, worauf sowohl ACLs als auch ein SPI und ein IPS-System installiert werden. Damit in Zukunft keine statischen IP-Adressen vergeben werden müssen, wird ebenfalls ein **DHCP Server** konfiguriert.

Die neuen Geräte sollen zugunsten der Ausfallsicherheit in einem **Failover Cluster** betrieben werden. Außerdem wird von jedem Gerät nach jeder Änderung ein **Backup** gemacht, sodass dieses bei einem Ausfall nicht neu konfiguriert werden muss. Darüber hinaus soll ein **Hardware Monitoring** betrieben werden, damit bei einem Ausfall einer Komponente schnellstmöglich reagiert werden kann.

Damit die Komponenten bei einem **weiteren Wachstum** der PHP Electronic GmbH nicht aufgrund zu schwacher Hardware/Software ausgetauscht werden müssen, darf diese bei der Installation nicht zu über 60 % ausgelastet sein. Darüber hinaus werden Geräte mit SFP-Ports bei der Komponentenauswahl bevorzugt behandelt.

Um eine möglichst **kosteneffiziente Nutzung** der Netzwerkhardware zu ermöglichen, soll wenn möglich Freeware genutzt werden. Außerdem soll auf wiederkehrende Kosten verzichtet werden. Natürlich nur, wenn dadurch die Verfügbarkeit, Sicherheit und Skalierbarkeit nicht nennenswert beeinträchtigt wird.

Projektumfeld:

Die PHP Electronic GmbH ist seit über 20 Jahren ein Einzelhandelsbetrieb für die Bereiche Unterhaltungselektronik, Hausgeräte, Hi-Fi, Telekommunikation, Satellitentechnik und Kaffeevollautomaten. Des Weiteren besitzen wir eine Reparaturwerkstatt und ein Installationsservice für alle Produkte, die wir vertreiben.

Um eine reibungslose Integration in den Geschäftsablauf zu ermöglichen, werde ich das Projekt in starker Absprache mit dem Filialleiter sowie dem betreuenden IT-Techniker durchführen.

Bei den technischen Schnittstellen in dem Projekt handelt es sich um den Internet Service Provider und der lokalen IT-Infrastruktur.

Durchführungszeitraum: vom: 29.03.2021 bis: 23.04.2021	Projektverantwortlicher im Ausbildungsbetrieb: Philipp Peitz +49 5250 930140

Antrag für die betriebliche Projektarbeit

Projektphasen mit Zeitplanung in Std.:

Bezeichnung:	Std.
Planung:	
Aussuchen der Hardware und Software	3
Erstellen eines Ablaufplans	1,5
Durchführung:	
Implementieren der Dual WAN Router	5
Implementieren der Firewall	8
Implementieren des Hardware Monitoring	2
Konfigurieren des DHCP-Servers	2
Erstellen von Backups	0,5
Projektabschluss:	
Abschlusstest des gesamten Systems	2
Dokumentation:	
Schreiben der Projektdokumentation	8
Schreiben der Betrieblichen Dokumentation	3
Gesamtstundenzahl für die Projektarbeit:	35 Stunden

Die Projektarbeit beinhaltet folgende Dokumente:
Nicht selbstständig erstellte Dokumente sind mit "(x)" zu kennzeichnen!

- Projektdokumentation
- Betriebliche Dokumentation

Geplante Präsentationsmittel (zutreffendes ankreuzen):

Flipchart ☐ Tageslichtprojektor ☐ Pinnwand ☐

andere Präsentationsmittel: Beamer (sind vom Prüfling funktionsfähig mitzubringen)

Persönliche Erklärung des Auszubildenden

Ich versichere, dass ich die Projektarbeit und die dazugehörige Dokumentation selbstständig erstellen werde.

Delbrück, 04.03.2021 — Ort, Datum

Corsmeier — Unterschrift des Prüfungsteilnehmers

Einverständniserklärung des Ausbildungsbetriebes zur Durchführung des Projektes

Delbrück, 04.03.2021 — Ort, Datum

EURONICS Kerstjng
PHP Electronic GmbH
Lange Str. 62
33129 Delbrück
Tel: 05250/53838
Fax: 05250/53838

i.V. — Stempel und Unterschrift/en

Prüfungsausschuss der IHK: genehmigt: ☐ abgelehnt: ☐

Ort, Datum — Unterschriften

A Anhang

A.1 Logische Topologie der alten IT-Infrastruktur

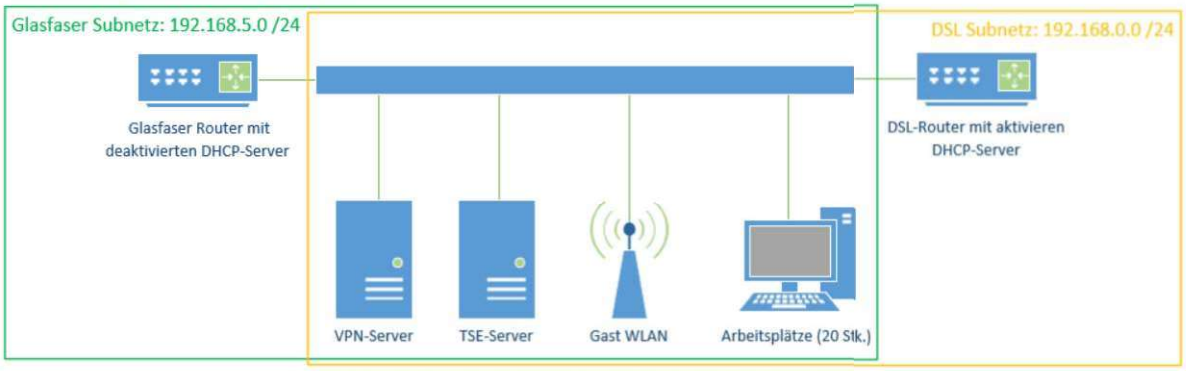

Abbildung 1: Logische Topologie der alten IT-Infrastruktur

Der DHCP-Server für das DSL-Subnetz wird genutzt, um neuen Arbeitsplätzen einen Internetzugang auch ohne statische IP-Adresse zu ermöglichen.

Alle Geräte bekommen eine statische Route, welche den Glasfaseranschluss priorisiert, mit Ausnahme des VPN- und des TSE-Servers. Diese priorisieren für eine bessere Lastenverteilung den DSL-Anschluss.

Technische Systemdokumentation für den Edge Router

Erstellungsdatum:
23.04.2021

Erstellt durch:
Lenard Corsmeier

Implementiert durch:
Lenard Corsmeier
l.corsmeier@euronics-owl.de
+49 5250 930140

Prüflingsnummer:
108 70263

Leitender Systemadministrator:
Andreas Breimhorst
a.breimhorst@php-electronic.de
+49 5250 930140

Auftraggeber:
PHP Electronic GmbH

Installationsort:
Lange Str. 62
33129 Delbrück
Germany

Inhaltsverzeichnis

Abbildungsverzeichnis

Quellenverzeichnis

Information	Quelle
Euronics Logo	Betriebsinterne Grafiksammlung
LANCOM Knowledge Base	https://support.lancom-systems.com/knowledge/
LANconfig und LANmonitor	https://www.lancom-systems.de/produkte/netzwerk-management/lantools/
Bilder	LANconfig

1 Einleitung

Diese technische Systemdokumentation beschreibt, die einzelnen Funktionen, welche am Erstellungsdatum in dem Edge Router implementiert sind.

Darüber hinaus werden die einzelnen Handlungsschritte erklärt, welche nötig sind um Änderungen an den beschriebenen Funktionen vorzunehmen.

Handlungsschritte in einem gestrichelten Rechteck müssen nur unter bestimmten Bedingungen durchgeführt werden. Weil die Wahrscheinlichkeit bei der momentanen Konfiguration sehr hoch ist, dass diese Bedingungen erfüllt werden, sind diese Punkte trotzdem in der jeweiligen Konfigurationsanleitung aufgeführt. Diese werden für eine bessere Übersicht jedoch gekennzeichnet.

Als Edge Router dient der LANCOM 1793 VA.

Ein Datenblatt des Routers lässt sich über die LANCOM Website oder mithilfe des QR-Codes downloaden.

Funktionen, welche nicht in der dieser Systemdokumentation beschrieben sind, können mithilfe der LANCOM Knowledge Base recherchiert werden.

Für einen Schnellzugriff steht ebenfalls ein QR-Code zur Verfügung.

Es ist zu beachten, dass keine Haftung für die Richtigkeit externer Inhalte übernommen wird.

Datenblatt des Routers:

Ersatzteile und Zubehör:

LANCOM Knowledge Base:

Für die Konfiguration wird die von LANCOM empfohlene und entwickelte Konfigurationssoftware LANconfig verwendet. Das Monitoring wird mithilfe des LANmonitors durchgeführt. Die Software kann ebenfalls über die LANCOM Website oder die dafür bereitgestellten QR-Codes geladen werden.

Download LANconfig.exe:

Download LANmonitor.exe:

2 Konfigurationsassistenten öffnen

Für die Konfiguration wird der LANCOM Router über das mitgelieferte Netzteil mit Strom versorgt. Danach wird ein PC mithilfe eines RJ45 Patchkabels mit dem einen Ethernet LAN-Port des Routers verbunden. Hierbei ist zu beachten, dass der Port ETH 1 als WAN Schnittstelle konfiguriert ist. Dieser kann also nicht verwendet werden.

Als nächstes wird die Konfigurationssoftware auf dem PC geöffnet. Der Router sollte automatisch gefunden werden. Andernfalls kann eine automatische oder manuelle Suche gestartet werden. Dies geschieht über die im Bild rot gegenzeichneten Buttons.

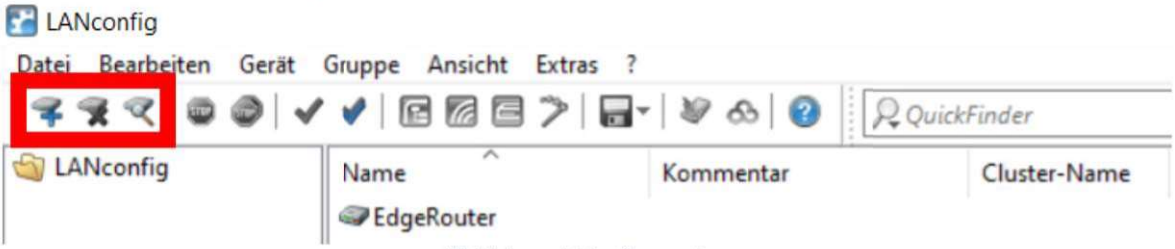

Abbildung 1:Geräte suchen

Wenn der Router trotzdem nicht angezeigt wird, sollte die Netzwerkkonfiguration geprüft oder gegebenenfalls der Router resettet werden. Wie der Router auf Werkseinstellungen gesetzt wird, kann der Systemdokumentation unter Punkt drei entnommen werden.

Sobald der Router registriert ist, kann der Konfigurationsassistent durch einen Doppelklick auf dem Gerät geöffnet werden. Für den Zugriff wird ein Benutzerkonto mit den richtigen Berechtigungen benötigt.

3 Werksreset durchführen

Das Gerät kann mithilfe des Resetbutton auf Werkseinstellungen zurückgesetzt werden.

Dieser kann mit einer Nadel durch ein kleines Loch auf der rechten Vorderseite betätigt werden. Auf dem Bild ist der Button rot markiert. Der Knopf muss gedrückt werden, bis alle Lampen rot leuchten.

Abbildung 2:LANCOM Router 1793VA

4 QuickFinder

Um die in der Systemdokumentation beschriebenen Punkte leicht zu finden, kann der QuickFinder genutzt werden. Dieser befindet sich in der Ecke oben links.

5 Updatestrategie

Der Router prüft täglich zwischen 0 und 1 Uhr, ob ein neues Softwareupdate (ausschließlich Stable Versionen) zur Verfügung steht. Sollte das der Fall sein, wird dieses zwischen 2 bis 4 Uhr installiert. Dadurch wird sichergestellt, dass die Software immer aktuell ist und somit die Gefahr eines Angriffes über eine Sicherheitslücke in der Software des Routers minimiert wird. Außerdem wird so verhindert, dass der Geschäftsablauf durch ein Update gestört wird.

Diese Einstellungen lassen sich unter dem Punkt „Software-Update“ anpassen.

6 Backupstrategie

Nach jeder Konfigurationsänderung über die LANconfig Software wird ein Backup des Routers erstellt.

Die Backups werden unter dem verschlüsselten Ordner „Backup Edge Router“ auf dem NAS-Laufwerk gespeichert. Den Zugang zu diesem Ordner besitzen Herr Bremhorst und Herr Corsmeier.

Dadurch wird sichergestellt, dass immer die aktuelle Konfiguration zur Verfügung steht, falls bei dem Router ein Softwareproblem vorliegt. Somit kann dieser schnellstmöglich wieder auf den Zustand der letzten Konfiguration zurückgesetzt werden. Die Verschlüsselung des Backup Ordners bewirkt, dass keine unberechtigten Personen Zugriff auf die Backupdatei bekommen.

Die Backupeinstellungen können in der LANconfig geändert werden. Dafür muss folgender Pfad geöffnet werden: Eigenschaften → Sicherung

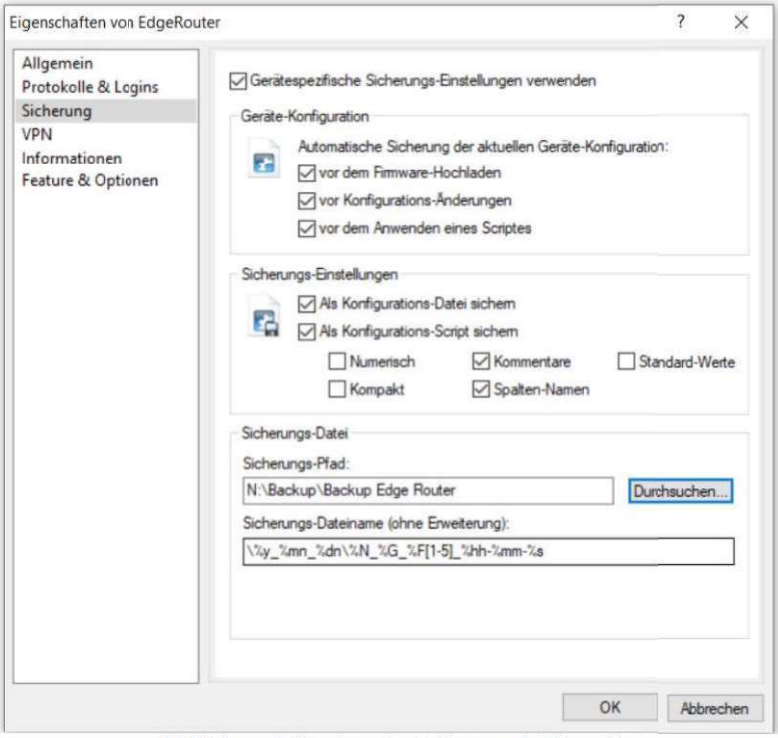

Abbildung 3:Backupeinstellungen LANconfig

7 Geräteinformationen ändern

Die Geräteinformationen geben einer Person grundlegende Informationen über das System.

Dazu gehören unter anderen Informationen über den zuständigen Administrator und die aktuelle Firmwareversion. Die genauen Parameter können dem Screenshot entnommen werden.

Mithilfe des Konfigurationsassistenten wird die manuelle Konfiguration geöffnet. Dort können unter folgenden Pfad die Geräteinformationen eingesehen oder geändert werden:

Management → Allgemein

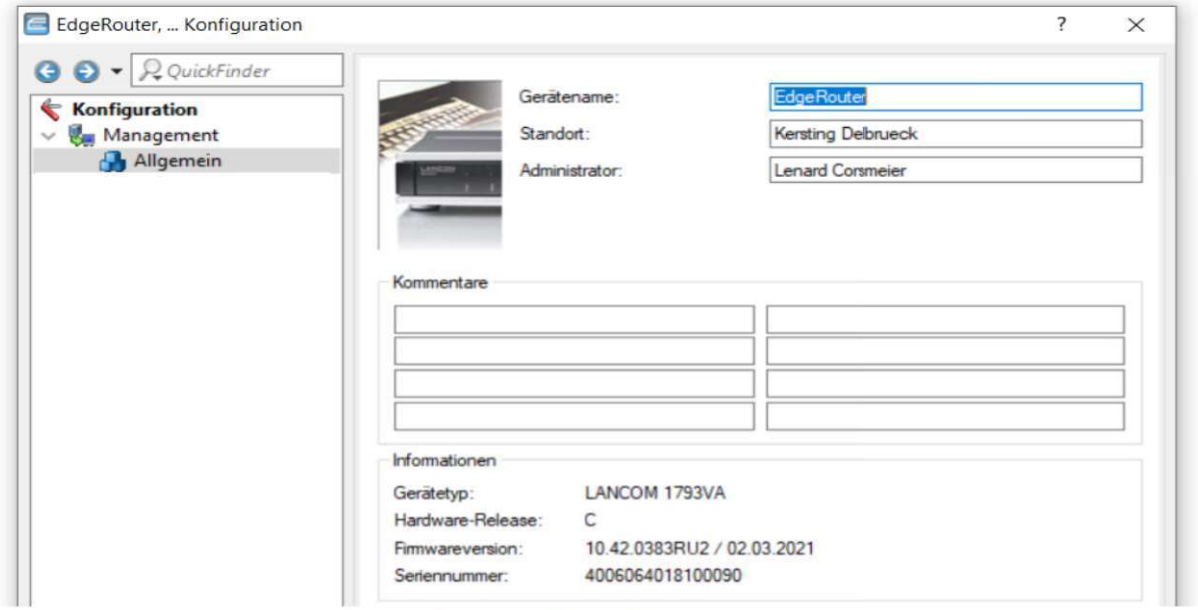

Abbildung 4:Grundinformationen

8 Benutzerkonten anlegen oder bearbeiten

Benutzerkonten lassen sich unter dem Punkt „Weitere Administratoren“ im manuellen Konfigurationsmenü anpassen oder editieren. Momentan ist dort ein Benutzerkonto für den Zugang über den LANmonitor konfiguriert. Dies Benutzerkonto wurde angelegt, da es die Möglichkeit gibt, mit den im LANmonitor hinterlegten Zugangsdaten das Konfigurationsmenü zu öffnen. Somit können Mitarbeiter den LANmonitor nutzen, aber nicht die Konfiguration ändern. Darüber hinaus besteht ein weiterer Sicherheitsaspekt darin, dass mit kompromittierten Zugangsdaten aus dem LANmanager kein Zugriff auf die Konfiguration besteht.

Der Screenshot zeigt die aktuelle Konfiguration des Benutzerkontos.

Für die Konfiguration eines Benutzerkontos gibt es zwei Autorisierungsebenen. Einmal die Zugriffsrechte, welche eine Grundlage für alle Funktionen bietet und die Funktionsrechte, welche die Zugriffsrechte übergehen. Hat ein Benutzer beispielsweise das Zugriffsrecht „nur lesen“, aber das Funktionsrecht „Grundeinst.-Assistent“, so kann dieser trotzdem den Grundeinstellungsassistenten öffnen und dessen Parameter bearbeiten.

Abbildung 5:Benutzerrechte

8.1 Root-Benutzer

Zusätzlich zu den manuell angelegten Benutzerkonten gibt es ein root-Benutzerkonto. Dieses bietet allumfassende Rechte und kann nicht eingeschränkt werden, weshalb dieses Konto besonders schützenswert ist und keinesfalls an dritte weitergegeben werden darf.

Das Passwort des Root-Benutzer lässt sich direkt unter dem Punkt Admin bearbeiten, solange die passenden Zugriffsrechte vorhanden sind.

8.2 Passwortrichtlinien

Passwörter, vor allen das des root Benutzers werden für eine maximale Sicherheit mithilfe eines Passwortgenerators und folgenden Parametern erzeugt.

- 15 Zeichen (maximal zulässige Passwortlänge)
- Groß- und Kleinbuchstaben
- Zahlen von 0 bis 9
- Sonderzeichen.

Spätestens nach einem Jahr werden die Passwörter durch den Administrator neu vergeben.

8.3 Anti Brute Force

Damit die Wahrscheinlichkeit verringert wird, dass Passwörter mithilfe eines Brute Force Angriffes kompromittiert werden, wird eine Login-Sperre von 5 Minuten verhängt, sollte ein Benutzer seine Logindaten 5-mal falsch eingegeben haben.

Die Anzahl der Login-Versuche und die Dauer der Sperre kann unter dem Punkt „Konfigurations-Login-Sperre“ geändert werden.

8.4 Zugriffsmöglichkeiten auf Interfaceebene

Die Zugriffsmöglichkeiten auf den Router können für Interfaces eingeschränkt werden. Diese Konfiguration kann unter dem Punkt Zugriffseinstellungen → Zugriffs-Rechte angepasst werden. Dafür muss das passende Interface gewählt werden. Dort können nun bestimmte Protokolle eingeschränkt werden.

Der Screenshot zeigt die momentane Konfiguration des LAN-Interfaces.

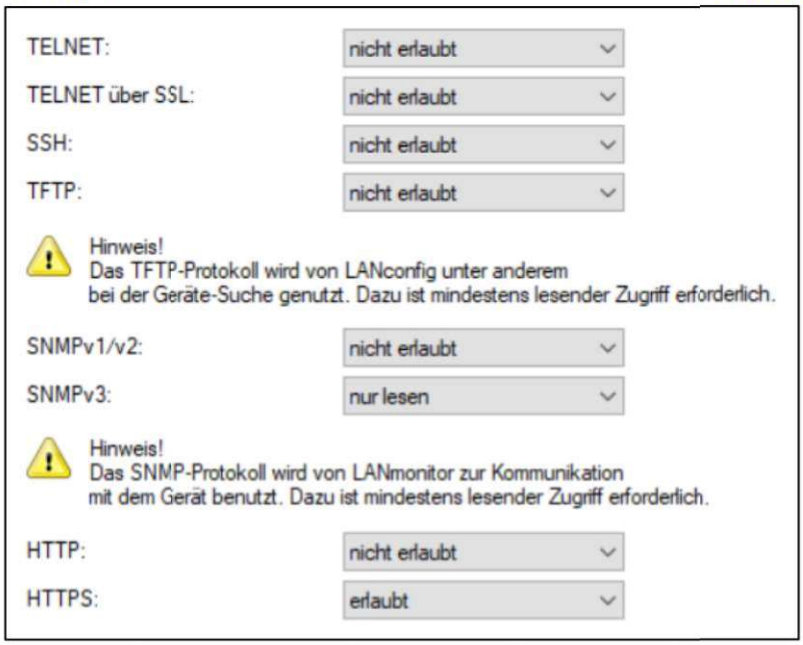

Abbildung 6:Protokolle für den Zugriff aus dem LAN

Da der Zugriff auf den Router nur durch das LAN erfolgen soll, sind alle Protokolle für die anderen Schnittstellen deaktiviert.

Hinweis: Diese Konfiguration lässt sich beispielweise mithilfe einer Fernwartungssoftware umgehen. Die ACL, welche unter Punkt 19 erläutert wird, blockiert jedoch den Traffic für Fernwartungsprotokolle. Sollte allerdings eine End to End VPN-Verbindung über HTTPS etabliert werden, so ist auch dieser Filter nutzlos.

9 WAN-Port für ein dediziertes Modem konfigurieren

Es können bis zu 3 Ethernet-Schnittstellen als WAN-Port konfiguriert werden. Damit bieten diese eine Anschlussmöglichkeit für beispielweise ein dediziertes Modem.

Um einen Ethernet-Port als WAN-Port zu konfigurieren muss der Konfigurationsassistent „Internetzugang einrichten“ gewählt werden.

Momentan ist der Port „ETH 1“ als WAN-Schnittstelle für den Glasfaseranschluss konfiguriert.

Die folgenden Handlungsschritte erläutern die Konfiguration eines Ethernet-Ports für die Verwendung eines Internetanschlusses der Deutschen Glasfaser. Diese können gegebenenfalls mit kleinen Änderungen auch für andere Provider übernommen werden.

1. Als erstes wird das gewünschte Interface ausgewählt. Da ein Ethernet-Port konfiguriert werden soll, wird hier der Punkt Ethernet-Schnittstelle gewählt
2. Danach wird die gewünschte Schnittstelle gewählt.
   (Bsp.: ETH 1 für die Deutsche Glasfaser)
3. Jetzt wird die Bezugsmöglichkeit der IP-Adressen gewählt. Die Deutsche Glasfaser betreibt hierfür einen eigenen DHCPv6-Server.
4. Als nächstes wird ausgewählt, wie der Provider den Zugang für IPv4 und IPv6 Netze bereitstellt. Die Deutsche Glasfaser nutzt hierfür DS-Lite (nur natives IPv6).
5. Als nächstes wird für den Anschluss eine Bezeichnung vergeben, damit dieser zu einem späteren Zeitpunkt eindeutig zugeordnet werden kann. Für den Glasfaseranschluss wird die Bezeichnung „GLASFASER“ gewählt.

6. Sollte der Provider einen VLAN-Tag verwenden, muss dieser nun eingetragen werden. Die Deutsche Glasfaser verwendet für diesen Anschluss keinen VLAN-Tag mehr, weshalb der Reiter „Es wird kein VLAN-Tag verwendet“ ausgewählt wird.
7. Sollten bereits weitere Internetanschlüsse konfiguriert sein, kann nun eine Backupverbindung ausgewählt werden. Sollte der Glasfaseranschluss ausfallen wird der gesamte Traffic automatisch über die Backupverbindung gleitet.
8. Wenn mindestens ein weiterer Internetanschluss vorhanden ist, wird nun eingestellt, wie der neue Anschluss genutzt werden soll. Dafür gibt es drei Funktionen, welche dem Screenshot zu entnehmen sind.

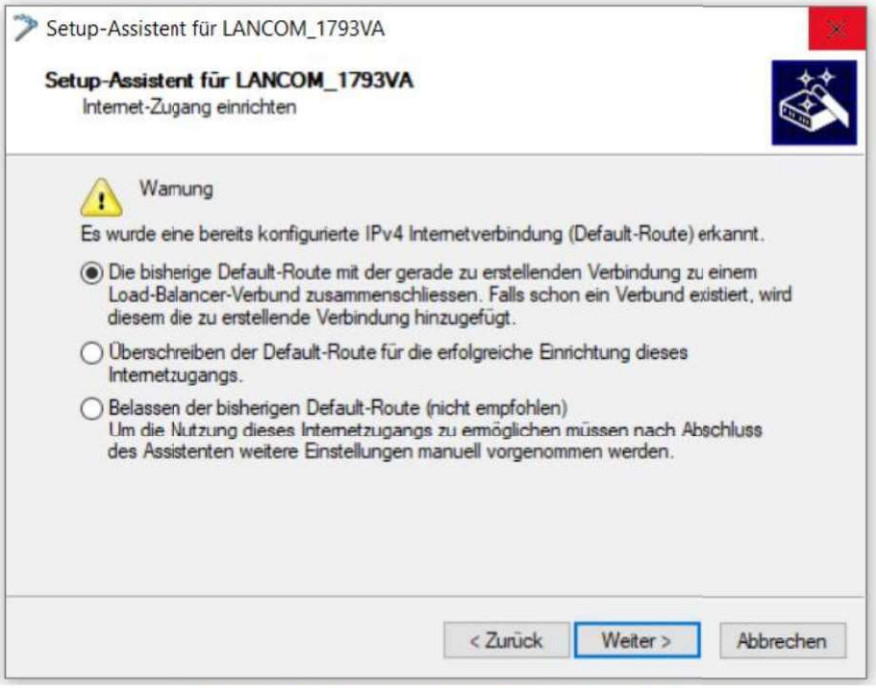

Abbildung 7:Konfiguration einer zweiten Default-Route

Weil die Internetanschlüsse in einen Load Balancer Verbund betrieben werden, wird wie auf dem Screenshot die Funktion Load Balancer gewählt.

9. Als nächstes wird abgefragt, welches IPv6 Parameter der Router nutzen soll. (Präfix, etc.) Da hierfür keine besondere Konfiguration benötigt wird, wird die Funktion „IPv6-Paramterer automatisch beziehen“ gewählt.
10. Danach wird nach dem gewünschten DS-Lite Gateway gefragt. Hierfür wird das Gateway des Providers genutzt. Die Adresse wird dem Router über den DHCPv6-Server des Providers mitgeteilt.

Nach diesem Schritt ist die Konfiguration abgeschlossen.

10 DSL-Anschluss konfigurieren

Die folgenden Handlungsschritte erläutern, wie der DSL-Port für einen Telekomanschluss konfiguriert wird.

Um mit der Konfiguration beginnen zu können muss der Konfigurationsassistent „Internetzugang einrichten“ gewählt werden.

1. Als erstes wird das gewünschte Interface ausgewählt. Da ein VDSL-Anschluss konfiguriert werden soll, wird hier der Punkt VDSL-Interface (ADSL) gewählt.
2. Danach wird das Land und der Provider ausgewählt.
3. Als nächstes wird ausgewählt, wie der Provider den Zugang für IPv4 und IPv6 Netze bereitstellt. Die Telekom nutzt hierfür Dual Stack (natives IPv6 und IPv4).

4. Als nächstes werden die Zugangsdaten für den Telekom Anschluss eingetragen.
5. Sollten bereits weitere Internetanschlüsse konfiguriert sein, kann nun eine Backupverbindung ausgewählt werden. Sollte der DSL-Anschluss ausfallen, wird der gesamte Traffic automatisch über die Backupverbindung gleitet.
6. Wenn mindestens ein weiterer Internetanschluss vorhanden ist, wird nun eingestellt, wie der neue Anschluss arbeiten soll. Dafür gibt es drei Funktionen, welche dem Screenshot zu entnehmen sind.

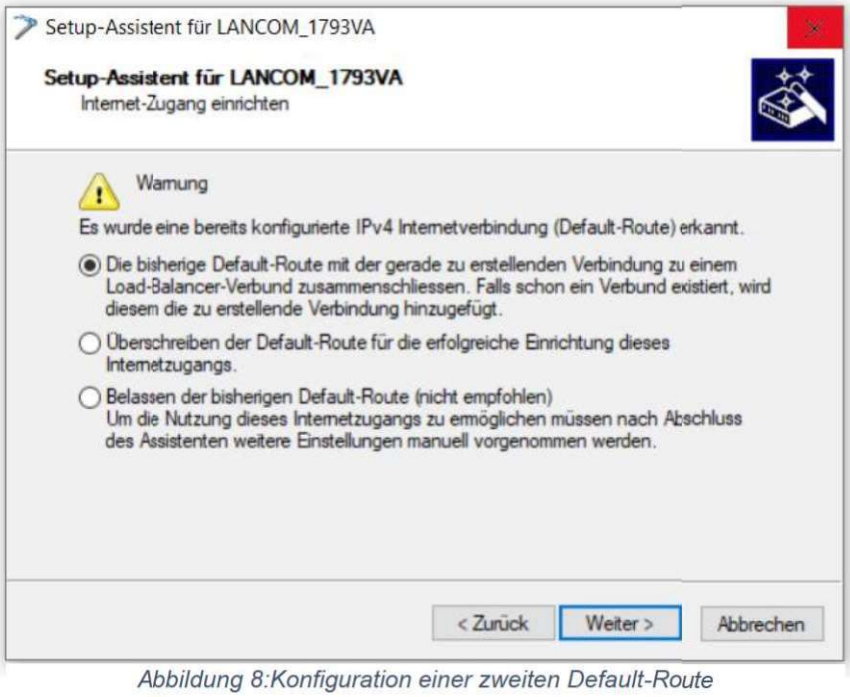

Abbildung 8:Konfiguration einer zweiten Default-Route

Weil die Internetanschlüsse in einen Load Balancer Verbund betrieben werden, wird wie auf dem Screenshot die die Funktion Load Balancer gewählt.

11. Als nächstes wird abgefragt, welches IPv6 Parameter der Router nutzen soll. (Präfix, etc.) Da hierfür keine besondere Konfiguration benötigt wird, wird die Funktion „IPv6-Paramterer automatisch beziehen“ gewählt.

Sobald alle oben beschriebenen Handlungsschritte bearbeitet sind, ist der Anschluss konfiguriert

11 Routing Protokoll

In dem Firmennetz sind keine Core Router vorhanden, weshalb die Implementierung eines dynamischen Routingprotokolls nicht notwendig ist. Allerding ist zu erwähnen, dass RIP standardmäßig aktiviert ist. Sollten mehrere Core Router über redundante Verbindungen implementiert werden, empfiehlt sich allerding die Nutzung von Link State Protokollen wie open shortest path first.

Sollte die Verwendung eines anderen Routing Protokolls gewünscht sein, dann kann dieses über den Reiter „Routing Protokolle“ aktiviert und konfiguriert werden.

12 Statisches Routing

Für den VPN-Server muss eine statische Route konfiguriert werden, damit das dahinterliegende LAN adressiert werden kann.

Statische IPv4 Routen können unter dem Punkt „IPv4 Routingtabelle“ eingetragen werden.

Dafür müssen folgende Handlungsschritte durchgeführt werden:

1. Eintragen des IPv4-Netzes mit Subnetzmaske oder eintragen einer IP-Adresse mit der Subnetzmaske 255.255.255.255
2. Als Schaltzustand wird „Route ist immer aktiv“ gewählt. Somit werden Datenpakete immer an das Ziel geschickt, auch wenn dieses offline sein sollte.
3. Als Router wird die statische IP-Adresse des lokalen Ziels oder die gewünschte Gegenstelle ausgewählt.

Info: Alle anderen Werte können im Regelfall bei den Standardwerten belassen werden.

Für den VPN-Server ergibt sich somit folgender Eintrag:

Abbildung 9:Statisches Routing

Hinweis: Da es sich bei dem VPN-Server um ein lokales Gerät handelt, wird keine IP-Maskierung durchgeführt.

13 Load Balancing

Damit die beiden Internetanschlüsse bestmöglich genutzt werden, wird ein Load Balancing für die beiden Anschlüsse eingerichtet.

Damit der Load Balancer einwandfrei arbeitet, müssen einige Einstellungen angepasst werden.

13.1 Datenrate anpassen

Da der Load Balancer die Verteilung der einzelnen Verbindungen anhand der Datenrate des Anschlusses gewichtet (Weighted Least Connection), muss der zur Verfügung stehende Downstream und Upstream angegeben werden.

Für einen Ethernet WAN-Port (beispielweise der Glasfaseranschluss) müssen dafür folgende Handlungsschritte durchgeführt werden:

1. Interface-Einstellungen öffnen
2. den gewünschten Anschluss auswählen.
3. die zur Verfügung stehende Downloadrate und Uploadrate eintragen
4. Der externe Overhead ergibt sich aus den Daten, die das Modem selbst noch vor jedes Paket setzt. Bei einem dedizierten Modem beträgt dieser im Regelfall 0 Byte, da die Pakte direkt weitergeleitet werden. Sollte der Anschluss über eine PPPoE Verbindung betrieben werden, wird der externe Overhead beispielweise auf 10 Byte gesetzt.

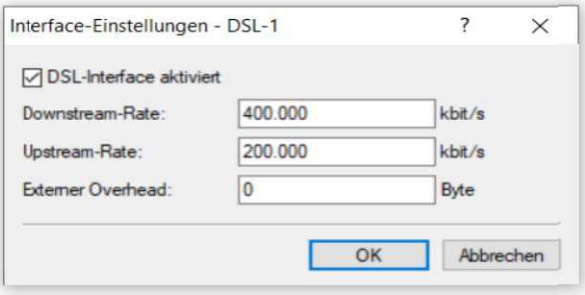

Abbildung 10: Interface Einstellungen

Der DSL-Anschluss muss nicht angepasst werden, da dieser seine Konfiguration direkt vom Provider bezieht.

13.2 Balance-Sekunden und Binding-Minuten

Bei dem Load Balancer ist zu beachten, dass dieser mit sogenannten Balance-Sekunden (Für eine möglichst schnelle Datenrate werden in diesen Zeitraum beide Internetanschlüsse genutzt) und Binding-Minuten (Nachdem die Balance Sekunden abgelaufen sind, wird die Verbindung während dieses Zeitraums auf eine der beiden Leitungen gebunden) arbeitet. Da ein Server, welcher eine Authentizitätsprüfung durchführt, die Verbindung abbricht, wenn dieser Datenpakete mit zwei verschieden Quell IP-Adressen bekommt, werden die Balance Sekunden auf 0 gestellt. Dadurch besteht eine geringere Datenrate, welche bei der Bandbreite der beiden Internetanschlüsse nicht zwingend notwendig ist. Dafür wird verhindert, dass beispielweise ein Online Shop die Verbindung abricht, wenn ein Mitarbeiter oder ein Passwortmanager probiert, sich während des Balancing-Zeitraums zu authentifizieren. Damit der Mitarbeiter genügend Zeit hat, die gewünschte Tätigkeit durchzuführen, werden die Binding Minuten auf 30 gesetzt. Dies bietet auch noch darin einen Sicherheitsaspekt, dass eine Verbindung höchstwahrscheinlich nach 30 Minuten beendet wird, sollte ein Mitarbeiter vergessen, sich auszuloggen. Das hängt aber von der Konfiguration des jeweiligen Servers ab.

Die beiden Werte können unter dem Punkt Load-Balancing geändert werden.

Darüber hinaus können bei Bedarf über den Punkt „Load-Balancing…“ weitere Gegenstellen hinzugefügt werden.

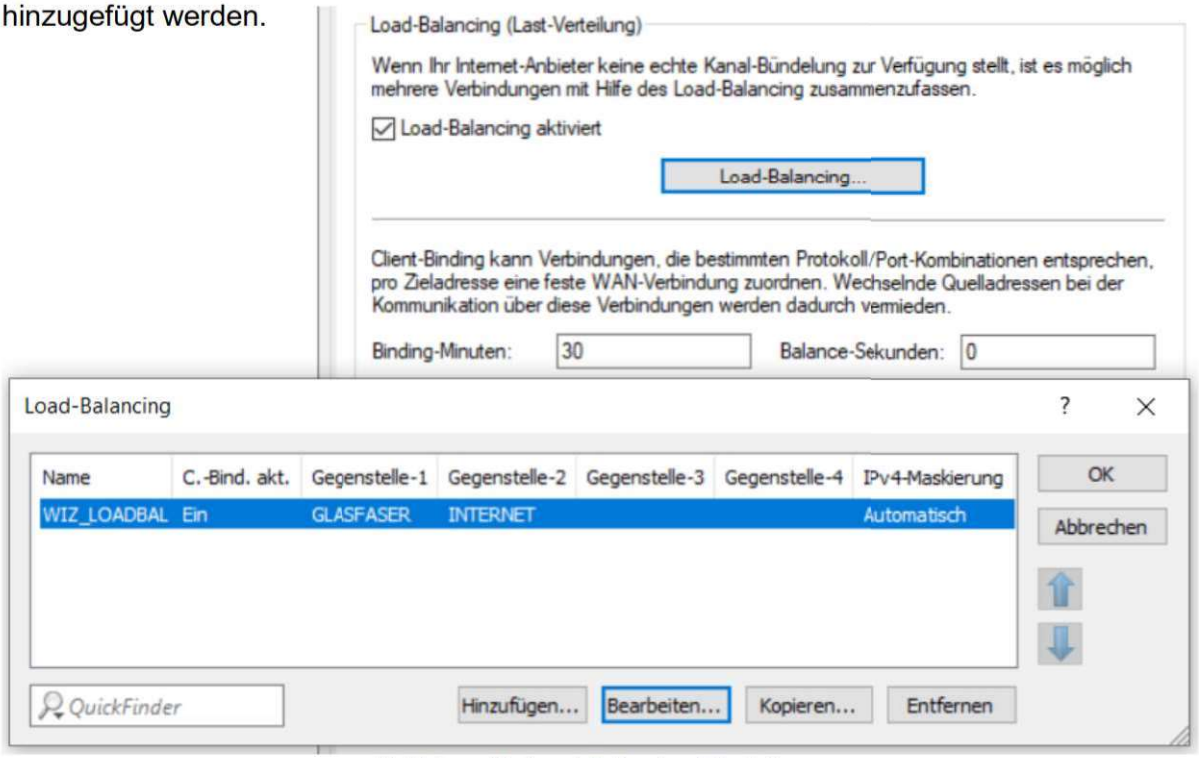

Abbildung 11: Load Balancing Einstellungen

14 IPv6

Die Vergabe von Globaler IPv6-Adressen an Endgeräte ist aufgrund der Nutzung eines Load Balancers deaktiviert. Es besteht zwar die Möglichkeit, beiden Internetanschlüssen das gleiche statische Präfix zuzuweisen, oder Dienste wie NPTv6 oder NAT66 einzusetzen. Die Implementierung ist aber mit zusätzlichen Kosten verbunden und bietet dem Unternehmen momentan keinen entscheidenden Vorteil, weshalb der Auftraggeber vorerst die Implementierung eines klassischen IPv4 Netzes beauftragt hat.

IPv6 kann unter dem Reiter IPv6 → Allgemein aktiviert werden.

15 Zeiteinstellungen anpassen

Als Zeitzone wurde +01 gewählt. Zwischen Sommer und Winterzeit wird automatisch gewechselt. Als NTP-Server dient „pool.ntp.org“, welcher alle 60 Sekunden abgefragt wird. Dabei handelt es sich um ein Internet Cluster von NTP-Server, wodurch eine sehr hohe Verfügbarkeit garantiert wird.

Die Zeitzone kann unter dem Punkt „Datum und Uhrzeit“ ausgewählt werden.

Der NTP-Server und der Abfrageintervall lassen sich unter dem Punkt „NTP-Client-Einstellungen“ ändern

16 DHCP-Server

Damit jedes Endgerät einfach und schnell eine IP-Adresse bekommt, ist ein DHCP-Server konfiguriert. Die momentane Konfiguration ist dem Screenshot zu entnehmen. Die Konfiguration wurde aus einem bereits vorhandenen DHCP-Server übernommen und bietet eine ausreichende Skalierbarkeit. Außerdem besitzen mehrere Geräte statische IP-Adressen.

Der DHCP-Server kann unter dem Reiter „DHCP-Netzwerke“ konfiguriert werden.

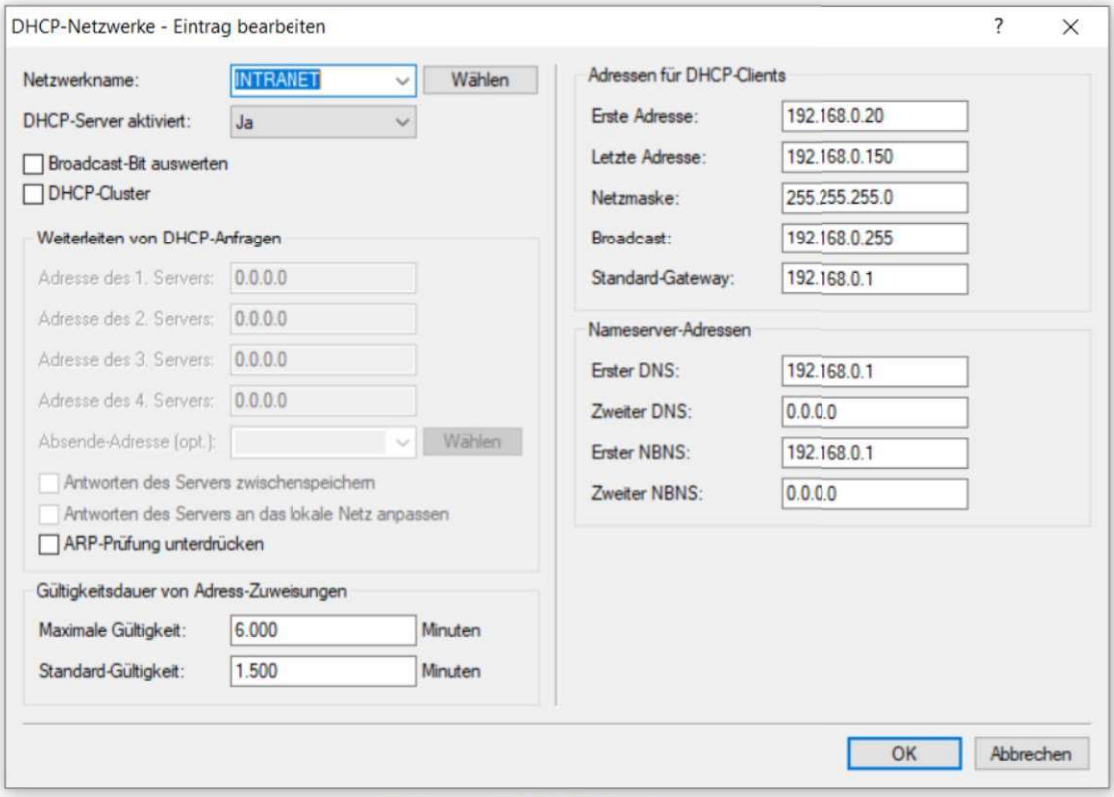

Abbildung 12:DHCP Konfiguration

17 DNS-Server

In der Konfiguration des DHCP-Servers ist der lokale DNS-Server als Primärer DNS-Server eingetragen. Dadurch werden DNS-Anfragen gecached und können schnellstmöglich erneut abgefragt werden. Außerdem ist es so in Zukunft möglich einfach DNS-Filterregeln zu implementieren.

Sollte eine Anfrage nicht durch den lokalen DNS-Server beantwortet werden, stellt dieser eine Anfrage an den Cloudflare DNS-Server.

Der Cloudflare DNS-Server wurde aus fünf Gründen gewählt:

1. Bietet eine geringere Latenz als die DNS-Server der Provider.
2. Daten werden für maximal 24 Stunden gespeichert.
3. Bietet einen rudimentären Malwareschutz.
4. Steht kostenfrei zur Verfügung.
5. Eine Nutzung für gewerbliche Zwecke ist in den AGB erlaubt.

Die DNS-Weiterleitungen können unter dem Reiter DNS → Weiterleitungen erstellt oder bearbeitet werden.

Dafür muss lediglich die primäre und sekundäre IP-Adresse des Servers unter dem Reiter „Gegenstelle“ eingetragen werden.

Die momentane Konfiguration sieht wie folgt aus:

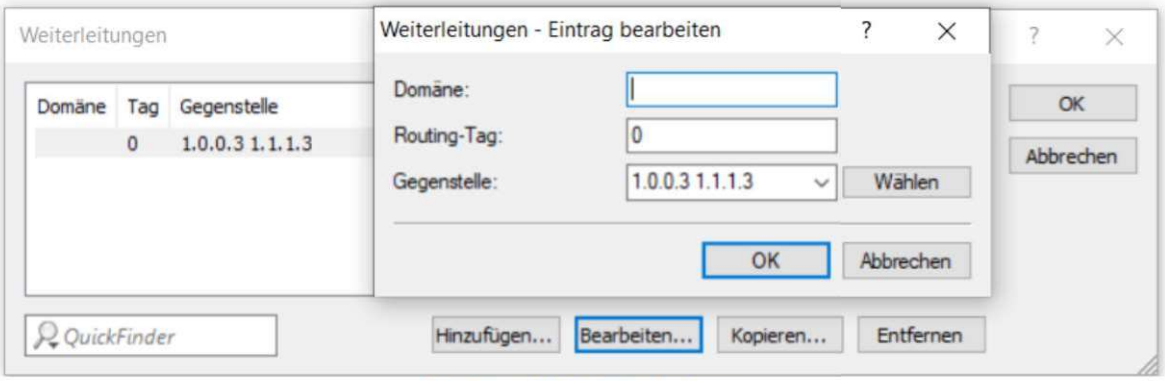

Abbildung 13:DNS-Forwarding

Sollte die Nutzung des DNS-Servers eines ISP gewünscht sein, dann kann dieser einfach mit der Auswahl des jeweiligen Internetanschlusses ausgewählt werden. Alternativ kann auch der Load Balancer gewählt werden. Dann entscheidet dieser auf Grundlage seiner Konfiguration, an welchem ISP DNS-Server die Anfrage weitergeleitet wird.

18 System Monitoring

Für das System Monitoring wird der LANmonitor verwendet. Das Protokoll für das Monitoring ist SNMPv3 (Authentifizierung mit SHA256 und Verschlüsselung mit AES256). Somit wird ein Angreifer daran gehindert, eigenständig Anfragen an den Router zu stellen oder authentifizierte Anfragen mitzulesen (Man in the middle attack). Die Autorisierung erfolgt anhand der Benutzerrechte des Benutzerkontos, welches für die Authentifizierung genutzt wird. Wie unter Punkt 5 bereits erwähnt, besteht für die Verwendung des LANmonitors eine eigenes Benutzerkonto.

Momentan ist der Zugriff über SNMP v1 und v2 deaktiviert. Für SNMPv3 bestehen nur Leserechte.

Die Konfiguration des Simple Network Management Protocol erfolgt unter folgendem Pfad:

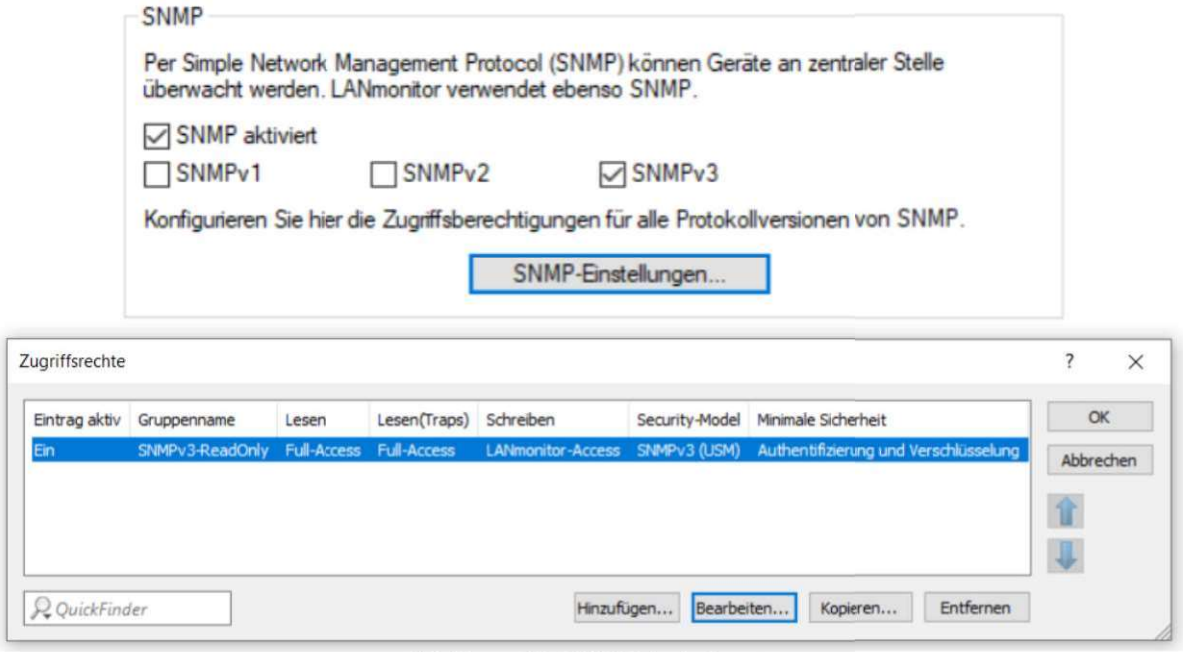

Abbildung 14: SNMP Einstellungen

Unter dem Punkt „SNMP“ können zusätzlich die Protokollversionen v1 und v2 aktiviert werden. Da diese keine Verschlüsselung und Authentifizierung besitzen wird davon abgeraten.

Die Konfiguration des LANmonitors funktioniert genau wie die Konfiguration der LANconfig.

Somit kann die Anleitung unter Punkt 2 auch für die Konfiguration des LANmonitors genutzt werden.

19 Access Control List

Die Konfiguration der ACL erfolgt als Whitelist. Somit wird der jeglicher Zugriff erst einmal blockiert.

Die jeweiligen IP-Adressen und Ports werden für eine bessere Verständlichkeit nicht aufgezählt, liegen aber sowohl Herrn Breimhorst als auch Herrn Corsmeier in Schriftform vor.

In der ACL sind folgende Einträge vorhanden:

1. **PERMIT_HTTP_HTTPS_SMTP_IMAP:** Erlaubt jedem Gerät im LAN über HTTPS und HTTP Anfragen an einen Web-Server zu stellen, Mails mit SMTP zu versenden und Mails über IMAP zu empfangen.
   Hinweis: POP3 wird in dem Unternehmen nicht genutzt.
2. **PERMIT_DNS:** Erlaubt jedem Gerät im LAN DNS-Anfragen an den lokalen DNS-Server zu stellen.
3. **PERMIT_ICMP:** Erlaubt jedem Gerät im LAN für Testzwecke ICMP Anfragen an den Google DNS-Server zu senden.
4. **PERMIT_EURONICS_VPN:** Erlaubt nur dem VPN-Server über die für den ordnungsgemäßen Betrieb benötigten Ports zu kommunizieren.
   Hinweis: Portweiterleitungen beachten!
5. **PERMIT_TSE:** Erlaubt nur dem TSE-Server über die für den ordnungsgemäßen Betrieb benötigten Ports zu kommunizieren.
   Hinweis: Portweiterleitungen beachten!
6. **DENY_ANY:** Verbietet jeglichen Zugriff auf das System, solange keine Ausnahme konfiguriert ist.

Die ACL kann unter dem Reiter „IPv4-Regeln“ → „Regeln…“ konfiguriert werden.

Dafür müssen folgende Handlungsschritte durchgeführt werden:

1. Unter den Punkt „Allgemein“ wird eine Bezeichnung für die Regel vergeben. Außerdem kann diese dort aktiviert und deaktiviert werden.
2. Unter dem Punkt Aktionen kann ausgewählt werden, wie mit den Paketen verfahren wird, z.B.: zulassen oder verwerfen.
3. Unter dem Punkt QoS können bestimmte Einstellungen für das weitere Verfahren mit der Sitzung getroffen werden. Z.B. kann die Bandbreite für die Sitzung, einen Client oder für jeglichen Datendurchsatz limitiert oder garantiert werden.
4. Als nächstes wird unter dem Punkt Stationen die Quell- und Ziel-Station ausgewählt. Dafür können unter andern einzelne IP-Adressen, IP-Netze oder MAC-Adressen dienen.
5. Unter dem Punkt Dienste werden nun die gewünschten Quell- und Ziel-Ports ausgewählt. Es besteht die Möglichkeit, Ports manuell einzugeben oder diese über ein Menü auszuwählen.

20 SPI-System

Stateful Paket Inspection ist ein dynamischer Paketfilter. Dieser verwirft jegliche Pakete, welche nicht durch einen Client aus dem LAN angefragt wurden oder für die keine Portfreigabe konfiguriert ist.

Unter dem Punkt „Port-Forwarding“ können Portfreigaben konfiguriert werden. Durch eine Portfreigabe kann beispielweise ein Web-Server, welcher hinter einer SPI-Firewall steht trotzdem erreicht werden.

In dem Router wurden Portfreigaben für den VPN- und dem TSE-Server konfiguriert.

Für eine Konfiguration werden folgende Schritte durchgeführt:

1. eintragen des gewünschten Ports auf Seitens des WANs
2. eintragen der Gegenstelle, über welche der Port geöffnet werden soll.
3. eintragen der Server-Adresse im LAN.
4. eintragen des Map-Ports für die LAN-Seite. (Über diesen Port wird das Packet im LAN weitergeleitet.)
5. das zu nutzende Protokoll wählen (TCP/UDP)
6. ggf. eine WAN-Adresse, wenn der Port nur für einen bestimmten Server geöffnet werden soll.

Beispiel:

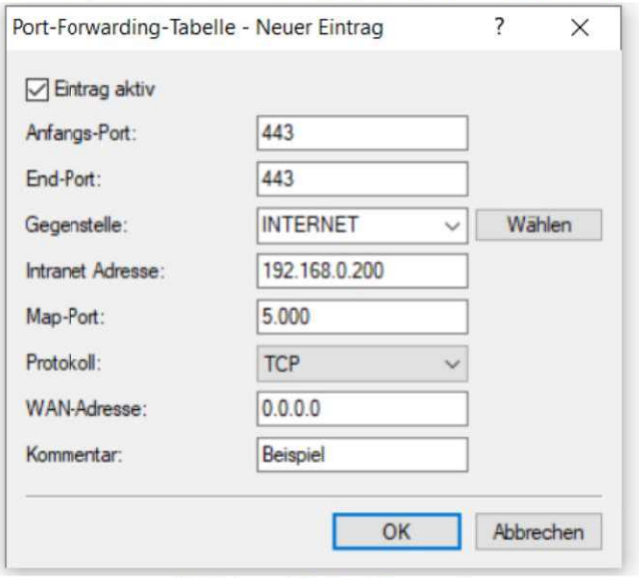

Abbildung 15: Port-Forwarding

Anfrage aus dem WAN
Port: 443
IP: beliebig
Gegenstelle: INTERNET
Protokoll: TCP

Weiterleitung im LAN
Port: 5.000
IP: 192.168.0.200
Protokoll: TCP

21 DoS-Protection

Bei einem DoS-Angriff wird das Zielsystem mit so vielen Anfragen konfrontiert, dass dieses nicht mehr in der Lage ist, seine Aufgabe wie gewünscht zu erfüllen.

Um einen solchen Angriff abzuwehren, ist eine DoS-Protection konfiguriert.

Diese sorgt dafür, dass ab einer vorher definierten Anzahl an initialisierten Verbindungen von einer Quelle alle bestehenden Anfragen verworfen werden. Darüber hinaus ist das System so konfiguriert, dass dieses eine SNMP-Meldung versendet und die Absenderadresse für 10 Minuten sperrt. Dadurch ist ein weiterer DoS-Angriff von dieser Adresse erst einmal ausgeschlossen. Das System hat Zeit, um die noch ausstehenden legitimen Anfragen abzuarbeiten und der Administrator kann geeignete Gegenmaßnahmen durchführen.

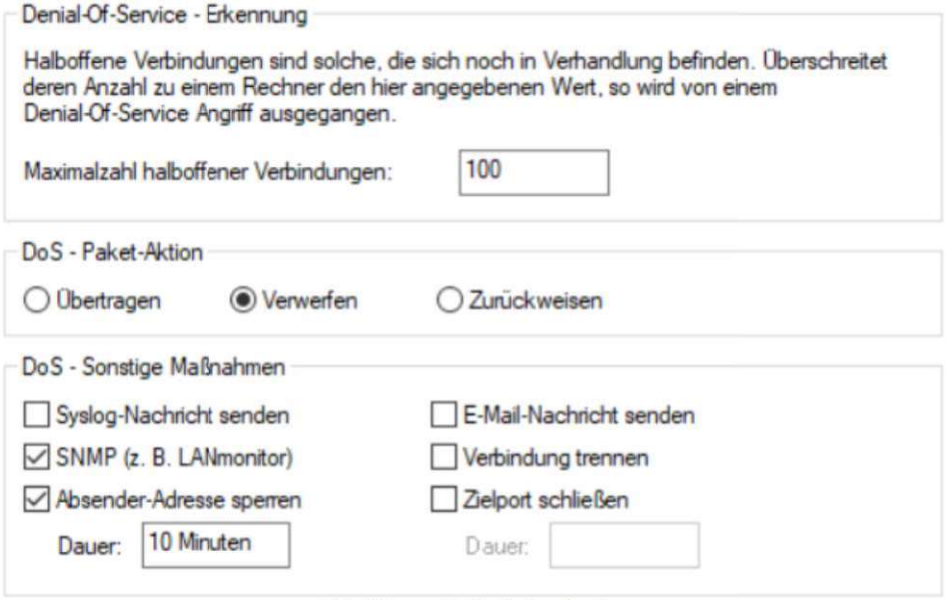

Abbildung 16:DoS-Protection

22 Intrusion Prevention/ Detection System

Das von dem Router genutzte IPS/IDS System ist signaturbasiert (ohne Deep Packet Inspection). Dieses wird momentan als Intrusion Prevention System eingesetzt.

Für den momentanen Anwendungsfall kann die Konfiguration bei den Standartwerten belassen werden.

Die Konfiguration kann unter dem Reiter „IDS“ angepasst werden. Momentan wird das System mit der im Screenshot gezeigten Konfiguration verwendet.

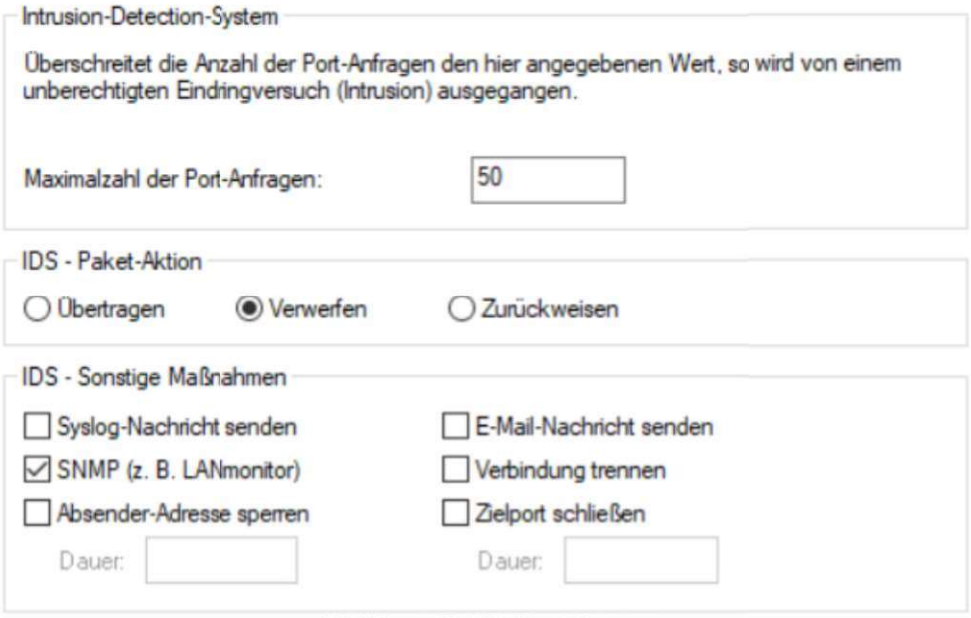

Abbildung 17:IPS Einstellungen

Hinweis: Wenn die Funktion „Übertragen“ ausgewählt ist und unter dem Punkt „IDS – Sonstige Maßnahmen“ keine weitere Abwehrmaßnahme aktiviert sind, dann wechselt das System von dem Intrusion Prevention Modus in den Intrusion Detection Modus. Daraufhin versendet das System nur noch Warnungen über die gewählten Informationskanäle.

23 Voice over IP für eine ISDN Telefonanalage

Bei VoIP werden die Daten nicht analog wie bei der herkömmlichen Telefonie übertragen, sondern als digitales Signal mithilfe des Internet Protokolls. Die Kommunikation erfolgt über einen SIP-Server, welcher als Schnittstelle zwischen dem IP-Netz und dem TK-Netz dient.

Die bisher genutzte ISDN TK-Anlage bietet keine VoIP-Schnittstelle, weshalb der Router in diesen Fall als Schnittstelle zwischen der TK-Anlage und dem SIP-Gateway fungiert.

Der Telefonie Anbieter ist die Telekom.

Für die Konfiguration müssen folgende Handlungsschritte durchgeführt werden:

1. In dem ersten Schritt wird die gewünschte Leitung gewählt. Bei der Telekom handelt es sich um einen SIP-Provider.
2. Als nächstes muss ausgewählt werden, für welches Endgerät die Leitung konfiguriert wird. Für die ISDN TK-Anlage wird der Punkt „ISDN-Endgerät“ gewählt.
3. In dem nächsten Handlungsschritt wird der SIP-Provider (T-Online) ausgewählt und die interne Standardnummer vergeben. An diese Nummer werden später alle ankommenden Anrufe weitergeleitet. Als Standardnummer wird die 930140 genutzt.
4. Danach werden die Logindaten für den SIP-Provider angegeben. Bei der Telekom bestehen die Logindaten aus der Rufnummer, der hinterlegten E-Mail-Adresse und dem Passwort.
5. Als nächstes wird der gewünschte ISDN-Port ausgewählt, an welchen später die TK-Anlage angeschlossen werden wird.
6. Danach werden ISDN-Benutzer angelegt. Dabei handelt es sich um die beim SIP-Provider hinterlegten Rufnummern. Welche Rufnummern hinterlegt sind, und welche Daten für das Anlegen eines ISDN-Benutzers benötigt werden, kann den Screenshots entnommen werden.

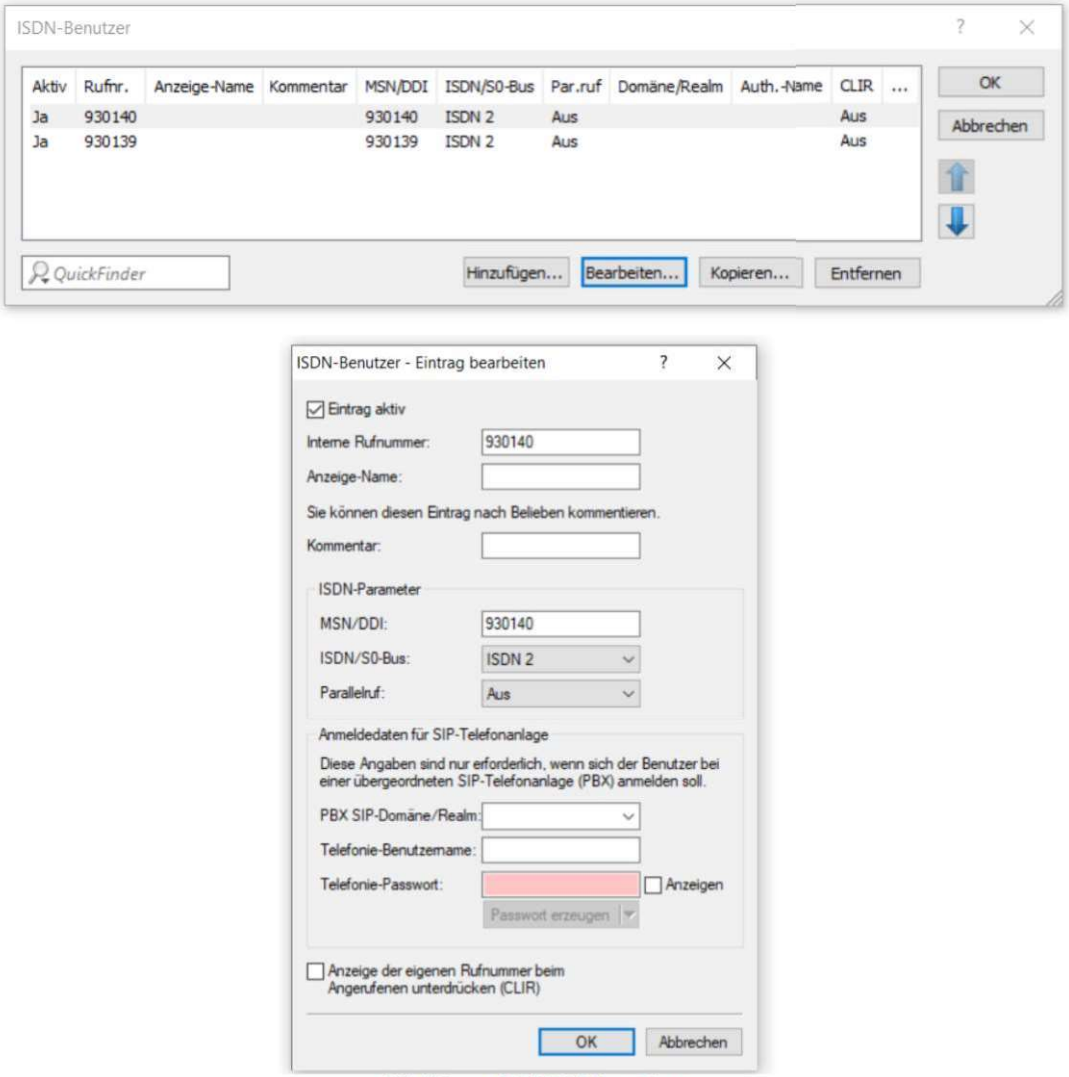

Abbildung 18:ISDN-Benutzer

Hinweis: Für den SIP-Server muss weder ein Eintrag in die ACL noch eine Portfreigabe implementiert werden. Dies übernimmt der Router automatisch.

Die Funktion kann unter folgenden Pfad durch entfernen des Hakens deaktiviert werden: Sonstige Dienste → Dienste → Firewall-Sperregeln für SIP-Pakete ignorieren.

7. Als nächstes wird die spontane Amtseinholung aktiviert. Diese sorgt dafür, dass direkt Amtsgespräche geführt werden können. Es muss also keine Null vorgewählt werden. Für die Interne Telefonie muss dafür „**“ gewählt werden, damit der Router weiß, dass es sich um eine interne Rufnummer handelt.
8. Danach wird die Landesvorwahl (49) und die Ortsvorwahl (5250) gewählt, damit der Router Ortgespräche und nationale Gespräche passend zuordnen kann. Diese sind ohne führende Null anzugeben.