Projekt Dokumentation Messeauftritt:

Gruppenmitglieder: Samuel Schreiber

Inhalt

[1 Einführung 3](#_Toc124368643)

[2 Anforderungsanalyse 3](#_Toc124368644)

[2.1 Situationsbeschreibung 3](#_Toc124368645)

[2.1.1 Teilprojekt SAE: Datenerfassung Neukunden 3](#_Toc124368646)

[2.1.2 Teilprojekt ITS: WLAN 3](#_Toc124368647)

[3 Teilprojekt ITS 4](#_Toc124368648)

[3.1 Netzwerkinfrastruktur Stand 4](#_Toc124368649)

[3.1.1 Netzwerkaufbau 4](#_Toc124368650)

[3.1.2 Anbindung Messenetzwerk 4](#_Toc124368651)

[3.1.3 Netzwerk Einrichtung und IP-Zuweisung 4](#_Toc124368652)

[3.1.4 Routing 5](#_Toc124368653)

[3.2 WLAN 5](#_Toc124368654)

[3.2.1 Zugangsbeschränkung 5](#_Toc124368655)

[3.2.2 Sicherheit 5](#_Toc124368656)

[3.2.3 Anbindung von Clients 5](#_Toc124368657)

[3.3 VPN 5](#_Toc124368658)

[3.3.1 Konfiguration im Packet-Tracer: 5](#_Toc124368659)

[3.3.2 Alternative Konfiguration mit WireGuard 7](#_Toc124368660)

[3.4 Messe-App 8](#_Toc124368661)

[3.5 Alternativer Lösungsansatz für mehr Komfort 8](#_Toc124368662)

Tabellenverzeichnis

[Tabelle 1: Verwendete Netzwerke 4](#_Toc124091702)

Abbildungsverzeichnis

[Abbildung 1: Netzwerkaufbau - Packet Tracer 4](#_Toc124363732)

Abbildung 2: Startbildschirm - Messe-App................................................................................8

# Einführung

Im Rahmen des Projekts Messeauftritt soll eine WLAN-Infrastruktur und eine Software zur Erfassung von Kundendaten bereitgestellt werden.

# Anforderungsanalyse

## Situationsbeschreibung

Die Firma XYZ plant den Besuch einer Messe. Auf der Messe sollen neben den üblichen Tätigkeiten nach Möglichkeit auch Daten potenzieller Neukunden erhoben und gespeichert werden. Zu diesem Zweck kann der Messestand Gutscheine ausstellen, mit denen vergünstigte Angebote auf der Messe wahrgenommen werden können. Voraussetzung ist die Registrierung im Portal der Firma XYZ.

### Teilprojekt SAE: Datenerfassung Neukunden

Während des Messeauftritts sollen von Kunden im Self-Service Kundenkarten erstellt werden können, mit denen dann der Zugang zu weiteren Messeangeboten möglich wird. Dabei sollen Nachname, Vorname, Anschrift erfasst werden. Zusätzlich sollen ein oder mehrere Produktgruppen angegeben werden können, für die besonderes Interesse besteht.

Die Speicherung der Daten kann in einer Datenbank oder einem anderen geeigneten Format erfolgen. Da das Firmen-Netzwerk über VPN angebunden werden soll, können Sie davon ausgehen, dass Sie die Datenbank oder ein gemapptes Verzeichnis direkt ansprechen können.

Die gespeicherten Daten sollen von den MitarbeiterInnen auch abgerufen und durchsucht werden können. Da es sich um einen Self-Service handelt muss sichergestellt werden, dass nicht jede Person das System frei nutzen kann.

### Teilprojekt ITS: WLAN

Sie sollen für den Messeauftritt ein WLAN planen, da Sie nicht auf das dort verfügbare öffentliche WLAN zugreifen wollen. Zu diesem Zweck erhalten Sie vom Messeveranstalter einen LAN-Zugang mit einem eigenen Subnetz. Das WLAN soll nicht öffentlich sein und eine /26 Subnetzmaske haben.

Das Netzwerk muss so aufgebaut sein, dass die im Teilprojekt SAE erfassten Daten bei Bedarf an die Firmenzentrale übermittelt werden können. Die Nutzung des Netzwerks soll nur für berechtigte Personen möglich sein. MitarbeiterInnen des Messestandes sollen sich mit Benutzername und Passwort anmelden. Sollte es bei Ihrem Ansatz notwendig sein, dass Besucher sich in das von Ihnen angebotene WLAN einwählen, dürfen MitarbeiterInnen und Besucher sich nicht im gleichen WLAN befinden.

# Teilprojekt ITS

## Netzwerkinfrastruktur Stand

### Netzwerkaufbau

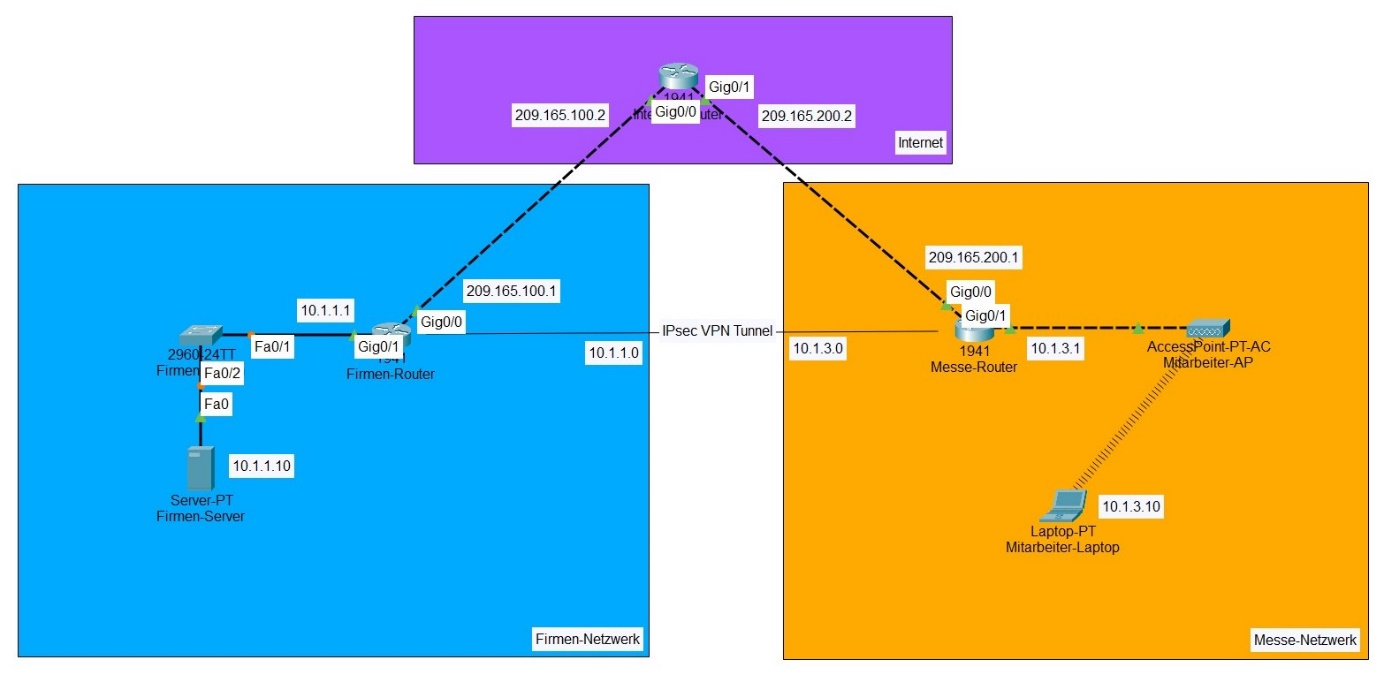


Abbildung 1: Netzwerkaufbau - Packet Tracer

|  |  |
| --- | --- |
| **Subnetz** | **Subnetzmaske** |
| 10.1.1.0 | 255.255.255.0 |
| 10.1.3.0 | 255.255.255.192 |
| 209.165.100.0 | 255.255.255.0 |
| 209.165.200.0 | 255.255.255.0 |

Tabelle 1: Verwendete Netzwerke

### Anbindung Messenetzwerk

Der Messebetreiber stellt am Messe-Stand einen direkten Anschluss ins Internet zur Verfügung. Der Messe-Router muss von einem Mitarbeiter am Messe-Stand an den dort vorhandenen Internet-Anschluss des Messebetreibers angeschlossen werden. Der Messe-Router ist vollständig konfiguriert und stellt die VPN-Verbindung zum Firmen-Netz automatisch her. Auch das Firmen-WLAN wird automatisch zur Verfügung gestellt. Es ist also kein weiterer Eingriff des Mitarbeiters notwendig.

### Netzwerk Einrichtung und IP-Zuweisung

Der Messe-Router wird an den Anschluss vom Messebetreiber angeschlossen. Der Access-Point wird an den Messe-Router angeschlossen (Im Packet Tracer sind Router, Access Point und Switch getrennt. Es wird angenommen, dass der Messe-Router ein All-in-One-Gerät ist.). Der Mitarbeiter-Laptop wird mit dem Access-Point über WLAN verbunden. Die Clients erhalten ihre IP-Adresse vom DHCP des Messe-Routers.

Folgende IPs wurden vergeben:

Öffentliche IP des Firmen-Routers: 209.165.100.1/24

Öffentliche IP des Messe-Routers: 209.165.200.1/24

Lokale IP des Firmen-Routers: 10.1.1.1/24

Lokale IP des Firmen-Servers: 10.1.1.10/24

Lokale IP des Messe-Routers: 10.1.3.1/26

Lokale IP des Mitarbeiter-Laptop: 10.1.3.10/26

### Routing

Der Messe-Router kennt die öffentliche IP-Adresse des Firmen-Routers und kann so die VPN-Verbindung zum Endpunkt herstellen.

## WLAN

Es soll ein WLAN-Netzwerk für die Mitarbeiter geben. Das Netzwerk ist durch einen eindeutigen Namen erkennbar (z.B. „Firmen-Name“-Mitarbeiter für die Mitarbeiter).

### Zugangsbeschränkung

Das Mitarbeiter-WLAN ist durch WPA3-Enterprise geschützt. Durch einen Radius-Server im Corporate-Network können sich die Mitarbeiter im WLAN mit ihren Zugangsdaten anmelden. Die Anmeldedaten werden durch den VPN-Tunnel zum Radius-Server geschickt, welcher die Clients der Mitarbeiter authentifiziert.

### Sicherheit



Der WLAN-Zugang für die Mitarbeiter bietet dank WPA3-Enterprise den höchsten Sicherheitsstandard. Durch Authentifizierung mit Nutzername und Passwort kann sich kein Dritter mit dem WLAN verbinden. Durch die Verschlüsselung im VPN ist auch der Verkehr im Internet geschützt.

### Anbindung von Clients



Die Clients der Mitarbeiter sind primär per WLAN verbunden. Alternativ kann eine Kabelverbindung zum Messe-Router genutzt werden. Das WLAN arbeitet im 5GHz-Band mit Fall-Back auf 2,4GHz und unterstützt den Standard 802.11ax. Das WLAN hat genug Leistung, um den gesamten Messe-Stand damit zu versorgen.

## VPN

### Konfiguration im Packet-Tracer:

**Grund-Konfiguration der Router (Hostname, Interfaces, Standard-Gateway)**

Firmen-Router(config)# hostname Firmen-Router

Firmen-Router(config)# interface g0/0

Firmen-Router(config-if)# ip address 209.165.100.1 255.255.255.0



Firmen-Router(config-if)# no shut

Firmen-Router(config-if)# exit

Firmen-Router(config)# interface g0/1

Firmen-Router(config-if)# ip address 10.1.1.1 255.255.255.0

Firmen-Router(config-if)# no shut

Firmen-Router(config-if)# exit

Firmen-Router(config)# ip route 0.0.0.0 0.0.0.0 209.165.100.2

Internet-Router(config)# hostname Internet-Router

Internet-Router(config)# interface g0/0 209.165.100.2 255.255.255.0

Internet-Router(config-if)# ip address

Internet-Router(config-if)# no shutdown

Internet-Router(config-if)# exit

Internet-Router(config)# interface g0/1 209.165.200.2 255.255.255.0

Internet-Router(config-if)# ip address

Internet-Router(config-if)# no shutdown

Internet-Router(config-if)# exit

Messe-Router(config)# hostname Messe-Router

Messe-Router(config)# interface g0/0

Messe-Router(config-if)# ip address 209.165.200.1 255.255.255.0

Messe-Router(config-if)# no shutdown

Messe-Router(config-if)# exit

Messe-Router(config)# interface g0/1

Messe-Router(config-if)# ip address 10.1.3.1 255.255.255.192

Messe-Router(config-if)# no shutdown

Messe-Router(config-if)# exit

Messe-Router(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.2

**Installation der erforderlichen Security Lizenz (VPN)**

Firmen-Router(config)# license boot module c1900 technology-package securityk9

Firmen-Router# copy run start

Firmen-Router# reload

Internet-Router(config)# license boot module c1900 technology-package securityk9

Internet-Router# copy run start

Internet-Router# reload

Messe-Router(config)# license boot module c1900 technology-package securityk9

Messe-Router# copy run start

Messe-Router# reload

**Anlegen der ACLs**

Firmen-Router(config)# access-list 100 permit ip 10.1.1.0 0.0.0.255 10.1.3.0 0.0.0.255

Messe-Router(config)# access-list 100 permit ip 10.1.3.0 0.0.0.255 10.1.1.0 0.0.0.255

**ISAKMP policy/ISAKMP key**

Firmen-Router(config)# crypto isakmp policy 10

Firmen-Router(config-isakmp)# encryption aes 256

Firmen-Router(config-isakmp)# authentication pre-share

Firmen-Router(config-isakmp)# group 5

Messe-Router(config)# crypto isakmp policy 10

Messe-Router(config-isakmp)# encryption aes 256

Messe-Router(config-isakmp)# authentication pre-share

Messe-Router(config-isakmp)# group 5

Firmen-Router(config)# crypto isakmp key secretkey address 209.165.200.1

Messe-Router(config)# crypto isakmp key secretkey address 209.165.100.1

**IPsec transform-set**

Firmen-Router(config)# crypto ipsec transform-set Firmen-Router-Messe-Router esp-aes 256 esp-sha-hmac

Messe-Router(config)# crypto ipsec transform-set Messe-Router-Firmen-Router esp-aes 256 esp-sha-hmac

Firmen-Router(config)# crypto map IPSEC-MAP 10 ipsec-isakmp

Firmen-Router(config-crypto-map)# set peer 209.165.200.1

Firmen-Router(config-crypto-map)# set pfs group5

Firmen-Router(config-crypto-map)# set security-association lifetime seconds 86400

Firmen-Router(config-crypto-map)# set transform-set Firmen-Router-Messe-Router

Firmen-Router(config-crypto-map)# match address 100

Messe-Router(config)# crypto map IPSEC-MAP 10 ipsec-isakmp

Messe-Router(config-crypto-map)# set peer 209.165.100.1

Messe-Router(config-crypto-map)# set pfs group5

Messe-Router(config-crypto-map)# set security-association lifetime seconds 86400

Messe-Router(config-crypto-map)# set transform-set Messe-Router-Firmen-Router

Messe-Router(config-crypto-map)# match address 100

**Crypto-Map auf Interfaces anwenden**

Firmen-Router(config-crypto-map)# int g0/0

Firmen-Router(config-if)# crypto map IPSEC-MAP

Messe-Router(config-crypto-map)# int g0/0

Messe-Router(config-if)# crypto map IPSEC-MAP

### Alternative Konfiguration mit WireGuard

WireGuard-Interface Firmen-Router:

[Interface]

PrivateKey = yAnz5TF+lXXJte14tji3zlMNq+hd2rYUIgJBgB3fBmk=

ListenPort = 51820

[Peer]

Public Key = xTIBA5rboUvnH4htodjb6e697QjLERt1NAB4mZqp8Dg=

AllowedIPs = 10.1.3.0/26

WireGuard-Interface Messe-Router:

[Interface]

PrivateKey = gI6EdUSYvn8ugXOt8QQD6Yc+JyiZxIhp3GInSWRfWGE=

[Peer]

Public Key = HIgo9xNzJMWLKASShiTqIybxZ0U3wGLiUeJ1PKf8ykw=

Endpoint = 209.165.100.1:51820

AllowedIPs = 0.0.0.0/0

Die beiden Konfigurationen müssen in der jeweiligen WireGuard-Konfiguration der Endpunkte angegeben werden. Sobald beide Interfaces aktiv sind, können Daten ausgetauscht werden. Bei WireGuard handelt es sich nicht mehr um eine traditionelle VPN-Verbindung, sodass keine Verbindung im klassischen Sinne aufgebaut werden muss. Die Pakete werden „einfach losgeschickt“.

## Messe-App

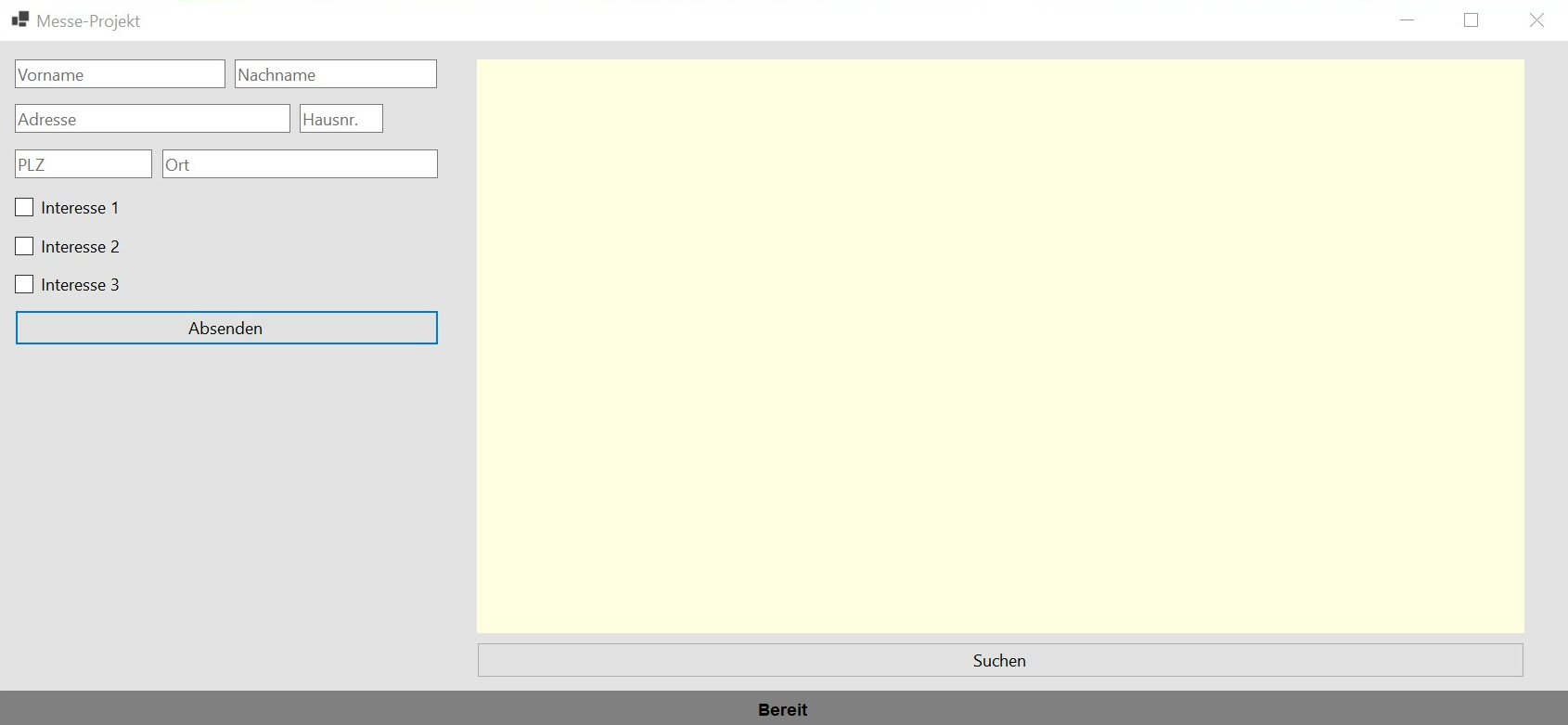


Abbildung 2: Startbildschirm – Messe-App

Über die App können die Nutzerdaten am Messe-Stand gespeichert und abgerufen werden.

Im linken Bereich können die persönlichen Daten wie Name, Anschrift und die persönlichen Interessen eingetragen und mit Button „Absenden“ in der Datenbank gespeichert werden.

Die Statusbar am unteren Rand bietet ein Sofort-Feedback zur getätigten Aktion. Sind alle Felder entsprechend ausgefüllt und die Daten erfolgreich gespeichert worden, wird die Statusbar grün und meldet „Daten wurden gespeichert“. Sollten nicht alle Felder ausgefüllt worden sein, meldet die App mit einer gelben Statusbar „Eingaben ungültig!“ und verhindert das Absenden. Sollte die Verbindung zur Datenbank nicht hergestellt werden können, meldet die Datenbank mit rot „Connection Error“.

Im rechten Bereich können die gespeicherten Einträge von der Datenbank abgerufen werden. Durch einen Klick auf den Button „Suchen“, werden alle Einträge, sortiert nach der ID im gelben Feld ausgegeben. Mit dem „Nachname“-Feld im linken Bereich kann durch Eingabe des gesuchten Namens und dem anschließenden Klicken auf den Button „Suchen“ gezielter nach dem Nachnamen gesucht werden. Im gelben Feld stehen dann alle Einträge zum gesuchten Nachnamen. Die Interessen werden mit einer „1“ für „ja/wahr“ und einer „0“ für „nein/falsch“ abgespeichert. Das liegt daran, dass die Datenbank keine booleschen Werten speichern kann. Die Daten werden daher in den Datentyp „tinyint“ umgewandelt.

## Alternativer Lösungsansatz für mehr Komfort

Dies war der erste Lösungsansatz. Aufgrund zu hoher Komplexität für den Anwendungsfall wurde der Ansatz verworfen:

Es soll 2 WLAN-Netzwerke geben, eins für die Mitarbeiter und eins für die Besucher. Die Netzwerke sollen durch eindeutige Namen erkennbar sein. „Firmen-Name“-Mitarbeiter für die Mitarbeiter und „Firmen-Name“-Besucher für Besucher.

Clients im Mitarbeiter- und Besucher-WLAN können nicht miteinander kommunizieren. Während die Mitarbeiter vollen Zugriff auf das Corporate-Network haben, ist der Zugang zum Internet über das Besucher-WLAN nicht möglich. Dadurch lassen sich Probleme wie Datenschutz- und Nutzungsbedingungen aus der Welt räumen.

Das Mitarbeiter-WLAN ist durch WPA3-Enterprise geschützt. Durch einen Radius-Server im Corporate-Network können sich die Mitarbeiter im WLAN mit ihren Zugangsdaten anmelden. Die Anmeldedaten werden durch den VPN-Tunnel zum Radius-Server geschickt, welcher die Clients der Mitarbeiter authentifiziert.

Das Besucher-WLAN ist durch WPA3-Personal im Transition Mode geschützt. Dadurch können auch ältere Geräte das Angebot nutzen.

Am Stand der Firma wird ein QR-Code ausgehängt. Diesen können die Besucher einscannen, um sich mit dem Besucher-WLAN zu verbinden. Durch ein Captive-Portal werden die Besucher automatisch auf eine Webseite weitergeleitetet, wenn sie sich mit dem WLAN verbinden. Dort können sie die entsprechenden Daten angeben, welche dann beim Absenden auf dem Messe-Router zwischengespeichert und an den Datenbank-Server weitergeleitet werden. Durch die Zwischenverarbeitung der Daten kann ein direkter Zugang vom Besucher-WLAN ins Firmen-Netz vermieden und Schwachstellen vermieden werden.