

Die Aufgaben 1 bis 4 beziehen sich auf die folgende Ausgangssituation:

Sie arbeiten als Fachinformatiker bei der 1234-IT-Systemhaus GmbH. Für Ihren Arbeitgeber beraten Sie u. a. das Möbelhaus Rusticus GmbH. Den Netzwerkplan des Möbelhauses finden Sie in der perforierten Anlage.

Zwischen beiden Standorten existiert eine VPN-Verbindung. Außendienstmitarbeiter sind bereits teilweise mit Laptops ausgestattet, die über das Mobilfunknetz eine Datenverbindung zum Internet herstellen können. Für die Verbindung zum Hauptstandort soll zukünftig ebenfalls ein VPN eingesetzt werden.

1. Aufgabe (24 Punkte)

Sie sind damit beauftragt, das Netzwerk der Rusticus GmbH zu betreuen.

- a) Für die DMZ wird das Netzwerk 203.0.113.64 /29 verwendet, welches Ihnen vom Provider zugewiesen wurde. Dieses Netzwerk soll überprüft werden.
- aa) Der Router zum Internet (R-Rusticus-ext) soll die erste mögliche IP-Adresse im Netzwerk erhalten, der Router zum Firmennetz (R-Rusticus-int) die letzte mögliche IP-Adresse im Netzwerk.

Ergänzen Sie die folgende Tabelle.

2 Punkte

Router, Schnittstelle	IP-Adresse
R-Rusticus-ext, ETH	
R-Rusticus-int, ETH0	

- ab) Geben Sie die vollständige Routingtabelle für den Router R-Rusticus-ext an. Die Subnetzmaske ist in Punkt-Dezimal-Schreibweise anzugeben. In der Spalte „Schnittstelle oder Next-Hop“ ist, wann immer möglich, die Next-Hop-Adresse zu verwenden.

8 Punkte

Hinweis: Die Anzahl der Zeilen der Tabelle ist keine Vorgabe für die Anzahl der notwendigen Einträge.

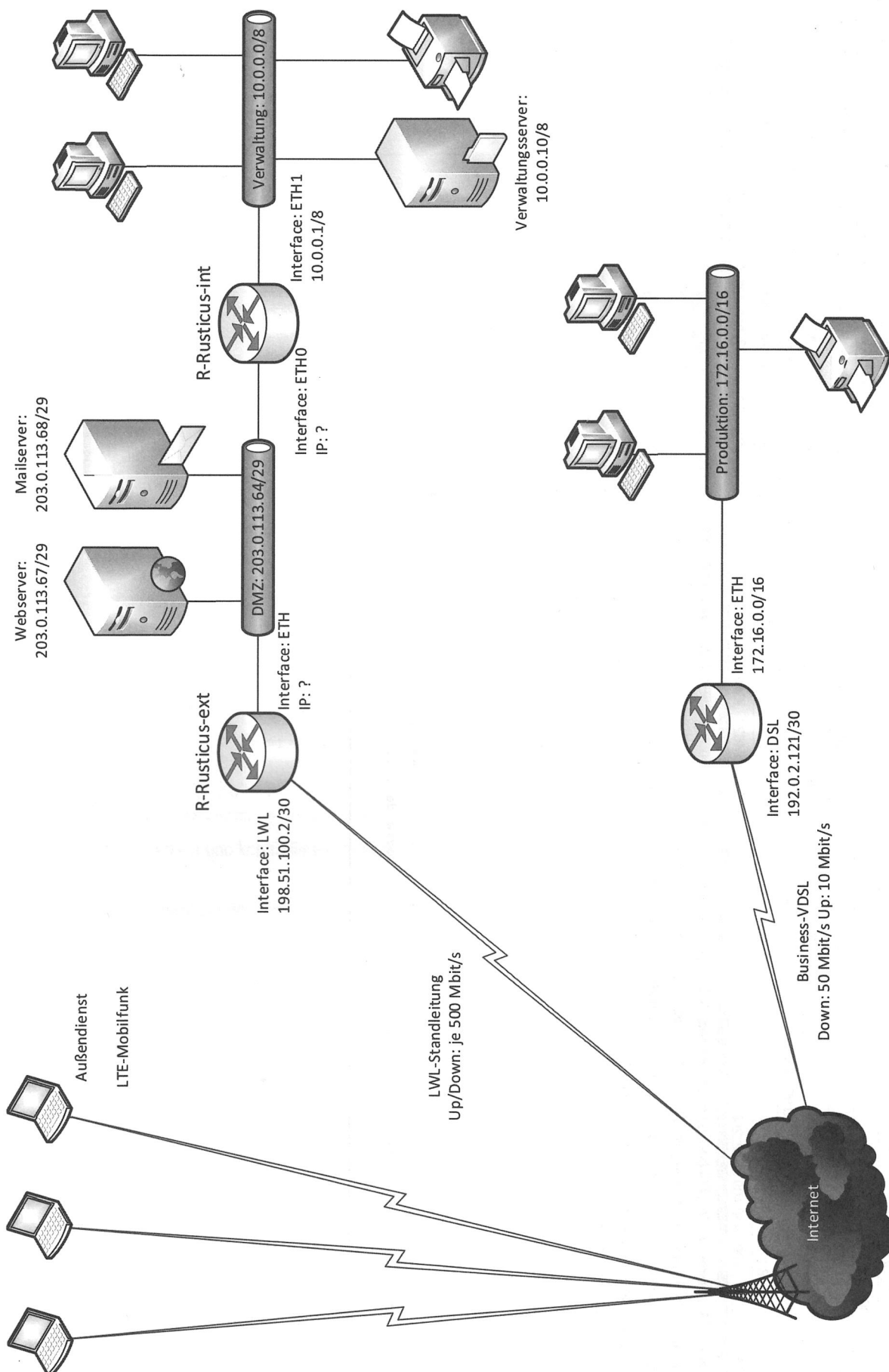
Netzwerk-ID	Subnetzmaske	Schnittstelle oder Next-Hop

- b) Auf dem Router wird eine Firewall betrieben, zu deren Funktionsumfang auch SPI (Stateful Packet Inspection) zählt.

Erläutern Sie die Unterschiede einer Firewall mit aktivierter SPI-Funktion im Vergleich zu einer Firewall mit deaktivierter SPI-Funktion.

4 Punkte

Anlage 1: Netzwerkplan



Anlage 2: Mitschnitt des Netzwerkverkehrs

No.	Time	Source	Destination	Protocol	Length	Info
126	57041894	2001:db8:3726:1a00:70cd:9f70:a8a8:4627	fd00::7642:7fff:fe0c:62f7	DNS	93	Standard query 0xd771 A www.google.de
127	57042168	2001:db8:3726:1a00:70cd:9f70:a8a8:4627	fd00::7642:7fff:fe0c:62f7	DNS	93	Standard query 0x8737 AAAA www.google.de
128	57067860	10.0.0.101	8.8.4.4	DNS	73	Standard query 0x8737 AAAA www.google.de
129	57067860	10.0.0.101	8.8.4.4	DNS	73	Standard query 0xd771 A www.google.de
130	57083607	8.8.4.4	10.0.0.101	DNS	89	Standard query response 0xd771 A www.google.de A 142.251.36.163
131	57084949	fd00::7642:7fff:fe0c:62f7	2001:db8:3726:1a00:70cd:9f70:a8a8:4627	DNS	121	Standard query response 0x8737 AAAA www.google.de AAAA 2a00:1450:4001:812::2003
132	57085082	fd00::7642:7fff:fe0c:62f7	2001:db8:3726:1a00:70cd:9f70:a8a8:4627	DNS	109	Standard query response 0xd771 A www.google.de A 142.250.184.227
133	57094497	2001:db8:3726:1a00:70cd:9f70:a8a8:4627	2a00:1450:4001:812::2003	ICMPv6	94	Echo (ping) request id=0x0001, seq=13, hop limit=128 (reply in 135)
134	57096359	8.8.4.4	10.0.0.101	DNS	101	Standard query response 0x8737 AAAA www.google.de AAAA 2a00:1450:4016:809::2003
135	57108031	2a00:1450:4001:812::2003	2001:db8:3726:1a00:70cd:9f70:a8a8:4627	ICMPv6	94	Echo (ping) reply id=0x0001, seq=13, hop limit=118 (request in 133)
Frame 126: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \DeviceNPF_{58E06F70-38E4-4725-85A1-79AB4C68C102}, id 0 Ethernet II, Src: hardware_5d:c2:ae (70:cd:cc:5d:c2:ae), Dst: distro_0c:62:f7 (76:42:7f:0c:62:f7) Internet Protocol Version 6, Src: 2001:db8:3726:1a00:70cd:9f70:a8a8:4627, Dst: fd00::7642:7fff:fe0c:62f7 User Datagram Protocol, Src Port: 57616, Dst Port: 53 Domain Name System (query)						
0000	76 42 7f 0c 62 f7 70 cd cc 5d c2 ae 86 dd 60 0e	b...!...].....`				
0010	59 59 00 27 11 ff 20 01 0d b8 37 26 1a 00 70 cd	YX.'... ...7&...p.				
0020	9f 70 a8 a8 46 27 fd 00 00 00 00 00 00 76 42	.p..F'.....vB				
0030	7f ff fe 0c 62 f7 e1 10 00 35 00 27 c5 7e d7 71	b.....5.'..~.q				
0040	01 00 00 01 00 00 00 00 00 03 77 77 77 06 67	www.g				
0050	6f 6f 67 6c 65 02 64 65 00 00 01 00 01	oogle.de.....				

- c) Stellen Sie für folgende Situationen passende Regeln für die Firewall auf, die den Traffic aus dem Internet regulieren: 10 Punkte
- Der Webserver soll von außen über HTTP erreichbar sein.
 - Der Webserver soll von außen über HTTPS erreichbar sein.
 - Andere Mailserver können Mails beim Mailserver über SMTP einliefern.
 - Mails können mit dem Protokoll IMAP vom Mailserver abgerufen werden.
 - Aller anderer Traffic aus dem Internet wird verworfen.

Aktion	Protokoll	Quelle	Ziel	Quellport	Zielpport	Von Interface	Nach Interface

2. Aufgabe (23 Punkte)

Der Provider bietet für die Internetverbindung der Rusticus GmbH die Adressierung mittels IPv6 an. Auf den Netzwerkkomponenten wird daher zusätzlich das Protokoll IPv6 aktiviert.

Sie sollen die Netzwerkkonnektivität testen und zeichnen den Netzwerkverkehr für eine Überprüfung der Frames bzw. Pakete auf.

Sie geben an einem Client den Befehl `ping -n 1 www.google.de` ein.

Bildschirmausgabe:

```
C:\Users\user1>ping -n 1 www.google.de
```

```
Ping wird ausgeführt für www.google.de [2a00:1450:4001:812::2003] mit 32 Bytes Daten:
```

```
Antwort von 2a00:1450:4001:812::2003: Zeit=13ms
```

```
Ping-Statistik für 2a00:1450:4001:812::2003:
```

```
  Pakete: Gesendet = 1, Empfangen = 1, Verloren = 0  
  (0% Verlust),
```

```
Ca. Zeitangaben in Millisek.:
```

```
  Minimum = 13ms, Maximum = 13ms, Mittelwert = 13ms
```

Sie analysieren den Netzwerkverkehr und kontrollieren die Aufzeichnung der dazugehörigen Frames No. 126 bis 135 (siehe Rückseite perforierte Anlage).

- a) Beschreiben Sie den Grund, weshalb der Client zuerst eine DNS-query (DNS-Abfrage) startet.

3 Punkte

- b) Ermitteln Sie den Rückgabewert der Antwort auf die DNS-Anfrage aus Frame No. 126.

4 Punkte

Fortsetzung 2. Aufgabe →

Fortsetzung 2. Aufgabe

- c) Bestimmen Sie die lokale IPv4-Adresse und die genutzte IPv6-Adresse des Clients.

4 Punkte

IPv4	
IPv6	

- d) Ermitteln Sie die IP-Adresse des genutzten lokalen DNS-Servers.

3 Punkte

- e) Begründen Sie, warum der PING an die IP-Adresse 2a00:1450:**4001:812**::2003 und nicht an die Adresse 2a00:1450:**4016:809**::2003 gesendet wurde.

3 Punkte

- f) Berechnen Sie mithilfe der Werte aus den aufgezeichneten Frames die Anzahl der Router (hops), über die die ping-Antwort gelaufen ist.

3 Punkte

A large rectangular grid of graph paper, consisting of 20 columns and 10 rows of squares, intended for drawing a picture.

- g) Beschreiben Sie einen möglichen Grund, warum Sie mehrere IPv4- und IPv6-Adressen für `www.google.de` als Antworten erhalten haben. 2 Punkte

3 Punkte

3. Aufgabe (27 Punkte)

Korrekturrand

Der Zugriff der Außendienstmitarbeiter auf den Server der Rusticus GmbH soll über TLS-Verbindungen erfolgen.

a) Nennen Sie zwei Eigenschaften, welche eine TLS-Verbindung sicherer machen als eine normale TCP/IP-Verbindung. 4 Punkte

b) Im August 2018 wurde die Version TLS1.3 in RFC8446 verabschiedet. Innerhalb Ihres Teams wird zurzeit beraten, ob für die Zugänge der Rusticus-Außendienstmitarbeiter ausschließlich TLS1.3 zugelassen wird, oder ob auch Verbindungen nach TLS1.2 noch akzeptiert werden.

Begründen Sie anhand von drei Argumenten aus dem RFC8446, warum Verbindungen nach TLS1.2 für den Online-Zugang bei der Rusticus GmbH nicht mehr zugelassen werden sollten. 9 Punkte

RFC8446 (Auszug):

Major Differences from TLS 1.2

The following is a list of the major functional differences between TLS 1.2 and TLS 1.3. It is not intended to be exhaustive, and there are many minor differences.

- The list of supported symmetric encryption algorithms has been pruned of all algorithms that are considered legacy.
- Static RSA and Diffie-Hellman cipher suites have been removed; all public-key based key exchange mechanisms now provide forward secrecy.
- All handshake messages after the ServerHello are now encrypted.
- Session resumption has been replaced by a single new PSK exchange.

Vokabel-Hilfe:

exhaustive – erschöpfend, vollständig

to prune (of) – bereinigen, säubern von

resumption – Fortsetzung, Wiederaufnahme

Fortsetzung 3. Aufgabe →

Fortsetzung 3. Aufgabe

- c) Zur Authentifizierung des Servers werden bei SSL/TLS-Verbindungen Zertifikate nach X.509 eingesetzt, die von einer sogenannten CA (Certificate Authority) signiert sein müssen. Diese CA kann sowohl intern (self-signed), als auch von einer externen Zertifizierungsstelle betrieben werden.

Entscheiden Sie sich für eines der beiden Verfahren (interne CA/externe CA), und begründen Sie die Entscheidung anhand von zwei Argumenten. 6 Punkte

- d) Nach erfolgreichem SSL/TLS-Verbindungsaufbau ist lediglich der Server der Rusticus GmbH gegenüber dem Endgerät des Mitarbeiters authentifiziert. Eine umgekehrte Authentifizierung steht noch aus. Diskutiert werden aktuell vier verschiedene Verfahren, um den Client gegenüber dem Server zu authentifizieren.

1. Username + Passwort
2. Username + Passwort + Client-Zertifikat
3. Username + Passwort + Krypto-Smart-Card
4. Username + Passwort + OneTimePassword (Authenticator-App)

Erläutern Sie zu jedem Verfahren einen Vorteil, der für den Einsatz des jeweiligen Verfahrens spricht.

8 Punkte

Verfahren	
1	
2	
3	
4	

4. Aufgabe (26 Punkte)

- a) Im Möbelhaus Rusticus sind 100 VoIP-Telefonanschlüsse vorhanden. Der VoIP-Server befindet sich in der Cloud. Das bedeutet, dass auch interne Gespräche zwischen den Nebenstellen über den Internetanschluss laufen. Die Cloud-Telefonanlage nutzt standardmäßig den Codec G.722 (64 kBit/s). Der Protokolloverhead beträgt 10 %.

Berechnen Sie die benötigte Bandbreite in kBit/s, wenn gleichzeitig fünf Gespräche intern und fünfzehn Gespräche extern geführt werden. 5 P

5 Punkte

[illegible]

- b) Für Videokonferenzen nutzt das Möbelhaus Rusticus Software, über die Sie im Datenblatt folgende Hinweise finden:

This software is designed to give the best audio, video, and content sharing experience regardless of your network conditions. That said, when bandwidth is insufficient, our product prioritizes audio quality over video quality. Where bandwidth isn't limited, our product optimizes media quality, including high-fidelity audio, up to 1080p video resolution, and up to 30fps (frames per second) for video and content.

This table describes how we use bandwidth. Our software is always conservative on bandwidth utilization and can deliver HD video quality in under 1.5Mbps. The actual bandwidth consumption in each audio/video call or meeting will vary based on several factors, such as video layout, video resolution, and video frames per second. When more bandwidth is available, quality and usage will increase to deliver the best experience.

- ba) Erläutern Sie, was geschieht, wenn die Bandbreite für die gleichzeitige Audio- und Videoübertragung nicht ausreicht.

3 Punkte

- bb) Nennen Sie drei Faktoren, von denen die aktuell genutzte Bandbreite abhängt.

3 Punkte

Fortsetzung 4. Aufgabe →

Fortsetzung 4. Aufgabe

- c) Das Möbelhaus Rusticus führt derzeit regelmäßig Videokonferenzen durch, an denen maximal zehn Personen teilnehmen. Wie hoch ist der hierbei entstehende zusätzliche Traffic auf dem Internetanschluss im Upload und Download, wenn die empfohlene Bandbreite genutzt wird?

Modality	Bandwidth requirements (bitrate kBit/s up/down)		
	Minimum	Recommended	Best performance
Audio			
One-to-one	10/10	58/58	76/76
Meetings	10/10	58/58	76/76
Video			
One-to-one	150/150	1.500/1.500	4.000/4.000
Meetings	150/200	2.500/4.000	4.000/4.000

[illegible]

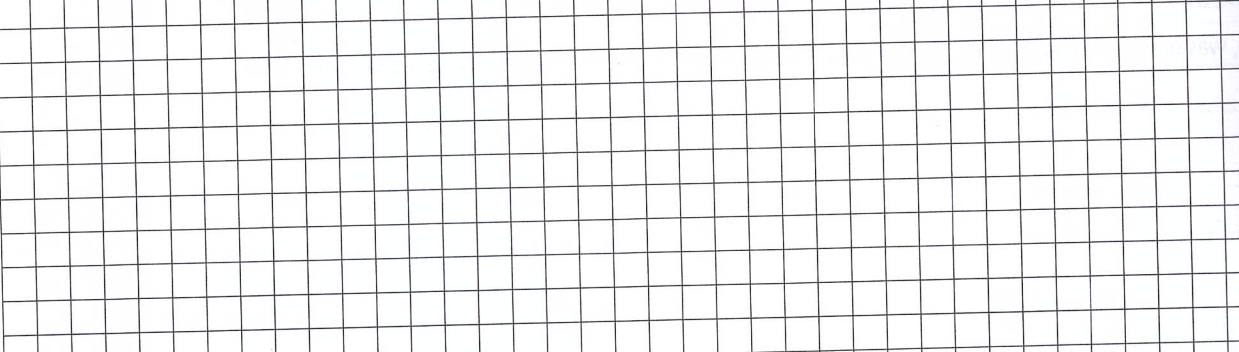
- d) Das Möbelhaus Rusticus bietet seinen Kunden 3D-Animationsfilme an, die die fertige Küche zeigen. Die Filme dauern jeweils 5 Minuten und werden den Kunden zum Download angeboten. Die Videos haben durchschnittlich eine Größe von 34 MiB pro Minute. Der Kunde verfügt über einen ADSL-Anschluss (Download: 16 Mbit/s, Upload: 2 Mbit/s).

Wie lange dauert die Übertragung eines solchen Videoclips mindestens?

Das Ergebnis ist auf volle Sekunden aufzurunden.

4 Punkte

Das Ergebnis ist auf volle Sekunden aufzurunden.



- e) Die Rusticus GmbH nutzt für die Datenübertragung QoS.

Erläutern Sie die Funktionsweise von QoS und welche Auswirkungen für den Benutzer man sich durch den Einsatz von QoS bei der Übertragung von Telefonie- und Videodaten verspricht.

4 Punkte

der Übertragung von Telefonie- und Videodaten. Versprechen:

- f) In der Kommunikation mit einem Zulieferer bedient sich das Möbelhaus Rusticus nach wie vor der Dokumentenübertragung per Telefax. Seit der Umstellung auf VoIP berichtet das mit dem Fax-Versand betraute Personal immer wieder von Schwierigkeiten beim Versand sowie dem Erhalt von Fax-Dokumenten, insbesondere von unvollständigen Übertragungen, wenn mehrere Seiten übermittelt werden sollen.

Korrekturrand

Beschreiben Sie eine mögliche Ursache, die im Zusammenhang mit VoIP-Übertragungsprotokollen zu diesen Schwierigkeiten beim Versand bzw. Empfang von Fax-Dokumenten führen kann.

5 Punkte

PRÜFUNGSZEIT – NICHT BESTANDTEIL DER PRÜFUNG!

Wie beurteilen Sie nach der Bearbeitung der Aufgaben die zur Verfügung stehende Prüfungszeit?

- ☐ 1 Sie hätte kürzer sein können.
- ☐ 2 Sie war angemessen.
- ☐ 3 Sie hätte länger sein müssen.

☐