

Familienname, Vorname (bitte durch eine Leerspalte trennen)

[illegible]

IHK

Bereich		Berufsnummer				IHK-Nummer			Prüflingsnummer			
7	0	1	2	0	2							
Sp. 1-2		Sp. 3-6				Sp. 7-9			Sp. 10-14			

Termin: Mittwoch, 27. November 2024

Abschlussprüfung Winter 2024/25

1202

2 Analyse und Entwicklung von Netzwerken

Fachinformatiker
Fachinformatikerin
Systemintegration

Teil 2 der Abschlussprüfung

4 Aufgaben

90 Minuten Prüfungszeit

100 Punkte

Bearbeitungshinweise

1. Bevor Sie mit der Bearbeitung der Aufgaben beginnen, überprüfen Sie bitte die **Vollständigkeit** dieses Aufgabensatzes. Die Anzahl der zu bearbeitenden Aufgaben ist auf dem Deckblatt links angegeben. Wenden Sie sich bei Unstimmigkeiten sofort an die Aufsicht, weil Reklamationen am Ende der Prüfung nicht anerkannt werden können.
2. Füllen Sie zuerst die **Kopfzeile** aus. Tragen Sie Ihren Familiennamen, Ihren Vornamen und Ihre Prüflings-Nr. in die oben stehenden Felder ein.
3. Lesen Sie bitte den **Text** der Aufgaben ganz durch, bevor Sie mit der Bearbeitung beginnen.
4. Halten Sie sich bei der Bearbeitung der Aufgaben genau an die **Vorgaben der Aufgabenstellung** zum Umfang der Lösung. Wenn z. B. vier Angaben gefordert werden und Sie sechs Angaben anführen, werden nur die ersten vier Angaben bewertet.
5. Tragen Sie die frei zu formulierenden **Antworten dieser offenen Aufgaben** in die dafür lt. Aufgabenstellung vorgesehenen Bereiche (Lösungszeilen, Formulare, Tabellen u. a.) des Arbeitsbogens ein.
6. Sofern nicht ausdrücklich ein Brief oder eine Formulierung in ganzen Sätzen gefordert werden, ist eine **stichwortartige Beantwortung** zulässig.
7. Schreiben Sie deutlich und gut lesbar. Ein nicht eindeutig zuzuordnendes oder **unleserliches Ergebnis** wird als **falsch** gewertet.
8. Zur Lösung der Rechenaufgaben darf ein nicht programmierter, netzunabhängiger **Taschenrechner** ohne Kommunikationsmöglichkeit mit Dritten verwendet werden.
9. Wenn Sie ein **gerundetes Ergebnis** eintragen und damit weiterrechnen müssen, rechnen Sie (auch im Taschenrechner) nur mit diesem gerundeten Ergebnis weiter.
10. Für **Hilfsaufzeichnungen** können Sie das in der Tasche beigelegte Konzeptpapier verwenden. Bewertet werden jedoch grundsätzlich nur Ihre Eintragungen in diesem Aufgabensatz.

Wird vom Korrektor ausgefüllt!

Bewertung

Für die Bewertung gilt die Vorgabe der Punkte in den Lösungshinweisen.

1. Aufg.

--	--

 Punkte 2. Aufg.

--	--

 Punkte 3. Aufg.

--	--

 Punkte 4. Aufg.

--	--

 Punkte

Prüfungszeit
23
Die entsprechende Ziffer (1, 2 oder 3)
finden Sie in der Abfrage nach der
Prüfungszeit im Anschluss an die letzte
Aufgabe.

Gesamtpunktzahl

24	25	26

Prüfungsort, Datum

Unterschrift

Gemeinsame Prüfungsaufgaben der Industrie- und Handelskammern. Dieser Aufgabensatz wurde von einem überregionalen Ausschuss, der entsprechend § 40 Berufsbildungsgesetz zusammengesetzt ist, beschlossen. Hinweis: Im Interesse einer besseren Lesbarkeit wird in der Aufgabenstellung und in den Angaben zur Aufgabenstellung nur die männliche Form (generisches Maskulinum) verwendet. Die verkürzte Sprachform beinhaltet keine Wertung und die gewählten männlichen Formulierungen gelten uneingeschränkt auch für die weiteren Geschlechter. Die Vervielfältigung, Verbreitung und öffentliche Wiedergabe der Prüfungsaufgaben und Lösungen ist nicht gestattet. Zuwiderhandlungen werden zivil- und strafrechtlich (§§ 97 ff., 106 ff. UrhG) verfolgt. – © ZPA Nord-West 2024 – Alle Rechte vorbehalten!

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

Sie arbeiten als Fachinformatiker (Systemintegration) bei der 1234-IT-Systemhaus GmbH. Dabei handelt es sich um einen mittelständischen IT-Dienstleister, der neben der Zentrale mehrere bundesweit verteilte Standorte hat.

Aktuell betreuen Sie für Ihren Arbeitgeber die „IHK-Med AG“, ein Unternehmen aus der Medizinforschung. Der Kunde plant aktuell den Umzug in ein neu errichtetes Gebäude, für das Sie das zukünftige Netzwerk planen sollen.

1. Aufgabe: Konfigurieren des geschichteten Netzwerks
2. Aufgabe: IP-Adressierung für das Netzwerk durchführen
3. Aufgabe: Fehlersuche im Netzwerk
4. Aufgabe: Einrichten einer Next Generation Firewall

1. Aufgabe (25 Punkte)

a) Bei der Netzwerkplanung für die IHK-Med AG sollen Sie einzelne Unternehmensbereiche in virtuelle LANs (VLANs) strukturieren.

aa) Durch die Planung einer Netzwerkstruktur mit VLANs ergeben sich erhebliche Vorteile.

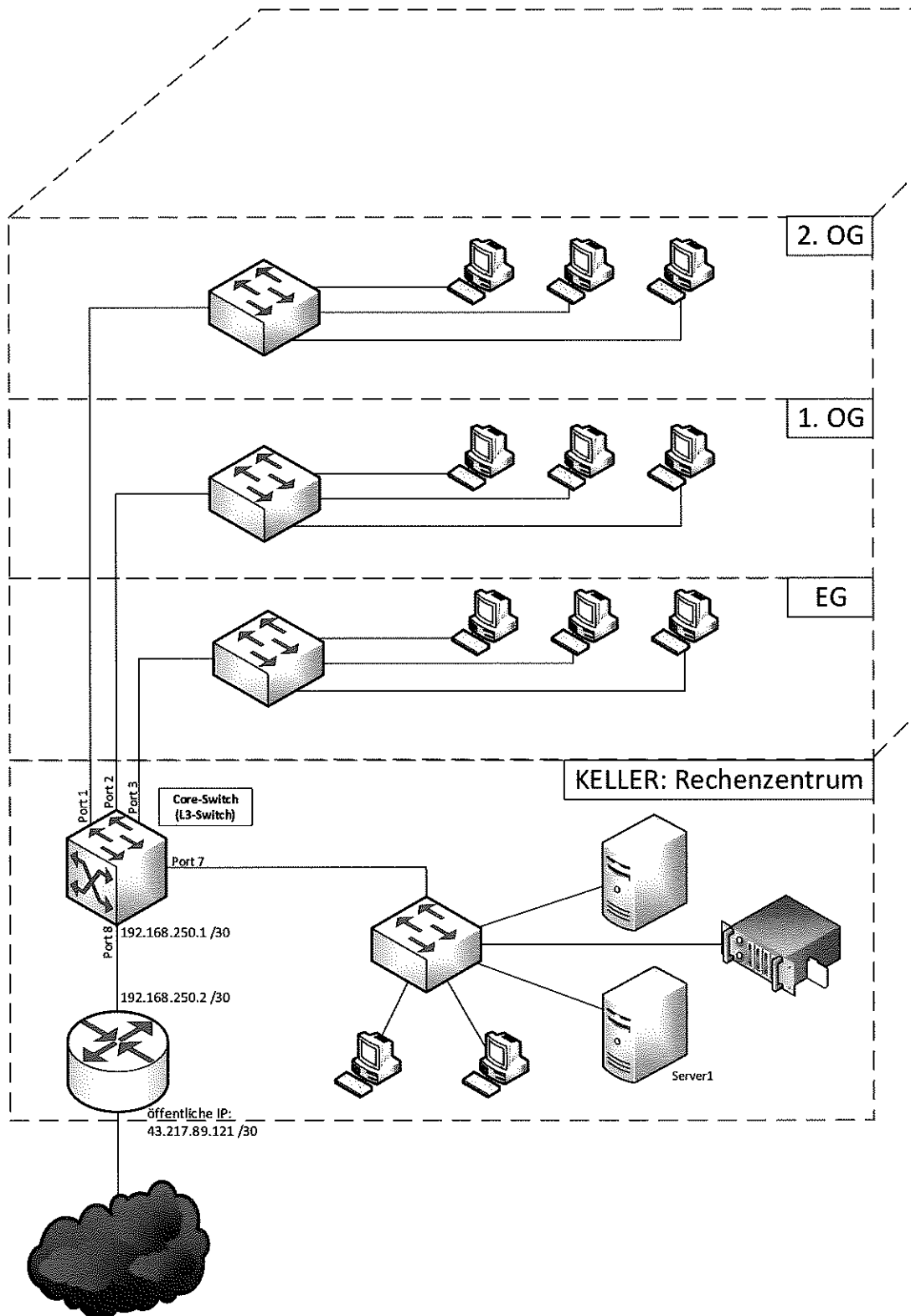
Beschreiben Sie drei Vorteile für die IHK-Med AG, die sich durch eine Netzwerkstruktur mit VLANs ergeben. 6 Punkte

ab) Portbasierte VLANs und dynamische VLANs sind zwei verschiedene Ansätze zur Zuordnung zu virtuellen LANs in einem Netzwerk.

Erläutern Sie, wie in beiden Ansätzen Geräte zu einem VLAN zugeordnet werden können. 6 Punkte

Dieses Blatt kann an der Perforation aus dem Aufgabensatz herausgetrennt werden!

Netzwerkskizze der IHK-Med AG



b) In der weiteren Planung werden entsprechend der Unternehmensstruktur folgende VLANs festgelegt

Korrekturrand

VLAN	Abteilung
10	Verwaltung
20	Forschung
30	Labor
40	Marketing
99	IT

Die einzelnen Abteilungen der IHK-Med AG sind im gesamten Gebäude verteilt. Im Untergeschoss befindet sich zusätzlich das eigene Rechenzentrum (siehe beigefügte Netzwerkskizze, perforierte Anlage).

ba) Die Switches der IHK-Med AG bieten die Option, einen Port zu „taggen“ (802.1Q).

Erläutern Sie, welche Auswirkungen die Aktivierung dieser Option jeweils für den ein- bzw. ausgehenden Datenverkehr hat.
3 Punkte

bb) Markieren Sie in der folgenden Tabelle alle Ports auf dem Core-Switch, die „getaggt“ werden müssen. 2 Punkte

Core-Switch	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8
Option: Tagged	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

c) In der Konfigurationsoberfläche des Switches finden Sie die Einstellungsmöglichkeiten für das „native VLAN“. Sie recherchieren im Internet, was es damit auf sich hat, und stoßen auf den folgenden Text:

A native VLAN is a special VLAN whose traffic traverses on the 802.1Q trunk (i.e. tagged port) without any VLAN tag. A native VLAN is defined in 802.1Q trunk port standard which supports traffic coming from several VLANs as well as the traffic that doesn't come from a VLAN. The native VLAN is per trunk per switch configuration. The 802.1Q trunk port assigns untagged traffic on a native VLAN. That is, the native VLAN detects and identifies traffic coming from each end of a trunk link. By default, the native VLAN is VLAN 1, but it is recommended to be changed to any other number such as VLAN 99, VLAN 666, VLAN 777, etc. to prevent the risk of 'VLAN hopping'.

Quelle: frei nach <https://www.geeksforgeeks.org/difference-between-default-vlan-and-native-vlan/>

ca) Erläutern Sie, welche Auswirkungen das native VLAN für den Transport eines Frames über einen „Trunk“ (tagged port) hat.
2 Punkte

cb) Erläutern Sie, warum das native VLAN nicht identisch mit dem default VLAN (VLAN 1) sein sollte. 2 Punkte

Fortsetzung 1. Aufgabe

Korrekturrand

d) Nach dem Einbau und der Verkabelung der Switches sollen diese über das Netzwerk administriert werden.

Nennen Sie vier Einstellungen, die Sie vornehmen sollten, um den Zugriff auf den Switch zu ermöglichen und abzusichern.

4 Punkte

2. Aufgabe (30 Punkte)

a) Für die festgelegten VLANs sollen im nächsten Arbeitsschritt passende IP-Netze definiert werden.

aa) Für die VLANs 10, 20, 30 und 40 soll der private Adressbereich 172.16.0.0 / 12 verwendet und passend aufgeteilt werden.

Teilen Sie den angegebenen Bereich in vier gleich große Subnetze auf und ergänzen Sie die Tabelle in aufsteigender Reihenfolge.

4 Punkte

VLAN	Netzwerk-ID	Subnetzmaske (dezimal)
10		
20		
30		
40		

ab) Die IP des Standardgateways soll jeweils die letzte mögliche IP-Adresse der in Aufgabe aa) ermittelten Netzwerke sein.

5 Punkte

VLAN	IP des Standardgateways
10	
20	
30	
40	

Für das Rechenzentrum und die IT-Abteilung (VLAN 99) soll das komplette private Netzwerk 10.0.0.0 /8 verwendet werden. Auch hier soll das Standardgateway die letzte mögliche IP-Adresse im Netzwerk erhalten.

VLAN	IP des Standardgateways
99	

ac) Neben den beiden oben verwendeten privaten Bereichen existiert ein weiterer privater IP-Adressbereich, der für interne Netze genutzt werden kann (RFC 1918).

Geben Sie für diesen Bereich die Netz-ID und Netzmaske in CIDR-Notation an.

2 Punkte

- b) Die Verteilung der IP-Adressen der einzelnen VLANs soll ein zentraler DHCP-Dienst auf dem Server1 im Rechenzentrum übernehmen. Für jedes VLAN wurde auf dem Server ein passender Bereich eingerichtet.

- ba) Da die Internetverbindung an einem Client im VLAN 10 nicht funktioniert, überprüfen Sie die Netzwerkkonfiguration:

Ethernet-Adapter Ethernet:

IPv4-Adresse : 169.254.134.79

Subnetzmaske : 255.255.0.0

Beschreiben Sie, warum der Client diese IP-Adresse verwendet.

2 Punkte

- bb) Bei einer genaueren Analyse des Problems stellen Sie fest, dass alle Clients in den VLANs 10-40 eine IP-Adresse aus diesem Bereich verwenden. Lediglich die Clients im Rechenzentrum im VLAN 99 (IT) erhalten vom DHCP-Server eine IP-Adresse aus dem eigentlich vorgesehenen Bereich.

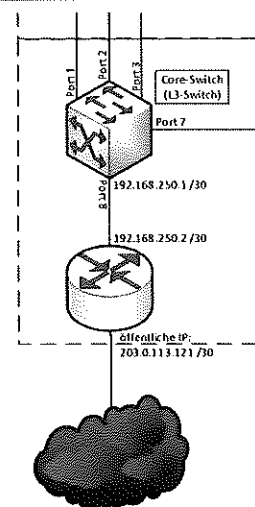
Beschreiben Sie eine mögliche Ursache und Lösung dieses Problems.

4 Punkte

- c) Für die Verbindung zwischen den VLANs wird der abgebildete Core-Switch verwendet, der für jedes VLAN als Standardgateway dient. Dieser ist über ein Verbindungsnetz (192.168.250.0 /30) mit dem Router des Unternehmens verbunden, der die Verbindung zum Internet herstellt (siehe Ausschnitt aus dem Netzwerkplan rechts).

- ca) Erläutern Sie, warum Sie beim Core-Switch lediglich eine Default-Route in der Routingtabelle ergänzen müssen.

2 Punkte



- cb) Tragen Sie die notwendige Route in die folgende Tabelle ein.

2 Punkte

Netzwerk-ID	Subnetzmaske (dezimal)	Next-Hop

- d) Aktuell erhält die Firma von ihrem Provider über einen DSL-Anschluss eine einzige öffentliche IPv4-Adresse.

- da) Erläutern Sie, wie es technisch realisiert wird, dass alle internen Geräte mit einer einzigen öffentlichen IP-Adresse mit dem Internet kommunizieren können.

3 Punkte

Fortsetzung 2. Aufgabe

Korrekturrand

db) Nennen Sie einen Vor- und einen Nachteil einer solchen Konfiguration.

2 Punkte

e) Die Firma erwägt, zukünftig auch über IPv6 auf das Internet zuzugreifen und erhält daher von ihrem Provider das öffentliche Präfix 2001:db8:1234::/56. Intern möchte die Firma bei der Adressvergabe SLAAC verwenden.

ea) Berechnen Sie nachvollziehbar, wie viele Subnetze die Firma mit diesem Netzwerk maximal erstellen kann.

2 Punkte

eb) Geben Sie die Netz-ID für das erste und das letzte dieser Subnetze in gekürzter Schreibweise an.

2 Punkte

3. Aufgabe (22 Punkte)

a) Sie sind an der Inbetriebnahme des Netzwerks am neuen Standort beteiligt.

aa) Sie prüfen intern die Erreichbarkeit des Internetgateways/Routers mittels ping.

Linux:

```
user@client:~$ ping -c 4 router.ihk-med.de
PING router.ihk-med.de (router.ihk-med.de(2001:db8:1234::1)) 56 bytes of data.
64 bytes from (2001:db8:1234::1): icmp_seq=1 ttl=63 time=0.533 ms
64 bytes from (2001:db8:1234::1): icmp_seq=2 ttl=63 time=0.497 ms
64 bytes from (2001:db8:1234::1): icmp_seq=3 ttl=63 time=0.456 ms
64 bytes from (2001:db8:1234::1): icmp_seq=4 ttl=63 time=0.468 ms

--- router.domain.de ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3072ms
rtt min/avg/max/mdev = 0.456/0.488/0.533/0.029 ms
```

Windows:

```
C:\Users\user>ping router.ihk-med.de
```

```
Ping wird ausgeführt für router.ihk-med.de [2001:db8:1234::1] mit 32 Bytes Daten:
Antwort von 2001:db8:1234::1: Zeit<1ms
Antwort von 2001:db8:1234::1: Zeit<1ms
Antwort von 2001:db8:1234::1: Zeit<1ms
Antwort von 2001:db8:1234::1: Zeit<1ms
```

```
Ping-Statistik für 2001:db8:1234::1:
```

```
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
            (0% Verlust),
```

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

```
    Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms
```

Nennen Sie den Rückschluss, den Sie aus den Ausgaben hinsichtlich der Erreichbarkeit und des verwendeten Protokolls ziehen können.

2 Punkte

ab) Sie überprüfen die Namesauflösung im Netzwerk:

Korrekturrand

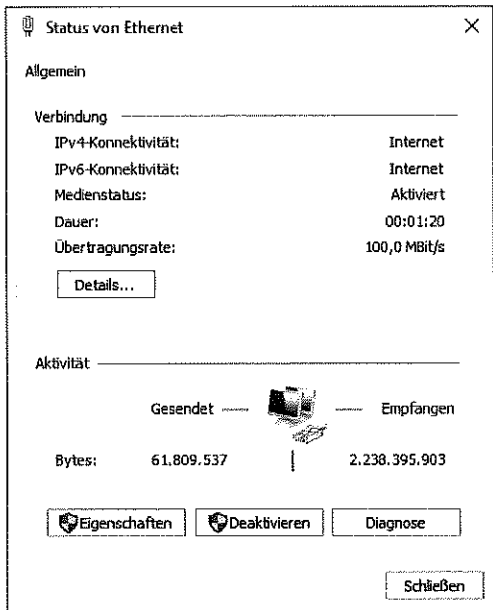
- (1) C:\Users\user>nslookup www.google.de
- (2) Server: ns.ihk-med.de
- (3) Address: 2001:db8:1234::53
- (4) Nicht autorisierende Antwort:
- (5) Name: www.google.de
- (6) Addresses: 2a00:1450:4001:815::2003
- (7) 142.251.36.163

Beschreiben Sie stichwortartig die Zeilen 2 bis 7.

6 Punkte

Zeile 2:	
Zeile 3:	
Zeile 4:	
Zeile 5:	
Zeile 6:	
Zeile 7:	

b) Einer der Mitarbeiter klagt über die lange Übertragungsdauer bei der Speicherung von großen Dateien auf den Fileserver. Switch und Netzwerkkarte im Client sind Gigabitfähig! Am Client wird angezeigt:



Nennen Sie zwei mögliche Ursachen für diesen Fehler.

2 Punkte

- c) Der Webserver der IHK-Med AG funktioniert nicht zuverlässig. Sie prüfen die Erreichbarkeit des Servers von mehreren Geräten aus.

Linux:

```
user@client:~$ ping -c 4 www.ihk-med.de
PING www.ihk-med.de (51.38.104.145) 56(84) bytes of data.

--- www.ihk-med.de ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3073ms
```

Windows:

```
C:\Users\user>ping www.ihk-med.de

Ping wird ausgeführt für www.ihk-med.de [51.38.104.145] mit 32 Bytes Daten:
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.

Ping-Statistik für 51.38.104.145:
    Pakete: Gesendet = 4, Empfangen = 0, Verloren = 4
            (100% Verlust),
```

Sie prüfen die Erreichbarkeit des HTTP-Dienstes:

Linux:

```
user@client:~$ telnet www.ihk-med.de 80
Trying 51.38.104.145...
Connected to www.ihk-med.de.
Escape character is '^]'.
^]
telnet> q
Connection closed.
```

Windows (powershell):

```
PS C:\Users\user> test-netconnection www.ihk-med.de -port 80
```

```
ComputerName      : www.ihk-med.de
RemoteAddress     : 51.38.104.145
RemotePort        : 80
InterfaceAlias    : Ethernet
SourceAddress     : 10.50.60.1
TcpTestSucceeded  : True
```

- ca) Beschreiben Sie eine mögliche Ursache, warum der Ping zu www.ihk-med.de keine Antwort liefert, der Test des HTTP-Dienstes über die Kommandozeile aber funktioniert. 3 Punkte

cb) Beim Aufruf der Webseite www.ihk-med.de im Webbrowser erhalten Sie folgende Fehlermeldung:

Korrekturrand



404 - File not found

content parameter is null

Beschreiben Sie eine mögliche Fehlerursache.

3 Punkte

d) Der Kunde betreibt am alten Standort einen FTP-Server. Am neuen Standort wird ein leistungsfähigerer Server mit dem FQDN ftp1.ihk-med.de aufgebaut. Für den alten FQDN ftp.ihk-med.de wurde eine Weiterleitung eingerichtet. Nun berichten externe Nutzer von Verbindungsproblemen beim Zugriff über den alten FQDN. Sie prüfen die DNS-Einträge:

ihk-med.de.	A	203.0.113.80
ihk-med.de.	AAAA	2001:db8:1234::80
ftp1.ihk-med.de.	A	03.0.113.21
ftp1.ihk-med.de.	AAAA	2001:db8:1234::21
ftp.ihk-med.de.	CNAME	ihk-med.de.
ns.ihk-med.de.	A	203.0.113.53
ns.ihk-med.de.	AAAA	2001:db8:1234::53

Beschreiben Sie den Grund, warum der Server nicht erreichbar ist, und machen Sie einen Vorschlag zur Fehlerbeseitigung.

6 Punkte

4. Aufgabe (23 Punkte)

Korrekturrand

Die IHK-Med AG setzt zur Sicherung des internen Netzes eine sogenannte *Next Generation Firewall* (NGFW) ein. Auf dieser ist unter anderem das Feature „SSL/TLS Inspection“ vorhanden, über dessen Einsatz bei einer Besprechung entschieden werden soll.

a) Ihr Vorgesetzter bittet Sie, zur Vorbereitung auf die Besprechung einige Fragen zu beantworten.

aa) Erläutern Sie, wie es der NGFW gelingt, den HTTPS-Traffic eines internen Clients zu einer externen Webseite trotz der TLS-Verschlüsselung zu untersuchen. 6 Punkte

ab) Nennen Sie einen sicherheitsrelevanten Vorteil für die IHK-Med AG, welcher für den Einsatz von SSL/TLS Inspection spricht. 2 Punkte

ac) Nennen Sie zwei Nachteile für das Unternehmen, die gegen den Einsatz von SSL/TLS Inspection sprechen. 4 Punkte

ad) Nennen Sie eine rechtliche bzw. organisatorische Maßnahme, welche Sie durchführen müssen, bevor Sie SSL/TLS Inspection durchführen dürfen. 2 Punkte

- b) Nach Abwägen der Vor- und Nachteile hat sich die IHK-Med AG für den Einsatz der SSL/TLS Inspection entschieden und die notwendigen rechtlichen bzw. organisatorischen Maßnahmen wurden durchgeführt. Auf der NGFW wurde eine Intermediate CA eingerichtet, um die NGFW-Zertifikate zu signieren.

Bei ersten Tests treten Probleme beim Zugriff auf HTTPS-Websites auf, bei denen der Zugriff zuvor reibungslos ablief. Sie sind mit der Analyse der Fehler beauftragt.

Erläutern Sie die folgenden Fehlermeldungen der Webbrowser und machen Sie jeweils einen Vorschlag zur Fehlerbehebung bezogen auf die NGFW. Dabei soll die SSL-TLS-Inspection weiterhin aktiv bleiben.

ba) Fehlermeldung: SEC_ERROR_UNKNOWN_ISSUER

3 Punkte

bb) Fehlermeldung: SEC_ERROR_EXPIRED_ISSUER_CERTIFICATE

3 Punkte

bc) Fehlermeldung: SSL_ERROR_VERSION_OR_CIPHER_MISMATCH

3 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.

☐

