Abschlussprüfung Sommer 2022
Lösungshinweise

Fachinformatiker/Fachinformatikerin
Systemintegration (AO 2020)
1202

2 Analyse und Entwicklung von Netzwerken

Teil 2 der Abschlussprüfung

Allgemeine Korrekturhinweise

Die Lösungs- und Bewertungshinweise zu den einzelnen Handlungsschritten sind als Korrekturhilfen zu verstehen und erheben nicht in jedem Fall Anspruch auf Vollständigkeit und Ausschließlichkeit. Neben hier beispielhaft angeführten Lösungsmöglichkeiten sind auch andere sach- und fachgerechte Lösungsalternativen bzw. Darstellungsformen mit der vorgesehenen Punktzahl zu bewerten. Der Bewertungsspielraum des Korrektors (z. B. hinsichtlich der Berücksichtigung regionaler oder branchenspezifischer Gegebenheiten) bleibt unberührt.

Zu beachten ist die unterschiedliche Dimension der Aufgabenstellung (nennen – erklären – beschreiben – erläutern usw.).

Für die Bewertung gilt folgender Punkte-Noten-Schlüssel:

Note 1	=		100 – 92 Punkte	Note 2	=	unter	92 – 81 Punkte
Note 3	=	unter	81 – 67 Punkte	Note 4	=	unter	67 – 50 Punkte
Note 5	=	unter	50 – 30 Punkte	Note 6	=	unter	30 – 0 Punkte

1. Aufgabe (30 Punkte)

aa) 5 Punkte

Netz-ID	203.0.113.160
Erste mögliche Host-IP	203.0.113.161
Letzte mögliche Host-IP	203.0.113.190
Broadcast	203.0.113.191
Subnetzmaske (dezimal)	255.255.255.224

ab) 4 Punkte

Die letzten 64 Bit dürfen nicht verwendet werden. Für das Subnetting steht der Bereich ab dem 56. Bit zur Verfügung: 64 – 56 = 8
Mit diesen 8 Bit können 256 Subnetze gebildet werden (2 hoch 8).

Erstes Netz: 2001:db8:ca::/64
Letztes Netz: 2001:db8:ca:ff::/64eg

ba) 3 Punkte

	Öffentliche IPv4-Adresse	Private IPv4-Adresse	Global Unicast IPv6-Adresse	Link-Local IPv6-Adresse
Herr Meier	x		x	
Frau Schmitt		x	x	
Herr Pfeiffer		x	x	

bb) 3 Punkte

	IPv4 only	IPv6 only	Dual Stack
Herr Meier			x
Frau Schmitt			x
Herr Pfeiffer			x

bc) 3 Punkte

	Herr Meier	Frau Schmitt	Herr Pfeiffer
Mobilfunk			x
Telefonkabel	x		
Koaxialkabel		x	

ca) 3 Punkte

1 Punkt für:
VPN = Virtual Private Network
2 Punkte für:
Verschlüsselte Datenverbindung (von Endgerät/Netzwerk zu anderen Endgerät/Netzwerk).

Oder
Traffic wird durch einen Tunnel geleitet, der die Verschlüsselung sicherstellt.
Nur „verschlüsselte Verbindung" nicht volle Punkte.
Andere Antworten möglich

cb) 4 Punkte

Traffic vom Dienstgerät enthält in der Regel sensible Daten, sodass der Traffic aus Gründen des Datenschutzes/der Datensicherheit nur zwischen Endgerät und Versicherung ausgetauscht werden darf.
Traffic des Mitarbeiters, der für externe Netze bestimmt ist (z. B. für das Internet) kann so von der Versicherung überwacht und bspw. auf Schadsoftware gefiltert werden.
Andere Antworten möglich

cc) 5 Punkte

Nach RFC 3021 benötigt ein Netzwerk für eine Punkt-zu-Punkt-Verbindung keine eigene IP für Netz-ID und Broadcast. Es können also Netze der Größe /31 verwendet werden.
Von /16 bis /31 sind 15 Bit für das Subnetting verfügbar: 2^15 = 32.768 Netze mit jeweils 2 IP-Adressen.

2. Aufgabe (28 Punkte)

aa) 3 Punkte
- Ausleuchtung mittels site survey (frequenzabhängig)
- Anzahl der benötigten Accesspoints (AP)
- Standort der AP
- Authentifizierung
- Verschlüsselung
- Anbindung an das Unternehmensnetzwerk
- Sonstige Sicherheitsaspekte (z. B. Gastzugang)
- u. a.

ab) 6 Punkte
Authentication: Prüfen der User-Credentials
Authorization: Berechtigung des Users festlegen
Accounting: Aktivitäten des Users protokollieren

ac) 4 Punkte
Vorteil:
- Kein gemeinsamer Schlüssel für alle User
- Individuelle Userverwaltung
- User kann z. B. deaktiviert werden bei Beendigung der Betriebszugehörigkeit

Andere Lösungen möglich

ad) 6 Punkte

technische Voraussetzung	Erklärung/Begründung
eigene SSID	Das Gastnetzwerk ist durch einen Namen eindeutig identifizierbar.
eigener IP-Adressbereich	logische Trennung; einfachere Verwaltung; getrenntes Routing der Pakete
Captive-Portal (Voucher)	Begrenzung der Nutzungs-Zeit für einzelne Gäste; Zuordnung des Traffics zu einzelnen Gästen

Andere Lösungen möglich

ba) 4 Punkte
Unterteilung des physischen Netzwerks auf Layer 2
Verkleinern der Broadcast-Domäne
Traffic eines VLANs ist von den anderen VLANs abgetrennt

Andere Antworten möglich

bb) 2 Punkte
Beide Switchports müssen auf VLAN-Tagging (z. B. 802.1q) gesetzt werden.

bc) 3 Punkte
- Port Security schränkt das Limit von MAC-Adressen, welche pro Switchport gespeichert werden dürfen, ein. Beim Erreichen des Limits erfolgt eine „security violation" und der Port leitet keinen Traffic mehr weiter bzw. wird deaktiviert. So lassen sich die zulässigen Endgeräte festlegen, die an den jeweiligen Port angeschlossen werden dürfen.
- Einloggen nur für authentifizierte Benutzer nach 801.1x bzw. über RADIUS, sodass nur zulässige Geräte eine Datenverbindung aufbauen können (z. B. Cisco ISE).
- Einloggen nur für Geräte, die im Radius-Server in der Gerätedatenbank z. B. anhand ihrer MAC freigeschaltet wurden

Andere Lösungen möglich

3. Aufgabe (20 Punkte)

a) 3 Punkte
Die Option „Entschlüsseln und scannen" sollte gewählt werden, da nur so die aufgerufenen Webseiten auf Schadsoftware gescannt und hochgeladene Daten geprüft werden können. (Bei der Option „Nur URL-Filterung" kann keine Prüfung des Inhaltes auf Schadsoftware durchgeführt werden.)

ba) 4 Punkte
(Hinweis: Die Fehlermeldung erscheint, da der Proxyserver den Datenverkehr zwischen Proxy und dem IHK-Webserver entschlüsselt, scannt und die Daten mit einem selbstausgestellten Zertifikat Richtung Client erneut verschlüsselt. Siehe Aufgabenteil 3a)).
Hier ist das verwendete Root-Zertifikat des Proxyservers dem Client nicht bekannt bzw. nicht als vertrauenswürdig hinterlegt und daher werden die selbstausgestellten Zertifikate des Proxyservers als „nicht sicher" markiert.

Andere Antworten möglich

bb) 2 Punkte
- Root-Zertifikat des Proxyservers auf dem Client in die Liste der vertrauenswürdigen Stammzertifizierungsstellen aufnehmen (manuell oder bspw. über GPO)
- Root-Zertifikat des Proxy-Server durch eine bereits vertrauenswürdige Stammzertifizierungsstelle des Clients signieren lassen
- Der Benutzer fügt eine dauerhafte Ausnahme für diese Seite hinzu.

Andere Antworten möglich

ca) 4 Punkte
- Anonymisierung: Als einziger Zugang zum internen Netzwerk fängt ein Reverse-Proxy sämtliche Anfragen an Server im Hintergrund ab und agiert Client-Programmen gegenüber so, als ob sie es mit dem eigentlichen Zielsystem zu tun hätten.
- Schutz und Verschlüsselung: Ein vorgeschalteter Reverse-Proxy bietet die Möglichkeit, Kontrollsysteme wie Virenscanner oder Paketfilter zu konfigurieren. Darüber hinaus lassen sich Reverse-Proxy-Server zur Verschlüsselung einsetzen.
- Load-Balancing: Durch einen vorgeschalteten Reverse-Proxy lässt sich eine URL mit mehreren Servern im privaten Netzwerk verknüpfen und die eingehenden Anfragen auf mehrere Server verteilen. Die Verfügbarkeit der URL wird so auch bei Ausfällen weiterhin sichergestellt.
- Caching: Um die Geschwindigkeit von Serverdiensten zu beschleunigen, bietet der Reverse-Proxy die Funktion, Serverantworten zwischenzuspeichern. Dabei werden statische Inhalte wie Bilder oder häufig aufgerufene dynamische Webseiten im Cache des Proxys vorgehalten.
- Kompression: Ein Reverse-Proxy kann zur Kompression eingehender und ausgehender Daten eingesetzt werden.

cb) 3 Punkte
Eine DMZ (demilitarisierte Zone) ist ein eigener Netzwerkbereich, der zwischen dem internen und dem externen Netzwerk steht und Dienste beheimatet, die von außen erreichbar sein müssen. Ein direkter Durchgriff auf das interne Netzwerk wird so verhindert.

cc) 4 Punkte
Reverse-Proxy, Webserver und Mailserver sollten in der DMZ platziert werden, da diese aus dem Internet (und von innen) erreichbar sein müssen und deshalb vom internen Netz abgetrennt sein sollten.
Datenbank-Server, AD-Server und Druck-Server: sollten im internen Netz verbleiben, da ihre Dienste nicht von außen erreichbar sein müssen.

Andere Begründungen möglich

4. Aufgabe (22 Punkte)

aa) 4 Punkte
Eine 16 Mbit/s ADSL-Leitung hat eine zu geringe Bandbreite, vor allem im Upload. Wenn anderer Datenverkehr in Richtung Internet geht, steht nicht genug Bandbreite für gute Bildqualität und/oder Tonqualität bereit.

ab) 4 Punkte
1.634 MiB = 1.634 * 1.024 * 1.024 * 8 Bit = 13.706.985.472 Bit
13.706.985.472 Bit / 16.000.000 Bit/s = 856,69 Sekunden = 14,28 Minuten (14 Minuten, 17 Sekunden)

ba) 6 Punkte

Beispiele für weitere Filterregel
Nicht mehr als 100 Empfänger der Mail bei bekanntem Absender
Absender steht auf der White-List
Im Betreff kommen unerwünschte Begriffe vor.
Absender-Domain und angezeigter Absender-Name stimmen nicht überein.
Anhänge haben unbekannte Datei-Formate.

Weitere Lösungen möglich

bb) 4 Punkte
Die Firma muss ihre Mitarbeiter nachweislich auf die Kontrolle durch Spamfilter oder Administratoren hinweisen oder privaten Mailverkehr untersagen. Wenn es sich nur um geschäftliche Inhalte handelt, darf die Firma den Mailverkehr einsehen.

bc) 4 Punkte
Eine Sandbox ist eine abgeschottete virtuelle Maschine mit verschieden Betriebssystem-Konfigurationen. Darin kann die Datei automatisiert auf unerwünschtes Verhalten überprüft werden.