

Datum:

IP-Konfiguration und Firewall-Regeln überprüfen und vervollständigen.

Sie sind Mitarbeiterin / Mitarbeiter der Rain GmbH.

Die Rain GmbH plant eine umfangreiche Reorganisation ihres IT-Systems. Sie sollen im Rahmen dieses Projekts folgende Aufgaben erledigen:

Die RAIN GmbH verfügt über die abgebildete Netzwerkstruktur (siehe perforierte Anlage).

- a) In der DMZ und im LAN sollen IP-Adressen und Subnetzmasken ergänzt werden.
- aa) Erläutern Sie, wie viele Hosts in der DMZ zusätzlich zu den vorhandenen Geräten noch angeschlossen werden können.

- ab) Die ETH0-Schnittstelle der Firewall II hat die IP-Adresse 10.0.7.254 erhalten.

Diese IP-Adresse soll die letzte Adresse im Subnetz sein.

Ermitteln Sie die entsprechende Subnetzmaske. Der Rechenweg ist anzugeben.

[illegible]

- b) Auf der Firewall II, die nach dem Prinzip der Stateful Packet Inspection arbeitet, wurden folgende Firewall-Regeln aufgestellt:

| Nr | Aktion | Protokoll | Quell-IP | Ziel-IP | Quell-Port | Ziel-Port | von Interface | nach Interface |
|----|--------|-----------|------------|------------|------------|-----------|---------------|----------------|
| 1 | Permit | IP | Admin-PC | Any | - | - | ETH0 | ETH1 |
| 2 | Permit | IP | DC mit DNS | Any | - | - | ETH0 | ETH1 |
| 3 | Permit | TCP | Proxy | Any | any | 80 | ETH0 | ETH1 |
| 4 | Permit | TCP | Proxy | Any | any | 443 | ETH0 | ETH1 |
| 5 | Permit | TCP | LAN | Mailserver | any | 25 | ETH0 | ETH1 |
| 6 | Permit | TCP | LAN | Mailserver | any | 110 | ETH0 | ETH1 |
| 7 | Deny | IP | Any | Any | | | | |

Sie versuchen, am Client 1 die Internet-Seite www.ihk.de im Browser zu öffnen. Dabei erhalten Sie die Fehlermeldung, dass die Webseite nicht angezeigt werden kann. Die Verbindung zum internen Mailserver funktioniert. Der Admin-PC kann die Seite www.ihk.de im Browser öffnen.



ba) Erläutern Sie anhand der Firewall-Regeln und des Netzwerkplans die Ursache dieser Fehlermeldung.

bb) Erläutern Sie, wie Sie Client 1 Zugriff auf das Internet ermöglichen können.

c) Beim Versuch, vom Admin-PC aus die Erreichbarkeit des Mail Transfer Agents des Providers mit dem Befehl *ping* zu überprüfen, erhalten Sie die folgende Fehlermeldung:

Antwort von 10.0.7.254: Zielhost nicht erreichbar

Ein Ping auf den internen Mailserver funktioniert dagegen einwandfrei.

Sie lassen sich die Routingtabellen der beiden Firewalls anzeigen:

Firewall I

| Netzwerk | Subnetzmaske | Schnittstelle/Next-Hop |
|--------------|-----------------|------------------------|
| 192.168.99.0 | 255.255.255.248 | ETH0 |
| 0.0.0.0 | 0.0.0.0 | ETH1 / 82.84.90.1 |

Firewall II

| Netzwerk | Subnetzmaske | Schnittstelle/Next-Hop |
|--------------|-----------------|------------------------|
| 10.0.0.0 | 255.255.248.0 | ETH0 |
| 192.168.99.0 | 255.255.255.248 | ETH1 |
| 0.0.0.0 | 0.0.0.0 | ETH1 / 192.168.99.1 |

Erläutern Sie, welcher Fehler in den Routing-Tabellen vorliegt und wie Sie diesen Fehler beheben können.

d) Auf Firewall I wird die folgende Portforwarding-Regel eingerichtet:

| Protokoll | Quell-IP | Ziel-Port | Aktion | Ziel-IP | Ziel-Port |
|-----------|------------------------------|-----------|---------|------------|-----------|
| TCP | Mail Transfer Agent Provider | 25 | Forward | Mailserver | 25 |

Erläutern Sie den Zweck dieser Regel.



Netzwerkplan der RAIN GmbH

