Technische Hochschule Ingolstadt
Fakultät Informatik

Prof. Dr. Michael Jarschel
Kommunikationsnetze & Cybersecurity

Raum B109
Tel +49 841 9348-5184
Email michael.jarschel@thi.de
Web www.thi.de

Prüfungssemester: **SoSe 2022**

Prüfungsdatum: **13.07.2022**

Studiengang: **Informatik (IM)**

Prüfungsfach: **Sicherheit moderner Netzwerke**

Dozent: **Prof. Dr. Michael Jarschel**

Matrikel-Nr.: _____

Semester: _____

Raum: **J101, 11:15 Uhr**

Platzziffer: _____

Hinweise:

- Legen Sie bitte ihren Personalausweis und Studierendenausweis bereit.
- Bitte verwenden Sie nur Kugelschreiber oder Füller, auf keinen Fall rote oder grüne Stifte.
- Es sind keine Hilfsmittel zugelassen!
- Bei Platzmangel benutzen Sie bitte die Rückseite des jeweiligen Angabenblattes.

Aufgabe	1	2	3	4	5	Summe
Punkte (max.)	(13)	(15)	(21)	(20)	(21)	(90)

Note:

Aufgabe 1: Netzsicherheit allgemein (13 Punkte):

a) Die Maßnahmen, die wir Angreifern aus dem Internet entgegenstellen, um die Sicherheit unsere Netze zu gewährleisten, lassen sich in drei große Kategorien einordnen. Wie lauten diese Kategorien?

b) Erläutern Sie den Unterschied zwischen dem Schutzziel Verfügbarkeit und Vertraulichkeit.

c) Botnetze gehören zu den Standardwerkzeugen von Angreifern. Für welche Art von Angriff werde diese am häufigsten verwendet? Begründen Sie ihre Antwort!

d) Phishing ist einer der weit verbreitetsten Angriffsarten. Was versteht man darunter und wie unterscheidet sich Phishing von Spear-Phishing?

e) Was versteht man unter einem Honeypot und wofür wird er eingesetzt?

f) Die stark ansteigende Anzahl von Internet-fähigen Geräten im Bereich „Internet of Things“ (IoT) stellt die Netzsicherheit vor große neue Herausforderungen. Nennen Sie zwei Gründe, warum eine große Anzahl von IoT Geräten ein Sicherheitsrisiko darstellen können.

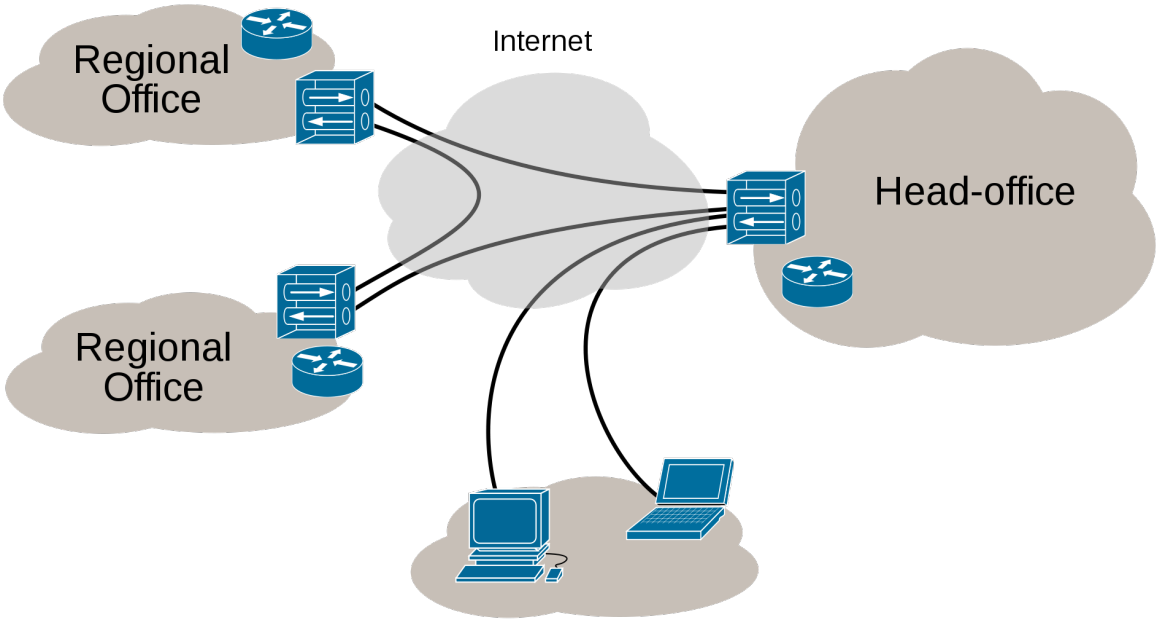
Aufgabe 2: IPSec (15 Punkte):

a) Sie sind über WLAN mit dem lokalen Netz Ihrer Firma verbunden. Warum kann es sinnvoll sein in dieser Situation sich dennoch zusätzlich mit dem IPSec-VPN (Virtual Private Network) zu verbinden?

b) Welche Daten könnte ein Man-in-the-Middle im Falle von ESP im Tunnel-/Transportmodus lesen?

c) Welche Sicherheitsziele verfolgt IPSec?

d) Welches Problem tritt bei IPSec in Kombination mit NAT (Network Address Translation) auf?

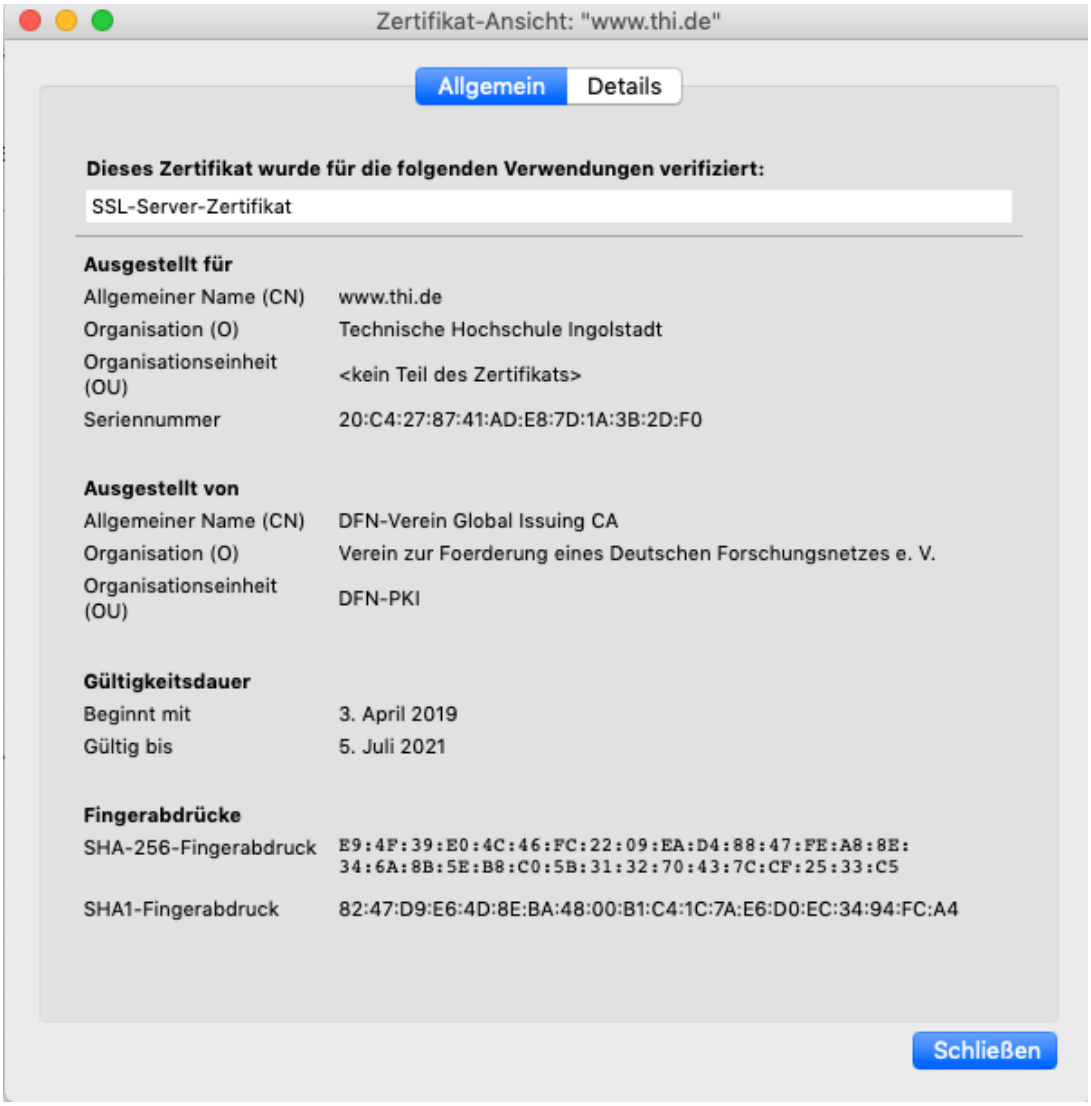


e) Sie sind der Netzverantwortliche eines mittelständischen Unternehmens. Das Unternehmen ist kürzlich stark gewachsen und hat wie abgebildet nun zwei Zweigniederlassungen sowie Außendienstmitarbeiter dazu gewonnen. Sowohl die Niederlassungen als auch die Mitarbeiter sollen über IPSec mit der Zentrale Daten austauschen können. Die Daten sind unbedingt vertraulich zu behandeln. Welche IPSec Variante setzen Sie jeweils ein? Begründen Sie ihre Entscheidung!

Aufgabe 3: TLS und Zertifikate (21 Punkte):

a) Unter dem Begriff „Crypto Agility“ versteht man das dynamische Aushandeln kryptografischer Verfahren. Beschreiben Sie kurz, wie TLS Crypto Agility realisiert.

b) Die folgende Abbildung zeigt die Darstellung eines Zertifikats im Firefox Browser beim Zugriff auf https://www.thi.de.

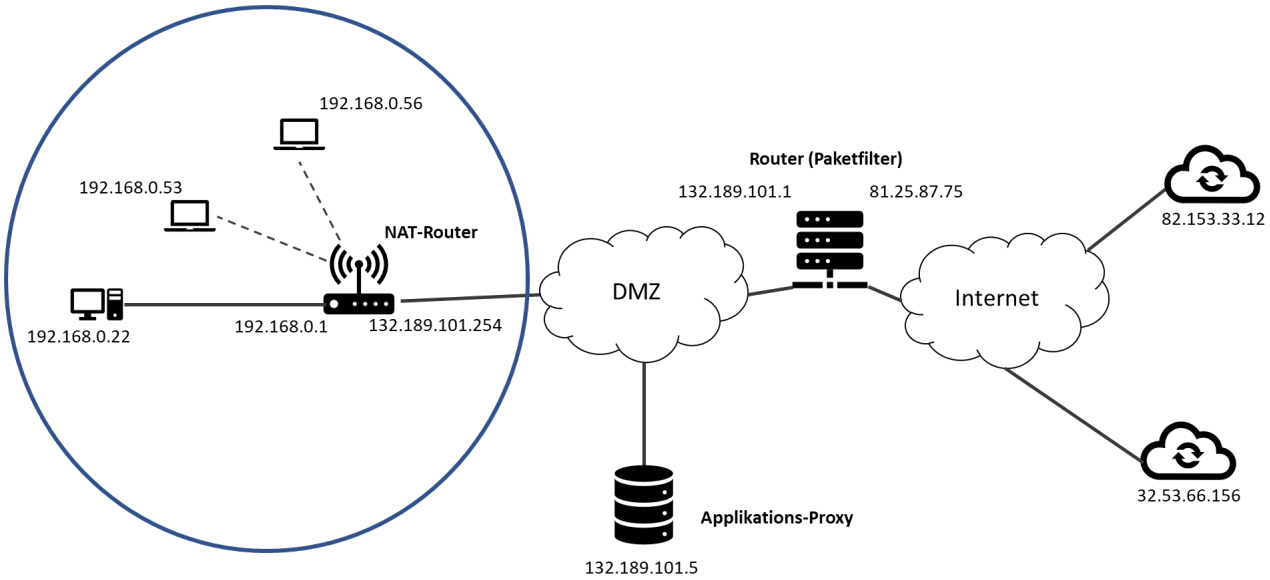


Beschreiben Sie die einzelnen Schritte die der **Firefox-Browser allgemein** durchführen muss, um die Vertrauenswürdigkeit **der Webseite https://www.thi.de** zu überprüfen.

c) Müsste der **Firefox-Browser** das **abgebildete** Zertifikat akzeptieren oder ablehnen? Begründen Sie Ihre Antwort!

Aufgabe 4: Firewalls (20 Punkte):

Gegeben ist das abgebildete Szenario eines Firmennetzes. Das Netz besteht aus einem internen Bereich (192.168.0.0/24), der über einen NAT-Router an die DMZ (Demilitarized Zone) angebunden ist. Im internen Netz hat der Router die IP Adresse 192.168.0.1. In der DMZ liegt der Adressbereich 132.189.101.0/24 an, der bereits öffentlich geroutet wird. Der NAT-Router besitzt hier die IP Adresse 132.189.101.254. Die DMZ ist über einen Router mit einer zustandslosen Paket-Filter Firewall an das Internet angebunden. Dieser hat zur DMZ hin die IP Adresse 132.189.101.1 und die externe IP Adresse 81.25.87.75. Weiterhin steht in der DMZ ein Bastion Host mit der IP Adresse 132.189.101.5, der als Applikationsproxy fungiert. Alle Hosts im internen Netz können nur über diesen Applikationsproxy auf das Internet zugreifen.



Der Nutzer der Workstation mit der IP 192.168.0.22 im internen Netz möchte gerne auf den Cloud-Dienst im Internet mit der IP Adresse 32.53.66.156 (TCP Port 80) zugreifen. Die Nutzer der beiden Laptops mit den IP Adressen 192.168.0.53 und 192.168.0.56 wollen ebenfalls auf einen Cloud-Dienst mit der Adresse 82.153.33.12 (TCP Port) zugreifen.

a) Damit diese Verbindung möglich wird, muss zunächst etwas auf den Client-Hosts konfiguriert werden. Worum handelt es sich dabei und warum ist die Konfiguration notwendig?

b) Geben Sie die NAT-Übersetzungstabelle des NAT-Routers zwischen internem Netz und DMZ für die Verbindungen der drei Hosts aus dem internen Netz an!

LAN IP	LAN Port	DMZ IP	DMZ Port

c) Die Firewall zwischen DMZ und Internet soll standardmäßig keinen Verkehr durchlassen. Erlaubte Zugriffe müssen explizit eingetragen werden (Whitelisting). Spezifizieren die Paketfilterregeln, die in der Firewall eingetragen sein müssen, damit nur die TCP Verbindungen zwischen den internen Hosts und den Cloud-Diensten zulässig sind!

Nr.	**Quell IP**	**Ziel IP**	**Protokoll**	**Quellport**	**Zielport**	**Aktion**

d) Nennen Sie einen Vorteil und einen Nachteil, den zustandsbehaftete Firewalls gegenüber zustandslosen Firewalls haben!

Aufgabe 5: Mobilfunknetze (Punkte):

a) Skizzieren Sie **entweder** den logischen Aufbau eines **LTE oder 5G** Mobilfunknetzes mit seinen funktionalen Komponenten. Geben weiterhin stichpunktartig **5 Aufgaben des Mobilfunk-Kernnetzes** an!

b) Welche Informationen (Daten, o.ä.) sind in der SIM-Karte permanent gespeichert?

c) Beschreiben Sie bitte die Anmeldeprozedur eines Teilnehmers an einem GSM-Mobilfunknetz. **(Bitte eine Skizze)**
Achten Sie auch auf die zeitliche Reihenfolge.
Welche Informationen zur Authentifizierung eines Teilnehmers liegen der MSC vor?