

**Arbeitsauftrag: LF9**

## Realisierung der virtuellen Netzwerk-Infrastruktur zu LF 9 (2. LJ)

### Erstellung logischer Netzwerkplan

#### Ausgangssituation

Für die Durchführung der Projektaufträge im LF9 ist die Netzwerk-Laborumgebung bereitzustellen. Die Infrastruktur ist unter Einhaltung der Sicherheitsanforderung „Security by Default“ grundsätzlich über eine administrierbare Firewall (IP-Fire) inklusive einer DMZ zu konzipieren.

Nachstehende Eigenschaften sind als **Mindestforderungen** der Infrastruktur zu garantieren.

#### 1. Einsatz

- Das Setup ist die für Schul-Umgebung zu konzipieren.
- Das VM-Netzwerk für das Routing in das Schulnetz ist das Netzwerk VMNet8 („rot“) mit der Netzwerkadresse wie im Schulimage vorgegeben. Virtuelles NAT-Gateway, DNS und DHCP bleiben aktiv.
- Die virtuellen Gateways und die DHCP Dienste der Host-Only-Netze („orange“ und „grün“) aus dem Schulimage sind für das Projekt zu deaktivieren.

#### 2. Individualisierung

Die IPv4 Klasse-C-Netzwerkadressen des Intranets hinter der Firewall („grün“) und die DMZ („orange“) sind nach folgenden Regeln zu bilden:

- „grün“ VMNet1 = Klassenbuchnummer des Projektleiters im dritten Segment
- „orange“ VMNet2 = 100 + Klassenbuchnummer des Projektleiters im dritten Segment

#### 3. Administration

Die Firewall-Instanz ist ausschließlich aus dem Intranet administrierbar.

#### 4. Funktionalität

Die virtuellen Maschinen im Intranet und in der DMZ können externe DNS-Namen auflösen.

#### 5. Sicherheitshinweis

Als DNS für den IP-Fire Server ist ausschließlich der DNS-Dienst des virtuelle Gateways des VMnet8-Netzwerkes mit dem Protokoll UDP oder TCP zu verwenden.

Zur fehlerfreien Kommunikation mit dem VMnet8-Gateway ist vor der Einrichtung des DNS die Datei „unbound.conf“ aus dem Vorlagenverzeichnis in das Verzeichnis „/etc/unbound/“ der IP-Fire-VM zu kopieren.

**Arbeitsauftrag: LF9****Planung**

Die Netz-Infrastruktur ist **vor** der Realisierung mit folgenden Mindestangaben als logischer Netzwerkplan in *elektronischer Form* zu dokumentieren und **abzugeben**:

**1. Endsysteme**

- a. Netzwerkserver von DNS und Proxy des Schulnetzwerkes
- b. Physischer Virtualisierungshost
- c. VM-Firewall-Server
- d. VM-Client zur Browser-Administration der Firewall

Die VM-Endsysteme und der Virtualisierungshost sind mit folgenden Informationen zu versehen:

- Hostname und Domänenzugehörigkeit  
der Hostname der VMs ist sinnvoll festzulegen
- IP - aller Netzwerkinterfaces
- MAC-Adressen aller Netzwerkinterfaces des VM-Firewall-Servers
- Betriebssystem mit Version
- projektrelevante Software und Dienste mit Portangabe
- verwendete Benutzerkonten für administrative Zwecke

**2. Zwischensysteme**

- VM-Netz und Schulnetz bis Proxy
- Angabe der Funktion im Netzwerk
- Angabe der funktionale IP-Adressen der Systeme (z.B. für virtuelles Gateway in VMnet8)

**Arbeitshinweise für die berufstypische Softwareumgebung**

Nutzen Sie „<https://app.diagrams.net/>“ oder ein gleichwertiges Softwareprodukt für die Erstellung des logischen Netzwerkplanes.

Verwenden Sie standardisierte Symbole und Beschriftungen für virtuelle und physische End- und Zwischensysteme. Erstellen Sie eine Legende.

**Abgabe**

Die Abgabe erfolgt am Ende der 2. Unterrichtswoche, spätestens Freitag 24 Uhr.

Laden Sie das Arbeitsergebnis als PDF-Dokument in den Unterordner „Schülerlösungen/ Netzwerkplan“ im Projektverzeichnis zu „IP-Fire“ des Lernfeldes 9 im Lernsax.

Benennen Sie das Dokument eindeutig in Bezug auf die Zuordnung zum Projektnamen und den Projektteilnehmern und geben Sie im Dokument Informationen zum Projekt (Thema, Projektteilnehmer, Klasse, Datum, Versionierung)

**Arbeitsauftrag: LF9**

## Bewertung

Netzplan als PDF im Ordner abgelegt / Beschriftung des Dokumentes laut Vorgabe	1
Projektinformationen im Dokument vollständig	1
VM-Netze und Schul-Netz (incl. Proxy) dargestellt / Struktur der Netze korrekt	3
Systeme im Schulnetz für DNS und PROXY sowie Zwischensysteme sind incl. ermittelbarer IP-Adressen dargestellt	3
IP-Adressvorgabe der VM-Netze entspricht der Vorgabe, Netzadressen sind in der Abbildung vollständig angegeben	2
Virtualisierungshost und VM-Endsysteme sind mit Darstellung der Netzanbindung an Ihre Netze dargestellt	3
Angaben zu VM-Endsystemen und Virtualisierungshost sind vollständig	6
IP Adressen aller Interfaces sind angegeben (VM und Schulnetzes)	3
NAT- Gateway im roten Netz ist mit Adressen und Diensten ist dargestellt	2
Legende aller Symbole oder vollständige Beschriftungen vorhanden	1
Abzug: 10 Prozent der erreichbaren Punkte bei verspäteter Abgabe	-2,5
Abzug: 30 Prozent der erreichbaren Punkte bei verspäteter Abgabe von mehr als 3 Tagen	-7,5

Erreichbare Punkte: 25

0	6
7,5	5
12,5	4
17	3
20,5	2
23	1