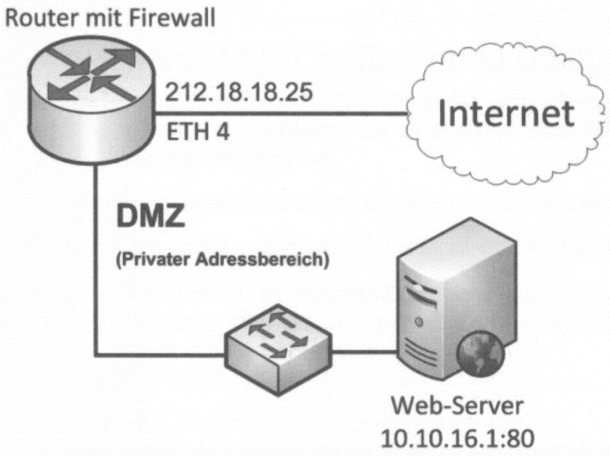
Berufliche Schule der Landeshauptstadt Schwerin – Technik

LF: Firewall Datum:

Aufgabe: Einen Internetzugangsrouter anschließen und konfigurieren.

Der Internetzugangsrouter der VeloShop GmbH muss angeschlossen und konfiguriert werden. Ein wesentlicher Teil ist dabei die sicherheitstechnische Konfiguration.

Installationen im Technik-Raum



a) Der Webserver in der DMZ soll gegen Gefahren aus dem Internet geschützt werden.

Nennen Sie vier Gefahren, gegen die am Router entsprechende Maßnahmen ergriffen werden müssen. 2 Punkte

Sicherheitsmaßnahmen zum Schutz des Routers

- Der **Router** als Einfallstor für Malware. ...
- Die 6 wichtigsten Schutzmaßnamen für **Router**. ...
- **Router**-Passwort, WLAN-Passwort und WLAN-Namen (SSID) ändern. ...
- Firewall aktivieren und nicht benötigte Funktionen deaktivieren. ...
- WPA2-Verschlüsselung nutzen. ...
- Firmware regelmäßig updaten.
- Ports überprüfen und unnötige schließen.

Viren, Malware, Botangriffe, Trojaner etc.

b) Zur Konfiguration der Firewall finden sich in der Beschreibung des Herstellers folgende Angaben:

> Die Firewall der NetBox bietet folgende Sicherheitsfunktionen:
> - **IP-Masquerading** bzw. **Network Address Translation (NAT)**
> - **Stateful Packet Inspection**

Beschreiben Sie, wie folgende Funktionen zum Schutz des Unternehmensnetzwerkes beitragen. 6 Punkte

IP-Masquerading bzw. NAT:

NAT (Network Address Translation oder Network Address Translator) ist die Übersetzung einer Internet-Protocol-Adresse (IP-Adresse), die in einem Netzwerk verwendet wird, in eine andere IP-Adresse, die in einem anderen Netzwerk verwendet wird.

Durch Umsetzung der internen IP auf eine öffentliche IP sind die Rechner nicht direkt erreichbar.

Stateful Packet Inspection:

Unter Stateful Packet Inspection (SPI; deutsch Zustandsorientierte Paketüberprüfung) versteht man eine dynamische Paketfiltertechnik, bei der jedes Datenpaket einer bestimmten aktiven Session zugeordnet wird.
Die Datenpakete werden analysiert und der Verbindungsstatus wird in die Entscheidung einbezogen.

Pakete werden nur durchgelassen, wenn eine Anfrage von innen erfolgt ist.

c) Der Zugangsrouter muss für den http-Zugriff auf den internen Webserver konfiguriert werden (siehe logischer Netzwerkplan).

Für das Portforwarding und die Erstellung der notwendigen Firewallregel (SPI) stellt der Zugangsrouter die folgenden zwei Konfigurationsdialoge zur Verfügung.

ca) Ergänzen Sie im Konfigurationsdialog für das Portforwarding die fehlenden Parameterwerte. 5 Punkte

Portforwarding-Parameter	
Beschreibung:	Webserver-Zugriff
Schnittstelle:	ETH 4
Art des Datenverkehrs:	Eingehend (Ziel-NAT)
Ursprünglichen Datenverkehr angeben	
Dienst/Protokoll/Port:	80
Quell-IP-Adresse:	beliebig oder any
Originale Ziel-IP-Adresse:	212.18.18.25
Substitutionswerte	
Neue Ziel-IP-Adresse:	10.10.16.1
Neuer Ziel-Port:	Original [x] oder Port _____
OK	Abbrechen

cb) Ergänzen Sie im Konfigurationsdialog die fehlenden Parameterwerte der Firewall für den http-Zugriff. 4 Punkte

Firewall-Regel-Parameter	
Quell-IP:	Any
Ziel-IP:	10.10.16.1
Dienst/Protokoll:	http
Aktion:	Permitt oder Accept oder Allow
OK	Abbrechen

d) Die Router bietet die Möglichkeit, den Webserver in einer DMZ oder als „Exposed Host" (siehe englischer Text) erreichbar zu machen.

> Some routers refer to an **Exposed Host**. A home router exposed host is a single address (e.g., IP address) on the internal network that has all traffic sent to it which is not otherwise forwarded to other LAN hosts. By definition this is not a true DMZ (demilitarized zone), since it alone does not separate the host from the internal network. That is, the DMZ host is able to connect to hosts on the internal network, whereas hosts within a real DMZ are prevented from connecting with the internal network by a firewall that separates them, unless the firewall permits the connection.

Begründen Sie, weshalb die Option „Exposed Host" nicht verwendet werden sollte. 3 Punkte

e) Für den Betrieb des Webservers wird der Einsatz von DynDNS in Erwägung gezogen.

ea) Erläutern Sie die Arbeitsweise und Funktion von DynDNS. 3 Punkte

Dynamisches DNS, DDNS oder DynDNS ist eine Technik, um Domains im Domain Name System (DNS) dynamisch zu aktualisieren.
Der Zweck ist, dass ein Computer (bspw. ein PC oder ein Router) nach dem Wechsel
seiner IP-Adresse automatisch und schnell den dazugehörigen Domaineintrag ändert.

eb) Begründen Sie, ob das Angebot des Providers DynDNS erfordert. 2 Punkte

NEIN -> Feste IP-Adresse

Einige Router verweisen auf einen Exposed Host. Ein exponierter Host eines Heimrouters ist eine einzelne Adresse im internen Netzwerk, an die der gesamte Datenverkehr gesendet wird, der sonst nicht an andere LAN-Hosts weitergeleitet wird. Per Definition ist dies keine echte demilitarisierte Zone, da sie allein den Host nicht vom internen Netzwerk trennt. Das heißt, der DMZ-Host kann sich mit Hosts im internen Netzwerk verbinden, während Hosts innerhalb einer echten DMZ durch eine Firewall, die sie trennt, daran gehindert werden, sich mit dem internen Netzwerk zu verbinden, es sei denn, die Firewall erlaubt die Verbindung.

Exposed Host können sich mit dem Webserver im gleichen Subnetz befinden. Also wäre eine lokaler Zugriff möglich.