Fragen zur Theorie - VPN

1.1 Fragen zur Theorie

1. Was ist VPN?

   Virtual Private Network,

   Ein Virtual Private Network (VPN) ist ein Computernetz, welches zum Transport privater Daten ein öffentliches Netz, zum Beispiel das Internet, nutzt. Die Verbindung über das öffentliche Netz wird üblicherweise verschlüsselt.

2. Nutzen von VPN?

   Es ermöglicht somit eine sichere Übertragung über ein unsicheres Netzwerk. Teilnehmer eines VPN können Daten wie in einem LAN (lokales Netzwerk) austauschen. Die einzelnen Teilnehmer selbst müssen hierzu nicht direkt miteinander verbunden sein.

3. Wo wird es eingesetzt?

   Wirtschaft, Schule, etc.

4. Was ist der Unterschied zwischen Site-to-Site VPN und Remote Access VPN?

   Site-to-Site VPN verbindet die Filialen über eine öffentliche Infrastruktur.

   - *Intranet – Nur den Mitarbeitern des Unternehmens ist der Zugriff gestattet.*
   - *Extranet – Mitarbeitern, Lieferanten, Geschäftspartnern ist der Zugriff gestattet.*

   Remote Access VPN ist an mobile Benutzer (Handy, Laptop) und Heimbüros gerichtet.

   - *Client-Initiated*
   - *Network Access Server-Initiated*

5. Wie kann VPN gewährleisten, dass sich kein Sniffer zwischen den Peers befindet? Nennen Sie drei Mechanismen.

   - *Geheimhaltung des Inhalts (Encryption) – Der Sender verschlüsselt die Pakete, bevor er sie durch das Netzwerk übermittelt. Nur ein berechtigter Empfänger kann das Paket entpacken.*
   - *Datenintegrität (Hash) – Der Empfänger überprüft, ob die ankommenden Daten während der Reise durch das Internet verändert wurden.*
   - *Authentifizierung des Senders – Der Empfänger überprüft den Absender, woher das Paket kommt, und ob der Sender berechtigt war, Informationen mitzuteilen.*

6. Was ist der Unterschied zwischen Tunnel- und Transport Mode?

   Im Transport-Modus (host-to-host) führen die Host eine IPSec Verschlüsselung ihrer eigenen Daten durch. Auf jedem Host muss eine IPSec Konfiguration vorgenommen werden.

   Im Tunnel-Modus (peer-to-peer) stellen die Gateways eine IPSec Verschlüsselung bereit.

7. Die folgenden Einstellungen werden wir an einem VPN Peer vornehmen. Erläutern Sie kurz die Begriffe und deren Aufgabe.

Peer-IP-Address	133.3.3.2	Remote-VPN-Server IP
Local Network	172.16.0.0/24	Eigene IP
Remote Network	10.0.0.0/24	Netzwerk welches Remote ist.
IKE (ISAKMP Policy)	Authentication: Pre-shared key „cisco“ Encryption: 3DES Hash: SHA D-H Group: 1 Lifetime: 86400	Internet Key Exchange (IKE) ist ein Protokoll zur Herstellung einer sicheren Verbindung. Es verwaltet und tauscht authentifiziertes Schlüsselmaterial aus.
IPsec	Encryption: 3DES Authentication: SHA PFS D-H Group: 1	Verschlüsselung für die Datenübertragung

3.6 Kontrollfragen

1. Was erzielt man mit dem Command nameif ?
   Definiert einen Namen für das Interface, welcher dann im GUI verwendet wird.

2. Was ist der Unterschied zwischen PAT und NAT?
   PAT: Port Address Translation, es wird die IP und der Port umgeschrieben.
   NAT: Network Address Translation, die IP-Adresse wird "übersetzt" (unabhängig des Ports)

   Port and Address Translation (PAT) oder Network Address Port Translation (NAPT) ist eine Technik, die in Computernetzwerken verwendet wird. Sie ist eine spezielle Form von NAT (1 zu n NAT). Dabei werden im Gegensatz zu NAT nicht nur die IP-Adressen, sondern auch Port-Nummern umgeschrieben. PAT wird eingesetzt, wenn mehrere private IP-Adressen aus einem LAN zu einer öffentlichen IP-Adresse übersetzt werden sollen.

4.4 Kontrollfragen

1. Wieso muss man die NAT Regel (any, any) der Grundkonfiguration in die 2. Position verschieben? Was geschieht wenn man Sie an der ersten Stelle belässt?
   Damit für der VPN Traffic kein NAT gemacht wird.

2. Wie behandelt ASA Luzern die IP-Pakete, welche nach Bern wollen? Erläutern Sie.
   Es wird kein NAT gemacht, die Pakete werden via IPSec verpackt und durch den Tunnel geschickt.

5.5 Kontrollfragen

1. Wieso wurde bei der Konfiguration von ASA Luzern (siehe Abb. 14) bei Remote Network anstatt Subnetz Bern, any eingetragen?
   Damit sämtlicher Traffic durch den VPN-Tunnel geschickt wird.

6.5 Kontrollfragen

1. Wäre es möglich auch ASA Luzern durch einen Router zu ersetzen? Wenn ja, erstellen Sie eine Konfiguration.
   Ja.

7.4 Kontrollfragen

1. Ist es möglich mehrere AnyConnect-Sessions bei einer ASA gleichzeitig zu betreiben? Wenn ja, wie viele?
   Ja, Default 10, kann auf 50 oder Unlimitiert mit zusätzlichen Lizenzen angepasst werden.

2. Wäre es möglich auch hier den ASA mit einem Router zu ersetzen?
   Nein.