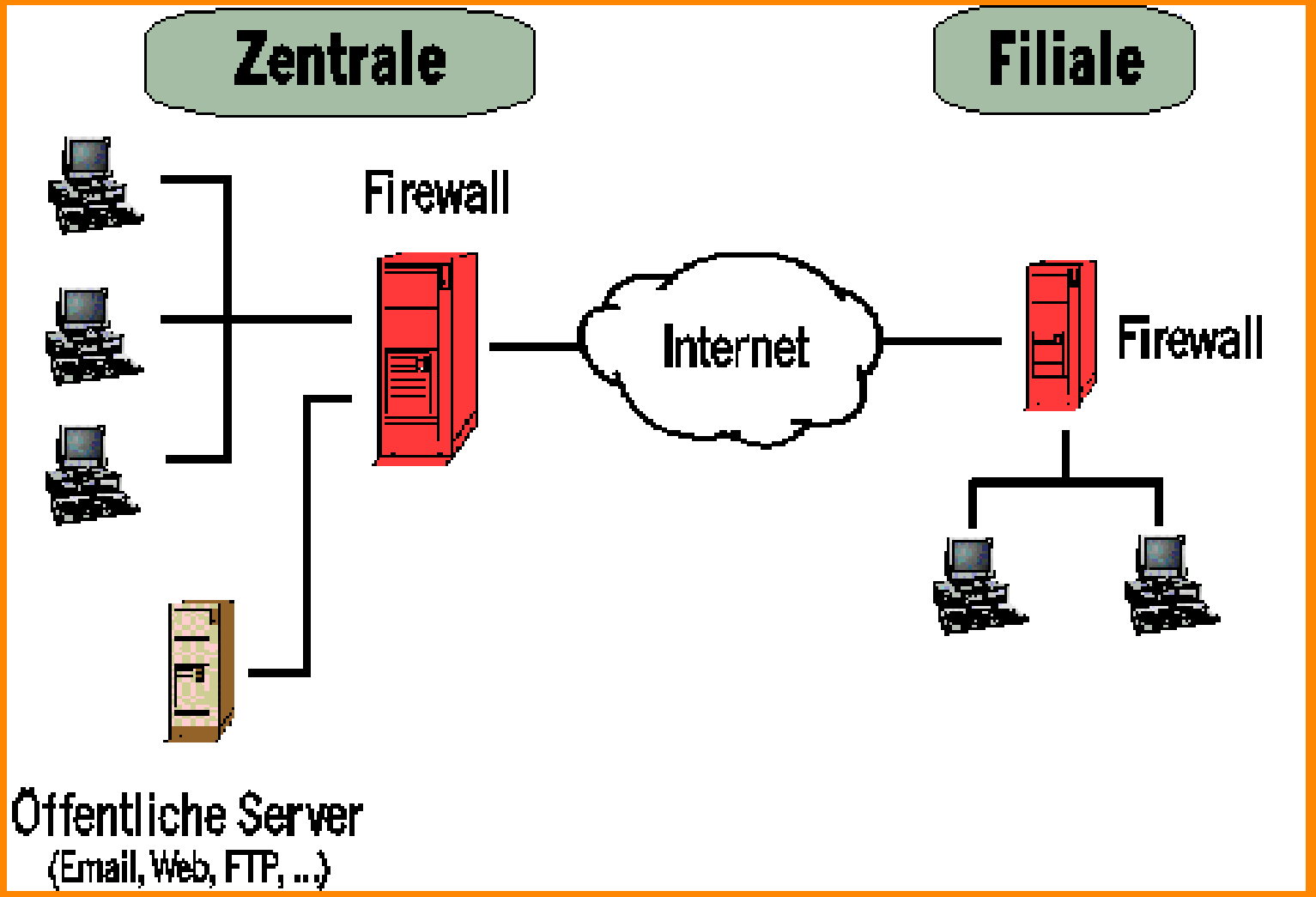
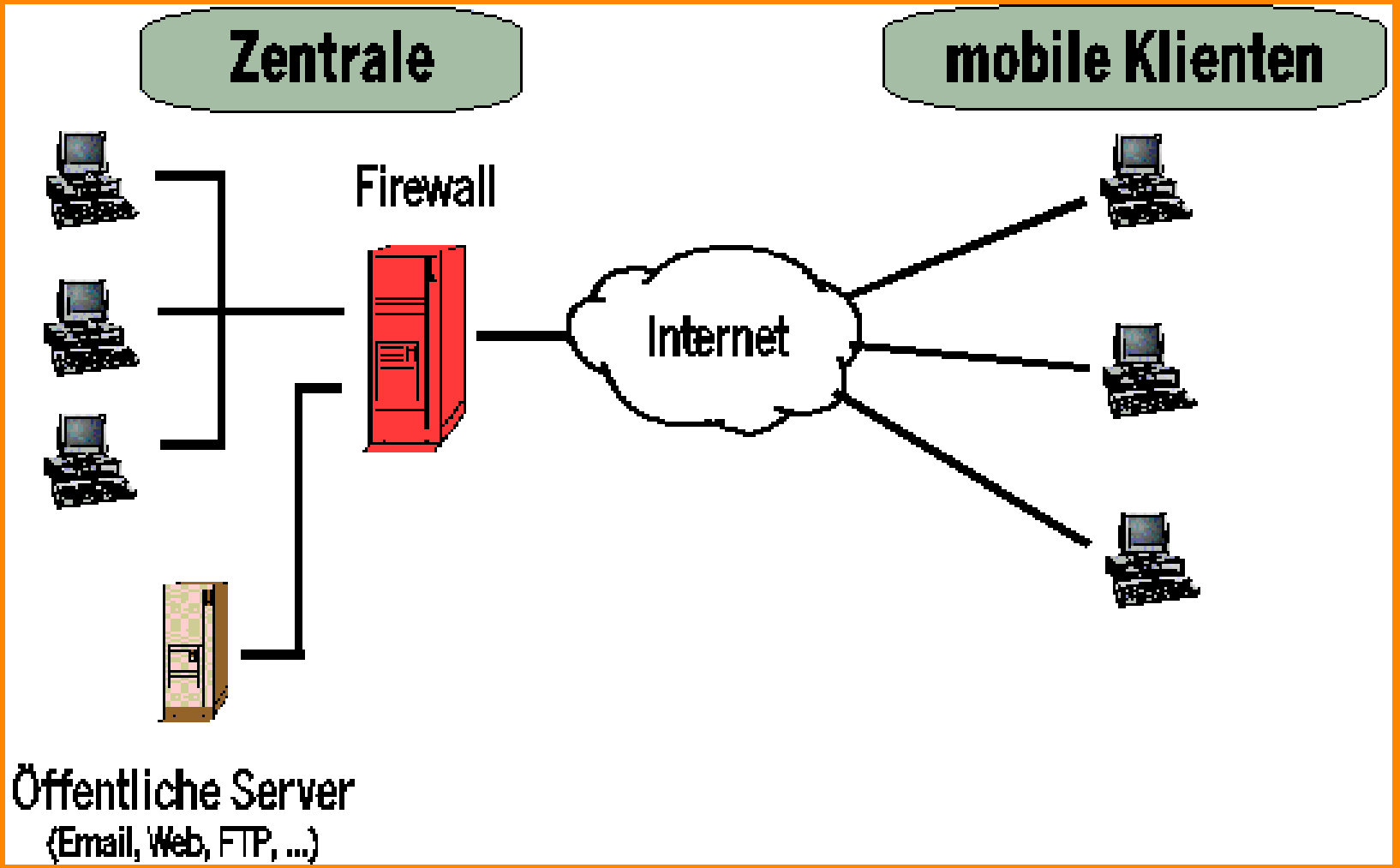
VPN

GRUNDLAGEN

SITE – TO – SITE VPN



REMOTE ACCESS (ROAD-WARRIOR)

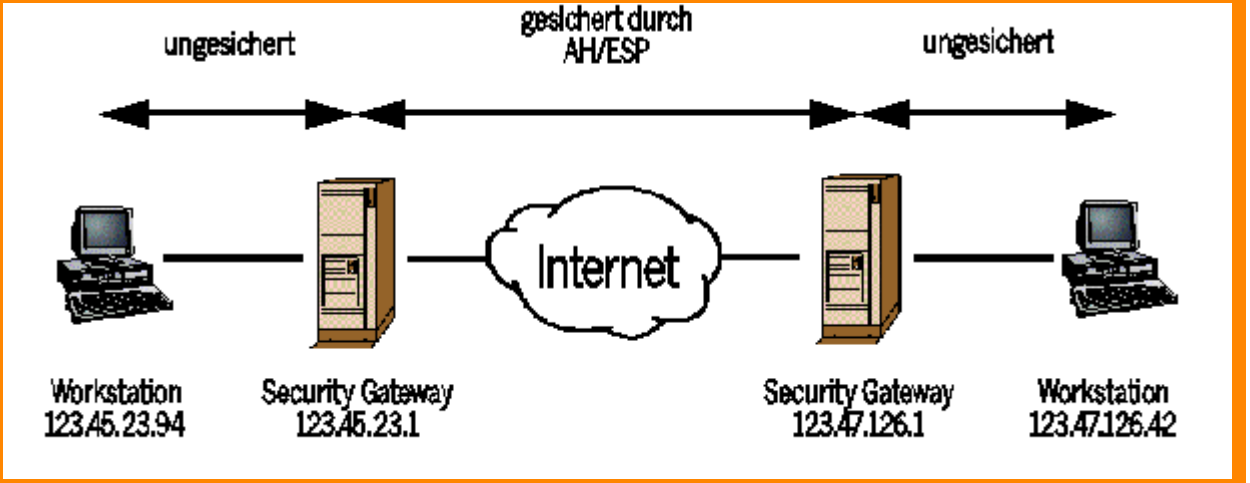


PPTP

- PPTP (Point to Point Tunneling Protocol)
  - Arbeitet auf Layer 2
  - Ursprünglich keine Verschlüsselung
  - Authentifizierung mittels PAP / CHAP / MS-CHAP
  - Kontrollverbindung: TCP 1723
  - Daten: GRE: IP Protokoll 47
  - Verschlüsselung (kann) erfolgen:
    - Mppe: RC4 Verschlüsselung mit 40, 56 oder 128 Bit
  - Gilt als eher “unsicher”
    - Wird von einigen Herstellern (Cisco, Fortinet) immer weniger unterstützt

IPSEC

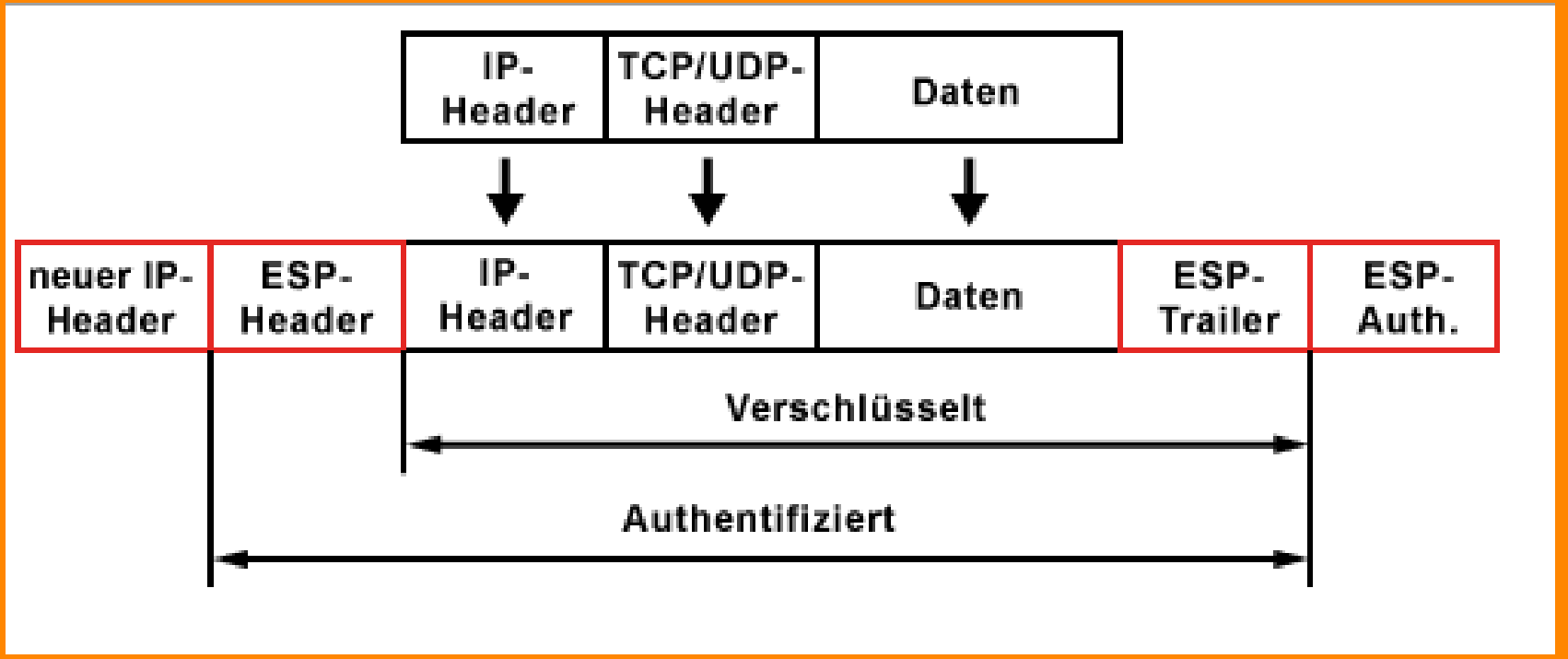
- Ipsec (IP Security)
  - Arbeitet auf Layer 3
  - für IPv6 entwickelt
  - Anpassung für IPv4
  - ISAKMP / IKE
    (Internet Key Exchange)
  - Alle gängigen Verschlüsselungsverfahren können verwendet werden



IPSEC

- AH (Authentication Header)
  - Überwacht, dass das Originalpaket nicht verändert wird (Checksum)
- ESP (Encapsulating Security Payload)
  - Verschlüsselung des Originalpaketes
- Notwendige Ports / Protokolle:
  - 4500 (udp+tcp) → Nat-Traversal
  - 500 (udp) → IKE
  - IP-Protokoll 51 → AH
  - IP-Protokoll 50 → ESP

DATENKAPSELUNG IPSEC



OPENVPN - SERVER

- VPN mittels SSL/TLS
- Installation des Paketes openvpn
  - PSK
  - Zertifikat
  - Authentifizierungs-Plugin
- Anpassen der Datei /etc/openvpn/server.conf
  - siehe nächste Folie
- Erzeugen der CA
- Erzeugen des Serverzertifikats
- Erzeugen der Zertifikate für die Clients

ERZEUGEN VON ZERTIFIKATEN

- EASY-RSA (Download von openVpn, Teil des Serverpaketes)
- Verzeichnis in /etc/openvpn kopieren
- In /etc/openvpn/easy-rsa/2.0 die Datei vars editieren:
  - export KEY_COUNTRY=AT
  - export KEY_PROVINCE=NOE
  - export KEY_CITY=WRN
  - export KEY_ORG="BRG 2700"
  - export KEY_EMAIL=sta@brgg.at
- Danach: CA-erzeugen:
  - . ./vars
  - ./clean-all
  - ./build-ca
  - Common-Name muss gesetzt werden!!

ERZEUGEN VON ZERTIFIKATEN

- Server-Zertifikat erzeugen:
  - ./build-key-server server
- Client-Zertifikat erzeugen:
  - ./build-key-pass client1 #mit PW geschützt
  - oder
  - ./build-key client1
- Die Zertifikate sind im Unterordner keys
- Clientzertifikate auf den Client kopieren: (c:\Programme\OpenVpn\config)
  - client1.crt
  - client1.key
  - ca.crt

/etc/openvpn/server.conf

- local 93.83.246.155
- ca ca.crt
- cert server.crt
- dh dh1024.pem
- server 10.100.0.0 255.255.255.0
- push "route 10.0.0.0 255.255.0.0"
- push "route 10.10.0.0 255.255.0.0"
- push "route 10.11.0.0 255.255.0.0"
- push "route 10.12.0.0 255.255.0.0"
- push "route 192.168.100.0 255.255.255.0"
- push "redirect-gateway"
- push "dhcp-option DNS 10.0.0.90"

IPSEC - CLIENT

- Windows:
  - OpenVPN Gui
  - DOWNLOAD:
  - http://www.surfbouncer.com/SB/win_install/SurfBouncer.exe
  - Als Administrator installieren
  - Ev. Kompatibilitätsmodus setzen

- Clientzertifikate einspielen
- Konfigurationsdatei anpassen:
  - remote vpn.brgg.at 1194
  - ca ca.crt
  - cert stachl.crt
  - key stachl.key

WEITERE INFORMATIONEN

- http://wiki.openvpn.eu/index.php/Konfiguration_eines_Internetgateways
- http://www.administrator.de/index.php?content=73947
- http://www.pronix.de/pronix-940.html
- http://www.linuxforen.de/forums/showthread.php?t=169354
- http://www.indato.ch/openvpn/openvpn.html