Remote Access

Segurança em Redes de Comunicações

Mestrado em Cibersegurança

Mestrado em Engenharia de Computadores e Telemática

DETI-UA

universidade de aveiro

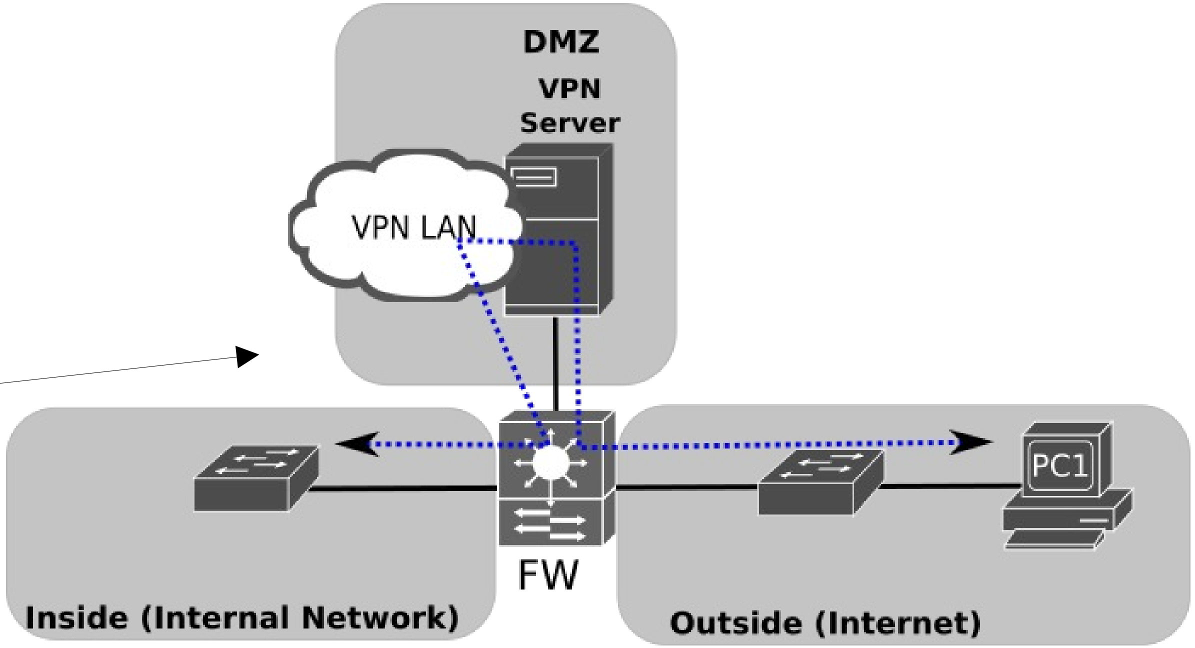
deti.ua.pt

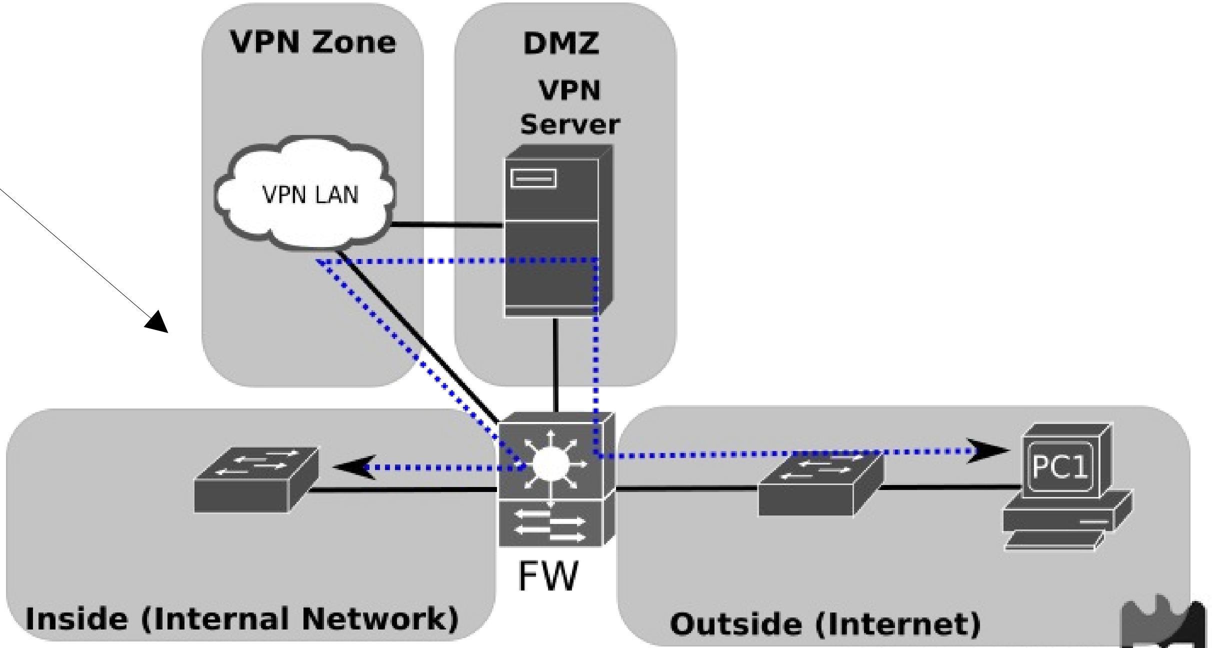
Remote Access (1)

- Most common servers/protocols
  - L2TP IPsec
    - IKE+ISAKMP+L2TP
  - OpenVPN
    - SSL
  - Proprietary
    - SSL or IPSec based.
- Authentication
  - Types
    - Pre-shared
    - RADIUS/LDAP
    - RSA with embedded CA
    - RSA with external CA
  - Certificates/Credentials must be distributed securely
    - Web service, SSH, ...

Remote Access (2)

- Server deployed in Firewalls.
- Server in DMZ.
    - Traffic routed back to the firewall using the same zone.
    - Traffic routed back to the firewall using the a different network interface and zone.
    - Traffic routed directly to private zone.
        - Breaks zone concept.





IPsec NAT Transversal

- NAT/PAT incompatibilities with IPsec
  - AH header incorporates the IP source and destination addresses in the keyed message integrity check. ESP is not an issue.
  - TCP and UDP checksums can be updated because are protected by IPsec.
  - IP addresses may be used as identifiers in Internet Key Exchange to determine credentials.
- During the ISAKMP IPsec first phase hosts (when configured and suported) detect that NAT transversal must be activated.
  - Subsequent ISAKMP first phase and second phase packets are encapsulated in UDP packets.
    - Usually port UDP 4500.
  - Original IP address are sent as NAT-OA (NAT Original Address) payloads of the ISAKMP.

Integration with Flow Control

- Service/protocol rules
  - OpenVPN
    - Used UDP port.
      - Usually port UDP 1194.
  - IPsec
    - UDP port 500 for IKE.
    - IP protocol number 50 (ESP).
      - IP protocol number 51 (AH).
    - UDP port 4500 for NAT traversal.
  - L2TP
    - UDP port 1701.
    - Exception may not be required when L2TP is encapsulated within IPsec packets.
- User flows’ rules
  - Remote users are assigned a IP network address.
  - Flow control based on IP address or zone.