UNIUNEA EUROPEANĂ

GUVERNUL ROMÂNIEI

Instrumente Structurale
2007-2013

Platformă de e-learning și curriculă e-content pentru învățământul superior tehnic

Securizarea rețelelor folosind sisteme dedicate

24. Implementarea sistemelor IPS

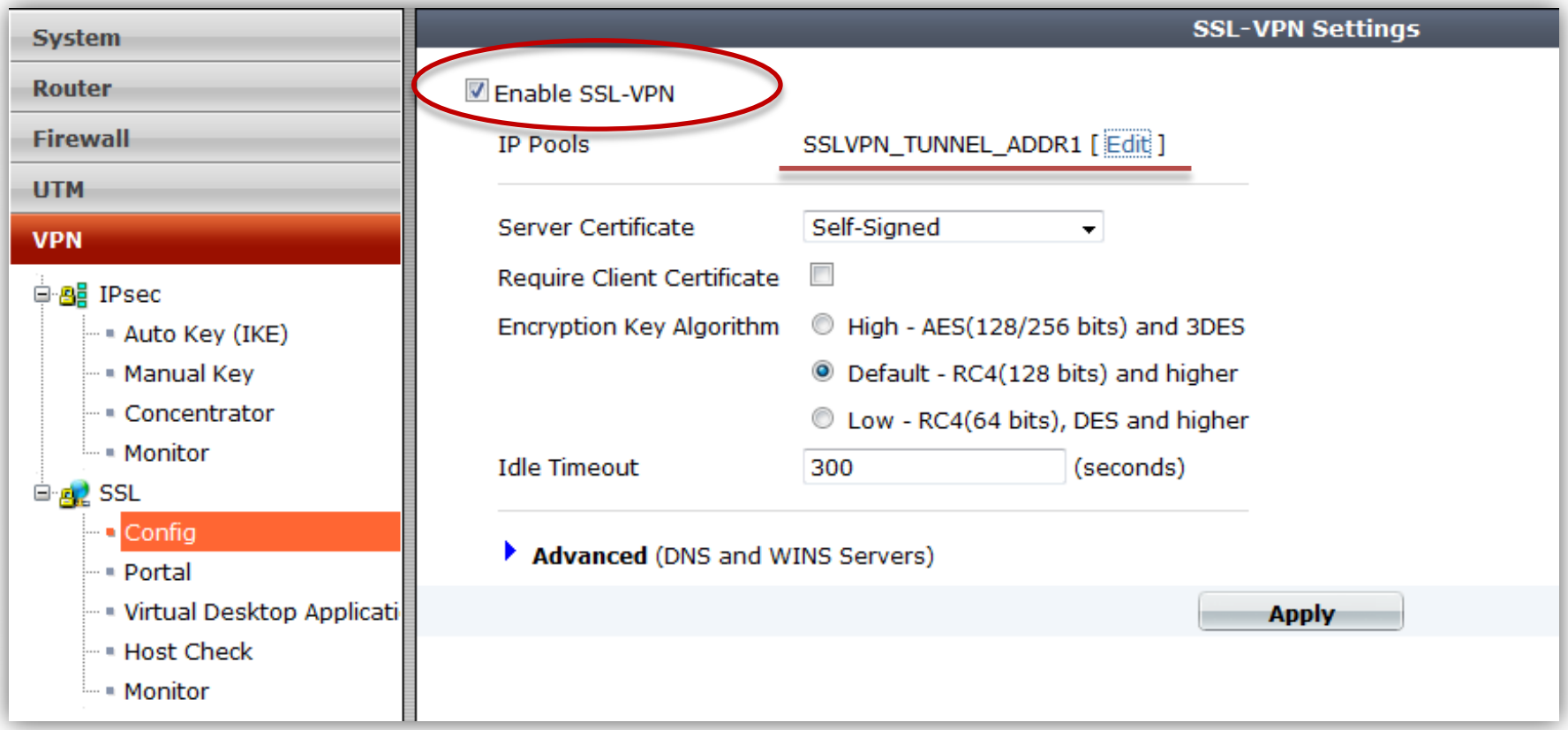
SSL VPN pe FortiOS 4.0 MR2

- Există 2 moduri de configurare a SSL VPN
  - Web-only mode
  - Tunnel mode
- Web – only mode
  - Nu are nevoie de client dedicat – folosește browserul
  - Partea de server are două componente: daemon SSL și portal VPN
  - Portalul VPN oferă după autentificare acces la HTTP/HTTPS pentru rețelele din spatele firewallului dar și la telnet, FTP, SMB/CIFS, VNC, RDP și SSH prin appleturi/widgeturi Java
  - Portalul vine cu template-uri default și poate fi personalizat de:
    - Administrator – schimbările vor fi vizibile de toți utilizatorii
    - Fiecare utilizator – schimbările vor fi locale pentru acel utilizator

Fortigate SSL VPN – tunnel mode

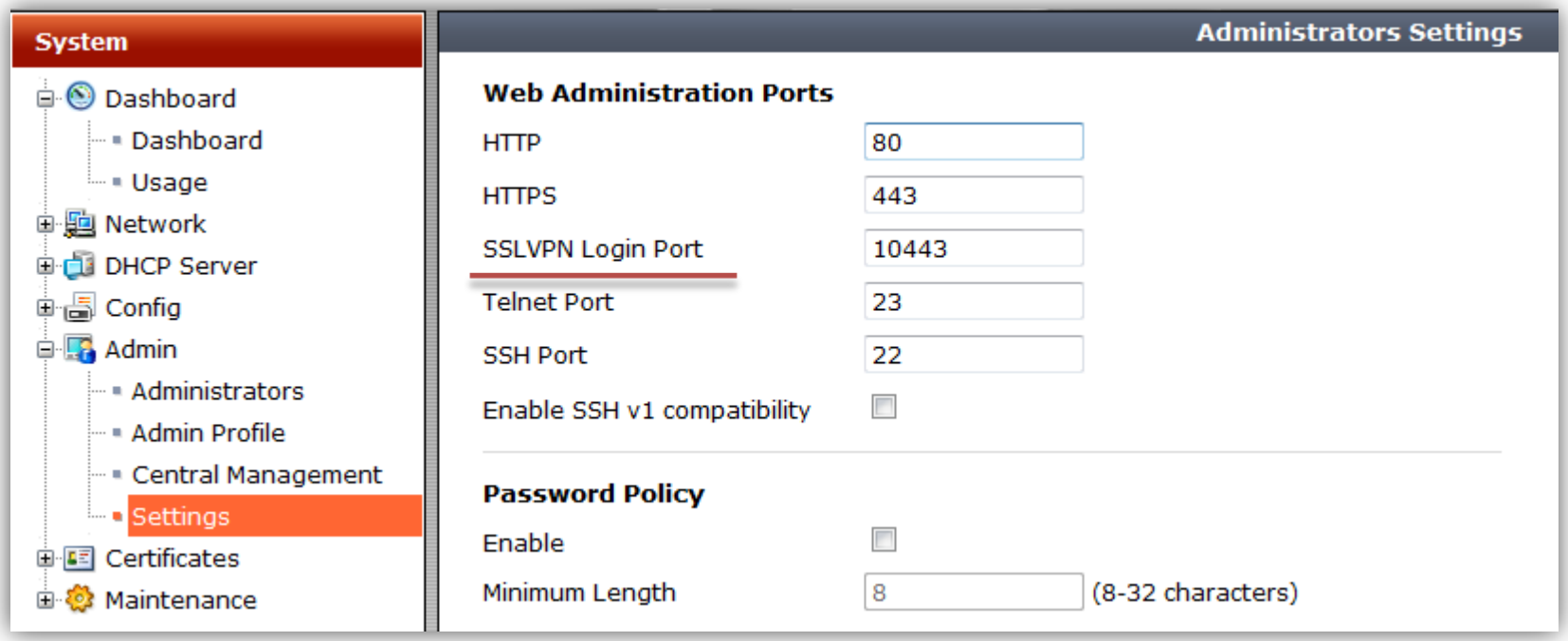
- Tunnel mode
  - Oferă acces complet la orice aplicație prin tunelul SSL VPN
  - În tunnel mode portalul VPN oferă un link către descărcarea kitului pentru client
  - Clientul este multi-platform (Windows/MAC OS/Linux)
  - Tunnel-mode suportă split-tunneling
    - Doar traficul către resursele interne ale companiei este trecut prin tunel
    - Traficul către Internet sau către alte resurse nesigure nu este trecut prin VPN
  - SSO: pe portalul WEB utilizatorul/adminul poate configura “Bookmarks” către rețelele interne ale companiei care să conțină și credențialele de autentificare

Configurarea SSL VPN



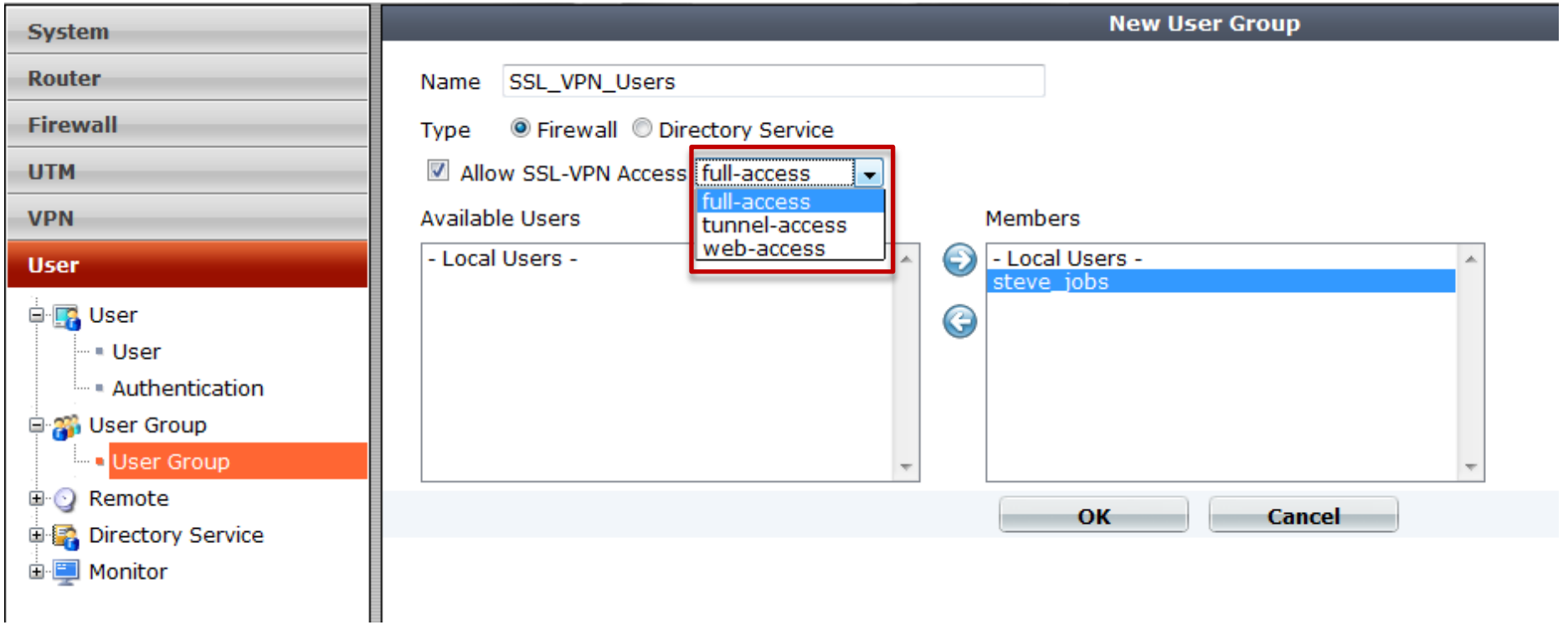
- Pasul 1: activare SSL VPN
- Se poate specifica un pool de adrese din care să se ofere adrese IP adaptorului de VPN de pe client

Configurarea SSL VPN



- Pasul 2: configurarea portului pentru tunelul de SSL
  - Implicit 10443
  - 443 este folosit implicit pentru administrare remote

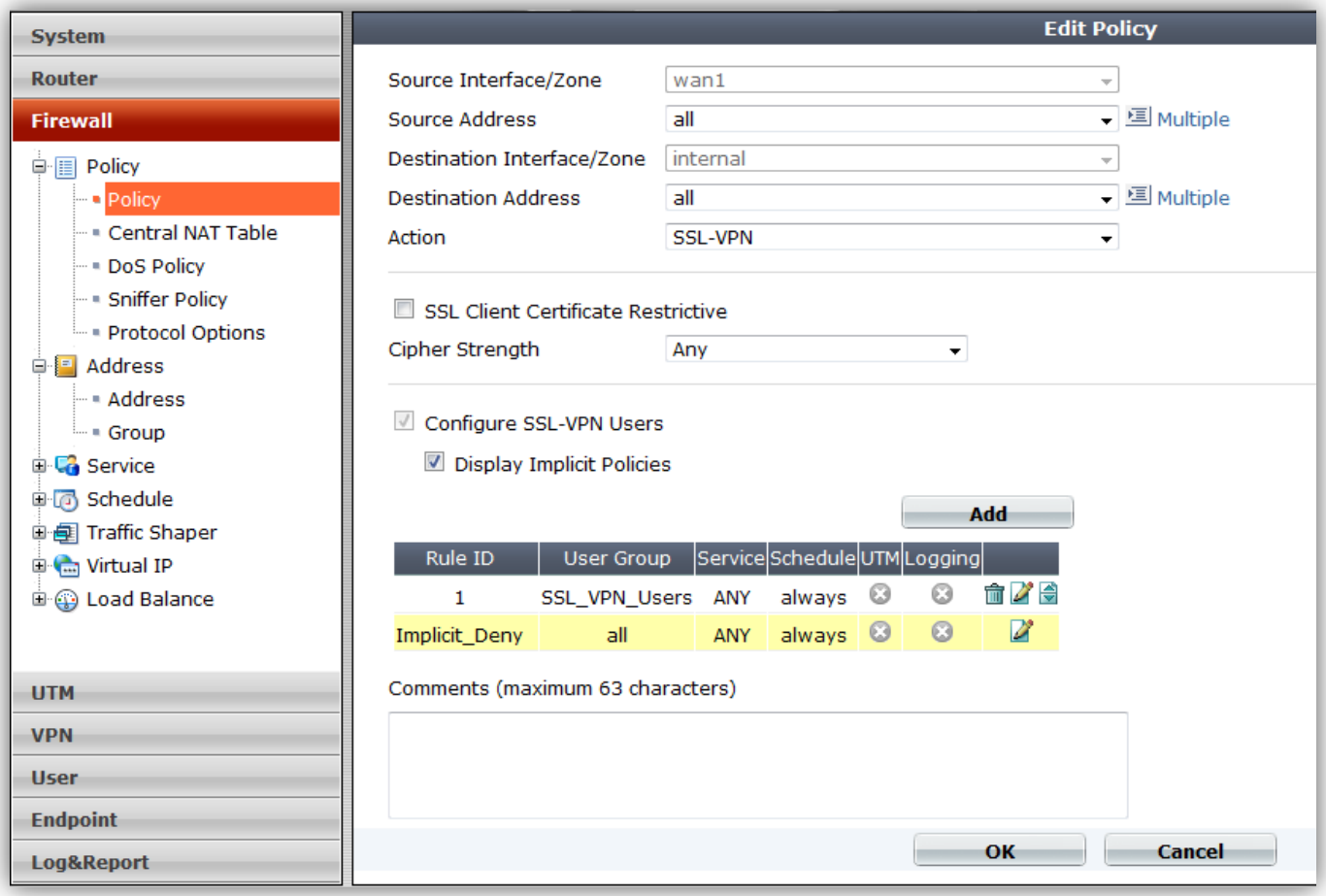
Configurarea utilizatorilor SSL VPN



- Pasul 3: configurarea unui utilizator și unui grup pentru VPN
- Trebuie specifica faptul că este un grup de tip SSL users și specificat tipul de acces oferit

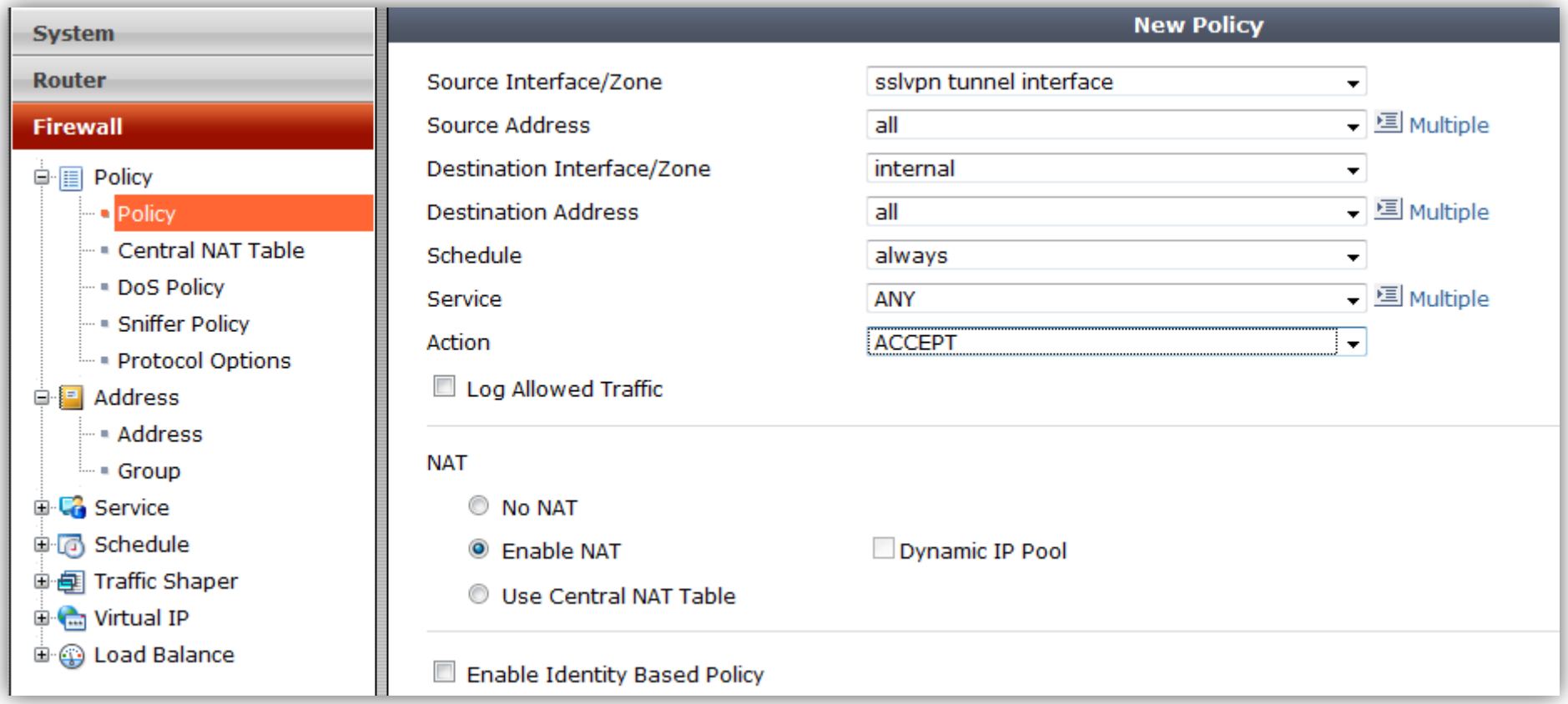
Configurarea politici de firewall – web vpn

- Pasul 4: pentru web-vpn e nevoie doar de o politică de la interfața “outside” la cea “inside” cu acțiunea SSL-VPN



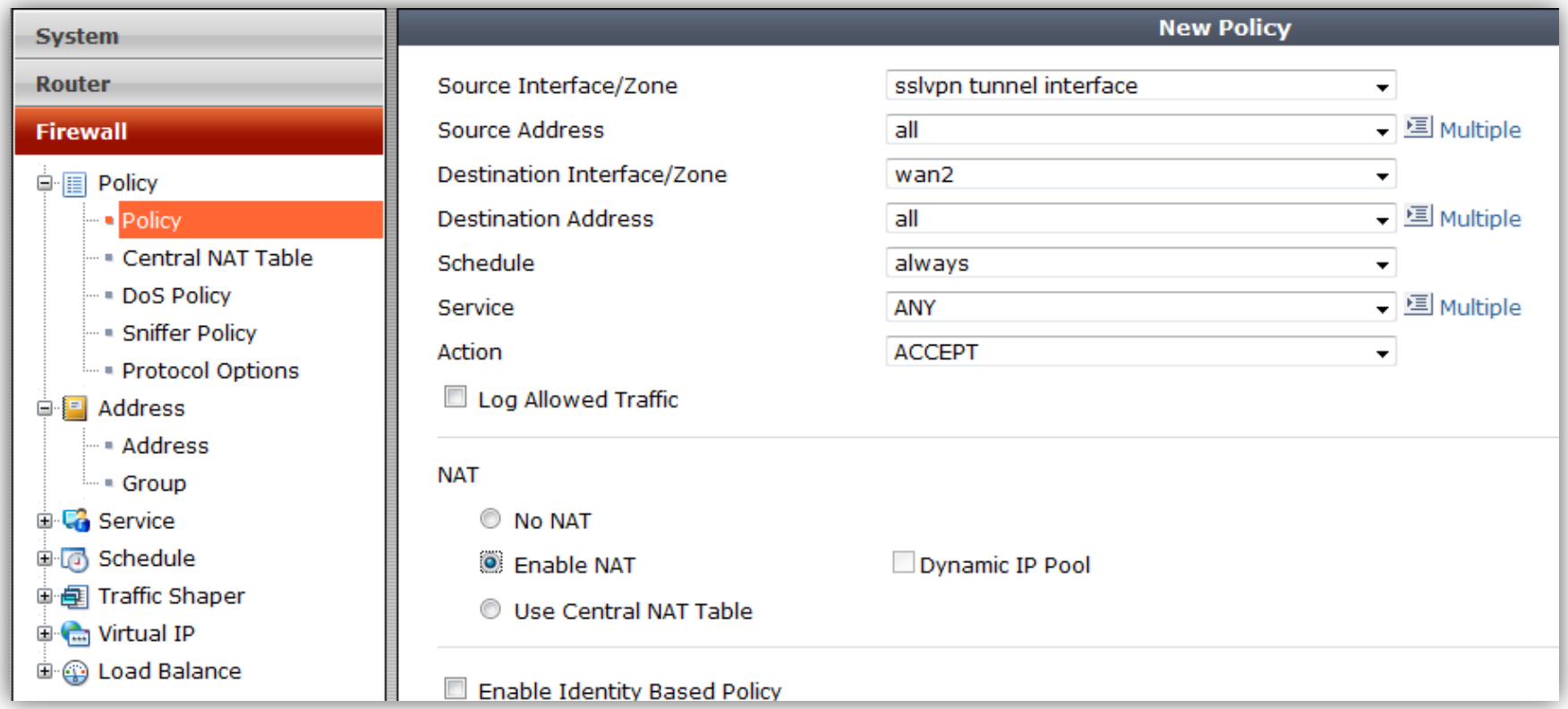
Configurarea politici de firewall – tunnel mode

- Pentru acces full prin modul tunnel, trebuie configurată o politică de intrarea în LAN

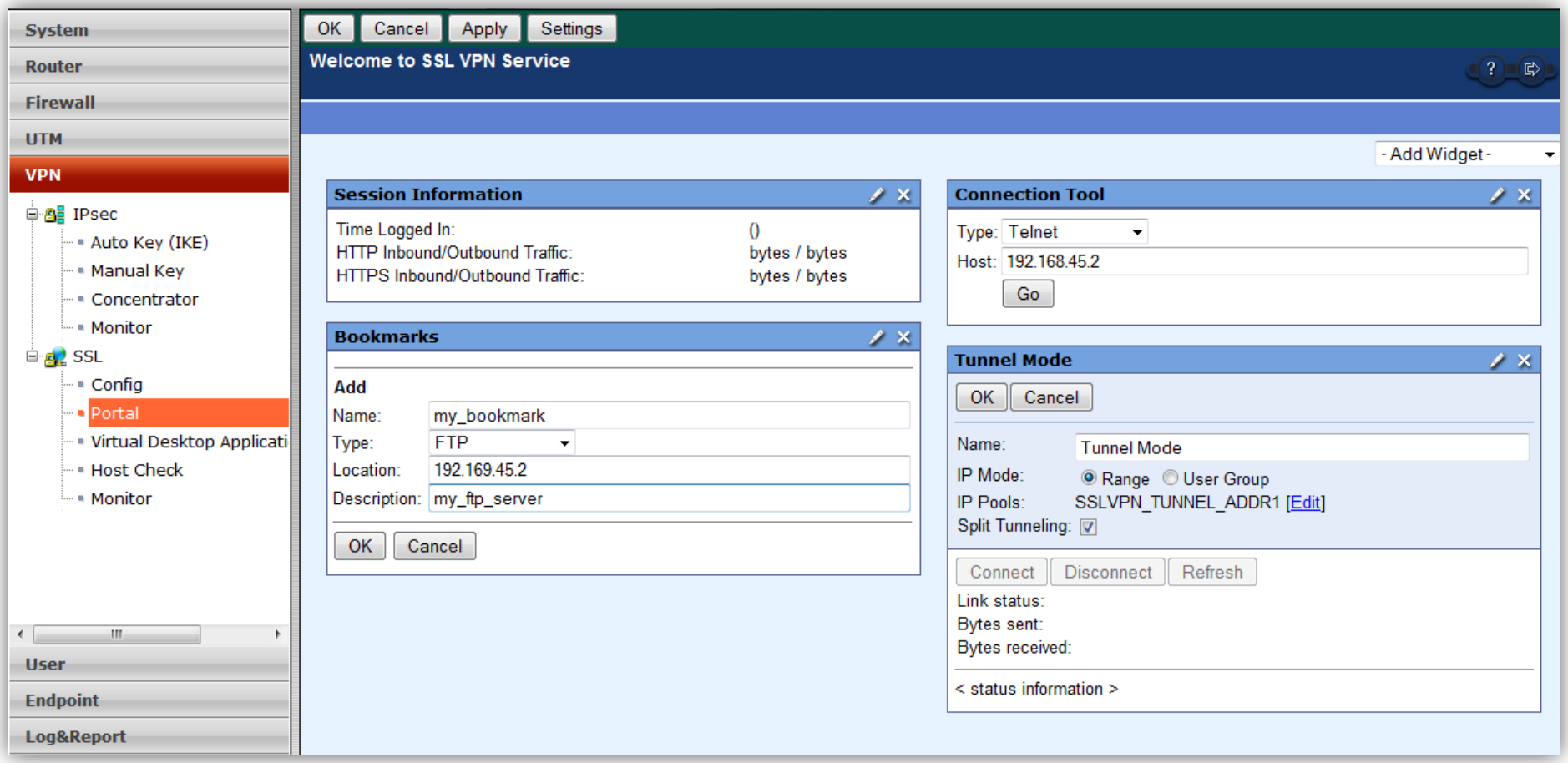


Internet browsing policy

- O topologie din ce în ce mai comună este cea în care utilizatorul se conectează prin VPN până la server și apoi iese în Internet în mod nesecurizat
- Este astfel protejat în rețeaua locală de orice atac

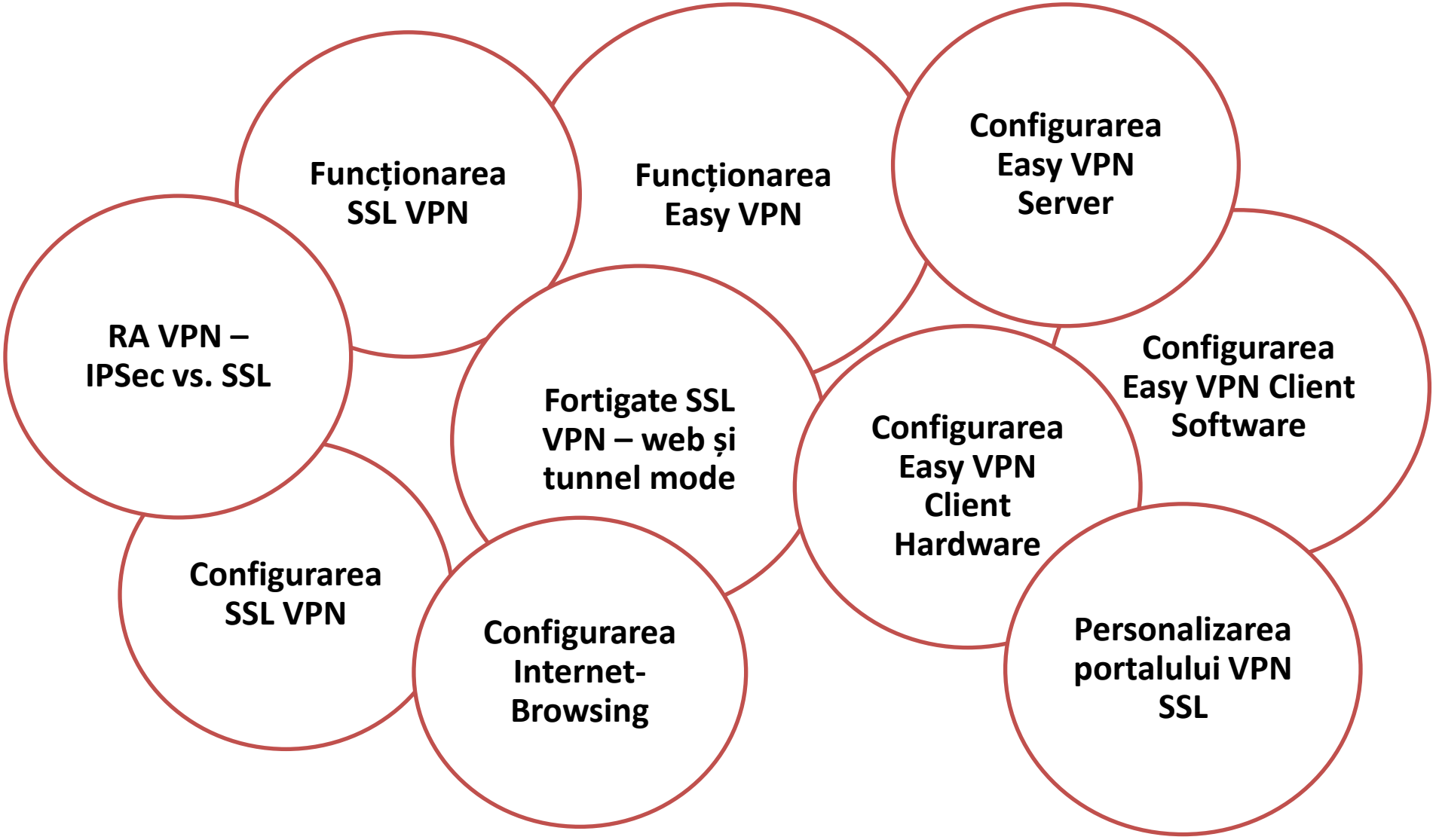


Personalizarea portalului VPN



- Personalizarea portalului: bookmarks, connection tools, session information, tunnel mode

Overview


Funcționarea SSL VPN
Funcționarea Easy VPN
Configurarea Easy VPN Server
RA VPN – IPSec vs. SSL
Fortigate SSL VPN – web și tunnel mode
Configurarea Easy VPN Client Software
Configurarea Easy VPN Client Hardware
Configurarea SSL VPN
Configurarea Internet-Browsing
Personalizarea portalului VPN SSL