



UNIUNEA EUROPEANĂ



GUVERNUL ROMÂNIEI



Instrumente Structurale  
2007-2013



# Platformă de e-learning și curriculum 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

The screenshot displays the 'SSL-VPN Settings' configuration page. On the left, a navigation menu shows 'VPN' selected, with 'Config' highlighted. The main content area features the following settings:

- Enable SSL-VPN (circled in red)
- IP Pools: SSLVPN\_TUNNEL\_ADDR1 [ [Edit](#) ]
- Server Certificate: Self-Signed
- Require Client Certificate:
- Encryption Key Algorithm:
  - High - AES(128/256 bits) and 3DES
  - Default - RC4(128 bits) and higher
  - Low - RC4(64 bits), DES and higher
- Idle Timeout: 300 (seconds)

At the bottom, there is an 'Advanced (DNS and WINS Servers)' section and an 'Apply' button.

- ▶ 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

The screenshot shows the Mikrotik Router configuration interface. On the left, the 'System' menu is expanded, with 'Settings' highlighted. On the right, the 'Administrators Settings' page is displayed. The 'Web Administration Ports' section is visible, with the following settings:

Port Name	Value
HTTP	80
HTTPS	443
<u>SSLVPN Login Port</u>	10443
Telnet Port	23
SSH Port	22

Below the 'Web Administration Ports' section, there is a 'Password Policy' section with the following settings:

Setting	Value
Enable	<input type="checkbox"/>
Minimum Length	8 (8-32 characters)

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

# Configurarea utilizatorilor SSL VPN

The screenshot displays the 'New User Group' configuration window. The 'Name' field is 'SSL\_VPN\_Users'. The 'Type' is 'Firewall'. The 'Allow SSL-VPN Access' checkbox is checked. A dropdown menu is open, showing three options: 'full-access', 'tunnel-access', and 'web-access'. The 'Members' list contains 'Local Users -' and 'steve\_jobs'. The 'OK' and 'Cancel' buttons are visible at the bottom.

- ▶ Pasul 3: configurarea unui utilizator și unui grup pentru VPN
- ▶ Trebuie specificat 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

**System**

**Router**

**Firewall**

- Policy
  - Policy
  - Central NAT Table
  - DoS Policy
  - Sniffer Policy
  - Protocol Options
- Address
  - Address
  - Group
- Service
- Schedule
- Traffic Shaper
- Virtual IP
- Load Balance

**UTM**

**VPN**

**User**

**Endpoint**

**Log&Report**

**Edit Policy**

Source Interface/Zone: wan1

Source Address: all Multiple

Destination Interface/Zone: internal

Destination Address: all Multiple

Action: SSL-VPN

SSL Client Certificate Restrictive

Cipher Strength: Any

Configure SSL-VPN Users

Display Implicit Policies

**Add**

Rule ID	User Group	Service	Schedule	UTM	Logging	
1	SSL_VPN_Users	ANY	always	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Implicit_Deny	all	ANY	always	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Comments (maximum 63 characters)

**OK** **Cancel**

# Configurarea politici de firewall – tunnel mode

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

The screenshot displays the Mikrotik WinBox interface for configuring a new firewall policy. The left sidebar shows the navigation tree with 'System' > 'Router' > 'Firewall' > 'Policy' selected. The main panel is titled 'New Policy' and contains the following configuration fields:

- Source Interface/Zone: sslvpn tunnel interface
- Source Address: all (Multiple)
- Destination Interface/Zone: internal
- Destination Address: all (Multiple)
- Schedule: always
- Service: ANY (Multiple)
- Action: ACCEPT
- Log Allowed Traffic

The NAT section is visible below the Action field:

- No NAT
- Enable NAT  Dynamic IP Pool
- Use Central NAT Table

At the bottom of the NAT section, there is an option:  Enable Identity Based Policy



# 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

The screenshot displays the Mikrotik WinBox interface for configuring a new Firewall Policy. The left sidebar shows the navigation tree with 'Firewall' selected and 'Policy' highlighted. The main area is titled 'New Policy' and contains the following configuration fields:

- Source Interface/Zone: sslvpn tunnel interface
- Source Address: all (Multiple)
- Destination Interface/Zone: wan2
- Destination Address: all (Multiple)
- Schedule: always
- Service: ANY (Multiple)
- Action: ACCEPT
- Log Allowed Traffic

The NAT section is visible below the main configuration:

- No NAT
- Enable NAT
  - Dynamic IP Pool
- Use Central NAT Table

At the bottom, there is an option  Enable Identity Based Policy.

# Personalizarea portalului VPN

The screenshot displays the 'Welcome to SSL VPN Service' configuration page. On the left, a navigation tree shows 'VPN' selected, with sub-items for IPsec and SSL. The 'SSL' section is expanded, and 'Portal' is highlighted. The main area contains several widgets:

- Session Information:** Shows 'Time Logged In: ()' and traffic statistics for HTTP and HTTPS.
- Bookmarks:** A form to add a bookmark with fields for Name (my\_bookmark), Type (FTP), Location (192.169.45.2), and Description (my\_ftp\_server).
- Connection Tool:** A form to configure connection parameters, including Type (Telnet) and Host (192.168.45.2).
- Tunnel Mode:** A form to configure tunnel settings, including Name (Tunnel Mode), IP Mode (Range selected), IP Pools (SSLVPN\_TUNNEL\_ADDR1), and Split Tunneling (checked).

Buttons for 'OK', 'Cancel', 'Apply', and 'Settings' are visible at the top of the main area.

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

# Overview

---

