



Advanced VPNs

24 aprilie 2014

Objective

- ▶ Soluții de remote access VPN
 - ❑ IPSec
 - ❑ SSL
- ▶ Cisco ASA
 - ❑ Easy VPN – soluție de remote-access IPSec VPN
- ▶ Fortinet
 - ❑ Implementarea SSL VPN
 - Web-VPN
 - Tunnel-VPN
 - Internet Browsing
 - Personalizarea portalului SSL VPN

Telecommuting

- ▶ Pentru multe companii, soluția de *telecommuting* este deseori preferată
 - ❑ Angajatul locuiește departe de sediu și timpul petrecut pe drum este foarte mare
 - ❑ Tipul de job presupune mult timp petrecut călătorind
 - ❑ Lucrul de acasă - multe studii arată că angajatul care își poate permite un somn de după-masă de 1h, este mult mai eficient în a doua parte a zilei de muncă



Remote access VPN

- ▶ Telecommuting este totuși o soluție pentru o minoritate din angajați pentru că există dezavantaje:
 - ❑ Lucrând acasă angajații pot fi distrași mai ușor decât într-un mediu de muncă comun
 - În general joburile ce presupun creativitate au mari avantaje în telecommuting
 - ❑ Riscurile de securitate de a trece date sensibile pentru companie peste o rețea publică sunt mari

- ▶ Remote access VPN

- ❑ IPSec
- ❑ SSL



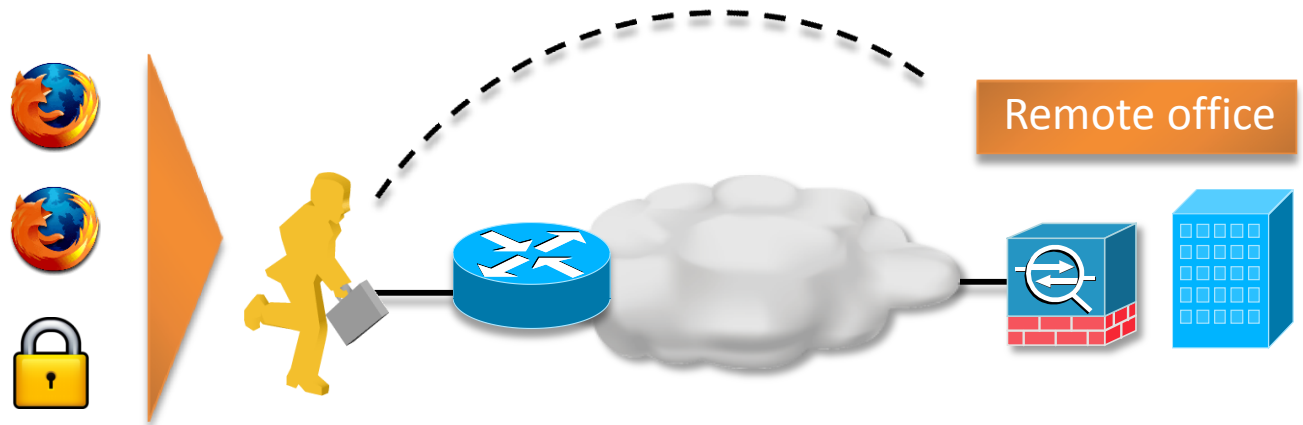
IPSec vs SSL

	IPSec	SSL
Aplicații	Orice aplicație IP based	WEB, e-mail, file sharing în modul nativ (clientless)
Putere de criptare	Puternică – chei de la 56 la 256 biți	Moderată – chei de la 40 la 128 de biți
Autentificare	Puternică – two-way authentication	Moderată – one-way sau two-way authentication
Ușurință în utilizare	Moderată – poate fi provocator pentru un utilizator non-tehnic	Foarte ușoară
Variante de conectare	Este nevoie de un client dedicat pre-configurat	Nu e nevoie de client specializat. Browserul este clientul.

- ▶ Ca și soluții de RA, cele două nu se exclud
 - ❑ IPSec = securitate
 - ❑ SSL = mobilitate, flexibilitate

SSL VPN

- ▶ Arhitectura SSL VPN presupune:
 - ❑ Serverul SSL VPN care se află la locația companiei
 - ❑ Clientul SSL VPN care se află întotdeauna la utilizator
- ▶ Clientul SSL VPN are 3 moduri de funcționare
 - ❑ Clientless
 - ❑ Thin client
 - ❑ Full client



Thin client/clientless

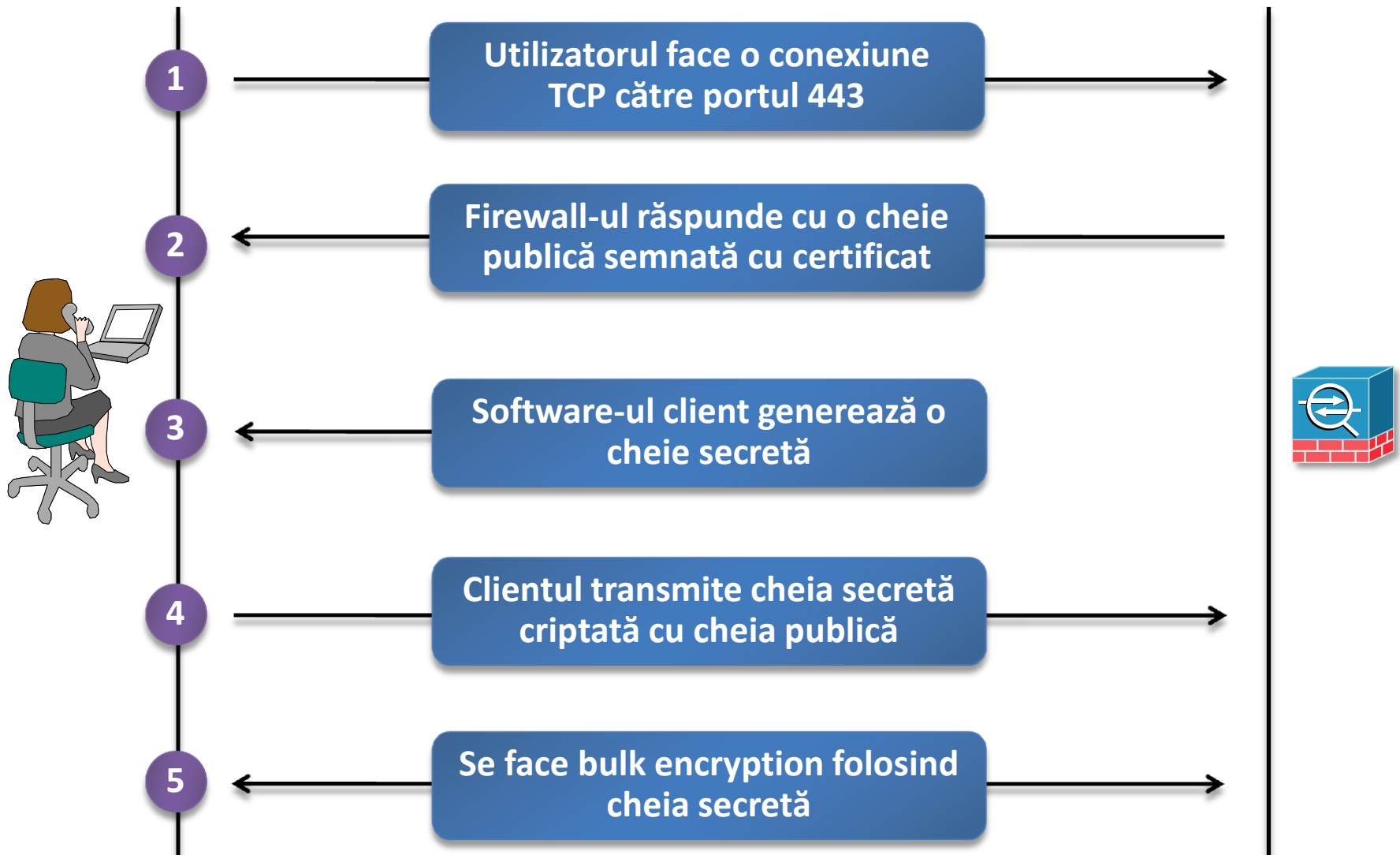
- ▶ Pentru ambele moduri clientul este browserul
- ▶ Clientless nu permite în general decât aplicații HTTP/HTTPS folosind un portal WEB
 - ❑ Utilizatorul se autentifică pe portalul WEB pentru a primi acces la resursele interne
- ▶ Thin client
 - ❑ În acest mod utilizatorul descarcă Applet-uri Java din portatul WEB
 - ❑ Applet-ul se comportă ca un TCP Proxy pentru anumite aplicații
 - ❑ Utilizatorul se conectează la o aplicație suportată de TCP Proxy (POP3, SMTP, IMAP, Telnet, SSH, CIFS)
 - ❑ TCP Proxy realizează o conexiune HTTPS la serverul SSL care conține în interiorul ei numele și portul serverului
 - ❑ Serverul SSL realizează conexiunea către serverul destinație



Full client

- ▶ Varianta de full-client poate fi de obicei descărcată de pe portalul WEB creat de serverul VPN
- ▶ Depinzând de vendor, clientul se poate instala dinamic, fără intervenția utilizatorului sau poate fi instalat ca o aplicație de sine stătătoare obișnuită
 - ❑ Varianta instalată automat se comportă tot ca un proxy dar este mai puțin configurabilă
 - ❑ Varianta instalată manual permite un grad de control al setărilor mai mare
- ▶ Ambele variante de instalare oferă acces la orice aplicație prin tunelul SSL

Stabilirea unui tunel SSL VPN





Cisco ASA – Implementarea IPSec VPN

Easy VPN Server/Client

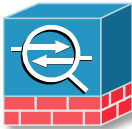
- ▶ Cisco folosește o arhitectură client server numită **Easy VPN**
- ▶ Atât parametrii de rețea (IP, DNS etc) cât și politicile IPSec sunt “pushed” de către server la clientul VPN
- ▶ Clientul Easy VPN poate fi:
 - ❑ Software – VPN client instalat pe laptopul utilizatorului
 - ❑ Hardware – ruter cu IOS, PIX Firewall, VPN 3002 Concentrator
- ▶ Folosind un client hardware se simplifică foarte mult configurația Site-to-Site pentru că nu mai trebuie sincronizați parametrii între cele două locații



Easy VPN – Pasul 1



Authentication mode?



- ▶ Pasul 1: funcție de metoda de autentificare folosită se alege tipul IKE Phase 1
 - ❑ Autentificare PSK > Aggressive mode
 - ❑ Autentificare RSA > Main mode
- ▶ Este recomandată folosirea certificatelor deoarece aggressive mode este mai puțin securizat

Easy VPN – Pasul 2: ISAKMP

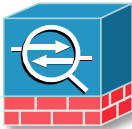
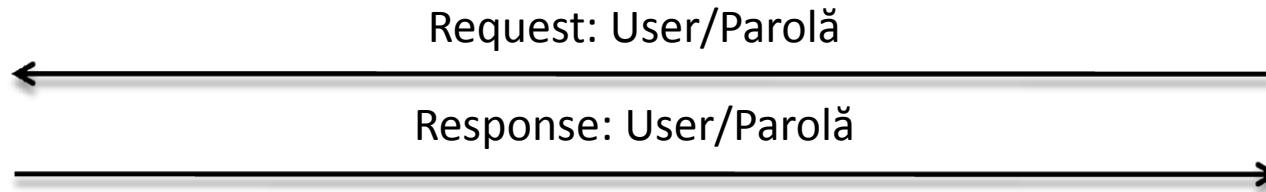


propunerea 1, propunerea 2, propunerea 3



- ▶ În pasul 2 Cisco VPN client încearcă să stabilească un SA ISAKMP prin trimiterea de propuneri către server
- ▶ Pentru a reduce cantitatea de configurație manuală, pe VPN Client sunt deja definite toate combinațiile de:
 - ❑ Algoritmi de criptare și hashing
 - ❑ Metode de autentificare
 - ❑ Grupuri DH
- ▶ ASA va accepta prima propunere care face match în ordinea priorităților
- ▶ Trebuie configurată pe client cheia partajată

Easy VPN – Pasul 2: XAUTH



- ▶ În pasul XAUTH, utilizatorul este autentificat
- ▶ Parola și numele de utilizator sunt definite în clientul de VPN
- ▶ Credențialele sunt verificate de ASA local sau remote (RADIUS, Kerberos etc.)
- ▶ Acest transfer este protejat de tunelul ISAKMP creat anterior

Easy VPN – Pasul 3: Mode configuration



Clientul face o cerere pentru parametrii de configurație



Parametrii sunt oferți de ASA



- ▶ Dacă autentificare a avut loc cu succes, parametrii de configurație necesari pentru conectivitate sunt ceruți de client
- ▶ Deși se pot configura multipli parametrii (IP, DNS, split tunneling etc) singurul parametru obligatoriu este adresa IP

Easy VPN – Pasul 3: IKE Quick mode



- ▶ Odată ce conectivitatea L3 este realizată peste IP-ul adaptorului clientului, se pornește IKE Phase 2
- ▶ Politicile IPsec sunt “pushed” de la ASA la clientul VPN
- ▶ După crearea SA-urilor din Phase 2, poate începe transferul de trafic conform acestora

Configurarea Easy VPN server

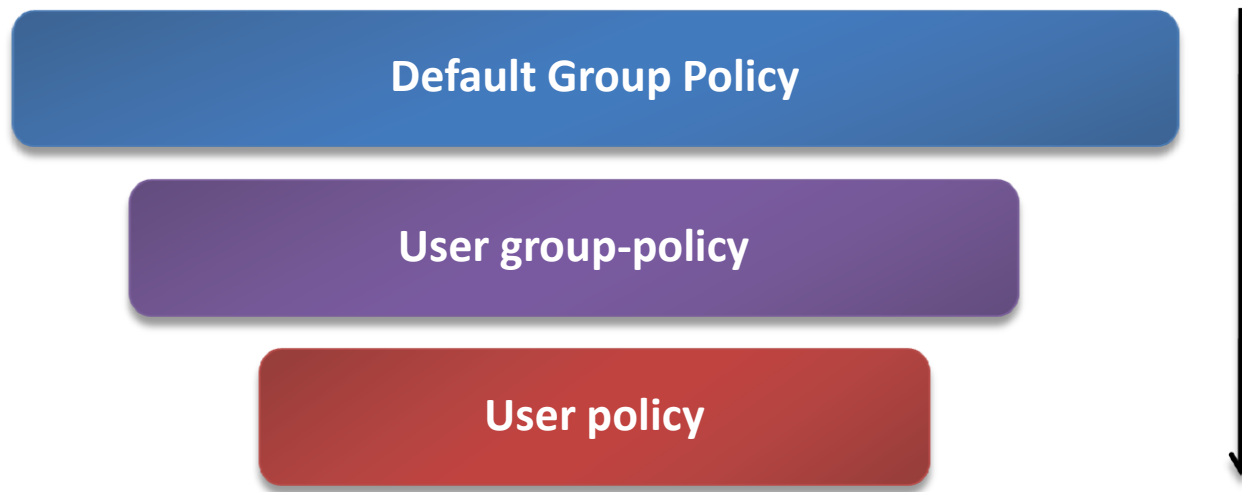


► Activarea ISAKMP și definirea unei politici

```
Pitesti(config)# isakmp enable outside
Pitesti(config)# isakmp policy 20
Pitesti(config-isakmp-policy)# authentication pre-share
Pitesti(config-isakmp-policy)# encryption des
Pitesti(config-isakmp-policy)# hash sha
Pitesti(config-isakmp-policy)# group 2
```

Definirea Remote-Access attributes

- ▶ Configurarea parametrilor de mode-config se poate face pe ASA la 3 nivele



- ▶ Este un model de moștenire (orice parametru definit la un nivel superior este moștenit la un nivel inferior)
- ▶ Parametrii definiți la nivel inferior sunt prioritari celor definiți la nivel superior

Definirea Remote-Access attributes



- ▶ Orice group-policy poate fi:
 - ❑ Internal – attributele politicii sunt definite local
 - ❑ External – attributele politicii sunt definite pe un RADIUS
- ▶ **DfltGrpPolicy** este un nume rezervat ce reprezintă Default Group Policy (cel mai înalt nivel de moștenire) și e în mod implicit internă

```
Pitesti(config)# group-policy DfltGrpPolicy attributes
Pitesti(config-group-policy)# vpn-simultaneous-logins 3
Pitesti(config-group-policy)# ip-comp enable
```

Definirea Remote-Access attributes

- ▶ Definirea unui group-policy de tip *internal*

```
Pitesti(config)# group-policy MSSR internal
Pitesti(config)# group-policy MSSR attributes
Pitesti(config-group-policy)# default-domain value
securemeinc.com
```

- ▶ Definirea user-policy se face după definirea unui utilizator

```
Pitesti(config)# username ciscouser password cisco123
Pitesti(config)# username ciscouser attributes
```

Definirea Remote-Access attributes

- ▶ La nivel de user-policy se pot defini attribute care vor avea cea mai mare prioritate: adresă IP, ACL etc.
- ▶ În exemplul de mai jos adaptorul clientului VPN primește
 - ❑ Adresa IP 192.168.50.1
 - ❑ ACL-ul 102 care restricționează ce fel de trafic se poate face prin VPN

```
Pitesti(config)# username ciscouser password cisco123
Pitesti(config)# username ciscouser attributes
Pitesti(config-username)# vpn-group-policy SecureMeGrp
Pitesti(config-username)# vpn-framed-ip-address 192.168.50.1
255.255.255.255
Pitesti(config-username)# vpn-filter value 102
```

Configurarea tipului de tunel și PSK



- ▶ Trebuie configurat tipul `ipsec-ra`

```
Pitesti(config)# tunnel-group ciscovpn type ?
  ipsec-121 IPSec Site to Site group
  ipsec-ra IPSec Remote Access group
Pitesti(config)# tunnel-group ciscovpn type ipsec-ra
Pitesti(config)# tunnel-group ciscovpn ipsec-attributes
Pitesti(config-ipsec)# pre-shared-key cisco123
```

- ▶ Atenție: numele grupului trebuie să fie configurat la fel pe VPN Client

Definirea utilizatorilor și tip de autentificare



- ▶ Tipul de autentificare este configurat pentru a folosi baza de date locală

```
Pitesti# configure terminal
Pitesti(config)# username ciscouser password cisco1
Pitesti(config)# username adminuser password cisco2
Pitesti(config)# tunnel-group ciscovpn general-attributes
Pitesti(config-group-policy)# authentication-server-group LOCAL
```

Definirea unui pool de adrese local



- ▶ Serverul poate oferi adrese clientului VPN în 3 moduri
 - ❑ Local
 - Printr-o definire statică în user-policy care ia mereu precedență
 - Printr-un pool definit în general-attributes la un grup
 - ❑ Dintr-un pool definit pe un server RADIUS
 - ❑ Prin trecerea cererii printr-un proxy către un server DHCP

```
Chicago(config)# vpn-addr-assign ?  
aaa      Allow AAA servers to specify an IP address  
dhcp     Allow DHCP servers to specify an IP address  
local    Allow local pools to specify an IP address
```


Asignarea unei adrese IP

- ▶ Asignarea se poate face static la nivel de user-policy

```
Pitesti(config)# username ciscouser attributes
Pitesti(config-username)# vpn-framed-ip-address 192.168.50.1
```

- ▶ Sau local prin definirea unui pool

```
Pitesti(config)# ip local pool vpnpool 192.168.50.2-
192.168.50.199
Pitesti(config)# tunnel-group ciscovpn general-attributes
Pitesti(config-general)# address-pool vpnpool
```

- ▶ Sau prin proxy către DHCP

```
Pitesti(config)# vpn-addr-assign dhcp
Pitesti(config)# tunnel-group ciscovpn general-attributes
Pitesti(config-general)# dhcp-server 192.168.10.10
```

Definirea transform-setului și unui dynamic crypto-map

► Definirea transform-setului

```
Pitesti(config)# crypto ipsec transform-set myset esp-aes-256 esp-sha-hmac
```

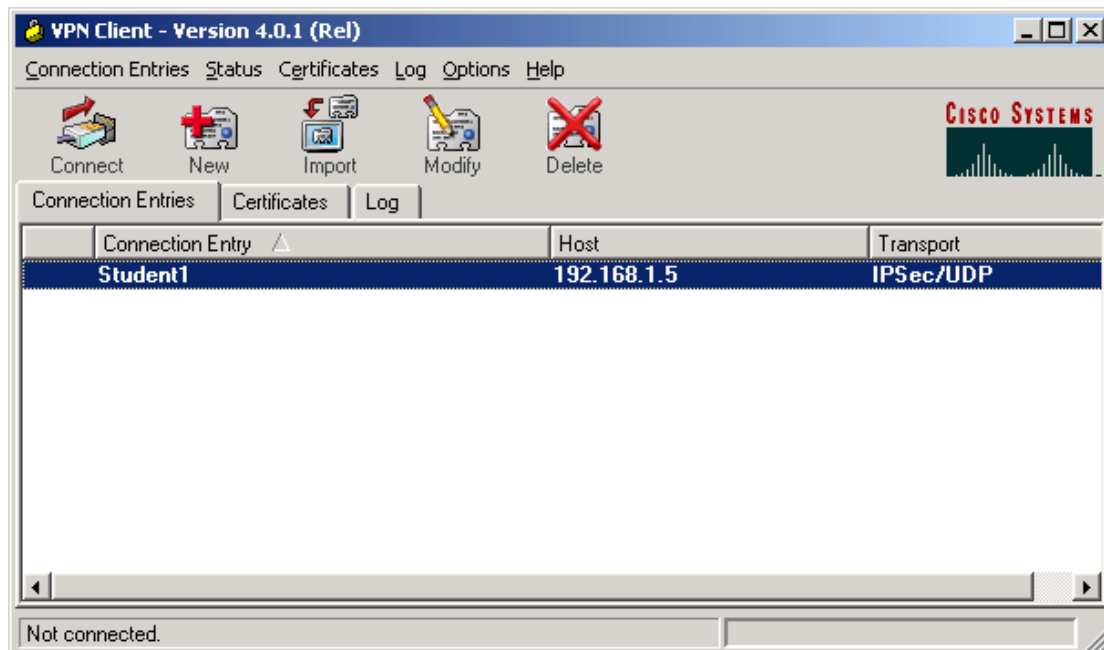
► Se folosește un crypto-map dinamic

- ❑ Motivul este că mulți ISP oferă IP-uri dinamice
- ❑ Într-un crypto-map peer-ul trebuie definit static astfel încât trebuie introdusă altă structură de date
- ❑ Transform set-ul este legat în dynamic crypto-map
- ❑ Dynamic crypto-mapul va fi legat de crypto-map-ul obișnuit

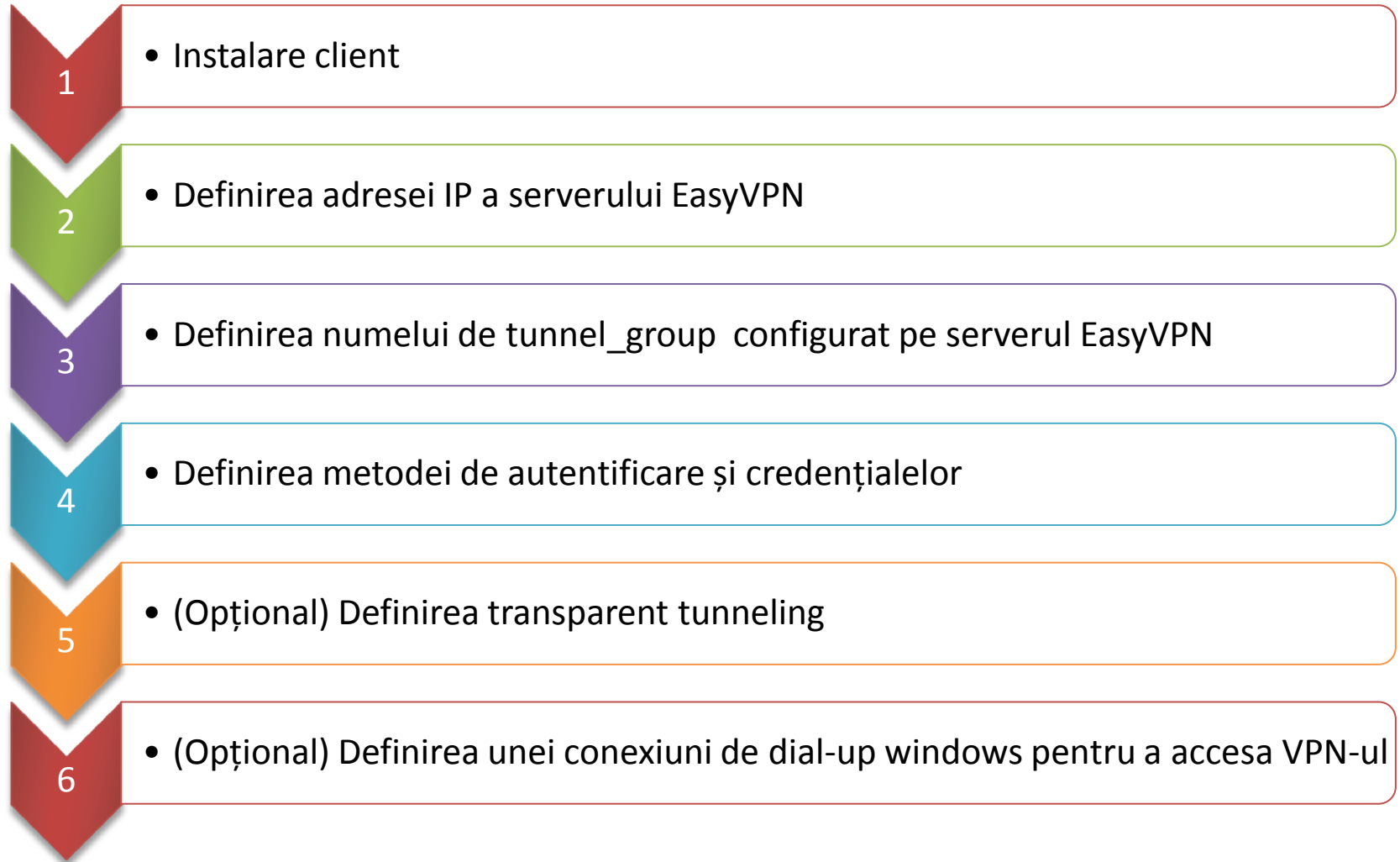
```
# definirea crypto-mapului dinamic
Pitesti(config)# crypto dynamic-map dynmap 10 set transform-set myset
# definirea crypto-mapului static și asocierea cu cel dinamic
Pitesti(config)# crypto map IPsec_map 65535 ipsec-isakmp dynamic dynmap
# aplicarea crypto-mapului static pe interfață
Pitesti(config)# crypto map IPsec_map interface outside
```

Clienți Cisco - VPN

- ▶ Există 2 tipuri de clienți Cisco VPN
 - ❑ Software – client ce se instalează în OS
 - ❑ Hardware – IOS/PIX/VPN 3002 Concentrator
 - <http://www.cisco.com/go/easyvpn>
- ▶ Versiune pentru Windows(x86, x64)/Linux/MacOS



Configurarea Cisco VPN Client



Crearea unei noi conexiuni

VPN Client | Create New VPN Connection Entry

Connection Entry: Bean Town Sales Office

Description: Boston Sales Office

Host: 192.168.0.5

Authentication | Transport | Backup Servers | Dial-Up

Group Authentication Mutual Group Authentication

Name: account_managers

Password: *****

Confirm Password: *****

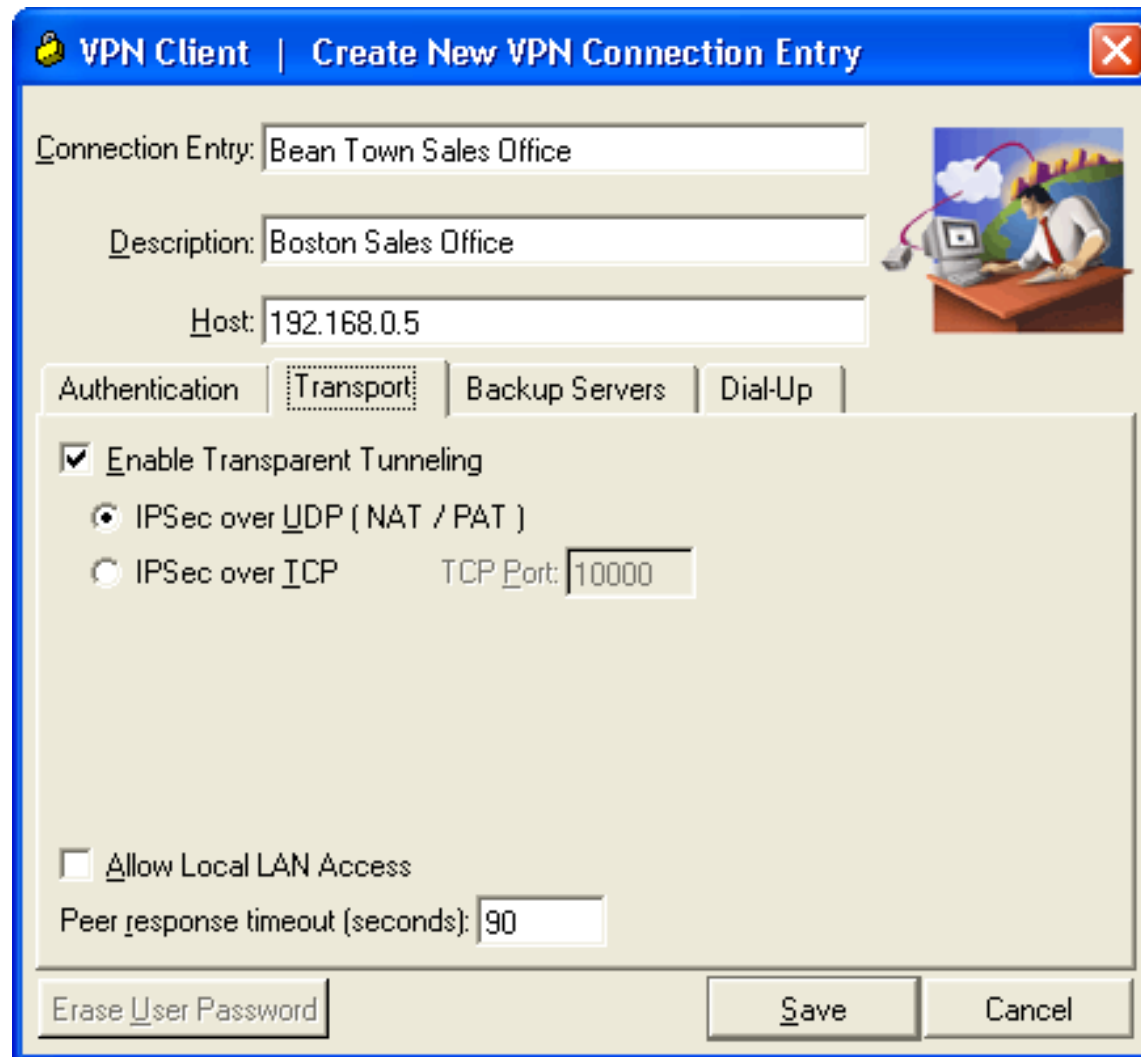
Certificate Authentication

Name: []

Send CA Certificate Chain

Erase User Password | Save | Cancel

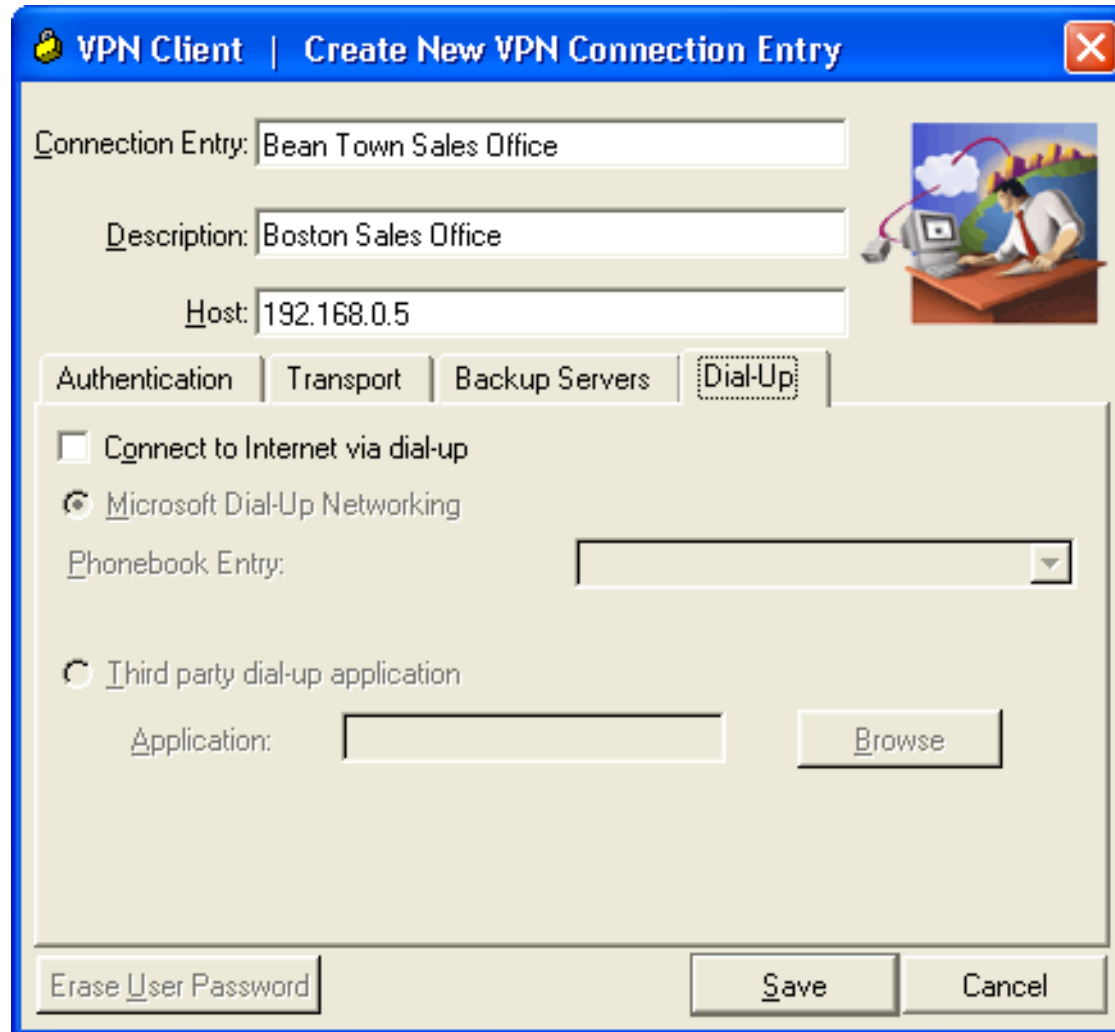
Configurarea NAT Traversal



The screenshot shows the 'VPN Client | Create New VPN Connection Entry' dialog box. The 'Transport' tab is selected, and the following settings are visible:

- Connection Entry: Bean Town Sales Office
- Description: Boston Sales Office
- Host: 192.168.0.5
- Authentication: Authentication
- Transport: Transport (selected)
- Backup Servers: Backup Servers
- Dial-Up: Dial-Up
- Enable Transparent Tunneling
 - IPsec over UDP (NAT / PAT)
 - IPsec over ICP TCP Port: 10000
- Allow Local LAN Access
- Peer response timeout (seconds): 90
- Erase User Password
- Save
- Cancel

Configurarea dial-up



The screenshot shows the 'VPN Client | Create New VPN Connection Entry' dialog box. The 'Dial-Up' tab is selected. The fields are filled with: Connection Entry: Bean Town Sales Office, Description: Boston Sales Office, and Host: 192.168.0.5. Under the 'Dial-Up' tab, there are three radio button options: 'Connect to Internet via dial-up' (unchecked), 'Microsoft Dial-Up Networking' (checked), and 'Third party dial-up application' (unchecked). The 'Microsoft Dial-Up Networking' option has a 'Phonebook Entry' dropdown menu. The 'Third party dial-up application' option has an 'Application' text box and a 'Browse' button. At the bottom, there are buttons for 'Erase User Password', 'Save', and 'Cancel'. An illustration of a person at a computer is visible on the right side of the dialog box.

VPN Client | Create New VPN Connection Entry

Connection Entry: Bean Town Sales Office

Description: Boston Sales Office

Host: 192.168.0.5

Authentication | Transport | Backup Servers | **Dial-Up**

Connect to Internet via dial-up

Microsoft Dial-Up Networking

Phonebook Entry: [Dropdown]

Third party dial-up application

Application: [Text Box] [Browse]

Erase User Password | Save | Cancel

VPN Client - statistics

VPN Client | Statistics

Tunnel Details | Route Details | Firewall

Address Information	Connection Information
Client: 10.0.21.1	Entry: student1
Server: 192.168.1.2	Time: 0 day(s), 00:04.04
Bytes	Crypto
Received: 0	Encryption: 56-bit DES
Sent: 23324	Authentication: HMAC-MD5
Packets	Transport
Encrypted: 134	Transparent Tunneling: Inactive
Decrypted: 0	Local LAN: Disabled
Discarded: 124	Compression: None
Bypassed: 56	

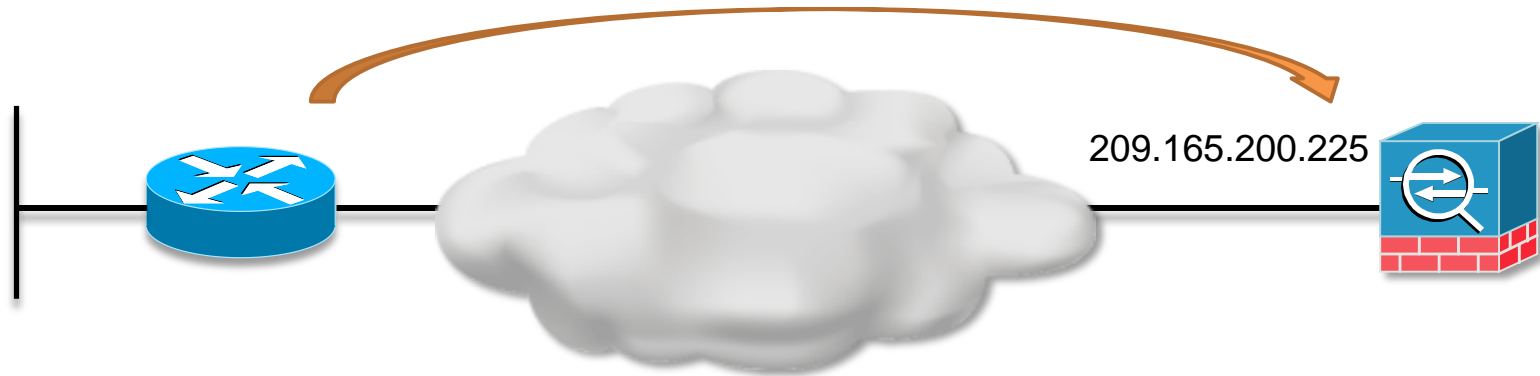
Reset

Close

Client VPN Hardware

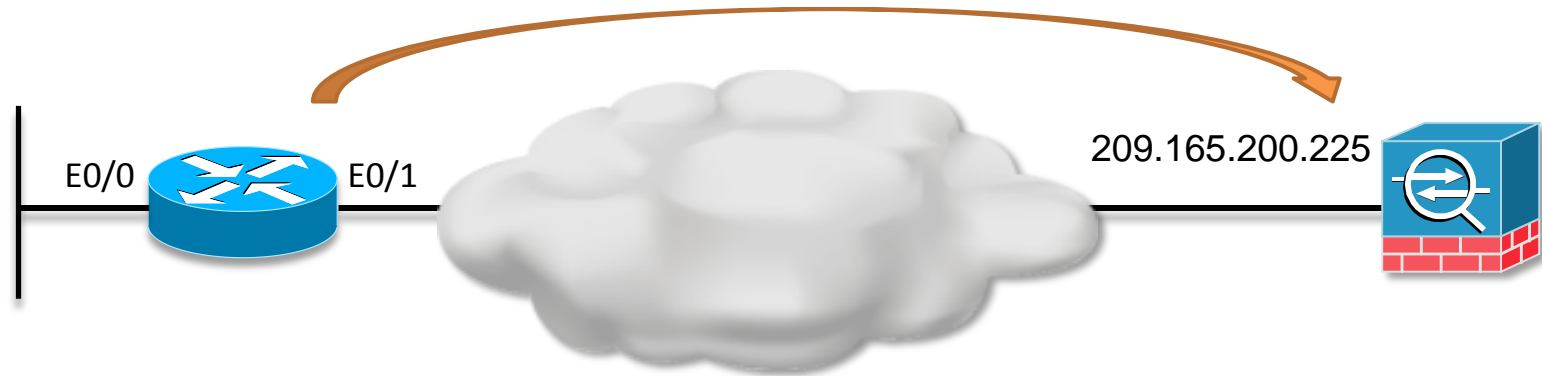
- ▶ Client mode – cunoscut și sub numele de PAT mode
 - ❑ Ruterul IOS face PAT pentru întreaga rețea ce se conectează prin VPN
 - ❑ Adresa IP publică folosită pentru PAT este asignată interfeței virtuale de VPN
 - ❑ Doar host-urile cu IP-uri private din spatele ruterului pot iniția conexiuni prin VPN
- ▶ Network extension mode (NEM)
 - ❑ Similar site-to-site, traficul prin VPN poate fi inițiat de oriunde
 - ❑ Inițierea VPN-ului poate fi făcută decât de client (ruterul IOS)
 - ❑ În acest mod nu există o interfață virtuală de VPN cu nevoia de a îi asigura o adresă IP deci ruterul IOS nu va face PAT pentru traficul prin tunel

Configurație Client VPN Hardware



```
Waters-aws-sm-client(config)# crypto ipsec client ezvpn
EZVPN_Client
Waters-aws-sm-client(config-crypto-ezvpn)# connect auto
Waters-aws-sm-client(config-crypto-ezvpn)# group ciscovpn key
cisco123
Waters-aws-sm-client(config-crypto-ezvpn)# mode network-extension
Waters-aws-sm-client(config-crypto-ezvpn)# peer 209.165.200.225
Waters-aws-sm-client(config-crypto-ezvpn)# username ciscouser
password cisco1
```

Configurație Client VPN Hardware



```
Waters-aws-sm-client(config)# interface Ethernet0
Waters-aws-sm-client(config-if)# crypto ipsec client ezvpn
EZVPN_Client inside
Waters-aws-sm-client(config)# interface Ethernet1
Waters-aws-sm-client(config-if)# crypto ipsec client ezvpn
EZVPN_Client outside
```



Fortinet – Implementarea SSL VPN

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 firewall-ului dar și la telnet, FTP, SMB/CIFS, VNC, RDP și SSH prin applet-uri/widget-uri 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

System

Router

Firewall

UTM

VPN

- IPsec
 - Auto Key (IKE)
 - Manual Key
 - Concentrator
 - Monitor
- SSL
 - Config**
 - Portal
 - Virtual Desktop Applicati
 - Host Check
 - Monitor

SSL-VPN Settings

Enable SSL-VPN

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)

Advanced (DNS and WINS Servers)

Apply

- ▶ 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 a configuration interface with a left-hand navigation menu and a main content area. The navigation menu is titled 'System' and includes items like Dashboard, Network, DHCP Server, Config, Admin, Certificates, and Maintenance. The 'Admin' section is expanded, showing 'Administrators', 'Admin Profile', 'Central Management', and 'Settings', which is highlighted in orange. The main content area is titled 'Administrators Settings' and contains two sections: 'Web Administration Ports' and 'Password Policy'. The 'Web Administration Ports' section has the following settings:

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

The 'Enable SSH v1 compatibility' checkbox is unchecked. The 'Password Policy' section has 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, and the dropdown menu is open, showing 'full-access', 'tunnel-access', and 'web-access'. The 'Available Users' list contains '- Local Users -'. The 'Members' list contains '- Local Users -' and 'steve_jobs'. The 'User Group' menu item in the left sidebar is highlighted.

- ▶ 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 politicii 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"/>
Implicit_Deny	all	ANY	always	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>

Comments (maximum 63 characters)

OK **Cancel**

Configurarea politicii de firewall – Tunnel mode

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

The screenshot displays the Mikrotik WinBox configuration interface for 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 a network management interface with a sidebar on the left and a main configuration area on the right. The sidebar is titled 'System' and includes a 'Router' section with a 'Firewall' sub-section. Under 'Firewall', there is a 'Policy' folder containing a 'Policy' item (highlighted in orange), 'Central NAT Table', 'DoS Policy', 'Sniffer Policy', and 'Protocol Options'. Other folders in the sidebar include 'Address', 'Service', 'Schedule', 'Traffic Shaper', 'Virtual IP', and 'Load Balance'. The main configuration area is titled 'New Policy' and contains the following settings:

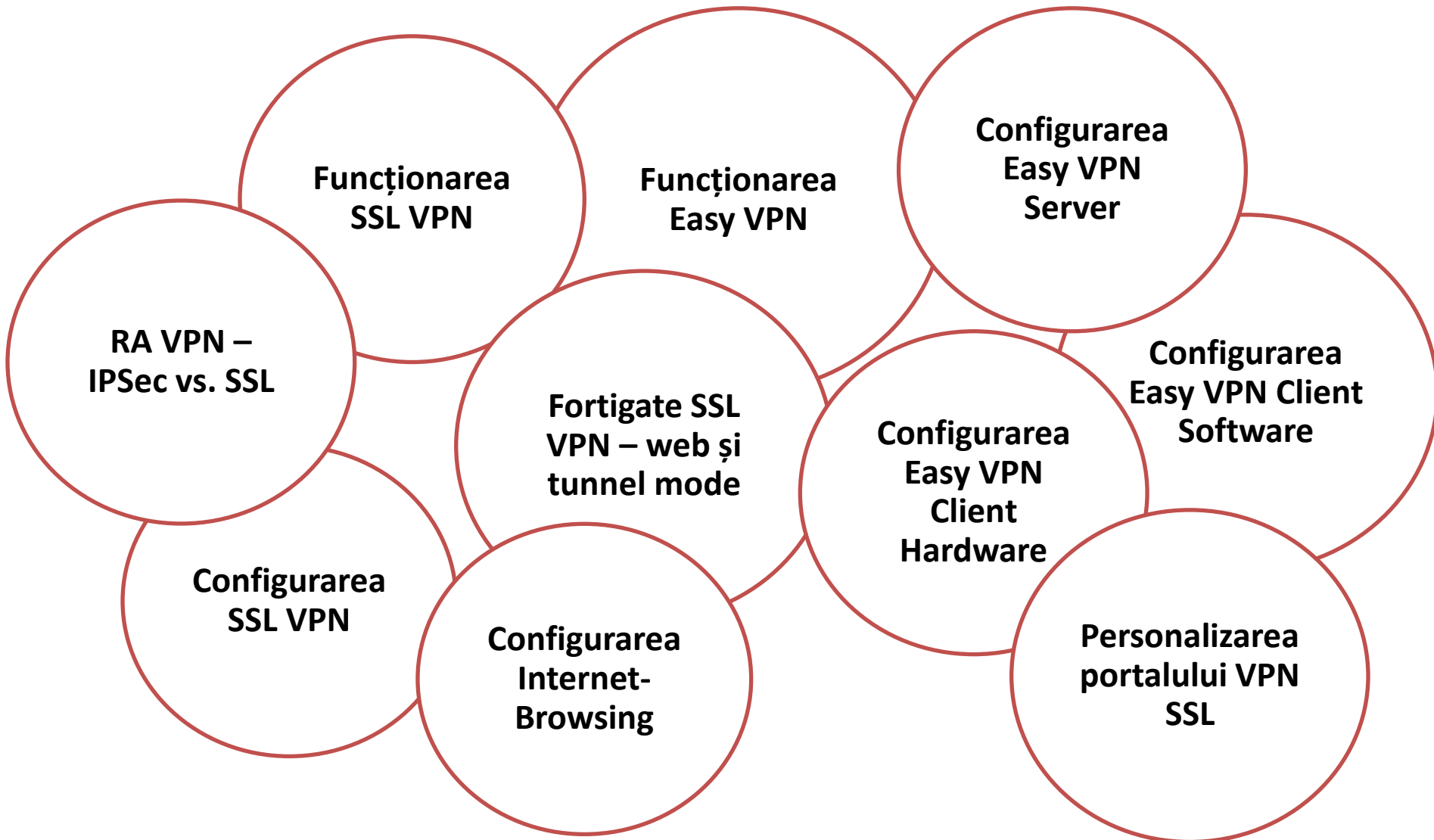
- Source Interface/Zone: sslvpn tunnel interface
- Source Address: all (Multiple)
- Destination Interface/Zone: wan2
- Destination Address: all (Multiple)
- Schedule: always
- Service: ANY (Multiple)
- Action: ACCEPT
- Log Allowed Traffic
- NAT:
 - No NAT
 - Enable NAT
 - Dynamic IP Pool
 - Use Central NAT Table
- Enable Identity Based Policy

Personalizarea portalului VPN

The screenshot displays the 'Welcome to SSL VPN Service' interface. On the left, a navigation menu includes System, Router, Firewall, UTM, VPN (highlighted), User, Endpoint, and Log&Report. Under VPN, there are sub-items for IPsec (Auto Key (IKE), Manual Key, Concentrator, Monitor) and SSL (Config, Portal, Virtual Desktop Application, Host Check, Monitor). The main area contains four widgets: 'Session Information' showing traffic statistics, 'Bookmarks' with a form to add a new bookmark (Name: my_bookmark, Type: FTP, Location: 192.169.45.2, Description: my_ftp_server), 'Connection Tool' (Type: Telnet, Host: 192.168.45.2), and 'Tunnel Mode' (Name: Tunnel Mode, IP Mode: Range, IP Pools: SSLVPN_TUNNEL_ADDR1, Split Tunneling: checked). Buttons for OK, Cancel, Apply, and Settings are visible at the top.

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

Overview



Cursul viitor...

- ▶ Transparent firewall
 - ❑ Unele funcționalități limitate (VPN, UTM)
 - ❑ Schimbări de strategie în securizarea rețelei



- ▶ WAN Optimization
 - ❑ WEB-caching
 - ❑ Byte-caching
 - ❑ Protocol optimization