VPN sau Virtual Private Network vă permite să conectaţi mai multe locaţii folosind Internetul şi să vă asiguraţi că datele care se transmit nu pot fi furate sau compromise într-un alt mod. Acest lucru se obţine prin crearea "tunelelor de securitate" prin care trec datele transferate de pe o locaţie pe alta. Tunele VPN se folosesc în general pentru a conecta birourile de la distanţă sau utilizatorii care lucrează de acasă cu biroul central.

Odată cu creşterea vitezei de Internet creşte şi posibilitatea lucrului de la distanţă: de acasă, dintr-un hotel etc. VPN-urile devin tot mai populare, deoarece reprezintă cea mai bună soluţie pentru siguranţa transferului de datele. Odată cu dezvoltarea VPN-ului, vin şi noi funcţionalităţi, precum DirectAccess (care a fost introdus odată cu sistemele de operare Windows 7 şi Windows 2008 R2) şi VPN Reconnect care este prezent în sistemele de operare Windows 8 şi Windows server 2012.

Astăzi sunt disponibile două tipuri de tunele VPN:

- Remote Access – care este cunoscut şi ca conexiunea Point-to-Point. Acesta este un tip de conexiune mai popular şi reprezintă situaţia în care utilizatorul accesează din orice locaţie reţaua companiei şi resursele de pe aceasta folosind propria conexiune la Internet.

- Site-to-Site – acest tip de conexiune leagă birourile de la distanţă folosind conexiunile lor de Internet. Este cunoscut şi sub denumirea de Wide-Area Network (WAN). Acest tip de VPN creează o structură a tunelului care permite utilizatorilor de pe o locaţie să acceseze resursele de pe altă locaţie şi invers.

Windows 8 susţine patru tipuri de protocoale pentru tunelling şi crearea conexiunilor VPN:

- Point-to-Point Tunneling Protocol (PPTP) – PPTP se bazează pe protocolul PPP (point-to-point) original. Are o encripţie şi o

autentificare slabă şi nu este considerat sigur pentru utilizare.

- Layer 2 Tunneling Protocol (L2TP) / IP security (IPSec) - L2TP este o altă generaţie de protocoale pentru tunneling, bazată original pe protocolul PPTP. L2TP face tunelele pe un alt nivel (nivelul Data Link) pentru conexiunea prin intermediul reţelei deja existente (în general prin Internet). De fapt L2TP transmite sesiuni PPP şi nu oferă o siguranţă mai mare decât protocolul PPTP. Ceea ce îl face sigur este IPSec. IPSec oferă posibilitatea de a verifica confidenţialitatea, autentificarea şi integritatea datelor care sunt trimise prin reţeaua publică. IPSec este alcătuit din două protocoale: AH (authentication header) care este responsabil pentru verificarea autentificării şi integrităţii, şi ESP (Encapsulating Security Payload) care criptează conţinutul.

- Secure Socket Tunneling Protocol (SSTP) – Introdus în sistemul de operare Windows Vista, SSTP utilizează Hypertext Transfer Protocol Secure (HTTPS) şi TCP port 443 pentru a trece traficul prin firewall-ul care poate să blocheze PPTP sau L2TP/IPSec. SSTP are posibilitatea de a cripta traficul PPP folosind canalul Secure Socket Layer (SSL) al protocolului HTTPS. Utilizarea PPP-ului permite utilizarea unor metode de autentificare puternice, precum Extensible Authentication Protocol – Transport Layer Security (EAP-TSL). SSL oferă securitatea la nivel de transport folosind mecanisme mai calitative pentru schimbarea cheilor de criptare şi o encripţie şi o integritate mai puternică.

- Internet Key Exchange (IKEv2) – Este introdus odată cu sistemul de operare Windows 7. Acest protocol creează tunele IPSec prin portul UDP. Tunelele IKEv2 VPN sunt foarte utile în situaţiile în care utilizatorul trece permanent de pe o conexiune wirelles pe alta sau de pe conexiunea wirelles pe cablu. Unirea tehnologiilor IKEv2 şi IPSec oferă o autentificare şi o encripţie puternică în

timpul transportului.

Pe fiecare dintre aceste conexiuni VPN, puteţi face următoarele setări:

- Încapsularea – Datele se încapsulează cu ajutorul header-ului. Doar header-ul conţine informaţii despre rutare, lucru ce permite datelor să circule prin reţea şi să ajungă la o anumită destinaţie.

- Autentificarea – aceasta poate avea trei forme diferite:
  - Autentificare la nivel de utilizator
  - Autentificare la nivel de calculator
  - Autentificare pe baza sursei de date

- Criptarea – Criptarea datelor permite ca datele să rămână confidenţiale şi necompromise cât timp trec prin reţeaua publică (Internet). Expeditorul criptează datele folosind cheia pentru criptare, iar receptorul le decriptează folosind cheia pentru decriptare.

Protocol VPN	Încapsulare	Criptare
PPTP	TCP/IP	MS-CHAPv2 sau EAP-TLS
L2TP/IPSec	L2TP/UDP + IPSec	Advanced Encryption Standard (AES) sau Triple Data Encryption

		Standard (3DES)
SSTP	TCP/IP 443	HTTPS SSL
IKEv2	ESP/AH	AES256 sau 3DES

Tabel 21.1 Protocoale VPN

Metodele de autentificare care astăzi se folosesc cel mai des sunt:

- Password Authentication Protocol (PAP) – un protocol de autentificare nu foarte sigur. Transmite parolele într-un text curat. Se foloseşte doar în situaţiile în care clientul şi serverul nu pot folosi un protocol mai sigur pentru autentificare. Acest protocol nu este posibil în Windows 8, dar îl puteţi activa manual, iar în Windows 2008 şi în sistemele de operare pentru server mai noi nici măcar nu e susţinut.
- pentru criptare. Este mai avansat decât PAP, deoarece nu foloseşte PPP pentru transmiterea pachetului, ceea ce înseamnă că numele de utilizator şi parola nu sunt trimise în textul curat.
- Microsoft CHAP version 2 – susţine autentificarea bidirecţională reciprocă. Oferă o securitate mai mare în transferul informaţiilor decât CHAP.
- EAP-MS-CHAPv2 – Permite autentificarea clientului care se conectează folosind schema de autentificare EAP. EAP oferă cel mai înalt nivel de protecţie datorită flexibilităţii sale atunci când este vorba de alegerea metodei. Acest protocol necesită deţinerea unui certificat instalat pe calculatorul pe care se vor conecta clienţii.

Windows 8 este optimizat pentru utilizarea pe ecranele sensibile la atingere. Cu aceasta, şi sarcinile administrative sunt uşurate şi accelerate. Acum, crearea conexiunii VPN este mai uşoară. Iconiţele conexiunilor VPN create apar acum în listă printre celelalte conexiuni la reţea, în cadrul secţiunii View Available Networks.

Crearea conexiunii VPN nu solicită multe informaţii. Tot ce vă trebuie sunt informaţţii despre serverul la care vă conectaţi. Crearea unui VPN pe server va fi abordată în alte cursuri. Pentru moment este suficient să ştiţi cum să creaţi conexiunea de la client către server.

- Pe ecranul de start tastaţi „vpn“, daţi clic pe secţiunea Settings şi selectaţi „Set Up A Virtual Private Network (VPN) Connection“.

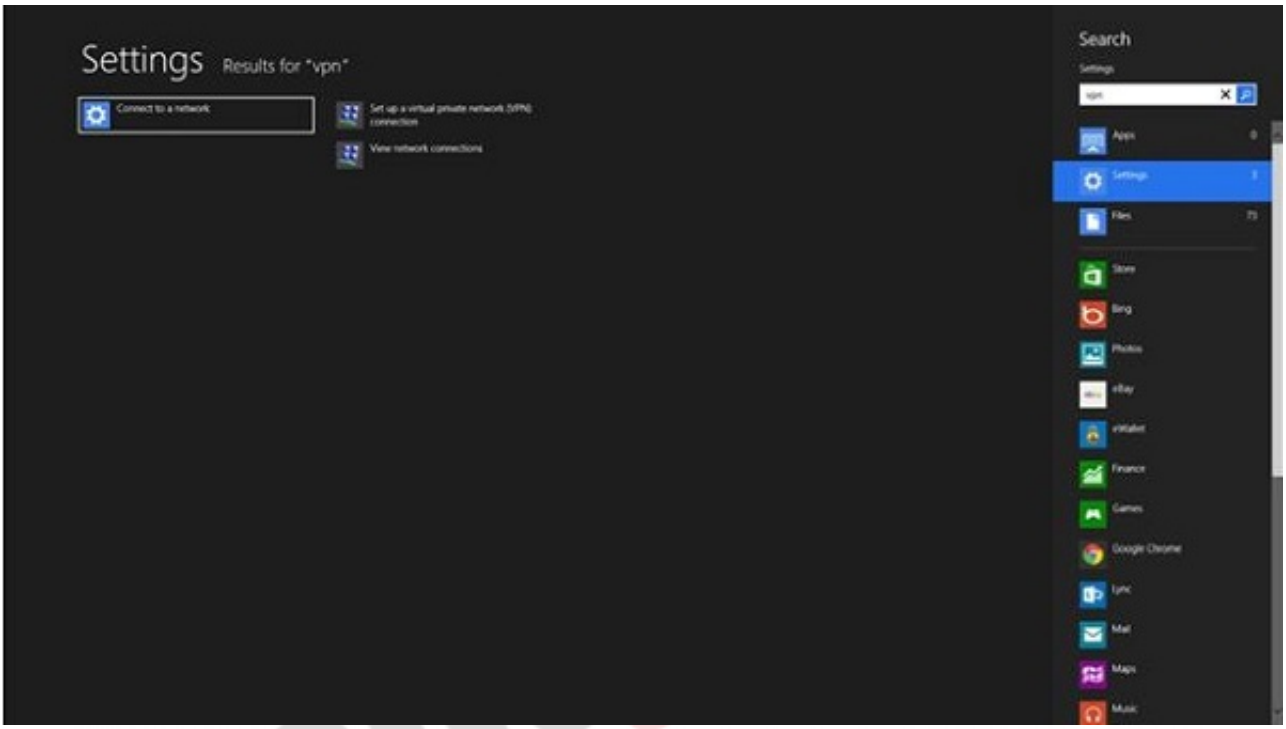

Figura 19.1 Crearea conexiunii VPN

- Introduceţi adresa IP publică a serverului VPN la care doriţi să vă conectaţi.
- Introduceţi numele conexiunii în câmpul “Destination name“. Acesta este numele conexiunii VPN care va apărea atunci când veţi dori să vă conectaţi.
- Selectaţi câmpul „Remember My Credentials“ dacă vreţi ca numele de utilizator şi parola să se memoreze la prima loogare cu succes.

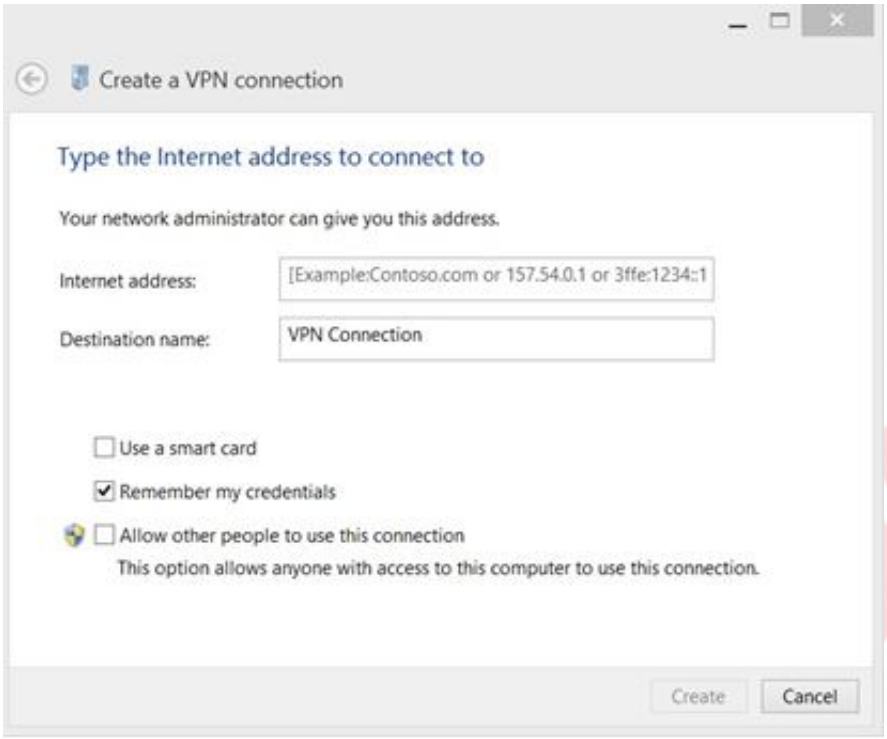

Figura 19.2 Crearea conexiunii VPN

După ce aţi terminat cu crearea conexiunii VPN, este momentul să o folosiţi şi să vă conectaţi cu locaţia dorită.

1. simultan tastele Windows + I de pe tastatură pentru a deschide meniul Settings.
2. Daţi un clic pe iconiţa pentru reţea.
3. Daţi un clic pe conexiunea VPN pe care vreţi să o porniţi şi daţi clic pe Connect.
4. Conexiunea VPN începe să stabilească legătura cu serverul folosind acreditările salvate. Dacă nu reuşeşte să se conecteze folosind aceste acreditări, vi se va cere să introduceţi acreditări noi.

5. Când se termină procesul de conexiune, wizzard-ul va dispărea, ceea ce înseamnă că conexiunea este stabilită.

Fiecare conexiune creată o puteţi schimba. Toţi parametrii pe care i-aţi introdus în timpul creării se pot înlocui cu alţii noi.

1. simultan tastele Windows + I de pe tastatură pentru a deschide meniul Settings.
2. Daţi un clic pe iconiţa pentru reţea.
3. Daţi un clic dreapta pe conexiunea VPN pe care vreţi să o modificaţi şi selectaţi „View Connection Properties“

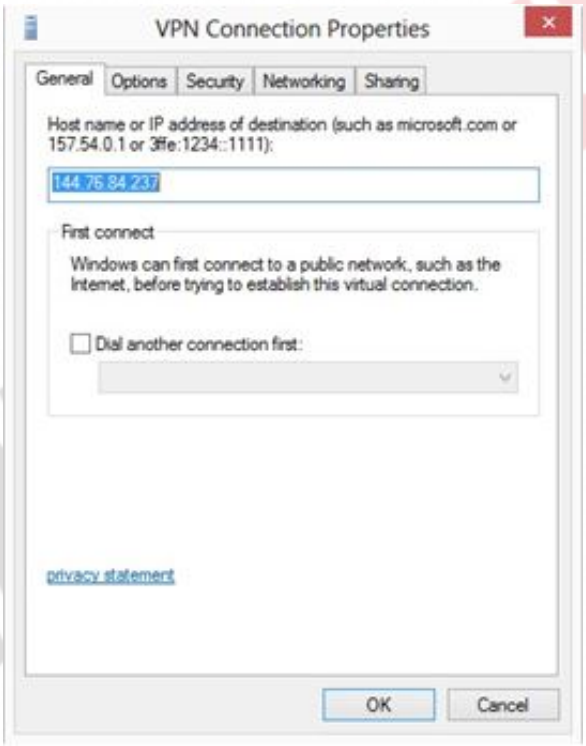

Figura 19.3 Modificări în conexiunea VPN

VPN-ul se poate seta ca o conexiune între două locaţii de la distanţă sau între un utilizator şi compania mamă. Windows 8 vă oferă posibilitatea de a seta cu uşurinţă conexiunea respectivă. În cazul unei conexiuni la Internet slabe, conexiunea VPN, respectiv tunelul VPN se întrerupe. Aceasta nu este o problemă foarte mare pentru un utilizator care se conectează la resursele companiei. Este suficient să repornească conexiunea şi să continue să lucreze. Însă, în situaţiile în care prin VPN sunt conectate două locaţii aflate la distanţă, aceasta fiind, în general, o conexiune între două servere la care nu lucrează nimeni non-stop, administratorul va trebui să se conecteze la serverele

respective şi să restabilească legătura manual. IKEv2 aduce un supliment care se numeşte VPN Reconnect şi care permite stabilirea automată a legăturii dintre client şi server. VPN Reconnect este disponibil începând cu Windows 7 pentru tunelul IKEv2 VPN.

La sistemul de operare Windows 8, VPN Reconnect este activat în mod implicit. Perioada de timp în care conexiunea VPN va încerca să stabilească din nou conexiunea, respectiv timpul în care îi este permis VPN-ului să nu fie conectat, se poate seta în cadrul ferestrei Properties a conexiunii VPN. În tab-ul Security, în cadrul secţiunii Advanced Settings, tab-ul IKEv2, aveţi posibilitatea de a schimba Network outage time. Această opţiune vă permite să convingeţi conexiunea VPN să încerce să se conecteze din nou pe acelaşi server la 30 de minute până la 8 ore după întreruperea conexiunii.

WIN8_19 - Windows 8

1. Protocolul care foloseşte protocolul Hypertext Transfer Protocol Secure pentru transmiterea pachetelor şi pentru realizarea traficului este:

- ◯ a) PPTP
- ◯ b) SSTP
- ◯ c) L2TP
- ◯ d) PPLP

2. Protocolul care creează tunelul IPSec prin intermediul protocolului UDP este:

- ◯ a) PPTP
- ◯ b) SSTP
- ◯ c) L2TP
- ◯ d) IKEv2

3. Care dintre protocoalele VPN menţionate folosesc encripția TripleDES pentru criptarea datelor care trec prin ele:

- ☐ a) PPTP
- ☐ b) L2TP/IPSec
- ☐ c) SSTP
- ☐ d) IKEv2

4. Care dintre variantele menţionate nu reprezintă o metodă pentru autentificare?

- ◯ a) PAP
- ◯ b) EAP
- ◯ c) CHAP
- ◯ d) GAP

5. Opţiunea care vine cu sistemul de operare Windows 8, dar care permite stabilirea automată a tunelului IKEv2 VPN după întreruperea conexiunii la Internet, se numeşte:

- ◯ a) VPN Connect
- ◯ b) VPN Tunneling
- ◯ c) VPN Reconnect
- ◯ d) VPN Troubleshooter

6. CHAP foloseşte schema Message Diagest 5 (MD5) pentru criptare.

- ◯ a) adevărat
- ◯ b) fals

7. Care sunt cele două protocoale care alcătuiesc IPSec?

- ☐ a) AH
- ☐ b) PPP
- ☐ c) ESP
- ☐ d) EAP

1. Protocolul care foloseşte protocolul Hypertext Transfer Protocol Secure pentru transmiterea pachetelor şi pentru realizarea traficului este:

b

2. Protocolul care creează tunelul IPSec prin intermediul protocolului UDP este:

d

3. Care dintre protocoalele VPN menţionate folosesc encripția TripleDES pentru criptarea datelor care trec prin ele:

b, d

4. Care dintre variantele menţionate nu reprezintă o metodă pentru autentificare?

d

5. Opţiunea care vine cu sistemul de operare Windows 8, dar care permite stabilirea automată a tunelului IKEv2 VPN după întreruperea conexiunii la Internet, se numeşte:

c

6. CHAP foloseşte schema Message Diagest 5 (MD5) pentru criptare.

a

7. Care sunt cele două protocoale care alcătuiesc IPSec?

a, c