Routing and Remote Access Service / Virtual Private Network (RRAS/VPN)

ΕΙΣΑΓΩΓΗ

α. Στη σημερινή εποχή όπου όλες οι επιχειρήσεις και οι οργανισμοί χρησιμοποιούν δίκτυα Η/Υ, σχεδόν όλοι οι υπάλληλοί τους είναι χρήστες της Λογικής Περιοχής (domain) του δικτύου της επιχείρησης/οργανισμού. Οι χρήστες αυτοί έχουν πρόσβαση στους κοινόχρηστους πόρους αυτών των δικτύων. Αυτό όμως ισχύει για τους χρήστες που εργάζονται μέσα στο κτήριο της έδρας της επιχείρησης/οργανισμού. Τι γίνεται όμως με τους υπαλλήλους που εργάζονται με τους υπαλλήλους που εργάζονται με τους υπαλλήλους που εργάζονται από το σπίτι (teleworking);

β. Αρκετές επιχειρήσεις και οργανισμοί έχουν την έδρα τους, και το κεντρικό κτήριο των γραφείων τους, μέσα στον πολεοδομικό ιστό μιας πόλης. Ομως τις εγκαταστάσεις παραγωγής τους και τις αποθήκες τους τις έχουν σε ΒΙομηχανικές ΠΕριοχές εκτός των πόλεων. Πως μπορούν τα δίκτυα Η/Υ των κεντρικών γραφείων, της εγκατάστασης παραγωγής και της αποθήκης να ανήκουν στην ίδια Λογική Περιοχή (domain) του δικτύου της επιχείρησης/οργανισμού;

γ. Δύο επιχειρήσεις/οργανισμοί που έχουν δίκτυα Η/Υ με διαφορετικές Λογικές Περιοχές (domains) θέλουν για συγκεκριμένους λόγους να διασυνδέσουν τα δίκτυά τους. Πως θα γίνει αυτό;

Στην α. περίπτωση χρειαζόμαστε μια υπηρεσία τύπου: Remote Access.

- Η β. περίπτωση είναι ένα intranet και χρειάζεται μια υπηρεσία τύπου Routing.
- Η γ. περίπτωση είναι ένα extranet και χρειάζεται μια υπηρεσία τύπου Routing.

Για να υλοποιηθούν τα παραπάνω χρειάζεται το internet και η δημιουργία Εικονικών Ιδιωτικών Δικτύων (Virtual Private Networks) με τη χρήση "σηράγγων (tunnels)" μέσα από αυτό. Θεωρώντας ότι το λειτουργικό σύστημα των προαναφερθέντων δικτύων είναι τα Windows, θα πρέπει οι servers αυτών των δικτύων να υποστηρίζουν την υπηρεσία Routing and Remote Access.

Στο παρακάτω Σχήμα 1 φαίνεται παραστατικά ένα Εικονικό Ιδιωτικό Δίκτυο. Ως clients ορίζονται οι απομεμακρυσμένοι χρήστες. Τα "tunnels" δημιουργούνται με τη χρήση των PPTP και L2TP (πρωτόκολλα του 2ου επιπέδου κατά OSI αρχιτεκτονικής και του Link layer του 1ου επιπέδου κατά TCP/IP αρχιτεκτονικής).



Σχήμα 1. Virtual Private Network.

Στο παρελθόν οι φυσικές γραμμές επικοινωνίας για να υλοποιηθούν τα VPN των intranet και extranet ήταν οι μισθωμένες εξωκείμενες γραμμές (leased lines) ενώ οι αντίστοιχες γραμμές για τους απομεμακρυσμένους χρήστες ήταν συνήθως οι απλές τηλεφωνικές γραμμές με τη χρήση modems. Με την εξέλιξη της τεχνολογίας οι φυσικές γραμμές επικοινωνίας και για τις δύο χρήσεις έγιναν ISDN (PRI και BRI). Τώρα πλέον αυτές οι γραμμές επικοινωνίας είναι τύπου ADSL. Ακόμη και τώρα σε περίπτωση VPN για intranet όπου διακινείται μεγάλος όγκος δεδομένων χρησιμοποιούνται οι μισθωμένες εξωκείμενες γραμμές. (Τυπικώς όταν χρησιμοποιούνται οι μισθωμένες δεν χρειάζεται η υλοποίηση VPN. Στη πράξη όμως εφαρμόζεται για την ασφάλεια των διακινούμενων πληροφοριών, καθώς αυτές οι γραμμές διέρχονται από μέρη που δεν ελέγχει η κάθε επιχείρηση ή οργανισμός.)

ΠΡΑΓΜΑΤΟΠΟΙΗΣΗ ΕΡΓΑΣΤΗΡΙΑΚΟΥ ΔΙΚΤΥΟΥ VPN

Α. Εγκατάσταση ρόλου RRAS σε server του δικτύου

Η εγκατάσταση του ρόλου RRAS θα γίνει σε server με λειτουργικό σύστημα Windows 2008.

Η Microsoft προτείνει να μην εγκαθίστανται ο ρόλος RRAS σε server που είναι Domain Controller. Ομως καθώς εμείς δεν έχουμε τη δυνατότητα να διαθέσουμε και άλλο server θα χρησιμοποιήσουμε αυτόν που είναι DC.

Επίσης ο ρόλος RRAS πρέπει να παρέχεται από server που διαθέτει δύο κάρτες δικτύου (Network Interface Card). Η μία NIC συνδέεται στον router (WAN πλευρά) και η άλλη NIC στο switch (LAN πλευρά) (Σχήμα 2).



Σχήμα 2. VPN με δύο NIC

Ο ρόλος RRAS είναι δυνατόν να εγκατασταθεί και σε server που έχει μόνο μια NIC (Σχήμα 3) αν και δεν συνιστάται.



workstations

Σχήμα 3. VPN με μία NIC

Υλοποιούμε την συνδεσμολογία του Σχήματος 2. Και οι δύο NIC διαθέτουν στατικές IP διευθύνσεις. Στην "Internal for LAN" αποδίδουμε την: 192.168.1.10 και στην "External for VPN" αποδίδουμε την 10.67.80.31 (βλέπε Εικόνες 1 & 2). Στην "Internal for LAN" επιβάλλεται από την Microsoft να μην ορίζεται Default Gateway. Η IP διεύθυνση 127.0.0.1 του πεδίου: Preferred DNS Server είναι η loopback διεύθυνση, δηλώνοντας την διεύθυνση αυτού του ίδιου του Η/Υ δηλαδή την:192.168.1.10 ή 10.67.80.31 αντίστοιχα.

Η "Internal for LAN" NIC έπρεπε να είναι εγκατεστημένη πριν την εγκατάσταση του Active Directory σ' αυτόν τον Server.

Name - Status - Device Name - C	onnectivity 🔸 Network Category 🛛	▼ Owner	one # or Host Address 🔽
LAN or High-Speed Internet (2)			E
External for VPN 3epal3.local 2 Realtek PCIe GBE Family	Internal Network 3epal3.local 2 Realtek PCIe GBE Family		
	Internal Network Properties	x	
	Networking Sharing		
	Connect using:		
	Realtek PCIe GBE Family Con	itroller	
	This connection uses the following it	Configure	
	Client for Microsoft Network	.8	
	QoS Packet Scheduler	Miemeeft Networks	
	 Internet Protocol Version 6 	(TCP/IPv6)	
	Internet Protocol Version 4	(TCP/IPv4)	
	🗹 📥 Link-Layer Topology Discov	very Mapper I/O Driver	
	Internet Protocol Version 4 (T	CP/IPv4) Properties	<u>? ×</u>
	General		
	You can get IP settings assigne this capability. Otherwise, you	d automatically if your network sup need to ask your network administ	pports rator
	for the appropriate iP settings.		
	C Obtain an IP address auto	omatically	
	Use the following IP addre	ess:	
	IP address:	192 . 168 . 1 . 10	
	Subnet mask:	255 . 255 . 255 . 0	
	Default gateway:	<u> </u>	
	C Obtain DNS server addres	ss automatically	
	Use the following DNS ser	ver addresses:	
	Preferred DNS server:	127 . 0 . 0 . 1	
	Alternate DNS server:		
		Advan	red
		ОК	Cancel

Εικόνα 1. Δικτυακές Παράμετροι της "Internal for LAN" NIC.

iame 🔹 Status 👻 Device Name 👻 Con	nectivity 💌 Network Category 💌 Owner	▼ Type	▼ Phone # or Host Address ▼	
LAN or High-Speed Internet (2)				
External for VPN	Internal Network			
Realtek PCIe GBE Family	Realtek PCIe GBE Family			
1				
External for VPN Properties	×			
Networking Sharing	-			
Connect using:				
Realtek PCIe GBE Family Controller				
	Configure			
This connection uses the following items:				
Client for Microsoft Networks				
QoS Packet Scheduler	t Natworks			
✓ Internet Protocol Version 6 (TCP/IP)	v6)			
Internet Protocol Version 4 (TCP/IP	v4)			
Internet Protocol Version 4 (TCP/IPr4)	Properties 21×1			
General	1			
You can get IP settings assigned automatic this capability. Otherwise, you need to ask	ally if your network supports			
for the appropriate IP settings.				
C Obtain an IP address automatically				
Use the following IP address:				
IP address:	0 . 67 . 80 . 31			
Subnet mask: 25	55.255.255.0			
Default gateway:	0 . 67 . 80 . 1			
C Obtain DNS server address automatic	sally			
• Use the following DNS server address	Ses:			
Preferred DNS server:	27.0.0.1			
Alternate DNS server:				
	Advanced			
	OK Cancel			

Εικόνα 2. Δικτυακές Παράμετροι της "External for VPN" NIC.

1. Επιλέγουμε: Start -> Server Manager και στο παράθυρο που ανοίγει επιλέγουμε: Roles.



Εικόνα 3. Εγκατεστημένοι ρόλοι στον Server.

Στην Εικόνα 3 παρατηρούμε ότι έχουν εγκατασταθεί οι ρόλοι:

Active Directory Domain Services

DHCP Server

DNS Server

οι οποίοι είναι οι απολύτως απαραίτητοι για τη δημιουργία μιας Λογικής Περιοχής Δικτύου (Domain).

2. Επιλέγουμε: **Add Roles** (κόκκινο βέλος στην Εικόνα 3) και εμφανίζεται το παράθυρο της Εικόνας 4.



Εικόνα 4. Προαπαιτούμενα εγκατάστασης ρόλου στον Server.

 Σ' αυτό το παράθυρο φαίνονται τα προαπαιτούμενα για την εγκατάσταση ενός ρόλουν στον Server που είναι:

Ισχυρό Συνθηματικό για τον λογαριασμό του Administrator.

Να έχουν ορισθεί σωστά οι δικτυακές παράμετροι των ΝΙC.

Να έχουν εγκατασταθεί οι ενημερώσεις των Windows που αφορούν την ασφάλεια.

Πριν προχωρήσουμε στο επόμενο βήμα θα πρέπει να είμαστε σίγουροι ότι έχει εγκατασταθεί και η δεύτερη NIC, ότι λειτουργεί σωστά και ότι έχουν ορισθεί σωστά οι δικτυακές παράμετροι. Εαν κάτι από τα προηγούμενα δεν ισχύει επιλέγουμε: **Cancel** και κάνουμε τις απαραίτητες ενέργειες ώστε να ισχύουν τα προαπαιτούμενα.

Αφού όλα είναι εντάξει επιλέγουμε: Next.

3. Επιλέγουμε να εγκαταστήσουμε τον ρόλο: **Network Policy and Access Services** (Εικόνα 5) και κατόπιν επιλέγουμε: **Next**.

Server Roles	Select one or more roles to install on this server. Roles:	Description:
Network Policy and Access Services Role Services Confirmation Progress Results	 Active Directory Certificate Services Active Directory Pederation Services (Installed) Active Directory Federation Services Active Directory Lightweight Directory Services Active Directory Rights Management Services Application Server DHCP Server (Installed) DNS Server (Installed) Fax Server File Services Y Network Policy and Access Services UDDI Services UDDI Services UDDI Services Web Server (IIS) Windows Deployment Services 	Network Policy and Access Services provides Network Policy Server (NPS) Routing and Remote Access, Health Registration Authority (HRA), and Host Credential Authorization Protoco (HCAP), which help safeguard the health and security of your network.

Εικόνα 5. Επιλογή ρόλου: Network Policy and Access Services.

4. Σε αυτό το παράθυρο ενημερωνόμαστε περιληπτικά σχετικά με τις Network Policy and Access Services. Επιλέγουμε: **Next**.

Add Roles Wizard	×
Network Policy a	and Access Services
Before You Begin Server Roles Network Policy and Access Services Role Services Confirmation Progress Results	 Introduction to Network Policy and Access Services Network Policy and Access Services allows you to provide local and remote network access and to define and enforce policies for network access service, authorization, and client health using Network Policy Server (NPS), Routing and Remote Access Service, Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP). Things to Note You can deploy NPS as a Remote Authentication Dial-In User Service (RADIUS) server and proxy and as a Network Access Protection (NAP) policy server. After installing NPS using this wizard, you can configure NPS from the NPAS home page using the NPS console. That helps you ensure that computers connecting to the network are compliant with organization network and client health policies. After installing NPS using this wizard, you can configure NPAS home page using the NPS console. Overview of Network Policy and Access Services NAP enforcement methods Network Access Protection (NAP) in NPS Network Access Protection (NAP) in NPS Network Access Protection (NAP) in NPS
	< Previous Next > Install Cancel

Εικόνα 6. Εισαγωγή, Δυνατότητες και περαιτέρω Πληροφόρηση για τις Network Policy and Access Services.

5. Σε αυτό το παράθυρο επιλέγουμε και τις δύο υπηρεσίες (Remote Access και Routing). Εαν θέλαμε να εξυπηρετήσουμε μόνο την απομεμακρυσμένη σύνδεση χρηστών θα μπορούσαμε να ενεργοποιήσουμε μόνο την **Remote Access Service**. Ομως συνηθίζουμε να ενεργοποιούμε και την **Routing** καθώς είναι πιθανό να μας εξυπηρετήσει μελλοντικά σε πιο σύνθετες καταστάσεις όπως διασύνδεση απομακρυσμένων μεταξύ τους LAN της ίδιας εταιρείας. Κατόπιν επιλέγουμε: **Next**.

Before You Begin	Select the role services to install for Network Policy and Ac	cess Services:
Server Roles	Role services:	Description:
Network Policy and Access Services Role Services Confirmation Progress Results	Network Policy Server Routing and Remote Access Service Routing Routing Health Registration Authority Host Credential Authorization Protocol	Routing and Remote Access Services provides remote users access to resources on your private network over virtual private network (VPN) or dial-up connections. Servers configured with the Routing and Remote Access service can provide LAN and WAN routing services used t connect network segments within a small office or to connect two private networks over the internet.

Εικόνα 7. Ενεργοποίηση υπηρεσιών Routing and Remote Access.

6. Σε αυτό το παράθυρο επιβεβαιώνουμε την πρόθεση μας για την εγκατάσταση των υπηρεσιών Routing and Remote Access επιλέγοντας: Install.

Add Roles Wizard		×
Confirm Installati	ion Selections	
Before You Begin Server Roles Network Policy and Access Services	To install the following roles, role services, or features, click Install.	
Role Services	(j) This server might need to be restarted after the installation completes.	
Progress Results	Routing and Remote Access Services Remote Access Service Routing	
	Print, e-mail, or save this information	
	<pre>_ < Previous Next > Install Cancel</pre>	

Εικόνα 8. Επιβεβαίωση εγκατάστασης υπηρεσιών Routing and Remote Access.

Add Roles Wizard	
Installation Prog	ress
Before You Begin Server Roles Network Policy and Access Services Role Services Confirmation Progress Results	Initializing installation
	< <previous next=""> Install Cancel</previous>

Εικόνα 9. Εξέλιξη εγκατάστασης υπηρεσιών Routing and Remote Access.

7. Στο παράθυρο αυτό διαπιστώνουμε ότι η εγκατάσταση των υπηρεσιών Routing and Remote

Access ήταν επιτυχής. Επιλέγουμε: Close.



Εικόνα 10. Αποτέλεσμα εγκατάστασης υπηρεσιών Routing and Remote Access.

8. Στο παράθυρο του Server Manager φαίνονται οι εγκατεστημένοι ρόλοι του Server.



Εικόνα 11. Εγκατεστημένοι ρόλοι του Server.

Β. Παραμετροποίηση RRAS για την παροχή της υπηρεσίας VPN.

1. Επιλέγουμε Start \rightarrow Administrative Tools \rightarrow Server Manager, επεκτείνουμε το Roles container, επεκτείνουμε το Network Policy and Access Services container, κάνουμε δεξι click στο Routing and Remote Access και επιλέγουμε: Configure and Enable Routing and Remote Access (Εικόνα 12). Στο παράθυρο του Wizard που εμφανίζεται επιλέγουμε: Next.

🖡 Server Manager			
File Action View Help			
Server Manager (SERVER3)	anin Se Get an overview of the status of Access	this server, perform top management tasks, and add or remo	ve server roles and features.
Routing and Ren	Configure and Enable Routing and Remote Access		Server Summary Help
Group Policy Mana Diagnostics Configuration Storage	Disable Routing and Remote Access Auto Refresh Refresh Rate All Tasks	server3.3epal3.local	 Change System Properties View Network Connections Configure Remote Desktop
	Delete Refresh Properties	IPv4 address assigned by DHCP, IPv6 enabled 10.67.80.31, IPv6 enabled	
	Help	Disabled	
	Product ID:	92573-0EM-7502905-27565	_
	 Security Information Windows Firewall: Windows Updates: 	On Never check for updates	
	Last checked for updates:	Never	Configure IE ESC
	Last installed updates:	Never	
	IE Enhanced Security Configuration (ESC):	On for Administrators On for Users	
	Roles Summary		Roles Summary Help
•	Last Refresh: 3/9/2015 11:56:48 nµ Confi	igure refresh	
Configures Routing and Remote	Access for the selected server		

Εικόνα 12. Ενεργοποίηση του RRAS.

2. Στο επόμενο παράθυρο επιλέγουμε: Remote access (dial-up or VPN) και μετά: Next.

You can ena customize thi	ole any of the following server.	g combinations of se	ervices, or you can	
 Remote a Allow rem 	ccess (dial-up or VPN ite clients to connect 1) to this server throug	h either a dial-up co	nnection or a
secure vir	ual private network (V	(PN) Internet conne	ction.	
C Network	address translation (N/	AT)		
Allow inte	nal clients to connect	to the Internet using	g one public IP add	ness.
C Virtual pri Allow rem connect t	vate network (VPN) ac te clients to connect t the Internet using a s	ccess and NAT to this server throug single public IP addr	h the Internet and li ess.	ocal clients to
C Secure c	onnection between tw	o private networks		
Connect t	his network to a remot	e network, such as	a branch office.	
C Custom c	onfiguration			
Select an	combination of the fe	atures available in f	Routing and Remot	e Access.
For more inf	mation			
			_	-

Εικόνα 13. Επιλογή είδους απομεμακρυσμένης υπηρεσίας.

3. Στο επόμενο παράθυρο επιλέγουμε τη συγκεκριμένη υπηρεσία: VPN και μετά: Next.

Routing and Remote Access Server Setup V	Vizard
Remote Access You can set up this server to receive both o	dial-up and VPN connections.
VPN	
A VPN server (also called a VPN gate remote clients through the Internet.	way) can receive connections from
🗖 Dial-up	
A dial-up remote access server can re remote clients through dial-up media, s	ceive connections directly from such as a modem.
For more information	
	< Back Next > Cancel

Εικόνα 14. Επιλογή υπηρεσίας VPN.

4. Στο επόμενο παράθυρο επιλέγουμε από ποια NIC θα συνδέονται οι VPN πελάτες (δλδ. Οι απομεμακρυσμένοι χρήστες) στον RRAS. Εξ ορισμού είναι ενεργοποιημένα τα Στατικά Φίλτρα Πακέτων δεδομένων για μέγιστη ασφάλεια. Αυτά με πολύ "στατικό" τρόπο επιτρέπουν την κυκλοφορία των VPN πακέτων δεδομένων και κανενός άλλου αποκλείοντας έτσι την πρόσβαση στις υπηρεσίες Διαδικτύου των H/Y του LAN. Για τα δεδομένω της άσκησης αφήνουμε την προεπιλογή της ενεργοποίησης των Στατικών Φίλτρων Πακέτων, επιλέγουμε τη NIC που μας ενδιαφέρει και επιλέγουμε: Next.

lect the network i	nterface that connects this se	rver to the Internet.	
Name	Description	IP Address	
External for	/PN Gigabit PCI E	xpress Net 10.67.80.3	10
Finable se Static pac selected in	curity on the selected interfact ket filters allow only VPN traffi iterface. <u>about network interfaces</u> .	e by setting up static packe c to gain access to this sen	t filters. ver through the

Εικόνα 15. Επιλογή NIC σύνδεσης VPN πελατών στον RRAS.

5. Στο επόμενο παράθυρο επιλέγουμε τον τρόπο εκχώρησης των IP διευθύνσεων στους VPN χρήστες. Κατά την προεπιλεγμένη περίπτωση (Automatically) ο DHCP Server του LAN παρέχει αυτές τις διευθύνσεις. Εάν δεν υπάρχει DHCP Server ή εάν δεν θέλουμε να γίνεται η εκχώρηση αυτών των διευθύνσεων από τον DHCP Server επιλέγουμε: From a specified range of addresses και θα πρέπει σε επόμενο στάδιο να καθορίσουμε αυτή τη περιοχή διευθύνσεων. Στη περίπτωση που επιλέξουμε: From a specified range of addresses και υπάρχει και DHCP Server θα πρέπει να ληφθεί πρόνοια για να μην εκχωρούνται ίδιες IP διευθύνσεις. Για τα δεδομένα της άσκησης αφήνουμε την προεπιλογή και επιλέγουμε: Next.

ting and Remote Access Serv	ver Setup Wizard
P Address Assignment You can select the method for	r assigning IP addresses to remote clients.
How do you want IP addresse	s to be assigned to remote clients?
Automatically	
If you use a DHCP server If you do not use a DHCP	to assign addresses, confirm that it is configured properly. server, this server will generate the addresses.
C From a specified range of a	addresses
For more information	
	< Back Next > Cancel

Εικόνα 16. Επιλογή του τρόπου εκχώρησης των ΙΡ διευθύνσεων στους VPN χρήστες.

6. Στο επόμενο παράθυρο επιλέγουμε τον τρόπο πιστοποίησης της αυθεντικότητας των VPN χρηστών. Η προεπιλογή πραγματοποιεί, κατ' ουσία, αυτή την πιστοποίηση μέσω του Ενεργού Καταλόγου (Active Directory) που είναι και η επαρκής για μικρά και απλά δίκτυα. Για πιο μεγάλα και σύνθετα δίκτυα είναι επιβεβλημένη η χρήση των RADIUS servers. Για τα δεδομένα της άσκησης αφήνουμε την προεπιλογή και επιλέγουμε: **Next**.

Connection requests can Authentication Dial-In Use	be authenticated locally or forwarded to a Remote er Service (RADIUS) server for auth <mark>entication.</mark>
Although Routing and Re networks that include mul central authentication.	mote Access can authenticate connection requests, large tiple remote access servers often use a RADIUS server for
If you are using a RADIU: authentication requests to	S server on your network, you can set up this server to forward the RADIUS server.
Do you want to set up this	s server to work with a RADIUS server?
• No, use Routing and	Remote Access to authenticate connection requests
C Yes, set up this server	r to work with a RADIUS server
For more information	
rormore momadon	

Εικόνα 17. Επιλογή του τρόπου αυθεντικοποίησης των VPN χρηστών.

7. Στο επόμενο παράθυρο παρουσιάζονται περιληπτικά οι επιλογές που έχουμε κάνει μέχρι τώρα. Επιλέγουμε: **Finish**.



Εικόνα 18. Περίληψη των επιλογών που έχουμε κάνει.

8. Το επόμενο προειδοποιητικό παράθυρο μας επισημαίνει ότι εφ όσον θέλουμε να αναμεταδίδουμε τα αιτήματα παροχής υπηρεσίας DHCP από τους απομεμακρυσμένους VPN χρήστες, θα πρέπει καθορίσουμε καταλλήλως τις ιδιότητες του DHCP Relay Agent. Επιλέγουμε: OK.



Εικόνα 19. Υπενθύμιση καθορισμού ιδιοτήτων DHCP Relay Agent.

9. Στο επόμενο παράθυρο παρατηρούμε ότι η υπηρεσία Routing and Remote Access είναι ενεργή.



Εικόνα 20. Ενεργοποιημένη υπηρεσία Routing and Remote Access.

Γ. Εγγραφή χρηστών στην υπηρεσία VPN.

1. Η διαδικασία δημιουργίας χρηστών που θα χρησιμοποιούν την υπηρεσία VPN είναι η ίδια με αυτή της δημιουργίας των χρηστών μιας Λογικής Περιοχής Δικτύου που έχουμε δει σε προηγούμενη άσκηση. Μπορούμε επίσης σε υπάρχοντα χρήστη να δώσουμε τη δυνατότητα της απομεμακρυσμένης πρόσβασης π.χ. στον Administrator.

Ανοίγουμε τις ιδιότητες του χρήστη Administrator και επιλέγουμε την ετικέτα (tab) **Dial-in**. Η ετικέτα αυτή δεν υπάρχει αν δεν είναι ενεργή η υπηρεσία Routing and Remote Access (βλέπε την Εικόνα 20).

Member Of	Dial-in	Envir	ronment	Sessions
Remote control	Tem	inal Service	es Profile	COM+
General Address	Account	Profile	Telephone	s Organization
First name:			Initials:	
Last name:				
Display name:	[
Description:	Built-in accou	unt for admir	nistering the o	computer/doma
Office:	<u> </u>			
Telephone number:	[Other,
E-mail:				
				Other
Web page:	1			
Web page:	1.			

Εικόνα 21. Ιδιότητες Administrator.

2. Στο παράθυρο της ετικέτας Dial-in που ανοίγει (Εικόνα 22) φαίνονται τέσσερα διακριτά τμήματα.

Το δεύτερο τμήμα που περιλαμβάνει το Verify Caller-ID και τα Callback Options αφορά την σύνδεση του χρήστη μέσω ISDN ή PSTN με χρήση modem που δεν μας ενδιαφέρει σ΄ αυτή την περίπτωση.

Το τρίτο τμήμα αφορά την εκχώρηση στατικής IP διεύθυνσης στη δικτυακή σύνδεση αυτού του χρήστη που δεν μας ενδιαφέρει σ΄ αυτή την περίπτωση.

Το τέταρτο τμήμα που αφορά τη δημιουργία στατικών δικτυακών οδεύσεων μέσα από το υπόλοιπο δίκτυό μας για τη δικτυακή σύνδεση αυτού του χρήστη που δεν μας ενδιαφέρει σ΄ αυτή την περίπτωση.

	tor Propert	ies		<u> </u>
Remo	te control	Termin	nal Services Profile	COM+
General	Address	Account	Profile Telephones	Organization
Membe	er Of	Dial-in	Environment	Sessions
-Network	Access Perm	nission	ND.	
C Allow	/ access			
C Dem	/ access			
 Cont 	rol access thr	ough NPS Net	work Policy	
☐ Verify	y Caller-ID:			
-Callback	COptions		-	
-				
No (Jallback			
No (Set I	Lallback by Caller (Rou	iting and Remo	ite Access Service only)
No (Set I Alwa	Lailback by Caller (Rou ays Callback t	iting and Remo	te Access Service only)
No C Set I C Alwa	Jailback by Caller (Rou ays Callback t gn Static IP A	iting and Remo o: ddresses	ite Access Service only)
No (Set I C Alwa Define Dial-in (Jaliback by Caller (Rou ays Callback t gn Static IP A IP addresses connection.	iting and Remo o: ddresses to enable for th	nisStatic IP Ad)
No (Set I Alwa Define Dial-in (Apple	allback by Caller (Rou ays Callback t gn Static IP A IP addresses connection. y Static Route	uting and Remo o: ddresses to enable for th	ite Access Service only) dresses

Εικόνα 22. Ετικέτα Dial-in.

Και το πρώτο τμήμα Network Access Permission που αφορά τον τρόπο αδειοδότησης πρόσβασης στο δίκτυό μας για τον συγκεκριμένο χρήστη.

Η προεπιλογή δείχνει ότι δικτυακή πολιτική πρόσβασης καθορίζεται από τον Network Policy Server (NPS). Επειδή δεν θέλουμε να μπλέξουμε με τη δικτυακή πολιτική του NPS

και επειδή δεν θέλουμε να εμποδίσουμε την δικτυακή πρόσβαση (Deny access)

επιλέγουμε: Allow access. (Εικόνα 23)

Remote control Terminal S	Services Profile	COM+
General Address Account Pro	ofile Telephones	Organizatio
Member Of Dial-In	Environment	Sessions
Network Access Permission		
Allow access		
C Deny access		
C Control access through NPS Network	k Policy	
Verify Caller-ID:		
Callback Options	1	1
No Callback		
C Set by Caller (Routing and Remote A	Access Service only)	
C Always Callback to:		
Assign Static IP Addresses		
Define IP addresses to enable for this	Static IP Add	esses
Dial-in connection.		
Apply Static Routes		
Define routes to enable for this Dial-in	Static F	loutes
connection.		
		3

Εικόνα 23. Επίτρεψη πρόσβασης του χρήστη από VPN σύνδεση.

Τέλος επιλέγουμε: OK για να κλείσει το παράθυρο ιδιοτήτων του Administrator.

Δ. Δημιουργία VPN σύνδεσης σε απομεμακρυσμένο Η/Υ (XP) και δοκιμές λειτουργίας.

Το δίκτυό μας τώρα έχει τη μορφή που φαίνεται στην Εικόνα 24.



Εικόνα 24. Τα δίκτυα που διασύνδεει ο R.R.A.S. Server.

Δοκιμαστικά θα δημιουργήσουμε μια VPN σύνδεση σε ένα Η/Υ του δικτύου 10.67.80.0 για να επιτύχουμε VPN επικοινωνία με το δίκτυο 192.1698.1.0.

- Ευρισκόμενοι στην επιφάνεια εργασίας των windows XP του Η/Υ με IP διεύθυνση 10.67.80.176 επιλέγουμε: έναρξη → Πίνακας Ελέγχου → Συνδέσεις Δικτύου. Στο παράθυρο που ανοίγει επιλέγουμε: Δημιουργία νέας σύνδεσης. Ανοίγει το παράθυρο του Οδηγού δημιουργίας σύνδεσης. Επιλέγουμε: Επόμενο.
- 2. Στο παράθυρο που ανοίγει επιλέγουμε: Σύνδεση με το δίκτυο στην εργασία μου και Επόμενο (Εικόνα 25).



Εικόνα 25. Σύνδεση με το δίκτυο στην εργασία μου.

3. Στο παράθυρο που ανοίγει επιλέγουμε: Σύνδεση εικονικού ιδιωτικού δικτύου και Επόμενο (Εικόνα 26).

Οδηγός δημιουργίας σύνδεσης
Σύνδεση στο δίκτυο Πώς θέλετε να συνδεθείτε στο δίκτυο της εργασίας σας;
Δημιουργία της παρακάτω σύνδεσης:
🔿 Σύνδεση μέσω τηλεφώνου
Σύνδεση με χρήση ενός μόντεμ και μιας κανονικής τηλεφωνικής γραμμής ή μιας τηλεφωνικής γραμμής Ψηφιακού δικτύου ενοποιημένων υπηρεσιών (ISDN).
Ο Σύγδεση εικονικού ιδιωτικού δικτύου Σύγδεση στο δίκτυο χρησιμοποιώντας μια σύγδεση εικονικού ιδιωτικού δικτύου (VPN) μέσω του Internet.
< Προηγούμενο Επόμενο > Άκυρο

Εικόνα 26. Σύνδεση εικονικού ιδιωτικού δικτύου.

4. Στο παράθυρο που ανοίγει εισάγουμε ένα όνομα για τη σύνδεση μας π.χ. το όνομα του domain του δικτύου της εταιρείας και επιλέγουμε **Επόμενο** (Εικόνα 27).

Οδηγός δημιουργίας σύνδεσης
Όνομα σύνδεσης Καθορίστε ένα όνομα για αυτήν τη σύνδεση με την εργασία σας.
Πληκτρολογήστε ένα όνομα για αυτήν τη σύνδεση στο ακόλουθο πλαίσιο.
Επωνυμία εταιρείας
Bepal3
Για παράδειγμα, μπορείτε να πληκτρολογήσετε το όνομα της εργασίας σας ή το όνομα ενός διακομιστή στον οποίο θα συνδεθείτε.
< Προηγούμενο Επόμενο > Άκυρο

Εικόνα 27. Ονομα της VPN σύνδεσης.

5. Στο παράθυρο που ανοίγει εισάγουμε την ΙΡ Διεύθυνσης του R.R.A.S. Server και επιλέγουμε Επόμενο (Εικόνα 28).

Οδηγός δημιουργίας σύνδεσης
Επιλογή Διακομιστή VPN Ποιο είναι το όνομα ή η διεύθυνση του διακομιστή VPN;
Πληκτρολογήστε το όνομα ή τη διεύθυνση πρωτοκόλλου Internet (IP) του υπολογιστή στον οποίο συνδέεστε. Όνομα ή διεύθυνση IP κεντρικού υπολογιστή (για παράδειγμα microsoft.com ή 157.54.0.1):
10.67.80.31
< Προηγούμενο Επόμενο > Άκυρο

Εικόνα 28. ΙΡ διεύθυνση του R.R.A.S. Server.

6. Τέλος στο παράθυρο που ανοίγει επιλέγουμε την Προσθήκη συντόμευσης στην επιφάνειας εργασίας και επιλέγουμε: Τέλος (Εικόνα 29).

Οδηγός δημιουργίας σύνδεσης			
Ś	Ολοκλήρωση του "Οδηγού δημιουργίας σύνδεσης" Ολοκληρώσατε με επιτυχία τα απαιτούμενα βήματα για τη δημιουργία της παρακάτω σύνδεσης:		
	 3epal3 Κοινή χρήση με όλους τους χρήστες του υπολογιστή Η σύνδεση θα αποθηκευθεί στο φάκελο "Συνδέσεις Δικτύου". ✓ Προσθήκη συντόμευσης στην επιφάνεια εργασίας Για να δημιουργήσετε τη σύνδεση και να κλείσετε τον οδηγό, κάντε κλικ στο κουμπί "Τέλος". 		
	< Προηγούμενο Τέλος Άκυρο		

Εικόνα 29.

7. Πριν προχωρήσουμε στη προσπάθεια της VPN σύνδεσης ας δούμε πως φαίνονται οι Network Connections του R.R.A.S. Server και του Σταθμού Εργασίας με τη χρήση της εντολής ipconfig/all στο Command Prompt (Εικόνες 30 και 31). Συγκρίνουμε τις σημειούμενες με κίτρινα βέλη IP διευθύνσεις με τις αντίστοιχες της Εικόνας 24.

an Administrator: Command Prompt	_0>
Microsoft Windows [Version 6.0.6002] Copyright (c) 2006 Microsoft Corporation. All rights reserved.	4
C:\Users\Administrator.SERVER3>ipconfig/all	
Vindous IP Configuration	
Host Name	
Ethernet adapter External for UPN :	
Connection-specific DNS Suffix .: Description: Realtek PCIe GBE Family Con Physical Address: Realtek PCIe GBE Family Con Physical Address: No Autoconfiguration Enabled: Yes Link-local IPv6 Address: fo80::c805:1478:1de5:8fb2x1 IPv4 Address: 10.67.80.31(Preferred) Subnet Mask: 10.67.80.1 Default Gateway: 10.67.80.1 DHCPv6 Client DUID: 00-01-00-01-1D-1P-PB-74-	troller 2(Preferred) D4-35-92-C9-06
DMS Servers : ::1	
NetBIOS over Topip Disabled	
Ethernet adapter Internal Network:	
Connection-specific DNS Suffix .: Description	troller Ø <preferred> -D4-35-92-C9-Ø6</preferred>
DNS Servers : ::1 127.0.0.1 NetBIOS over Tcpip : Enabled	
Tunnel adapter Local Area Connection* 8:	
Media State Media disconnected Connection-specific DNS Suffix . : Description : isatap.(FE5B81C4-87EC-4F7E- 843)	A794-3E62DCAC7
Physical Address 00-00-00-00-00-00-00-E0 DHCP Enabled No Autoconfiguration Enabled : Yes	
Tunnel adapter Local Area Connection* 9:	
Media State Media disconnected Connection-specific DNS Suffix escription isatap.{003EB5D1-04D4-4965-	A33B-31A6CAF89
H857 Physical Address	
C:\Users\Administrator.SERVER3>_	

Εικόνα 30. Οι Network Connections του R.R.A.S. Server.

$(C) \Pi v \varepsilon i$	t Windows XP ΓΈκδοση 5.1.2600] ματικά δικαιώματα 1985-2001 Microsoft Corporation
Z:\>ipco 'ipcomf: εκτελέσι	π fig∕all g'δευ αυαγνωρίζεται ως εσωτερική ή εξωτερική εντα∂ή, μο πρόγραμμα ή αρχείο δέσμης ενεργειών.
Z:∖≻ipco	nfig/all
Ρύθμιση	παραμέτρων IP των Windows
Όνομα Επίθημ Τύπος Ενεργο Ενεργο Λίστα	κευτρικού υπολογιστή : LAN5 σ κύριου DNS : 4sek.local κόμβου : Υβριδικός ποίηση δρομολόγησης IP : Όχι ποίηση μεσολόβησης WINS . : Όχι ουσζήτρησης επιθημάτων DNS : 4sek.local
Προσαρμα	γέας Ethernet Τοπική σύνδεση:
Επίθημ Περιγή Φυσικτ Ενεργά Αυτόμα Διεύθα Μάσκα Προεπι Διακομ	α DNS συγκεκρ. σύνδεσης .: σφή: Realtek PCIe GBE Family Controller διεύθυσση : 10-FE-ED-05-E7-48 ποίηση DHCP : Yes τη ρύθμιση ευεργή : Nac υση IP : Nac υση IP : 10.67.80.176 μαδικτύου : 10.67.80.1 υστές DHCP : 10.67.80.1 υστές DHS : 10.67.80.1
Πρωτεί Έναρξι	ων διακομιστής WINS : 10.67.238.1 εκμίσθωσης : Τετόρτη, 7 Οκτωβρίου 2015 7:42:26 ημ ενμίσθωσης : Σάββητη, 7 Οκτωβρίου 2015 7:42:26 ημ

Εικόνα 31. Η Network Connection του Σταθμού Εργασίας.

8. Δοκιμαστικά από το Σταθμό Εργασίας προσπαθήσουμε να συνδεθούμε στον Server που εξυπηρετεί το δίκτυο 192.168.1.0. Επιλέγουμε: έναρξη → Εκτέλεση, εισάγουμε την IP διεύθυνση του Server και επιλέγουμε: OK (Εικόνα 32).

Εκτέλεση ? 🛛
Πληκτρολογήστε το όνομα ενός προγράμματος, φακέλου, εγγράφου ή πόρου Internet και τα Windows θα το ανοίξουν.
"Ауогуµа: [\\192.168.1.10]
ΟΚ Άκυρο Αναζήτηση
🛃 έναρξη

Εικόνα 32. Προσπάθεια σύνδεσης με 192.168.1.10.

Όμως καθώς ο Σταθμός Εργασίας και η NIC του Server στον οποίο θέλουμε να συνδεθούμε βρίσκονται όχι μόνο σε διαφορετικά network segments αλλά και σε διαφορετικά φυσικά δίκτυα εμφανίζεται το μήνυμα της Εικόνας 33.

Εξερεύν	νηση των Windows
8	Δεν είναι δυνατή η πρόσβαση στο \\192.168.1.10. Μπορεί να μην έχετε δικαίωμα να χρησιμοποιήσετε αυτόν τον πόρο δικτύου. Επικοινωνήστε με τον διαχειριστή αυτού του διακομιστή για να διαπιστώσετε εάν έχετε δικαίωμα πρόσβασης.
	Η διαδρομή του δικτύου δεν εντοπίστηκε.
	ОК

Εικόνα 33. Δεν είναι δυνατή η σύνδεση με 192.168.1.10.

Επιλέγουμε: ΟΚ.

9. Για να μπορέσουμε να συνδεθούμε, λοιπόν, με το διαφορετικό αυτό network segment θα πρέπει πρώτα να πραγματοποιήσουμε τη VPN σύνδεση.

Στον Σταθμό Εργασίας κάνουμε double click στο εικονίδιο της συντόμευσης της VPN σύνδεσης 3epal3 και στο παράθυρο που ανοίγει, εισάγουμε Ονομα χρήστη και Κωδικό πρόσβασης στα αντίστοιχα πεδία και επιλέγουμε: Σύνδεση (Εικόνα 34).

Σύνδεση 3epal3	? 🛛
Όνομα χρήστη:	administrator
Κωδικός πρόσβασης:	•••••
πρόσβασης, για τ Ο Μόνον εμένα Ο Οποιονδήποτε Σύνδεση	τους παρακάτω χρήστες: : χρήστη Ακυρο Ιδιότητες Βοήθεια
3epal3	

Εικόνα 34. Εκκίνηση της VPN σύνδεσης.

Στο παράθυρο που ανοίγει και δείχνει την εξέλιξη της σύνδεσης (Εικόνα 35) φαίνονται διάφορα ενδιαφέροντα μηνύματα που αποτελούν αντικείμενο διερεύνησης συνθετότερων ασκήσεων για τα δίκτυα VPN.

Γίνεται σύνδεση με 3epal3								
Σύνδεση στο 10.67.80.31								
	Акиро							

Εικόνα 34. Εξέλιξη της VPN σύνδεσης.

10. Αφού ο Σταθμός Εργασίας συνδέθηκε επιτυχώς, μέσω της VPN σύνδεσης, με τον R.R.A.S. Server ελέγχουμε πάλι τα network connections όπως κάναμε στο βήμα 7. Για τον R.R.A.S. Server βλέπετε την Εικόνα 35 και για τον Σταθμό Εργασίας βλέπετε την Εικόνα 36.

	📾 Administrator: Command Prompt	_ [] ×
	C:\Users\Administrator.SERVER3>ipconfig/all	-
	Windows IP Configuration	
	Host Name : server3 Primary Dns Suffix : 3cpal3.local Node Type : Hybrid IP Routing Enabled : Yes WINS Proxy Enabled : No DNS Suffix Search List : 3cpal3.local	
(Ethernet adapter External for UPN :	
	Connection-specific DNS Suffix .: Description	ed> C9-06
	DNS Servers : ::1 127.0.0.1	
>	NetBIOS over Tepip Disabled Ethernet adapter Internal Network:	
	Connection-specific DNS Suffix .: Description	ed)
	DNS Servers	
U	NetBIOS over Topip Enabled	
Ċ	PPP adapter RAS (Dial In) Interface:	
	Connection-specific DNS Suffix : Description	
	Tunnel adapter Local Area Connection* 8:	
	Media State Media disconnected Connection-specific DNS Suffix . : Description : isatap.(FE5B81C4-87EC-4F7E-A794-3E62	DCAC7
	8937 Physical Address 00-00-00-00-00-00-E0 DHCP Enabled No Autoconfiguration Enabled Yes	
	Tunnel adapter Local Area Connection* 9:	
	Media State Media disconnected Connection-specific DNS Suffix . : Description : isatap.<003EB5D1-04D4-4965-A33B-31A6 A85>	CAF89
	Physical Address	
	Tunnel adapter Local Area Connection* 11:	
	Media State : Media disconnected Connection-specific DNS Suffix . : Description : Microsoft ISATAP Adapter #3	-

Εικόνα 35. Οι Network Connections του R.R.A.S. Server με VPN σύνδεση.

Παρατηρούμε ότι έχουν δημιουργηθεί οι δικτυακές συνδέσεις με χαρακτηριστικό PPP (Point to Point Protocol) (πρωτόκολλο VPN σύνδεσης) (πράσινες αγκύλες). Αυτές οι δικτυακές συνδέσεις συμπεριφέρονται σαν κάρτες δικτύου αφού έχουν πάρει και IP διευθύνσεις (πράσινα βέλη). Προσέξτε ότι αυτές οι IP διευθύνσεις ανήκουν στο δίκτυο 192.168.1.0. Βλέπετε και το παραστατικό σχήμα της Εικόνας 37. Δηλαδή ο Σταθμός Εργασίας έχει ενσωματωθεί το δίκτυο 192.168.1.0 μέσω του δημιουργημένου tunnel.



Εικόνα 36. Οι Network Connections του Σταθμού Εργασίας με VPN σύνδεση.



Εικόνα 37. Τα δίκτυα που διασύνδεει ο R.R.A.S. Server μετά την επιτυχή VPN σύνδεση.

11. Αφού πλέον ο Σταθμός Εργασίας είναι μέρος του δικτύου 192.168.1.0, μπορούμε με τη διαδικασία του βήματος 8. (Εικόνα 32) να συνδεθούμε στον Server που εξυπηρετεί αυτό το δίκτυο. Το αποτέλεσμα φαίνεται στην Εικόνα 38 όπου εμφανίζονται οι κοινόχρηστοι φάκελοι αυτού του Server.

3 192.168.1.10			
Αρχείο Επεξεργασία Προβολή Αγαπημένα	Εργαλεία Βοήθεια		A.
🕝 Πίσω 🔹 🕑 🔹 🏂 🔎 Αναζήτηση	Φάκελοι	🔯 Συγχρονισμός φακέλου	
ຝະບໍ່ອິບvອງ 😼 \\192.168.1.10			💌 🔁 Μετάβαση
Εργασίες δικτύου 🛞	hetlogon)	sysvol	
 Προβολή συνδέσεων δικτύου Ρύθμιση ενός ασύρματου δικτύου για το σπίπ ή για μικρό γραφείο 	vpn	Προγραμματισμένες εργασίες	
 Αναζήτηση στο Active Directory Προβολή εικονιδίων δικτυακών συσκευών UPnP 			
Άλλες θέσεις 🛞			
💑 3epal3			
Συνολικό δίκτυο Ο Χπολογιστής μου			
🕒 Τα έγγραφά μου			
🦦 Εκτυπωτές και φαξ			
Λεπτομέρειες 📀			
4 αντικείμενα			

Εικόνα 38. Ο Σταθμός Εργασίας συνδέθηκε στον Server.

Ε. Δημιουργία VPN σύνδεσης σε απομεμακρυσμένο Η/Υ (win7)

 Κατ' αντιστοιχία προς την προηγούμενη ενότητα Δ και το βήμα 1 αυτής ευρισκόμενοι στην επιφάνεια εργασίας των windows 7 του Η/Υ με IP διεύθυνση 10.67.80.176 επιλέγουμε: Εναρξη → Πίνακας Ελέγχου → Δίκτυο και Internet → Κέντρο δικτύου και κοινής χρήσης → Ρύθμιση νέας σύνδεσης ή δικτύου. Στο παράθυρο που ανοίγει επιλέγουμε: Σύνδεση σε ένα χώρο εργασίας και Επόμενο (Εικόνα 39).



Εικόνα 39. Δημιουργία σύνδεσης σε ένα χώρο εργασίας.

2. Στο επόμενο παράθυρο επιλέγουμε: Χρήση της σύνδεσης μου στο Internet (VPN) (Εικόνα 40).



Εικόνα 40. Χρήση της σύνδεσης μου στο Internet (VPN).

3. Στο παράθυρο που ανοίγει εισάγουμε την ΙΡ Διεύθυνσης του R.R.A.S. Server, δίνουμε ένα σχετικό όνομα προορισμού στην σύνδεση και επιλέγουμε Επόμενο (Εικόνα 41).

🚱 🌆 Σύνδεση σε ένα χώρο :	ργασίας							
Πληκτρολογήστε τη διεύθυνση Internet για σύνδεση								
Ο διαχειριστής του δικτύου σας μπορεί να σας δώσει αυτές τις πληροφορίες.								
Διεύθυνση Internet:	10.67.80.31							
Όνομα προορισμού:	3epal3							
 Χρήση έξυπνης κάρτας Να επιτρέπεται σε άλλα άτομα να χρησιμοποιούν αυτήν τη σύνδεση Αυτή η επιλογή επιτρέπει τη χρήση αυτής της σύνδεσης από οποιονδήποτε έχει πρόσβαση στον υπολογιστή. Να μην γίνει σύνδεση τώρα, μόνο ρύθμισή της ώστε να μπορέσω να συνδεθώ αργότερα 								
	Επόμενο	Άκυρο						

Εικόνα 41. IP διεύθυνση του R.R.A.S. Server και όνομα προορισμού.

4. Εισάγουμε το όνομα και τον κωδικό πρόσβασης του χρήστη στα αντίστοιχα πεδία. Προαιρετικά αν θέλουμε εισάγουμε και το όνομα του τομέα. Τέλος επιλέγουμε: Σύνδεση (Εικόνα 42).

🚱 🌆 Σύνδεση σε ένα χώρο ε	ργασίας
Πληκτρολογήστε το	όνομα χρήστη και τον κωδικό πρόσβασης σας
Ό <u>ν</u> ομα χρήστη:	administrator
<u>Κ</u> ωδικός πρόσβασης:	•••••
<u>Τ</u> ομέας (προαιρετικό):	Εμφάνιση χαρακτήρων Α <u>π</u> ομνημόνευση αυτού του κωδικού πρόσβασης 3EPAL3.LOCAL
	Σύνδεση Άκυρο

Εικόνα 42. Διαπιστευτήρια VPN χρήστη.

5. Στο επόμενο παράθυρο βλέπουμε την εξέλιξη της διαδικασίας της VPN σύνδεσης (Εικόνα 43).

🧼 🌆 Σύνδεση σε ένα χώρο εργασίας	
Σύνδεση στο 3epal3	
N	
Γίνεται επαλήθευση του ονόματος χρήστη και του κωδικού πρόσβασης	j
	αράλειψη Άκυρο

Εικόνα 43. Εξέλιξη της διαδικασίας της VPN σύνδεσης.

ΣΤ. Σύνδεση μέσω Διαδικτύου.

Μέχρι τώρα οι συνδέσεις που δημιουργήσαμε στις ενότητες Δ. και Ε. και οι δοκιμές που κάναμε στην ενότητα Δ. αφορούσαν εργαστηριακές δοκιμές μέσα στα πλαίσια των σχετικών ασκήσεων για δίκτυα Η/Υ.

Θα μπορούσαν να αποτελούν και πραγματικές υλοποιήσεις VPN συνδέσεων εάν αφορούσαν τη διασύνδεση δύο εταιρειών μέσα στο ίδιο κτήριο, ή τη διασύνδεση δύο τμημάτων της ίδιας εταιρείας τα οποία για κάποιο λόγο θέλουν να διατηρήσουν τη σχετική αυτονομία των δικτύων των Η/Υ τους.

Η συνηθέστερη περίπτωση όμως που συμβαίνει στην πραγματικότητα είναι αυτές οι VPN συνδέσεις να πραγματοποιούνται μέσω Διαδικτύου. Σε αυτή την περίπτωση όμως ο VPN χρήστης δεν θα «δει» πρώτα τον R.R.A.S. Server αλλά τον dslmodem/router που διασύνδεει την εταιρεία με το Διαδίκτυο. Σε αυτή τη περίπτωση στο βήμα 5. στης ενότητας Δ. και στο βήμα 3. της ενότητας Ε. θα πρέπει να εισαγθεί η στατική και βέβαια δημόσια IP διεύθυνση που μάλλον θα έχει η εταιρεία.

Στην περίπτωση που η εταιρεία δεν έχει δημόσια στατική IP διεύθυνση και θέλει να κάνει χρήση των VPN συνδέσεων τότε θα πρέπει να κάνει χρήση υπηρεσιών δυναμικού DNS που παρέχουν κάποιες εταιρίες, μάλλον, έναντι αμοιβής. Στη περίπτωση αυτή στα προαναφερθέντα βήματα εισάγουμε τα ονόματα που δηλώσαμε στις εταιρείες παροχής υπηρεσιών δυναμικού DNS. (Περισσότερες πληροφορίες για τη χρήση του δυναμικού DNS μπορείτε να βρείτε στην ενότητα δ της άσκησης: Άλλες δικτυακές εφαρμογές στο site του 4^{ου} Ε. Κ. Γ' ΑΘΗΝΑΣ.

Ανεξάρτητα όμως από το είδος της IP διεύθυνσης του dslmodem/router θα πρέπει να επιτρέψουμε και την όδευση των κατάλληλων δικτυακών ports που αφορούν τις VPN συνδέσεις. Ανάλογα με τον dslmodem/router αυτή η δήλωση των οδεύσεων αναφέρεται ως port forwarding ή Virtual Server. Στην εικόνα 44 (κόκκινη αγκύλη) φαίνεται το port forwarding για διάφορα πρωτόκολλα της VPN επικοινωνίας.

ΟΤΕ												H108NS
Advanced	d Inter		Adva Se	inced tup	Access Management		ess ement	Maintenance			Status	
	Firewall	irewall Rout		NAT	AD	SL	QoS	PortBinding IPv6 Rout		Routing		
Virtual Server		Virtu	al Server for	Single IPs	Accou	nt/ PVC	:0					
	Start End	Protocol Port Number Port Number	TCP ▼ 0 0									
Start Po End Po			al IP Address umber(Local) umber(Local)	: 0.0.0.0 : 0 : 0								
virtual server Listing												
		Rule	Application	Protocol	Start Port	End port	Local IP Address	Start Port Local	End Port Local	Edit	Drop	
		0	IPCAMERA	ALL	8000	8000	10.67.80.100	8000	8000		8	
	_	1	DVR	ALL	8011	8011	10.67.80.101	8011	8011		<u>S</u>	
		2		ALL	1/23	1/23	10.67.80.31	1/23	1/23		No. 1	
	J	4	12TP_1	UDP	4500	4500	10.67.80.31	4500	4500			
)	5	L2TP_3	ALL	1701	1701	10.67.80.31	1701	1701	7	ă	
	li	6	SSTP	ТСР	443	443	10.67.80.31	443	443		Ö	
		7	N/A	N/A	N/A	N/A	N/A	N/A	N/A			
		8	N/A	N/A	N/A	N/A	N/A	N/A	N/A			
	ļ	9	N/A	N/A	N/A	N/A	N/A	N/A	N/A	🌌		
				APPLY	B	ACK	CANCEL					

Εικόνα 44. Port forwarding για πρωτόκολλα VPN επικοινωνίας.

Πάντως το θέμα της επίτρεψης των VPN συνδέσεων είναι λίγο πιο σύνθετο καθώς εμπλέκονται και Πάροχοι Υπηρεσιών Διαδικτύου (ISPs).

Π.χ. από γειτονική σχολική μονάδα καταφέραμε να δημιουργήσουμε VPN σύνδεση με τον δίκτυο 192.168.1.10 δηλώνοντας τη δημόσια στατική IP διεύθυνση του dslmodem/router του 4^{ου} Ε.Κ. Γ' ΑΘΗΝΑΣ στα προαναφερθέντα βήματα σύνδεσης.

Όμως αυτό δεν κατέστει δυνατόν από Η/Υ που ως ISP έχει την WIND. Και οι δύο πάροχοι (ΠΣΔ και WIND) όταν ερωτήθηκαν ισχυρίστηκαν ότι δεν παρεμποδίζουν την VPN επικοινωνία.