UAG - VPN access configuration

As you may already know ForeFront UAG is a solution to publish applications to external users.

It may also be used as VPN access point.

With UAG, you have 2 different ways to enable and configure VPN access:

- SSL Network Tunneling (SSTP)
- SSL Network Tunneling



Mainly, both are working in the same way BUT there is some key differences:

DHCP can not be used with SSL Network Tunneling for providing IP configuration to remote client; you
have to define a static pool as well as the IP configuration (DNS, gateway) – of course, this doesn't
change anything when UAG is working within an array

rom To etwork. Towneling Configuration Enable remote client VPN access General 19° Protocole III IP Address Assignment 18°, User Gro	Add Edit
etwork. Tunneling Configuration Brable renote cliert VPN access General (P. Postocale) III IP Address Assignment R. User Gro	
Specify how IP addresses are allocated to remote VPN client endpoints	roups ts.
C Assign addresses from a static address pool	
Array Member Start Address End Address	- Ad
	32
	Deb

• VPN access can be published through the UAG portal with SSL Network Tunneling (SSTP)

It this post I'll show you how to enable and configure VPN access for portal publication and SSTP connection.

1. Enable VPN access

1.1 Launch the UAG Management console and open the Admin menu and choose Remote Network

Access\SSL Network Tunneling (SSTP)

Admin Messages Help	
Authentication and Authorization Servers Authentication servers Network Evad Patiencing Network Patiencing Network Patiencing Postal Application Authorization	2010
Remote Network Access Event Logs Settings	 \$\$1, Network Tunneling (\$\$TP) \$\$1, Network Tunneling

1.2 Tick the box Enable remote client VPN access

SSL	N	etwork	Tunneling	Configuration
F	~	Enable r	emote client	VPN access

1.3 Select the portal trunk which will host the VPN access – you can't select an HTTP trunk, and define the

number of maximum VPN client allowed

SSL Network Tunneling Configuration
☑ Enable remote client VPN access
🔋 General 🖉 Protocols 🕅 🎛 IP Address Assignment 🕯
Maximum VPN client connections: 5
SSL Tunneling VPN Trunk
Trunk: Porta
Public host name: Portal

1.4 To allow the use of SSTP, tick the check box on the Protocols tab; this will allow end user to manually create a VPN connection (using SSTP)



1.5 Finally, define the IP configuration assignment (static pool or DHCP)

Specify how IP addres	ols 🛄 IP Address Ar	osignment 🔀 User Grou note VPN client endpoints.	PS
C Assign addresses	from a static address p	loci	
Array Member	Start Address	End Address	Add
F Acsign address us	ing DHCP		Advanced
This option is not a	valatie in a multi-servi	er array depkoyment.	

1.5 The last tab (User Group) is to defined which user group is allowed to use VPN connection; this has to be defined if your end user will configure manually the VPN connection (through the Network Center\Connect to a network).

Ok, your UAG is now configured to allow VPN access. Your end user can now created manually the VPN connection on their laptop based on the configuration you will provide to them.

Take in mind that this is a 'classical' VPN client and server configuration. I would recommend to continue with step 2 and inform your end user to use the UAG portal for VPN remote connection.

2. Publish and configure Remote Access through the UAG portal

As shown on step 1, we have enabled VPN access on UAG BUT there is no UAG endpoint policy applied with this step.

To implement and manage specific endpoint policy, you have to publish the remote access to the UAG portal and use it as a connection point.

2.1 Still on the UAG management console, browse to your HTTPS trunk (the one defined during step 1.3) and add an application to the portal and select **Client/Server and legacy – Network Access**



2.2 Follow the application publication wizard (name the application, select an endpoint policy, add to the

portal...)

Don't modify the settings shown during the step 4 (Configure server settings); except if you want to start the

connection when the user logon on

Add Application Wizard		×
Step 2 - Configure App	lication	
Enter an application name application type.	. If you are publishing a generic application, specify the	
Application name:	MIN Access	
	Remote Network Access	
-	, ,	
	-	_
Add Application Wizard	X	
Step 3 - Select Endpo	int Policies	
Access policy:	General Contraction Access	
	Cefault Non Web Application Access	-
	Default Session Access	
Add Application Wizard		X
Step 4 - Configure	e Server Settings	_
		_
6 mm 100	127.0.0.1	
Server:	4000	
Port	the second secon	
Executable:	suprogrammes suprecision Poremonic UP	

F Start the application automatically at user logon

Add Application Wizard		×
Step 5 - Portal Link		
Add a portal and to	ibar Ink	
Portal name:	VPN Access	_
Folder:		
Icon URL:	images/Applicons/NetworkConnector.c	

2.3 Once the application has been published on the portal, open his properties and go to the **Client settings** tab to define how it will work

- Disabled: that's mean NO remote access will be allowed even if you try to connect using 'a manual' VPN connection
- **Basic**: none of the applications that load the LSP or NSP modules are enabled access to configured corporate resources, unless the Forefront UAG SSL Application Tunneling component is running, and at least one tunnel is open
- **Extended**: this mode is identical to the Basic mode, except that Windows services are enabled access to configured corporate resources
- **VPN**: In this mode, the LSP and NSP modules are always active in all applications; that is, access is enabled to configured corporate resources except for the applications listed in the block list

oplication Properties (F	Remote Network Access)	0
Gereral - 5	mm Setreps - Corport Policy O Postal Link - St, Aufre	Cettege
Specify how the Social	Forwarding component is activated on cl	
Socket towarding mode		
C Dudiel		
C Sam		
C Lended		
IF SPN		1000
The Cleve Executable	e server IF addresses, poets and process fol	ei it
ClerifEenstable	5992 Signature	
The Socket Forwarding - Provide LSP) and New modules faces a postform The Mix Isoccel in the '	orsporert uns Virsuch Zuswen Dars hennen Prinder Phyliochiet, Teorem Statistics of lard blackal applications of lard blackal applications	474 274
The Societ Forwarding Provide JJP) and Harr moduli Intere a position to Mark Intere a position UKA evaluation denoting	omponent une Wissold Z Lawer Dar 5 envice PDPI moder Dar 16 of 2 biol of 2 b	2×. 4

After activating the configuration, a remote access application is available through the UAG portal



