How to configure Forefront UAG as a SSTP VPN Server

Abstract

In this article I will show you how to use Forefront UAG to provide VPN clients access to internal resources with a SSTP VPN connection.

Let's begin

Forefront UAG offers different VPN option for mobile users. DirectAccess for anywhere access as a permanent VPN connection for domain joined Windows 7 Ultimate and Enterprise clients, SSTP (Secure Socket Tunneling Protocol) for Windows Vista SP1 and higher clients, and the legacy SSL network Tunneling Server for older clients with Windows XP as the operating system.

To configure Forefront UAG as a SSTP Server start the Forefront UAG management console and click *Admin – Remote Network Access – SSL Network Tunneling* (SSTP).

59	iL Netv	vork Tunneling Co	onfiguration	X						
	🔽 Er	nable remote client V	PN access							
	🔒 G	eneral 🖉 Protoc	ols 🔠 IP Address Assignment 🎎 User Groups							
	Maximum VPN dient connections: 50									
		SSL Tunneling VPN	Trunk							
		Trunk:	webmail							
		Public host name:	webmail.trainer.de							
		Server certificate:	00 1B 48 78 1C 8B 4A 15 47 54 7F 5F E5 F5 5i							
			OK Car	icel						

Figure 1: Enable SSTP

Enable remote client VPN access, specify the maximum number of VPN client connections and select the UAG trunk for which SSTP VPN access should be enabled.

SSTP is enabled

SSL Network Tunneling Configuration	×
Enable remote client VPN access	
🗟 General 🖉 Protocols 🧮 IP Address Assignment 🍇 User Groups	
Select the protocols to use for SSL tunneling.	
Secure Socket Tunneling Protocol (SSTP)	
SSTP encapsulates PPP traffic in an SSL tunnel on Windows operating systems with SSTP support.	
OK Cancel	

Figure 2: SSTP is enabled

On the IP address assignment tab specify how VPN clients should get IP addresses. It is possible to assign addresses from a static IP address pool or from a internal DHCP Server. If you use a static IP address pool, the IP address pool must be different from the IP address ranges assigned to the internal network object on the underlying Forefront TMG Server.

Attention:

In the case of static IP address ranges it is possible to exclude the IP range from the definition of your internal network.

Add IP Address	×
Array member: UAG	ОК
From IP address: 172 . 17 . 100 . 2	Cancel
To IP address: 172 . 17 . 100 . 60	

Figure 3: IP address range for SSTP clients

If you click the *Advanced* button it is possible to manually enter the IP address of DNS and WINS Servers used by the SSTP clients.

Name Resolution	1							×		
Specify the DNS and WINS server IP addresses used for VPN client connections										
O Obtain DNS	Obtain DNS server addresses using DHCP									
	Use the following DNS servers									
Primary:	10		80		16		90			
Secondary:		•		•		•				
Obtain WIN	IS server a	addr	esses	using	g DHC	P				
C Use the fol	owing WII	NS se	ervers	-						
Primary:										
Secondary:										
		[(ок			Cancel			

Figure 4: Name resolution for SSTP clients

On the *User groups* tab it is possible to limit SSTP VPN client access to specific user and usergroups and to specific IP addresses or IP address ranges which clients should be able to access.

Define Remote VPN Client Authorization	×							
Select which IP addresses Active Directory users can access.								
Active Directory user group:								
WIN2012\Chef	Select							
Internal IP address or range:								
IP Addresses	Add Address							
10.80.16.1 - 10.80.16.254	Add Range							
	Edit							
	Delete							
0	Cancel							

Figure 5: Define remote VPN Client Authorization

The next step is to publish the SSTP VPN connection to the portal used by SSTP. Right click the Portal trunk and click *Add Application* and enter the radio button *Client/server and legacy* and select remote Network Access.

Add Application Wizard	×
Step 1 - Select Application	
Select the application you want to publish.	
C Built-in services:	
Portal	
C Web:	
Other Web Application (application specific hostname) 💌	
Client/server and legacy:	
Remote Network Access	
C Browser-embedded:	
Generic Browser-Embedded Application (multiple server 💌	
C Terminal Services (TS)/Remote Desktop Services (RDS):	
RemoteApp 💌	
Quarte	
(Perty Literate	Court 1
< Back Next >	

Figure 6: Publish SSTP to the portal

Enter an application name, an Endpoint access policy and if necessary in Step 4 another port used by Forefront UAG and if the application should be automatically started at user logon to the portal.

Add Application Wizard						
Step 4 - Configure Serve	er Settings					
⚠ Server:	127.0.0.1					
🔔 Port:	6003					
Executable:	Endpoint Components\3.1.0\whlioc.exe					
Arguments:	-srv %localip%:%localport% -egap {Ex					
Start the application aut	tomatically at user logon					
A						
W Help						
		_				
	< Back Next > Cancel					

Figure 7: Configure Server settings

In Step 6 of the wizard it is possible to limit access to the SSTP application in the portal to specific users and user groups.

Add	Application Wizard				×
	Step 6 - Authorization				
	Specify users and groups that can	view and access	the appl	lication via	
	the portal. Authorize all users				
	Users and groups:				
	Name	Allow	View	Deny	_
	,	Add	1	Remove	
@ E	lelp				
		< Back	Next :	>	Cancel

Figure 8: Configure access to the SSTP application

If the wizard has been finished, save and activate the configuration. During the activation process, Forefront UAG/TMG configures the Windows Server Routing and Remote Access component.



Figure 9: RRAS configuration

The UAG activation process also enable SSTP access in the Forefront TMG console.



Figure 10: SSTP in Forefront TMG

Don't be confused that there is no Weblistener configured for SSTP access in the Forefront TMG Management console. Forefront UAG will do the work.

Now it is time to test a SSTP connection from a Windows client. Log on to the Forefront UAG portal and launch the SSTP application.



Figure 11: Launch the SSTP connection

If you are using a certificate from your own Certificate Authority make sure, that the Certificate Distribution Point (CDP) is access able from the Internet, else, the SSTP VPN connection cannot be established, because SSTP requires a CRL check.



Figure 12: SSTP certificate revocation check failed

For testing purposes only it is possible to disable the Certificate revocation check on the client.

On the Windows client computer, open Regedit and create a DWORD value NoCertRevocationCheck under HKLM\System\CurrentControlSet\Services\SSTPSVC\Parameters. Set the value = 1.

The client is now connected with Forefront UAG Remote Network Access.



Figure 13: SSTP connection established

The SSTP connection installs a small application which allows users to get informed about the network connection status or to disconnect the SSTP connection.

Portal Activity	X
Active Connections	
https://webmail.trainer.de:443	Disconnect
	Homepage
4 III >	
Launched Applications	
II. SSTP	
	Exit
	Hide

Figure 14: SSTP client application

The SSTP clients gets an IP address from the static IP address pool configured on the Forefront UAG Server.

Administrator: C:\Windows\system32\cmd.exe									
C:\Users\administrator>ipconfig									
Windows IP Configuration									
PPP adapter UAGSSTPUPN:									
Connection-specific DNS Suffix . :									
IPv4 Address									
Subnet Mask									
Default Gateway 0.0.0.0									
Figure 15: SSTP client IP address									

The Forefront UAG Web Monitor allows you to monitor the SSTP connection

Hicrosoft Forefront Unified A	Access Gateway - W	eb Monitor - In	ternet Explorer						_ & ×
C C C K Microsoft Forefront Unified A X								i ☆ 🕸	
File Edit View Favorites Tools Help									
Web Monitor	User Monito	or - Active	Sessions			Server t	ime: 06/14/2	2014 15:5	i3 🕜
Session Monitor	Trunk: webmail	(S) 🗸							
Current Status	# Lead User		Session ID		Repository	Started At V	Duration	Events	Termina
Active Sessions	1. win2012.serve	er\administrator	B4BF0721-9A99-42F5-B15	7-FF314E3CE25A	DC	06/14/2014 15:49:58	00:03:22	4	8
Statistics	2. win2012.serve	er\administrator	FFAC9DB9-9997-4973-9A8	5-40347334B145	DC	06/14/2014 15:05:30	00:47:50	۹	8
Application Monitor	C Sessio	on Details - Inte	rnet Explorer				_		
Current Status									
Active Sessions	(Sessio	on Details						
Statistics	Lead U	ser: win2012.se	erver\administrator	Session ID: B4	BF0721-9A99-4	2F5-B157-FF314E3CE	25A		
User Monitor	Gene	ral Application	ons Endpoint Informatio	n Parameters					
Current Status									
Active Sessions		General Sess	ion Details						
Statistics		Session Star	rted At	14/06	/2014 15:49:58				
DirectAccess Monitor		Session Dur	ation	00:03	:36				
Current Status		Session Aut	henticated	×					
Active Sessions		Privileged Se	ession	×					
Farm Monitor		User 🔺		Repository		Lead User			
Current Status		win2012.serve	er\administrator	DC		V			
Array Monitor									
Current Status									
Event Viewer									
Svetem									
A Security									
Session									
Application									
V									~
Event Query	<								>

Figure 16: Forefront UAG Web Monitor

Conclusion

In this article I showed you how easy it is to publish a SSTP VPN connection with Forefront UAG for Windows Vista SP1 clients and higher.

Related links

Adding the SSTP Magic to the UAG Charm <u>http://blogs.technet.com/b/edgeaccessblog/archive/2009/07/05/adding-the-sstp-magic-to-the-uag-charm.aspx</u> How to publish a VPN SSTP using your UAG in a HTTPS trunk <u>http://blogs.technet.com/b/tugait/archive/2011/10/12/how-to-publish-a-vpn-sstp-using-your-uag-in-a-https-trunk.aspx</u> Microsoft Forefront UAG – Overview of Microsoft Forefront UAG <u>http://www.isaserver.org/tutorials/Microsoft-Forefront-UAG-Overview-Microsoft-Forefront-UAG.html</u> Forefront UAG technical overview <u>http://technet.microsoft.com/en-us/library/ee690443.aspx</u> Disable SSTP certificate verification check <u>http://support.microsoft.com/kb/947054/en-us</u>