Configuring Forefront TMG client VPN access with NAP

Abstract

This article will show you how to configure Forefront TMG for VPN client access with NAP (Network Access Protection).

Let's begin

In this article I will show you only the required steps to configure Forefront TMG VPN client access for NAP. The article will not cover how to configure Forefront TMG as a VPN Server for VPN client access and for this article I assume that Forefront TMG is correctly configured as a VPN Server so we will cover only the required changes to enable Forefront TMG VPN for NAP. If you want to know more about how to configure Forefront TMG as a VPN Server for VPN client access, read the following article.

Configuring Forefront TMG for VPN access with NAP is a three part process:

- 1) Configure Forefront TMG for VPN with NAP
- 2) Configure the NPS Server for NAP
- 3) Configure the VPN client for NAP

Configure Forefront TMG for VPN with NAP

As mentioned above I assume that Forefront TMG client VPN is already configured and we only have to change the TMG configuration for NAP. Navigate to the VPN properties and to the *Authentication* tab and enable the *EAP* checkbox.

Remote Access Policy (VPN) Properties	×
Access Networks Address Assignment Authentication RADIUS	
Authentication Methods Select the authentication methods used when the remote site gateway or the remote VPN client initiates a connection to Forefront TMG.	, i
Microsoft encrypted authentication version 2 (MS-CHAPv2)	
Extensible authentication protocol (EAP) with smart card or other certificate	ic
For NAP based quarantine, EAP must be configured. Help about configuring EAP	
Microsoft Forefront Threat Management Gateway	X
EAP authenticated users belong to the RADIUS namespace and are not part of the Windows namespace. To apply user-based access rules to these users you can either define a RADIUS user set for them or you can use user mapping to map these users to the Windows namespace. If user mapping is enabled, access rules applied to the Windows users and groups will be applicable to EAP authenticated users.	
ОК Нејр	
OK Cancel Apply	

Figure 1: Enable EAP as a Authentication method in Forefront TMG

Specify the NPS Server with the RADIUS Server component. We only use RADIUS for authentication.

R	emote Access Po	licy (VPN) Propertie	5		×
ļ	Access Networks	Address Assignment	Authentication	RADIUS	
	You can use a RAI site-to-site connec This configuration TMG computer.	DIUS server to authenti ctions. applies to all VPN conne	cate remote use ections made to	ers and this Forefront	P
	✓ Use RADIUS fo	or authentication			Р
	You can use RADI server logs.	US accounting to log VP	N connections ir	n the RADIUS	io
	Use RADIUS fo	or accounting (logging)			II.
	To view or modify	the list of RADIUS	RADIUS	S Servers	l
R	ADIUS Servers				×
	Servers are queried	In the order in which th	ev are listed		
			cy are indea.		_
	Name	Port	Description	Add	
	Name	Port	Description	Add Edit,.,	
	Name	Port	Description	Add Edit Remove	
	Name	Port	Description	Add Edit Remove	
	Name	Port	Description	Add Edit Remove	
	Name This list of RADIUS au	Port RADIUS servers is refer thentication is used.	Description	Add Edit Remove	

Figure 2: Specify the RADIUS Server

Enter the name of the RADIUS Server, the Authentication port (1812 is default and should not be changed), and the Shared Secret (PSK = PreSharedKey), which is used to authenticate the RADIUS client (Forefront TMG) and the RADIUS Server.

Add RADIUS Server				? ×
Type the RADIUS server name of will communicate with this server	r IP addı	ress and d	lefine ho	w Forefront TMG
Server name:	TRAINE	R-DC.TR/	AINER.IN	NTERN
Server description:				
By default, the shared se strongly recommend that configure the shared sec	ecret is e you crea ret on th	mpty. Foi ate a shar e RADIUS	r security ed secre server a	y reasons, we et. Be sure to as well.
Shared secret:				Change
Authentication port:	1812			
The port number used fo authentication port numb	r RADIUS er plus o	S accounti ine.	ng will be	e the
Time-out (seconds):	5			
Always use message authen	ticator			
		ОК		Cancel

Figure 3: Verify Authentication port and enter the Shared secret

After Forefront TMG is configured as a RADIUS client and RADIUS support is activated, enable VPN client Quarantine on the Quarantine tab. If the NPS Server is not located on the Forefront TMG Server activate the Radio button *Quarantine according to RADIUS server policies*, else use the other radio button.

VPN Clients Properties	×	
General Groups Protocols User Mapping Quarantine		
By enabling Quarantine Control, VPN dients connecting to held in the Quarantined VPN Client network until dient con requirements are met and verified. These dients have restricted access based on the policy o they dear quarantine and are moved to the VPN network.	the network are figuration f the network until	
Enable Quarantine Control		
Quarantine according to RADIUS server policies		
Quarantine configuration is not complete. Help about <u>configuring</u> guarantine and NAP.		
O Quarantine VPN clients according to Forefront TMG	policies	
Disconnect quarantined users after (seconds);	0	
Exempt these users from Quarantine Control:		
Name	Add	
	Edit	
	Remove	
OK Cancel	Apply	

Figure 4: Enable VPN Quarantine Control

If you want to exempt specify users from Quarantine control you can add these users here.

Configure the NPS Server for NAP

The most time consuming part to enable Forefront TMG client access for NAP is the configuration of the NPS Server. If the NPS role is not installed on the Server in the internal network, you have to install the role with the Server Manager of Windows Server 2008/R2.

After the NPS role is installed and correctly configured (don't forget to register the NPS Server in Active Directory), configure Forefront TMG as a RADIUS client. Start the NPS Server MMC navigate to the RADIUS clients and Servers node and add the Forefront TMG Server as a RADIUS client as shown in the following screenshot.

Tono 100 circine			
ttings Advanced			
Enable this RADIUS of	ient		
	-1-1		
 Select an existing tem 	plate:		
			_
Name and Address			
Friendly name:			
TMG-EN			
Address (IP or DNS):			
10.80.16.134			Verify
None To manually type a share secret, click Generate. \ secret entered here. Sha	ed secret, click Manual. T You must configure the R ared secrets are case-sen	To automatically ger ADIUS client with th ssitive.	▼ nerate a shared ne same shared
Manual Shared secret:	O Generate		
Manual Shared secret:	C Generate		
Manual Shared secret: Confirm shared secret:	C Generate		
Manual Shared secret: Confirm shared secret:	C Generate		

Figure 5: Add the Forefront TMG Server as a RADIUS client in the NPS Server settings

Don't forget to activate the checkbox that the RADIUS client (the Forefront TMG Server) is NAP-capable.

New RADIUS Client	×
Settings Advanced	
	1
Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.	
Vendor name:	
RADIUS Standard	<u> </u>
Additional Options	
Access-Request messages must contain the Message-Authenticator attribute	
RADIUS client is NAP-capable	
OK Ca	ncel

Figure 6: Don't forget to enable the option that the RADIUS client is NAP-capable

Configure the Windows Security Health Validator to verify at the client that only the Windows Firewall must be activated to gain unrestricted access to the corporate network.

Windows Security Health Valid	lator
Windows 7/Windows Vista Windows XP	Choose policy settings for Windows Security Health Validator
	Use the settings below to define a Windows Security Health Validator policy. Your selections define the requirements for client computers connecting to your network.
	How do I configure a security health policy?
	Firewall Settings
	A firewall is enabled for all network connections
	Antivirus Settings
	☐ An antivirus application is on
	Antivirus is up to date
	Spyware Protection Settings
	☐ An antispyware application is on
	Antispyware is up to date
	Automatic Updates Settings
	OK Cancel

Figure 7: Specify SHV requirements

After we configured the Windows Security Health Validator we have to configure two Health Policies. One Health Policy which makes the VPN client Compliant when the client passes all SHV checks and one Health Policy which makes the VPN client Noncompliant when more than one SHV checks failed. These Health Policies can be used by Network Policies to gain or restrict access for VPN clients.

Create New Health Policy	×
Settinge	
Jeungs	
Configure health policy settings. To enfo Health Policies condition of one or more	proce the health policy, add it to the network policies.
Select an existing template:	
	*
Policy name:	
Compliant	
Client SHV checks:	
Client passes all SHV checks	•
SHVs used in this health policy:	
Name	Setting
Windows Security Health Vali	Default Configuration 🔽
	OK Cancel

Figure 8: Compliant Health Policy

Create New Health Policy		×
Cottingen 1		
Settings		
Configure health policy settings. To enf Health Policies condition of one or mon	orce the health policy, add	l it to the
Select an existing template:		
		T
Policy name:		
NonCompliant		
Client SHV checks:		
Client fails one or more SHV checks		
SHVs used in this health policy:		
Name	Setting	
Windows Security Health Vali	Default Configuration	-
	ОК	Cancel

Figure 9: Noncompliant Health Policy

Next we must create new Network Policies for Compliant and Noncompliant VPN clients. In this article I will only show the required steps for creating a Network Policy for compliant VPN clients.

New Network I	Policy
	Specify Network Policy Name and Connection Type You can specify a name for your network policy and the type of connections to which the policy is applied.
Policy name Compliant Network conn Select the typ type or Vendo select Unspect (Type of ne Unspecifi C Vendor sp 10	e: nection method pe of network access server that sends the connection request to NPS. You can select either the network access server for specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, acified. pecific:
	Previous Next Finish Cancel

Figure 10: New Network Policy

As a condition select Health Policies and select the previously created Compliant Health Policy.

Select condi	tion		×
Select a con	dition, and then clic	k Add.	
Network Ac	cess Protection		
The suc	ntity Type Identity Type cond h as NAP statemer	lition restricts the policy to only clients that can be identified through the specified t of health (SoH).	mechanism,
The sco	-Service Class MS-Service Class pe that matches the	condition specifies that the connecting computer must have an IP address lease f e selected profile name.	from a DHCP
Hea The poli	a lth Policies Health Policies co cy.	ondition restricts the policy to only clients that meet the health criteria specified in t	the health
NA The part NPS	P-Capable Comp NAP-Capable Co icipating in NAP. 1 5.	Health Policies X Select the health policy that you want to enforce. To create a new health policy, click New. Health policies: Compliant New	eof ealth to ✓ Cancel
		OK Cancel	Remove

Figure 11: Select the Compliant Health Policy

Because the VPN client will be NAP compliant when the Windows Firewall is activated we grant full access to the corporate network.

New Network P	Policy
	Specify Access Permission Configure whether you want to grant network access or deny network access if the connection request matches thi policy.
 <u>A</u>ccess grading access <u>A</u>ccess <u>d</u>ered <u>A</u>ccess <u>d</u>ered <u>A</u>ccess is a construction of the second access 	anted ess if client connection attempts match the conditions of this policy. envied ess if client connection attempts match the conditions of this policy. determined by User Dial-in properties (which override NPS policy) env access according to user dial-in properties if client connection attempts match the conditions of this policy.
	Previous Next Einish Cancel

Figure 12: Grant access for compliant clients

As the Authentication method select all enabled and required authentication methods for your environment.

New Network Policy

	_	_	-		
1				х.	
11					
				_	
1.1	-	-		2	
	~			-	-

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

EAP types are negotiated between NPS and the client in the order in v	vhich they are listed.
EAP Types: Microsoft: Protected EAP (PEAP) Microsoft: Secured password (EAP-MSCHAP v2)	Move <u>Up</u> Move Do <u>w</u> n
Add Edit Remove Less secure authentication methods: ✓ ✓ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2) ✓ User can change password after it has expired ✓ Microsoft Encrypted Authentication (MS-CHAP) ✓ User can change password after it has expired ✓ User can change password after it has expired ✓ User can change password after it has expired ✓ User can change password after it has expired ✓ User can change password after it has expired ✓ User can change password after it has expired ✓ Unencrypted authentication (CHAP) ✓ Unencrypted authentication (PAP, SPAP) Aljow clients to connect without negotiating an authentication methods ✓ Perform machine health check only	hod.
	Previous Next Einish Cancel

Figure 13: Select EAP types

Do the same for a Noncompliant Network Policy.

As the next step we must create a Connection Request Policy (CRP) to allow VPN access. As the type of Network Access server select *Remote Access Server (VPN-Dial up)*.

×

New Connection Request Policy

	_	-	-	6	
1				١.	
1				c	
1.5	-		2.4	2	

VPN-access

Specify Connection Request Policy Name and Connection Type You can specify a name for your connection request policy and the type of connections to which the policy is applied. Policy name:

- Network exercise without -
Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server
type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

Type of network access server:
Remote Access Server(VPN-Dial up)
○ <u>V</u> endor specific:
10 =
Previous <u>N</u> ext Einish Cancel

Figure 14: Specify type of Network Access Server

As a condition select the Access Client IPv4 address of the internal Network Interface of the Forefront TMG Server.

elect condition		
Select a condition, and then click A	\dd.	
HCAP		<u> </u>
Location Groups The HCAP Location Grou required to match this pol network access servers (ps condition specifies the Host Credential Authorization Protocol (HCAP) locati icy. The HCAP protocol is used for communication between NPS and some thir (NASs). See your NAS documentation before using this condition.	ion groups d party
User Name		
User Name The user name that is use typically contains a realm	ed by the access client in the RADIUS message. This attribute is a character st n name and a user account name.	ring that
Connection Properties		
Access Client IPv4 Add The Access Client IPv4 Add from the RADIUS client.	Iress address condition specifies the IPv4 address of the Access Client that is reques	sting access
Access Circlin i Vo Au	Access Client IPv4 Address	X
	Specify the IPv4 address of the Access Client. You can use pattern matching syntax.	Cancel
	10.80.16.134	Hemove
	OK Cancel	Cancel

Figure 15: Add the IP address of the TMG Server to the CRP

Authenticate requests go to this Server.

New Connectio	on Request Policy		X
	Specify Con The connection req remote RADIUS se	nection Request Forwarding uest can be authenticated by the local server or it can be forwarded to RADIUS servers in a ver group.	
If the policy co	onditions match the cor	nection request, these settings are applied.	
Forwardin Request	g Connection tication nting	Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication. Authenticate requests on this server Forward requests to the following remote RADIUS server group for authentication: < <u>(not configured>) New</u> Accept users without validating credentials	
		Previous Next Finish Cancel	

Figure 16: Authentication requests are processed locally

As the supported EAP types select a minimum of one configured authentication method on your Forefront TMG Server and at the VPN client.

New Connection Request Policy

			1	1	7	-	-	e	1
		l	l					ł	۱
and the second se		ł						1	

Specify Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP.

\P <u>T</u> ypes:		
/licrosoft: Protected EAP (PEAP) /licrosoft: Secured password (EAP-MSCHAP v2)		Move <u>Up</u> Move Do <u>w</u> n
Add Edit		
ess secure authentication methods:		
Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)	
User can change password after it has expired		
Microsoft Encrypted Authentication (MS-CHAP)		
User can change password after it has expired		
Encrypted authentication (CHAP)		
Unencrypted authentication (PAP, <u>SPAP</u>)		
Allow clients to connect without negotiating an authenticati	on method.	

Figure 17: Select EAP types

In the Protected EAP Properties select the certificate which the Server uses to establish a secure connection with the client. The VPN client must trust the issuing Certificate Authority. You must also enable the checkbox *Enforce Network Access Protection*.

×

Configure Protected EAF	Properties		×
			the deal
This certificate will overrid Remote Access Policy.	server should use to p le the certificate select	ted for Protected E	EAP in
Certificate issued	FEP2010.trainer.int	ern	•
Friendly name:	fep2010.trainer.inte	rn	
Issuer:	RootCA		
Expiration date:	25.12.2011 14:58:5	6	
Enable East Reconnec	t		
Enforce Network Acce	ss Protection		
Eap <u>T</u> ypes			
Secured password (EAP- Smart Card or other certi	4SCHAP v2) ficate		Move <u>U</u> p
			Move <u>D</u> own
<u>A</u> dd Ed it	. <u>R</u> emove	ОК	Cancel

Figure 18: Enforce NAP and select the certificate

Configure the VPN client for NAP

Start *NAPCLCFG.MSC* on the Windows 7 client. This opens the NAP client configuration console. In Windows 7 the NAP VPN client is called the EAP Quarantine Enforcement client. Enable *the EAP Quarantine Enforcement Client* as shown in the following screenshot.

💼 napclcfg - [NAP Client Configuration (Li	ocal Computer	\Enforcement Clients]	
File Action View Help			
🗢 🔿 🗾 🚺 🚺			
RAP Client Configuration (Local Comp	Enforcement	Clients	Actions
C Enforcement Clients	Name	Status	Enforcement Clients
Health Registration Settings	S DHCP Qua	antine Enforcement Client Disabled	View
	Psec Rely	ng Party Disabled	Q Refresh
	Search Gatewa	titine Enforcement Client Disabled	Help
			EAP Ouarantine Enforceme
		EAP Quarantine Enforcement Client Properties	Enable
		General	Refresh
		Enabling the client allows Network Access Protection to be enforced from	Properties
		this device.	Help
		Enable this enforcement client	
	💺 EAP Qu		
	ID:		
	Name:		
	Description:	ted network connection	
	Version:		
	Vendor:		
	Status:		
		OK Cancel Apply	

Figure 19: Enable NAP enforcement on the Windows 7 client

Please note: In Windows Vista the client is called the Remote Access Quarantine Enforcement Client.

Set the startup type of the *Network Access Protection Agent* service to Automatic and start the service.

Services (Local)	🚫 Services (Local)					
	Network Access Protection Agent	Name	Description	Status	Startup Type	Log On As
	Stop the service Restart the service	Microsoft Network Inspection	Helps guard Manages so	Started	Manual Manual	Local Service Local Syste
	Description:	Multimedia Class Scheduler Net.Tcp Port Sharing Service	Enables rela Provides abi Maintains a	Started	Automatic Disabled	Local Syste Local Service
	The Network Access Protection (NAP) agent service collects and	Network Access Protection Agent	The Networ	Started	Automatic	Network S
	manages health information for client computers on a network.	Network Connections	Manages o Identifies th	Started Started	Manual Manual	Local Syste Local Service
	Information collected by NAP agent is used to make sure that the client	Network Location Awareness	Collects an	Started	Automatic	Network S
	computer has the required software and settings. If a client computer is	Offline Files	The Offline	Started	Automatic	Local Syste
	not compliant with health policy, it can be provided with restricted	🤐 Parental Controls	This service Enables serv		Manual Manual	Local Service Local Service
	is updated. Depending on the	Peer Networking Grouping Peer Networking Identity Manager	Enables mul Provides ide		Manual	Local Service
	computers might be automatically	Performance Logs & Alerts	Performanc		Manual	Local Service
	full network access without having to manually update their computer.	🍳 Plug and Play 🍳 PnP-X IP Bus Enumerator	Enables a c The PnP-X	Started	Automatic Manual	Local Syste Local Syste
		NIDD Marking Name Duklinsting Conting	TL:		Maran al	1 1 C

Figure 20: change the service startup type of the NAP client service

Configure the VPN client connection for NAP enforcement

Navigate to the Security tab and select the EAP radio button and click Properties.

VPN Properties
General Options Security Networking Sharing
Type of VPN:
Point to Point Tunneling Protocol (PPTP)
Data encryption:
Require encryption (disconnect if server declines)
Authentication
Use Extensible Authentication Protocol (EAP)
Microsoft: Protected EAP (PEAP) (encryption enabled)
Properties
Allow these protocols
Unencrypted password (PAP)
Challenge Handshake Authentication Protocol (CHAP)
Microsoft CHAP Version 2 (MS-CHAP v2)
Automatically use my Windows logon name and password (and domain, if any)
OK Cancel

Figure 21: Enable EAP for the VPN client

Activate the Checkbox *Enforce Network Access Protection* and the required Authentication Method which depends on the settings in your environment and your Forefront TMG Server settings. Select the Trusted Root Certification Authority which issued the certificate for the NPS Server.

Protected EAP Properties	x
When connectina:	
Validate server certificate	
Validate server cerditate	
Connect to these servers:	_
Trusted Book Contification Authorition	
Class 3 Public Primary Certification Authority	
Microsoft Root Authority	
Microsoft Root Certificate Authority	
V RootCA	
Thawte Timestamping CA	
Do not prompt user to authorize new servers or trusted	
certification authorities.	
Select Authentication Methods	
	_
Secured password (EAP-MSCHAP v2)	
📝 Enable Fast Reconnect	
Enforce Network Access Protection	
Disconnect if server does not present cryptobinding TLV	
Enable Identity Privacy	
OK Cance	

Figure 22: Enforce NAP on the client and select the issuing Root CA

Test the connection. Enable the Windows Firewall on the VPN client and the VPN connection should be successful. After the connection was successful, disconnect the VPN connection and disable the Windows Firewall and try to establish the VPN connection again. Depending on your NPS Server configuration the connection fails or you gain access to the restricted network for unhealthy VPN clients.

Conclusion

In this article I tried to show you in some high level steps how to configure Forefront TMG and the NPS Server for VPN client access with NAP. I hope that this article will give you enough information to create your own NAP environment with Forefront TMG.

Related links

Configuring VPN remote access connections to use NAP based quarantine <u>http://technet.microsoft.com/en-us/library/cc984479.aspx</u> Configuring VPN Client Access on Forefront TMG with NAP Integration <u>http://blogs.technet.com/b/yuridiogenes/archive/2008/09/29/configuring-vpn-client-access-on-forefront-tmg-with-nap-integration.aspx</u> Installing the remote access quarantine tool http://technet.microsoft.com/en-us/library/cc995091.aspx Enabling NAP on VPN clients http://technet.microsoft.com/en-us/library/cc984450.aspx Configuring NAP on the Network Policy Server (NPS) http://technet.microsoft.com/en-us/library/dd182017.aspx