Owner of the content within this article is www.isaserver.org
Written by Marc Grote – www.it-training-grote.de

Microsoft Forefront TMG – Using LDAP and RADIUS authentication

Abstract

In this article I will give you an overview about the various authentication methods in Forefront TMG 2010 and specially the usage of the LDAP and RADIUS authentication in Forefront TMG 2010. We will also cover the pros and cons of the LDAP and RADIUS authentication.

Let's begin

Beginning with ISA Server 2006, Microsoft enhanced the support of various authentication methods. All of these authentication methods are still supported in Forefront TMG 2010. The supported authentication methods are:

- Single sign on (SSO), in which a user authenticates once with ISA Server and can access any number of servers that are behind ISA Server, without reauthenticating.
- Two-factor authentication using forms-based authentication and a client certificate.
- Forms-based authentication support for publishing any Web server.
- Customizable forms for forms-based authentication and forms for mobile clients, and use of per-user-agent authentication schemes.
- Fallback from forms-based authentication to Basic authentication, for non-browser clients.
- Delegation of credentials by using NTLM or Kerberos authentication.
- Kerberos constrained delegation.
- Credentials caching.
- Password management, in which ISA Server can check the status of the user's account and report it to the user. This feature can also be configured to enable users to change their passwords.
- Secure Sockets Layer (SSL) client certificate constraints.
- Ability to assign a different digital certificate to each IP address on a network adapter.
- A new type of forms-based authentication: User name passcode/password, where the passcode is used for ISA Server authentication and the password is used for authentication delegation.
- Support for Active Directory® directory service authentication using the Lightweight Directory Access Protocol (LDAP), allowing Active Directory authentication when ISA Server is in a workgroup, or in a forest other than the one that contains the accounts of the user. ISA Server also supports multi-forest configurations, in which the user can be authenticated on a different set of LDAP servers.
- One-time password support for Remote Authentication Dial-In User Service (RADIUS). In ISA Server 2004, this support was provided for RSA SecurID only.

- Default blocking of authentication delegation

Authentication methods for Web Access and Webserver publishing

The following table lists the various authentication methods for outgoing Web access and Webserver publishing in Forefront TMG 2010:

Authentication method	Web access	Web publishing	Authentication Server
HTTP authentication: Basic	Yes	Yes	Active Directory Domain Services (AD DS) or Remote Authentication Dial-In User Service (RADIUS) Lightweight Directory Access Protocol (LDAP) for incoming requests only
HTTP authentication: Basic	Yes	Yes	AD DS, LDAP, or RADIUS
HTTP authentication: Digest/WDigest	Yes	Yes	AD DS
HTTP authentication: Integrated (NTLM)	Yes	Yes	AD DS
Client certificate	No (requests to upstream proxy server only)	Yes	AD DS
Forms-based authentication	No	Yes	AD DS, LDAP, RADIUS, RADIUS OTP, RSA SecurID

Table 1: Supported authentication methods

If you decide that Forefront TMG shouldn't be a member of an Active Directory domain and you want to create Firewall rules based on Active Directory group membership, the only option you have is to use LDAP or RADIUS. With the help of LDAP or RADIUS, Forefront TMG 2010 can be used to authenticate users against Active Directory.

LDAP authentication

LDAP authentication uses the normal communication channels to communicate with the Active Directory. LDAP uses the following ports:

LDAP = Port 389 TCP
LDAPS = Port 636 TCP
GC = Port 3268 TCP
Source: http://www.iana.org/assignments/port-numbers

If you place Forefront TMG 2010 into a DMZ with a Front- and Backend Firewall you must open the required ports on the Backfirewall.

RADIUS authentication

RADIUS is an industry standard authentication protocol which is also used in various Windows Server versions. RADIUS authenticates users between a RADIUS client and the RADIUS server. A RADIUS client like Forefront TMG 2010 passes information about a user to a designated RADIUS server, the NPS Server role in Windows Server 2008, and then acts on the response that the RADIUS server returns. Communications between the RADIUS client and the RADIUS server are authenticated through the use of a shared secret, which is configured in the RADIUS client properties in the NPS console and in the Forefront TMG 2010 management console.

RADIUS authentication uses the following ports:

RADIUS = Port 1812 TCP
RADIUS accounting = Port 1813 TCP
Source: http://www.iana.org/assignments/port-numbers

For normal RADIUS authentication with a Microsoft RADIUS Server it should not be necessary to use the RADIUS accounting port.

If you place Forefront TMG 2010 into a DMZ with a Front- and Backend Firewall you must open the required ports on the Backfirewall.

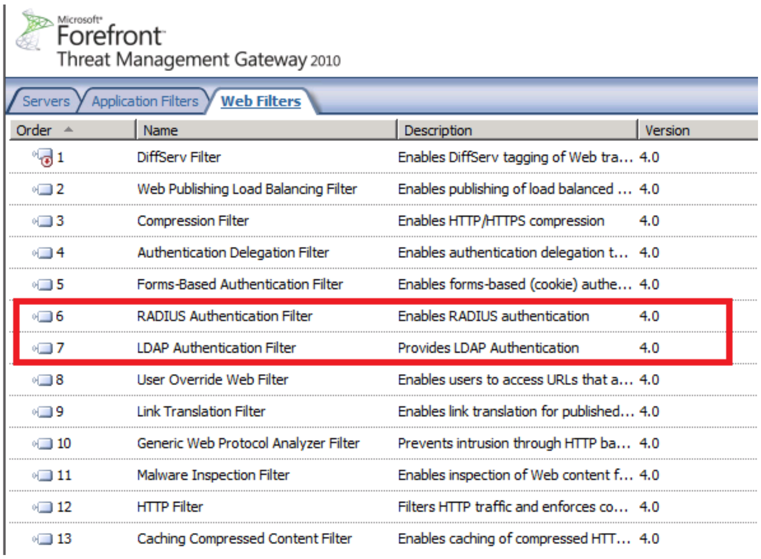
LDAP vs RADIUS

Feature	LDAP	RADIUS
Usage	Only for Webserver publishing (Incoming)	For outgoing Web access and Webserver publishing
Usage of Active Directory Groups and users	Users and Groups	Only user accounts can be used in user sets on TMG
Native Active Directory support	Yes	No, requires NPS (Network Policy Server)
Support for encryption	Yes with LDAPS	Yes with IPSEC
Implementation difficulty	Easy	Medium, requires NPS Server and RADIUS client settings

Forefront TMG 2010 supports LDAP and RADIUS authentication in form of Web filters which allows Forefront TMG to communicate with the Active Directory through LDAP or RADIUS.

Configuring LDAP and RADIUS in Forefront TMG 2010

After some theoretical information about LDAP and RADIUS let us have a look how to configure RADIUS and LDAP authentication in Forefront TMG 2010.



Order	Name	Description	Version
1	DiffServ Filter	Enables DiffServ tagging of Web tra…	4.0
2	Web Publishing Load Balancing Filter	Enables publishing of load balanced …	4.0
3	Compression Filter	Enables HTTP/HTTPS compression	4.0
4	Authentication Delegation Filter	Enables authentication delegation t…	4.0
5	Forms-Based Authentication Filter	Enables forms-based (cookie) authe…	4.0
6	RADIUS Authentication Filter	Enables RADIUS authentication	4.0
7	LDAP Authentication Filter	Provides LDAP Authentication	4.0
8	User Override Web Filter	Enables users to access URLs that a…	4.0
9	Link Translation Filter	Enables link translation for published…	4.0
10	Generic Web Protocol Analyzer Filter	Prevents intrusion through HTTP ba…	4.0
11	Malware Inspection Filter	Enables inspection of Web content f…	4.0
12	HTTP Filter	Filters HTTP traffic and enforces co…	4.0
13	Caching Compressed Content Filter	Enables caching of compressed HTT…	4.0

Figure 1: RADIUS and LDAP Web Filter

Click *Configure (Related) – RADIUS Server settings* to configure TMG 2010 for RADIUS and LDAP.

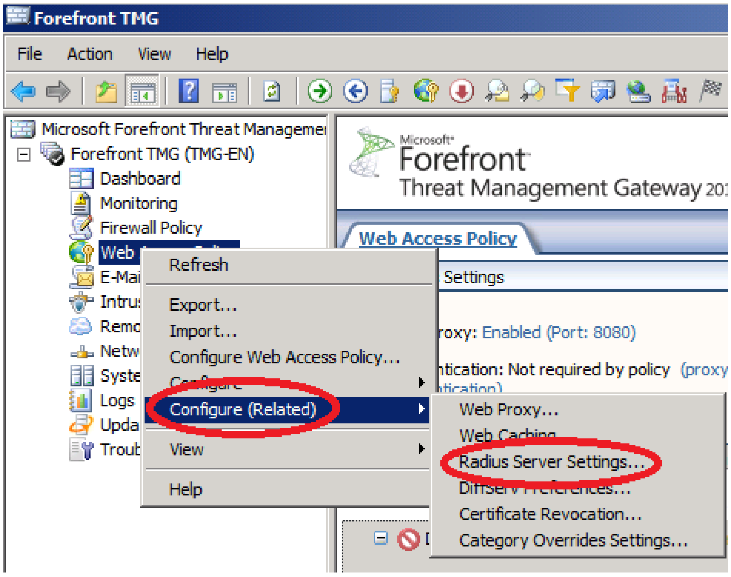
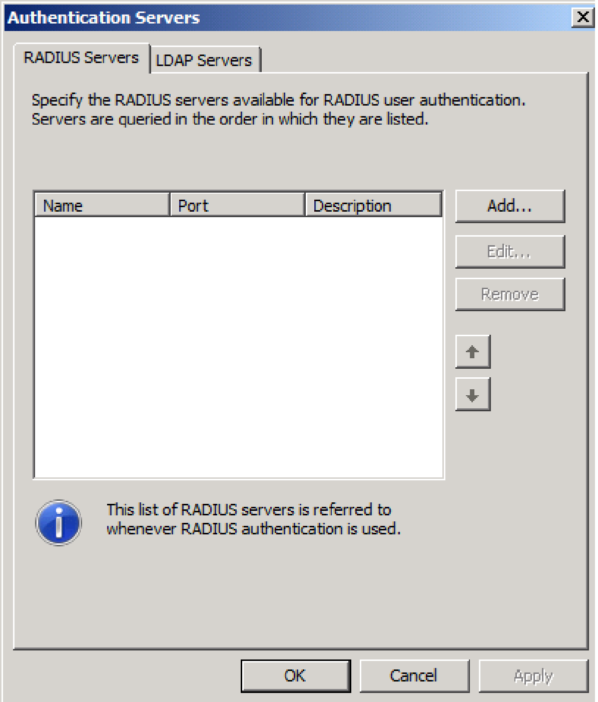


Figure 2: Configure LDAP and RADIUS settings

As a first step specify the RADIUS Server. Microsoft Windows Server 2008 comes with a Server role called Network Policy Server (NPS). One of the NPS functionalities is the support for a RADIUS Server implementation.

Please note: Before you configure Forefront TMG 2010 for RADIUS, you first have to configure Forefront TMG 2010 as a RADIUS client. To do so, start the NPS Server console and add the Forefront TMG 2010 machine as a RADIUS client. You will be asked for the name or IP address of the RADIUS client and you also have to specify the RADIUS shared secret which is used to secure the RADIUS authentication process between the RADIUS Server and the RADIUS client. For additional protection it is possible to enhance the security with the use of IPSEC for RADIUS traffic.


Authentication Servers

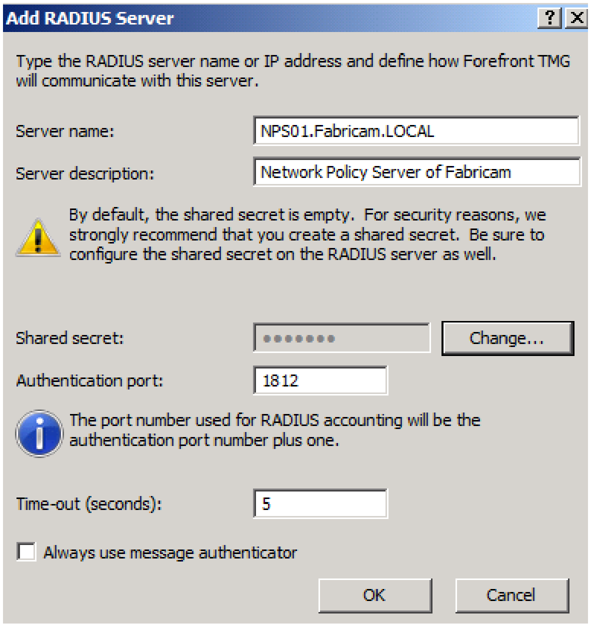
Specify the RADIUS servers available for RADIUS user authentication. Servers are queried in the order in which they are listed.

Name	Port	Description

This list of RADIUS servers is referred to whenever RADIUS authentication is used.

Figure 3: Configure RADIUS Servers

Specify the name of the internal Network Policy Server (NPS) and enter the Shared secret previously used in the RADIUS client settings on the NPS Server.


Add RADIUS Server

Type the RADIUS server name or IP address and define how Forefront TMG will communicate with this server.

Server name: NPS01.Fabricam.LOCAL

Server description: Network Policy Server of Fabricam

By default, the shared secret is empty. For security reasons, we strongly recommend that you create a shared secret. Be sure to configure the shared secret on the RADIUS server as well.

Shared secret: •••••••

Authentication port: 1812

The port number used for RADIUS accounting will be the authentication port number plus one.

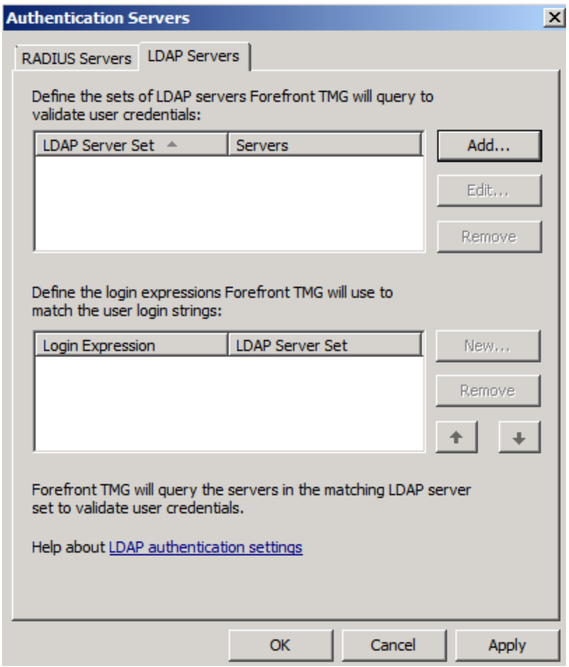
Time-out (seconds): 5

□ Always use message authenticator

Figure 4: Configure NPS Server and Shared Secret

This is all you have to do. Next it is possible to create new Forefront TMG 2010 user sets based on the RADIUS Server settings.

The process for creating LDAP Servers in Forefront TMG 2010 is nearly the same as for RADIUS. Click *Add* to create a new LDAP set.


Authentication Servers

Define the sets of LDAP servers Forefront TMG will query to validate user credentials:

LDAP Server Set	Servers

Define the login expressions Forefront TMG will use to match the user login strings:

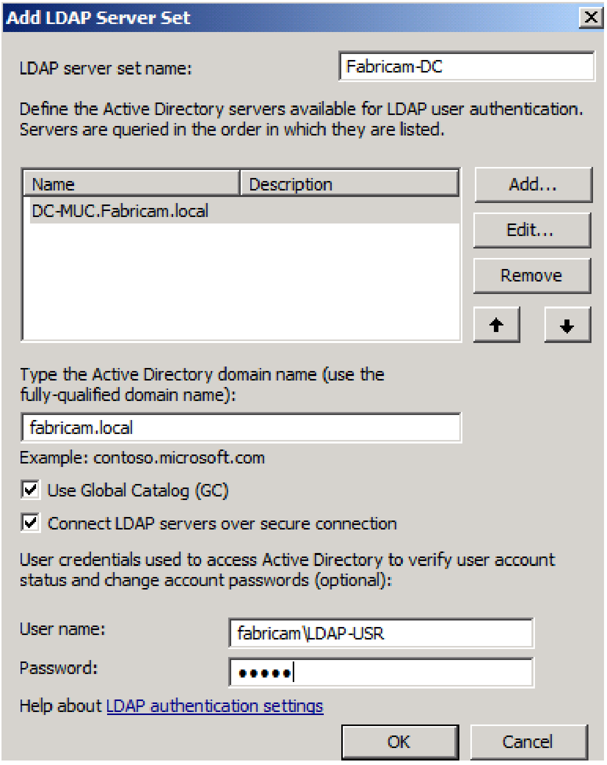
Login Expression	LDAP Server Set

Forefront TMG will query the servers in the matching LDAP server set to validate user credentials.

Help about LDAP authentication settings

Figure 5: Configure LDAP Servers

It is possible to specify more than one LDAP Server. LDAP Servers are grouped into a LDAP set. Add the Active Directory Domain Controller to the LDAP set.


Add LDAP Server Set

LDAP server set name: Fabricam-DC

Define the Active Directory servers available for LDAP user authentication. Servers are queried in the order in which they are listed.

Name	Description
DC-MUC.Fabricam.local	

Type the Active Directory domain name (use the fully-qualified domain name):

fabricam.local

Example: contoso.microsoft.com

☑ Use Global Catalog (GC)

☑ Connect LDAP servers over secure connection

User credentials used to access Active Directory to verify user account status and change account passwords (optional):

User name: fabricam\LDAP-USR

Password: •••••

Help about LDAP authentication settings

Figure 6: Specify LDAP Server and settings

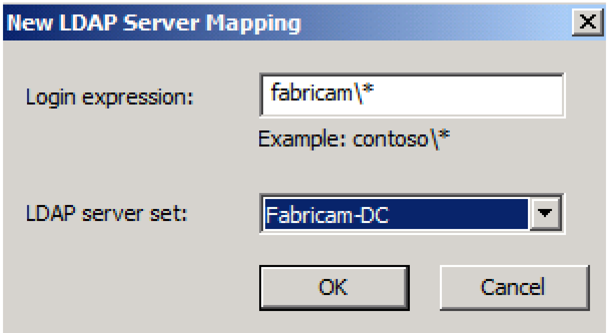
Enable to use the Global Catalog (GC) functionality. If you want to secure the LDAP authentication with LDAPS (Secure LDAP), Forefront TMG must have a valid Server certificate from a trusted Root Certificate Authority, which the Active Directory Domain Controller also trusts.

You must specify a normal user account which has the right to read Active Directory information. I recommend using a dedicated user account for this purpose, which password doesn't expire.

Forefront TMG 2010 has to know in which form user authentication should be presented in form of Login expression. It is possible to specify Login expression in two forms.

NETBIOS-Domain*
*@Domain.TLD.

as shown in the following screenshots. Create the Login Expression and specify the LDAP server set.



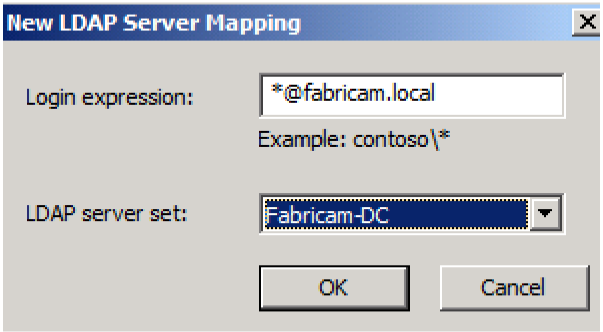
Login expression: fabricam*

Example: contoso*

LDAP server set: Fabricam-DC

Figure 7: Specify LDAP settings for NETBIOS domain

Login Expression for UPN (User Principal Name) authentication.



Login expression: *@fabricam.local

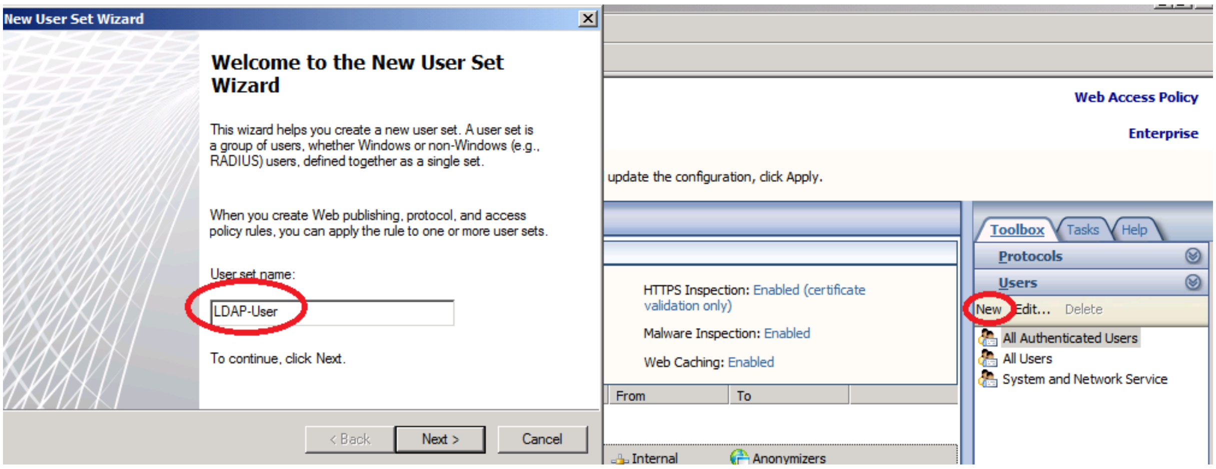
Example: contoso*

LDAP server set: Fabricam-DC

Figure 8: Specify LDAP settings for UPN

After we successfully configured the LDAP and RADIUS Server sets, we can now use Forefront TMG 2010 to create new user sets with the underlying Active Directory user groups and user accounts.

Important: If you use RADIUS you cannot use user sets based on Active Directory Group names, only Active Directory users can be used.



Welcome to the New User Set Wizard

This wizard helps you create a new user set. A user set is a group of users, whether Windows or non-Windows (e.g., RADIUS) users, defined together as a single set.

When you create Web publishing, protocol, and access policy rules, you can apply the rule to one or more user sets.

User set name: LDAP-User

To continue, click Next.

update the configuration, click Apply.

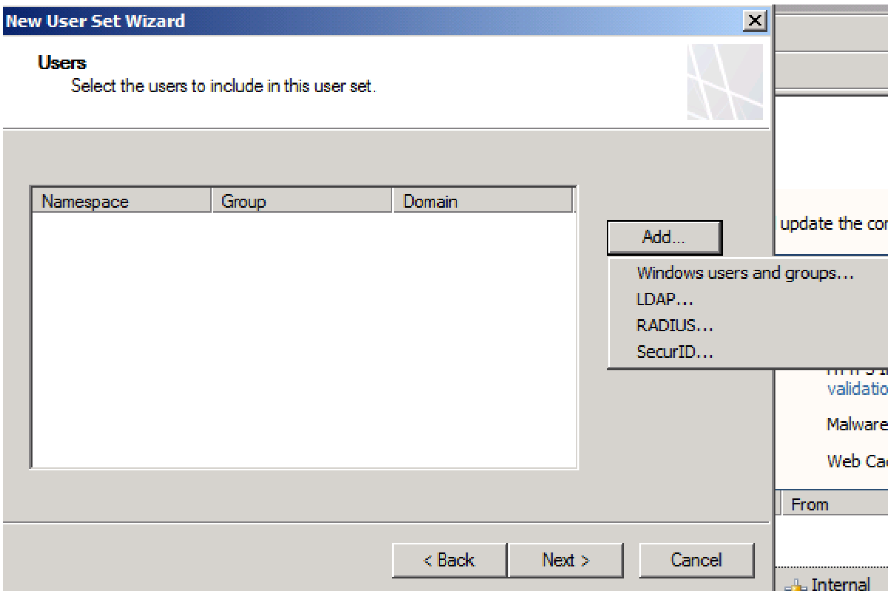
HTTPS Inspection: Enabled (certificate validation only)

Malware Inspection: Enabled

Web Caching: Enabled

Figure 9: Create LDAP User sets

Add Users or groups based on RADIUS or LDAP.

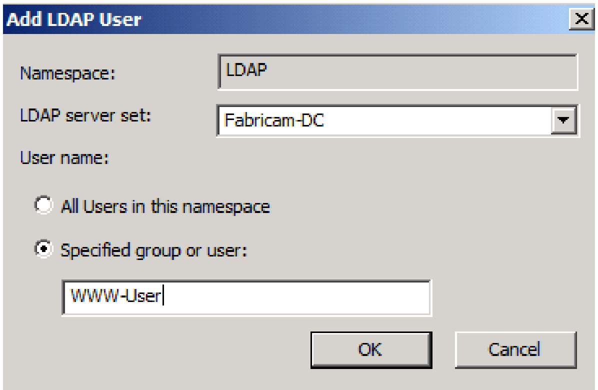


Users

Select the users to include in this user set.

Figure 10: Specify LDAP or RADIUS users

In our example we will add an Active Directory group called WWW-User to the LDAP set. Enter the name of the user group in the LDAP user set in Forefront TMG 2010.



Namespace: LDAP

LDAP server set: Fabricam-DC

User name:

○ All Users in this namespace

● Specified group or user: WWW-User

Figure 11: Select allowed Windows user group for LDAP set

We have successfully created a user set based on LDAP or RADIUS. You can now use the RADIUS user set for outgoing Firewall rules or incoming Webserver publishing rules. Please mention that you can use the LDAP user set only in reverse Proxy scenarios in form of Webserver publishing rules.

Conclusion

In this article I tried to show you the differences between LDAP and RADIUS authentication in Forefront TMG 2010. The article should also help you to decide which authentication method you should use when Forefront TMG 2010 is not a member of an Active Directory domain, but you would like create Firewall rules or Web Publishing rules with user authentication support.

Related links

Configuring LDAP authentication on AD LDS
http://technet.microsoft.com/en-us/library/dd440987.aspx
Configuring RADIUS authentication on NPS
http://technet.microsoft.com/en-us/library/cc441598.aspx
Overview of authentication in Forefront TMG
http://technet.microsoft.com/en-us/library/cc441695.aspx
Authentication in ISA Server 2006
http://technet.microsoft.com/en-us/library/bb794722.aspx