



FortiGate FortiOS v3.0 MR5
User Authentication User Guide



www.fortinet.com

FortiGate FortiOS v3.0 MR5 User Authentication User Guide

05 October 2007

01-30005-0347-20071005

© Copyright 2007 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

Trademarks

ABACAS, APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate, FortiGuard, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiManager, Fortinet, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

Introduction	5
About authentication.....	5
User's view of authentication	5
Web-based user authentication	6
VPN client-based authentication	6
FortiGate administrator's view of authentication	6
Authentication servers.....	7
Public Key Infrastructure (PKI) authentication	8
Peers.....	8
Users.....	8
User groups.....	8
Authentication timeout.....	9
Firewall policies	9
VPN tunnels	9
About this document.....	9
Document conventions.....	10
Typographic conventions.....	10
FortiGate documentation	10
Related documentation	12
FortiManager documentation	12
FortiClient documentation	12
FortiMail documentation	12
FortiAnalyzer documentation	12
Fortinet Tools and Documentation CD	13
Fortinet Knowledge Center	13
Comments on Fortinet technical documentation	13
Customer service and technical support	13
FortiGate authentication servers.....	15
RADIUS servers	15
Configuring the FortiGate unit to use a RADIUS server.....	15
Additional RADIUS request attributes.....	17
LDAP servers	17
Configuring the FortiGate unit to use an LDAP server.....	19
Active Directory servers	21
Configuring the FortiGate unit to use an Active Directory server	22
Active Directory user groups	22

Users, peers, and user groups	25
Users.....	25
Creating local users	25
Creating peer users	27
User groups	30
Protection profiles	30
Creating user groups	31
Active Directory user groups	32
Configuring authenticated access	33
Authentication timeout	33
Authentication protocols	33
Firewall policy authentication	34
Configuring authentication for a firewall policy.....	35
Configuring authenticated access to the Internet.....	36
Firewall policy order	36
VPN authentication.....	38
Authenticating PPTP VPN users.....	38
Authenticating L2TP VPN users	39
Authenticating remote IPSec VPN users using dialup groups	39
Enabling XAuth authentication for dialup IPSec VPN clients.....	41
Index.....	43

Introduction

This section introduces you to the authentication process from the user and the administrators perspective, and provides supplementary information about Fortinet publications.



Note: This document does not describe certificate-based VPN authentication. For information about this type of authentication, see the *FortiGate IPSec VPN Guide* and the *FortiGate Certificate Management User Guide*.

The following topics are covered in this section:

- [About authentication](#)
- [User's view of authentication](#)
- [FortiGate administrator's view of authentication](#)
- [About this document](#)
- [FortiGate documentation](#)
- [Related documentation](#)
- [Customer service and technical support](#)

About authentication

On a FortiGate unit, you can control access to network resources by defining lists of authorized users, called user groups. To use a particular resource, such as a network or a VPN tunnel, the user must:

- belong to one of the user groups that is allowed access
- correctly enter a user name and password to prove his or her identity, if asked to do so

This process is called authentication.

You can configure authentication for:

- any firewall policy with Action set to ACCEPT
- PPTP and L2TP VPNs
- a dialup IPSec VPN set up as an XAUTH server (Phase 1)
- a dialup IPSec VPN that accepts user group authentication as a peer ID

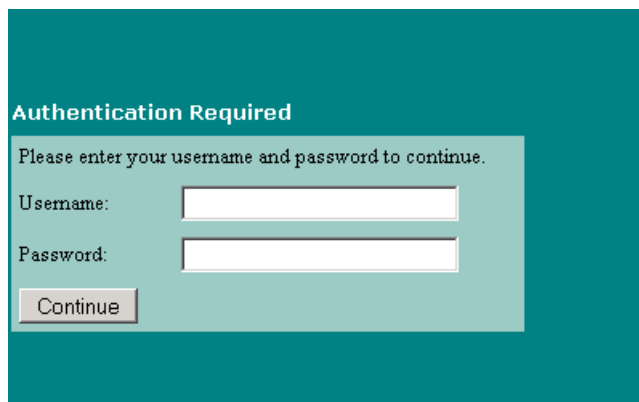
User's view of authentication

The user sees a request for authentication when they try to access a protected resource. The way in which the request is presented to the user depends on the method of access to that resource.

VPN authentication usually controls remote access to a private network.

Web-based user authentication

Firewall policies usually control browsing access to an external network that provides connection to the Internet. In this case, the FortiGate unit requests authentication through the web browser:



The user types a user name and password and then selects Continue. If the credentials are incorrect, the authentication screen is redisplayed with blank fields so that the user can try again. When the user enters valid credentials, they get access to the required resource.



Note: After a defined period of inactivity (the authentication timeout, defined by the FortiGate administrator), the user access will expire. The default is 15 minutes. To access the resource, the user will have to authenticate again.

VPN client-based authentication

VPNs provide remote clients with access to a private network for a variety of services that include web browsing, email, and file sharing. A client program such as FortiClient negotiates the connection to the VPN and manages the user authentication challenge from the FortiGate unit.

FortiClient can store the user name and password for a VPN as part of the configuration for the VPN connection and pass them to the FortiGate unit as needed. Or, FortiClient can request the user name and password from the user when the FortiGate unit requests them.



Note: After a defined period of inactivity (the idle timeout, defined by the FortiGate administrator), the user access will expire. The default is 1500 seconds or 20 minutes. To access the resource, the user will have to authenticate again.

FortiGate administrator's view of authentication

Authentication is based on user groups. You configure authentication parameters for firewall policies and VPN tunnels to permit access only to members of particular user groups. A member of a user group can be:

- a user whose user name and password are stored on the FortiGate unit
- a user whose name is stored on the FortiGate unit and whose password is stored on an external authentication server

- an external authentication server with a database that contains the user name and password of each person who is permitted access

You need to set up authentication in the following order:

- 1 If external authentication is needed, configure the required servers.
 - See [“Configuring the FortiGate unit to use a RADIUS server” on page 15.](#)
 - See [“Configuring the FortiGate unit to use an LDAP server” on page 19.](#)
 - See [“Configuring the FortiGate unit to use an Active Directory server” on page 22.](#)
- 2 Configure local and peer (PKI) user identities. For each local user, you can choose whether the FortiGate unit or an external authentication server verifies the password. Peer members can be included in user groups for use in firewall policies.
 - See [“Creating local users” on page 25.](#)
 - See [“Creating peer users” on page 27.](#)
- 3 Create user groups.

Add local/peer user members to each user group as appropriate. You can also add an authentication server to a user group. In this case, all users in the server's database can authenticate.

 - See [“Creating user groups” on page 31.](#)
- 4 Configure firewall policies and VPN tunnels that require authenticated access.

See [“Configuring authentication for a firewall policy” on page 35.](#)

See [“Authenticating PPTP VPN users” on page 38.](#)

See [“Authenticating remote IPsec VPN users using dialup groups” on page 39.](#)

See [“Enabling XAuth authentication for dialup IPsec VPN clients” on page 41.](#)

Authentication servers

The FortiGate unit can store user names and passwords and use them to authenticate users. In an enterprise environment, it might be more convenient to use the same system that provides authentication for local area network access, email and other services. Users who access the corporate network from home or while traveling could use the same user name and password that they use at the office.

You can configure the FortiGate unit to work with external authentication servers in two different ways:

- Add the authentication server to a user group.

Anyone in the server's database is a member of the user group. This is a simple way to provide access to the corporate VPN for all employees, for example. You do not need to configure individual users on the FortiGate unit.

or

- Specify the authentication server instead of a password when you configure the individual user identity on the FortiGate unit.

The user name must exist on both the FortiGate unit and authentication server. User names that exist only on the authentication server cannot authenticate on the FortiGate unit. This method enables you to provide access only to selected employees, for example.



Note: You cannot combine these two uses of an authentication server in the same user group. If you add the server to the user group, adding individual users with authentication to that server is redundant.

If you want to use external authentication servers, you must configure them before you configure users and user groups.

Public Key Infrastructure (PKI) authentication

A Public Key Infrastructure (PKI) is a comprehensive system of policies, processes, and technologies working together to enable users of the Internet to exchange information in a secure and confidential manner. PKIs are based on the use of cryptography - the scrambling of information by a mathematical formula and a virtual key so that it can only be decoded by an authorized party using a related key. The public and private cryptographic key pair is obtained and shared through a trusted authority. The public key infrastructure enables the creation of a digital certificate that can identify an individual or organization, and directory services that can store and also revoke the certificates.

Public Key Infrastructure (PKI) authentication utilizes a certificate authentication library that takes a list of 'peers', 'peer' groups, and/or user groups and returns authentication 'successful' or 'denied' notifications. Users only need a valid certificate for successful authentication - no username or password are necessary.

Peers

A peer is a user that is a digital certificate holder used in PKI authentication. To use PKI authentication, you must define peers to include in the authentication user group. You create peer identities in the **User > PKI** page of the web-based manager.

Users

You create user identities in the **User > Local** page of the web-based manager. Although it is simpler to define passwords locally, when there are many users the administrative effort to maintain the database is considerable. Users cannot change their own passwords on the FortiGate unit. When an external authentication server is part of an enterprise network authentication system, users can change their own passwords.



Note: Frequent changing of passwords is a good security practice.

User groups

A user group can contain individual users/peers and authentication servers. A user/peer or authentication server can belong to more than one group.

Authentication is group-based. Firewall policies can allow multiple groups access, but authentication for a VPN allows access to only one group. These considerations affect how you define the groups for your organization. Usually you need a user group for each VPN. For firewall policies, you can create user groups that reflect how you manage network privileges in your organization. For example, you might create a user group for each department or create user groups based on functions such as customer support or account management.

You select a protection profile for each user group. Protection profiles determine the level of web filtering, antivirus protection, and spam filtering applied to traffic controlled by the firewall policy to which members of this user group authenticate. For more information about protection profiles, see the *FortiGate Administration Guide*.

Authentication timeout

An authenticated connection expires when it has been idle for a length of time that you specify. The authentication timeout value set in **User > Authentication > Authentication** applies to every user of the system. The choice of timeout duration is a balance between security and user convenience. The default is 5 minutes. For information about setting the authentication timeout, see [“Authentication timeout” on page 33](#).

Firewall policies

Access control is defined in the firewall policy that provides access to the network resource. For example, access to the Internet through the external interface from workstations on the internal network is made possible by an Internal to External firewall policy.

Firewall policies apply web filtering, antivirus protection, and spam filtering to the traffic they control according to a protection profile. When a firewall policy requires authentication, its own protection profile option is disabled and the user group's protection profile is applied.

For more information about firewall policies and protection profiles, see the Firewall chapter of the *FortiGate Administration Guide*.

VPN tunnels

When you configure a PPTP or L2TP VPN, you choose one user group to be permitted access. For IPSec VPNs, you can use authentication by user group or XAUTH authentication using an external authentication server as an alternative to authentication by peer ID.

For more information about VPNs, see the *FortiGate PPTP VPN User Guide*, the *FortiGate SSL VPN User Guide*, or the *FortiGate IPSec VPN User Guide*.

About this document

This document explains how to configure authentication for firewall policies, PPTP and L2TP VPNs, and dialup IPSec VPNs, and contains the following chapters:

- [FortiGate authentication servers](#) contains procedures for configuring RADIUS, LDAP, and Microsoft Active Directory authentication servers.
- [Users, peers, and user groups](#) contains procedures for defining users/peers and user groups.
- [Configuring authenticated access](#) contains procedures to set authentication timeouts, configure authentication in firewall policies and for PPTP and L2TP VPNs and certain configurations of IPSec VPNs.

Document conventions

The following document conventions are used in this guide:

- In the examples, private IP addresses are used for both private and public IP addresses.
- Notes and Cautions are used to provide important information:



Note: Highlights useful additional information.



Caution: Warns you about commands or procedures that could have unexpected or undesirable results including loss of data or damage to equipment.

Typographic conventions

FortiGate documentation uses the following typographical conventions:

Convention	Example
Keyboard input	In the Name field, type <code>admin</code> .
Code examples	<pre>config sys global set ips-open enable end</pre>
CLI command syntax	<pre>config firewall policy edit id_integer set http_retry_count <retry_integer> set natip <address_ipv4mask> end</pre>
Document names	<i>FortiGate SSL VPN User Guide</i>
File content	<code><HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD><BODY><H4>You must authenticate to use this service.</H4></code>
Menu commands	Go to VPN > SSL > Config .
Program output	Welcome!
Variables	<code><group_name></code>

FortiGate documentation

The most up-to-date publications and previous releases of Fortinet product documentation are available from the Fortinet Technical Documentation web site at <http://docs.forticare.com>.

The following [FortiGate product documentation](#) is available:

- *FortiGate QuickStart Guide*
Provides basic information about connecting and installing a FortiGate unit.

- *FortiGate Installation Guide*
Describes how to install a FortiGate unit. Includes a hardware reference, default configuration information, installation procedures, connection procedures, and basic configuration procedures. Choose the guide for your product model number.
- *FortiGate Administration Guide*
Provides basic information about how to configure a FortiGate unit, including how to define FortiGate protection profiles and firewall policies; how to apply intrusion prevention, antivirus protection, web content filtering, and spam filtering; and how to configure a VPN.
- *FortiGate online help*
Provides a context-sensitive and searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.
- *FortiGate CLI Reference*
Describes how to use the FortiGate CLI and contains a reference to all FortiGate CLI commands.
- *FortiGate Log Message Reference*
Available exclusively from the [Fortinet Knowledge Center](#), the FortiGate Log Message Reference describes the structure of FortiGate log messages and provides information about the log messages that are generated by FortiGate units.
- *FortiGate High Availability User Guide*
Contains in-depth information about the FortiGate high availability feature and the FortiGate clustering protocol.
- *FortiGate IPS User Guide*
Describes how to configure the FortiGate Intrusion Prevention System settings and how the FortiGate IPS deals with some common attacks.
- *FortiGate IPSec VPN User Guide*
Provides step-by-step instructions for configuring IPSec VPNs using the web-based manager.
- *FortiGate SSL VPN User Guide*
Compares FortiGate IPSec VPN and FortiGate SSL VPN technology, and describes how to configure web-only mode and tunnel-mode SSL VPN access for remote users through the web-based manager.
- *FortiGate PPTP VPN User Guide*
Explains how to configure a PPTP VPN using the web-based manager.
- *FortiGate Certificate Management User Guide*
Contains procedures for managing digital certificates including generating certificate requests, installing signed certificates, importing CA root certificates and certificate revocation lists, and backing up and restoring installed certificates and private keys.
- *FortiGate VLANs and VDOMs User Guide*
Describes how to configure VLANs and VDOMs in both NAT/Route and Transparent mode. Includes detailed examples.

Related documentation

Additional information about Fortinet products is available from the following related documentation.

FortiManager documentation

- *FortiManager QuickStart Guide*
Explains how to install the FortiManager Console, set up the FortiManager Server, and configure basic settings.
- *FortiManager System Administration Guide*
Describes how to use the FortiManager System to manage FortiGate devices.
- *FortiManager System online help*
Provides a searchable version of the *Administration Guide* in HTML format. You can access online help from the FortiManager Console as you work.

FortiClient documentation

- *FortiClient Host Security User Guide*
Describes how to use FortiClient Host Security software to set up a VPN connection from your computer to remote networks, scan your computer for viruses, and restrict access to your computer and applications by setting up firewall policies.
- *FortiClient Host Security online help*
Provides information and procedures for using and configuring the FortiClient software.

FortiMail documentation

- *FortiMail Administration Guide*
Describes how to install, configure, and manage a FortiMail unit in gateway mode and server mode, including how to configure the unit; create profiles and policies; configure antispam and antivirus filters; create user accounts; and set up logging and reporting.
- *FortiMail online help*
Provides a searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.
- *FortiMail Web Mail Online Help*
Describes how to use the FortiMail web-based email client, including how to send and receive email; how to add, import, and export addresses; and how to configure message display preferences.

FortiAnalyzer documentation

- *FortiAnalyzer Administration Guide*
Describes how to install and configure a FortiAnalyzer unit to collect FortiGate and FortiMail log files. It also describes how to view FortiGate and FortiMail log files, generate and view log reports, and use the FortiAnalyzer unit as a NAS server.
- *FortiAnalyzer online help*
Provides a searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.

Fortinet Tools and Documentation CD

All Fortinet documentation is available from the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For up-to-date versions of Fortinet documentation see the Fortinet Technical Documentation web site at <http://docs.forticare.com>.

Fortinet Knowledge Center

Additional Fortinet technical documentation is available from the Fortinet Knowledge Center. The knowledge center contains troubleshooting and how-to articles, FAQs, technical notes, and more. Visit the Fortinet Knowledge Center at <http://kc.forticare.com>.

Comments on Fortinet technical documentation

Please send information about any errors or omissions in this document, or any Fortinet technical documentation, to techdoc@fortinet.com.

Customer service and technical support

Fortinet Technical Support provides services designed to make sure that your Fortinet systems install quickly, configure easily, and operate reliably in your network.

Please visit the Fortinet Technical Support web site at <http://support.fortinet.com> to learn about the technical support services that Fortinet provides.

FortiGate authentication servers

FortiGate units support the use of authentication servers. If you are going to use authentication servers, you must configure the servers before you configure FortiGate users or user groups that require them. An authentication server can provide password checking for selected FortiGate users or it can be added as a member of a FortiGate user group.

This section describes:

- [RADIUS servers](#)
- [LDAP servers](#)
- [Active Directory servers](#)

RADIUS servers

Remote Authentication and Dial-in User Service (RADIUS) servers provide authentication, authorization, and accounting functions. FortiGate units use the authentication function of the RADIUS server.

Your RADIUS server listens on either port 1812 or port 1645 for authentication requests. You must configure it to accept the FortiGate unit as a client.

The RADIUS server user database can be any combination of:

- user names and passwords defined in a configuration file
- an SQL database
- user account names and passwords configured on the computer where the RADIUS server is installed

The RADIUS server uses a “shared secret” key to encrypt information passed between it and clients such as the FortiGate unit.

See the documentation provided with your RADIUS server for configuration details.

Configuring the FortiGate unit to use a RADIUS server

On the FortiGate unit, the default port for RADIUS traffic is 1812. If your RADIUS server is using port 1645, you can either:

- Reconfigure the RADIUS server to use port 1812. See your RADIUS server documentation for more information.

or

- Change the FortiGate unit default RADIUS port to 1645 using the CLI:

```
config system global
    set radius_port 1645
end
```

To configure the FortiGate unit, you need to know the server's domain name or IP address and its shared secret key.

To configure the FortiGate unit for RADIUS authentication - web-based manager

- 1 Go to **User > RADIUS**.
- 2 Select Create New, enter the following information, and select OK.

Figure 1: Configure FortiGate unit for RADIUS authentication

Name	Name of the RADIUS server.
Primary Server Name/IP	Domain name or IP address of the primary RADIUS server.
Primary Server Secret	Server secret key for the primary RADIUS server.
Secondary Server Name/IP	Domain name or IP address of the primary RADIUS server, if available.
Secondary Server Secret	Server secret key for the secondary RADIUS server.
NAS IP/Called Station ID	IP address used as NAS-IP-Address and Called-Station-ID attribute in RADIUS access requests (RADIUS Attribute 31).
Include in every User Group	Enable to have the RADIUS server automatically included in all user groups.

To configure the FortiGate unit for RADIUS authentication - CLI

```

config user radius
  edit <radius_name>
    set all-usergroup {enable | disable }
    set nas-ip <nas_ip_called_id>
    set secondary-server <secondary_ip_address>
    set secondary-secret <secondary_password>
    set server <ip_address>
    set secret <password>
    set server <ip_address>
  end

```

To remove a RADIUS server from the FortiGate unit configuration - web-based manager

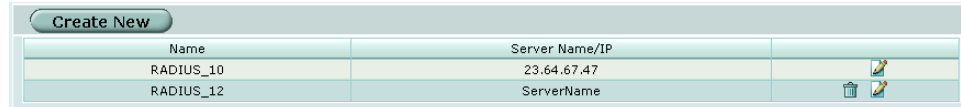


Note: You cannot remove a RADIUS server that belongs to a user group. Remove it from the user group first.

- 1 Go to **User > RADIUS**.

- 2 Select the Delete icon beside the name of the RADIUS server that you want to remove.
- 3 Select OK.

Figure 2: Delete RADIUS server



Name	Server Name/IP	
RADIUS_10	23.64.67.47	
RADIUS_12	ServerName	

To remove a RADIUS server from the FortiGate unit configuration - CLI

```
config user radius
  delete <radius_name>
end
```

Additional RADIUS request attributes

There are several additional attributes that can be added to RADIUS authentication requests via the CLI only. They include:

use-management-vdom	Enable to use the management VDOM to send all RADIUS requests.
use-group-for-profile	Enable to use the RADIUS group attribute to select the protection profile.

For more information, refer to the [FortiGate CLI Reference](#).

LDAP servers

Lightweight Directory Access Protocol (LDAP) is an Internet protocol used to maintain databases of user names, passwords, email addresses, and other information.

The scale of LDAP servers ranges from big public servers such as BigFoot and Infospace, to large organizational servers at universities and corporations, to small LDAP servers for workgroups. This document focuses on the institutional and workgroup applications of LDAP.

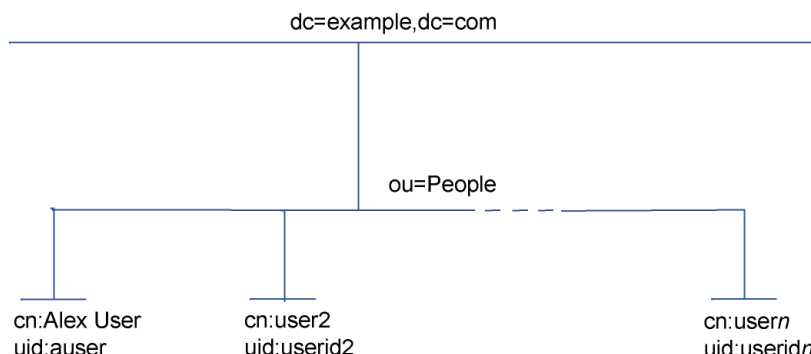
The FortiGate unit supports LDAP protocol functionality as defined in RFC 2251 for looking up and validating user names and passwords. FortiGate LDAP supports all LDAP servers compliant with LDAP v3.

FortiGate LDAP does not support proprietary functionality, such as notification of password expiration, which is available from some LDAP servers. FortiGate LDAP does not supply information to the user about why authentication failed.

To configure your FortiGate unit to work with an LDAP server, you need to understand the organization of the information on the server.

The top of the hierarchy is the organization itself. Usually this is defined as Domain Component (DC), a DNS domain. If the name contains a dot, such as "example.com", it is written as two parts: "dc=example,dc=com".

In this example, Common Name (CN) identifiers reside at the Organization Unit (OU) level, just below DC. The Distinguished Name (DN) is `ou=People,dc=example,dc=com`.



In addition to the DN, the FortiGate unit needs an identifier for the individual person. Although the FortiGate unit GUI calls this the Common Name (CN), the identifier you use is not necessarily CN. On some servers, CN is the full name of a person. It might be more convenient to use the same identifier used on the local computer network. In this example, User ID (UID) is used.

You need to determine the levels of the hierarchy from the top to the level that contains the identifier you want to use. This defines the DN that the FortiGate unit uses to search the LDAP database. Frequently used distinguished name elements include:

- pw (password)
- cn (common name)
- ou (organizational unit)
- o (organization)
- c (country)

One way to test this is with a text-based LDAP client program. For example, OpenLDAP includes a client, `ldapsearch`, that you can use for this purpose.

Enter the following command:

```
ldapsearch -x '(objectclass=*)'
```

The output is lengthy, but the information you need is in the first few lines:

```
version: 2

#
# filter: (objectclass=*)
# requesting: ALL
#

dn: dc=example,dc=com
dc: example
objectClass: top
objectClass: domain

dn: ou=People,dc=example,dc=com
ou: People
objectClass: top
objectClass: organizationalUnit

...

dn: uid=auser,ou=People,dc=example,dc=com
uid: auser
cn: Alex User
```

Configuring the FortiGate unit to use an LDAP server

After you determine the common name and distinguished name identifiers and the domain name or IP address of the LDAP server, you can configure the server on the FortiGate unit.

To configure the FortiGate unit for LDAP authentication - web-based manager

- 1 Go to **User > LDAP**.
- 2 Select Create New, enter the following information, and select OK.

Figure 3: Configure FortiGate unit for LDAP authentication

New LDAP Server	
Name	<input type="text"/>
Server Name/IP	<input type="text"/>
Server Port	636
Common Name Identifier	cn
Distinguished Name	<input type="text"/>
Secure Connection	<input checked="" type="checkbox"/>
Protocol	<input checked="" type="radio"/> LDAPS <input type="radio"/> STARTTLS
Certificate	Fortinet_CA
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Figure 4: LDAP server Distinguished Name Query tree

LDAP Distinguished Name Query	
LDAP Server: 172.20.120.102:389	
Name	Entries
▼ dc=fortinet,dc=com	1 Entries
▶ ou=People	54 Entries
Distinguished Name: dc=fortinet,dc=com	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Name	Type the name of the LDAP server.
Server Name/IP	Type the domain name or IP address of the LDAP server.
Server Port	The port used to communicate with the LDAP server. By default, LDAP uses port 389. Note: If you use a secure LDAP server, the default port will reflect your selection in Protocol.
Common Name Identifier	Type the common name identifier for the LDAP server. 20 characters maximum. The common name identifier for most LDAP servers is cn. However some servers use other common name identifiers such as uid.
Distinguished Name	Type the distinguished name used to look up entries on the LDAP server. Enter the base distinguished name for the server using the correct X.500 or LDAP format. The Fortinet unit passes this distinguished name unchanged to the server. For example, you could use the following base distinguished name: ou=marketing,dc=fortinet,dc=com where ou is organization unit and dc is domain component. You can also specify multiple instances of the same field in the distinguished name, for example, to specify multiple organization units: ou=accounts,ou=marketing,dc=fortinet,dc=com
Query icon	View the LDAP server Distinguished Name Query tree for the base Distinguished Name. The LDAP Distinguished Name Query list displays the LDAP Server IP address, and all the distinguished names associated with the Common Name Identifier for the LDAP server. The tree helps you to determine the appropriate entry for the DN field. Expand the Common Name identifier to see the associated DNs. Select the DN from the list. The DN you select is displayed in the Distinguished Name field. Select OK and the Distinguished Name you selected will be saved in the Distinguished Name field of the LDAP Server configuration. To see the users within the LDAP Server user group for the selected Distinguished Name, expand the Distinguished Name in the LDAP Distinguished Name Query tree.
Secure Connection	Select to use a secure LDAP server connection for authentication.
Protocol	Select a secure LDAP protocol to use for authentication. Depending on your selection, the value in Server Port will change to the default port for the selected protocol.
Certificate	Select a certificate to use for authentication from the drop-down list. The certificate list comes from CA certificates at VPN > Certificates > CA Certificates .

To configure the FortiGate unit for LDAP authentication - CLI

```
config user ldap
edit <name>
    set cnid <common_name_identifier>
    set dn <distinguished_name>
    set server <ip_address>
end
```



To remove an LDAP server from the FortiGate unit configuration - web-based manager



Note: You cannot remove a LDAP server that belongs to a user group. Remove it from the user group first.

- 1 Go to **User > LDAP**.
- 2 Select the Delete icon beside the name of the LDAP server that you want to remove.
- 3 Select OK.

Figure 5: Delete LDAP server

Create New					
Name	Server Name/IP	Port	Common Name Identifier	Distinguished Name	
LDAP_1	2.2.2.2	389	cn	ou=accounts,ou=marketing,dc=fortinet,dc=com	
LDAP_2	1.32.4.5	389	cn	ou=shipping,dc=fortinet,dc=com	

To remove an LDAP server from the FortiGate unit configuration - CLI

```
config user ldap
delete <name>
end
```

Active Directory servers

The Active Directory server stores information about network objects, such as users, systems, and services, on Microsoft Windows networks. Active Directory servers first became available with the Windows 2000 Server.

On networks that use Windows Active Directory (AD) servers for authentication, FortiGate units can transparently authenticate users without asking them for their user name and password.

You must install the Fortinet Server Authentication Extensions (FSAE) on the network domain controllers, and configure the FortiGate unit to retrieve information from the Windows AD server.

The FSAE has two components:

- A domain controller agent that must be installed on every domain controller to monitor user logons and send information about them to the collector agent.
- The collector agent that is installed on at least one domain controller to send the information received from the DC agent to the FortiGate unit.



Note: You can create a redundant configuration on your FortiGate unit if you install a collector agent on two or more domain controllers. If the current collector agent fails, the FortiGate unit switches to the next one in its list of up to five collector agents.

For more information about FSAE, see the *FSAE Technical Note*.

Configuring the FortiGate unit to use an Active Directory server

To configure the FortiGate unit for Active Directory server authentication - web-based manager

- 1 Go to **User > Windows AD**.
- 2 Select Create New, enter the following information, and select OK.

Figure 6: Configure FortiGate unit for Active Directory server authentication

New			
Name	WindowsAD_Server		
FSAE Collector IP	172.20.120.52	Port	8000
		Password	*****
FSAE Collector IP		Port	8000
		Password	
FSAE Collector IP		Port	8000
		Password	
FSAE Collector IP		Port	8000
		Password	
FSAE Collector IP		Port	8000
		Password	

OK Cancel

Name	Name of the Active Directory server. This name appears in the list of Windows AD servers when you create user groups.
FSAE Collector IP	IP address of the Active Directory server on which the FSAE collector agent is installed. You can specify up to five Windows AD servers on which you have installed a collector agent.
Port	TCP port used to communicate with the Active Directory server. Default is 8000. This must be the same as the FortiGate 'listening port' specified in the FSAE collector agent configuration.
Password	Authentication password generated by administrator for FSAE collector agent. This is only required if you configured your FSAE collector agent to require authenticated access.

Active Directory user groups

You cannot use Active Directory groups directly in FortiGate firewall policies. You must add Active Directory groups to FortiGate user groups.



Note: An Active Directory group should belong to only one FortiGate user group. If you assign it to multiple FortiGate user groups, the FortiGate unit only recognizes the last user group assignment.

To create an Active Directory user group

- 1 Go to **User > User Group**.
- 2 Select Create New, enter the following information, and select OK.

Figure 7: New User Group dialog box

The dialog box is titled "New User Group". It contains the following fields and controls:

- Name:** A text input field containing "New_AD_Group".
- Type:** A dropdown menu set to "Active Directory".
- Protection Profile:** A dropdown menu set to "unfiltered".
- Available Users:** A list box containing:
 - Active Directory groups -
 - DOCTEST/Documentation
 - DOCTEST/Domain Guests
 - DOCTEST/Engineering
 - DOCTEST/Sales
- Members:** A list box containing:
 - Active Directory groups -
 - DOCTEST/Developers
- Navigation:** Two green arrow buttons (right and left) between the Available Users and Members lists.
- Buttons:** "OK" and "Cancel" buttons at the bottom.

Name	Name of the Active Directory user group.
Type	Type of user group. Select Active Directory.
Protection Profile	Select the required protection profile from the list.
Available Users	Available Active Directory user groups. Select the groups you require and use the green right arrow to move your selection to the Members column.
Members	The list of Active Directory users that belong to the user group.
Right arrow button	Add a user to the Members list. Select a user in the Available Users list and select the right arrow button to move it to the Members list.
Left arrow button	Remove a user from the Members list. Select a user name in the Members list and select the left arrow button to move it to the Available Users list.

To view the domain and group information that the FortiGate unit receives from the AD server.

- 1 Go to **User > Windows AD**.
- 2 Use the blue right arrow to expand the details for the Active Directory server.

Figure 8: Domain and group information received from Active Directory server

The screenshot shows the "Windows AD" configuration page. It includes a "Create New" button and a table of configured servers:

Name	FSAE Collector IP	Actions
HQ_ADserver	192.168.1.5:8000	[Icons]
OurADS	172.20.120.52:8000	[Icons]
DOCTEST		
Developers		
Documentation		
Domain Guests		
Engineering		
Sales		

Create New	Add a new Windows AD server.
Name	The name of the Windows AD server with FSAE. You can expand the server name to display Windows AD domain group information.

FSAE Collector IP	The IP addresses and TCP ports of up to five collector agents that send Windows AD server logon information to the Fortinet unit.
Delete icon	Delete this Windows AD server.
Edit icon	Edit this Windows AD server.
Refresh icon	Get current domain and group information from the Windows AD server.

To remove an Active Directory server from the FortiGate unit configuration - web-based manager



Note: You cannot remove an Active Directory server that has been added to a user group. Remove it from the user group first.

- 1 Go to **User > Windows AD**.
- 2 Select the Delete icon beside the server name that you want to delete.
- 3 Select OK.

Users, peers, and user groups

Authentication is based on user groups. First you configure users/peers, then you create user groups and add users/peers to them.

This section describes:

- [Users](#)
- [User groups](#)

Users

A user is a user/peer account configured on the FortiGate unit and/or on an external authentication server. Users can access resources that require authentication only if they are members of an allowed user group.

Table 1: How the FortiGate unit authenticates different types of users

User type	Authentication
Local user with password stored on the FortiGate unit	The user name and password must match a user account stored on the FortiGate unit.
Local user with password stored on an authentication server	The user name must match a user account stored on the FortiGate unit and the user name and password must match a user account stored on the authentication server associated with that user.
Authentication server user	Any user with an identity on the authentication server can authenticate on the FortiGate unit by providing a user name and password that match a user identity stored on the authentication server.
Peer user with certificate authentication	A peer user is a digital certificate holder that authenticates using a client certificate.

This section describes how to configure local users and peer users. For information about configuration of authentication servers see [“FortiGate authentication servers” on page 15](#).

Creating local users

To define a local user you need:

- a user name
- a password or the name of an authentication server that has been configured on the FortiGate unit

If the user is authenticated externally, the user name on the FortiGate unit must be identical to the user name on the authentication server.

To create a local user - web-based manager

- 1 Go to **User > Local**.
- 2 Select Create New.

- 3 Enter the user name.
- 4 Do one of the following:
 - To authenticate this user locally, select Password and type a password.
 - To authenticate this user using an LDAP, select LDAP and select the server name.
 - To authenticate this user using a RADIUS server, select RADIUS and select the server name.

If you want to use an authentication server, you must configure access to it first. See [“FortiGate authentication servers” on page 15](#).







- 5 Select OK.

User Name	Type or edit the user name.
Disable	Select Disable to prevent this user from authenticating.
Password	Select Password to authenticate this user using a password stored on the Fortinet unit. Type or edit the password. The password should be at least six characters long.
LDAP	Select LDAP to authenticate this user using a password stored on an LDAP server. Select the LDAP server from the drop-down list. Note: You can only select an LDAP server that has been added to the FortiGate LDAP configuration.
RADIUS	Select RADIUS to authenticate this user using a password stored on a RADIUS server. Select the RADIUS server from the drop-down list. Note: You can only select a RADIUS server that has been added to the FortiGate RADIUS configuration.

Figure 9: Local user configuration

Create New	Add a new local user account.
User Name	The local user name.
Type	The authentication type to use for this user.
Delete icon	Delete the user. Note: The delete icon is not available if the user belongs to a user group.
Edit icon	Edit the user account.

Figure 10: Local user list

Create New		
User Name	Type	
User1	LOCAL	 
User2	RADIUS	 
User3	LDAP	 

To create a local user - CLI

```
config user local
  edit <user_name>
    set type password
    set passwd <user_password>
  end
```

or

```
config user local
  edit <user_name>
    set type ldap
    set ldap_server <server_name>
  end
```

or





```
config user local
  edit <user_name>
    set type radius
    set radius_server <server_name>
  end
```

To delete a user from the FortiGate unit configuration - web-based manager

Note: You cannot delete a user that belongs to a user group that is part of a firewall policy. Remove it from the user group first.

- 1 Go to **User > Local**.
- 2 Select the Delete icon beside the name of the user that you want to remove.
- 3 Select OK.

Figure 11: Delete local user

User Name	Type	
ADUser	LOCAL	
LDAP	LDAP	
SSL	LOCAL	 

To delete a user from the FortiGate unit configuration - CLI

```
config user local
  delete <user_name>
end
```

Creating peer users

A peer user is a digital certificate holder that can use PKI authentication. To use PKI authentication, you must define peers to include in the authentication user group that is incorporated in the authentication policy.

To define a peer user you need:

- a peer user name
- the text from the subject field of the certificate of the authenticating peer user, or the CA certificate used to authenticate the peer user.

To create a peer user for PKI authentication- web-based manager

- 1 Go to **User > PKI**.
- 2 Select **Create New**, enter the following information, and select **OK**.

Name Enter the name of the PKI user. This field is mandatory.

Subject Enter the text string that appears in the subject field of the certificate of the authenticating user. This field is optional.

CA Enter the CA certificate that must be used to authenticate this user. This field is optional.

Figure 12: PKI user configuration



Note: Even though **Subject** and **CA** are optional fields, one of them must be set. The following fields in the PKI User dialog correspond to the noted fields in the PKI User List:

Name: User Name
Subject: Subject
Issuer: CA (CA certificate)

Create New Add a new PKI user.

User Name The name of the PKI user.

Subject The text string that appears in the subject field of the certificate of the authenticating user.

Issuer The CA certificate that is used to authenticate this user.

Delete icon Delete this PKI user. **Note:** The delete icon is not available if the peer user belongs to a user group.

Edit icon Edit this PKI user.

Figure 13: PKI User list

Create New			
Name	Subject	CA	
PKIUser		Fortinet_CA	
pki_user1	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Fortigate, CN = Fortigate, emailAddress = support@fortinet.com	Fortinet_CA	
pki_user2	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Fortigate, CN = Fortigate, emailAddress = support@fortinet.com		
pkipeer1		Fortinet_CA	




To create a peer user for PKI authentication - CLI

```
config user peer
edit <peer name>
set subject <subject_string>
set ca <ca_cert_string>
end
```

To delete a PKI user from the FortiGate unit configuration - web-based manager

- 1 Go to **User > PKI**.
- 2 Select the Delete icon beside the name of the PKI user that you want to remove.
- 3 Select OK.

Figure 14: Delete PKI user

Name	Subject	CA	
pkj_user1	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Fortigate, CN = Fortigate, emailAddress = support@fortinet.com		
pkj_user2	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Fortigate, CN = Fortigate, emailAddress = support@fortinet.com		
pkipeer1			

To delete a PKI user from the FortiGate unit configuration - CLI

```
config user peer
  delete <peer_name>
end
```



Note: You cannot remove a peer user that belongs to a user group that is part of a firewall policy. Remove it from the user group first.

There are other configuration settings that can be added/modified for PKI authentication. For information about the detailed PKI configuration settings only available through the CLI, see the [FortiGate CLI Reference](#).

User groups

A user group is a list of user/peer identities. An identity can be:

- a local user account (user name/password) stored on the FortiGate unit
- a local user account with the password stored on a RADIUS or LDAP server
- a peer user account with digital client authentication certificate stored on the FortiGate unit
- a RADIUS or LDAP server (all identities on the server can authenticate)
- a user group defined on a Microsoft Active Directory server.

Firewall policies and some types of VPN configurations allow access to user groups, not to individual users.

There are three types of user groups - Firewall, Active Directory, and SSL VPN.

Firewall

A firewall user group provides access to a firewall policy that requires firewall type authentication and lists the user group as one of the allowed groups. A firewall user group can also provide access to an IPSec VPN for dialup users, and be used to provide override privileges for FortiGuard web filtering.

Active Directory

An Active Directory user group provides access to a firewall policy that requires Active Directory type authentication and lists the user group as one of the allowed groups.

SSL VPN

An SSL VPN user group provides access to a firewall policy that requires SSL VPN type authentication and lists the user group as one of the allowed groups.

For more information about users and user groups, see the *FortiGate Administration Guide*.

Protection profiles

Each user group is associated with a protection profile to determine the antivirus, web filtering, spam filtering, and intrusion protection settings that apply to the authenticated connection. The FortiGate unit contains several pre-configured protection profiles and you can create your own as needed.

When you create or modify any firewall policy, you can select a protection profile. But when a firewall policy requires authentication, its own protection profile is disabled and the user group protection profile applies.



Note: Protection profiles do not apply to VPN connections.

For more information about protection profiles, see the *FortiGate Administration Guide*.

Creating user groups

You create a user group by typing a name, selecting users and/or authentication servers, and selecting a protection profile.

To create a group - web-based manager

- 1 Go to **User > User Group**.
- 2 Select Create New and enter the following information.

Name	Name of the user group.
Type	Type of user group - Firewall, Active Directory, or SSL VPN.
Protection Profile	Select desired Protection Profile from list. Not applicable to SSL VPN user groups.
Available Users/Groups	Available user group members/user groups. Select the members/groups you require and use the green right arrow to move your selection to the Members column.

- 3 For Firewall and SSL VPN user groups, select the blue right arrow below Available Users/Groups and Members to expand the dialog box, and enter any additional information as required. For information about configuring FortiGuard web filtering override capabilities, see the *FortiGate Administration Guide*. For more information on SSL VPN user groups, see the *SSL VPN User Guide*.
- 4 Select OK.

To create a group - CLI

```
config user group
  edit <group_name>
    set group-type <grp_type>
    set member <user1> <user2> ... <usern>
    set profile <profile_name>
  end
```

Active Directory user groups

You cannot use Active Directory groups directly in FortiGate firewall policies. You must add Active Directory groups to FortiGate user groups.



Note: An Active Directory group should belong to only one FortiGate user group. If you assign it to multiple FortiGate user groups, the FortiGate unit only recognizes the last user group assignment.

To create an Active Directory user group

- 1 Go to **User > User Group**.
- 2 Select **Create New**, enter the following information, and select **OK**.

Name	Name of the Active Directory user group.
Type	Type of user group. Select Active Directory.
Protection Profile	Select the required protection profile from the list.
Available Users	Available Active Directory user groups. Select the groups you require and use the green right arrow to move your selection to the Members column.
Members	The list of Active Directory users that belong to the user group.
Right arrow button	Add a user to the Members list. Select a user name in the Available Users list and select the right arrow button to move it to the Members list.
Left arrow button	Remove a user from the Members list. Select a user name or server name in the Members list and select the left arrow button to move it to the Available Users list.

Figure 15: New User Group dialog box

Configuring authenticated access

When you have configured authentication servers, users, and user groups, you are ready to configure firewall policies and certain types of VPNs to require user authentication.

This section describes:

- [Authentication timeout](#)
- [Authentication protocols](#)
- [Firewall policy authentication](#)
- [VPN authentication](#)

Authentication timeout

You set the firewall user authentication timeout (Authentication Timeout) to control how long an authenticated connection can be idle before the user must authenticate again. The maximum timeout is 480 minutes (8 hours). The default timeout is 5 minutes.

To set the firewall authentication timeout

- 1 Go to **User > Authentication > Authentication**.
- 2 Enter the Authentication Timeout value in minutes.
The default authentication timeout is 5 minutes.
- 3 Select Apply.

You set the SSL VPN user authentication timeout (Idle Timeout) to control how long an authenticated connection can be idle before the user must authenticate again. The maximum timeout is 28800 seconds. The default timeout is 300 seconds.

To set the SSL VPN authentication timeout

- 1 Go to **VPN > SSL > Config**.
- 2 Enter the Idle Timeout value (seconds).
- 3 Select Apply.

Authentication protocols

User authentication can be performed for the following protocols:

- HTTP
- HTTPS
- FTP
- Telnet

When user authentication is enabled on a firewall policy, the authentication challenge is normally issued for any of the four protocols (dependent on the connection protocol). By making selections in the Protocol Support list, the user controls which protocols support the authentication challenge. The user must connect with a supported protocol first so they can subsequently connect with other protocols. If HTTPS is selected as a method of protocol support, it allows the user to utilize a customized Local certificate for authentication.

To set the authentication protocols

- 1 Go to **User > Authentication > Authentication**.
- 2 In Protocol Support, select the required authentication protocols.
- 3 If using HTTPS protocol support, in Certificate, select a Local certificate from the drop-down list.
- 4 Click Apply.

Figure 16: Authentication Settings

Firewall policy authentication

Firewall policies control traffic between FortiGate interfaces, both physical interfaces and VLAN subinterfaces. Without authentication, a firewall policy enables access from one network to another for all users on the source network. Authentication enables you to allow access only for users who are members of selected user groups.



Note: You can only configure user authentication for firewall policies where Action is set to Accept.

Configuring authentication for a firewall policy

Authentication is an Advanced firewall option.

The screenshot shows the 'Authentication' tab in the Firewall Policy configuration. The 'Protection Profile' is set to '[Please Select]'. The 'Log Allowed Traffic' checkbox is unchecked. The 'Authentication' checkbox is checked, and the 'Firewall' dropdown is selected. Below this, there are two lists: 'Available Groups' containing 'PKIGroup' and 'Allowed:' containing 'RadiusGroup'. Between these lists are two arrows: a right-pointing arrow and a left-pointing arrow. Below the lists, there is a 'Certificate' dropdown menu. Further down, there are checkboxes for 'Traffic Shaping' (unchecked) and 'User Authentication Disclaimer' (unchecked). Below these is a 'Redirect URL' text field and a 'Comments (maximum 63 characters)' text area.

To configure authentication for a firewall policy

- 1 Create users and one or more Firewall user groups.
You must select Type: Firewall for the user group. For more information, see [“Users, peers, and user groups” on page 25](#).
- 2 Go to **Firewall > Policy**.
- 3 Select Create New (to create a new policy) or select the Edit icon (to edit an existing policy).
- 4 From the Action list, select ACCEPT.
- 5 Configure the other firewall policy parameters as appropriate.
For information about firewall policies, see the Firewall chapter of the *FortiGate Administration Guide*.
- 6 Select Authentication.
- 7 One at a time, select user group names from the Available Groups list and select the right-pointing arrow button to move them to the Allowed list. All members of the groups in the Allowed list will be authenticated with this firewall policy.
- 8 To use a CA certificate for authentication, in Certificate, select the certificate to use from the drop-down list.
- 9 To require the user to accept a disclaimer to connect to the destination, select User Authentication Disclaimer.

The User Authentication Disclaimer replacement message is displayed. You can edit the User Authentication Disclaimer replacement message text by going to **System > Config > Replacement Messages**.

- 10 Type a URL in Redirect URL if the user is to be redirected after they are authenticated or accept the disclaimer.
- 11 Select OK.

Configuring authenticated access to the Internet

A policy for accessing the Internet is similar to a policy for accessing a specific network, but the destination address is set to all. The destination interface is the one that connects to the Internet service provider. For general purpose Internet access, the Service is set to ANY.

Access to HTTP, HTTPS, FTP and Telnet sites may require access to a domain name service. DNS requests do not trigger authentication. You must configure a policy to permit unauthenticated access to the appropriate DNS server, and this policy must **precede** the policy for Internet access.

To configure a firewall policy for access to a DNS server - web-based manager

- 1 Go to **Firewall > Policy**.
- 2 Select Create New to create a new firewall policy, enter the following information, and select OK.

Source Interface/Zone	List of source interfaces available. Select the interface to which computers on your network are connected.
Source Address	List of source address names. Select all.
Destination Interface/Zone	List of destination interfaces available. Select the interface that connects to the Internet.
Destination Address	List of destination address names. Select all.
Schedule	List of available schedules. Select always.
Service	List of available services. Select DNS.
Action	List of available authentication result actions. Select ACCEPT.



Note: You will position the DNS server in the firewall policy list according to the guidelines outlined in ["Firewall policy order"](#).

Firewall policy order

The firewall policies that you create must be correctly placed in the policy list to be effective. The firewall evaluates a connection request by checking the policy list from the top down, looking for the first policy that matches the source and destination addresses of the packet. Keep these rules in mind:

- More specific policies must be placed above more general ones.
- Any policy that requires authentication must be placed above any similar policy that does not.
- If a user fails authentication, the firewall drops the request and does not check for a match with any of the remaining policies.
- If you create a policy that requires authentication for HTTP access to the Internet, you must precede this policy with a policy for unauthenticated access to the appropriate DNS server.

To change the position of the DNS server in the policy list - web-based manager

- 1 Go to **Firewall > Policy**.
- 2 If necessary, expand the list to view your policies.
- 3 Select the Move To icon beside the DNS policy you created.

Figure 17: Firewall > Policy - Move To

Move To

Status	ID	Source	Destination	Schedule	Service	Profile	Action	
external -> internal (1)								
<input checked="" type="checkbox"/>	2	all	all	always	ANY		ACCEPT	
internal -> external (2)								
<input checked="" type="checkbox"/>	4	all	all	always	DNS		ACCEPT	
<input checked="" type="checkbox"/>	3	all	all	always	HTTP		ACCEPT	

The FortiGate unit performs authentication only on requests to access HTTP, HTTPS, FTP, and Telnet. Once the user is authenticated, the user can access other services if the firewall policy permits.

- 4 Select the position of the DNS policy so that it precedes the policy that provides access to the Internet.

Figure 18: Move firewall policy position selection

Move Policy	
Policy ID	4
Move to	<input checked="" type="radio"/> Before <input type="radio"/> After <input type="text" value="3"/> (Policy ID)
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

- 5 Select OK.

VPN authentication

All VPN configurations require users to authenticate. Authentication based on user groups applies to:

- PPTP and L2TP VPNs
- an IPsec VPN that authenticates users using dialup groups
- a dialup IPsec VPN that uses XAUTH authentication (Phase 1)

This document does not describe the use of certificates for VPN authentication. See the *FortiGate IPsec VPN User Guide* and the *FortiGate Certificate Management User Guide* for information on this type of authentication.

You must create user accounts and user groups before performing the procedures in this section. If you create a user group for dialup IPsec clients or peers that have unique peer IDs, their user accounts must be stored locally on the FortiGate unit. You cannot authenticate these types of users using a RADIUS or LDAP server.

Authenticating PPTP VPN users

To configure authentication for a PPTP VPN - web-based manager

- 1 Configure the users who are permitted to use this VPN. Create a user group and add them to it.

For more information, see [“Users, peers, and user groups” on page 25](#).

- 2 Go to **VPN > PPTP**.

- 3 Select **Enable PPTP**.
- 4 Enter Starting IP and Ending IP addresses. This defines the range of addresses assigned to VPN clients.
- 5 Select the user group that is to have access to this VPN. The FortiGate unit authenticates members of this user group.
- 6 Select **Apply**.

To configure authentication for a PPTP VPN - CLI

```
config vpn pptp
  set eip <starting_ip>
  set sip <ending_ip>
  set status enable
  set usrgrp <user_group_name>
end
```

You also need to define a firewall policy that permits packets to pass from VPN clients with addresses in the specified range to IP addresses that the VPN clients need to access on the private network behind the FortiGate unit. The Action for this firewall policy is ACCEPT, not ENCRYPT, because the allowed user group is defined in the PPTP VPN configuration, not in the firewall policy.

For detailed information about configuring PPTP, see the *FortiGate PPTP VPN User Guide*.

Authenticating L2TP VPN users

Authentication for the FortiGate L2TP configuration must be done using the `config vpn l2tp` CLI command.

To configure authentication for a L2TP VPN - CLI

```
config vpn l2tp
  set eip <starting_ip>
  set sip <ending_ip>
  set status enable
  set usrgrp <user_group_name>
end
```

For more information, see the *FortiGate CLI Reference*.

Authenticating remote IPSec VPN users using dialup groups

An IPSec VPN on a FortiGate unit can authenticate remote users through a dialup group. The user account name is the peer ID and the password is the pre-shared key. For information about authentication using peer IDs and peer groups, see “Enabling VPN access using user accounts and pre-shared keys” in the *FortiGate IPSec VPN User Guide*.

Authentication through user groups is supported for groups containing only local users. To authenticate users using a RADIUS or LDAP server, you must configure XAUTH settings. See [“Enabling XAuth authentication for dialup IPSec VPN clients” on page 41](#).

To configure user group authentication for dialup IPSec - web-based manager

- 1 Configure the dialup users who are permitted to use this VPN. Create a user group with Type:Firewall and add them to it.
For more information, see [“Users, peers, and user groups” on page 25](#).
- 2 Go to **VPN > IPSec > Auto Key (IKE)** and select Create Phase 1 to create a new VPN gateway.

Figure 19: Configure VPN IPSec dialup authentication

Name	Name for group of dialup users using the VPN for authentication.
Remote Gateway	List of the types of remote gateways for VPN. Select Dialup User.
Authentication Method	List of authentication methods available for users. Select Preshared Key.
Peer Options	Selection of peer ID options available. Select the user group that is to be allowed access to the VPN. The listed user groups contain only users with passwords on the FortiGate unit.



Note: The Accept peer ID in dialup group option does not support authentication of users through an authentication server.

- 3 Select Advanced to reveal additional parameters and configure other VPN gateway parameters as needed.
- 4 Select OK.

To configure user group authentication for dialup IPSec - CLI

```
config vpn ipsec phase1
  edit <gateway_name>
    set peertype dialup
    set usrgroup <user_group_name>
  end
```



Note: Parameters specific to setting up the VPN itself are not shown here. For detailed information, see the *FortiGate IPSec VPN User Guide*.

Enabling XAuth authentication for dialup IPSec VPN clients

XAuth can be used in addition to or in place of IPSec phase 1 peer options to provide access security through an LDAP or RADIUS authentication server. You must configure dialup users as members of a user group who are externally authenticated. None can have passwords stored on the FortiGate unit.

To configure authentication for a dialup IPSec VPN - web-based manager

- 1 Configure the users who are permitted to use this VPN. Create a user group and add them to it.
For more information, see [“Users, peers, and user groups” on page 25](#).
- 2 Go to **VPN > IPSec > Auto Key (IKE)** and select Create Phase 1 to create a new VPN gateway and enter the following information.

Name	Name for group of dialup users using the VPN for authentication through RADIUS or LDAP servers.
Remote Gateway	List of the types of remote gateways for VPN. Select Dialup User.
Authentication Method	List of authentication methods available for users. Select Preshared Key.

New Phase 1

Name:

Remote Gateway:

Local Interface:

Mode: ☐ Aggressive ☒ Main (ID protection)

Authentication Method:

Pre-shared Key:

Peer Options

☐ Accept any peer ID

☐ Accept this peer ID

☒ Accept peer ID in dialup group

Advanced... (XAUTH, Nat Traversal, DPD)

☒ **Enable IPsec Interface Mode**

Local Gateway IP: ☒ Main Interface IP ☐ Specify

P1 Proposal

1 - Encryption: Authentication:

2 - Encryption: Authentication:

DH Group: ☐ 1 ☐ 2 ☒ 5

Keylife: (120-172800 seconds)

Local ID: (optional)

XAuth ☐ Disable ☐ Enable as Client ☒ Enable as Server

Server Type: ☒ PAP ☐ CHAP ☐ AUTO

User Group:

Nat-traversal: ☒ Enable

Keepalive Frequency: (10-900 seconds)

Dead Peer Detection ☒ Enable

OK Cancel

- 3 Select Advanced to reveal additional parameters and enter the following information.

XAuth	Select Enable as Server.
Server Type	Select PAP, CHAP, or AUTO. Use CHAP whenever possible. Use PAP with all implementations of LDAP and with other authentication servers that do not support CHAP, including some implementations of Microsoft RADIUS. Use AUTO with the Fortinet Remote VPN Client and where the authentication server supports CHAP but the XAuth client does not.
User Group	List of available user groups. Select the user group that is to have access to the VPN. The list of user groups does not include any group that has members whose password is stored on the FortiGate unit.

- 4 Configure other VPN gateway parameters as needed.
- 5 Select OK.

For more information about XAUTH configuration, see “Using XAUTH authenticationFortiGate” in the *FortiGate IPsec VPN User Guide*.

To configure authentication for a dialup IPsec VPN - CLI

```
config vpn ipsec phase1
  edit <gateway_name>
    set peertype dialup
    set xauthtype pap
    set authusrgrp <user_group_name>
  end
```

Parameters specific to setting up the VPN itself are not shown here. For detailed information about configuring an IPsec VPN, see the *FortiGate IPsec VPN User Guide*.

Index

A

- Active Directory - see AD
- AD authentication servers
 - about
 - configuring the FortiGate unit to use 22
 - FSAE 21
 - user groups 22
- AD user groups
 - creating 32
- authenticated access
 - configuring 33
- authentication
 - about 5
 - access to DNS server 36
 - firewall policy 34, 35
 - FortiGate administrator's view 6
 - Internet access 36
 - PKI 8
 - protocols 33
 - timeout 33
 - user's view 5
 - VPN client-based 6
 - web-based user 6
- authentication protocols
 - setting 34
- authentication servers
 - AD
 - FortiGate administrator's view 7
 - LDAP 17
 - RADIUS 15
- authentication timeout 9
 - FortiGate administrator's view 9
 - setting 33

C

- comments, documentation 13
- configuring
 - authenticated access 33
 - firewall policy authentication 35
 - Internet access authentication 36
- creating
 - AD user groups 32
 - local users 25
 - peer users 27
 - user groups 31
- customer service 13

D

- deleting
 - local users 27
 - peer users 29
- documentation
 - commenting on 13
 - Fortinet 10

F

- firewall
 - DNS server access 36
 - Internet access authentication 36
 - policy authentication 34, 35
 - user authentication timeout 33
- firewall policies
 - FortiGate administrator's view 9
- firewall policy
 - list order 36
 - order 36
- FortiGate
 - configuring to use AD authentication server 22
 - configuring to use LDAP authentication server 19
 - configuring to use RADIUS authentication server 15
- FortiGate administrator's view
 - authentication 6
 - authentication servers 7
 - authentication timeout 9
 - firewall policies 9
 - peers 8
 - PKI authentication 8
 - user groups 8
 - users 8
 - VPN tunnels 9
- FortiGate documentation
 - commenting on 13
- Fortinet customer service 13
- Fortinet documentation 10
- Fortinet Knowledge Center 13
- FSAE 21

I

- Internet access authentication 36
- introduction
 - Fortinet documentation 10

L

- LDAP authentication servers
 - configuring the FortiGate unit to use 19
 - organization 17
 - users 19
- local users
 - creating 25
 - deleting 27

P

- peer users
 - creating 27
 - deleting 29
- peers
 - FortiGate administrator's view 8
- PKI authentication 8
 - FortiGate administrator's view 8

PKI authentication - see peer users

protection profiles 30

protocols

authentication 33

R

RADIUS authentication servers 15

additional request attributes 17

configuring the FortiGate unit to use 15

S

setting

authentication protocols 34

firewall policy authentication 34

firewall user authentication timeout 33

SSL VPN authentication timeout 33

SSL VPN

authentication timeout 33

T

technical support 13

timeout

authentication 9

types of users 25

U

user groups

about 30

AD 22

AD, creating 32

creating 31

FortiGate administrator's view 8

protection profiles 30

types of 30

user's view of authentication 5

VPN client-based authentication 6

web-based user authentication 6

users

about 25

FortiGate administrator's view 8

local, creating 25

local, deleting 27

peer, creating 27

peer, deleting 29

types 25

V

VPN

client-based authentication 6

VPN tunnels

FortiGate administrator's view 9

W

web-based user authentication 6



www.fortinet.com



www.fortinet.com