

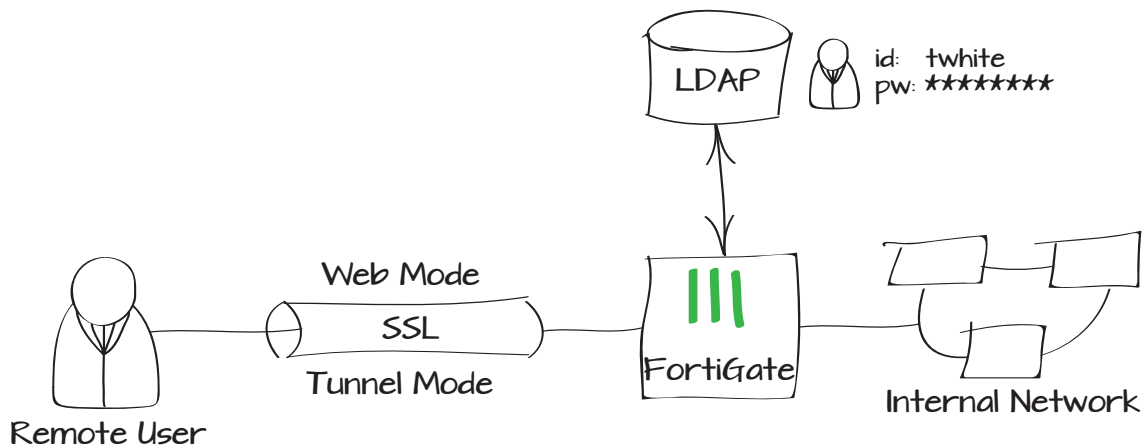
Authenticating SSL VPN users using LDAP

This example illustrates how to configure a FortiGate to use LDAP authentication to authenticate remote SSL VPN users. With a properly configured LDAP server, user and authentication data can be maintained independently of the FortiGate, accessed only when a remote user attempts to connect through the SSL VPN tunnel.



This recipe assumes that the LDAP server is already configured.

1. Registering the LDAP server on the FortiGate
2. Importing LDAP users
3. Creating the SSL VPN user group
4. Creating the SSL address range
5. Configuring the SSL VPN tunnel
6. Creating security policies
7. Results



Registering the LDAP server on the FortiGate

Go to **User & Device > Authentication > LDAP Servers** and select **Create New**.

Enter the LDAP Server's FQDN or IP in **Server Name/IP**. If necessary, change the Server Port Number (the default is 389.)

Enter the **Common Name Identifier**. Most LDAP servers use "cn" by default.

In the **Distinguished Name** field, enter the base distinguished name for the server, using the correct X.500 or LDAP format.

Set the **Bind Type** to **Regular**, and enter the LDAP administrator's distinguished name and password for **User DN** and **Password**.

Name	<input type="text" value="Example_LDAP"/>
Server Name/IP	<input type="text" value="10.10.10.1"/>
Server Port	<input type="text" value="389"/>
Common Name Identifier	<input type="text" value="cn"/>
Distinguished Name	<input type="text" value="Example LDAP Server"/>
Bind Type	<input type="radio"/> Simple <input type="radio"/> Anonymous <input checked="" type="radio"/> Regular
User DN	<input type="text" value="example_admin"/>
Password	<input type="password" value="....."/>
<input type="checkbox"/> Secure Connection	

Importing LDAP users

Go to **User & Device > User > User Definition**, and create a new user, selecting **Remote LDAP User**.

Choose your LDAP Server from the dropdown list.

You will be presented with a list of user accounts, filtered by the LDAP Filter to include only common user classes.



If you are using a different objectClass to identify users on your LDAP server, edit the filter to show them in the list.

1 Choose User Type 2 Specify LDAP Server

- ☐ Local User
- ☐ Remote RADIUS User
- ☐ Remote TACACS+ User
- ☒ Remote LDAP User

1 Choose User Type 2 Specify LDAP Server 3 Select Remote Users

- ☒ Choose Existing
- ☐ Create New

Confirm that the user information has been imported properly, and select **Done**.

Go to **User & Device > User > User Groups**, and create an LDAP user group.



Go to **Firewall Objects > Addresses > Addresses**, and create a new address.

Set the **Type** to **IP Range**, and in the **Subnet/IP Range** field, enter the range of addresses you want to assign to SSL VPN clients. Select **Any** as the **Interface**.




Then create another Address for each Subnet or IP Range within your internal network to which remote users will connect.



Name

Type ☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐

Members

Remote groups

 Add  Edit  Delete
Remote Server
Example_LDAP

Category	<input checked="" type="radio"/> Address <input type="radio"/> IPv6 Address <input type="radio"/> Multicast Address
Name	<input type="text" value="LDAP_SSL_range"/>
Color	 [Change]
Type	<input type="text" value="IP Range"/>
Subnet / IP Range	<input type="text" value="10.10.100.100-10.10.100.200"/>
Interface	<input type="text" value="Any"/>
Category	<input checked="" type="radio"/> Address <input type="radio"/> IPv6 Address <input type="radio"/> Multicast Address
Name	<input type="text" value="Local Network Subnet"/>
Color	 [Change]
Type	<input type="text" value="Subnet"/>
Subnet / IP Range	<input type="text" value="192.168.1.144"/>
Interface	<input type="text" value="Any"/>

Configuring the SSL VPN tunnel

Go to **VPN > SSL > Portal**, and select the plus icon in the upper right to create a new SSL Portal configuration.

Enable **Tunnel Mode**, and enable **Split Tunneling**. For the **IP Pool**, select the address range you created. Enable **Web Mode**, and set the options as desired.

Enable **Include Bookmarks**, and create a bookmark to access an internal network PC. In this example, the bookmark is an **RDP** connection, for remote desktop access.



By default, SSL authentication expires after 28800 seconds (8 hours). This limit can be changed in the CLI:

```
config vpn ssl settings
    set auth-timeout
```

Creating security policies

You will need to create two policies to handle web mode and tunnel mode SSL traffic.



Go to **Policy > Policy > Policy**, and create a new **VPN** policy to allow the SSL traffic through to the internal network.

Set the **Incoming Interface** to your Internet-facing interface, your **Remote Address** to all, your **Local Interface** to your internal network interface, and for the **Local Protected Subnet**, select the network access addresses you created.

Name:



Portal Message:

Theme:

Page Layout: ☐  ☒ 

☒ Enable Tunnel Mode

☒ Enable Split Tunneling

IP Pools  

Client Options ☐ Save Password ☐ Auto Connect ☐ Always Up (Keep Alive)

☒ Enable Web Mode

Applications

<input checked="" type="checkbox"/> HTTP/HTTPS	<input checked="" type="checkbox"/> FTP	<input checked="" type="checkbox"/> RDP	<input checked="" type="checkbox"/> SMB/CIFS
<input checked="" type="checkbox"/> SSH	<input checked="" type="checkbox"/> TELNET	<input checked="" type="checkbox"/> VNC	<input checked="" type="checkbox"/> PING
<input checked="" type="checkbox"/> CITRIX	<input checked="" type="checkbox"/> RDP NATIVE	<input type="checkbox"/> Port Forward	




☒ Include Session Info

☐ Include Connection Tool

☒ Include FortiClient Download



☐ Include Login History

☒ Include Bookmarks

 Create New  Edit SSL-VPN Portal  Delete			
Name	Type	Location	Description
▼ RDP (1)			
RDP_example	RDP	192.168.1.144	

☒ Prompt Mobile Users to Download FortiClient App

☒ Allow Multiple Concurrent Sessions For Each User

Policy Type	<input type="radio"/> Firewall <input checked="" type="radio"/> VPN
Incoming Interface	wan1
Remote Address	 all
Local Interface	port1 (Internal)
Local Protected Subnet	 Local Network Subnet

Under **Configure SSL-VPN Authentication Rules**, select **Create New** to create a new rule to govern SSL traffic.

Set the **Group** to your SSL VPN group, select your LDAP user as **User**, and select your **SSL-VPN Portal** from the list.

Configure the logging and security profiles as needed.

Return to the policy list, and select **Create New** again, to create the tunnel mode firewall policy. Leave the **Type** as **Firewall**, and the **Subtype** as **Address**.

Set the **Incoming Interface** to the SSL VPN tunnel interface. Set the **Source Address** to the VPN users address range. Set the **Outgoing Interface** to the internal network interface, and set the **Destination Address** to the internal network addresses that SSL users will need to reach.

Enable **NAT**, and configure logging and security policies as needed.

Group(s)

SSLVPN_LDAP_group

User(s)

twhite

Schedule

always

SSL-VPN Portal

LDAP_SSL Portal

Action

ACCEPT

Logging Options

No Log

Log Security Events

Log all Sessions

Security Profiles

ON

AntiVirus

OFF

Web Filter

ON

Application Control

OFF

IPS

OFF

Email Filter

ON

DLP Sensor

OFF

VoIP

OFF

ICAP

default

default

default

default

default

default

default

Policy Type

Firewall VPN

Policy Subtype

Address User Identity Device Identity

Incoming Interface

ssl.root (sslvpn tunnel interface)

Source Address

LDAP_SSL_range

Outgoing Interface

port1 (Internal)

Destination Address

Local Network Subnet

Schedule

always

Service

ALL

Action

ACCEPT

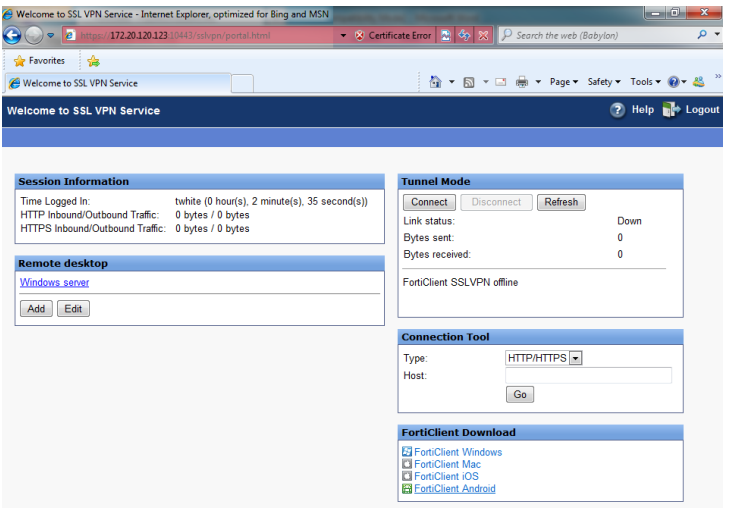
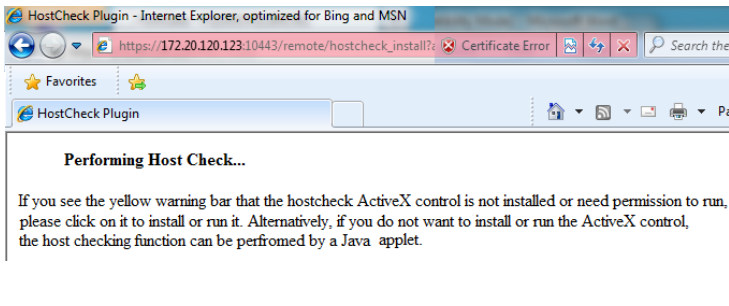
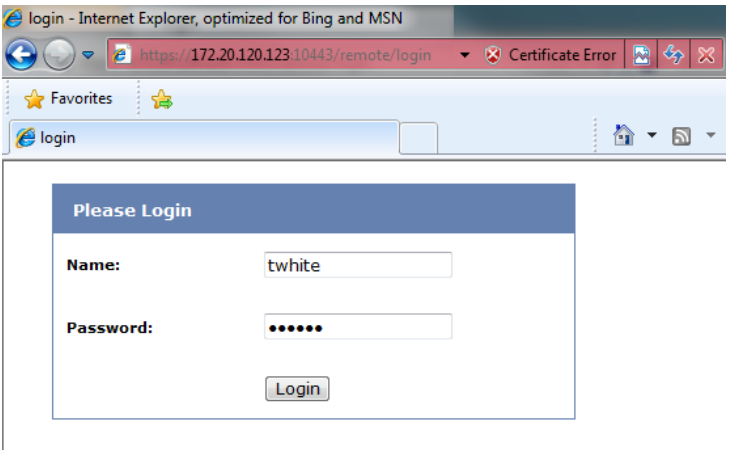
Enable NAT

Results

Log into the SSL portal using the LDAP user credentials. The FortiGate will automatically contact the LDAP server for verification.

The FortiGate unit performs the host check.

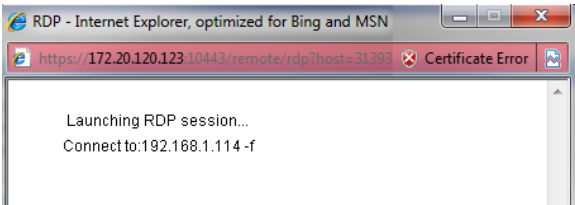
After the check is complete, the SSL portal appears.






Select a bookmark, such as the **RDP** link, to begin an RDP session, and connect to a PC on the internal network.

Go to **VPN > Monitor > SSL-VPN** to verify the list of SSL users. The Web Application description indicates that the user is using web mode.

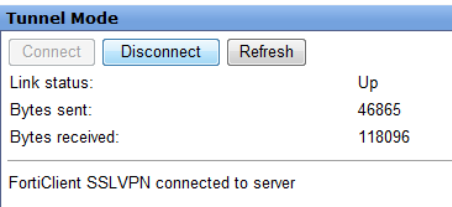
Go to **Log & Report > Traffic Log > Forward Traffic** to see details about SSL traffic.



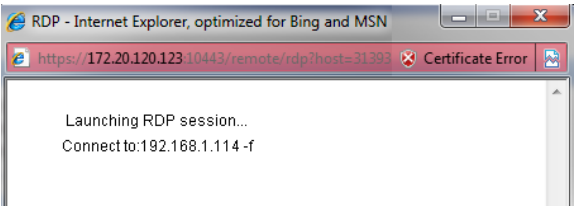
No.	User	Source IP	Begin Time	Desc
1	twhite	172.20.120.23	Wed Apr 17 11:41:06 2013	
Subsession		Web Application:RDP 192.168.1.114		

Dst	192.168.1.114	Virtual Domain	root
Received	85591	Source Country	Reserved
Sent / Received	8.71 KB / 83.58 KB	Duration	36
Sent	8923	Application Details	
Group	N/A	Service	RDP
Protocol	6	User	 twhite
Destination Country	Reserved	Dst Port	3389
roll	65389	Status	✓
Timestamp	Wed Apr 17 14:13:11 2013	Tran Display	noop
Sequence Number	2700	Policy ID	11
Src Interface	wan1	Src	 twhite (172.20.120.23)
VPN	sslvpn_web_mode	Sent Packets	71
Level	notice 	VPN Type	sslvpn
Src Port	53712	Log ID	13
Sub Type	forward	Threat	
Received Packets	98	Date/Time	14:13:11 (Wed Apr 17 14:13:11 2013)
Dst Interface	port1		

In the **Tunnel Mode** widget, select **Connect** to enable the tunnel.



Select the **RDP** bookmark to begin an RDP session.



Go to **VPN > Monitor > SSL-VPN** to verify the list of SSL users. The Tunnel description indicates that the user is using tunnel mode.

User	Source IP	Begin Time	Descrip
twhite	172.20.120.23	Wed Apr 17 11:41:06 2013	
Subsession			Tunnel IP:10.212.134.200