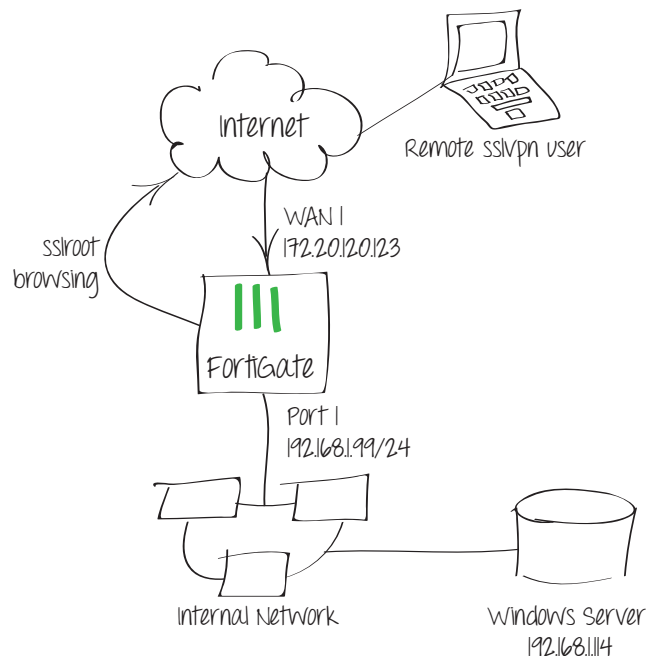


# Providing remote users with protected access to a corporate network and Internet using SSL VPN

This example sets up remote users to connect to the corporate network using SSL VPN, and use the FortiGate UTM for surfing the Internet. During the connecting phase, the FortiGate unit will also verify that the remote user's antivirus software is installed and current.

1. Create an SSL VPN tunnel for remote users
2. Create user definitions and add them to a group
3. Add an address for the local network
4. Add security profiles for access to the Internet and internal network
5. Set the FortiGate unit to verify users have current antivirus software
6. Results



Step One: Create an SSL VPN tunnel for remote users

Go to **VPN > SSL > Portal**.

Edit the full-access portal.

The full-access portal allows the use of tunnel mode and/or web mode. In this scenario we are using both modes.

**Enable Split Tunneling** is not enabled so that all internet traffic will go through the FortiGate unit and be subject to the corporate UTM profiles.

Select **Create New** in the **Include Bookmarks** area to add a bookmark for a remote desktop link/connection.

The screenshot shows the configuration page for the 'full-access' SSL VPN portal. The 'Name' field is 'full-access'. The 'Portal Message' is 'Welcome to SSL VPN Service'. The 'Theme' is 'Blue'. The 'Page Layout' shows two icons, with the second one selected. Under 'Enable Tunnel Mode', 'Enable Split Tunneling' is unchecked. The 'IP Pools' field contains 'SSLVPN\_TUNNEL\_ADDR1'. Under 'Client Options', 'Save Password', 'Auto Connect', and 'Always Up (Keep Alive)' are all unchecked. Under 'Enable Web Mode', several applications are checked: HTTP/HTTPS, FTP, RDP, SMB/CIFS, SSH, TELNET, VNC, PING, and CITRIX. There are also checkboxes for 'RDP NATIVE' and 'Port Forward'. Below these are four checked options: 'Include Session Info', 'Include Connection Tool', 'Include FortiClient Download', and 'Include Bookmarks'. At the bottom of the configuration area, there is a table with columns 'Name', 'Type', 'Location', and 'Description'. The table is empty, with the text 'No matching entries found' below it. At the very bottom of the page, there are two checked options: 'Prompt Mobile Users to Download FortiClient App' and 'Allow Multiple Concurrent Sessions For Each User'. A 'View Portal' button is located at the bottom left.

The screenshot shows the configuration page for adding a new bookmark. The 'Category' is 'Remote desktop'. The 'Name' is 'Windows server'. The 'Type' is 'RDP'. The 'Location' is '192.168.1.114'. The 'Screen Width' is '1024'. The 'Screen Height' is '768'. The 'Logon User' and 'Logon Password' fields are empty. The 'Keyboard Layout' is 'English, US'. The 'Description' field is empty. The 'Full Screen Mode' checkbox is checked.

Step Two: Create user definitions and add them to a group

Go to **User & Device > User > User Definition.**

Add a remote user.

The screenshot shows the 'User Definition' configuration page. The 'User Name' field is set to 'twhite'. There is a 'Disable' checkbox which is unchecked. The 'Password' field is filled with eight dots. Below the password field are three radio buttons: 'Password' (selected), 'Match user on LDAP server', 'Match user on RADIUS server', and 'Match user on TACACS+ server'. Each of the latter three options has a '[Please Select]' dropdown menu. Under the 'Contact Info' section, there is an 'Email Address' field and an 'SMS' checkbox. The 'SMS' checkbox is unchecked, and the 'FortiGuard Messaging Service' radio button is selected, with a 'Phone Number' field next to it.

Go to **User & Device > User > User Group.**

Add the user to a user group for SSL VPN connections.

The screenshot shows the 'User Group' configuration page. The 'Name' field is set to 'sslvpn\_group'. The 'Type' section has four radio buttons: 'Firewall' (selected), 'Fortinet Single Sign-On (FSSO)', 'Guest', and 'RADIUS Single Sign-On (RSSO)'. Below this are two list boxes: 'Available Users' and 'Members'. The 'Available Users' list contains '- Local Users - guest'. The 'Members' list contains '- Local Users - twhite'. There are blue arrows between the two lists, indicating the ability to move users between them.

Step Three: Add an address for the local network

Go to **Firewall Objects > Address > Address.**

Add the address for the local network.

The screenshot shows the 'Address' configuration page. The 'Category' section has three radio buttons: 'Address' (selected), 'IPv6 Address', and 'Multicast Address'. The 'Name' field is set to 'Local LAN'. There is a '[Change]' link next to the 'Color' field. The 'Type' dropdown menu is set to 'Subnet'. The 'Subnet / IP Range' field is set to '192.168.1.0/255.255.255.0'. The 'Interface' dropdown menu is set to 'port1'. The 'Show in Address List' checkbox is checked. The 'Comments' field is empty, with a character count of '0/255'.

Step Four: Add security profiles for access to the Internet and internal network

Go to **Policy > Policy > Policy**.

Add a security policy allowing access to the internal network.

Policy Type  Firewall  VPN  
 Policy Subtype  IPsec  SSL-VPN  
 Incoming Interface   
 Remote Address    
 Local Interface   
 Local Protected Subnet    
 SSL Client Certificate Restrictive  
 Cipher Strength

**Configure SSL-VPN Authentication Rules**

[Create New](#) [Edit](#) [Delete](#)

User/Group	Service	Schedule	UTM Security	SSL-VPN Portal	Logging	Action
sslvpn_group twhite	ALL	always	-	full-access		ACCEPT
ANY	ALL	always	-			DENY

**Tags**  
 Applied tags  
 Add tag    
 Comments  0/1023

Add a security policy allowing access to the Internet.

For this policy, the **Incoming Interface** is *sslvpn tunnel interface* and **Outgoing Interface** is *wan1*. This way, the remote SSL VPN users accessing the Internet through the FortiGate unit.

Policy Type  Firewall  VPN  
 Policy Subtype  Address  User Identity  Device Identity  
 Incoming Interface   
 Source Address    
 Outgoing Interface   
 Destination Address    
 Schedule   
 Service    
 Action

Enable NAT  
 Use Destination Interface Address  Fixed Port  
 Use Dynamic IP Pool   
 Use Central NAT Table

**Logging Options**  
 No Log  
 Log UTM Events  
 Log all Sessions

Step Five: Set the FortiGate unit to verify users have current antivirus software

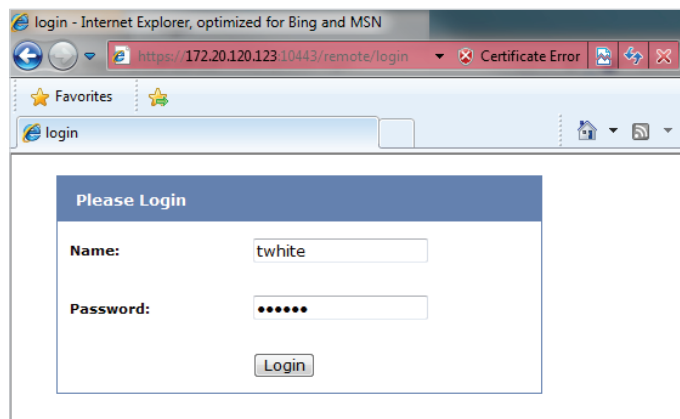
Go to **System > Status > Dashboard**.

In the **CLI Console** widget, enter the commands on the right to enable the host check for compliant antivirus software on the remote user's computer.

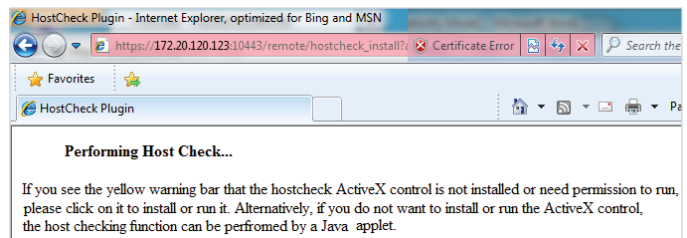
```
# config vpn ssl web portal
(portal) # edit full-access
(full-access) # set host-check av
(full-access) # end
#
```

## Results

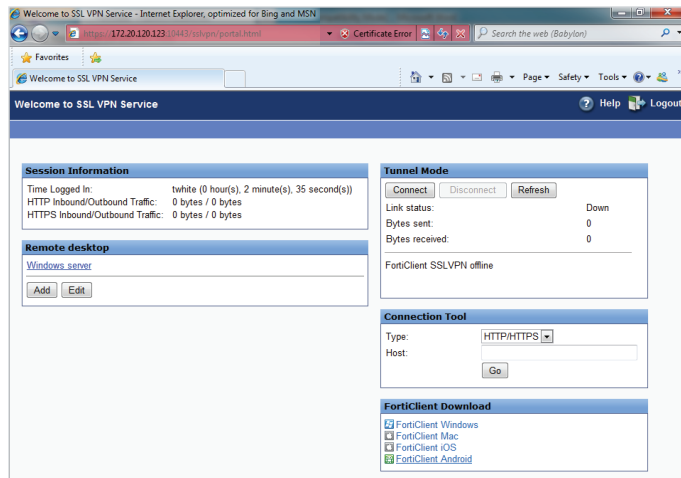
Log into the portal as twwhite.



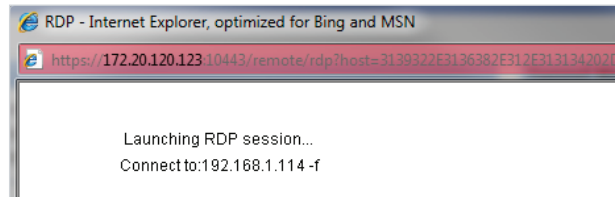
The FortiGate unit performs the host check.



After the check is complete, the portal appears.



Select the bookmark Remote Desktop link to begin an RDP session.



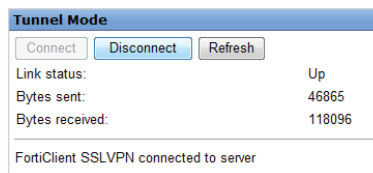
Go to **VPN > Monitor > SSL-VPN** to verify the list of SSL users. The Web Application description indicates that the user is using web mode.

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

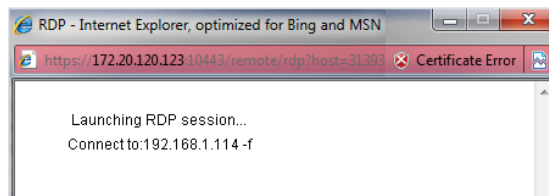
Go to **Log & Report > Traffic Log > Forward Traffic** and view the details for the SSL entry.

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

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



Select the bookmark Remote Desktop link to begin an RDP session.



Go to **VPN > Monitor > SSL-VPN** to verify the list of SSL users.

Id.	User	Source IP	Begin Time	Description
1	twhite	172.20.120.23	Wed Apr 17 11:41:06 2013	
	Subsession			Tunnel IP:10.212.134.200

The Tunnel description indicates that the user is using tunnel mode.

Go to **Log & Report > Traffic Log > Forward Traffic** and view the details for the SSL entry.

<b>Dst</b>	192.168.1.114	<b>Virtual Domain</b>	root
<b>Received</b>	326664	<b>Source Country</b>	Reserved
<b>Sent / Received</b>	54.36 KB / 319.01 KB	<b>Duration</b>	83
<b>Sent</b>	55665	<b>Application Details</b>	
<b>Group</b>	N/A	<b>Service</b>	RDP
<b>Protocol</b>	6	<b>User</b>	twhite
<b>Destination Country</b>	Reserved	<b>Dst Port</b>	3389
<b>roll</b>	65389	<b>Status</b>	✓
<b>Timestamp</b>	Wed Apr 17 14:17:15 2013	<b>Tran Display</b>	noop
<b>Sequence Number</b>	3618	<b>Policy ID</b>	11
<b>Src Interface</b>	wan1	<b>Src</b>	twhite (172.20.120.23)
<b>VPN</b>	sslvpn_web_mode	<b>Sent Packets</b>	329
<b>Level</b>	notice	<b>VPN Type</b>	sslvpn
<b>Src Port</b>	53820	<b>Log ID</b>	13
<b>Sub Type</b>	forward	<b>Threat</b>	
<b>Received Packets</b>	407	<b>Date/Time</b>	14:17:15 (Wed Apr 17 14:17:15 2013)
<b>Dst Interface</b>	unknown-0		

Go to **Log & Report > Traffic Log > Forward Traffic**.

Internet access occurs simultaneously through the FortiGate unit.

Download Raw Log

me	Src Interface	Dst Interface	Src	Dst	Ser
ssl.root	wan1	wan1	10.212.134.200	74.125.133.95	HTTP
ssl.root	wan1	wan1	10.212.134.200	173.194.77.94	HTTP
ssl.root	wan1	wan1	10.212.134.200	173.194.43.79	HTTP
ssl.root	wan1	wan1	10.212.134.200	66.171.121.34 (fortinet.com)	HTTP
ssl.root	wan1	wan1	10.212.134.200	74.121.50.17 (www.pages03.net)	HTTP
ssl.root	wan1	wan1	10.212.134.200	208.91.113.212	HTTPS
ssl.root	wan1	wan1	10.212.134.200	192.168.55.30	KERBE
ssl.root	wan1	wan1	10.212.134.200	192.168.55.30	KERBE
ssl.root	wan1	wan1	10.212.134.200	192.168.55.30	KERBE
ssl.root	wan1	wan1	10.212.134.200	213.199.179.159	40031/
ssl.root	wan1	wan1	10.212.134.200	213.199.179.159	HTTP
ssl.root	wan1	wan1	10.212.134.200	132.246.2.6 (www.msftncsi.com)	HTTP

Select an entry to see more information.

<b>Dst</b>	66.171.121.34 (fortinet.com)	<b>Virtual Domain</b>	root
<b>Received</b>	938	<b>Source Country</b>	Reserved
<b>Src NAT IP</b>	172.20.120.123	<b>Sent / Received</b>	535 B / 938 B
<b>Duration</b>	17	<b>Sent</b>	535
<b>Src NAT Port</b>	54165	<b>Application Details</b>	
<b>Service</b>	HTTP	<b>Protocol</b>	6
<b>Destination Country</b>	United States	<b>Dst Port</b>	80
<b>roll</b>	65389	<b>Status</b>	close
<b>Timestamp</b>	Wed Apr 17 14:26:03 2013	<b>Tran Display</b>	snat
<b>Sequence Number</b>	8096	<b>Policy ID</b>	8
<b>Src Interface</b>	ssl.root	<b>Src</b>	10.212.134.200
<b>Sent Packets</b>	6	<b>Level</b>	notice
<b>Src Port</b>	54165	<b>Log ID</b>	13
<b>Sub Type</b>	forward	<b>Threat</b>	
<b>Received Packets</b>	5	<b>Date/Time</b>	14:26:03 (Wed Apr 17 14:26:03 2013)
<b>Dst Interface</b>	wan1		