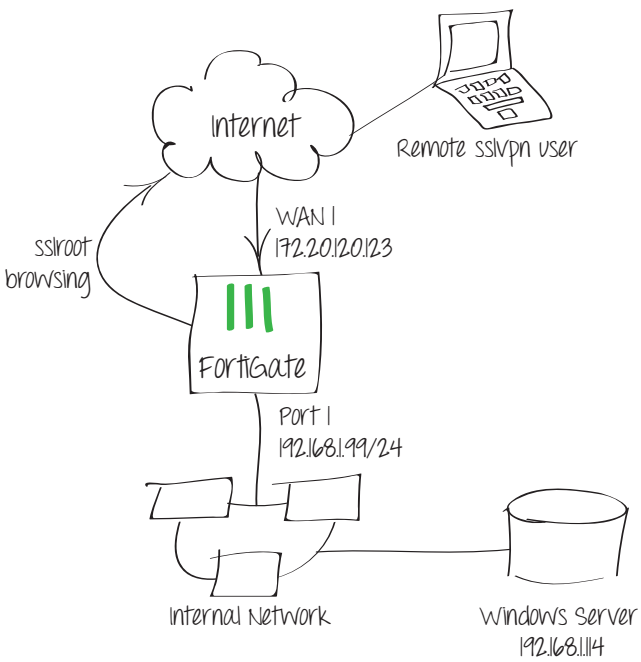
Providing remote users with protected access to a corporate network and Internet using SSL VPN

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



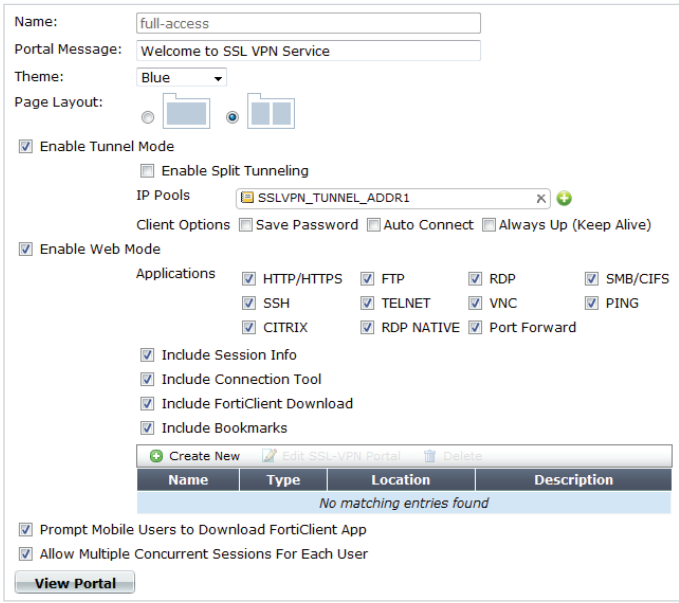
Step One: Create an SSL VPN tunnel for remote users

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

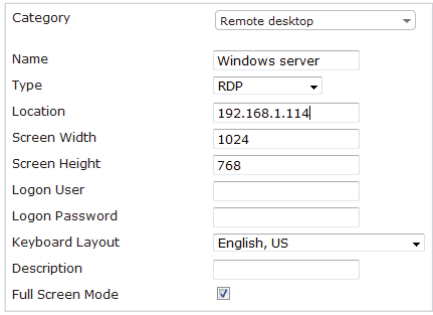
Edit the full-access portal.

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.



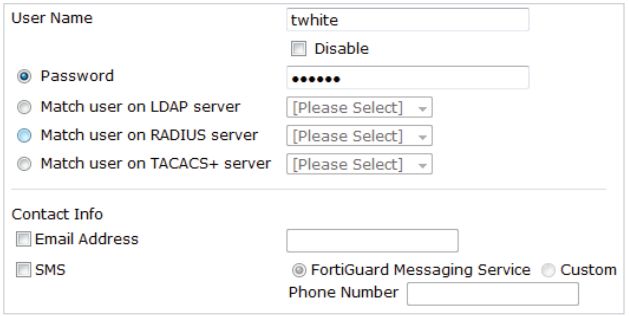
Select Create New in the Include Bookmarks area to add a bookmark for a remote desktop link/connection.



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

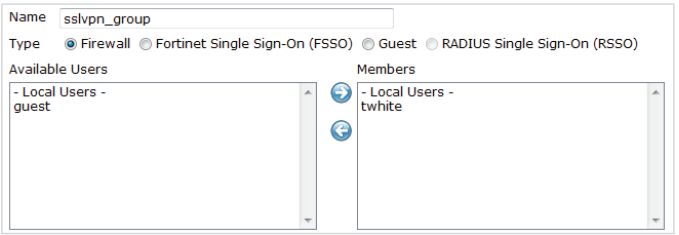
Go to **User & Device > User > User Definition**.

Add a remote user.



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

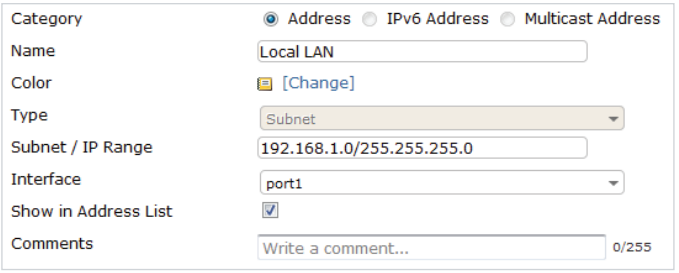
Add the user to a user group for SSL VPN connections.



Step Three: Add an address for the local network

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

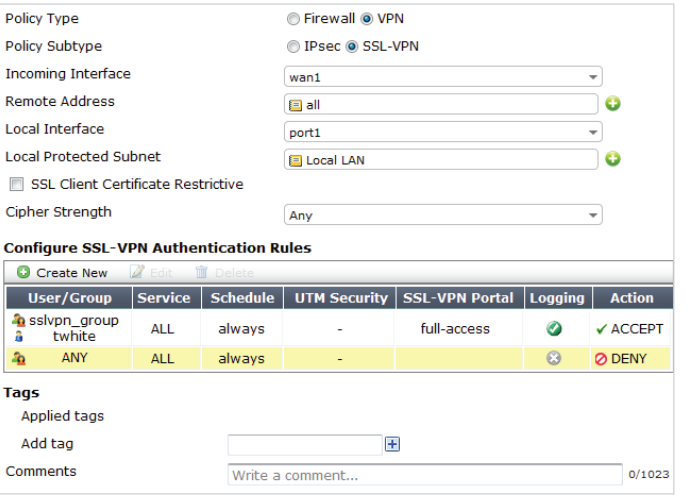
Add the address for the local network.



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

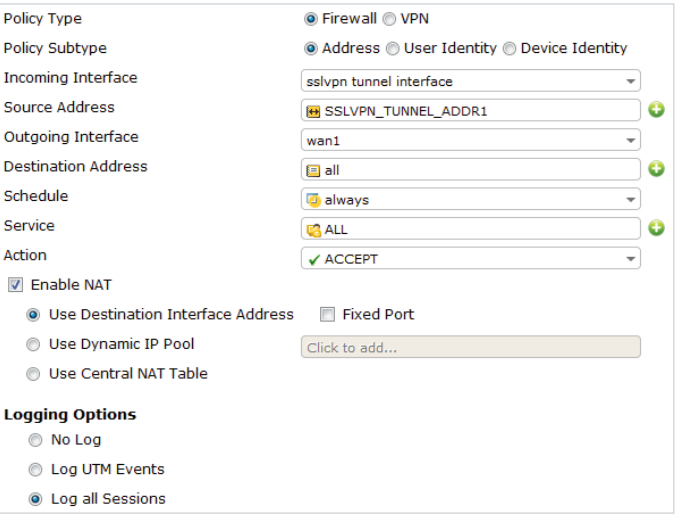
Go to **Policy > Policy > Policy**.

Add a security policy allowing access to the internal network.



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 FotiGate unit.



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

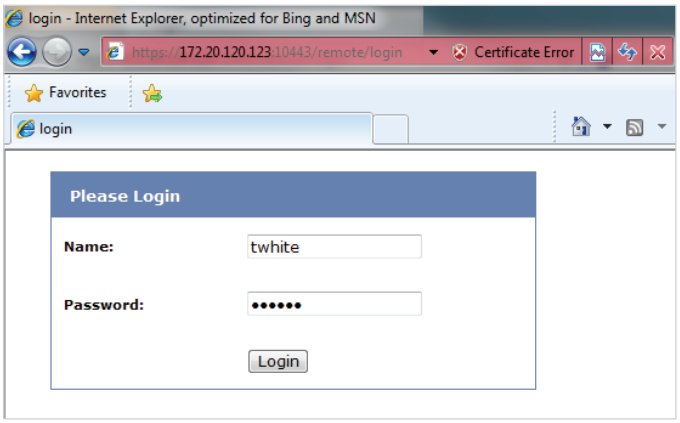
Go to **System > Status > Dashboard**.

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.

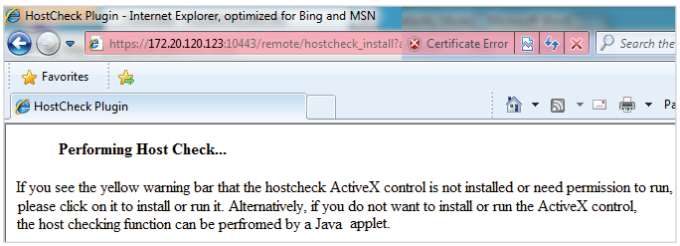
```
# config vpn ssl web portal
(portal) # edit full-access
(full-access) # set host-check av
(full-access) # end
#
```

Results

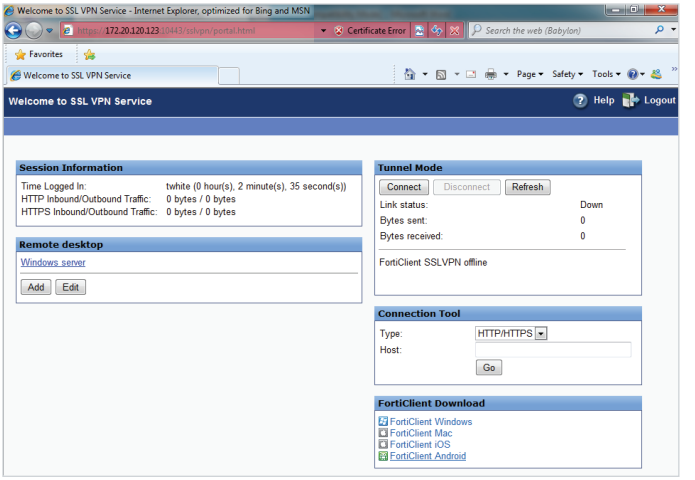
Log into the portal as twhite.



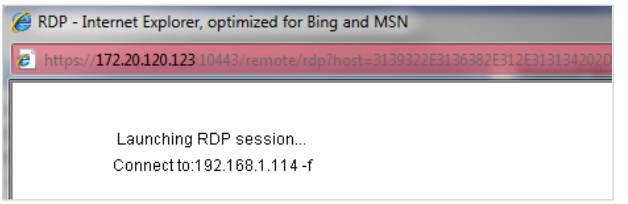
The FortiGate unit performs the host check.



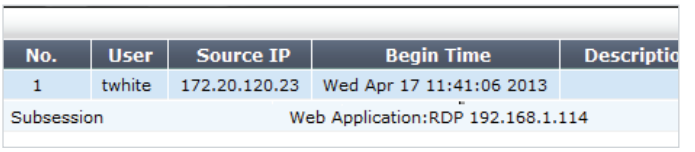
After the check is complete, the portal appears.



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.

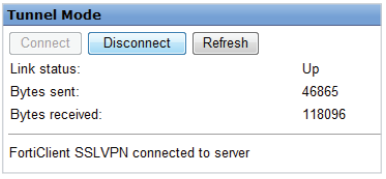


No.	User	Source IP	Begin Time	Descriptio
1	twhite	172.20.120.23	Wed Apr 17 11:41:06 2013	
Subsession			Web Application:RDP 192.168.1.114	

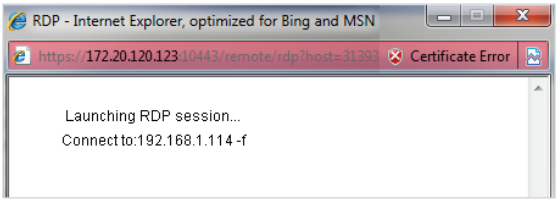
Go to **Log & Report > Traffic Log > Forward Traffic** and view the details for the SSL entry.

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 bookmark Remote Desktop link 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.

No.	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	

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

Dst	192.168.1.114	**Virtual Domain**	root
Received	326664	**Source Country**	Reserved
Sent / Received	54.36 KB / 319.01 KB	**Duration**	83
Sent	55665	**Application Details**	
Group	N/A	**Service**	RDP
Protocol	6	**User**	twhite
Destination Country	Reserved	**Dst Port**	3389
roll	65389	**Status**	✓
Timestamp	Wed Apr 17 14:17:15 2013	**Tran Display**	noop
Sequence Number	3618	**Policy ID**	11
Src Interface	wan1	**Src**	twhite (172.20.120.23)
VPN	sslvpn_web_mode	**Sent Packets**	329
Level	notice	**VPN Type**	sslvpn
Src Port	53820	**Log ID**	13
Sub Type	forward	**Threat**	
Received Packets	407	**Date/Time**	14:17:15 (Wed Apr 17 14:17:15 2013)
Dst Interface	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	10.212.134.200	74.125.133.95	HTTP
	ssl.root	wan1	10.212.134.200	173.194.77.94	HTTP
	ssl.root	wan1	10.212.134.200	173.194.43.79	HTTP
	ssl.root	wan1	10.212.134.200	66.171.121.34 (fortinet.com)	HTTP
	ssl.root	wan1	10.212.134.200	74.121.50.17 (www.pages03.net)	HTTP
	ssl.root	wan1	10.212.134.200	208.91.113.212	HTTPS
	ssl.root	wan1	10.212.134.200	192.168.55.30	KERBE
	ssl.root	wan1	10.212.134.200	192.168.55.30	KERBE
	ssl.root	wan1	10.212.134.200	192.168.55.30	KERBE
	ssl.root	wan1	10.212.134.200	213.199.179.159	40031/
	ssl.root	wan1	10.212.134.200	213.199.179.159	HTTP
	ssl.root	wan1	10.212.134.200	132.246.2.6 (www.msftncsi.com)	HTTP

Select an entry to see more information.

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