

Web VPN / SSL VPN

Since the network secure remote access high demanding large enterprise has risen up. To the users, the most reliable solution is the SSL VPN without installing any software or hardware. Only need to use the web browser and easily access the data transferring by SSL encryption.

The VPN terms

DES

„ The DES(Data Encryption Standard)is a kind of NIST W with 56 bytes preshared key.

3DES

„ The 3DES (Triple Data Encryption Standard)is more secure than DES with 168 bytes .

AES

„ The AES is the high standard of data encryption, and its standard is more strict than the DES. The AES Key Size can divided into 128 bytes, 192 bytes and 256 bytes.

Setting

VPN IP of Client

Creates the SSL VPN between the client and the SG-1000 appliance by login authentication, VPN IP range , encryption algorithm , Protocol , server port and connecting time . And set the end user can use the IP address distribute by the DNS or WINS server , to access the internal resources through the NAT mode.

„



The SSL VPN IP range can not be the same as the segment of LAN (LAN ,Multiple Subnet , DMZ) , WAN and PPTP server.

Internal Subnet of Server

„ To set the client user can access the internal subnet of server.

Status

User Name

„ To display the authentication name used by client.

Real IP

„ To display the client real IP.

VPN IP

„ To display the client IP distributed by the SG-1000.

Uptime

„ To display the uptime between client and SG-1000.

Configure

The MIS engineer can choose to disconnect the SSL VPN. (*Fig. 20-1*)

User Name	Real IP	VPN IP	Uptime	Configure
No Data				

Fig. 20-1 Status list

Set the Web / SSL VPN between SG-1000 and WAN Client

Step1 In **Interface** → **WAN** , enable HTTPS. (*Fig. 20-2*)

Balance Mode : <input type="text" value="Auto"/> (Auto Recommended)								
WAN No.	Connect Mode	IP Address	Saturated Connections	Ping	HTTP	HTTPS	Configure	Priority
1	Static IP	81.11.11.11	<input type="text" value="1"/>	✓	✓	✓	Modify	<input type="text" value="1"/>
2	Static IP	211.22.22.22	<input type="text" value="1"/>	✓	✓	✓	Modify	<input type="text" value="2"/>
3	(Disable)	---	<input type="text" value="0"/>	---	---	---	Modify	<input type="text" value="0"/>
4	(Disable)	---	<input type="text" value="0"/>	---	---	---	Modify	<input type="text" value="0"/>

Fig. 20-2 WAN interface setting

Step2 In **Authentication** → **User** , add the following settings : (*Fig. 20-3*)

Authentication-User Name	Configure
joy	Modify Remove
john	Modify Remove
jack	Modify Remove

New Entry

Fig. 20-3 Authenticaion user setting

Step3 In **Authentication** → **User Group** , add the following settings : (*Fig. 20-4*)

Name	Member	Radius	POP3	LDAP	Configure
laboratory	joy, john, jack				Modify Remove Pause

New Entry

Fig. 20-4 Authentication user group setting

Step4 In **Web VPN / SSL VPN** → **Setting** , add the following settings :

Click **Modify** . (*Fig. 20-5*)

Enable Web VPN.

VPN IP Range, enter 192.168.222.0 / 255.255.255.0 .

Encryption Algorithm, select 3DES .

„ **Protocol**, select TCP .

„ **Server Port** , enter the default value of 1194 .

„ **Authentication User or Group**, select laboratory .

„ **Auto-Disconnect if idle**, enter 0 .

„ Click **OK**.

„ It will automatically add the LAN interface which is the segment that allow the client to access (*Fig. 20-6*)

Web VPN Setting

Enable Web VPN (Please enable TCP port 443 in the "Interface > WAN > HTTPS")

VPN IP Range: 192.168.222.0 / 255.255.255.0

Encryption Algorithm: 3DES

Protocol: TCP

Server Port: 1194 (Range: 1024 - 65535)

Enable DNS and WINS server addresses to clients

DNS Server 1:

DNS Server 2:

WINS Server 1:

WINS Server 2:

Enable NAT mode

Authentication User or Group: laboratory

Auto-Disconnect if idle: 0 Minutes (Range: 0 - 120; 0 means always connected)

OK Cancel

Fig. 20-5 Enable Web VPN

Web/SSL VPN Example

VPN IP of Client

Web VPN : Enable (Server ports are TCP 443 and TCP 1194)

VPN IP Range : 192.168.222.0

Netmask : 255.255.255.0

Encryption Algorithm : 3DES

Authentication User or Group : laboratory

Modify

Internal Subnet of Server

Internal Subnet	Netmask	Configure
192.168.1.0	255.255.255.0	Modify Remove

New Entry

Fig. 20-6 Enable Web VPN

Step5 Enter the following settings in client web browser :

In **Address**, enter `http://61.11.11.11/sslvpn` or `http://61.11.11.11/webvpn` (It is the SG-1000 interface add the sslvpn or webvpn string) .

Click **Enter** (*Fig. 20-7*)

In **Security Alert** ,click **OK** .

In **Security Alert** , click **OK** .

In **Warning HTTPS** , click **Yes** .

In **Warning Security** , click **Yes** .

In **Authentication** , enter josh in **User Name** and 123456789 in **Password** . (*Fig. 20-8, Fig. 20-9, Fig. 20-10, Fig. 20-11, Fig. 20-12*)

Click **OK** . (*Fig. 20-13, Fig. 20-14*)

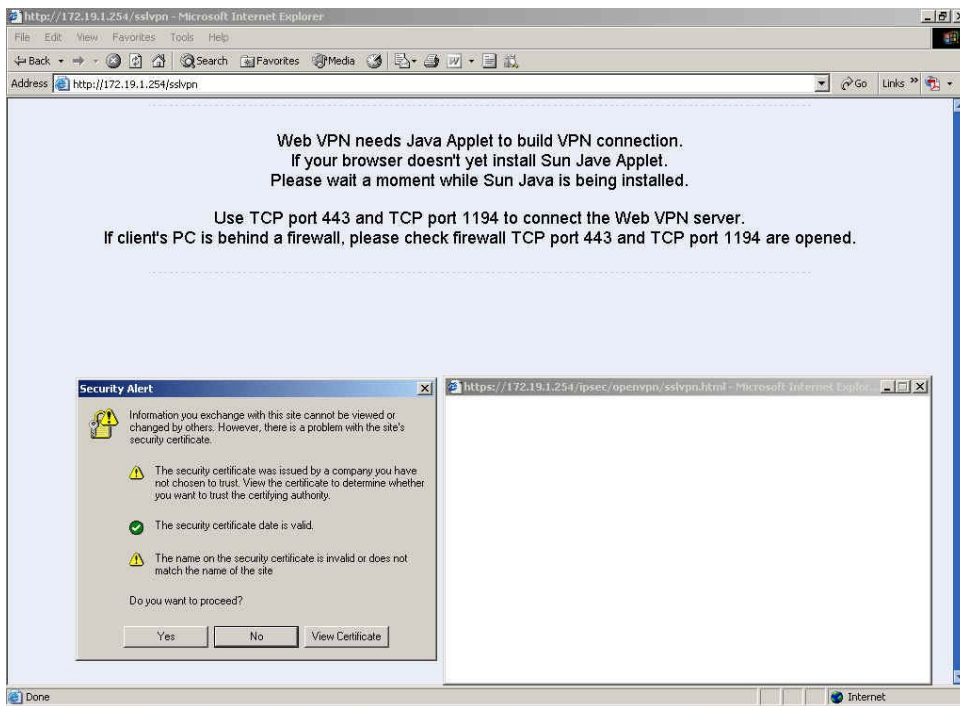


Fig. 20-7 Login SSL VPN



Fig. 20-8 The warning security window



Fig. 20-9 The warning security window



Fig. 20-10 The warning HTTP window



Fig. 20-11 The warning security window



Fig. 20-12 The authentication window

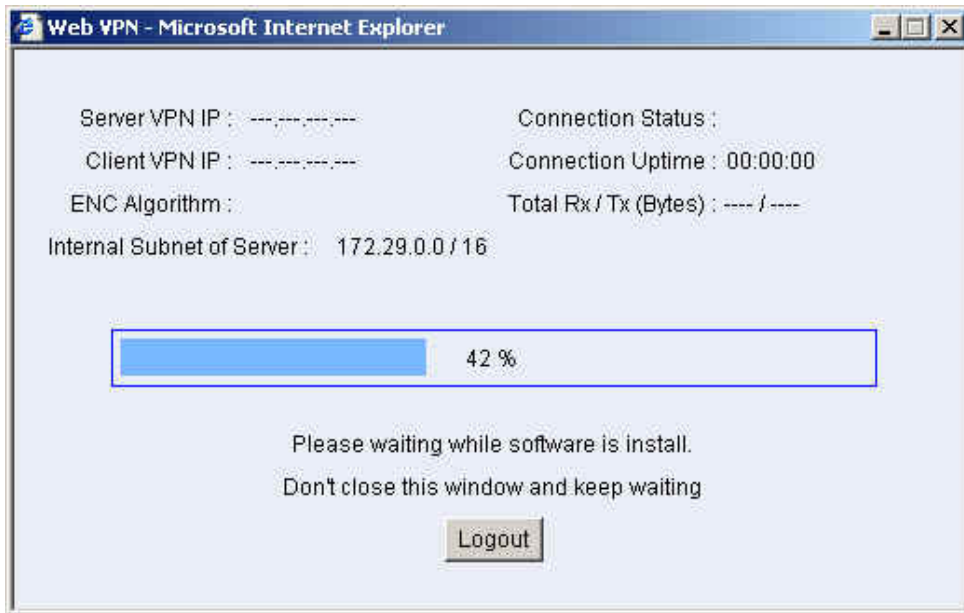


Fig. 20-13 The SSL VPN connection

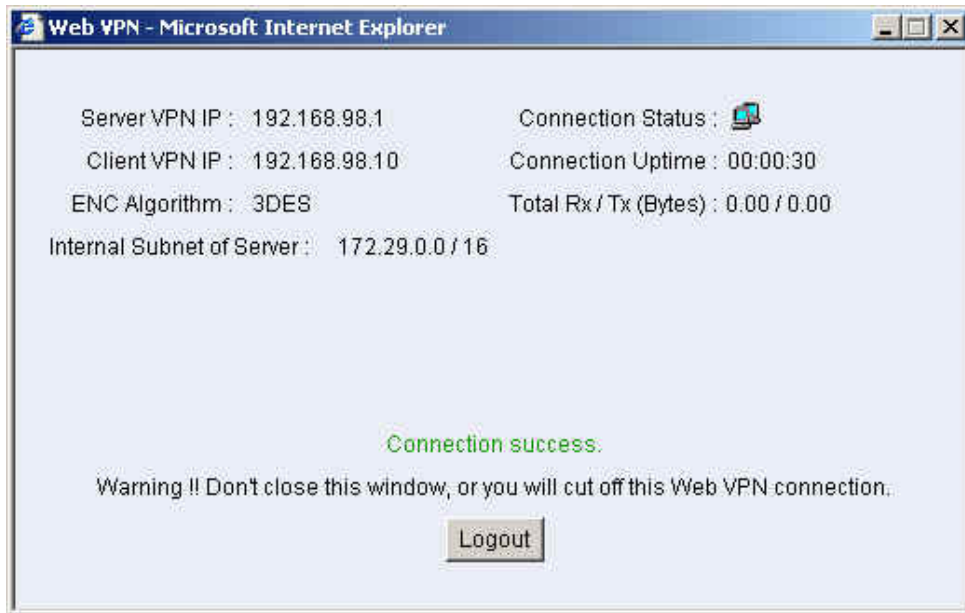


Fig. 20-14 Complete the SSL VPN connection

Step6 In **Web VPN / SSL VPN** → **Status**, it shows the connection status : (*Fig. 20-15*)

User Name	Real IP	VPN IP	Uptime	Configure
john	220.132.112.108	192.168.222.10	0:01:24	Disconnect

Fig. 20-15 SSL VPN status



When the client PC is not installed the SUN JAVA runtime environment software , it will automatically download and install this software as in SSL VPN connection (Fig. 20-16, Fig. 20-17) .



Fig. 20-16 The Java runtime environment plug-in CA certificate



Fig. 20-17 The Java runtime environment plug-in installation