



AnexGATE

(A Division of SSSPL)

Connectivity.Security.Productivity.Manageability



Installation Guide

www.anexgate.com

Table of Contents

Table of Contents

Quick Installation Guide.....	3
1 How to set up the AnexGATE firewall?	3
WELCOME TO ANEXGATE GUI	4
2 How to configure the Local Domain and Network Interfaces.	4
To configure the WAN—	4
To Configure the LAN –	5
CONFIGURE YOUR LOCAL DOMAIN AND DNS IP.	7
3. How to configure the Proxy ,content filtering in the AnexGATE.	7
4. How to create the default rule and Group rules in the AnexGATE Proxy.....	11
5 -How to configure the Group rules in the AnexGATE Proxy	14
6. How to configure the Time Period policy for Proxy users.	17
7.How to configure the firewall filter rule for the AnexGATE and enable to the AnexGATE for remort support.....	19
8- How to configure the PPTP VPN and IPSEC VPN in the AnexGATE.....	22

Quick Installation Guide

1 How to set up the AnexGATE firewall?

Ans- Switch on you AnexGATE and connect a monitor to see the booting of AnexGATE. After booting connect a cross cable one end into the LAN 3 port (In four port appliance) or LAN 4 port (in 6 port Appliance) and the other end to your LAPTOP or desktop.

As the AnexGATE by default IP is 192.168.10.1 , configure your LAPTOP /Desktop in the 192.168.10.x series like below-

IP—192.168.10.11

Subnet- 255.255.255.0

Gateway – 192.168.10.1

Primary DNS—192.168.10.1

After this now open a browser like Mozilla or IE version7 or 8 and hit the anexgate ip 192.168.10.1

Put the username password as the bydefault username /password is admin/admin00

Agree the terms and condition and

WELCOME TO ANEXGATE GUI

2 How to configure the Local Domain and Network Interfaces.

Ans -- To configure the you LAN and WAN IP please follow the below path

To configure the WAN—

Click on Network ---→Network Interface -→ WAN

Click on WAN1 interface—

Description – Put the description of your WAN interface Like BSNL , Airtel , Sify etc.

Port Name—WAN1 (By default)

Hardware Type – Ethernet (By default)

Port Speed -- Auto

MTU – 1500(By default)

Clone MAC address --

Interface Type—select your type for WAN like Static, DHCP, PPOE

Interface IP – configure your interface IP

Subnet Mask – provide by ISP

Broadcast IP – by default it will take after configure the subnet mask

Gateway—provided by ISP

Click Submit tab (wait until done) Please refer below Screen shot .

Similarly YOU CAN CONFIGURE ANOTHER WAN PORT

▼ WAN

Description	CITY ONLINE
Port Name	wan1
Hardware Type	Ethernet
Port Speed	Auto
Select VLAN Port	None
MTU*	1500
Clone MAC Address	
Interface Type	Static WAN

Configure Static WAN

Interface IP*	203.192.246.74
Subnet Mask*	255.255.255.248
Broadcast Address*	203.192.246.79
Gateway*	203.192.246.73

To Configure the LAN –

Network – Network Interface → LAN

Description – Provide any Name for your LAN

Port Name - LAN1 (by default)

Hardware type -- Ethernet (By default)

Port Speed -- Auto

MTU -- 1500 (By default)

Interface Type – Static LAN

Interface IP – configure your LOCAL LAN IP

Subnet – subnet of your local LAN

Broadcast IP – it will take automatically

DHCP – if you want to enable the DHCP check this tab (note-- use only if you want to use anexgate as a DHCP server. If you have any another DHCP server in your local LAN please do not enable this tab)

Click on submit (wait up to done).

Please refer below screen shot.

LAN

Description: SSSPL LAN

Port Name: lan1

Hardware Type: Ethernet

Port Speed: Auto

MTU*: 1500

Interface Type: Static LAN

Configure Static LAN

Interface IP*: 192.168.2.10

Subnet Mask*: 255.255.255.0

Broadcast Address*: 192.168.2.255

DHCP Enable:

Configure DHCP Server

Dynamic DNS:

Lease Time (Hours)*: 24

Pool Start IP*: 192.168.2.100

Pool End IP*: 192.168.2.150

DNS Domain Name:

DNS Server IP1: 192.168.2.10

DNS Server IP2:

Router IP: 192.168.2.10

NOTE-- SIMILARLY YOU CAN CONFIGURE ANOTHER LAN INTERFACE IF YOU WANT TO USE.

CONFIGURE YOUR LOCAL DOMAIN AND DNS IP.

Click on Network – Network --- domain – DNS configuration

Domain name -- configure your local domain (ex. box.sssl.co.in)

Use LAN1 IP for Domain name resolution (DNS) – enable

Alternate DNS server – enable and configure your ISP DNS IP.

Click on submit after configuration. Please refer below screen shot

Physical interfaces and networking parameters

Domain Network Interfaces Static Routes Multicast Routes

Domain

DNS Configuration Domains Conditional Forwarders

DNS Configuration	
Domain Name *	<input type="text" value="box.sssl.co.in"/>
Use lan1 IP for Domain Name Resolution	<input checked="" type="checkbox"/>
Enable Alternate DNS Servers	<input checked="" type="checkbox"/>
Alternate DNS Server IP1 *	<input type="text" value="4.2.2.2"/>
Alternate DNS Server IP2	<input type="text" value="203.192.246.2"/>

3. How to configure the Proxy, content filtering in the AnexGATE.

ANS -- to configure the Proxy (Non Transparent) please follow the below steps.

1. Click on the Security -> firewall -> Rule

The AnexGATE firewall is having some by default like below ---

The screenshot shows the 'Configure Security Settings for the Firewall' interface. The 'Rules' tab is selected, and a table of rules is displayed. The first rule, 'Web Proxy', has its 'Enable' field set to 'true', which is circled in red. The other rules shown are 'POP3 Proxy' (Enable: false), 'SMTP Proxy' (Enable: false), and 'ICMP/Ping to ALL' (Enable: true). A 'Submit' button is visible at the bottom left of the configuration area.

Rules	Predefined Rules	NAT	Net Map	Tunnels	Proxy ARP	Policy	View Zones	Emergency Access	Time Group
> Rules	A+ A+ ↓ ↑								
Rule Number 1	Enable true	Rule Name Web Proxy	Action Redirect	Source Zone LAN	Source Interface Any				
> Rules	A+ A+ ↓ ↑								
Rule Number 2	Enable false	Rule Name POP3 Proxy	Action Redirect	Source Zone LAN	Source Interface Any				
> Rules	A+ A+ ↓ ↑								
Rule Number 3	Enable false	Rule Name SMTP Proxy	Action Redirect	Source Zone LAN	Source Interface Any				
> Rules	A+ A+ ↓ ↑								
Rule Number 4	Enable true	Rule Name ICMP/Ping to ALL	Action Accept	Source Zone LAN	Source Interface Any				

Showing 1 - 4 of 4
* Displaying 10 records per page

Submit

Just disable the web proxy (Rule No 1) redirection rule and submit.

After that Click on Proxy TAB --- web proxy,

Configure the web proxy like below---

Web Proxy --- Enable (check the Box)

Click on Option –

Enable Web Guard --- Enable

Enable web Cache – Enable

Web cache size in MB – 2000 in MB (By default , you can increase upto 2000000 MB)

No of Child Process – 10 (By Default)

Port No --- 3128 (By default proxy port) { change the port as per your network proxy port)

Enable site access through IP address – If you want to access the website through IP address enable this option

Log Blocked Site --- Enable

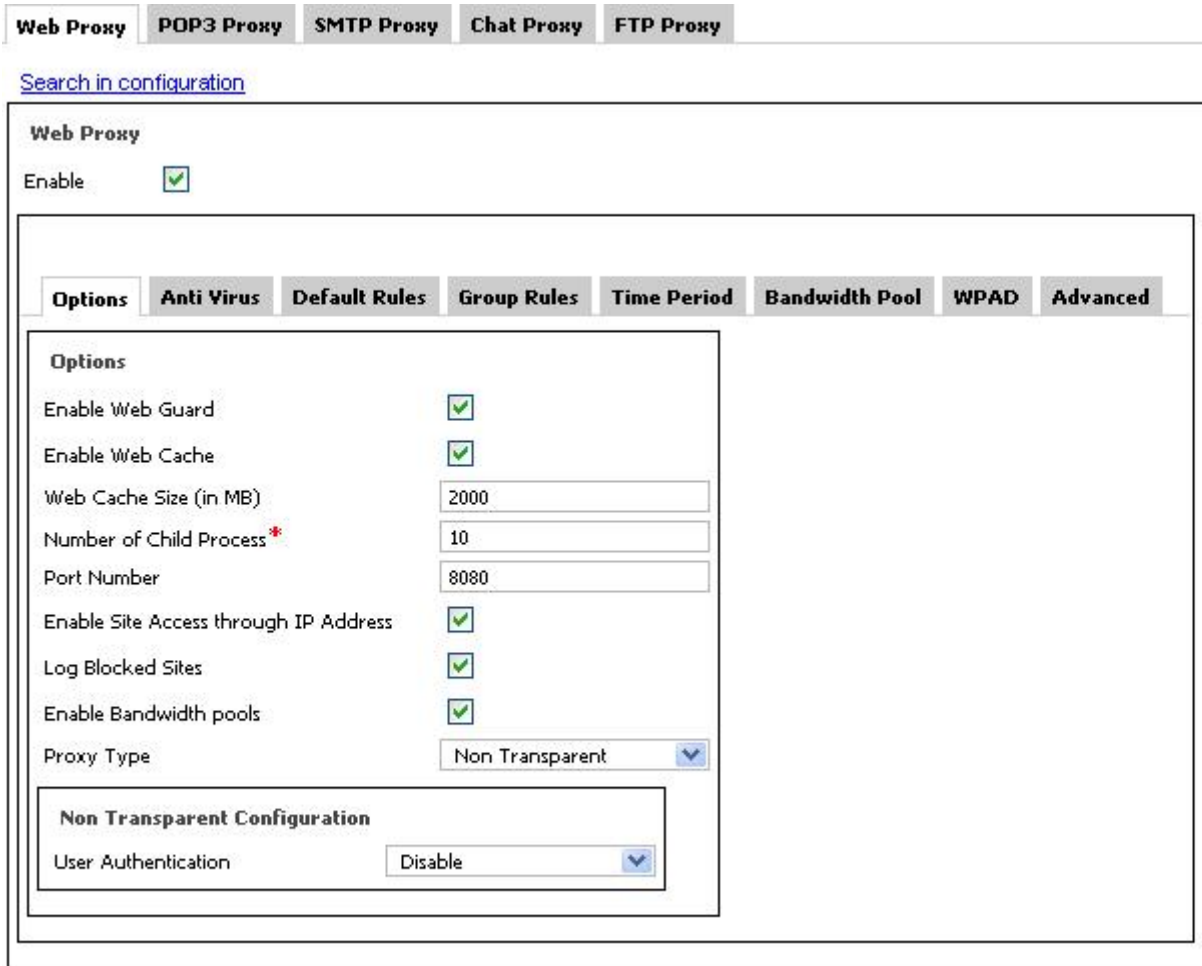
Proxy Authentication -- Non Transparent

User Authentication -- Disable (If you do not want user proxy with user name Authentication)

You can also use the Authentication method like External LDAP (Active directory) or Internal LDAP.

Click on Submit after configuration

Please refer below screen shot



If you select the user authentication with internal LDAP you need to configure user in the AnexGATE user management please follow the below path

Services → User Management

Create the user and enable the web access account.

Please refer below screen shot

[System](#)
[Network](#)
[Security](#)
[VPN](#)
[Proxy](#)
[Services](#)

[User Management](#)
[Monitoring](#)
[Reporting](#)
[Mail Server](#)
[Pop Mail](#)
[SNMP](#)

[Search in configuration](#)

User Management

[Users](#)
[Mail Domains](#)

Users

[A+](#)
[A+](#)
🗑️

First Name*
 Last Name*
 User-ID*
 Password*
 Confirm Password*
 User Type

Configuration Details

Create Mail Account

Create IM Account

Enable Web Access

Create PPTP Account

4. How to create the default rule and Group rules in the AnexGATE Proxy.

Ans- To configure the default rule in the AnexGATE Proxy please find the below path..

Proxy → Web proxy → Default Rules

Bandwidth Pool – Default

Max Simultaneously connection per user/ip -- By default its is 50

Http download limit --- to limit the http download for proxy user (Unlimited by default)

Https upload limit --- to limit the upload size for proxy users (unlimited by default)

Enable mime type --- check the box for enable (to limit the Audio, video and application, multipart etc)

Default Rule – Configure the default proxy rule for the Network .Define the custom category to allow and blocked.(Unselected mean allowed)

Allowed domain—Allow some particular domain for the Proxy users.

Blocked Domain – Blocked the domain for the network i.e orkut.co.in, Microsoft.com etc.

All other sites -- Allow or Blocked (Define for all other sites).Please refers below screen shot for the same.

After the above configuration please click on submit until done.

[Search in configuration](#)

Web Proxy

Enable

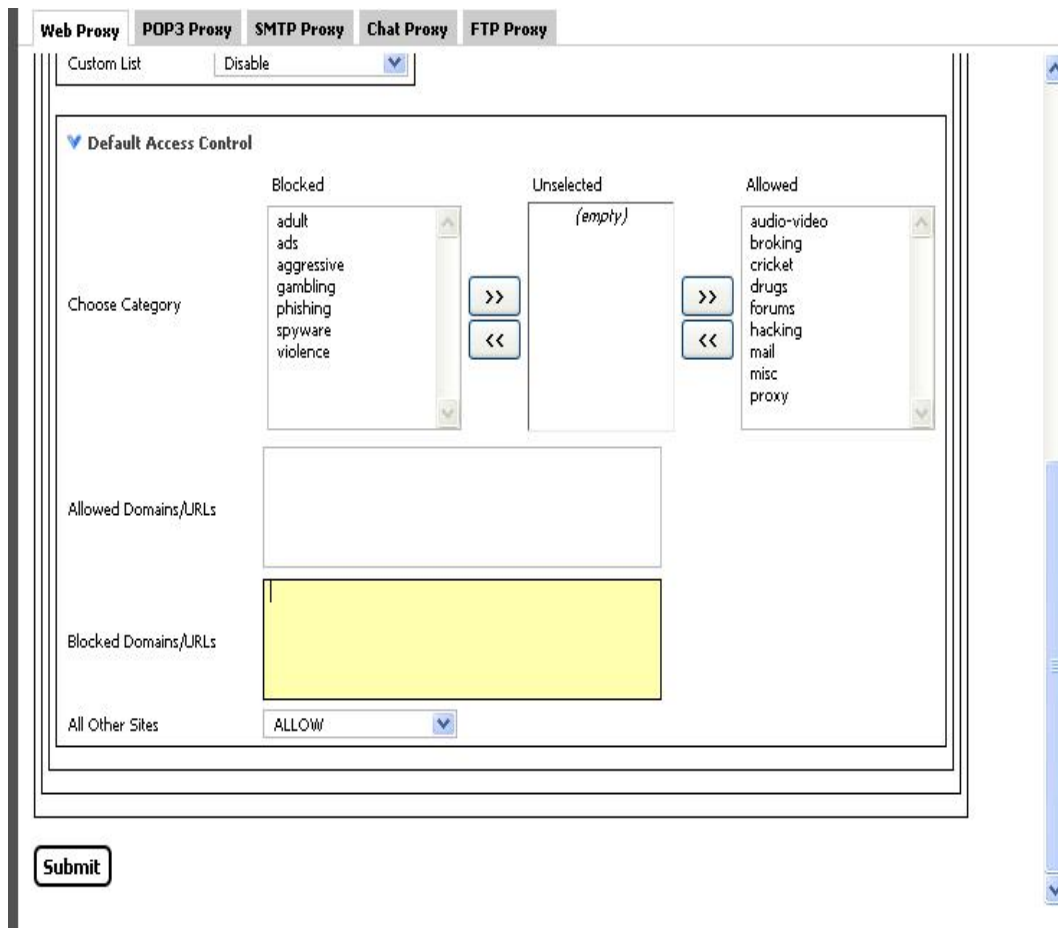
Options Anti Virus Default Rules Group Rules Time Period Bandwidth Pool WPAD Advanced

Default Rules

Bandwidth Pool
Max. Simultaneous Connections per User/IP
HTTP Download Limit
HTTP Upload Limit
Enable Mime Type Filter

Mime Type Filter

Block Audio
Block Video
Block Application
Block Multipart
Block Image
Custom List



5 -How to configure the Group rules in the AnexGATE Proxy .

Ans— Go to proxy → Web Proxy -→ Group Rules-→

In the group rules you can create and define the various policies for the groups .please see the below configuration

Enable Rule – Enable the Rules for the Group.

Rule No --Define as per your requirement .

Rule Name -- Define the Name for the Group

Do not generate the Report for this Group – enable or disable as per requirement.

IP address Group --- define the IP address of the Group Member.

User Group --- If the Proxy is on User Authentication Mode select the member of the Group.

No. of the Connection per Client -- 50 By Default

Http downlimit --- Set as per requirement (unlimited By Default)

Http download limit – Set as per requirement (Unlimited By default)

Mime type filter – Set as per requirement

Enable Time Period --- Enable if you want to define the time period wise policies.






Bandwidth Pool – By default

Define Access Control – as per requirement

Click on submit after configuration. Please refer below screen shot for help.

Web Proxy POP3 Proxy SMTP Proxy Chat Proxy FTP Proxy

Options Anti Virus Default Rules **Group Rules** Time Period Bandwidth Pool WPAD Advanced

Group Rules     

Enable Rule


Rule Number


Rule Name*

Do Not Generate Report For This Group

IP Address Group


Number of Connections per Client

HTTP Download Limit 

HTTP Upload Limit 

Enable Mime Type Filter

Enable Time Period

Bandwidth Pool 

Default Access Control

Name – define the time period name please refer the screen shoot

Web Proxy **POP3 Proxy** **SMTP Proxy** **Chat Proxy** **FTP Proxy**

[Search in configuration](#)

Web Proxy

Enable

Options **Anti Virus** **Default Rules** **Group Rules** **Time Period** **Bandwidth Pool** **WPAD** **Advanced**

Time Period A+ A+ 🗑️

Enable

Name

+ Create New Specify Time Duration

Submit

Click on Create new Specify time duration

Define the type – Week Based or date Based

Name – Duration Rule or any Name for the Rule

Please refer below screen shot

Specify Time Duration

Type: Week Based

Name: Duration Rule

WeekDay Rule

Select All Days

Mon

Tue

Wed

Thu

Fri

Sat

Sun

Time

From Hour (hh)*: 00

From Minute (mm)*: 00

To Hour(hh)*: 23

To Minute(mm)*: 59

After Configure the time slots you will get a new TAB at Group rule Access control within Time Slots and you can configure the time policy as same like the default rule.

7.How to configure the firewall filter rule for the AnexGATE and enable to the AnexGATE for remote support.

ANS- To configure the firewall filter rule click on Security--→Firewall -→ Rules

You will get some bydefault rules that is already configure.

To add a new rule Just click on Add above or add below rule A+.

You will get the tab like below-

Rule Number	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/>
Rule Name	<input type="text"/>
Action	<input type="text" value="Accept"/>
Source Zone	<input type="text" value="LAN"/>
Source Interface	<input type="text" value="Any"/>
Source IP/MAC Address	<input type="text"/>
Dest Zone	<input type="text" value="WAN"/>
Dest Interface	<input type="text" value="Any"/>
Dest IP Address	<input type="text"/>
Forward Port To	<input type="text"/>
Redirect Port To	<input type="text"/>
Protocol	<input type="text" value="TCP"/>
Original Dest Port	<input type="text"/>
ICMP Type	<input type="text"/>
Source Port	<input type="text"/>
Original Dest IP	<input type="text"/>
Rate Limit Per Second	<input type="text"/>

Enable—to enable or disable the rule

Rule Name – provide the rule name

Action – select the action Accept, Reject, Drop, Forward, Redirect

Source Zone—Select the Source Zone for the rule like LAN, WAN DMZ

Source Interface- select the Interface for the Particular Interface like lan1,wan1 etc Any is bydefault

Source IP—slect the source IP to create the rule for perticuluar IP or Subnet

Dest,Zone—select the destination zone for the firewall rule

Dest. Interface- select the destination interface like wan1,lan1 Any will be bydefault\

Deat. IP—enter the IP {if you want to create the rule for particular destination IP

Forward port-- add the forward port if required

Redirect port – Add the redirect port

Protocol- Select the Protocol like TCP, UDP, ICMP, All

Destination Port—Add the destination port

Original Destination IP – Add the destination IP

EX—Configure the Rule to open the custom firewall port for FTP, TELNET, SSH, and other Ports

The Rule be like below screen shot

Rule Number	1
Enable	<input checked="" type="checkbox"/>
Rule Name	CUSTOM PORT
Action	Accept
Source Zone	LAN
Source Interface	Any
Source IP/MAC Address	
Dest Zone	WAN
Dest Interface	Any
Dest IP Address	
Forward Port To	
Redirect Port To	
Protocol	TCP
Original Dest Port*	21,22,23,3000,3389
ICMP Type	
Source Port	
Original Dest IP	
Rate Limit Per Second	

And just submit the rule. The firewall will open the particular port from Source zone LAN to destination zone WAN.

If you want to configure the firewall rule for particular source and destination just add the source and destination IP.

To Enable to remote support for AnexGATE just click the Security --- firewall -->Predefined Rule and just enable the rule no 1 SECURE WEB LOGIN and Submit. Refer the below screen shot

▼ Predefined Rules	
Rule Number	1
Enable	<input checked="" type="checkbox"/>
Rule Name	Secure Web Login
Action	Accept
Source Zone	ALL
Source Interface	Any
Source IP/MAC Address	
Dest Zone	THIS-FIREWALL
Dest Interface	Any
Dest IP Address	
Forward Port To	
Redirect Port To	
Protocol	TCP
Original Dest Port*	4343
ICMP Type	
Source Port	

8- How to configure the PPTP VPN and IPSEC VPN in the AnexGATE

ANS- To configure the PPTP VPN please follow the below instruction.

please clicks on Security -->Firewall ->Tunnel and add new

▼ Tunnels	
Rule Number	1
Enable	<input checked="" type="checkbox"/>
Tunnel Name	PPTP vpn
Type	PPTP VPN
Zone*	WAN

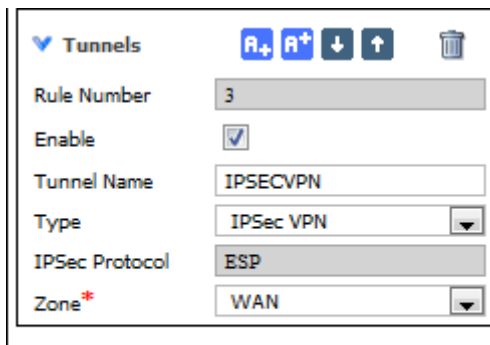
Enable --- to enable the rule

Tunnel Name – Give the Tunnel name

Type – Select the Type like PPTP VPN or IPSEC VPN

Zone – Zone will be WAN for PPTP and IPSEC VPN

NOTE – If you want to configure the PPTP and IPSEC VPN you have create separate rule for both (PPTP and IPSEC)



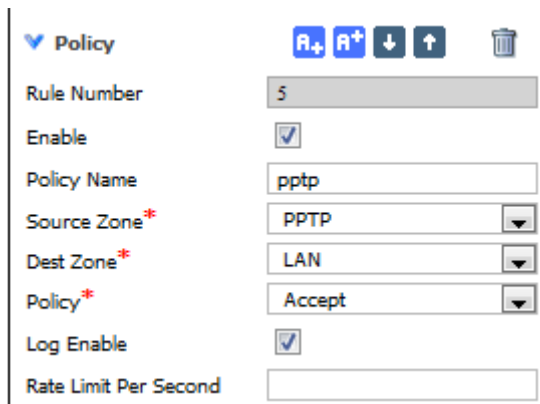
The screenshot shows a configuration form for a tunnel. At the top, there is a section titled "Tunnels" with a dropdown arrow on the left and four action buttons (Add, Edit, Down, Up) and a delete icon on the right. Below this, the form contains the following fields:

- Rule Number: 3
- Enable:
- Tunnel Name: IPSECVPN
- Type: IPsec VPN (dropdown menu)
- IPSec Protocol: ESP
- Zone*: WAN (dropdown menu)

Submit

Just click on submit to save the configuration

After the above configuration click on Security--- Firewall ---Policy and add the below two rule for PPTP



The screenshot shows a configuration form for a policy. At the top, there is a section titled "Policy" with a dropdown arrow on the left and four action buttons (Add, Edit, Down, Up) and a delete icon on the right. Below this, the form contains the following fields:

- Rule Number: 5
- Enable:
- Policy Name: pptp
- Source Zone*: PPTP (dropdown menu)
- Dest Zone*: LAN (dropdown menu)
- Policy*: Accept (dropdown menu)
- Log Enable:
- Rate Limit Per Second: (empty text box)

▼ Policy <input type="button" value="R+"/> <input type="button" value="R+"/> <input type="button" value="↓"/> <input type="button" value="↑"/> <input type="button" value="🗑️"/> 	
Rule Number	6
Enable	<input checked="" type="checkbox"/>
Policy Name	pptp
Source Zone*	LAN
Dest Zone*	PPTP
Policy*	Accept
Log Enable	<input checked="" type="checkbox"/>
Rate Limit Per Second	

And submit the configuration.

No need to add any additional rule in the POLICY for IPSEC VPN

After the Above configuration click on VPN --- PPTP

For the configuration of PPTP server please follow the below screen shot-

Configure PPTP	
Enable	<input checked="" type="checkbox"/>
PPTP VPN Configuration	
Server PPTP IP Address*	10.10.10.10
Client IP Pool*	10.10.10.11-100
CHAP	<input type="checkbox"/>
MS-CHAP-v1	<input type="checkbox"/>
MS-CHAP-v2	<input checked="" type="checkbox"/>
MPPE Encryption	128bit
DNS Server1	
DNS Server2	
WINS Server	
Client Idle Time Out (in sec)	18000
Client Failure Time Out (in sec)	60
Proxy ARP	<input type="checkbox"/>
Broadcast Relay Interface	none

Server IP address – Add any local IP address Except the IP of your Local LAN series

Client Pool -- Give the range of IP for the PPTP client

All other configuration is by default and submits to save the configuration.

After configure the PPTP server configure the PPTP users (VPN users)

To create the user click on Service --> User management and add the user.

Refer below screen shot---

The screenshot shows a web-based user configuration interface. At the top, there's a header 'Users' with two blue icons (A+ and A+) and a trash icon. Below this, there are several input fields: 'First Name*' with 'admin', 'Last Name*' with 'admin', 'User-ID*' with 'admin', 'Password*' with masked characters, and 'Confirm Password*' with masked characters. A 'User Type' dropdown menu is set to 'Administrator'. Below these fields are two sections: 'Configuration Details' with four checkboxes: 'Create Mail Account' (checked), 'Create IM Account' (unchecked), 'Enable Web Access' (checked), and 'Create PPTP Account' (checked). The second section is 'PPTP Configuration' with a field for 'Client PPTP IP Address'.

Configure the TAB and username and password and just enable the Create PPTP Account

Client IP Address--- Add the ip in the range of PPTP client IP pool.

To define the PPTP IP for the particular user add IP in the Client PPTP IP address and submit to submit to the configuration.

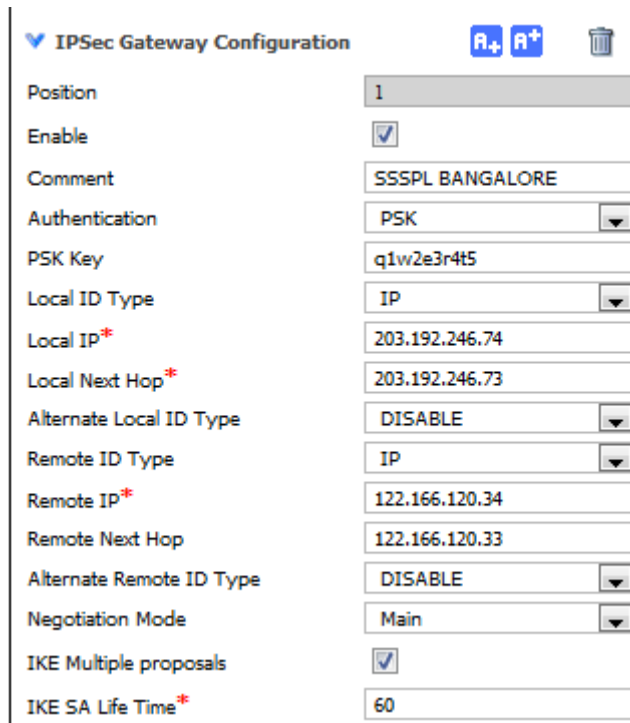
TO configure the IPSEC server click one VPN --- IPSEC VPN

Enable – to Enable the IPSEC VPN server

Enable NAT-T support --- Enable for the NAT traversal

Then Click on Add IPSEC GATEWAY

Please refer the below screen shot



The screenshot shows the 'IPSec Gateway Configuration' form. It includes fields for Position (1), Enable (checked), Comment (SSSPL BANGALORE), Authentication (PSK), PSK Key (q1w2e3r4t5), Local ID Type (IP), Local IP* (203.192.246.74), Local Next Hop* (203.192.246.73), Alternate Local ID Type (DISABLE), Remote ID Type (IP), Remote IP* (122.166.120.34), Remote Next Hop (122.166.120.33), Alternate Remote ID Type (DISABLE), Negotiation Mode (Main), IKE Multiple proposals (checked), and IKE SA Life Time* (60).

Position	1
Enable	<input checked="" type="checkbox"/>
Comment	SSSPL BANGALORE
Authentication	PSK
PSK Key	q1w2e3r4t5
Local ID Type	IP
Local IP*	203.192.246.74
Local Next Hop*	203.192.246.73
Alternate Local ID Type	DISABLE
Remote ID Type	IP
Remote IP*	122.166.120.34
Remote Next Hop	122.166.120.33
Alternate Remote ID Type	DISABLE
Negotiation Mode	Main
IKE Multiple proposals	<input checked="" type="checkbox"/>
IKE SA Life Time*	60

Enable – to Enable the Rule

Comment—Add the name for Rule

Authentication – Select PSK (Phase shift Key)

PSK Key—configure the PSK Key for the IPSEC Network

Local IP – select IP (for gateway to gateway configuration)

Local IP—configure your Static IP Hosted in your firewall

Local Nest Hop – Configure the gateway of Static IP hosted on AnexGATE

Alternate Local ID Type – Disable

Remote ID Type – IP

Remote IP – configure the Static IP of Your Destination Network (Client Static IP)

Remote Next Hop – configure the Gateway of your Remote Destination network

Alternate Remote ID type – Disable

Negotiation Mode – main

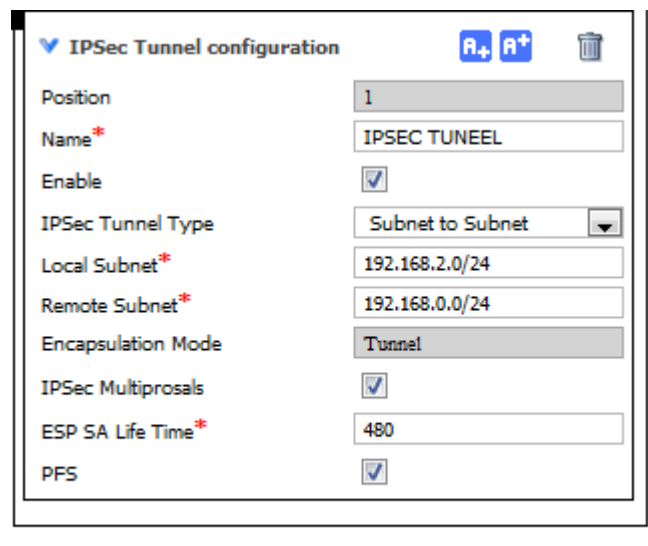
IKE Multiple Proposals – Enable

IKE SA Life time -- 60 By default that can be MAX 480 Min

After the above configuration add the IP Sec Tunnel

Click on Add IPSEC Tunnel

Refer the below screen shot



The screenshot shows the 'IPSec Tunnel configuration' window. It contains the following fields and values:

Field	Value
Position	1
Name*	IPSEC TUNEEL
Enable	<input checked="" type="checkbox"/>
IPSec Tunnel Type	Subnet to Subnet
Local Subnet*	192.168.2.0/24
Remote Subnet*	192.168.0.0/24
Encapsulation Mode	Tunnel
IPSec Multiprosals	<input checked="" type="checkbox"/>
ESP SA Life Time*	480
PFS	<input checked="" type="checkbox"/>

Submit

Name – Create the IPSEC Tunnel Name

Enable – to Enable the Tunnel

IP Sec Tunnel name – Subnet to Subnet/Host to Subnet / Subnet to Host

Local Subnet – configure the Local Subnet of your Network

Remote Subnet – Configure the Remote Network Subnet

Encapsulation Mode – Tunnel

IP Sec Multiprosals – Enable

ESP SA Life Time – 60 Min By Default (MAX upto 480 Min)


PFS – Enable

Submit to save the configuration

To check the IP SEC connection Click on Node Status -> IP Sec VPN and click on details

Port Status	Bandwidth Usage	System Status	Process List	Service Detail	SecureVPN	PPTP	IPSecVPN	WIFI HotSpot
-------------	-----------------	---------------	--------------	----------------	-----------	------	----------	--------------

IPSec Active Sessions

State	Name	Tunnel ID	Status	Remote Gateway	Details
	IPSEC TUNEEL	ipsectunnel_1_1	Phase 2 Quick mode/IPSec SA Established	122.166.120.34	Details



AnexGATE

Connectivity.Security.Productivity.Manageability

AnexGATE

www.anexgate.com

Contact Address:
AnexGate Network Security Solution Division,
Smile Security and Surveillance Pvt. Ltd.(SSSPL)
HQ, #21/2, MRI Building, First Floor, 14KM, Old Madras Road, Bhattarahalli,
K.R Puram, Bangalore -560 049. (INDIA)
Tel : +91- 80- 25614 773/774/775/776 Fax: +91- 80- 25614666

