Configuration Example for the D-Link NetDefend Firewall Series

[Case]

Configure SIP ALG for SIP Phone

Implement mode: DFL-210/260/260E/800/860/860E/1600/1660/2500/2560/2560G

Firmware: 2.27.01

Why SIP

The Session Initiation Protocol (SIP) is widely used on multimedia communication such as voice over IP, video conferring, instant messaging, etc. SIP is responsible for initiating, terminating, and modifying sessions. VoIP is one of the most important SIP applications and provides a chance to move telecommunication from analog TDM signals to digital IP packets. By SIP, VoIP, moreover, can integrate with instant messages or presences services to support unified communications. With expansion of an organization, more and more branches located in different countries are built up. Managers may want to develop an inter-offices telephone system on existing Internet networks rather than on additional PSTN networks. The most attractive reason driving managers to do this is to save money especially for the bill of international calls. In this document, you can find the step by step setting of SIP ALG for SIP phone. Before start, please notice:

- The screenshots of the document are retrieved from firmware version 2.27.01. If you are using the firmware version which earlier than this one, the screenshots may not identical to what you see on your browser.
- To prevent existing setting to interfere with the settings in this guides, reset the firewall to factory defaults before starting.
- For the detail introduction of NetDefend system interface and IP Address insert method, please refer to document “Configure IP Host Network Range”.

How to configure SIP ALG for SIP phone

SUPERSTAR Corporation is an international company with many branches, factory, and warehouses all over the world. In order to save overseas phone bills, SUPERSTAR decides to set up an Internet phone system with a SIP server and several SIP phones.

Helpful Tips

- Create ALGs for specific services
- Create a service object to associate with the ALG function

The network topology (Figure 1) is as below. The external connection “a” refers to wan1 network 192.168.110.0/24 connecting to Firewall at the interface IP 192.168.110.1; the internal connection “b” refers to lan network 192.168.1.0/24 connecting to Firewall at the interface IP 192.168.1.1. The “c” is SIP Phone with IP 192.168.1.247. The external SIP server “d” serves an IP range from 192.92.160.45 to 192.92.160.47.

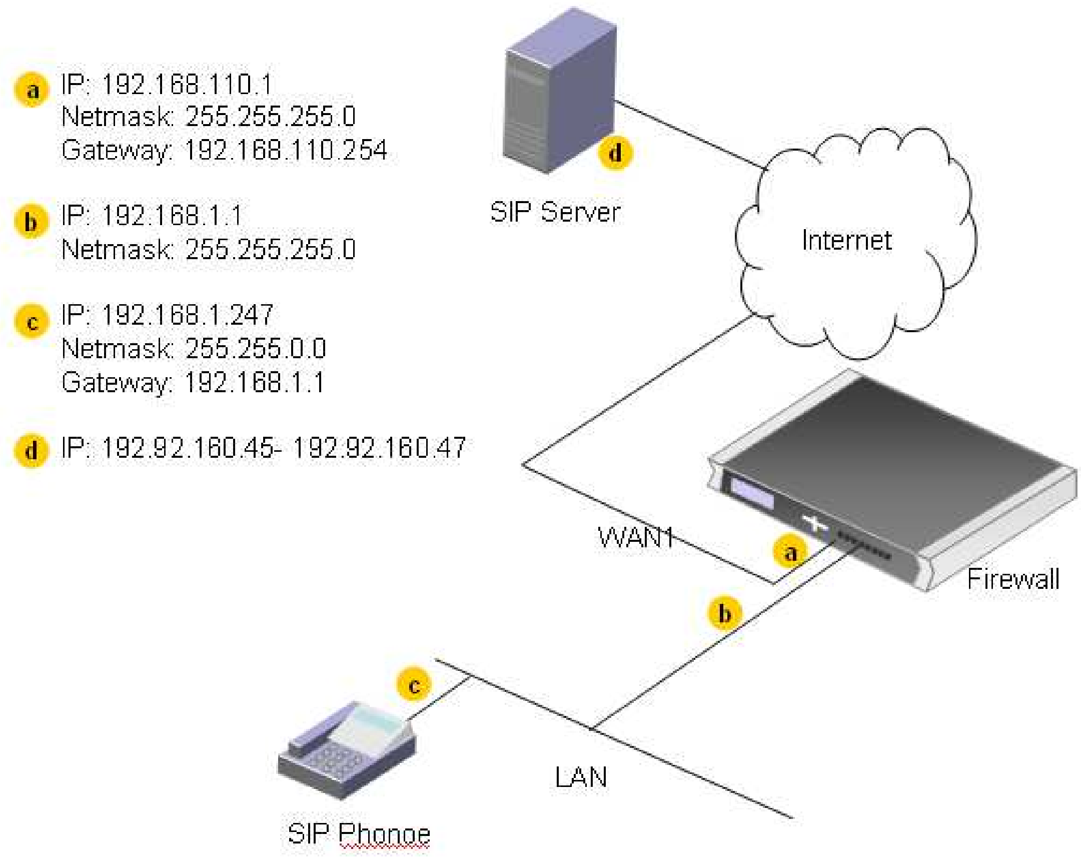


Figure 1: Network Topology

STEP 1: Address

Insert the relative network IP addresses into Address Book. Navigate to **Objects>Address Book> Interface Addresses**. The address data pool for Firewall is:

Name	Address	Remark
wan1_ip	192.168.110.1	wan1 external network connection point to Firewall
wan1net	192.168.110.0/24	wan1 external network group
wan1_gw	192.168.110.254	wan1 external gateway
lan_ip	192.168.1.1	lan internal network connection point to Firewall
lannet	192.168.1.0/24	lan internal network group

Add an additional IP address object for SIP server into Address Book.

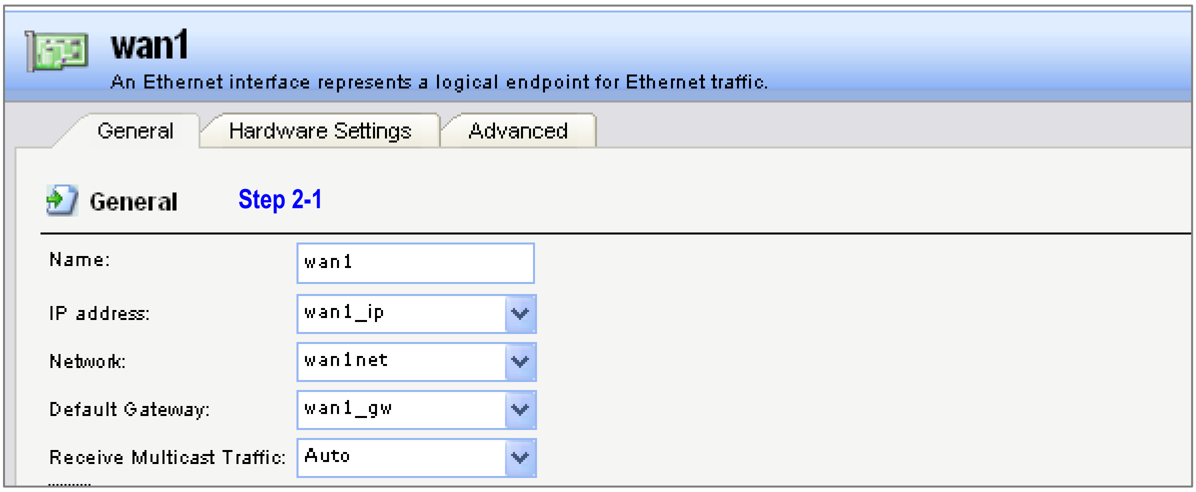
Name	Address	Remark
SIP-server	192.92.160.45-192.92.160.47	SIP server

STEP 2: Ethernet Interfaces

Define Ethernet and LAN interfaces.

Navigate to **Interfaces> Ethernet** > **wan1.**

WAN 1



wan1

An Ethernet interface represents a logical endpoint for Ethernet traffic.

Name: wan1

IP address: wan1_ip

Network: wan1net

Default Gateway: wan1_gw

Receive Multicast Traffic: Auto

Figure 2: Ethernet Interface, Wan 1

In General tab (Figure 2), fill in relative information:

Step 2-1: General

Name: wan1

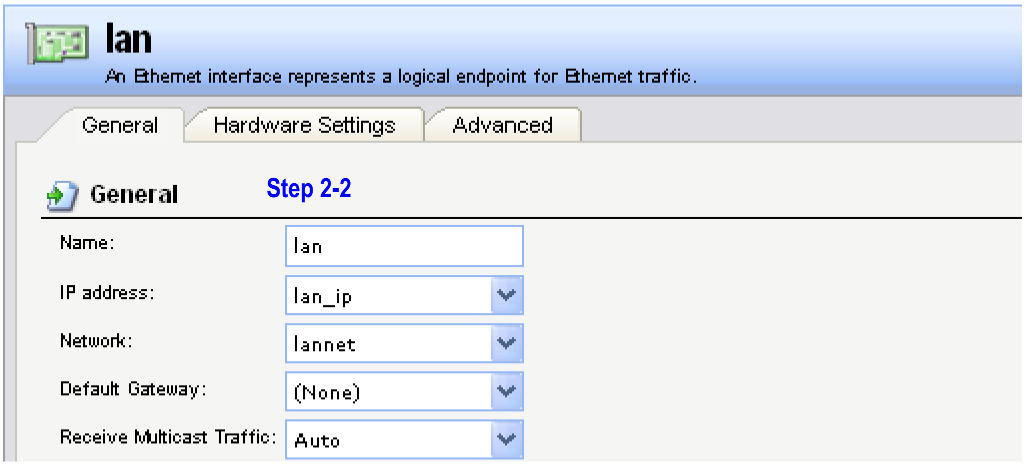
IP address: wan1_ip

Network: wan1net

Default Gateway: wan1_gw

Click OK

Navigate to **Interfaces> Ethernet > lan.**



lan

An Ethernet interface represents a logical endpoint for Ethernet traffic.

General Step 2-2

Name: lan

IP address: lan_ip

Network: lannet

Default Gateway: (None)

Receive Multicast Traffic: Auto

Figure 3: Ethernet Interface, lan

<u>LAN</u>

In General tab (figure 3), fill in relative information:

Step 2-2: General

Name: lan

IP address: lan_ip

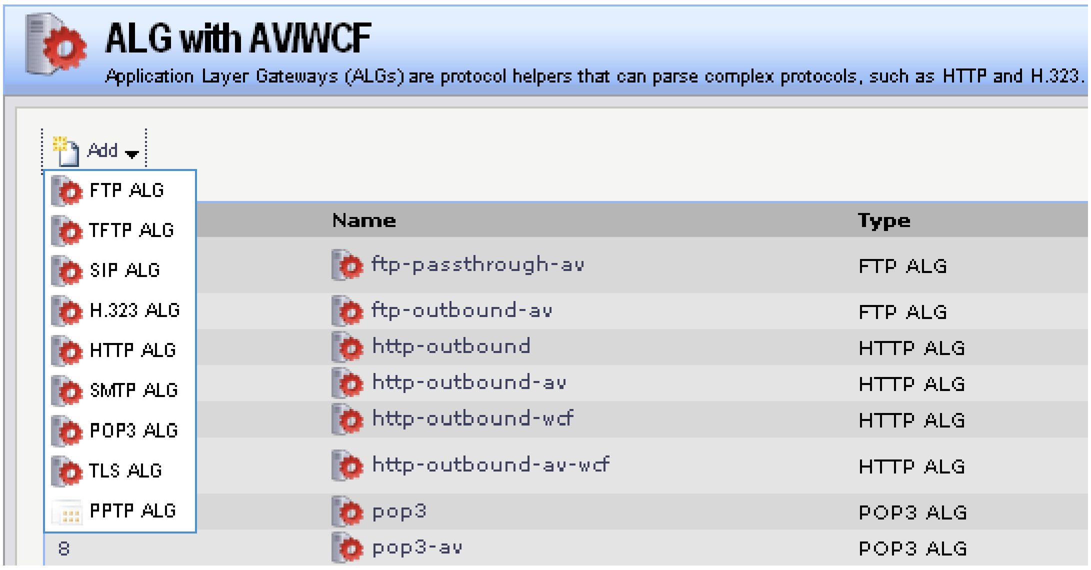
Network: lannet

Default Gateway: (None)

Click OK

STEP 3: ALG with AV/WCF

Navigate to **Objects> ALG with AV/WCF** and add a new *SIP ALG* or edit the pre-define rule *SIP*.

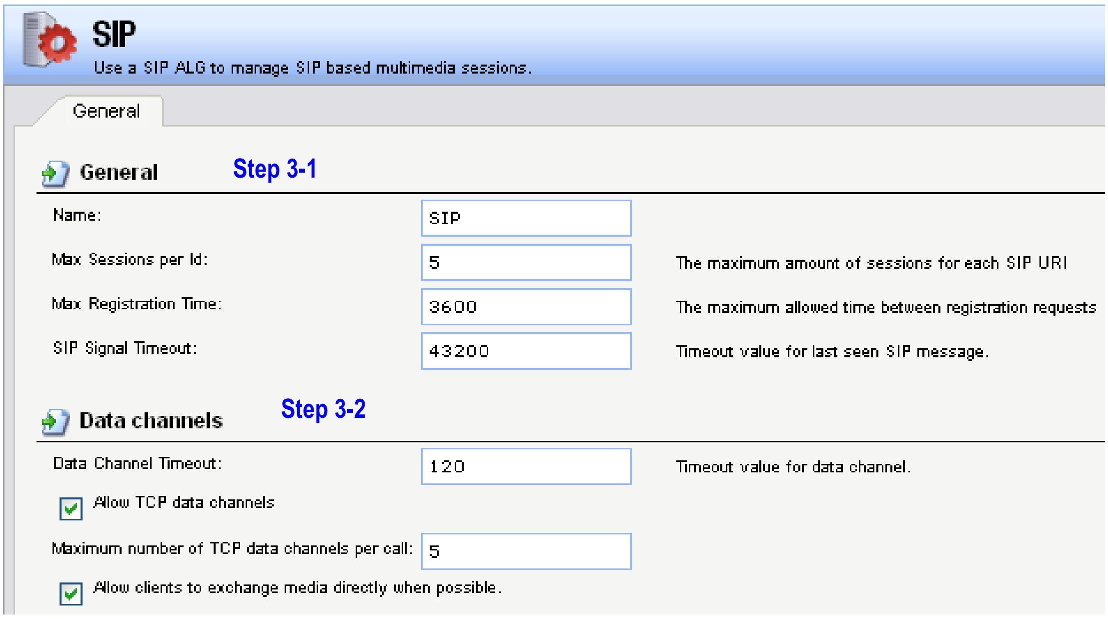


ALG with AV/WCF

Application Layer Gateways (ALGs) are protocol helpers that can parse complex protocols, such as HTTP and H.323.

Name	Type
ftp-passthrough-av	FTP ALG
ftp-outbound-av	FTP ALG
http-outbound	HTTP ALG
http-outbound-av	HTTP ALG
http-outbound-wcf	HTTP ALG
http-outbound-av-wcf	HTTP ALG
pop3	POP3 ALG
pop3-av	POP3 ALG

Figure 4: Add a SIP ALG



SIP

Use a SIP ALG to manage SIP based multimedia sessions.

General Step 3-1

Name:	SIP	
Max Sessions per Id:	5	The maximum amount of sessions for each SIP URI
Max Registration Time:	3600	The maximum allowed time between registration requests
SIP Signal Timeout:	43200	Timeout value for last seen SIP message.

Data channels Step 3-2

Data Channel Timeout:	120	Timeout value for data channel.

☑ Allow TCP data channels

Maximum number of TCP data channels per call: 5

☑ Allow clients to exchange media directly when possible.

Figure 5: Pre-defined SIP ALG, General

In General tab (Figure 5):

Step 3-1: General

Name: SIP

Max Sessions per Id: 5

Max Registration Time: 3600

SPI Signal Timeout: 43200

Step 3-2: Data channels

Data Channel Timeout: 120

Tick box "Allow TCP data channels".

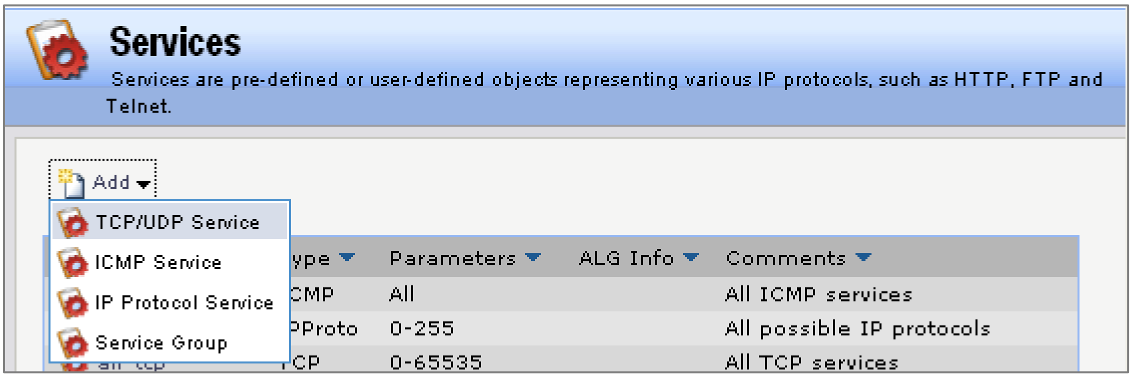
Maximum number of TCP data channels per call: 5

Tick box "Allow clients to exchange media directly when possible."

Click OK

STEP 4: Services

Navigate to **Objects> Services** and add a new *TCP/UDP service* or edit the pre-define *sip-udp* service. The service object will be listed on the *Service* field in IP rules on later step.

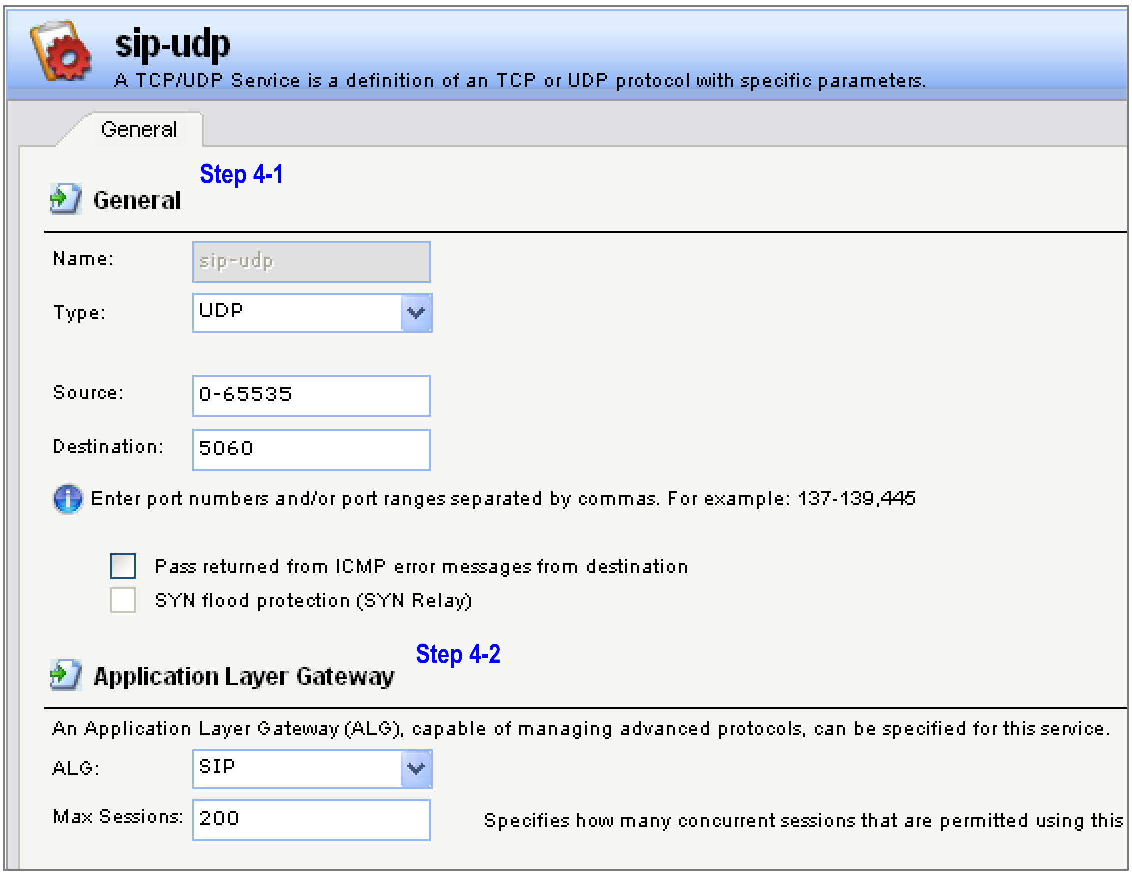


Services

Services are pre-defined or user-defined objects representing various IP protocols, such as HTTP, FTP and Telnet.

ype	Parameters	ALG Info	Comments
CMP	All		All ICMP services
PProto	0-255		All possible IP protocols
CP	0-65535		All TCP services

Figure 6: Add TCP/UDP Service



sip-udp

A TCP/UDP Service is a definition of an TCP or UDP protocol with specific parameters.

General

Step 4-1

General

Name: sip-udp

Type: UDP

Source: 0-65535

Destination: 5060

Enter port numbers and/or port ranges separated by commas. For example: 137-139,445

□ Pass returned from ICMP error messages from destination

□ SYN flood protection (SYN Relay)

Step 4-2

Application Layer Gateway

An Application Layer Gateway (ALG), capable of managing advanced protocols, can be specified for this service.

ALG: SIP

Max Sessions: 200 Specifies how many concurrent sessions that are permitted using this

Figure 7: TCP/UDP Service

In General tab (Figure 7):

Step 4-1: General

Name: sip-udp

Type: UDP

Source: 0-65535

Destination: 5060

Step 4-2: Application Layer Gateway

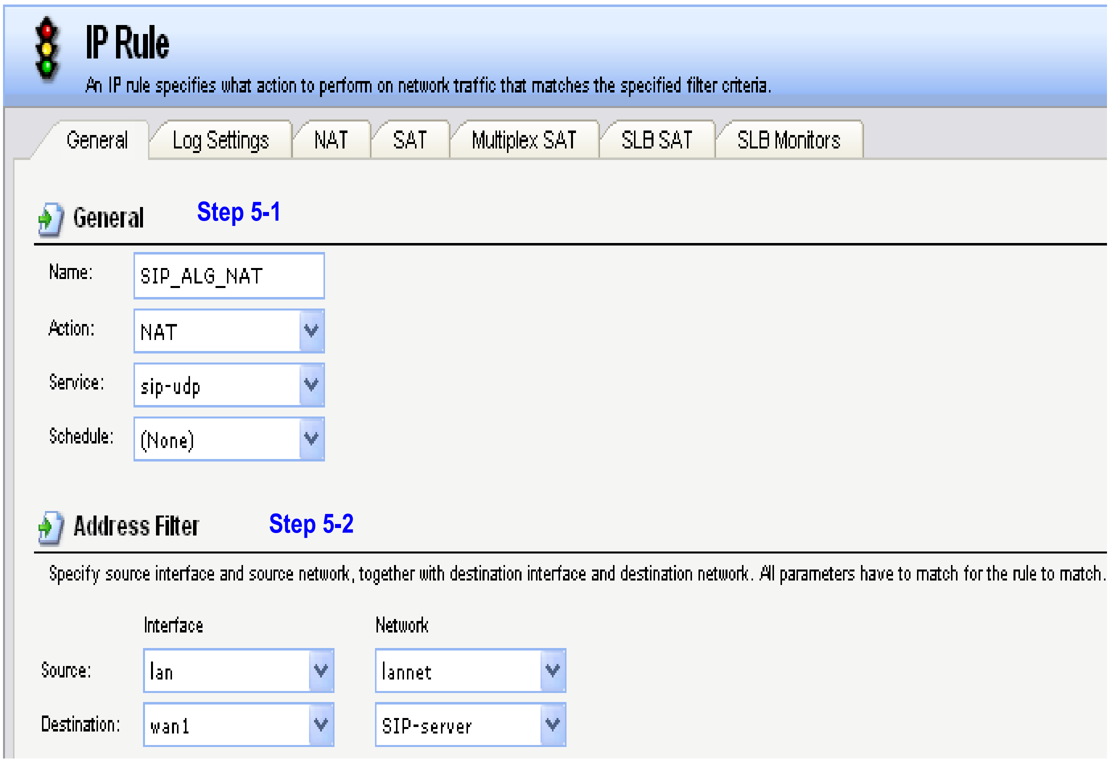
Select the Application Layer Gateway (ALG), which is created in *ALG with AV/WCF* to specify for this service.

ALG: SIP

Click OK

STEP 5: Rules

Navigate to **Rules> IP Rules** and add a new *IP Rule*. The first IP Rule defines the connection originating from a user to SIP server. Use *NAT* to handle all outbound traffic from users or SIP phones on internal network to SIP server. The SIP ALG will take care of all address translation for NAT.



IP Rule

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General Step 5-1

Name: SIP_ALG_NAT

Action: NAT

Service: sip-udp

Schedule: (None)

Address Filter Step 5-2

Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

	Interface	Network
Source:	lan	lannet
Destination:	wan1	SIP-server

Figure 8: Rules (SIP_ALG_NAT)

In General tab (Figure 8), fill in relative information:

Step 5-1: General

Name: SIP_ALG_NAT (defined by user)

Action: NAT

Service: sip-udp

Schedule: (None) (defined by user)

Step 5-2: Address Filter

Source Interface: lan

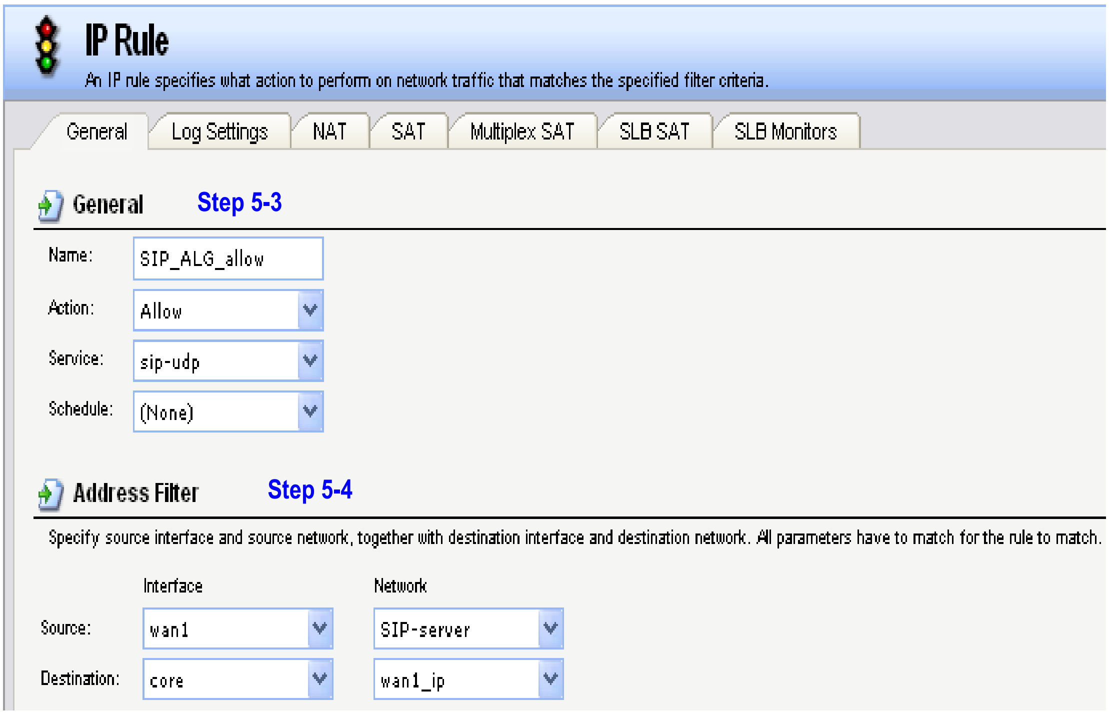
Source Network: lannet

Destination Interface: wan1

Destination Network: SIP-server

Click OK

The second IP Rule defines the connection originating from SIP server to a user/SIP phone. Use *Allow* rule to handle this inbound traffic form SIP server to the firewall. The reason why we choose *Allow* rather than *SAT* rule is ALG has handled IP addresses mapping between user private and pubic IP addresses. Since ALG is offered by the firewall, we select *core* as the destination interface. After registering with SIP server, the firewall can receive a SIP invitation including SIP URI from SIP server when an external user is trying to initiate a call to a user/SIP phone behind the firewall. At this moment, ALG would modify SIP URI in the SIP invitation and forward to the correct internal user/SIP phone.



IP Rule

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General Step 5-3

Name: SIP_ALG_allow

Action: Allow

Service: sip-udp

Schedule: (None)

Address Filter Step 5-4

Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

	Interface	Network
Source:	wan1	SIP-server
Destination:	core	wan1_ip

Figure 9: Rules (SIP_ALG_allow)

In General tab (Figure 9), fill in relative information:

Step 5-3: General

Name: SIP_ALG_allow (defined by user)

Action: Allow

Service: sip-udp

Schedule: (None) (defined by user)

Step 5-4: Address Filter

Source Interface: wan1

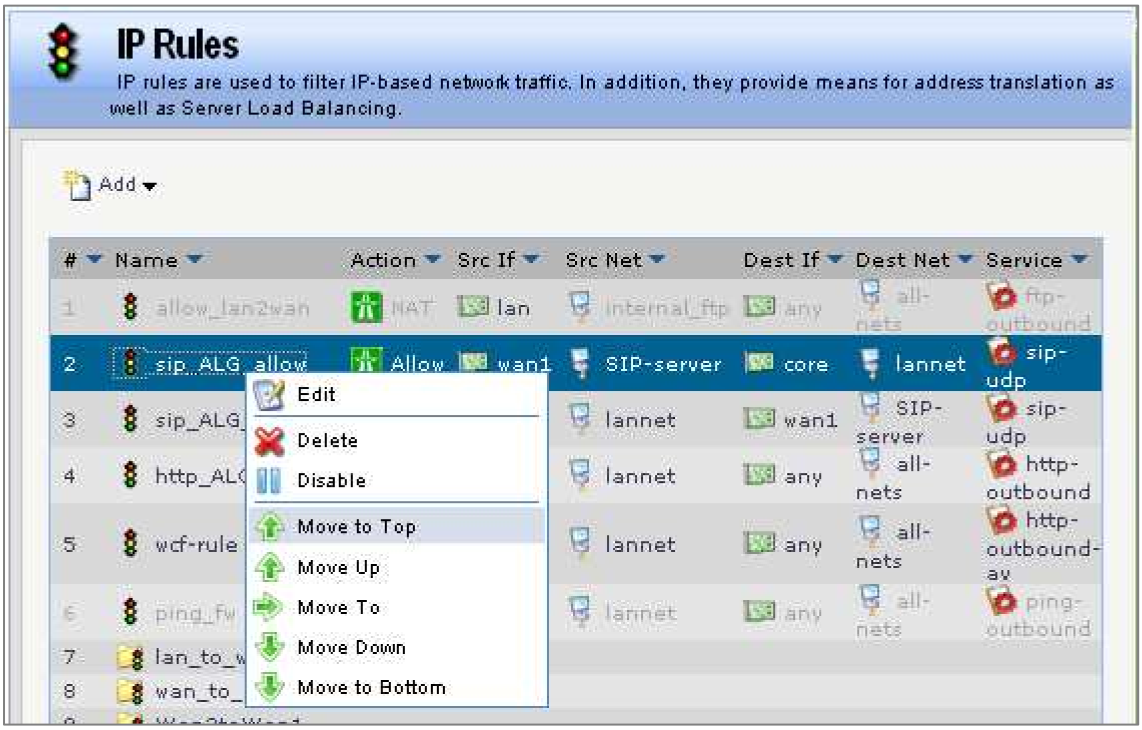
Source Network: SIP-server

Destination Interface: core

Destination Network: wan1_ip

Click OK

In the IP Rule list, move these two IP rules to the top.



IP Rules

IP rules are used to filter IP-based network traffic. In addition, they provide means for address translation as well as Server Load Balancing.

#	Name	Action	Src If	Src Net	Dest If	Dest Net	Service
1	allow_lan2wan	NAT	lan	internal_ftp	any	all-nets	ftp-outbound
2	sip_ALG_allow	Allow	wan1	SIP-server	core	lannet	sip-udp
3	sip_ALG_			lannet	wan1	SIP-server	sip-udp
4	http_ALC			lannet	any	all-nets	http-outbound
5	wcf-rule			lannet	any	all-nets	http-outbound-av
6	ping_fw			lannet	any	all-nets	ping-outbound
7	lan_to_w						
8	wan_to_						

Figure 8: Rules List

Step 5-5: Change the order

Click Right-Click on sip_ALG_nat.

Click Move to Top.

Click Right-Click on sip_ALG_allowt.

Click Move to Top.

[[Save and active the configuration]]