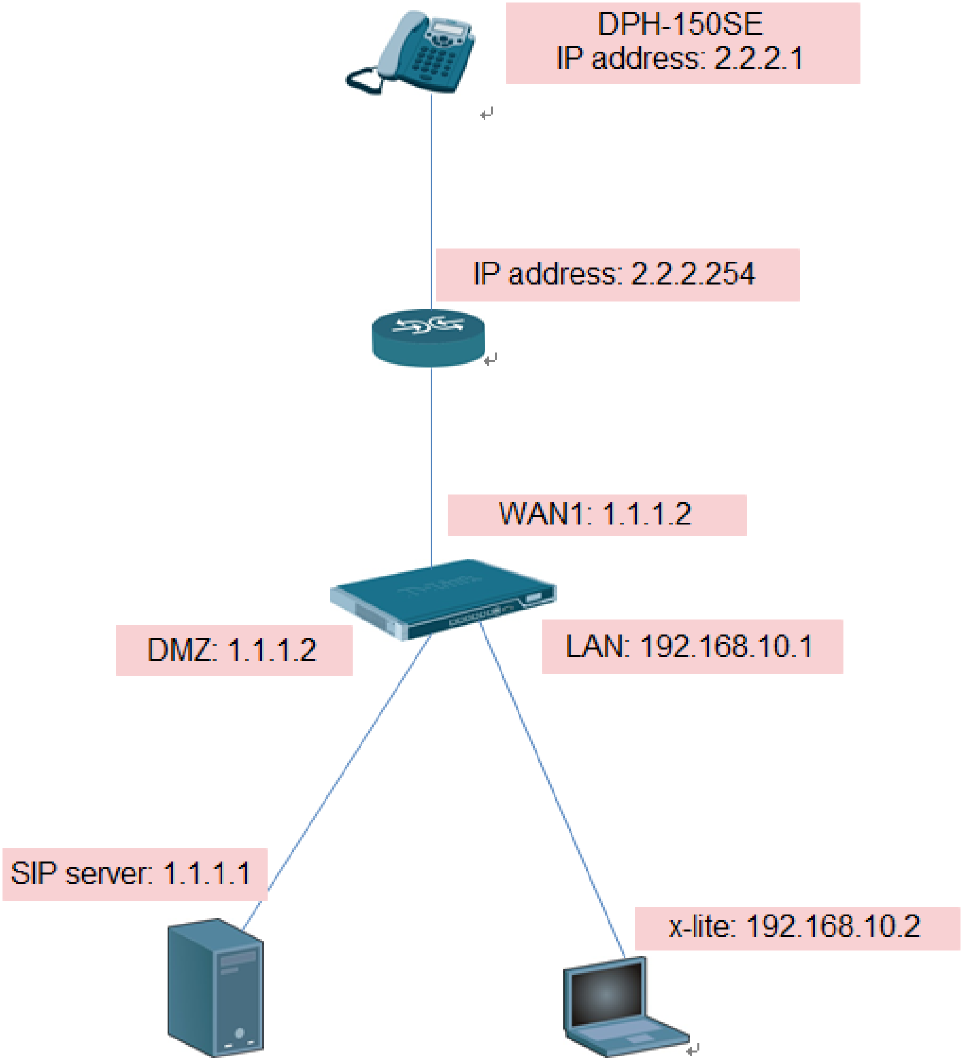
Protecting proxy and local clients - Proxy on the DMZ interface

This scenario is similar to the previous but the major difference is the location of the local SIP proxy server. The server is placed on a separate interface and network to the local clients. This setup adds an extra layer of security since the initial SIP traffic is never exchanged directly between a remote endpoint and the local, protected clients.



This scenario can be implemented in a topology hiding setup with DMZ (Solution A below) as well as a setup without NAT (Solution B below).
In this document, I only tell you how to setup solution A.

Solution A - Using NAT

The following should be noted about this setup:
The IP address of the SIP proxy must be a globally routable IP address. The NetDefend Firewall does not support hiding of the proxy on the DMZ.

The IP address of the DMZ interface must be a globally routable IP address. This address can be the same address as the one used on the external interface.

Setup SIP server & SIP phone:

In this test, all parameter use default setting, only need to add user account.

DPH-150SE:

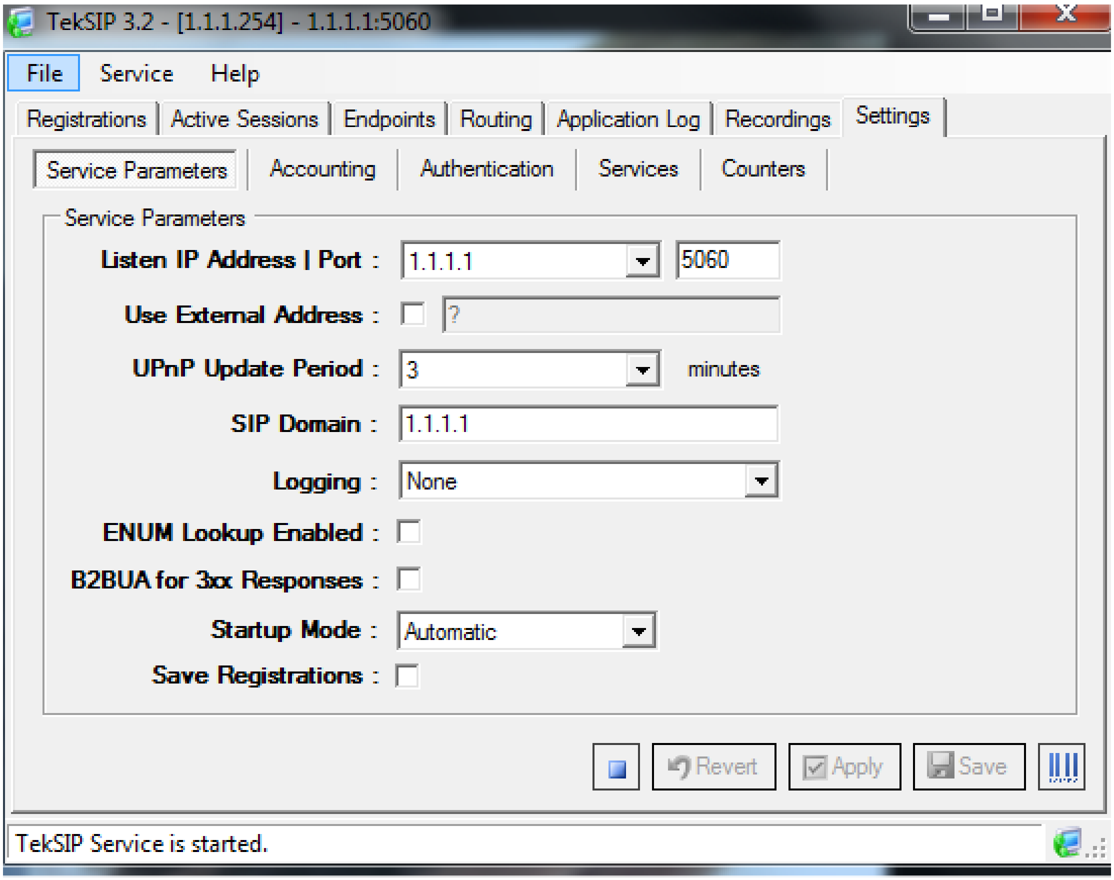
IP address: 2.2.2.1 GW: 2.2.2.254 SIP server address: 1.1.1.1

X-lite 5:

IP address: 192.168.10.2 GW: 192.168.10.1 SIP server address: 1.1.1.1

SIP server:

IP address: 1.1.1.1 GW: 1.1.1.254



Service Parameters

Listen IP Address | Port : 1.1.1.1 5060

Use External Address : □ ?

UPnP Update Period : 3 minutes

SIP Domain : 1.1.1.1

Logging : None

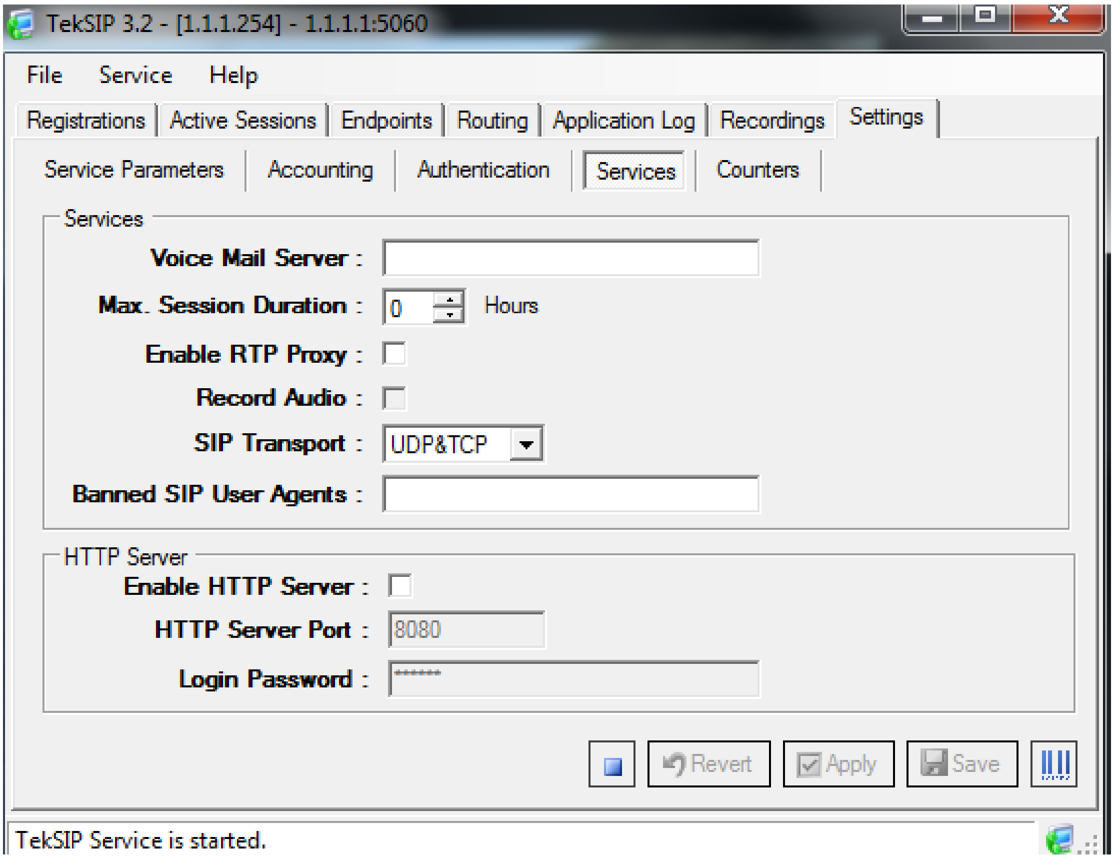
ENUM Lookup Enabled : □

B2BUA for 3xx Responses : □

Startup Mode : Automatic

Save Registrations : □

TekSIP Service is started.



Services

Voice Mail Server :

Max. Session Duration : 0 Hours

Enable RTP Proxy : □

Record Audio : □

SIP Transport : UDP&TCP

Banned SIP User Agents :

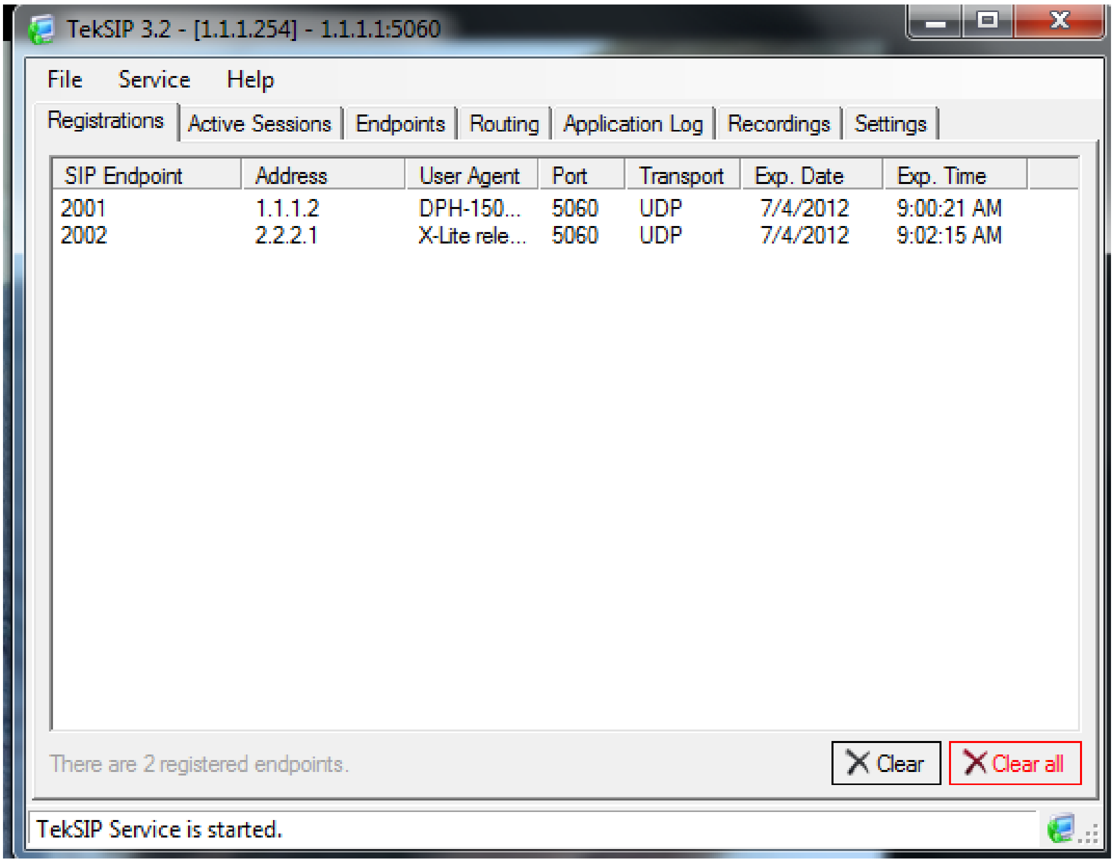
HTTP Server

Enable HTTP Server : □

HTTP Server Port : 8080

Login Password : ******

TekSIP Service is started.



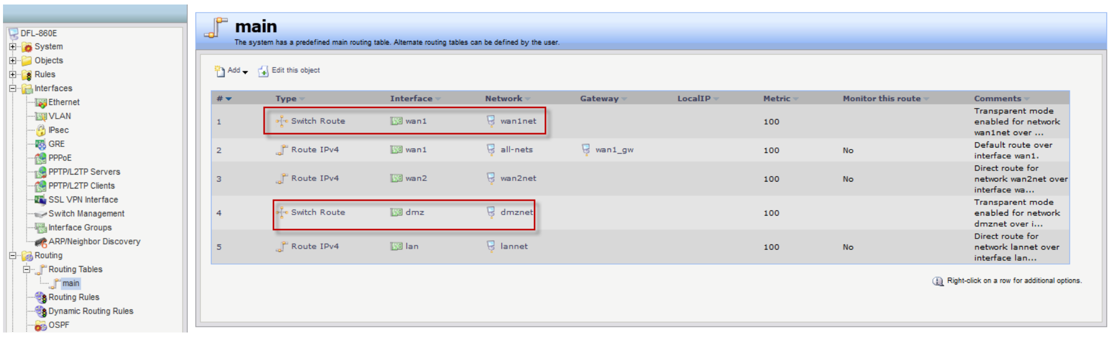
SIP Endpoint	Address	User Agent	Port	Transport	Exp. Date	Exp. Time
2001	1.1.1.2	DPH-150...	5060	UDP	7/4/2012	9:00:21 AM
2002	2.2.2.1	X-Lite rele...	5060	UDP	7/4/2012	9:02:15 AM

There are 2 registered endpoints.

TekSIP Service is started.

DFL setup:

(1) Enable transparent mode on WAN1 and DMZ then you will see switch route in the main table.



main

The system has a predefined main routing table. Alternate routing tables can be defined by the user.

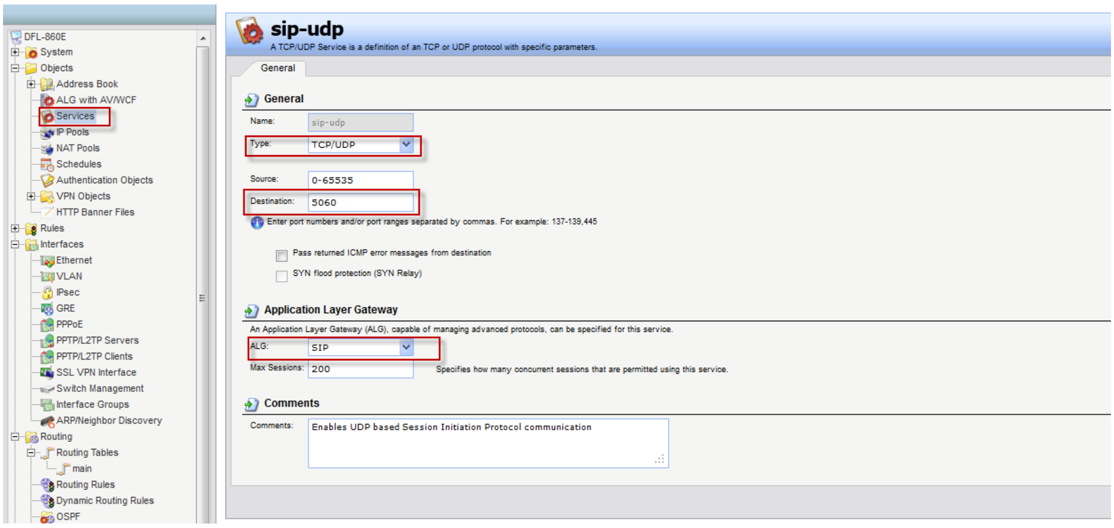
#	Type	Interface	Network	Gateway	LocalIP	Metric	Monitor this route	Comments
1	Switch Route	wan1	wan1net			100		Transparent mode enabled for network wan1net over ...
2	Route IPv4	wan1	all-nets	wan1_gw		100	No	Default route over interface wan1.
3	Route IPv4	wan2	wan2net			100	No	Direct route for network wan2net over interface wa...
4	Switch Route	dmz	dmznet			100		Transparent mode enabled for network dmznet over i...
5	Route IPv4	lan	lannet			100	No	Direct route for network lannet over interface lan...

Right-click on a row for additional options.

(2) Check “sip-udp” services.

Destination port: 5060

Type: TCP/UDP



sip-udp

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

General

Name: sip-udp

Type: TCP/UDP

Source: 0-65535

Destination: 5060

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

□ Pass returned ICMP error messages from destination

□ SYN flood protection (SYN Relay)

Application Layer Gateway

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

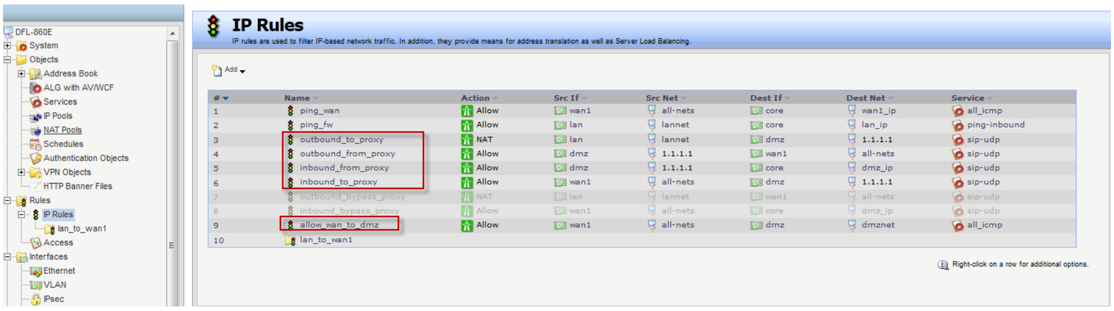
ALG: SIP

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

Comments

Comments: Enables UDP based Session Initiation Protocol communication

(3) Define four rules in the IP rule set:



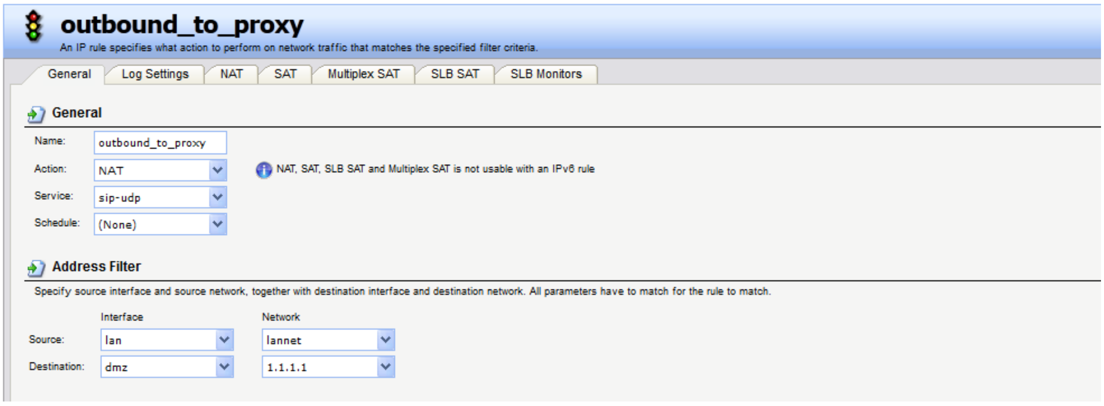
IP Rules

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	ping_wan	Allow	wan1	all-nets	core	wan1_ip	all_icmp
2	ping_fw	Allow	lan	lannet	core	lan_ip	ping-inbound
3	outbound_to_proxy	NAT	lan	lannet	dmz	1.1.1.1	sip-udp
4	outbound_from_proxy	Allow	dmz	1.1.1.1	wan1	all-nets	sip-udp
5	inbound_from_proxy	Allow	dmz	1.1.1.1	core	dmz_ip	sip-udp
6	inbound_to_proxy	Allow	wan1	all-nets	dmz	1.1.1.1	sip-udp
7	outbound_bypass_proxy	NAT	lan	lannet	wan1	all-nets	sip-udp
8	inbound_bypass_proxy	Allow	wan1	all-nets	core	dmz_ip	sip-udp
9	allow_wan_to_dmz	Allow	wan1	all-nets	dmz	dmznet	all_icmp
10	lan_to_wan1						

Right-click on a row for additional options.

A NAT rule for outbound traffic from the clients on the internal network to the proxy located on the DMZ interface. The SIP ALG will take care of all address translation needed by the NAT rule. This translation will occur both at the IP level and at the application level.



outbound_to_proxy

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

General

Name: outbound_to_proxy
Action: NAT
Service: sip-udp
Schedule: (None)

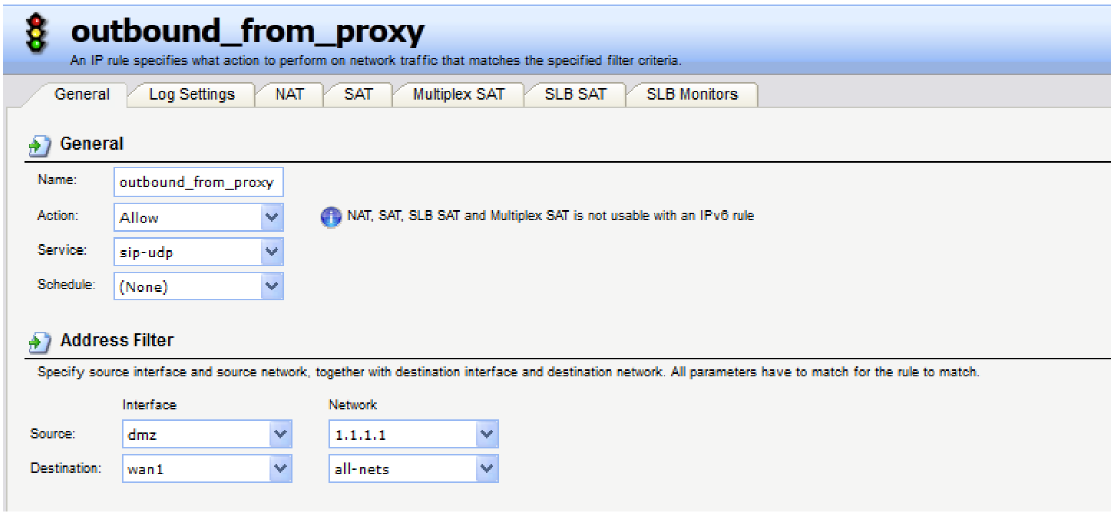
NAT, SAT, SLB SAT and Multiplex SAT is not usable with an IPv6 rule

Address Filter

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:	dmz	1.1.1.1

An Allow rule for outbound traffic from the proxy behind the DMZ interface to the remote clients on the Internet.



outbound_from_proxy

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

General

Name: outbound_from_proxy
Action: Allow
Service: sip-udp
Schedule: (None)

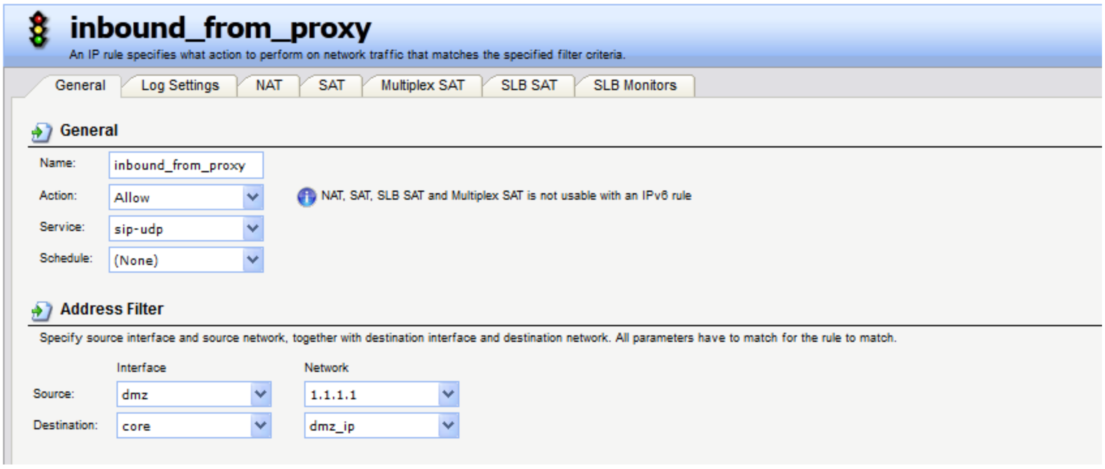
NAT, SAT, SLB SAT and Multiplex SAT is not usable with an IPv6 rule

Address Filter

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:	dmz	1.1.1.1
Destination:	wan1	all-nets

An Allow rule for inbound SIP traffic from the SIP proxy behind the DMZ interface to the IP address of the NetDefend Firewall. This rule will have core (in other words, NetDefendOS itself) as the destination interface.



inbound_from_proxy

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

General

Name: inbound_from_proxy

Action: Allow

Service: sip-udp

Schedule: (None)

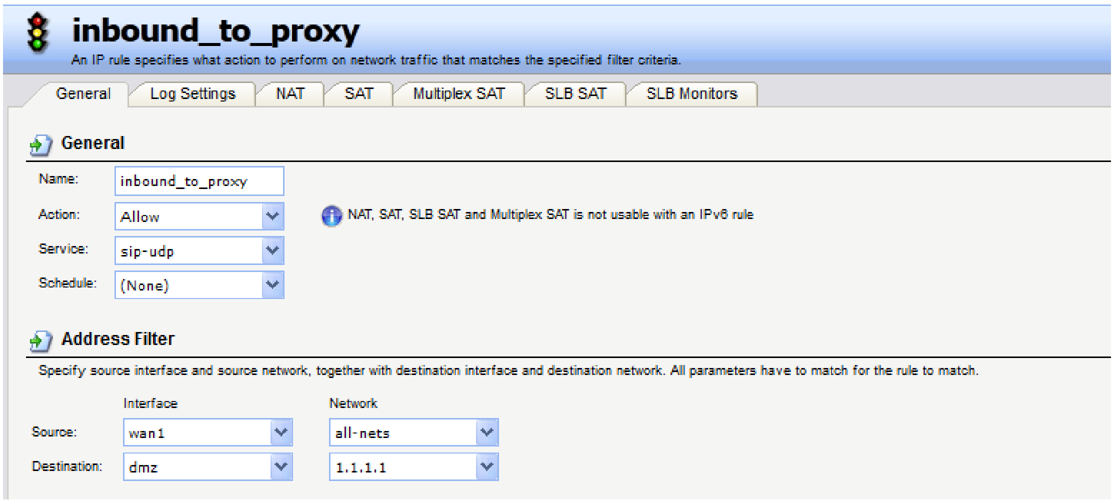
NAT, SAT, SLB SAT and Multiplex SAT is not usable with an IPv6 rule

Address Filter

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:	dmz	1.1.1.1
Destination:	core	dmz_ip

An Allow rule for inbound traffic from, for example the Internet, to the proxy behind the DMZ.



inbound_to_proxy

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

General

Name: inbound_to_proxy

Action: Allow

Service: sip-udp

Schedule: (None)

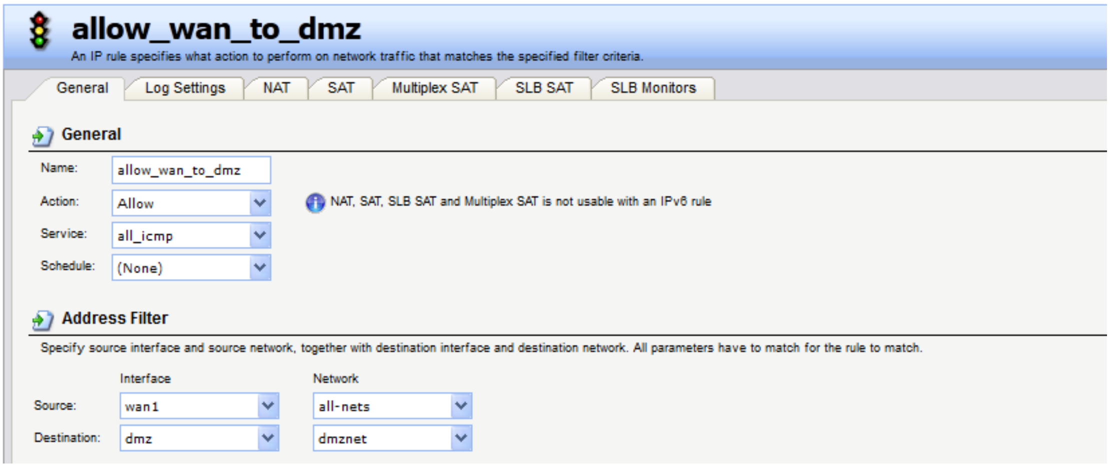
NAT, SAT, SLB SAT and Multiplex SAT is not usable with an IPv6 rule

Address Filter

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	all-nets
Destination:	dmz	1.1.1.1

An allow rule is for other WAN traffic can go into DMZ.



allow_wan_to_dmz

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

General

Name: allow_wan_to_dmz

Action: Allow

Service: all_icmp

Schedule: (None)

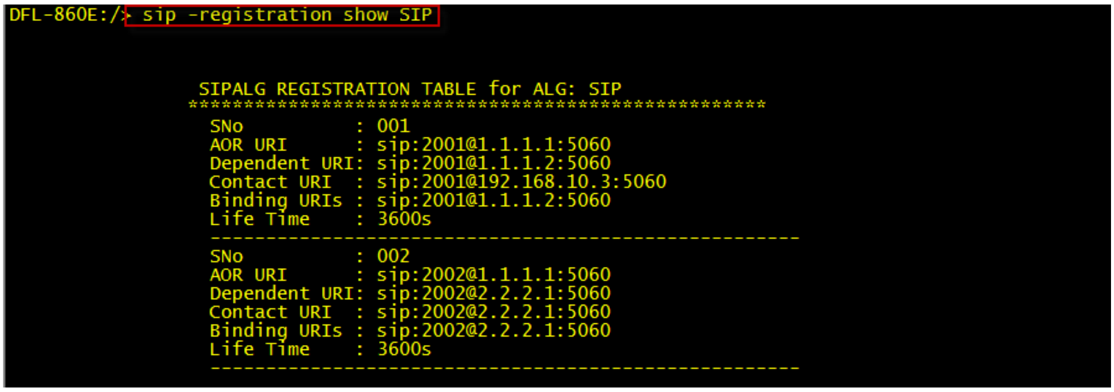
NAT, SAT, SLB SAT and Multiplex SAT is not usable with an IPv6 rule

Address Filter

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

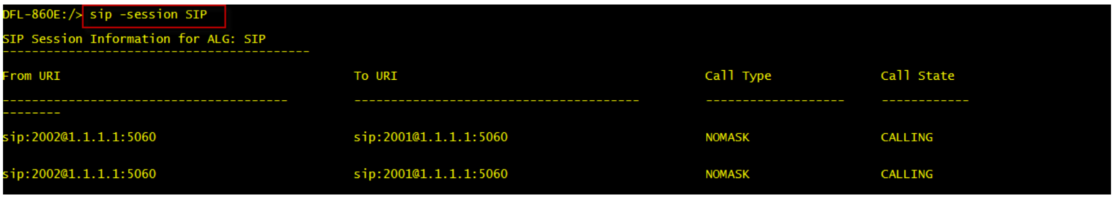
	Interface	Network
Source:	wan1	all-nets
Destination:	dmz	dmznet

When your SIP client registers to SIP server successful, you can see registration information on CLI.

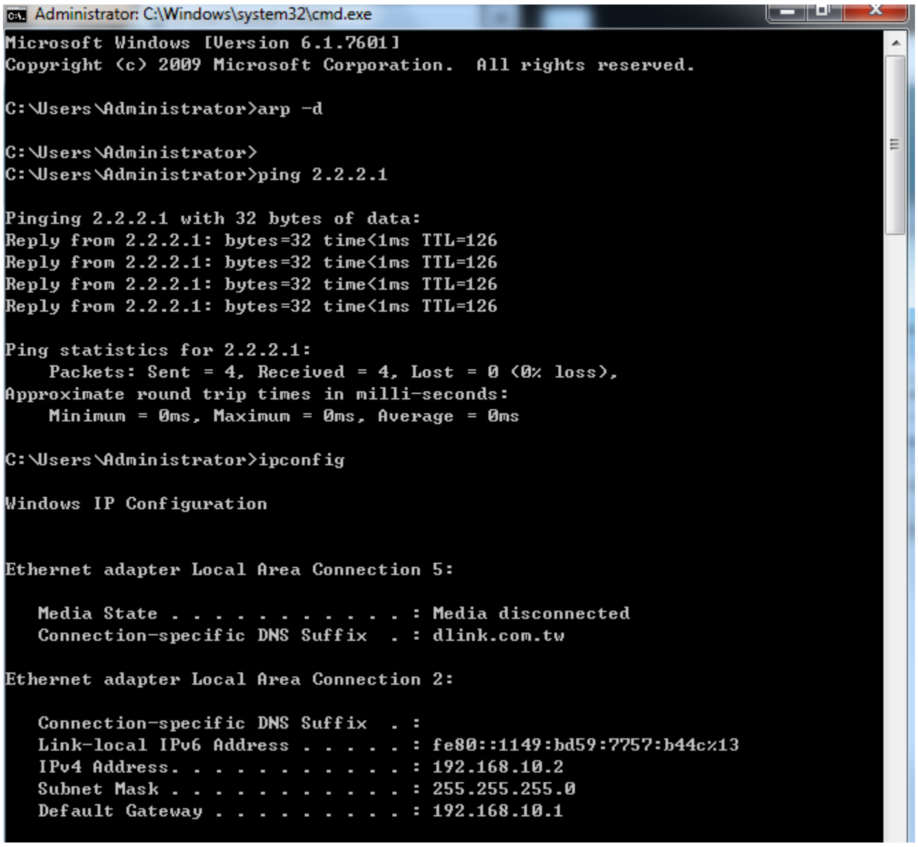


```
DFL-860E:/> sip -registration show SIP


                SIPALG REGISTRATION TABLE for ALG: SIP
               ****************************************************
                 SNo          : 001
                 AOR URI      : sip:2001@1.1.1.1:5060
                 Dependent URI: sip:2001@1.1.1.2:5060
                 Contact URI  : sip:2001@192.168.10.3:5060
                 Binding URIs : sip:2001@1.1.1.2:5060
                 Life Time    : 3600s
                 -----------------------------------------------------
                 SNo          : 002
                 AOR URI      : sip:2002@1.1.1.1:5060
                 Dependent URI: sip:2002@2.2.2.1:5060
                 Contact URI  : sip:2002@2.2.2.1:5060
                 Binding URIs : sip:2002@2.2.2.1:5060
                 Life Time    : 3600s
                 -----------------------------------------------------
```

You can use “sip –session SIP” to check your calling session is successful or not.



```
DFL-860E:/> sip -session SIP

SIP Session Information for ALG: SIP
------------------------------------------

From URI                                    To URI                                      Call Type            Call State

---------------------------------------     ---------------------------------------     -------------------  ------------
--------

sip:2002@1.1.1.1:5060                       sip:2001@1.1.1.1:5060                       NOMASK               CALLING

sip:2002@1.1.1.1:5060                       sip:2001@1.1.1.1:5060                       NOMASK               CALLING
```



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>arp -d

C:\Users\Administrator>
C:\Users\Administrator>ping 2.2.2.1

Pinging 2.2.2.1 with 32 bytes of data:
Reply from 2.2.2.1: bytes=32 time<1ms TTL=126
Reply from 2.2.2.1: bytes=32 time<1ms TTL=126
Reply from 2.2.2.1: bytes=32 time<1ms TTL=126
Reply from 2.2.2.1: bytes=32 time<1ms TTL=126

Ping statistics for 2.2.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 5:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : dlink.com.tw

Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1149:bd59:7757:b44c%13
   IPv4 Address. . . . . . . . . . . : 192.168.10.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1
```

END