Configuration examples for the D-Link NetDefend Firewall series

Scenario: How to configure SIP ALG for SIP Phones

Platform Compatibility: All NetDefend Firewall Series

Last update: 2008-03-13

Overview

In this document, the notation *Objects->Address book* means that in the tree on the left side of the screen **Objects** first should be clicked (expanded) and then **Address Book**.

Most of the examples in this document are adapted for the DFL-800. The same settings can easily be used for all other models in the series. The only difference is the names of the interfaces. Since the DFL-1600 and DFL-2500 has more than one lan interface, the lan interfaces are named lan1, lan2 and lan3 not just lan.

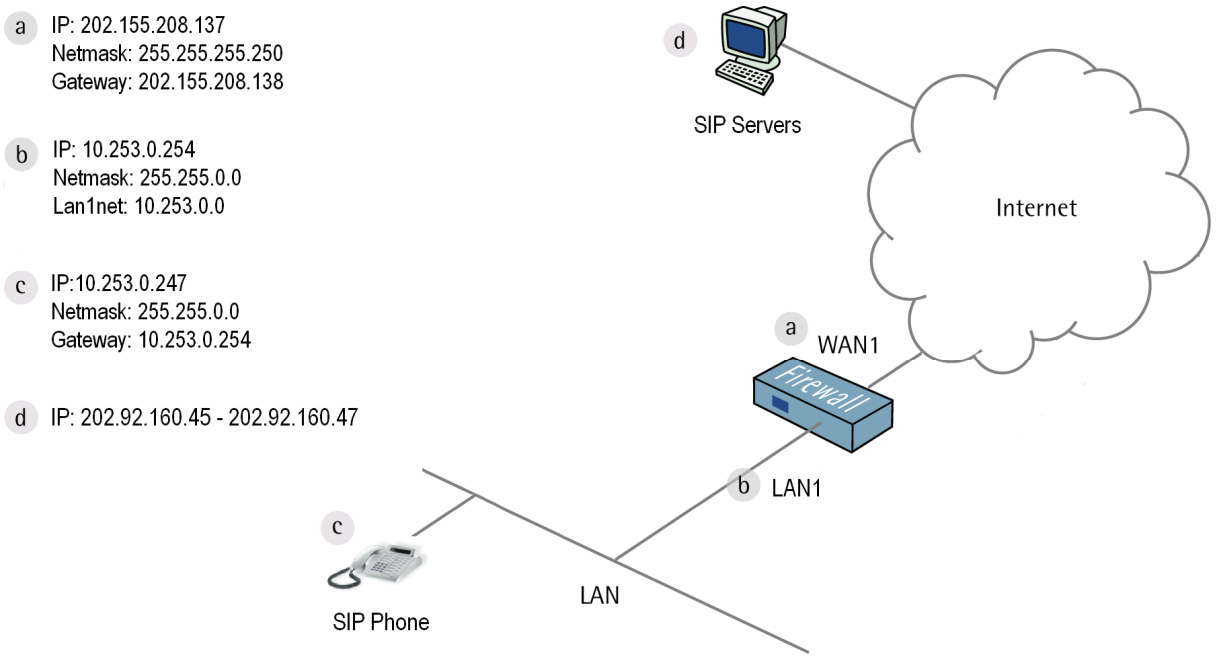
The screenshots in this document is from firmware version 2.20. If you are using an earlier version of the firmware, the screenshots may not be identical to what you see on your browser. Please notice that NetDefendOS starts to support SIP ALG from firmware version 2.20, if you use firmware version earlier than 2.20, this feature is not available.

To prevent existing settings to interfere with the settings in these guides, reset the firewall to factory defaults before starting.

How to configure SIP ALG for SIP Phones

This scenario shows how a firewall can use a SIP ALG to manage SIP based multimedia sessions for SIP phones.

In this scenario the firewall is connected to ISP. The SIP phone is behind the NetDefend Firewall.



Note:

1. This configuration scenario has been testing with D-Link DPH-300 and SIP software X-Lite.

2. In FW 2.20 release, NetDefendOS currently supports SIP sessions from Internal to External scenario only. The application scenario is the SIP sessions between a peer on the protected side of a D-Link NetDefend Firewall and a peer which is on the external, unprotected side. Communication typically takes place across the public.

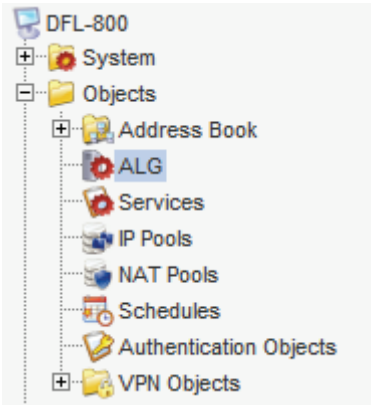
   Support for SIP phones and servers locate in the same network, a.k.a. the internal to internal scenario will be available in the future release.

Step 1: Go to *Objects ->Address book*:

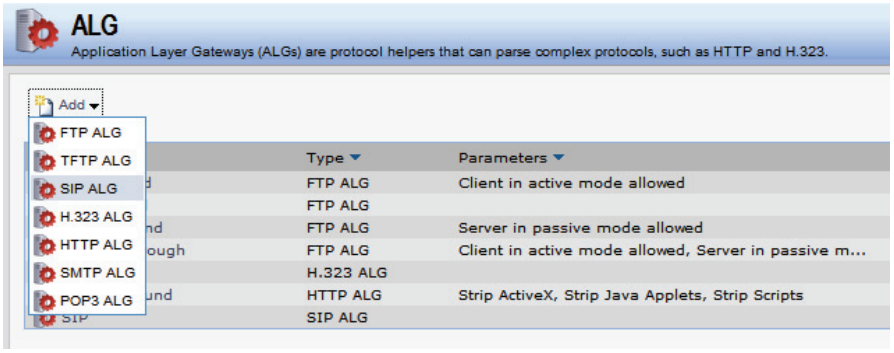
Create a new IP address for SIP Servers:
Name: SIP-Servers
IP address: 202.92.160.45-202.92.160.47

Click Ok.

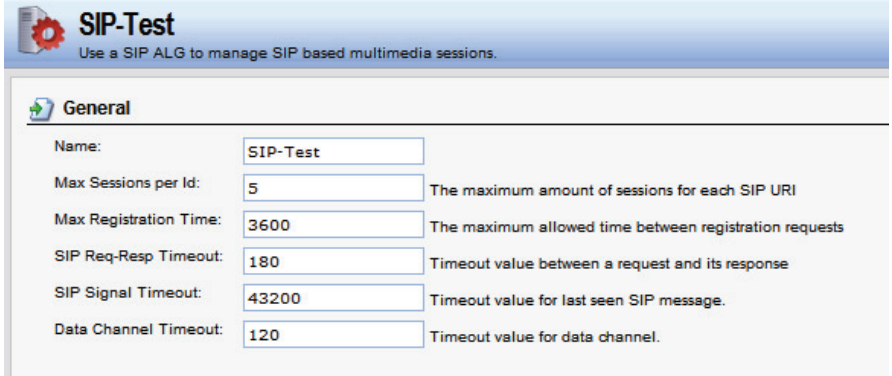
Step 2: Go to *Objects ->ALG*



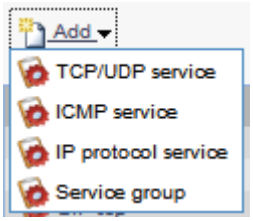
Step 3: Add a new SIP ALG, e.g. *SIP-Test*
Or edit pre-define rule *SIP*

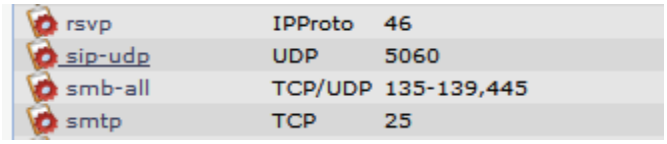


Step 4: Configure parameters for *SIP ALG*
Click *OK*



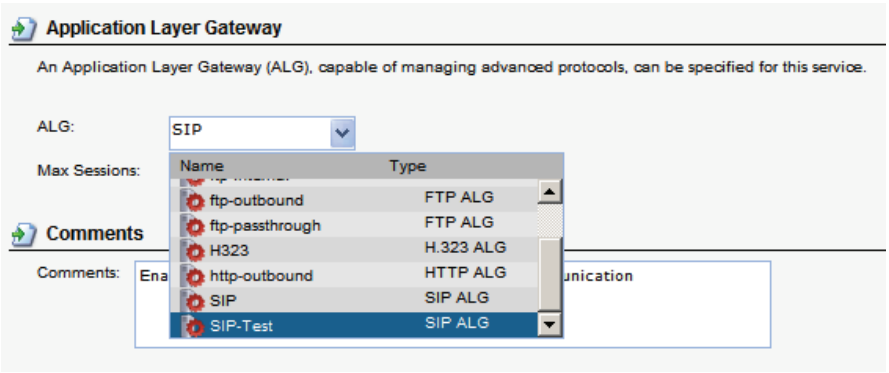
Step 5: Go to *Objects* ->*Services*, add *TCP/UDP service*
Or edit pre-define *sip-udp* service



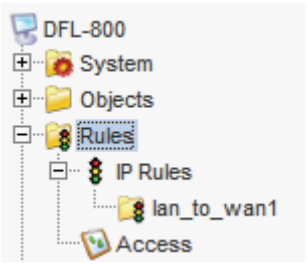


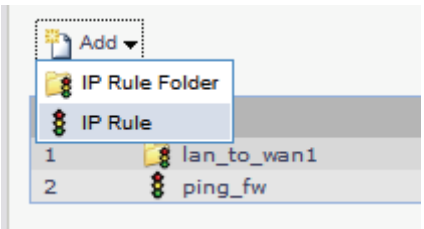
Step 6: In Application Layer Gateway option, select a predefined ALG or custom ALG, here custom ALG *SIP-Test* as the example.

Click *OK*



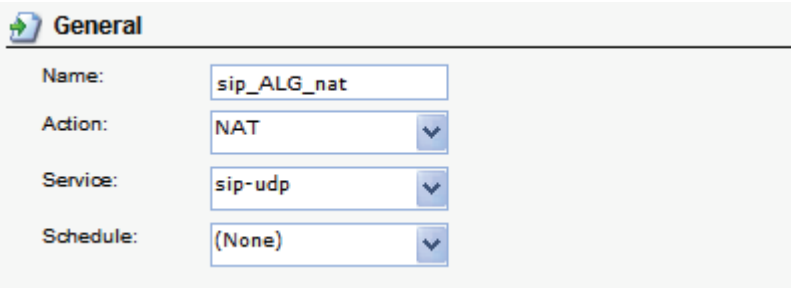
Step 7: Go to *Rule-> IP Rules*
Add *IP Rule*





Step 8: In General tab

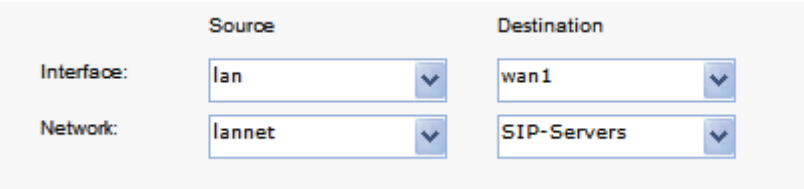
Name: sip_ALG_nat
Action: *NAT*
Service: *sip-udp*



Source Interface: *lan*
Source Network: *lannet*

Destination Interface: *wan1*
Destination Network: *SIP-Servers*

Click *OK*



Step 9: Add another new **IP Rule**.

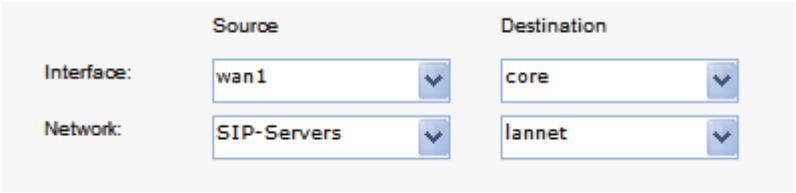
In General tab

Name: sip_ALG_allow
Action: Allow
Service: *sip-udp*

Source Interface: *wan1*
Source Network: *SIP-Servers*

Destination Interface: core
Destination Network: *lannet*

Click *OK*



Step 10: Click Right-Click on *sip_ALG_nat* rule
Click *Move to Top*

Repeat Step 10 for sip_ALG_allow rule

Click *Save and Active* to activate the configuration on the firewall.