IPS/Anti-Virus Signature Update Problem

This chapter is talking about how to debug IPS/Anti-Virus signature update issue, keeps your signatures are up-to-date can avoid malicious incursion.

The D-Link firewall signature database is updated on a daily basis with new Virus/IPS signatures. Older signatures are seldom retired but instead are replaced with more generic signatures covering several viruses. The local NetDefendOS copy of the signature database should therefore be updated regularly and this updating service is enabled as part of the subscription to the D-Link IPS/Anti-Virus subscription.

If you can't update your firewall signatures, please follow below troubleshooting guide and try to fix your problem.

Troubleshooting Guide

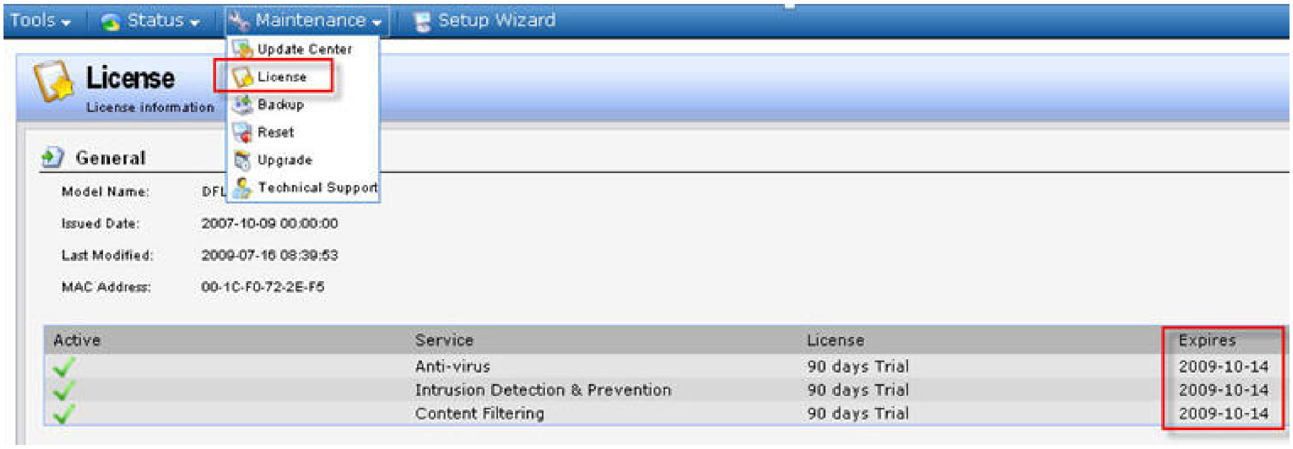
For better understanding on how to solve these issues, given below is a list of troubleshooting steps for a test case scenario.

[Symptom]

[Syptom1: IPS/Anti-Virus Update Fail]

[Step 1] Check your IPS/Anti-Virus license keys expiration dateline, if keys are expire, please purchases new license to extend expiration date.

Via WebUI:



License

License information

General

Model Name: DFL

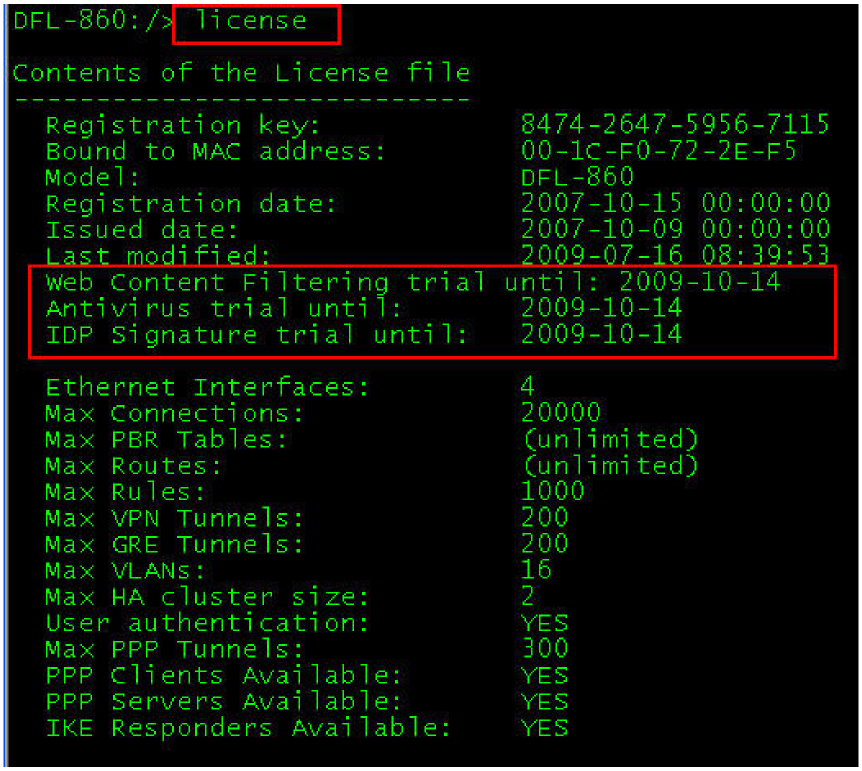
Issued Date: 2007-10-09 00:00:00

Last Modified: 2009-07-16 08:39:53

MAC Address: 00-1C-F0-72-2E-F5

Active	Service	License	Expires
✓	Anti-virus	90 days Trial	2009-10-14
✓	Intrusion Detection & Prevention	90 days Trial	2009-10-14
✓	Content Filtering	90 days Trial	2009-10-14

Via CLI, issue “license” command, and you can see:



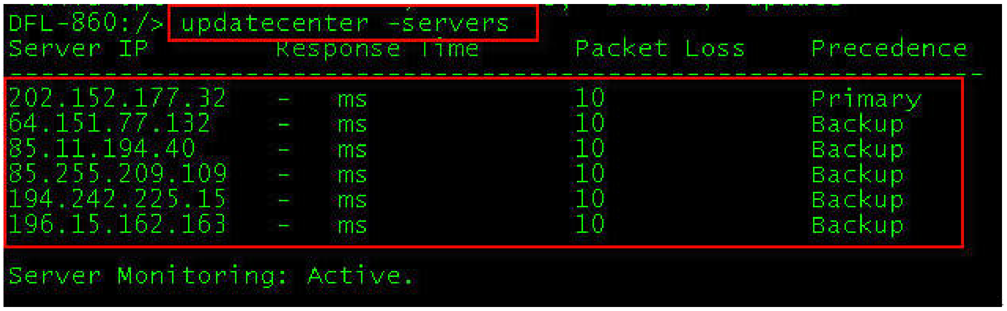
```
DFL-860:/> license

Contents of the License file
----------------------------
   Registration key:               8474-2647-5956-7115
   Bound to MAC address:           00-1C-F0-72-2E-F5
   Model:                          DFL-860
   Registration date:              2007-10-15 00:00:00
   Issued date:                    2007-10-09 00:00:00
   Last modified:                  2009-07-16 08:39:53
   Web Content Filtering trial until: 2009-10-14
   Antivirus trial until:          2009-10-14
   IDP Signature trial until:      2009-10-14

   Ethernet Interfaces:            4
   Max Connections:                20000
   Max PBR Tables:                 (unlimited)
   Max Routes:                     (unlimited)
   Max Rules:                      1000
   Max VPN Tunnels:                200
   Max GRE Tunnels:                200
   Max VLANs:                      16
   Max HA cluster size:            2
   User authentication:            YES
   Max PPP Tunnels:                300
   PPP Clients Available:          YES
   PPP Servers Available:          YES
   IKE Responders Available:       YES
```

[Syptom2: Fail to look up update server]

Please make sure if firewall has correct UTM update server IP addresses.

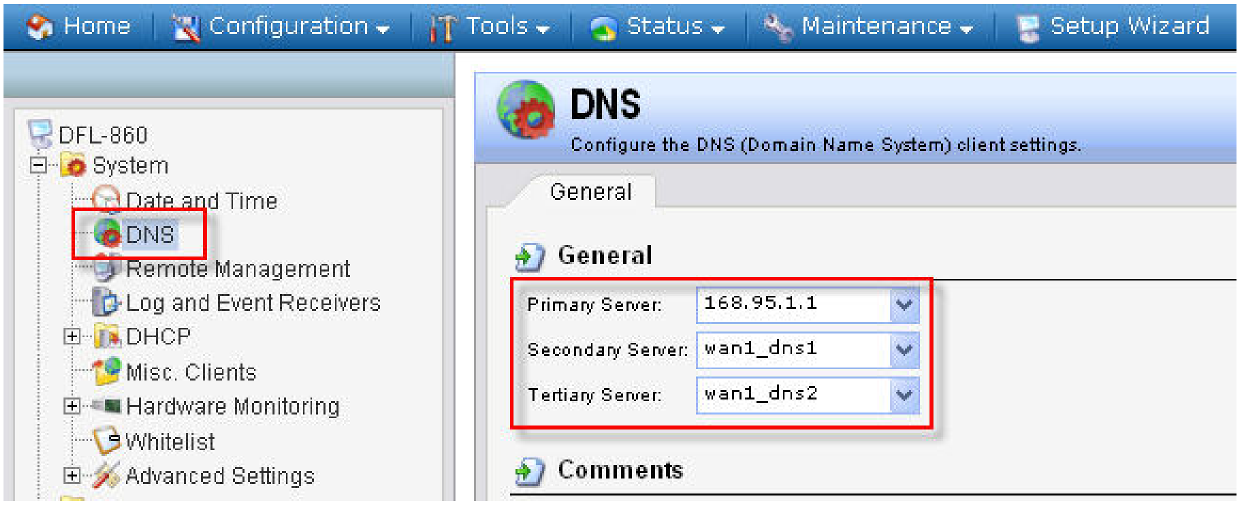
[Step 2] Login to CLI.

[Step 3] Check update servers status, please issue “updatecenter –servers” command.



```
DFL-860:/> updatecenter -servers
Server IP        Response Time        Packet Loss     Precedence
-----------------------------------------------------------------
202.152.177.32    -   ms              10              Primary
64.151.77.132     -   ms              10              Backup
85.11.194.40      -   ms              10              Backup
85.255.209.109    -   ms              10              Backup
194.242.225.15    -   ms              10              Backup
196.15.162.163    -   ms              10              Backup

Server Monitoring: Active.
```

[Step 4] If you can’t see server IP addresses like above, please check DNS server configuration, make sure all DNS servers are workable.



DNS

Configure the DNS (Domain Name System) client settings.

General

Primary Server: 168.95.1.1

Secondary Server: wan1_dns1

Tertiary Server: wan1_dns2

[Step 5] Please make sure DNS servers can resolution URL: *dl-lic.clavister.com*.