Configuration Example for the D-Link NetDefend Firewall Series

[Case]

Configure Anti-Virus on UTM Firewall

Implement mode: DFL-260E/860E/1660/2560/2560G

Why Anti-Virus

Anti-Virus module protects users against malicious codes hidden in a file, which may attach to an email or download form Internet. While Intrusion Detection and Prevention (IDP) monitors specific whole computer system or network, Anti-Virus focus on scanning files received by users. D-Link Anti-Virus module contains various malicious codes and can assist users to avoid most threats. In this document, you can find the step by step setting of anti-virus on UTM firewall. 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.
- This function only for DFL-260/260E/860/860E/1660/2560/2560G.

How to configure anti-virus

HTTP service is the most frequently used service in SUPERSTAR Corporation. In order to avoid unpredictable risks raised from malicious codes hidden in files, SUPERSTAR force Anti-Virus scanning for each download file from HTTP web pages.

- Create ALG for the specified service
- Create a service object for an ALG function
- Create IP Rules for service objects

STEP 1: ALG with AV/WCF

Navigate to **Objects> ALG with AV/WCF** and add a new *HTTP ALG*.

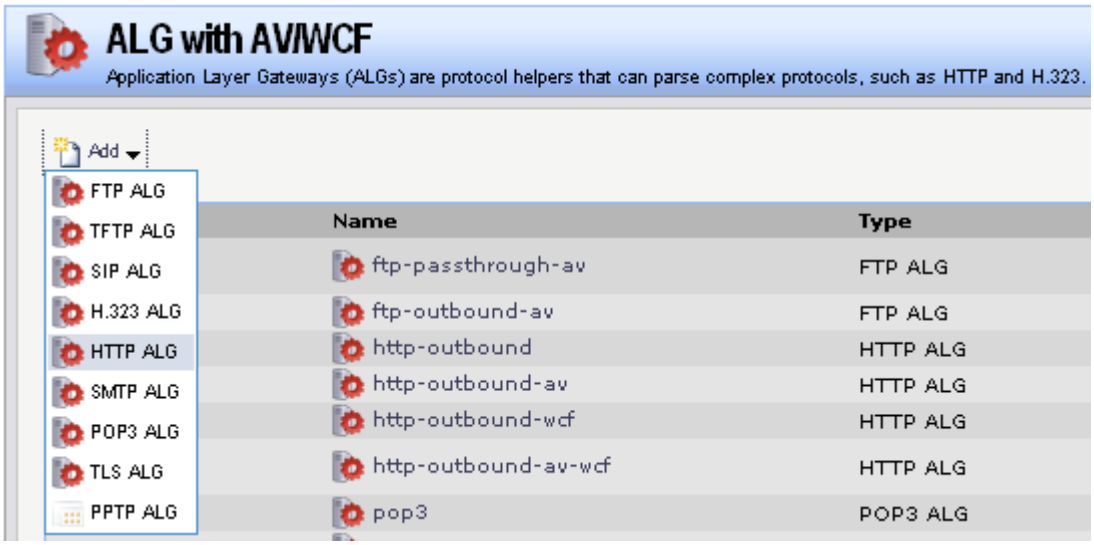

Figure 1: Add HTTP ALG

Figure 2: HTTP ALG, General

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

Step 1-1: General

Name: http-outbound-av (defined by user)

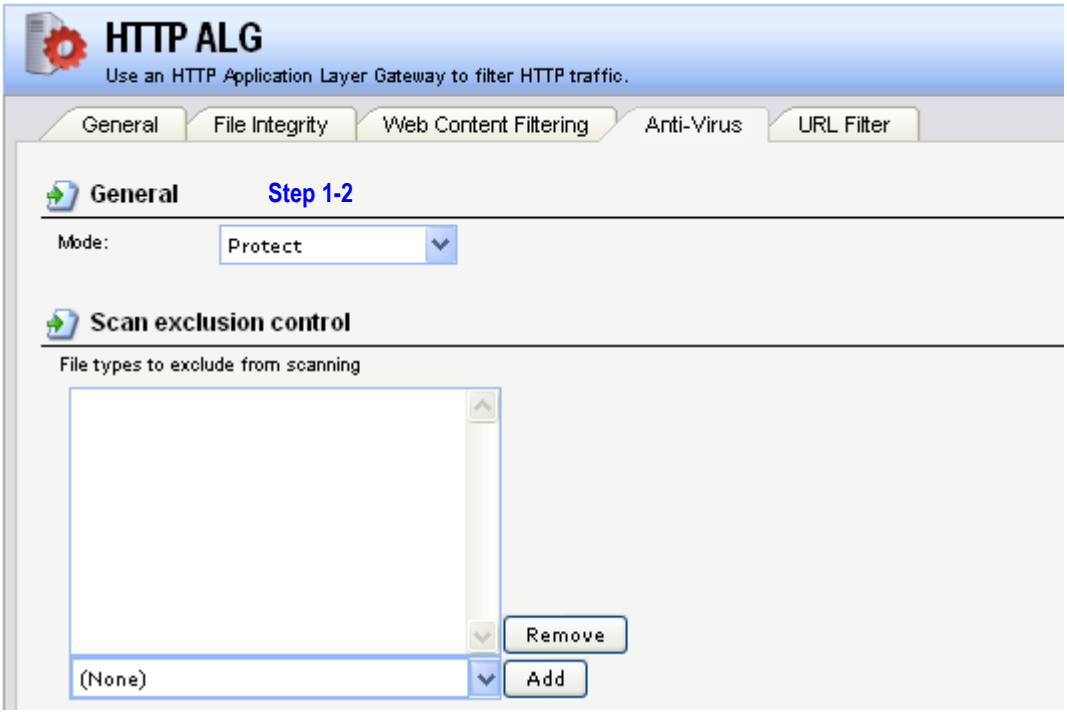

Figure 3: HTTP ALG, Anti-Virus

In Anti-Virus tab (Figure 3), trigger Anti-Virus function.

Step 1-2: General

Mode: Protect (or Audit)

Click OK

STEP 2: Service

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

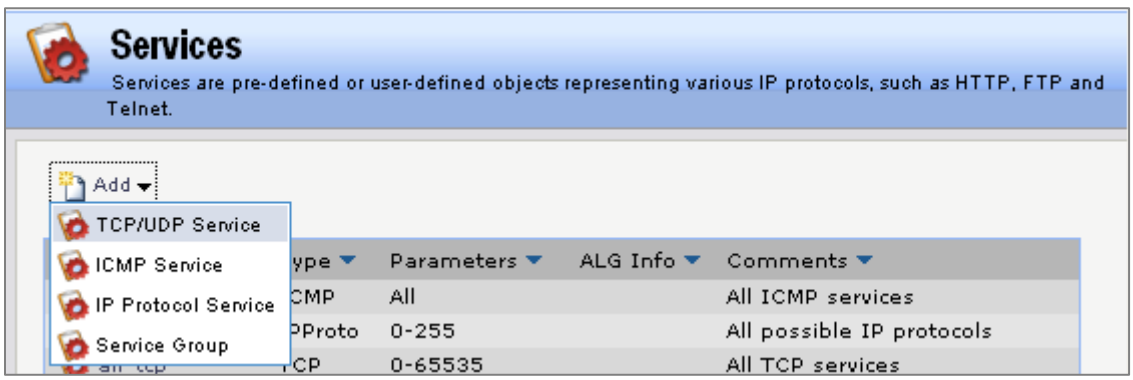

Figure 4: Add TCP/UDP Service

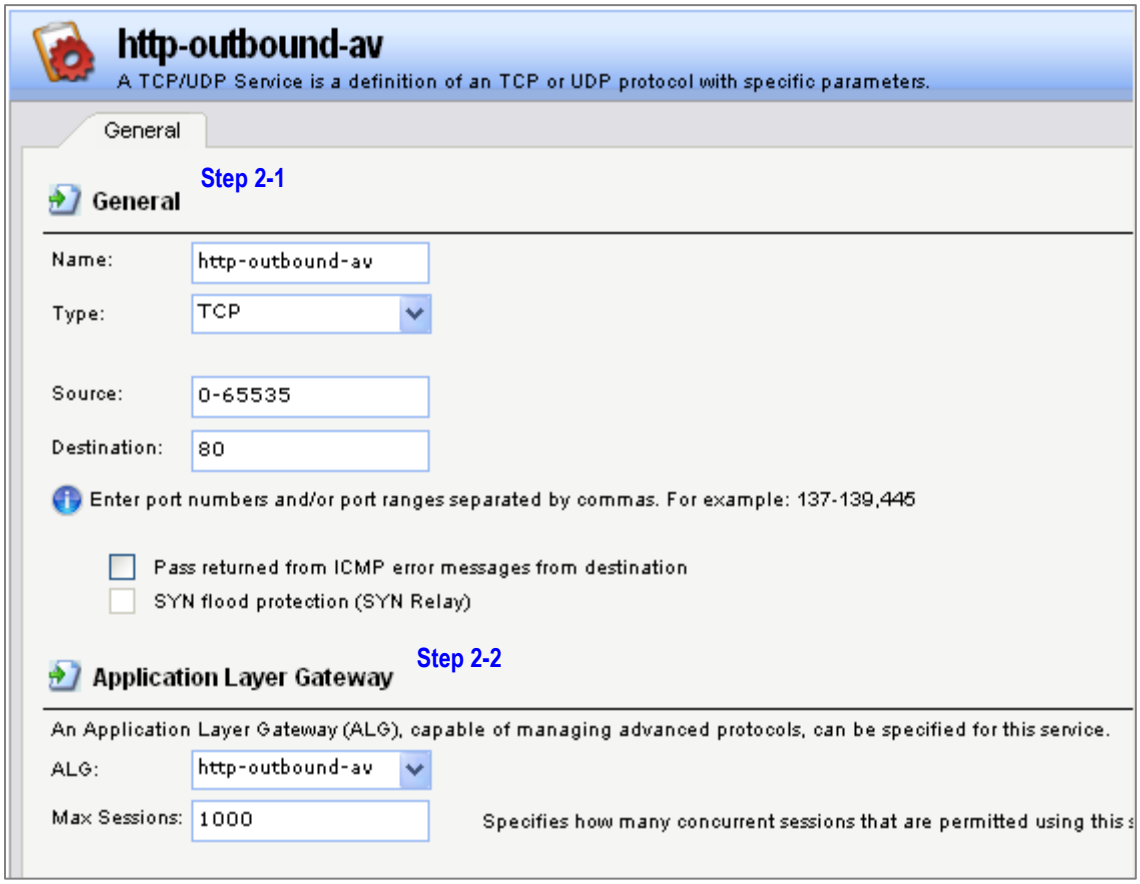

Figure 5: TCP/UDP Service

In General tab (Figure 5), fill in the related information:

Step 2-1: General

Name: http-outbound-av

Type: TCP

Source: 0-65535

Destination: 80

Step 2-2: Application Layer Gateway

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

ALG: http-outbound-av

Click OK

STEP 3: Rules

Navigate to **Rules> IP Rules** and add a new *IP Rule*. In this example, we would call Anti-Virus scanning for each file download by users, so the connection is from LAN to all networks.

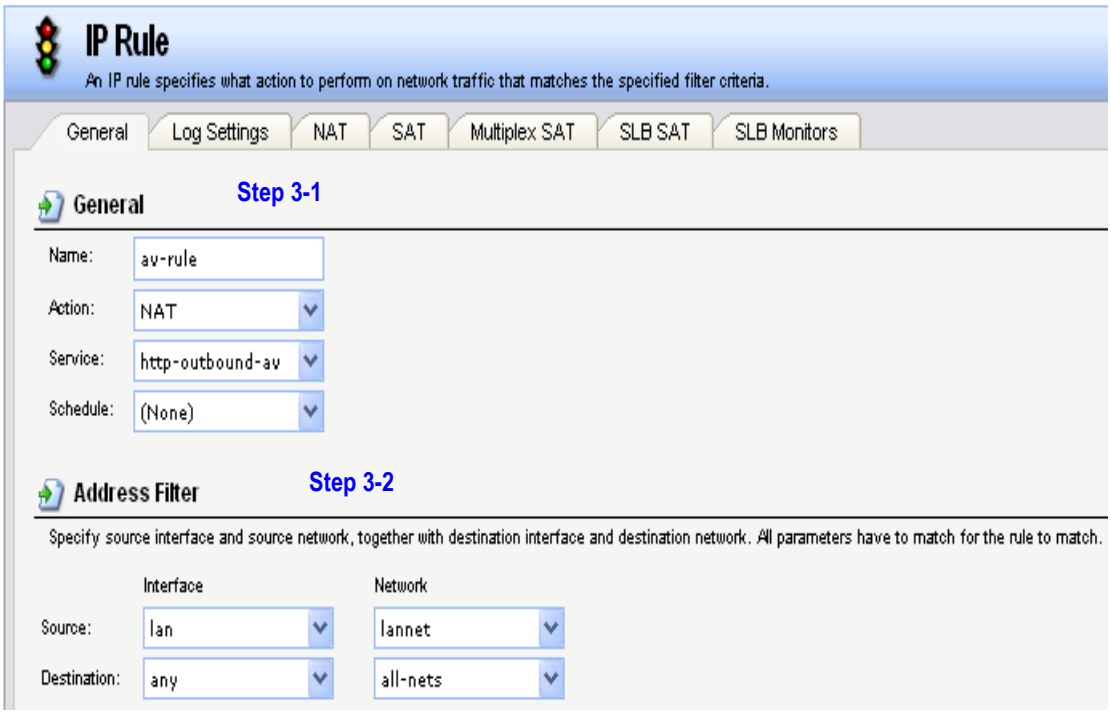

Figure 6: IP Rules

In General tab (Figure 6), fill in the related information:

Step 3-1: General

Name: av-rule (defined by user)

Action: NAT

Service: http-outbound-av

Schedule: (None) (defined by user)

Step 3-2: Address Filter

Source Interface: lan

Source Network: lannet

Destination Interface: any

Destination Network: all-nets

Click OK

In the IP Rules list, move this IP rule to the top (Figure 7).

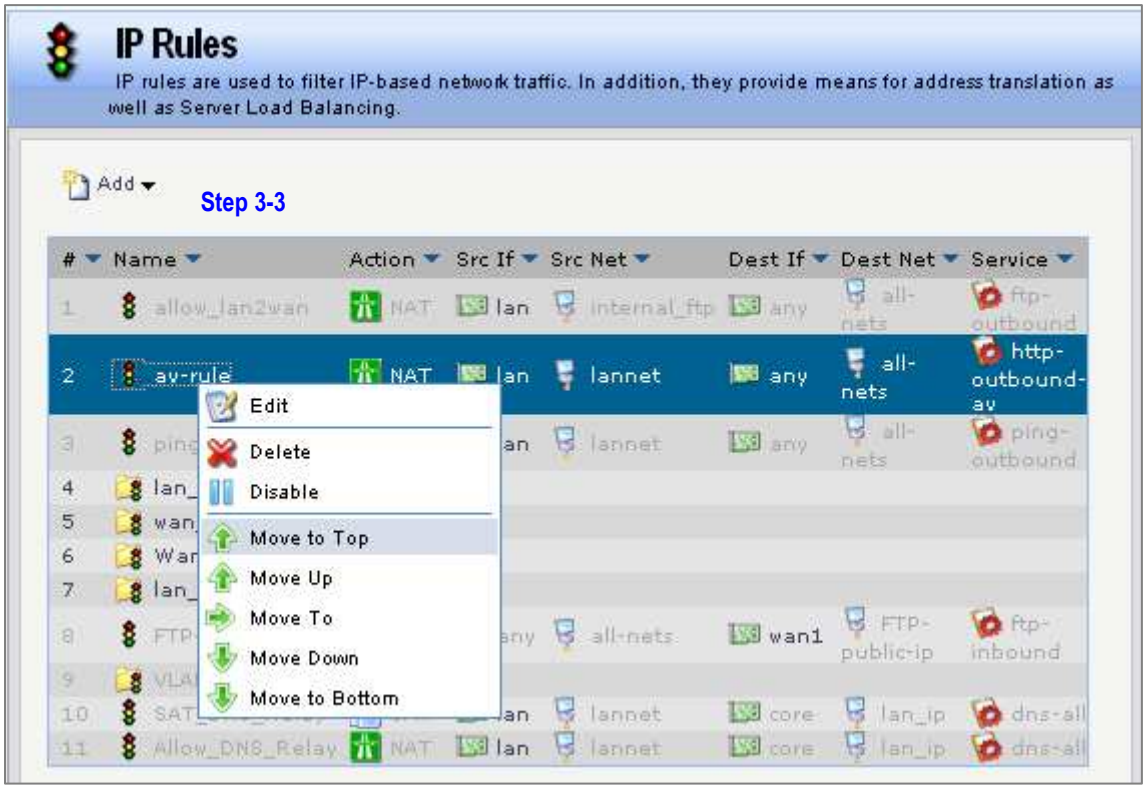

Figure 7: Rules List

Step 3-3: Change the order

Click Right-Click on av-Rule.

Click Move to Top.

[[Save and active the configuration]]