

# Configuration Example for the D-Link NetDefend Firewall Series

[Case]

**Configure Anti-Virus on UTM Firewall** 

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

**D-Link Confidential** 



#### 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*.

| ALG with AV/WCF<br>Application Layer Gateways (ALGs) are protocol helpers that can parse complex protocols, such as HTTP and H.323. |                        |          |  |  |  |
|---|------------------------|----------|--|--|--|
| Add 🗸   |                        |          |  |  |  |
| trp ALG   |                        |          |  |  |  |
| tFTP ALG  | Name                   | Туре     |  |  |  |
| b SIP ALG   | 🔯 ftp-passthrough-av   | FTP ALG  |  |  |  |
| 🏠 H.323 ALG   | 🔯 ftp-outbound-av      | FTP ALG  |  |  |  |
| b HTTP ALG  | 🔯 http-outbound        | HTTP ALG |  |  |  |
| b SMTP ALG  | 🔯 http-outbound-av     | HTTP ALG |  |  |  |
| POP3 ALG  | 🄯 http-outbound-wef    | HTTP ALG |  |  |  |
| tls ALG   | 눦 http-outbound-av-wcf | HTTP ALG |  |  |  |
| PPTP ALG  | pop3                   | POP3 ALG |  |  |  |

#### Figure 1: Add HTTP ALG

| Use an HTTP ALG            |  |  |  |  |  |
|----------------------------|--|--|--|--|--|
| General                    | File Integrity Web Content Filtering Anti-Virus URL Filter |  |  |  |  |
| 🔊 General                  | Step 1-1   |  |  |  |  |
| Name:                      | http-outbound-av   |  |  |  |  |
| 魡 Active C                 | ontent Handling  |  |  |  |  |
| Strip Acti                 | veX objects (including Flash)                              |  |  |  |  |
| Strip Java                 | a applets  |  |  |  |  |
| Strip Javascript///BScript |  |  |  |  |  |
| Block Co                   | okies  |  |  |  |  |

## 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)* 



| Use an HTTP ALG     |  |        |  |  |  |  |  |
|---------------------|--|--------|--|--|--|--|--|
| General             | General File Integrity Web Content Filtering Anti-Virus URL Filter |        |  |  |  |  |  |
| 約 General           | Step 1-2   |        |  |  |  |  |  |
| Mode:               | Protect  | ✓      |  |  |  |  |  |
| 約 Scan exclu        | 🔊 Scan exclusion control   |        |  |  |  |  |  |
| File types to exclu | ude from scanning  |        |  |  |  |  |  |
|                     |  |        |  |  |  |  |  |
|                     |  |        |  |  |  |  |  |
|                     |  |        |  |  |  |  |  |
|                     |  |        |  |  |  |  |  |
|                     |  | Remove |  |  |  |  |  |
| (None)              |  | Add    |  |  |  |  |  |

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



| A TCP/UDP Service is a definition of an TCP or UDP protocol with specific parameters.  |                         |  |  |  |
|--|-------------------------|--|--|--|
| General  |                         |  |  |  |
| 🛃 General  | Step 2-1                |  |  |  |
| Name:  | http-outbound-av        |  |  |  |
| Туре:  | тср 🗸                   |  |  |  |
| Source:  | 0-65535                 |  |  |  |
| Destination:   | 80                      |  |  |  |
| <ul> <li>Enter port numbers and/or port ranges separated by commas. For example: 137-139,445</li> <li>Pass returned from ICMP error messages from destination</li> <li>SYN flood protection (SYN Relay)</li> </ul> |                         |  |  |  |
| Application Layer Gateway  |                         |  |  |  |
| An Application   | Layer Gateway (ALG), ca | pable of managing advanced protocols, can be specified for this service. |  |  |
| ALG:   | http-outbound-av 🗸 🗸    |  |  |  |
| Max Sessions:  | 1000                    | Specifies how many concurrent sessions that are permitted using this     |  |  |

Figure 5: TCP/UDP Service

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

| Step 2-1: General      |
|------------------------|
| Name: http-outbound-av |
| Туре: ТСР              |
| 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.

| 8 IP F       | 8 IP Rule<br>An IP rule specifies what action to perform on network traffic that matches the specified filter oriteria. |            |                             |                         |                           |                                      |
|--------------|---|------------|-----------------------------|-------------------------|---------------------------|--------------------------------------|
| General      | Log Settings  | NAT        | SAT Multiple>               | SAT SLB SAT             | SLB Monitors              |                                      |
| 約 Gener      | General     Step 3-1  |            |                             |                         |                           |                                      |
| Name:        | av-rule   |            |                             |                         |                           |                                      |
| Action:      | NAT   | *          |                             |                         |                           |                                      |
| Service:     | http-outbound-av  | ¥          |                             |                         |                           |                                      |
| Schedule:    | (None)  | ¥          |                             |                         |                           |                                      |
| 約 Addre      | Address Filter Step 3-2   |            |                             |                         |                           |                                      |
| Specify sou  | rce interface and source  | network, t | ogether with destination ir | terface and destination | network. All parameters l | have to match for the rule to match. |
|              | Interface   |            | Network                     | _                       |                           |                                      |
| Source:      | lan   | *          | lannet                      | *                       |                           |                                      |
| Destination: | any   | *          | all-nets                    | *                       |                           |                                      |

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



8 **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. Add 🗸 Step 3-3 🔻 Name 🔻 Action 💌 Src If 🔻 Src Net 👻 Dest If 🔻 Dest Net 👻 Service 👻 # 8 O ftp 8 allow\_lan2wan 👬 NAT 🛛 🖾 lan 😼 internal\_ftp 🖾 any 👩 http-🖣 all-👫 NAT 🖼 Jan 🚦 av-rule 💡 lannet 🖼 any outbound nets 🞯 Edit av G allping: an 😽 lannet 💈 ping SI arty 8 Delete 4 § lan\_ 11 Disable 5 🚦 wan Move to Top 🛔 War 6 Move Up 7 g lan\_ Move To FTP-🚺 ftp-8 all-mets wan1 S FTP л Move Down 8 Move to Bottom \$ 2 8 Jan ip SAT lannet Core o dos-all an R lan ip 8 Allow\_DNS\_Relay 8 ES core 🔝 lan 6

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]]