

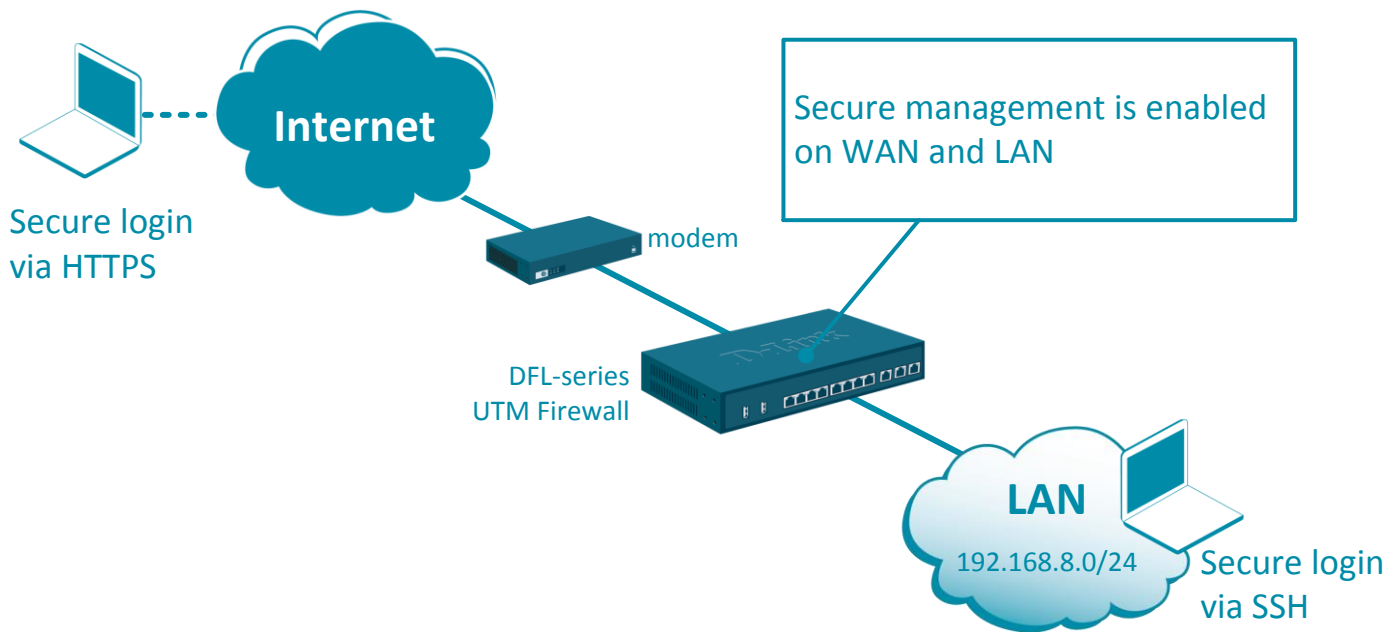
NETDEFEND

Configuration examples for the D-Link NetDefend Firewall series



How to enable remote management

This configuration example is based on the following setup:



Step 1. Log into the firewall. The default access to LAN is via <https://192.168.10.1>. Default username is "admin" and password is "admin".

Step 2. Enabling HTTPS Management on WAN: Go to System > Remote Management.

Add HTTP/HTTPS Management and specify protocol, allowed users, WAN interface and allowed networks.

The screenshot shows the 'Remote Management' configuration page. The 'HTTP/HTTPS Management' tab is selected. The 'Name' field is 'WAN_access'. The 'HTTPS' checkbox is checked. The 'Access' section shows 'User Database' set to 'AdminUsers' and 'Access Level' set to 'Admin'. The 'Access Filter' section shows 'Interface' set to 'wan1' and 'Network' set to 'all-nets'. A red arrow points to the 'Advanced Settings' button.

Step 3. Enabling SSH Management on LAN: Go to System > Remote Management. Add SSH Management and specify which interface and the allowed networks.

The screenshot shows the D-Link web interface. At the top, there are tabs for 'Status', 'System' (selected), 'Objects', and 'Netwo'. Below these are sub-tabs for 'Device' and 'Advanced Settings'. On the left, a navigation menu includes 'Device', 'Date and Time', 'DNS', 'Remote Management' (highlighted), 'Log and Event Receivers', 'Monitoring', and 'Hardware Monitoring Settings'. The main content area is titled 'Remote Management' and contains a '+ Add' button and an 'Advanced Settings' button. Below these is a table with columns for management type and 'Type'. The table has three rows: 'HTTP/HTTPS Management', 'SNMP Management', and 'SSH Management' (highlighted in blue with a red arrow pointing to it). The 'Type' column for 'SSH Management' is currently empty.

| | Type |
|-----------------------|------|
| HTTP/HTTPS Management | |
| SNMP Management | |
| SSH Management | |

The screenshot shows the 'SSH Management' configuration dialog box. It has a title bar 'SSH Management' and a subtitle 'Configure a Secure Shell (SSH) Server to enable remote'. The fields are: 'Name: LAN_SSH', 'Listening Port: 22', and 'Max Concurrent Clients: 5'. Below these are two sections: 'Access' and 'Access Filter'. The 'Access' section has 'User Database: AdminUsers' and 'Access Level: Admin'. The 'Access Filter' section has 'Interface: lan' and 'Network: lannet'.

SSH Management
Configure a Secure Shell (SSH) Server to enable remote

Name:

Listening Port:

Max Concurrent Clients:

Access
Select the user database to use for login and the access level.

User Database:

Access Level:

Access Filter
Remote access is granted from the following interface and network.

Interface:

Network:

Step 4. After the configuration is done, click “Configuration” in main bar and select “Save and Activate”. Then click OK to confirm. Wait for 15 sec. You will be automatically redirected to the firewall’s LAN IP address.

NOTE: If you do not re-login into the firewall within 30 sec, the configuration is reverted to its previous state. The validation timeout can be adjusted under System > Remote Management > Advanced Settings.

