

This document provides a description of the configuration of the Barracuda NG Firewall settings for Models F10-F301 as delivered with default factory settings and the corresponding few steps needed to activate these settings. For further instructions (e.g. on how to introduce and configure a VPN service) please see the **Administrator's Guide** that comes as a PDF file on the USB thumb drive with every Barracuda NG Firewall appliance and is also available for download from [www.barracudanetworks.com](http://www.barracudanetworks.com) in the Barracuda NG Firewall product section.

Service / Model	F10	F100	F101	F200	F201	F300	F301
<b>Firewall</b>	✓	✓	✓	✓	✓	✓	✓
<b>WiFi</b>	-	-	✓	-	✓	-	✓
<b>Port 4 assigned by DHCP</b>	✓	✓	✓	✓	✓	✓	✓
<b>Transparent HTTP Proxy</b>	-	✓	✓	✓	✓	✓	✓
<b>DHCP Server</b>	-	-	✓	-	✓	-	✓
<b>Import license (recommended)</b>	✓	✓	✓	✓	✓	✓	✓

✓=Available in default configuration

## Firewall

For the default configuration it is assumed that port4 is dynamically assigned by a DHCP service as it is available in most of today's internet connection devices such as xDSL internet routers and cable modem routers. Connecting port4 with a port on the internet device will automatically assign an IP address, network, a default route and DNS services to the Barracuda NG Firewall appliance. There are only a few manual steps required to activate this.

## WiFi

For appliances F101, F201, F301 with included WiFi hardware and antenna a corresponding WiFi service is pre-configured. For security reasons, this is not activated by default and requires a few manual steps to activate.

## WAN IP Assigned on Port 4 via DHCP

For the default configuration it is assumed that port4 is dynamically assigned by a DHCP service as it is available in most of today's internet connection devices such as xDSL internet routers and cable modem routers. Connecting port4 with a port on the internet device will automatically assign an IP address, network, a default route and DNS services to the Barracuda NG Firewall appliance. There are only a few manual steps required to activate this.

## Transparent HTTP Proxy

All models with pre-configured WiFi will also include a pre-configured http caching proxy operating in transparent mode.

## DHCP Server

For appliances F101, F201, F301 with included WiFi a DHCP service is pre-configured to dynamically assign IP addresses from the pool between 192.168.201.1 to 192.168.201.16.

## Import License (recommended)

Barracuda NG Firewalls provide firewall, VPN and L7AP functionality in DEMO MODE to be used for evaluation and training purposes without a license, but this includes severe restrictions concerning security. The default root password of **ngf1r3wall** will always work and no access control lists (ACL) from where remote login is permissible can be set up. Encryption of a VPN tunnel is limited to 56 bit keys. As long as no valid Barracuda NG Firewall license files are imported, the system will remain in DEMO MODE and must not be used for production environments.

Please note that security options like Web Filter and Malware Protection always require a valid license.

Please follow the instructions as given in points 1 to 4 in the “Barracuda NG Firewall - Quick Start Guide” for setting up and connecting to the appliance before proceeding with the next steps. The “Barracuda NG Firewall - Quick Start Guide” comes with every Barracuda NG Firewall appliance and is available for download from [www.barracudanetworks.com](http://www.barracudanetworks.com) in the Barracuda NG Firewall product section.

As indicated above, activation of this default configuration requires some manual steps. A description of these steps is given below. Please refer to the table at the beginning of this document on the necessary steps to activate the corresponding functions on your model of Barracuda NG Firewall appliance and follow the applicable steps as given below.

## FIREWALL

### 1 Connect

Copy the **ngadmin-XXXX.exe** application from the included USB thumb drive to the local hard disk.

Reconfigure the network settings of your PC to have an IP address in the 192.168.200.0/24 network other than 192.168.200.200.

Connect a RJ 45 network cable (crossed or straight wired) from your local LAN port to port1 of the appliance.

Start **ngadmin-XXXX.exe**, select **Box** and log on to **192.168.200.200** with user **root** and password **ngf1r3wall**



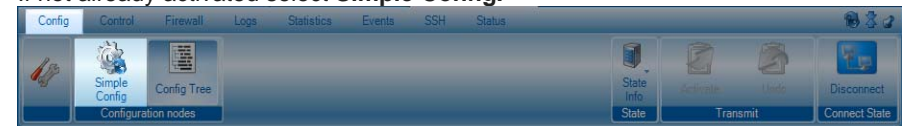
If you log on to the appliance for the first time or you login to a different appliance that now has the same IP address, a security warning may appear. Click **Trust Key** to continue



By default, the status page is displayed after logging in. Select **Config** from the tab selection menu.

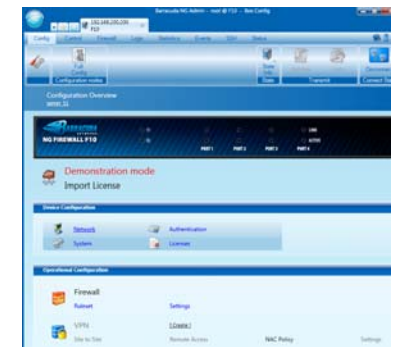


If not already activated select **Simple Config**.



The next screen displayed is the **Simple config** screen. In the section **Operational Configuration** under **Firewall** click on the **Ruleset** link.

This will display the firewall ruleset screen. Make sure the Forwarding ruleset is selected by clicking on the **Forwarding Rules** button on the left.



## 2 Forwarding Rule Configuration

To the right of the rule set screen the currently active firewall rule set is displayed. Please note that by default the **BLOCKALL** rule is on first place on top blocking all traffic.

Note:  
Depending on the model of Barracuda NG Firewall there might be more rules displayed.

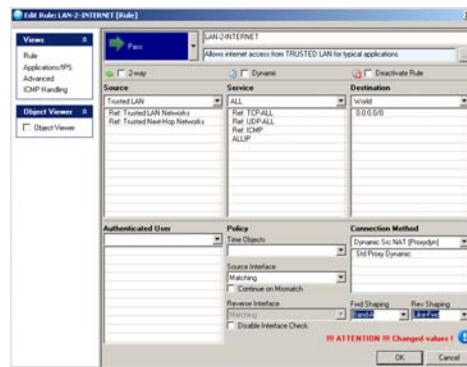
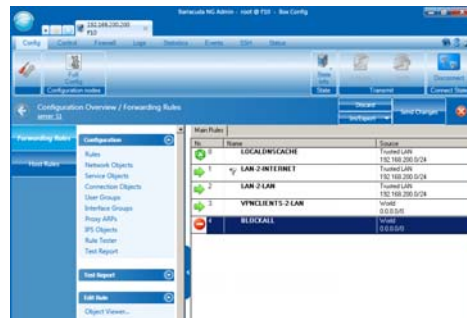
Drag the **BLOCKALL** firewall rule to the bottom of the rule list.

Open the firewall rule LAN-2-INTERNET by double-clicking the rule.

If this rule is not strict enough modify the rule according to your needs. For a detailed description on how to modify firewall rules please have a look to the **Administrator's Guide**. Residing on the USB thumb drive delivered with your Barracuda NG Firewall appliance and is also available for download at [www.barracudanetworks.com](http://www.barracudanetworks.com) in the Barracuda NG Firewall product section..

Click **OK** when done.

Continue with any other firewall rule specifying access to the internet.



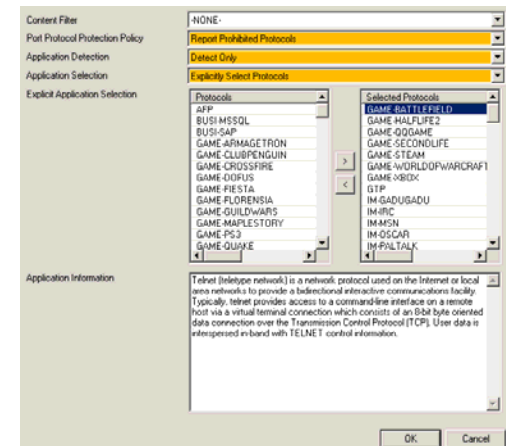
## 3 Enable Layer 7 Application Profiling

Click **Application/IPS** in the **Views** section on the left side of the rule window.

If needed set **Application Detection** to **Limit Bandwidth or Drop Traffic**.

Under **Explicit Application Selection** review, and if necessary, modify the protocols. The **Protocols** column represents all available protocols, the **Selected Protocols** column represents the currently selected ones that will be detected.

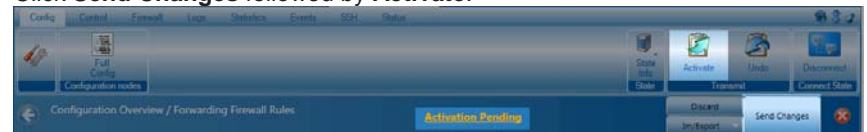
When done click **OK**.



## ! Commit Changes

To commit all previously done configuration steps, the new configuration needs to be activated at the Barracuda NG Firewall. This is indicated by the **Activation Pending** label.

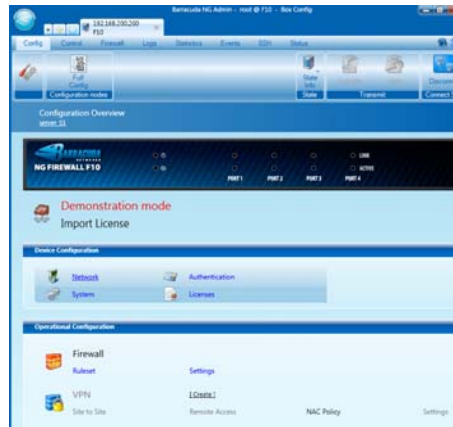
Click **Send Changes** followed by **Activate**.



## WiFi

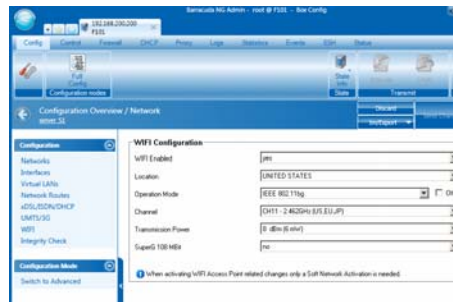
### 1 Enable WiFi

Open the **Simple Config** screen and open the **Network** link within the **Device Configuration** section.



This will open the network configuration window. On the left side menu (**Configuration**), open the **WiFi** link.

- Set **WiFi Enabled** to **yes**.
- Select your **Location**.
- Select a **Channel** appropriate to your country
- Select a **Transmission Power level**



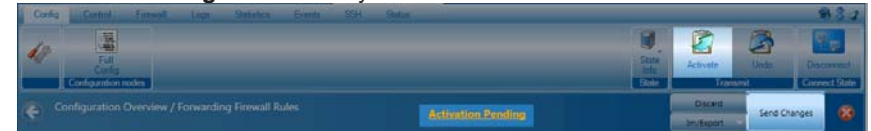
Note:

As model F101 has no active cooling fan, the highest **Transmission Power** is only recommended, if the appliance is located in a cool and well ventilated location.

### ! Commit Changes

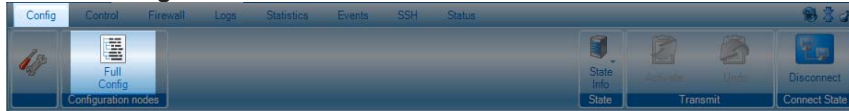
To commit all previously done configuration steps, the new configuration needs to be activated at the Barracuda NG Firewall. This is indicated by the **Activation Pending** label.

Click **Send Changes** followed by **Activate**.

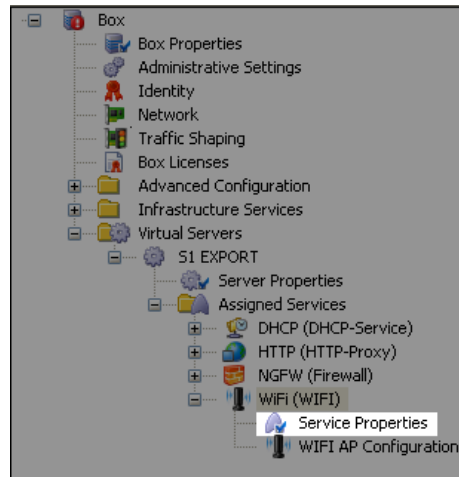


## 2 WiFi Configuration

Select **Config** from the tab selection menu and switch to Full Config by clicking the **Full Config** button.

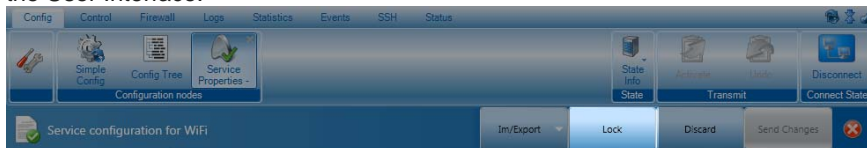


In the upcoming tree structure navigate to **WiFi**:  
**Virtual Servers > S1 EXPORT > Assigned Services > WiFi** and open the configuration node by double clicking it.



Double click on **Service Properties**.

To enable modification of settings, click the Lock button in the upper-right area of the User Interface.




In the **Service Definition** section set **Disable Service** to **No** and enter an optional descriptive text in the **Description** field.

## Commit Changes

To commit all previously done configuration steps, the new configuration needs to be activated at the Barracuda NG Firewall. This is indicated by the **Activation Pending** label.

Click **Send Changes** followed by **Activate**.



Close the configuration window by clicking .

## 3 WiFi Security Options

Stay in Full Config mode and open the **WiFi AP Configuration** node in the configuration tree.



- Enter **Network Name (SSID)**
- Click **Insert** to define a **Preshared Key (PSK) Combination**

**Basic Configuration**

Network Name (SSID)

Virtual Access Point Device (VAP)

802.11i Security

Key Management

Encryption Mode

Associated MAC	Preshared Key (PSK)
00:00:00:00:00:00	*****

Enter a password in the **New** and **Confirm** field in the appearing window. The passwords have to match and must be at least 8 characters long.

**Preshared Key (PSK) Combination**

Associated MAC

Preshared Key (PSK)  Current

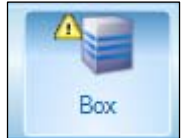
New

Confirm

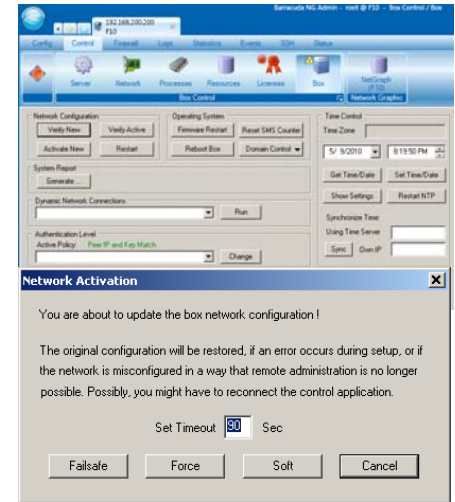
Note:  
If 00:00:00:00:00:00 is entered in the **Associated MAC** field every MAC address is accepted by the WiFi access point with that pre-shared key.

## 4 Network Activation

Some changes within the network configuration require an activation of the box network infrastructure. This is indicated by a warning symbol of the **Box** control.



Navigate to **Control > Box** and click **Activate New** within the **Network Configuration** section.



Click **Force** in the appearing **Network Activation** pop-up window.

Wait for the **Activation Succeeded** dialog, then click **OK**.

## 5 Verification

To verify the successful network activation, navigate to **Control > Network** and check if the WiFi interface **ath0** is available.

Interface/IP	Label	Ping	MAC of duplicate IP
<input checked="" type="checkbox"/> ath0 192.168.201.201/32	S1	ok	-
<input checked="" type="checkbox"/> ath2			
<input checked="" type="checkbox"/> ath3			

## ! Commit Changes

To commit all previously done configuration steps, the new configuration needs to be activated at the Barracuda NG Firewall. This is indicated by the **Activation Pending** label.

Click **Send Changes** followed by **Activate**.

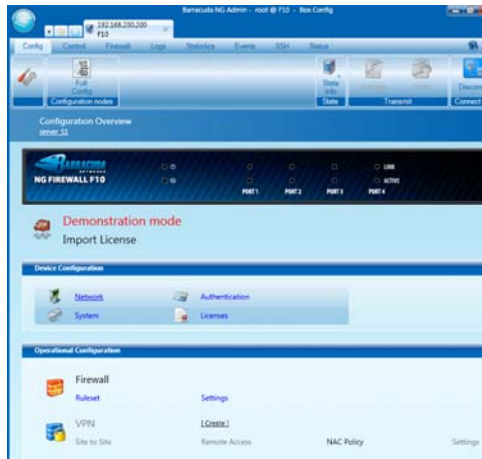


Close the configuration window by clicking

## WAN IP Assignment on Port 4 via DHCP

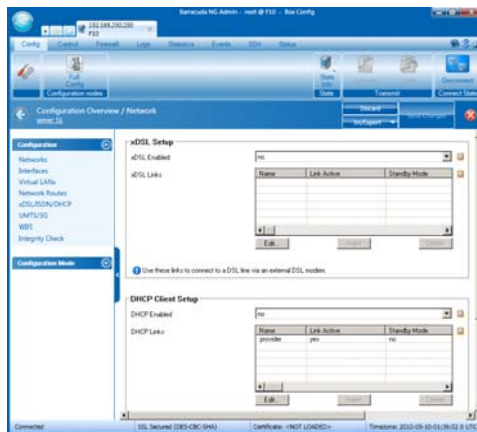
### 1 Enable WAN IP Assignment

Open the **Simple Config** and open the Network link within the **Device Configuration** section.



This will open the network configuration window. On the left side menu (**Configuration**), open the **xDSL/ISDN/DHCP** link.

- Set **DHCP Enabled** to **yes**.




### ! Commit Changes

To commit all previously done configuration steps, the new configuration needs to be activated at the Barracuda NG Firewall. This is indicated by the **Activation Pending** label.

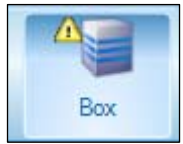
Click **Send Changes** followed by **Activate**.



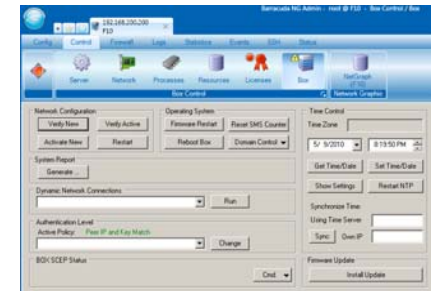
Close the configuration window by clicking .

### 2 Network Activation

Some changes within the network configuration require an activation of the box network infrastructure. This is indicated by a warning symbol of the **Box** control.

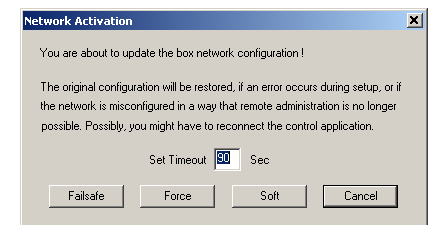


Navigate to **Control > Box** and click **Activate New** within the **Network Configuration** section.



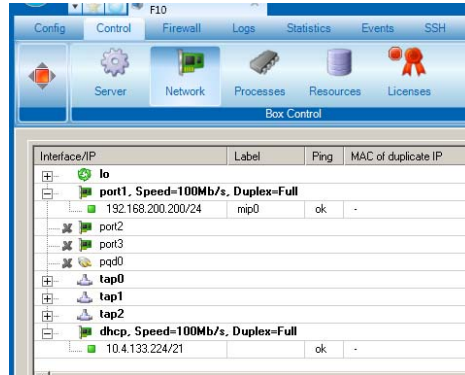
Click **Force** in the appearing **Network Activation** pop-up window.

Wait for the **Activation Succeeded** dialog and click **OK**.



## 3 Verification

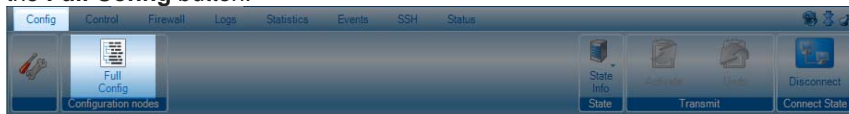
To verify the successful network activation, navigate to **Control > Network** and check if the **dhcp** interface is available.



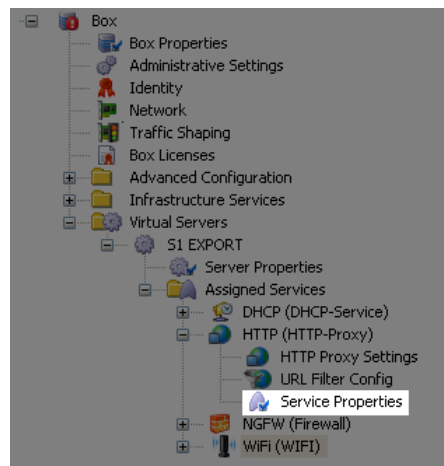
## Transparent HTTP Proxy

### 1 Enable Transparent HTTP Proxy

Select **Config** from the tab selection menu and switch to Full Config by clicking the **Full Config** button.

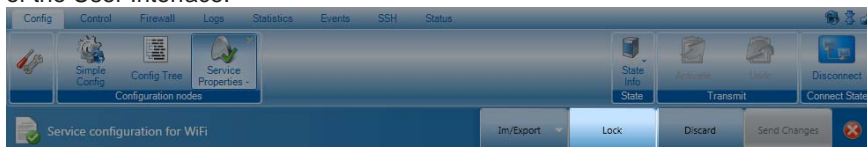


In the upcoming tree structure navigate to **HTTP: Virtual Servers > S1 EXPORT > Assigned Services > HTTP** and open the configuration node by double clicking it.



Double click on **Service Properties**.

To enable modification of settings, click the **Lock** button in the upper-right area of the User Interface.



In the **Service Definition** section set **Disable Service** to **No** and enter an optional descriptive text in the **Description** field.

### ! Commit Changes

To commit all previously done configuration steps, the new configuration needs to be activated at the Barracuda NG Firewall. This is indicated by the **Activation Pending** label.

Click **Send Changes** followed by **Activate**.

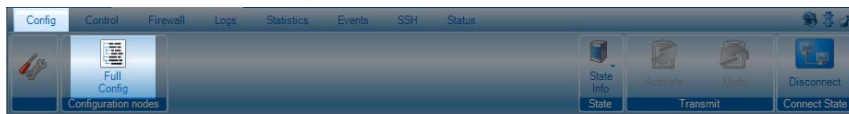


Close the configuration window by clicking .

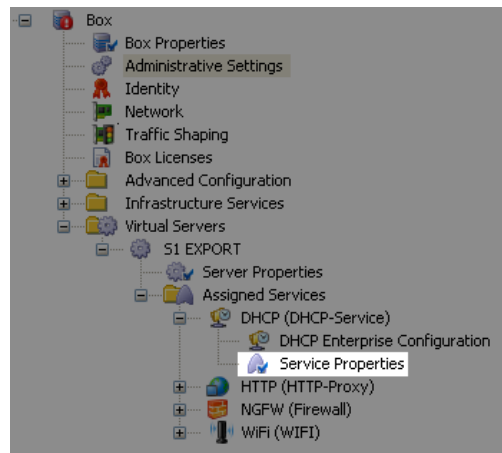
## DHCP Server

### 1 Enable DHCP Service

Select **Config** from the tab selection menu and switch to Full Config by clicking the **Full Config** button.



In the upcoming tree structure navigate to **DHCP(DHCP Service): Virtual Servers > S1 EXPORT > Assigned Services > DHCP(DHCP Service)** and open the configuration node by double clicking it.



Double click **Service Properties**.

To enable modification of settings, click the **Lock** button in the upper-right area of the User Interface.

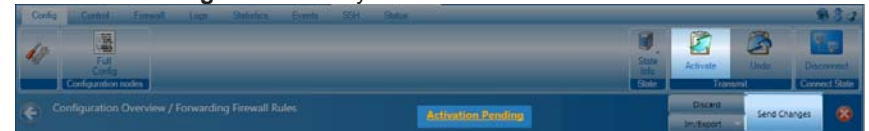


In the **Service Definition** section set **Disable Service** to **No** And enter an optional descriptive text in the **Description** field.

### ! Commit Changes

To commit all previously done configuration steps, the new configuration needs to be activated at the Barracuda NG Firewall. This is indicated by the **Activation Pending** label.

Click **Send Changes** followed by **Activate**.

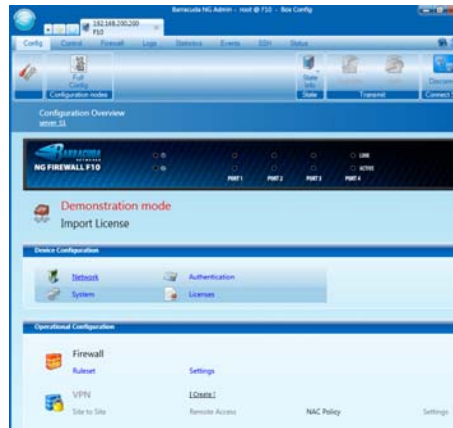


Close the configuration window by clicking .

## Import License (recommended)

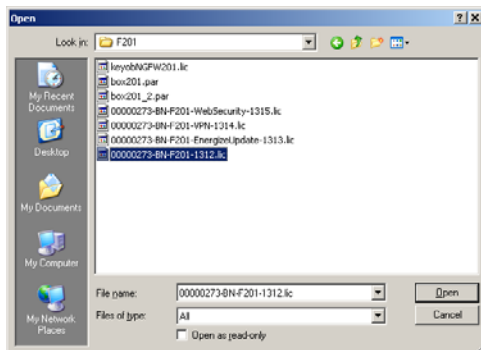
### 1 License Import

Open the **Simple Config** screen and open the **Licenses** link within the **Device Configuration** section.



This will open the **License configuration** window.

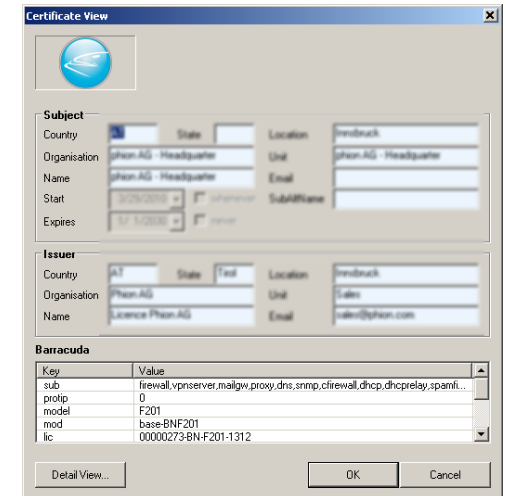
On the bottom side of the menu, click the **Import** button and select **Import from File**.



Use the appearing file-browser and navigate to the location where the license files are stored.

- **Basic license for the NG Firewall appliance**  
XXXXX-BN-F201-XXX.lic
- **License for Energize Updates**  
XXXXX-BN-F201-EnergizeUpdate-XXX.lic
- **License for SSL VPN and NAC subscription**  
XXXXX-BN-F201-VPN-XXX.lic
- **License for Web Security Subscription**  
XXXXX-BN-F201-Web Security-XXX.lic

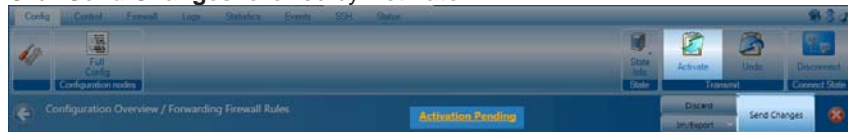
Each license file needs to be imported manually. As each license file is a digital certificate, the digital certificate info is displayed and needs to be confirmed by clicking **OK**.




## 1 Commit Changes

To commit all previously done configuration steps, the new configuration needs to be activated at the Barracuda NG Firewall. This is indicated by the **Activation Pending** label.

Click **Send Changes** followed by **Activate**.



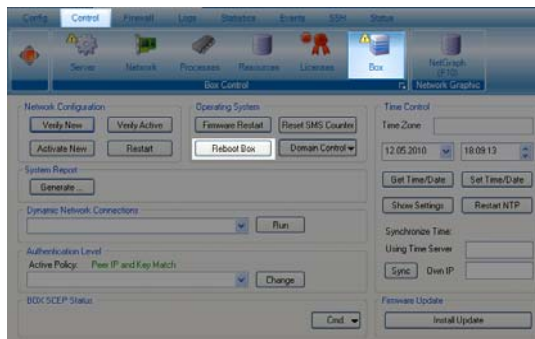
Close the configuration window by clicking .

## 2 Reboot

After importing all available license files, the Barracuda NG firewall needs to be rebooted.

Navigate to **Control > Box** and click **Reboot Box** to perform a restart of the Barracuda NG Firewall.

Caused by the reboot process you will temporarily lose connection to the Barracuda NG Firewall.



To proceed, re-connect to the Barracuda NG Firewall.

## 2 Verification

To verify the successful license import, navigate to **Control > Licenses** and check if all licenses were imported correctly.

