



Initial Configuration of PacketAlarm Intrusion Detection

created by: Rainer Bemsel - Version 1.0 - Dated: Apr/19/2003

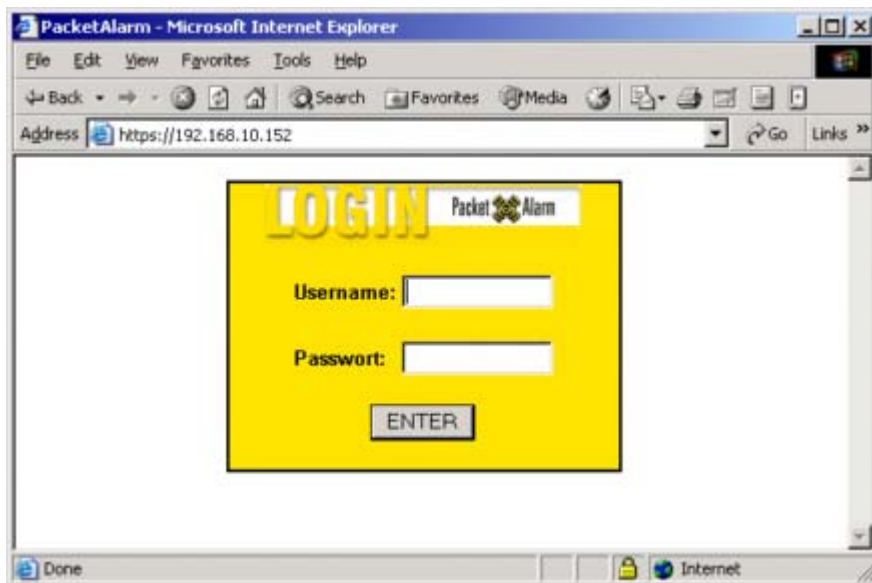
The purpose of this document is the initial configuration of Packet Alarm's Intrusion Detection. This document is based on my TechTip: "Installing a Network Based Intrusion Detection System". A more comprehensive description is available with the product.

<http://www.bemsel.com/TechTip/PacketAlarm/packetalarm.html>

It's pretty straight forward, however, once the initial configuration is done, you have to decide what rules should be activated. This can be done via Web interface.

1. Login the first time

To configure PacketAlarm you have to connect via Web browser using an SSL-Connection. Type on your browser <https://<PacketAlarm's IP Address>>. You will be asked to accept the certificate. Type in the Username "admin" and the password, you have defined during Installation.



After clicking ENTER, you will be asked to keep current password or you can set a new password.



DISCLAIMER

This Technical Tip or TechNote is provided as information only. I cannot make any guarantee, either explicit or implied, as to its accuracy to specific system installations / configurations. Readers should consult each Vendor for further information or support.

Although I believe the information provided in this document to be accurate at the time of writing, I reserve the right to modify, update, retract or otherwise change the information contained within for any reason and without notice. This technote has been created after studying the material and / or practical evaluation by myself. All liability for use of the information presented here remains with the user.



Admin Password

Your password will replace the initial admin password, which was displayed on the LCD display (appliance) or which you entered (software version) during the basic setup. If you want to keep the current password click the corresponding check box below.

Keep current password

New Password

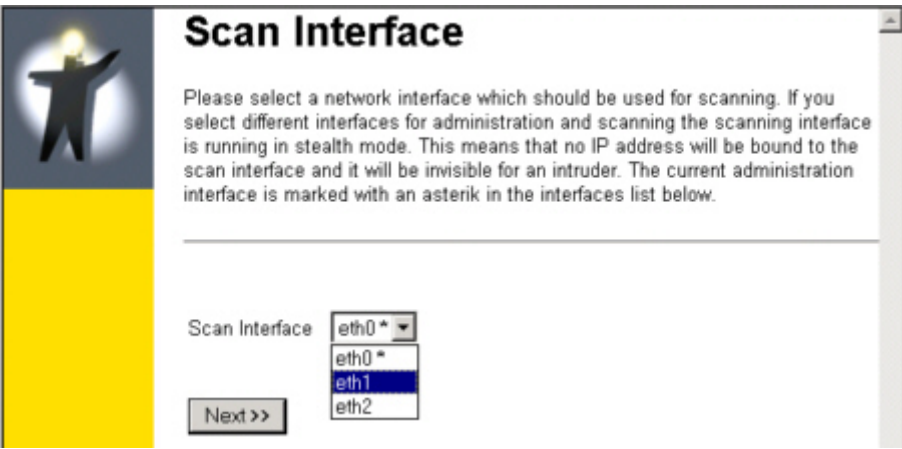
Confirm Password

Next >>

Click **NEXT** to continue

2. Set Scan interface

I was running the box as Manager and Sensor. Therefore I have to define the scan interface for my sensor type activity.



Scan Interface

Please select a network interface which should be used for scanning. If you select different interfaces for administration and scanning the scanning interface is running in stealth mode. This means that no IP address will be bound to the scan interface and it will be invisible for an intruder. The current administration interface is marked with an asterik in the interfaces list below.

Scan Interface

eth0 *
eth1
eth2

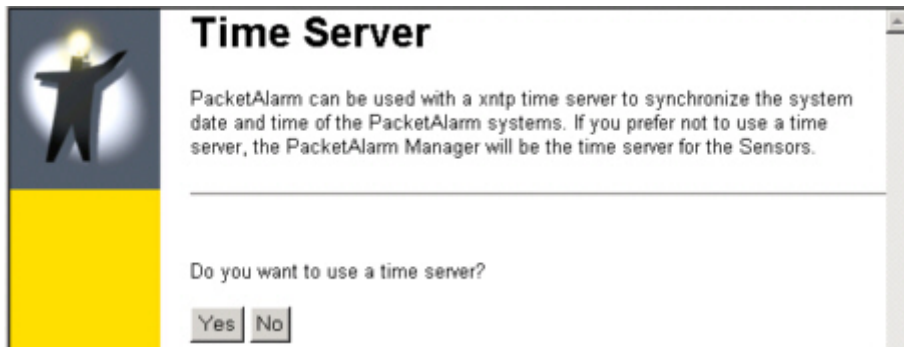
Next >>

My box is having 3 Interfaces. One is already bound for management (see *), so I can choose between eth1 and eth2. Make your choice and click **NEXT**



3. Time Server?

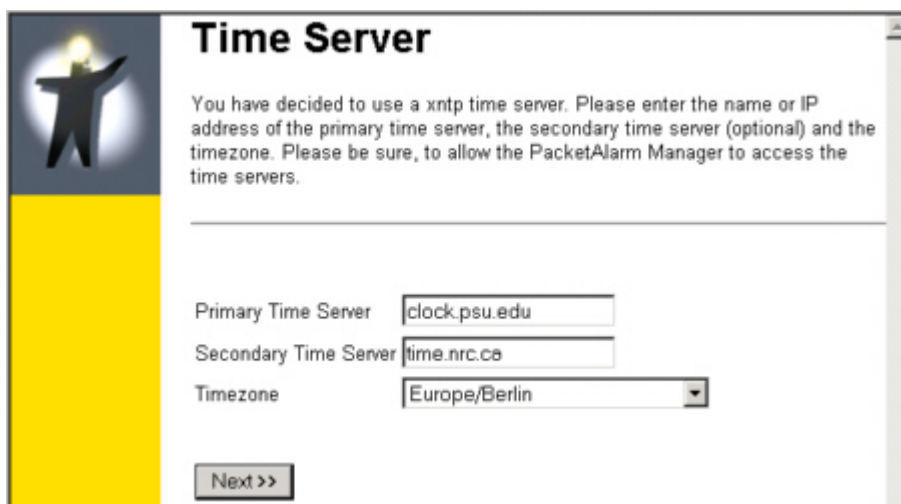
For proper time stamps, it may be useful to synchronize with a timeserver. If you have already a timeserver running on your local environment, use for security reason the local timeserver.



Time Server

PacketAlarm can be used with a xntp time server to synchronize the system date and time of the PacketAlarm systems. If you prefer not to use a time server, the PacketAlarm Manager will be the time server for the Sensors.

Do you want to use a time server?



Time Server

You have decided to use a xntp time server. Please enter the name or IP address of the primary time server, the secondary time server (optional) and the timezone. Please be sure, to allow the PacketAlarm Manager to access the time servers.

Primary Time Server

Secondary Time Server

Timezone

4. Set up SMTP Email



SMTP (Email)

PacketAlarm requires a smtp server to send email messages (notifications, reports ...). The smtp server can be specified by its hostname or IP address. Please be sure, to allow relaying on your smtp server for the PacketAlarm Manager. In addition you have to enter the FROM address of the emails sent by PacketAlarm.

SMTP Server

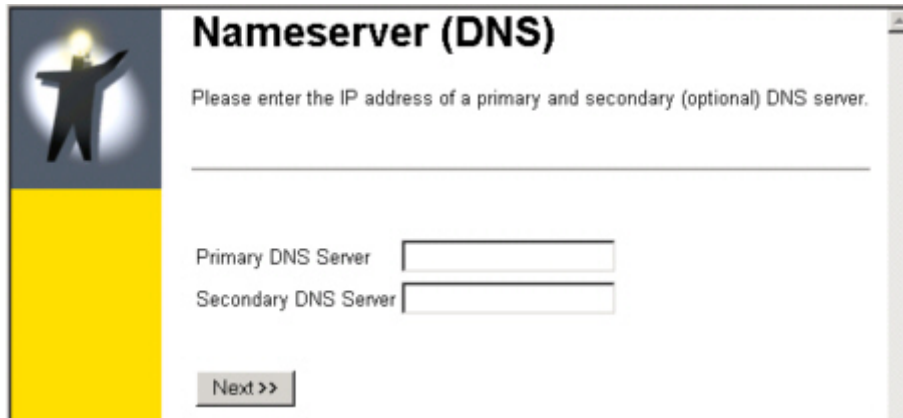
FROM Address



To get alarming, message and reports via Email, PacketAlarm need to know, what SMTP Server and what Email Address should be used.

5. DNS Server

To resolve hostnames, PacketAlarm needs to know, how DNS Server can be contacted. DNS Server has to be reachable via Administration Interface.



Nameserver (DNS)

Please enter the IP address of a primary and secondary (optional) DNS server.

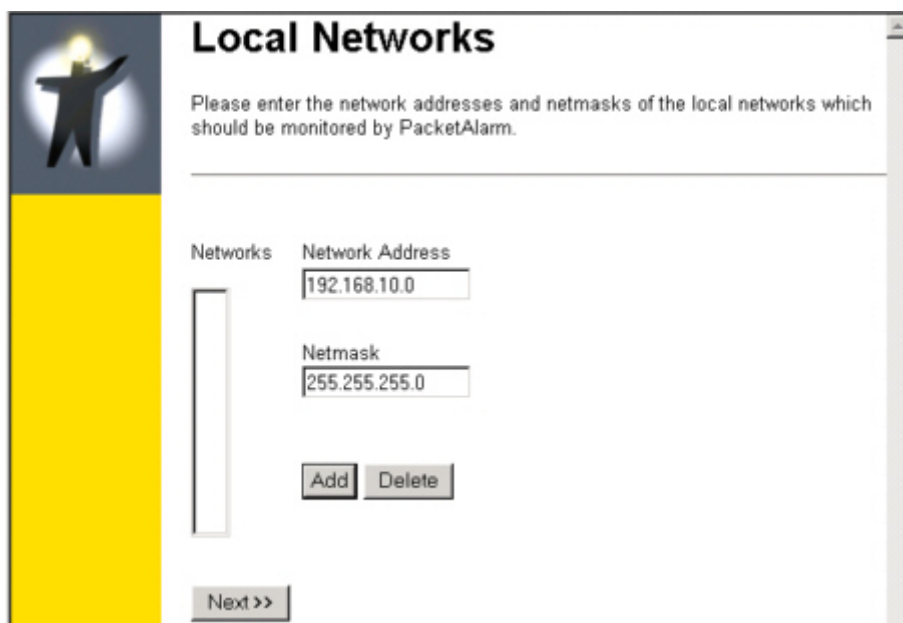
Primary DNS Server

Secondary DNS Server

Next >>

6. Local Network

This is the sensor part of PacketAlarm. If you have configured you box as Manager only, you won't see following mask.



Local Networks

Please enter the network addresses and netmasks of the local networks which should be monitored by PacketAlarm.

Networks	Network Address
<input type="text"/>	192.168.10.0

Netmask:

Add Delete

Next >>



If you have a local DNS Server, you will have to add this as well. It doesn't matter if PacketAlarm is using the local DNS Server or not. This is to prevent False Positives.

Local DNS Servers

Please enter the IP addresses of all DNS servers in the specified local networks.

Servers	IP Address
	<input type="text"/>

7. Alarm Recipient

Type in the email address, you wish to have alarms, messages and reports sent to.

Notification Email Address

Please enter an email address to receive basic notifications.

Email Address

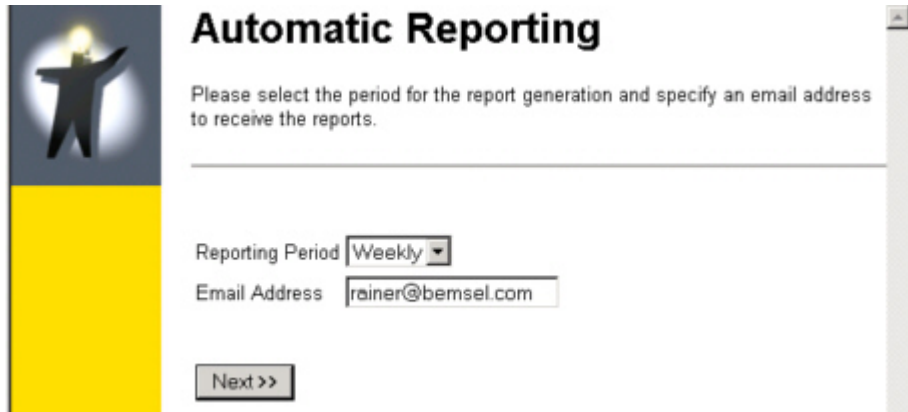
8. Automatic Reports

If you wish to get reports on a regular base, you can set it up here.

Automatic Reporting

Do you want to receive automatic reports about detected events?





Automatic Reporting

Please select the period for the report generation and specify an email address to receive the reports.

Reporting Period:

Email Address:

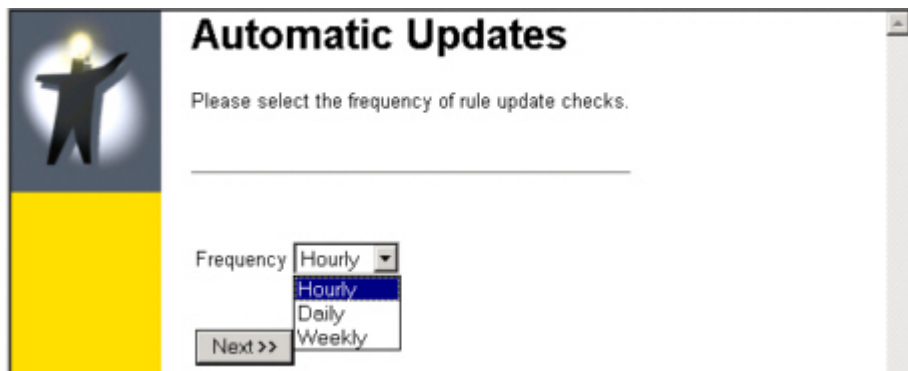
9. Automatic Updates

When using automatic update feature, you have to activate by clicking yes and setting the interval.



Automatic Updates

Do you want automatic checks for rule updates?



Automatic Updates

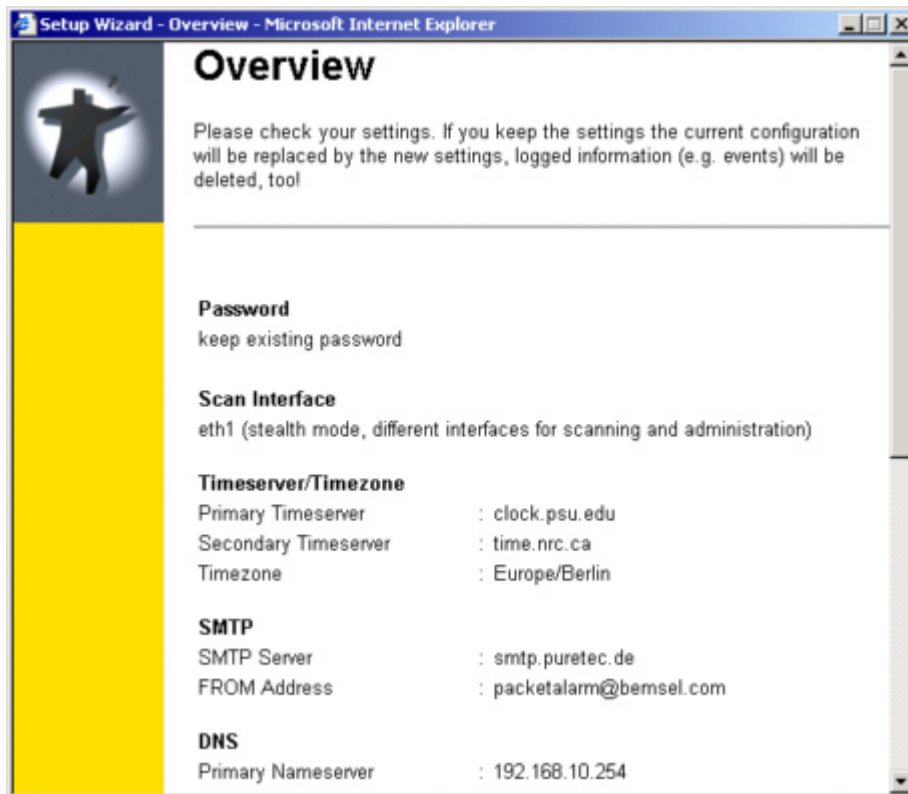
Please select the frequency of rule update checks.

Frequency:



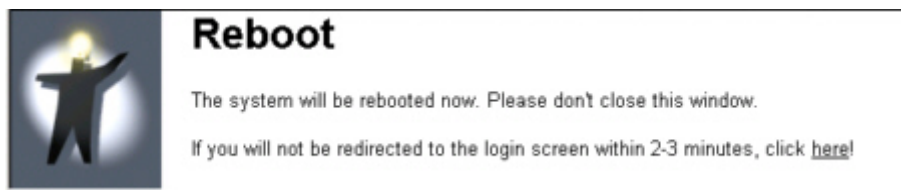
10. Verification

Finally, you have the possibility to verify all your settings. If you wish to change, just click BACK you set other values.



11. REBOOT

To have all values integrated and configured you have to reboot the box.



12. Registration

Once you have PacketAlarm installed, you have to register on <http://www.packetalarm.com>. You can choose between DEMO-License or Full-License. I run DEMO-License to see, what Packet Alarm is capable to perform.

