



User's Guide



Nettion® Copyright 2002-2008 by Nettion Information Security.

This material¹ can freely be reproduced, since that kept notes of copyright and its original content. Send critics and suggestions to *suporte@nettion.com.br*.

Revised and updated by Deyvson Matos, in July 23, 2008

Translated to english by Marcos Correia (*solsticio2for@hotmail.com*).

¹This User's Guide is based on Nettion® 4.0 Series. To download User's Guide from Nettion® 3.0 Series, access: <http://www.nettion.com.br/comunicacao/geral/Manual-Nettion3.pdf>

Contents

1	Introduction	11
1.1	Presentation	11
2	Installation/Register/Login	13
2.1	Installation	13
2.2	Register	13
2.3	Login	14
3	Settings	17
3.1	Basic	17
3.1.1	Administrator	17
3.1.2	Date/Time	18
3.2	Network	20
3.2.1	Interface/connection	20
3.2.2	Sub-Interfaces	21
3.2.3	Gateways	24
3.2.4	DNS	27
3.2.5	Routing	27
3.2.6	Dynamic DNS	31
3.2.7	Graphics	32
4	Objects	35
4.1	Objects support	35
4.1.1	Objects Inclusion	36
4.1.2	Objects Edition	36
4.1.3	Support Object Items	36
4.1.4	Object Exclusion	37
4.1.5	Object Search	37
4.2	Hosts and Networks	37

4.2.1	Support of Hosts and Networks Cadastre	38
4.3	Domains	38
4.3.1	Support of Domains Cadastre	39
4.4	Expressions	40
4.4.1	Support of Expressions Cadastre	40
4.5	Schedules	40
4.5.1	Support of Schedules Cadastre	40
4.5.2	Determining Intervals	41
4.6	Services	41
4.6.1	Predefined	41
4.6.2	Personalized	41
5	User/Groups	43
5.1	Authentication	43
5.1.1	NIS Server	43
5.1.2	Windows Server	44
5.2	Groups	45
5.2.1	Support for Groups Cadastre	45
5.3	Users	46
5.3.1	Support for Users Cadastre	46
5.4	Access Profiles	47
6	Proxy	49
6.1	Necessary Firewall Rules	49
6.1.1	Intranet → Nettion	49
6.1.2	Nettion → Internet	49
6.2	Settings	50
6.2.1	Proxy with Authentication	50
6.2.2	Transparent Proxy	50
6.2.3	General Settings	50
6.2.4	Error Messages	51
6.3	Rules	52
6.4	Composition of Proxy Rules	53
6.4.1	Screen 1 – Rule Definition	53
6.4.2	Screen 2 – Schedule	54
6.4.3	Screen 3 – Apply for:	55
6.5	Reports	56

6.5.1	Default	56
6.5.2	By Domain	57
6.5.3	Top	57
6.5.4	Blocked Accesses	57
6.5.5	On-line	57
6.6	Graphics	57
6.6.1	Selecting a Period	58
6.6.2	Visualizing Accesses Starting from the Graph	58
6.6.3	Realtime Monitoring	58
6.7	Configuring Net Stations	58
7	Bandwidth Control	61
7.1	Reprioritizing packages	61
7.2	Dynamic Band Redistribution	62
7.3	Settings	62
7.3.1	Network Interface Definition	63
7.3.2	Classes	63
7.3.3	Rules	64
7.4	Activating Bandwidth Control Service	65
8	Firewall	67
8.1	Settings	67
8.2	Rules	68
8.2.1	Including a New Rule	68
8.3	Firewall Basic Rules	72
8.3.1	Access to Nettion	72
8.3.2	Access Nettion -> Internet	73
8.3.3	Local Network Names Resolution	73
8.4	Reports	73
9	VPN	75
9.1	VPN PPTP	75
9.1.1	Settings	76
9.1.2	Support of clients' cadastre for VPN PPTP	77
9.2	VPN IPSec	78
9.2.1	Settings	79
9.2.2	Connections	81
9.3	OpenVPN	84

10 NIDS	85
10.1 Settings	85
10.1.1 Interfaces Selection	85
10.1.2 Objects	86
10.1.3 PortScan Settings	86
10.1.4 Detection of Signatures	87
10.1.5 E-mail alert	87
10.1.6 Reports	88
10.1.7 Alerts	88
10.1.8 Last Signatures	88
10.1.9 Blocked IPs	89
11 DHCP	91
11.1 Settings	91
11.1.1 Global Settings	91
11.1.2 Interface	92
11.2 Hosts	92
11.2.1 Support for Hosts Cadastre	92
11.3 Networks	93
11.3.1 Support for Networks Cadastre	93
12 E-mail	95
12.1 Settings	95
12.1.1 Authentication	95
12.1.2 Relay	96
12.1.3 Webmail	97
12.1.4 Messages	98
12.1.5 Extensions	98
12.2 Domains	99
12.2.1 Including a Domain	99
12.3 Users	100
12.3.1 Searching Users	100
12.3.2 Editing Users	101
12.3.3 Inserting Users	101
12.4 Aliases	102
12.4.1 Creating a Alias	102
12.5 Antivirus	103

12.5.1	Updating	103
12.5.2	Scheduling	104
12.5.3	Historical	104
12.6	Antispam	105
12.6.1	Settings	105
12.6.2	Learning	106
12.6.3	Whitelist	108
12.7	Reports	108
12.7.1	Queue	108
12.7.2	Logs	109
12.7.3	Auditing	109
12.7.4	Quarantine	110
12.7.5	Top Mail	111
13	Tools	113
13.1	Reverse	113
13.2	Whois	113
13.3	Ping	113
13.4	Route Trace	114
13.5	DNS Diagnosis	114
14	System	115
14.1	Services	115
14.2	Plugins	116
14.3	Backup	116
14.3.1	Settings	116
14.3.2	Manual	118
14.3.3	Reports	119
14.4	Restore	120
14.5	Pruning	120
14.5.1	Settings	121
14.5.2	Manual	121
14.6	Update	122
14.7	Graphs	123
14.7.1	CPUs	123
14.7.2	Memory	124
14.7.3	Disks	124

14.8 About	125
14.9 Audit	125
14.10 On/Off	126
15 NettionPlugs	127
15.1 What's NettionPlugs?	127
15.2 Installing a NettionPlug	127
15.3 Chat Server	128
15.3.1 Settings	128
15.3.2 Client Software (Stations)	129
15.3.3 Firewall	129
15.3.4 Launching the ChatSever Service	130
15.3.5 More Information	130
15.4 Blitz	130
15.4.1 How It works?	130
15.4.2 Blocking MSN Direct Access	130
15.4.3 Audit	132
15.4.4 Firewall	132
15.4.5 Settings	133
15.4.6 Automatic Cataloguing of Contacts	134
15.4.7 Rules	134
15.4.8 Beginning the Blitz Service	137
15.4.9 Configuring the Stations	137
15.4.10 More Information	138
15.5 OpenVPN	138
15.5.1 Nettion-Nettion	138
15.5.2 Configuring OpenVPN Server	138
15.5.3 Nettion-Users	142
15.5.4 Settings	143
15.5.5 Active Connections	145
15.5.6 More Information	148
15.6 DNS	148
15.6.1 How it Works?	149
15.6.2 Master Domains	149
15.6.3 Master Domain Items	151
15.6.4 Slave Domains	152
15.6.5 Slave Domain Items	153

- 15.6.6 Reverse Domains 153
 - 15.6.7 Starting DNS Service 153
 - 15.6.8 Firewall with DNS 153
 - 15.6.9 More Information 154
- 15.7 GetMail 154
 - 15.7.1 Advantages 154
 - 15.7.2 Settings 154
 - 15.7.3 Source Accounts 155
 - 15.7.4 Rules 156
 - 15.7.5 Starting GetMail Service 157
 - 15.7.6 More Information 157

Chapter 1

Introduction

1.1 Presentation

With the need of organizations direct connection to internet, the factor Security of Information became a primordial investment, stopping being a characteristic just of great institutions. The reason of this change is that without the protection network environment of the company, it will be subject, sooner or later, to a significant institutional damage, either moral or material.

Besides, the easiness of the 24 hours connection with the internet leads, a lot of times, employees to waste his time of work accessing several personal information, provoking a significant fall of individual productivity and, consequently, of the company.

Many times internet becomes slow, compelling to acquire a link of larger speed. However, you don't know that is possible to implement a control on that traffic in your link, having not need of extra costs with larger links in most cases.

In this reality, NIS (Nettion Information Security) offers, through Nettion®, the complete solution for the 24 hours internet connection of your organization, propitiating the implantation of an administrative politics of safety and optimization use of your link, besides the detailed control of the information that pass through it. All of that through an interactive administration of management and monitoring tool.

Nettion® benefits:

- Nettion® can make the load swinging and redundancy of your internet links, where, through simple and intuitive rules, you establish for which link the services should be directed by pattern and through where they should leave in case of fails, all this in an automatic way.
- The proxy module of Nettion® makes possible an increase of the speed when accessing pages in the internet without, necessarily, have to invest in larger links. That's possible due the Nettion®'s capacity of storing the visited pages in your cache. Another advantage, the software allows you to make a meticulous net traffic control by user, establishing rules, schedules and blocking unwanted sites. With Nettion®, you also can implant rules of safety on the local net access by users of the internet and it avoids the total exhibition to the hackers attack.
- Through reports and established rules the computer users will make more professional use of Internet, increasing the productivity and reducing the risks associated

to IT. The applied rules are flexible offering limits by users and/or by schedules. System Setting is very simple and there won't be need of specialized staff. The reports are diversified and intuitive, propitiating fair and real analyses.

- The Network Intrusion Detection System (NIDS) of Nettion® have records of almost 2.000 invasion attempt ways, what makes possible the blockade of users' access with "bad intentions".
- Another Nettion®'s resource disposes is the Bandwidth Control that allows you to establish percentile of link use for webpage access, e-mail traffic etc, optimizing and guaranteeing that all these services are simultaneously available.
- With VPN (Virtual Private Network) of Nettion®, you will use the internet as communication way in a safe mode, because your cryptographed data (shufflings) after going into internet communication tunnels. With this feature you can reduce the costs sensibly with local net interconnection, as head office and other stores, and of users physically separate from the local net using Internet as communication way and guaranteeing the safety of the data.
- The Integrated Authentication System of Nettion® facilitates the local net control with users' synchronization and integration and groups with Linux (NIS) or Windows, not needing to reregister or additional works with maintenance. Also allows integrated authentication NTLMV2, avoiding retype the password whenever it begins the internet session.
- E-mail service makes possible full autonomy for administration of mail accounts with multiple domains, allowing audit of messages, system AntiSPAM application (with system training for the local net users) and Antivirus integrated system. The accounts administration and the users' authentication come integrated with Nettion authentication system, facilitating the administration of the e-mail accounts.
- The Automated Backup and Restore Systems make possible a fast recovery of all services and information in case of hardware failure.
- Updating through Internet - the constant updating provide more safety with safety bugs upgrade and with the inclusion of new resources to the tool.

These and other Nettion tools are available in an easy and simple way, not requesting, therefore, advanced technical knowledge to operate them. With this document you will learn 'how to do it', the settings of Nettion to adapt it to your net environment.

Chapter 2

Installation/Register/Login

2.1 Installation

Nettion works on Linux distribution (Nettion Linux) totally appropriate and optimized to the operation of all your resources. Therefore, your installation, demands a dedicated machine, doesn't request a preinstalled operating system. Your Installer Setup already integrates Nettion Linux's installation and the Interface of Administration of the resources.

The Installation Guide of the product in your hardware is in a separate document, which can be easily accessed on the Nettion®'s website or through the Installation Guide link.

2.2 Register

After the installation, access your Nettion through a browser (Mozilla Firefox or Internet Explorer) using the IP address that you configured during the installation (Example: <http://192.168.254.1>). At this time you will have access the Interface Logon screen of Administration of the product, through which you will make all the necessary settings to adapt Nettion to the atmosphere of net of your company.

Logging on by the first time, the software register process will begin. The product registration it's an obligatory procedure, because only after registration it's use is allowed. In the first register form the administrator should fill out the fields with your company information and Nettion's Version that is being registered, according with illustration 2.1.

The image shows a web-based registration form for Nettion Security Software. The form has a dark blue header with the word "REGISTER" in white. On the left, there is a logo for "Nettion Security Software". The main area of the form contains three input fields: "CNPJ" with the value "01.001.001/0001-01", "Company" with the value "YOUR COMPANY NAME INC.", and "Product" with a dropdown menu showing "Nettion Enterprise". Below these fields, the text "Unregistered Version" is displayed in red. At the bottom right, there is a blue button labeled "Next>>".

Figure 2.1: First Registration Form

- CNPJ/CPF: CNPJ in the case of legal entity or CPF, if natural person;
- Social denomination: social denomination of natural person or legal entity. Example: Fortes Computer Science Inc;
- Product: Product Type. Example: Nettion Professional (in agreement with the license acquired).

Filled out the fields of the first registration form, the administrator should click in the **Next** button. The second registration form will appear, as shown in the illustration 2.2.

Figure 2.2: Second Registration Form

- Operational code: Code for generation of the answer code;
- Answer Code: Code to liberate the registration of the product;

In this second form, you should supply the **Answer Code**. Administrator will obtain the answer code after liberation requesting of your software version in our commercial department, clicking in the **Get On-line** button. A window will open up with the code and the administrator should copy the code, informed for the field **Answer Code** of that form and, finally, to click in **Register**.

Register Success. We will discover how to configure it in way to use all the resources that the software offers.

2.3 Login

To access Netition®'s administration Interface, the administrator log in, informing user's name and password, as shown in the illustration 2.3 in page 15:

- User: the user's name. Example: nettion;
- Password: the user's password. Example: nettion.

Note: the original password of nettion user is "nettion". For measures of safety it's important that you alter it soon after the first logon.

It's possible to choose between Portuguese and English languages, besides accessing the interface of the Netition using a HTTPS connection.

In case you want to use HTTPS, mark box **Secure Connection**.

It's time to begin your software settings. It's important that you begin for Product's Basic



Figure 2.3: Login form

Settings (see chapter 3). In this chapter you will learn how to altering the administrator's password, configure the other net interfaces of the equipment and how to go online with Nettione.

Chapter 3

Settings

3.1 Basic

In the first access to Nettion, the administrator should access Basic Settings and update your data, in relation to password pattern and to the sending of e-mails of the system, as well as system's Date/Time for registration in the software reports.

For your safety, the administrator should alter the Nettion user's password for a personal password, which should only have been known by authorized people to configure the system. Remember to alter that password, case it becomes known for unauthorized personal.

Note: On Chapter 5, you will obtain information about how to create users and system access profiles. This way, you will be able to create a user and define the Nettion modules which can be accessed.

3.1.1 Administrator

Password

To change password, fill out the current password field, new password and confirmation and click in the **Save Settings** button.



Figure 3.1: Change Password

For E-mail setting, fill out the Administrator's fields E-mail, your Server SMTP and click in the button to Save Settings. This e-mail will be used by Nettion to send some notification to the administrator, as for instance, notification of some problem in the backup system.

The image shows a web form titled "E-mail Settings". It has two input fields: "E-mail" and "SMTP(MX) Server". Below these fields is a "Save settings" button with a floppy disk icon. At the bottom of the form, there are two circular buttons: "Back" with a left arrow and "Items" with a list icon.

Figure 3.2: E-mail Setting

3.1.2 Date/Time

To configure system's date and hour, you have two options: to configure manually (Local Clock) or to synchronize with some server NTP (Network Time Protocol).

(a) Clock Local

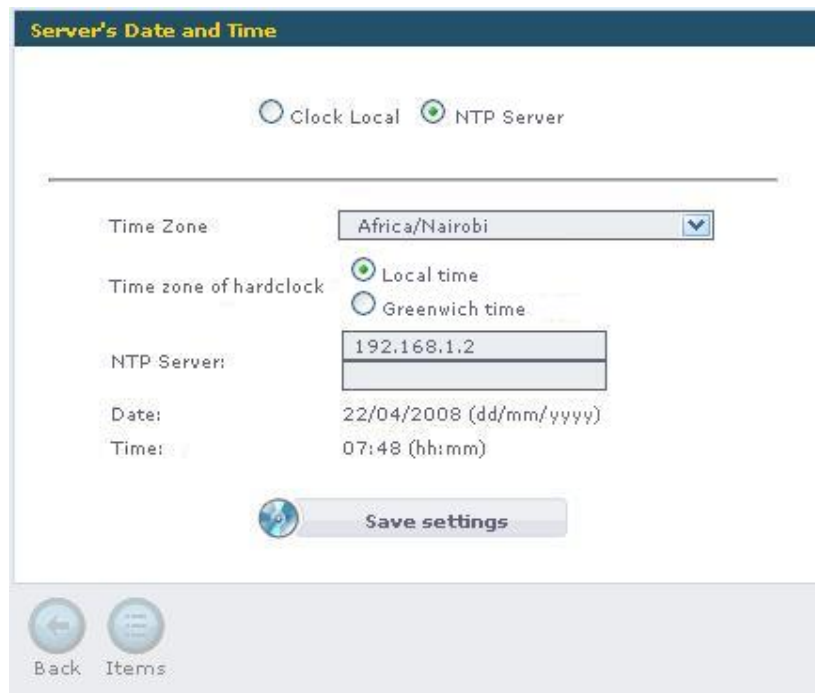
The image shows a web form titled "Server's Date and Time". At the top, there are two radio buttons: "Clock Local" and "NTP Server", with "NTP Server" being selected. Below this is a horizontal separator line. The form contains several fields: "Time Zone" is a dropdown menu showing "Africa/Nairobi"; "Time zone of hardclock" has two radio buttons, "Local time" (selected) and "Greenwich time"; "NTP Server:" is a text input field containing "192.168.1.2"; "Date:" shows "22/04/2008 (dd/mm/yyyy)"; and "Time:" shows "07:48 (hh:mm)". A "Save settings" button with a floppy disk icon is at the bottom. At the very bottom, there are "Back" and "Items" buttons with circular icons.

Figure 3.3: Manual Date and Hour Setting

- Time Zone: select your time zone;
- Time zone of hardclock: choose if you want to use your time zone (Local time) or the Greenwich time (GMT);
- Date: adjust the date in the format day/month/year (DD/MM/YYYY);
- Time: adjust the hour in the format hour:minute (HH:MM).

(b) NTP Server

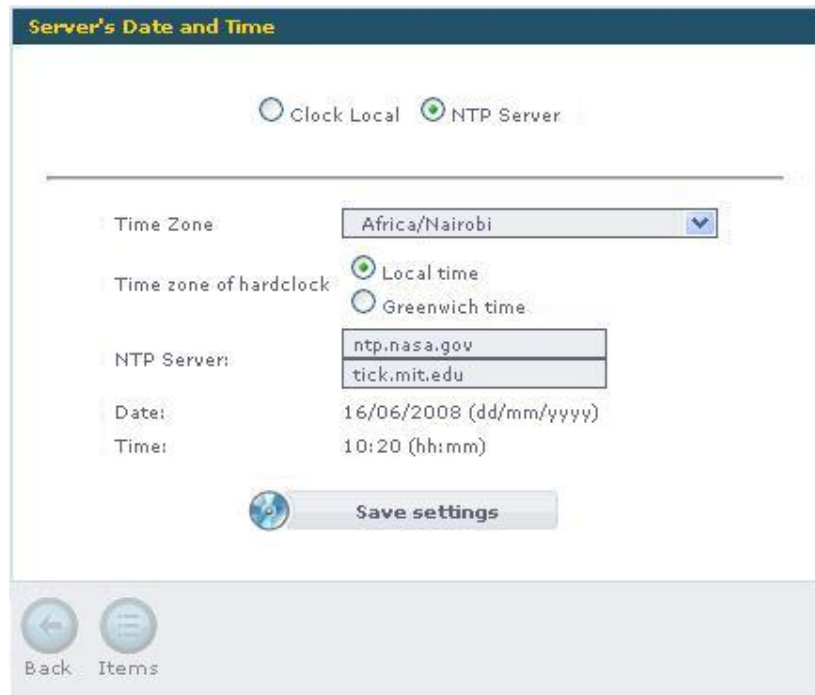


Figure 3.4: NTP Server Settings

- Time Zone: select your time zone;
- Time zone of hardclock: choose if you want to use your time zone (Local time) or the Greenwich Time (GMT);
- NTP Servers: The NTP server addresses that you which synchronize date and time. Remember to add at least one server if you want to use this function.

Firewall

It's necessary to crate a rule of Firewall to allow Nettion communicate with the NTP servers configured. An Example of the necessary rule is in table 3.1 (page 19).

Rule: Nettion -> NTP Servers			
Source	Destiny	Destiny Serv.	Action
localhost	Any	ntp	Accept

Table 3.1: Liberating Nettion for NTP servers

All the details of “how to configure” Firewall and your rules are in the Chapter 8 in page 67.

3.2 Network

3.2.1 Interface/connection

In this section you can make the setting of other interfaces and net connections of your equipment (the first was already configured during the installation).

Ethernet Interfaces (LAN)

As it was previously commented, Nettion already configure the first interface Ethernet of the equipment (eth0) during the software installation. To add other net Interfaces, access menu option Settings → Network → Interfaces/Connections. In the following screen, you'll have access the listing of interfaces already registered in your Nettion, as it proceeds in the example of illustration 3.5 (page 20).



Interface	IP	Mask	Description	Velocity	Status
eth0	192.168.0.1	255.255.255.0	Internal Net (LAN)	100Mbit	
eth1	200.200.200.1	255.255.255.192	External Net (WAN)	1Gbit	
eth2	200.200.200.32	255.255.255.224	DMZ Area	100Mbit	

Page 1 of 1 Go to .. 3 record(s)

Back Add Edit Items Del

Figure 3.5: Listing of Interfaces and Connections

To add a new Interface Ethernet follow these steps (you also can see the illustration 3.6 in page 21):

- Click in the button “Add” located below the listing;
- In the following screen, select the interface Ethernet “type” and click in “Next” and wait;
- At this time Nettion will try to detect your net devices installed and its respective drivers. Each detected interface will be shown in the following screen. Select one of them and click “Next”.

Important: In case the driver of the device has not been automatically identified, the device will be listed marked with a “ * ”. In these cases, it’s probable, that Nettion doesn’t possess the appropriate driver to support it. Please, contact with the manufacturer through the address suporte@nettion.com.br and send the largest number of information of the device, as model, manufacturer and chipset.

- In the following screen it fills out the information of your network device:
 - Driver: Detected automatically by default;
 - IP address: Indicate IP address that will be attributed to device, or click in DHCP option for Nettion use a supplied IP by your DHCP net server;
 - Net Mask: Indicate the mask of your actual net;

- Speed: Indicate the speed of the device. This information will be used in Bandwidth Control service;
- Description: It indicates a description on the net interface, as “Intranet Interface”;
- Obtain server DNS: To obtain the setting of DNS automatically. That’s possible in cases of activated DHCP;
- Answer DNS requests in this interface: This option makes Nettion announces your service of DNS in this interface;
- Boot activate: Indicate “Yes” to activate the interface automatically in the boot of Nettion®.

Specify the parameters below

Interface Eth0 ()

MAC Address: 00:30:6E:2E:0B:8C

Driver: Intel(R) PRO/100 Network Driver (e100)

IP Address: 192.168.0.1 ☐ DHCP

Netmask: Default class C /24

Rate: 100Mbits

Description: Internal Interface

☐ Get DNS from Server

☐ Respond DNS requests on this Interface

Active on boot: ☒ Yes ☐ No

[Save settings](#)

[Back](#) [Items](#)

Figure 3.6: Add/Edit of Ethernet Interface

3.2.2 Sub-Interfaces

Nettion also supports the inclusion of net sub-interfaces. They’re always associated to physical Interface and they possess two purposes basically:


1. Additional IPs in an Interface: it allows an interface to answer for other IPs addresses, besides the principal;
2. ADSL connections: it allows that an ADSL connection is attributed to an Interface. This option will only be available on DHCP Interface, as you will be seen more ahead.

Additional IPs

To add an additional address to an Interface follows the steps (see the illustration 3.7 in page 22):

- In the listing screen, select the Interface that will receive additional IP and click in the button “Items”;
- In the following screen, a listing of device sub interfaces will be presented. Click “Inclusion” button;
- In the following screen, select “Sub interface” type and click in Next;
- Now indicate: IP Address, Net Mask, Description and if the interface will answer for requisitions DNS in the sub interface;
- To conclude click in “Add Interface” button.

Specify the parameters below


 **Eth0:0**

IP Address: 10.0.0.1

Netmask: Default class A /8

Description: Sub-interface

Respond DNS requests on this Interface ☐

 **Save settings**




 **Back**  **Items**

Figure 3.7: Sub Interface Inclusion

After the inclusion, the Sub interface will be listed as shown in illustration 3.8 (page 22). Note that the nome of the subinterface has the same name of the main device + number of subinterface. If needed, include others subinterfaces following the same steps.

Interface	IP	Mask	Description	Status
eth0:0	192.168.0.30	255.255.255.0	Service 01 Sub-Interface	

Page 1 of 1 Go to .. 1 record(s)





 **Back**  **Add**  **Edit**  **Items**  **Del**

Figure 3.8: Sub Interfaces Listing of a Net Device

ADSL Connections (WAN)

To add a ADSL Connection the main Interface (physics) should be configured to receive IP through DHCP and should be with the setting “to Activate in the boot” as “No”, as

shown in the illustration 3.9 of the page 23.

Specify the parameters below

Interface Eth1 ()

MAC Address

Driver: RealTek RTL-8139 Fast Ethernet

IP Address: ☒ DHCP

Netmask: Default class A /8

Rate: 100Mbits

Description: ADSL Interface

☐ Get DNS from Server

☐ Respond DNS requests on this Interface

Active on boot: ☒ Yes ☐ No

Save settings

Back Items

Figure 3.9: Interface Setting for ADSL Connection

Important: These connections depend properly on a modem ADSL installed and configured. The modems ADSL can be configured in “bridge”, where Nettion will make the administration of the connection ADSL and it will be with the IP given by provider (recommended), or in “router”, where the modem will be responsible for doing this management. The settings to proceed are for “bridge”. In case it’s in “router” configures ethernet interface to communicates with the modem and configure Nettion’s Gateway appearing for modem’s IP.

The procedure is similar for inclusion of additional IPs (see illustration 3.10 in page 24):

- In the listing screen, select the Interface that will receive ADSL connection and click in the “Items” button;
- In the following screen, a listing of device’s sub interfaces will be presented. Click in the button “Inclusion”;
- In the following screen, select “ADSL(wan)” and click in Next;
- In the following screen, fill out provider ADSL’S information:
 - User: access login;
 - Password: access password;
 - Extra parameters: only if necessary and supplied by the provider;
 - Speed: indicate the speed of the link;
 - To obtain Server DNS: mark for Nettion to receive the information of the provider’s DNS;
 - To activate in the boot: indicating “Yes”, connection will be activated automatically in the boot.

Specify the parameters below

Adsl0 Connection

User: 8532221122@telem

Password: *****

Extra Parameters: (pppoe)

Rate: 1Mbit

Get DNS from Server: ☒

Active on boot: ☒ Yes ☐ No

Add Connection

Back **Items**

Figure 3.10: Setting of ADSL connection

After your ADSL interface inclusion will be listed as follows it in the illustration 3.11 (page 24), with information of IP and Connection status. In case the Status isn't ok (red) verify again the settings of the connection.

Interface	IP	Mask	Description	Status
adsl0	200.200.200.200	255.255.255.255	ADLS Interface - Velox	

Page 1 of 1 Go to .. 1 record(s)

Back **Add** **Edit** **Items** **Del**

Figure 3.11: Listing of the ADSL Connection

3.2.3 Gateways

So that Nettion can have Internet access, it's necessary that it has at least one Gateway, in other words, at least an access exit for Internet. Therefore, this is one important setting in the implantation of your Nettion. You'll also see that Nettion management multiples Gateways, making the whole redundancy treatment and swinging of the links.

Edition of Gateways

A Gateway is usually configured already during the Nettion's installation in the equipment. In case you want to edit your information follows the steps below:

- Access the menu Settings → Net → Gateways;
- In the following screen, of registered gateways listing, select Gateway that you want to edit and click in the button “edit”;
- In the following screen:
 - Interface: indicates the Nettion’s interface that is directly linked to the gateway. In the case of a Gateway for ADSL connection, select the ADSL Interface corresponding;
 - Gateway: indicate Gateway’s IP, in other words, IP through which Nettion will have Internet access – that is supplied by your access provider. In the case of a dynamic gateway, like DHCP or ADSL, mark the option “Dynamic Obtained”;
 - Participation in the route default: it indicates the percentage of this link’s participation in the Internet’s standard exit of Nettion. In case of one only link the pattern will be 100%;
 - Timeout: indicate here the maximum time without answer (in seconds) in that Nettion will consider that a gateway is offline. Nettion will change the gateway’s state for “down” when stops answering inside here of the stipulated time. For not indicating a time limit, select the option “Limitless”;
 - Redefine settings in the change of gateway’s state: mark this option in case you want that the Nettion redefines gateways’ settings to each state change, as for instance, the participation settings of gateways in the default route.

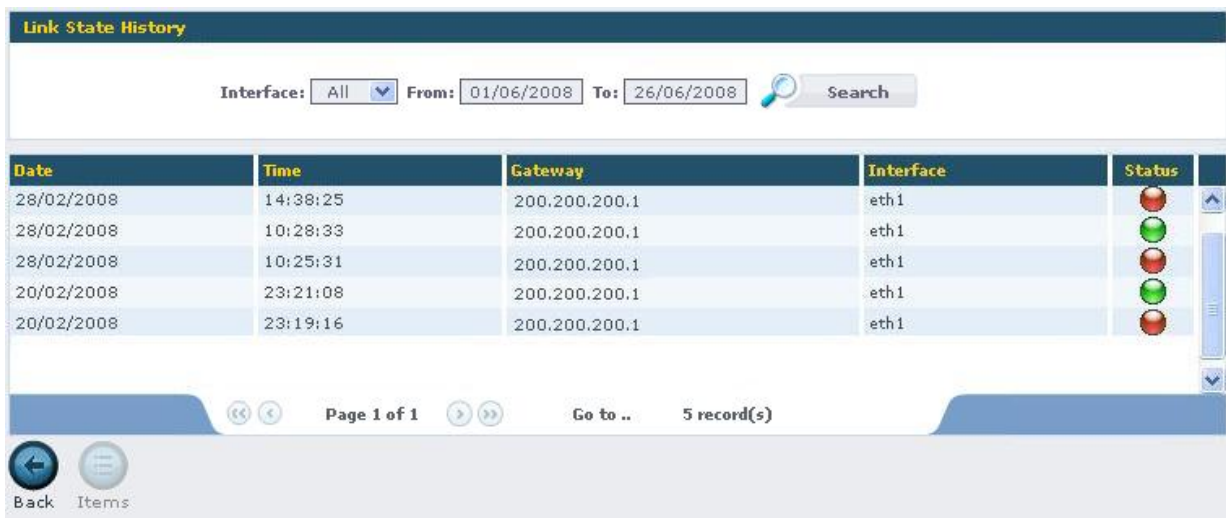
Inclusion of new Gateways and Internet Multiple Links

In case there is not any configured Gateway, or you want to do the inclusion of additional Gateways, for the case of Internet multiple Links, follow the steps to proceed.

- Access the Settings menu → Net → Gateways;
- In the following screen, of the registered gateways’ listing, select Gateway that you want to edit and click in the button “Inclusion”.
- In the following screen:
 - Interface: indicates the Nettion’s interface that is directly linked to the gateway. In the case of a Gateway for ADSL connection, select the ADSL Interface corresponding;
 - Gateway: indicate Gateway’s IP, in other words, IP through which Nettion will have Internet access – that is supplied by your access provider. In the case of a dynamic gateway, like DHCP or ADSL, mark the option “Dynamic Obtained”;
 - Participation in the route default: it indicates the percentage of this link’s participation in the Nettion’s standard exit for Internet in relation to other Gateways already registered. In case of an only link the default will be 100%.
 - Timeout: indicate here the maximum time without answer (in seconds) in that Nettion will consider that a gateway is offline. Nettion will change the gateway’s state for “down” when stops answering inside here of the stipulated time. For not indicating a time limit, select the option “Limitless”;
 - Redefine settings in the change of gateway’s state: mark this option in case you want that the Nettion redefines gateways’ settings to each state change, as for instance, the participation settings of the gateways in the default route.

Notice that the traffic can be divided in agreement with a specified percentile (**participation in pattern route**), allowing to define priorities with relationship to the use of one of the links. It's also possible that a gateway doesn't participate in default route (0%). In this case, the link will be used through two forms: for accesses, originated externally to available services in your net (Example.: VPN, E-mail, Portal Web) and for traffic, foreseen in "advanced routing" rules as it will be shown ahead in the topic.

Monitoring By default, the links are monitored by the system that reconfigures automatically the atmosphere in agreement with the availability. Each change is registered in the state of your links, allowing your audit. For that to select a gateway and click in Items button. The state report of the gateways will be exhibited, according the illustration 3.12 below:



Link State History

Interface: All From: 01/06/2008 To: 26/06/2008 Search

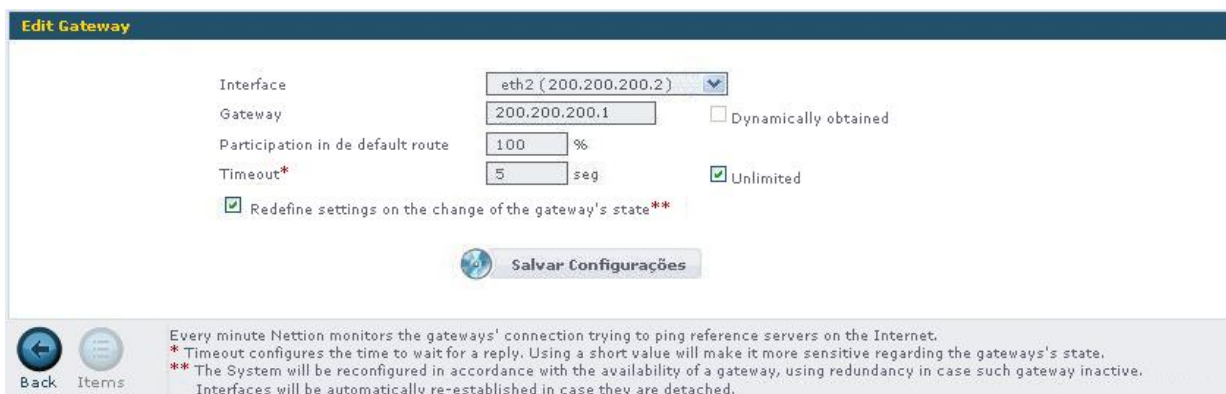
Date	Time	Gateway	Interface	Status
28/02/2008	14:38:25	200.200.200.1	eth1	
28/02/2008	10:28:33	200.200.200.1	eth1	
28/02/2008	10:25:31	200.200.200.1	eth1	
20/02/2008	23:21:08	200.200.200.1	eth1	
20/02/2008	23:19:16	200.200.200.1	eth1	

Page 1 of 1 Go to .. 5 record(s)

Back Items

Figure 3.12: Gateways Monitoring

However, it's possible to edit the monitoring options of gateways state in accordance with your need. For that, select the wanted gateway and click in the "Edit" button. The edition options of the gateway will be exhibited as display the illustration 3.13 below:



Edit Gateway

Interface: eth2 (200.200.200.2)

Gateway: 200.200.200.1 ☐ Dynamically obtained

Participation in de default route: 100 %

Timeout*: 5 seg ☒ Unlimited

☒ Redefine settings on the change of the gateway's state**

Salvar Configurações

Back Items


Every minute Nettion monitors the gateways' connection trying to ping reference servers on the Internet.
 * Timeout configures the time to wait for a reply. Using a short value will make it more sensitive regarding the gateways's state.
 ** The System will be reconfigured in accordance with the availability of a gateway, using redundancy in case such gateway inactive.
 Interfaces will be automatically re-established in case they are detached.

Figure 3.13: Gateways Edition

Modify the setting options according to section "Gateways Edition" of this chapter.

3.2.4 DNS

In this section, you configure the machine's name and DNS servers that will be consulted by Netion for resolution of Internet names. The machine's name should be complete (machine's name + domain). If you don't possess a domain, it can use **localdomain**. At least a DNS server should be configured for correct operation of product. That setting can be automatic, if you have an activate Ethernet interface configured through DHCP, or an ADSL connection, in this case select the item **Obtain DNS from server** in the respective connection setting. Netion can be DNS server, since it possesses Internet direct access in the port 53 TCP and UDP. To use it as server, indicate IP 127.0.0.1.



The screenshot shows two configuration panels. The top panel, titled "Host Name", has a text input field labeled "Host + Domain" containing "nettion.yourcompany.com" and a "Save settings" button. The bottom panel, titled "DNS Servers", has two input fields: "Primary" with "127.0.0.1" and "Secondary" with "200.200.200.200", followed by a "Save settings" button. At the bottom of the interface are "Back" and "Items" navigation buttons.

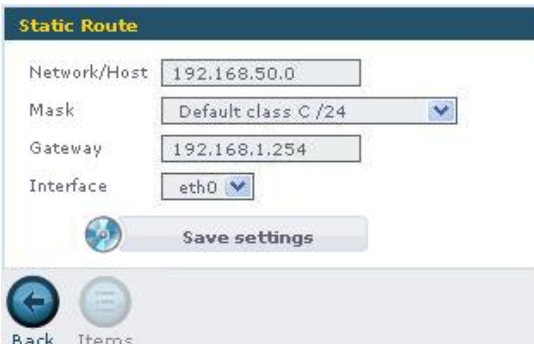
Figure 3.14: Machine's Name and DNS Setting

3.2.5 Routing

In that section it's possible to add rules that will control the net traffic destiny.

Basic

Basic routing or else by destiny it's the functionality that turns reachable a net/host through a host (gateway), also reachable.



The screenshot shows a "Static Route" configuration panel. It contains four input fields: "Network/Host" with "192.168.50.0", "Mask" with a dropdown menu showing "Default class C /24", "Gateway" with "192.168.1.254", and "Interface" with a dropdown menu showing "eth0". Below these fields is a "Save settings" button. At the bottom of the interface are "Back" and "Items" navigation buttons.

Figure 3.15: Basic Route Inclusion

Example: The following route makes that the traffic for net 192.168.254.0/24 it can be given with the mediation of host 10.0.0.254 by eth0 interface (see illustration 3.16).

Network/Host	Mask	Gateway	Device	Status
192.168.50.0	255.255.255.0	192.168.1.254	eth0	
172.16.20.0	255.255.0.0	192.168.1.253	eth0	








Page 1 of 1 Go to .. 2 record(s)

Back Add Edit Items Del

Figure 3.16: Listing of Routes

Advanced

The advanced routing makes only sense in an environment that possesses more than one internet link. In it, you have the power to choose a complete group of characteristics of traffic that will specifically be directed by one of registered gateways. Each rule can contain a priority list of gateways through where that traffic should be directed, being always used the first, with active status, as in illustration 3.17.

Pos	Description	Source Service	Source	Destination	Dest. Service	Schedule	Gateways	Status
1	HTTP Access	 Any	 localhost	 Any	 web		 eth0	

Page 1 of 1 Go to .. 1 record(s)

Back Add Edit Items Del

Figure 3.17: Rules list of Advanced Routing

The creation of these rules is very simple. Firstly, it would be more interesting if you'd already have in your mind what you need to do. If necessary, create a draw of the traffic before. After this, using the Advanced Routing Wizard, create the rules as you wish. The creation of these rules contains four steps as shown below:

- Step 1 Inform a description, position that rule will occupy in list and in your status (activate or inactive) according to following illustration 3.18 ahead.

Route Schedule Apply to Route by Advanced

Description: HTTP Access

Pos: 1

Status: Active

Back Items

Finish

Figure 3.18: Creating Rule - Step 1

- Step 2 Select the schedule in which that rule will be valid. The available schedules are defined in Objects > Schedules it conforms the following illustration 3.19 below.

Route Schedule Apply to Route by Advanced

Schedule: Any

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
SUN																									
MON																									
TUE																									
WED																									
THU																									
FRI																									
SAT																									

Back Items

Finish

Figure 3.19: Creating Rule - Step 2

- Step 3 In this step you will select the services and/or hosts that will have your traffic routed for a specific link.
 - In “Origin Filters - Hosts” selects for left box the Host(s) or Network(s) from where start the connections. In case you want to specify any origin, leave left box empty;
 - In “Origin Filters - Services” selects for left box the origin service(s). In case you want to specify any service, leave empty the left box;
 - In “Destiny Filters - Hosts” selects for left box the Host(s) or destiny Network(s) of the connection. In case you want to specify any destiny, leave empty the left box;

- In “Destiny Filters - Services” selects for left box the destiny service(s). In case you want to specify any service, leave empty the left box;
- Notice that through these options you’ll have all flexibility of specifying the traffic that you want to control, given by a certain origin and/or for a certain destiny.



Figure 3.20: Creating Rule - Step 3

- Step 4 The gateways can be selected in a priorities list, where which that is above, will be the first used. The following gateways will be used in agreement with established order measuring that the superior gateways fail.

Turn on the option **Case all the selected Gateways fail to direct for default route** it does with that Netion’s standard gateway is used in flaw case of all the selected exits. See following illustration 3.21 bellow.



Figure 3.21: Creating Rule - Step 4

- Advanced Settings

By default Nettion does the masks (NAT) of connections done by the hosts with private IPs destined for Internet (which come of your internal net, for instance). This section allows you to disable this function, for the case where you want literally to inform for Nettion not to mask the traffic (coming of the net DMZ with public IPs, for instance) or it allows the IP selection that will be used for the masks of each Gateway, as shown in the following illustration 3.22 ahead.

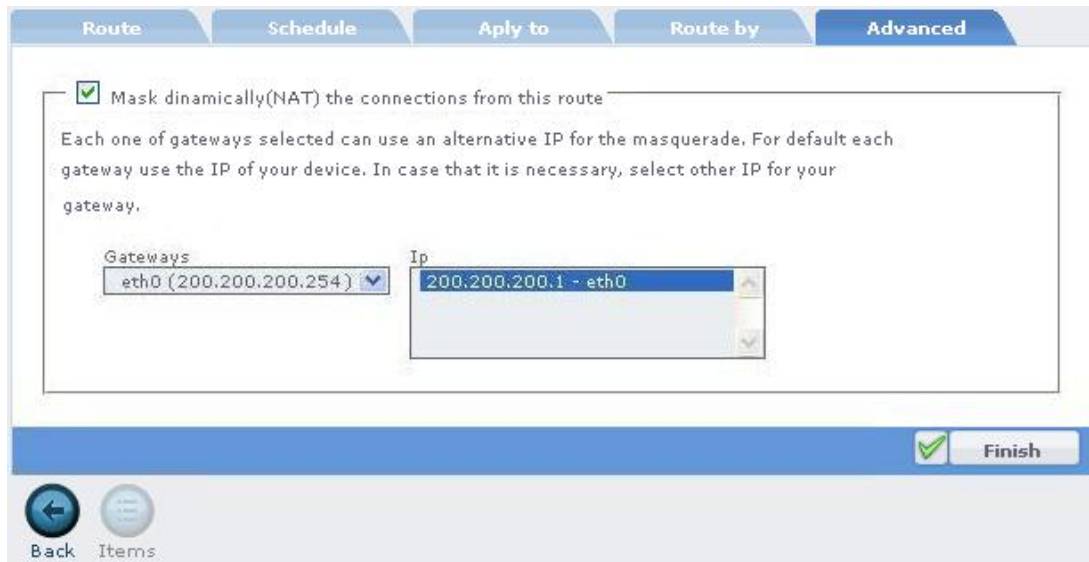


Figure 3.22: Creating Rule – Advanced Settings

3.2.6 Dynamic DNS

The services of Dynamic DNS are especially useful for Internet connections with dynamic IP address because they allow you to find your Nettion® starting from a name, as for instance, `nettion-mycompany.dyndns.org` and make connections, like VPN.

This service setting in Nettion guarantees the updating of DNS when there is change of interface IP address sort of ADSL or Ethernet with DHCP. With that, it will always be possible to access your Nettion® for configured **Host**.

To configure this service, you should be registered in one of the unpaid listed following Dynamic DNS services:

- No-IP (<http://www.no-ip.com>)
- DynDNS (<http://www.dyndns.com>)
- ChangeIP (<http://www.changeip.com>)

After the cadastre done in the service site you'll have information about "User", "password" and "host" that will serve as entrance for the Nettion Settings. To add a service, click in the button "Inclusion" and fill out the information below in agreement with the illustration 3.24 bellow.

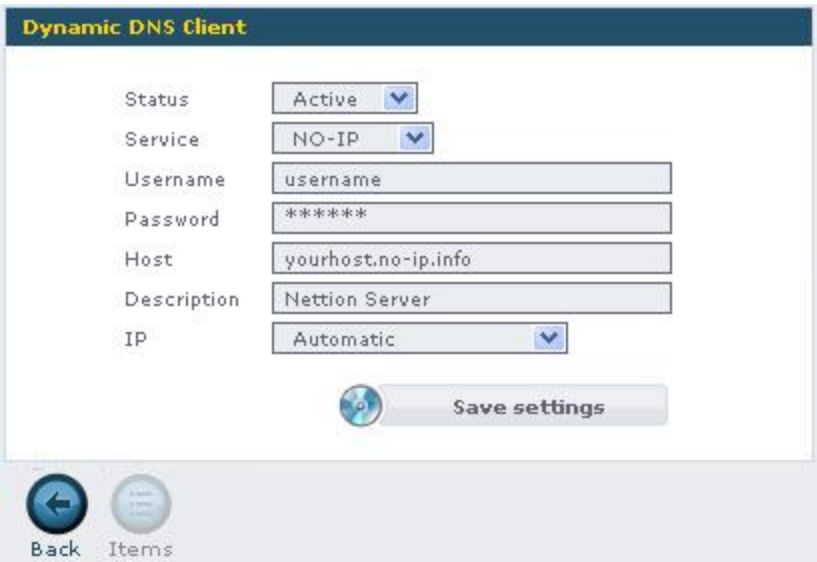


Figure 3.23: Inclusion Dynamic DNS services

The listing of illustration 3.24 (page 32) shows the example of a Dynamic DNS service configured in Nettton.

Service	Host	Description	Last IP	Last Update	Status	Action
NO-IP	yourhost.no-ip.info	Nettton Server	189.70.156.170	23/4/2008 21:34		Update

<<

<

Page 1 of 1

>

>>

Go to ..

1 record(s)

BackAddEditItemsDel

Figure 3.24: List of Dynamic DNS services

3.2.7 Graphics

Interfaces

In this section they are the graphs of band’s use by Nettton’s interface. Besides the on-line monitoring resource, you still have the option of consulting whole report of each graph. See example in following illustration 3.25 ahead.

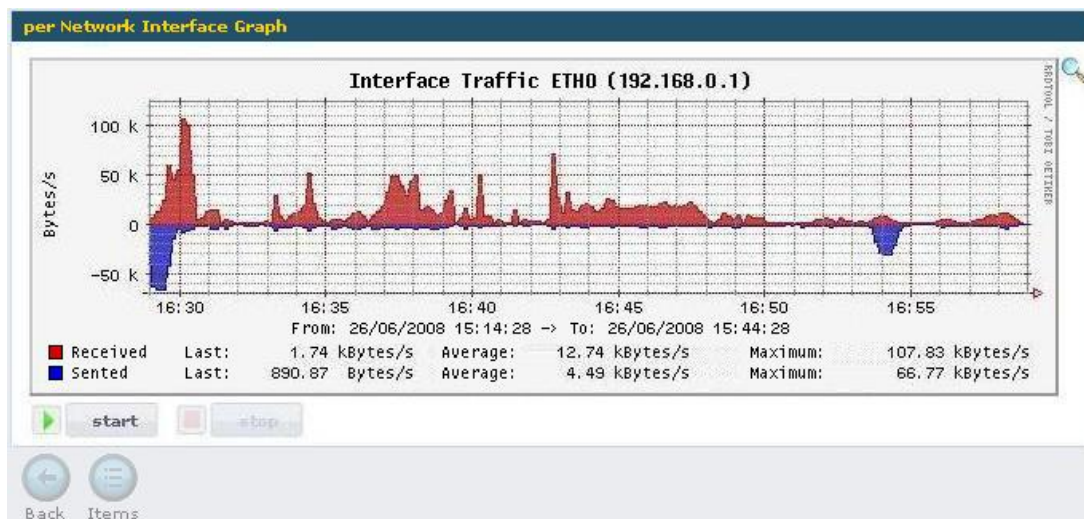


Figure 3.25: Band's Use Graphic by Network Interface

Chapter 4

Objects

With the intention of simplifying the way of configuring the services, Nettion® works with the concept of objects that consists on a group of information mapped in objects that will be used by the several services available by the software.

The objects are classified according of information's type that you store, facilitating your support. Ideal is that the administrator makes a previous evaluation of the network environment, identifying which objects should be created and saving time in the services setting.

We related some of Nettion® services available below and its respective objects for them used:

- Advanced Routing: hosts and nets, services and schedules;
- Proxy: domains, expressions, schedules, hosts and nets;
- Bandwidth Control: hosts and nets;
- Firewall: hosts and nets, services and schedules;
- NIDS: hosts and nets;
- OpenVPN: hosts and nets;
- DHCP: hosts and nets.

Observe this example:

To give reference to a company work station IP, an administrator created a host kind object with the name **PC_01**, attributing a certain IP 192.168.254.10 with NetMask 255.255.255.255. Soon after, he used the object PC_01 in the proxy rules, Bandwidth Control, Firewall and NIDS.

If, for some reason, you have to alter IP of **PC_01** it's enough to alter Object IP and all the Nettion's Settings that use this Object will be automatically updated for new IP.

4.1 Objects support

After selecting object's class (type) in the main menu, it will be exhibited for administrator a list containing the registered objects (in case they exist). The exhibition can be

ordered by any one of the shown columns, being only necessary that the administrator clicks on the specific column for the system to alternate the exhibition and ordination of list items. Use the scroll bar to navigate among the registered objects. The administrator will be able to, then, add, alter or exclude an object, for instance, clicking in the respective buttons.¹

4.1.1 Objects Inclusion

To add new objects, the administrator should click in the button “Inclusion” (see illustration 4.1 in page 36).



Figure 4.1: **Add** button

When clicking in the **Add** button, the inclusion screen will be exhibited, where you should fill out the object’s referring fields to be created. To confirm the inclusion, click in the **Save Settings** button.

4.1.2 Objects Edition

To access the edition module, the administrator should give a double click on the object that wants to edit or to select it and click in the **Edit** button (see illustration 4.2 in page 36).



Figure 4.2: **Edit** button

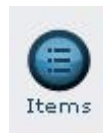
In the edition screen, the administrator can alter the cadastral data of selected object and confirm the alterations with a click in the **Save Settings** button.

4.1.3 Support Object Items

The objects Domains, Expressions, Schedules and Services are formed by groups of objects, in other words, each object contains your items. To have access to the items, select wanted object and click in the **Items** button (see illustration 4.3 in page 37).

Will be exhibited the list of cadastre items and its controls for cadastre maintenance of object items. The maintenance of used items follows the procedures default used for object maintenance (inclusion, edition and exclusion).

¹The buttons **Edit**, **Items** e **Delete** will just be enabled when there is a selected object.

Figure 4.3: **Items** button

4.1.4 Object Exclusion

To exclude a specific object, it's enough to select it and to click in the **Delete** button.

Figure 4.4: **Delete** button

The administrator can add more than one and delete all of them clicking only one time in the appropriate button. To select consecutive objects, maintain pressed the **Shift** key, click once in the object that will give start to selection and click a second time in the object that the conclude selection. A screen will be exhibited requesting the exclusion confirmation of selected object(s), to avoid that the administrator excludes one or more objects accidentally.

Note: System **won't** make the exclusion in case of object possess registered items or when it's associated with firewall rules, proxy or Bandwidth Control, etc, without before association is removed.

4.1.5 Object Search

To accomplish the consultation of an object, it's enough to access consultations guide in the cadastre of wanted object. Each object possesses your own consultation options, however all the screens follow the same operation pattern. The illustration 4.5 that follows, display the objects search screen "Hosts and Networks".

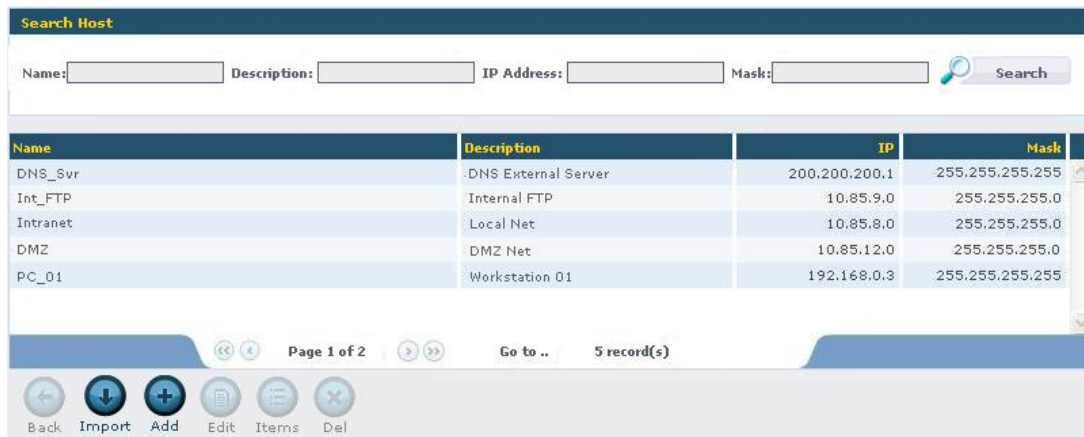
A screenshot of a web application interface titled "Search Host" in a dark blue header bar. Below the header, there is a search form with four input fields: "Name:", "Description:", "IP Address:", and "Mask:". To the right of these fields is a magnifying glass icon and a "Search" button.
Figure 4.5: **Objects search** screen

Note: Remember that the search screen follows the same operation pattern, just changing the fields in agreement with the selected object.

4.2 Hosts and Networks

In the network and hosts cadastre the administrator will create the IP's list that will be used in Nettion®'s Setting. We understand for host the IP of a specific machine, as well

as we understand net as an IP that represents an interval of IP's. Nettion® interprets as host the object of mask 255.255.255.255; the others, they will be interpreted as being nets. See the listing example of hosts objects and nets in the illustration 4.6 (page 38).



The screenshot shows a web interface titled "Search Host". It has search fields for Name, Description, IP Address, and Mask, with a "Search" button. Below is a table with 5 records. At the bottom, there are navigation buttons: Back, Import, Add, Edit, Items, and Del.

Name	Description	IP	Mask
DNS_Svr	:DNS External Server	200.200.200.1	255.255.255.255
Int_FTP	Internal FTP	10.85.9.0	255.255.255.0
Intranet	Local Net	10.85.8.0	255.255.255.0
DMZ	DMZ Net	10.85.12.0	255.255.255.0
PC_01	Workstation 01	192.168.0.3	255.255.255.255

Page 1 of 2 Go to .. 5 record(s)

Back Import Add Edit Items Del

Figure 4.6: Hosts and Networks

4.2.1 Support of Hosts and Networks Cadastre

The hosts and networks cadastre maintenance follow the established pattern previously (see section 4.1). For hosts and networks should be filled out the following fields (according to illustration 4.7 in page 38).

- Object: name to be given to object. Example: Web Server;
- IP Address: IP address of the host or net. Example: 192.168.1.2;
- Mask: mask of the net where is object. In case the object is a host, remember to use mask 255.255.255.255/32;
- Description: explanatory text on the object. Former: Company's Web Server.



The screenshot shows a form titled "Host or Network". It has fields for Object, IP Address, Mask, and Description. The Mask field has a dropdown menu showing "Host 255.255.255.255 /32". There is a "Save settings" button and "Back" and "Items" buttons at the bottom.

Figure 4.7: Adding a Host/Network Object

4.3 Domains

In the cadastre of domains, the administrator should create the list of the group domains that will be used in the Nettion's Setting. Each group can contain one or more domains.

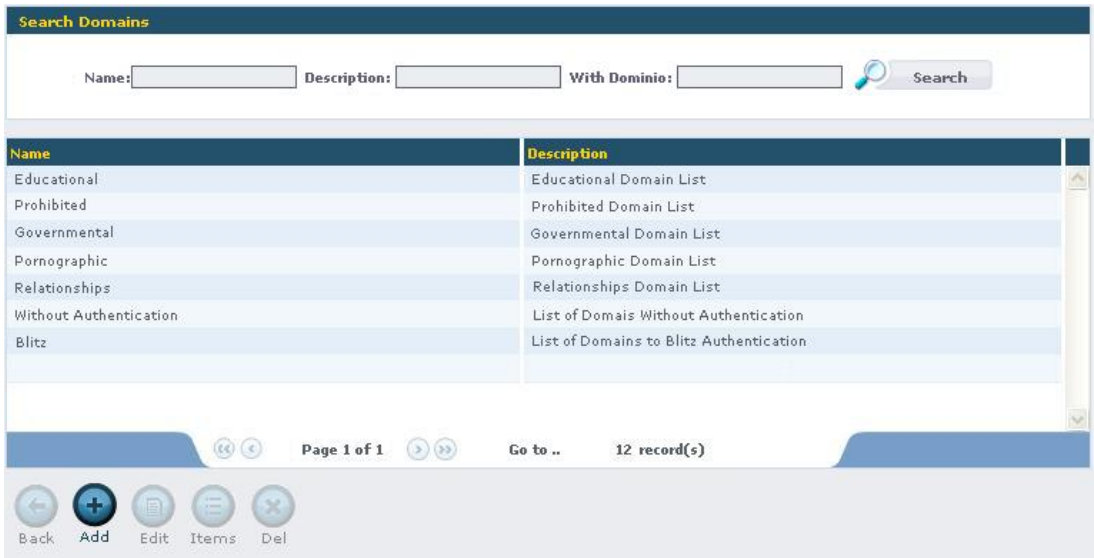


Figure 4.8: Domain Objects Listing

See a domain objects listing example in the illustration 4.8 in page 39.

4.3.1 Support of Domains Cadastre

The support of domains cadastre and of items follows the previously established default. For domains, the following fields should be filled out (see illustration 4.9 in page 39):

- Name: name that you want to give to the Former group: Government;
- Description: description concerning the group. Former: Government domains.



Figure 4.9: Setting Form of Domains Group

To add items of Domains Group, select wanted group and click in Items button. In the following screen you will find a screen with the listing of items of the domain. Click in the button "Inclusion" and fill out the information on the item:

- Domain: type the domain beginning for dot (".") to identify whole domain (example: .hotmail.com) or to identify a specific host that domain uses without the point (Example: login.hotmail.com).
- Description: description concerning the item. Example: Blocked domains.

4.4 Expressions

In this section, the administrator can register expression groups (words or regular expressions) for been used in proxy setting, and, as happens with domains, each group can contain one or more items, making possible use of whole group in one only proxy rule.

4.4.1 Support of Expressions Cadastre

The maintenance of expressions and items cadastre follow established previously pattern. For expressions some following fields should be filled out:

- Name: name that you want to give to group. Example: Forbidden Expressions;
- Description: description concerning the group. Example: Expressions that should be blocked.

To add items of Expressions Group, select the wanted group and click in the Items button. In following screen you'll find the items listing of expressions group. Click in the "Inclusion" button and fill out the information on item:

- Type: type of item to be created, if **Word** or **Regular Expression**².
- Word: word that should be identified in URL for Nettion's Proxy. Example: sex.
- Position: position in which the word should be identified. In case you want, for instance, identify URLs finished by ".exe", choose the "in the end" option.
- Complete Word: just select "Yes" to identify only the whole expression, in other words, it won't be identified when the word is contained in other words. For example of word sex, sexology would not hit the pattern. Select "No" to criticize the word even inside of other words. In that case, the sexology example will match with sex word.

4.5 Schedules

In schedules cadastre, should be created a list of schedules that will be used in Nettion's Setting. With those schedules, the administrator can create rules in Proxy, Firewall, etc, to do access control.

4.5.1 Support of Schedules Cadastre

The maintenance of schedules cadastre and of items follows a previously established pattern. For schedules, following fields should be filled out:

²Nettion makes possible the inclusion of more complex regular expressions through the choice of Regular Expression type, however, the choice of associated Word type to other options as "Position" and "whole expression" can assist great part of cases.

- Object: name to be given a schedule. Example: Expedient;
- Description: detailing schedule text. Example: Schedule of normal work.

4.5.2 Determining Intervals

The administrator can define schedule by selecting one or more cells of table composed by days and schedules. The selection will be made with mouse in the following way: the administrator should click in the initial cell with left mouse button, maintaining it pressed during the cursor displacement in the screen and selecting the wanted interval. Once selected the wanted area, click in “Mark” button. A same schedule object can have several schedule regions selected. In case you want to do an adjustment for division of hours, after selecting the wanted area, a line will be exhibited together with the fields for fittings with the buttons to **Mark** and **Unmark**. User can alter content of fields in agreement with your need and click in **Marking** or **Unmarking** according to the case. To confirm the interval definitions, the user should click in **Save Settings** button.

4.6 Services

In this section administrator can register services for further use on Nettion’s Setting functionalities. There is also one option of predefined services check. Nettion already possesses registered a series of services, the more acquaintances in Internet, which are the predefined services objects.

4.6.1 Predefined

On this option, the administrator can consult the predefined services list by Nettion®. When selecting a service, click in items button to visualize the ports that certain service uses.

4.6.2 Personalized

In case the wanted service isn’t registered in Nettion, the administrator can create personalized services and to do so, he should increase a new group of services, clicking in “Inclusion”. In the following screen, identify a name and description for your new Service.

To add items to a service, select the wanted service and click in “Items”. Each Service can contain one or more protocol/port combinations.

For each item of service the items below should be configured:

- Protocol: TCP, UDP, ICMP, GRE, ESP or HA;
- Port: It can be a number, a strip or a special P2P service;
- Description: it adds a description for the item;

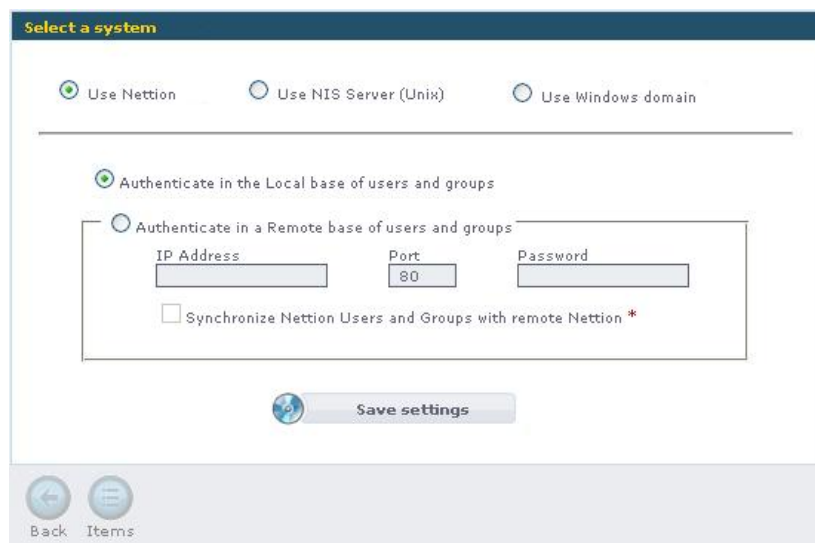
- To also add this service for the UDP protocol: Mark this option in case you want to insert this same port for UDP protocol (this option will only be available in case you are inserting a TCP service).

Chapter 5

User/Groups

5.1 Authentication

Nettion® possesses three alternatives in users' authentication. The first is to use a base of users' data that will be registered in own Nettion®; Second is to authenticate from a users base already existent in a UNIX/Linux machine, through NIS (Network Information System); and the third are through a users' base data registered in a server Windows. This option also supports the authentication through NTLM, that doesn't request login and password in the browser of Windows stations that make part of a Windows domain. This schema uses the login information of the Windows domain to authenticate in proxy.



The screenshot shows a web-based configuration interface titled "Select a system". It features three radio buttons at the top: "Use Nettion" (selected), "Use NIS Server (Unix)", and "Use Windows domain". Below these, there are two more radio buttons: "Authenticate in the Local base of users and groups" (selected) and "Authenticate in a Remote base of users and groups". The "Remote base" option is enclosed in a box and includes input fields for "IP Address", "Port" (with "80" entered), and "Password". Below these fields is a checkbox labeled "Synchronize Nettion Users and Groups with remote Nettion *". At the bottom of the form is a "Save settings" button. The interface also includes "Back" and "Items" navigation buttons at the very bottom.

Figure 5.1: User's Authentication

5.1.1 NIS Server

To use the **Server NIS (Unix)** option, fill out the fields:

- Domain NIS (Network Information System): domain where are the registered users in the Server. Example: NISGROUP
- Address IP: Server's IP Address. Example: 192.168.0.1

5.1.2 Windows Server

To use option **Windows Domain**, fill out the fields:

- Domain: domain where the users are registered in the Server. Example: corporation
- Server Name: Example: Serv-corp
- IP Address: Server's IP Address. Example: 10.0.0.2

Activate the settings clicking in **Save Settings** button.

Windows Server with Synchronization and NTLM

Operation of NTLM system This option does with that Netition negotiates with Server Windows the rehearsed authentication by the browser users, avoiding the need of identification (user's login and password) each times you use navigation. Remember that this option will only work in a network environment Windows/Samba where the machines and users are properly logged to domain.

NTLM in Netition Since the version 2.5, Netition® Security Software supports the NTLM authentication scheme, making transparent the authentication scheme of proxy to user.

To use this authentication scheme, it's necessary the setting of some referring fields to the Windows domain. Another important characteristic of this authentication scheme is the compulsory nature of the users' synchronization between Netition and controller domain.

Enabling NTLM authentication To enable the NTLM service, the administrator should enable the option "Synchronize Users and Groups of Netition with Users and Groups of Windows domain" and add the login and password of some user with administrator's level. In case server Windows is of AD type (Active Directory) activates the option **The Windows server possesses Active Directory service enabled**.

Therefore, it's enough to save the information so that Netition can connect itself with Domain Controller, synchronizing the users and authenticating through NTLM.

Important Observations:

1. The users have to be connected to the Windows domain to authenticate and navigate in Internet;
2. Should create an additional firewall rule to give access permission to Netition -> Domain Controlling Server using the predefined Services such as **smb**, **win2000** and **winnt**.
3. For authentication works, it's primordial that proxy rules exist. For more information see chapter 6 (Proxy).
4. For each alteration in users' information in the domain Controller, it's necessary to synchronize the users again in Netition®.
5. In some situations, Netition® can lose communication with the controller domain(In case of temporary shutting down of Domain Controller, for instance). In these cases, Netition® should be reconnected, to make authentications again.

IMPORTANT: When synchronizing the data with the domain controller, all the groups and users previously registered will be deleted. It's of extreme importance to do a settings backup before accomplishing this procedure.

Synchronization and reconnection There are two additional options in the NTLM settings:

- To synchronize Users and Groups

This option is to synchronize the Nettion® users again with the domain controller's users. It should be used whenever alterations are made in the users and domain controller's groups.

- Reconnecting to the Domain

This option is to reconnect Nettion to the controller domain in case the communication among them is lost (Example: server shutdown).

5.2 Groups

Nettion® allows administrator to create groups of users and to use it in the Proxy rules creation. This makes possible that the users from a group can be subjected to specific rules, controlling their Internet access.



Figure 5.2: Groups Management

5.2.1 Support for Groups Cadastre

We have two forms of working with users' groups, being divided in agreement with the authentication type chosen:

Case 1: remote base authentication by NIS or Windows without users' synchronization, or in Local base.

The group's maintenance cadastre proceeds like pattern previously established. For users' groups the following fields should be filled out (see illustration 5.3 below.)

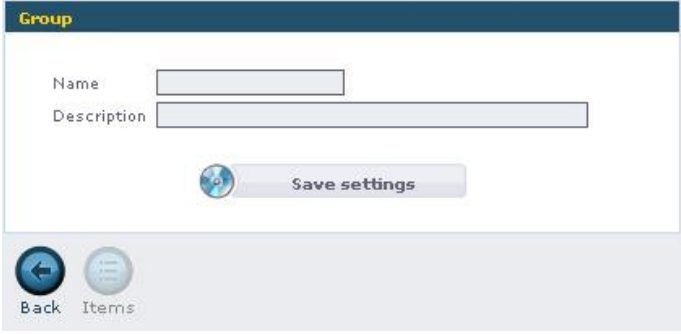


Figure 5.3: Inclusion/Edit Groups

- Name: name that you want to give to the group. Example: Financial
- Description: description on what refers this group. Example: Financial Section

Case 2: authentication with user's synchronization (by NIS or Windows).

In this case, administrator should edit the groups in Windows or NIS controller domain and synchronize the users' bases again in **authentication** option of **Users and Groups**. See the Windows Server item.

5.3 Users

We have two forms of working with users, being divided in agreement with the type of chosen authentication:

Case 1: authentication by NIS, or Windows without NTLM synchronization.

Nettion® allows you to register, independent of authentication's kind, the users that need of differentiated treatment on internet access, being able to administrator to attribute the user in one or more groups to facilitate the maintenance of proxy rules for these.

Case 2: Windows authentication with NTLM

In this case, the administrator should edit the users in the domain controller and synchronize users' bases again in the **Authentication** option of **Users and Groups** menu. See the Windows Server item.

5.3.1 Support for Users Cadastre

The users' cadastre maintenance proceeds like pattern previously established. For users' cadastre the following fields should be filled out (see illustration 5.4 bellow):

Edit users

User:

Name:

Password:

Confirm:

Group:

Extra groups:

Groups list:

Access Profile**:

**Access Profile to the System Management Interface

Figure 5.4: Inclusion/Edit Users

- User Field: user’s login. Example: John
- Name: user’s name. Example: John Simpson
- Password: password for access. Example: *****
- Confirmation: confirmation of the password. Example: *****
- Group: default group which user will be part of. Example: Commercial
- Additional groups: additional group which user will be part of. Example: Financial

5.4 Access Profiles

Starting from version 3.98, **Nettion®** Security Software starts to contain access profiles. To create access profiles and to attribute a profile to each user, access **Users/Groups > Access Profiles**.

Name	Description
System Manager	Total Access to System
Top Proxy	Access to Top Proxy Report
Firewall Manager	Access to Firewall Functionality

Page 1 of 1 Go to .. 3 record(s)

Figure 5.5: List of profiles

This functionality allows the Administrator to define which modules of the tool can be visualized in the users’ access menu in a certain profile. Handling is very simple, as displays the illustration 5.6 ahead.

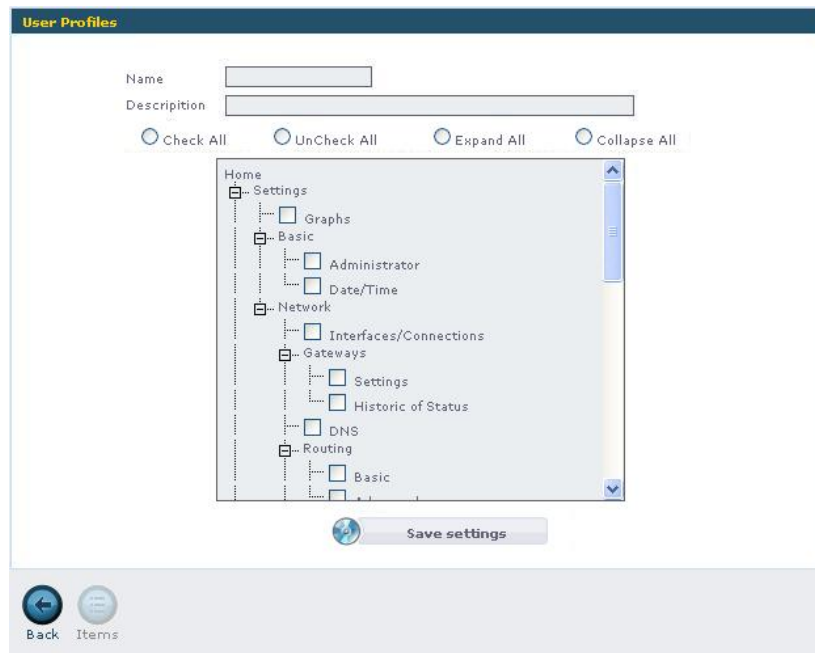


Figure 5.6: Selection of the Modules

After a profile creation, administrator should link it to users which apply. This link is made directly in user's cadastre. Will be attributed a standard profile automatically with limited access to users that aren't linked to a specific profile.

Chapter 6

Proxy

The Proxy service possesses two basic functions. The first is Cache, that makes possible an increase of the speed, when accessing pages in internet without, necessarily, to invest in larger links, because it optimizes the navigation making a local cache of objects (web) accessed by users. Allows that objects already accessed and still valid they're locally available to users which need that same object, avoiding link use for each access to the same site or file, for instance. Besides, Proxy also acts as a firewall in application level. This way, it's possible that administrator does users' accesses control through related rules: schedules, domains, words or regular expressions, user's groups or related to hosts and nets objects.

6.1 Necessary Firewall Rules

As any other service, Proxy needs that liberations are made in Firewall to work appropriately. The necessary rules are:

6.1.1 Intranet → Nettion

It's necessary to create a rule that allows that intern net users (and of nets that are also necessary) they can access Nettion in the services squid (port 3128) and DNS (port 53). See in table 6.1 a summary of the rule of Firewall (page 49).

Rule: Intranet → Nettion			
Source	Destiny	Destiny serv.	Action
Intranet	localhost	squid dns	Accept

Table 6.1: Firewall Liberation: Intranet -> Nettion

6.1.2 Nettion → Internet

It is also necessary allow Nettion to Internet access to look for sites. For that Nettion should access the default Web services (http, https and tomcat) and also the DNS service (resolution of names). See a summary of necessary rule in the table 6.2 in the page 50.

Rule: Nettion → Internet			
Source	Destiny	Destiny serv.	Action
localhost	Any	http https tomcat dns	Accept

Table 6.2: Firewall Liberation: Nettion -> Internet

6.2 Settings

Nettione® makes possible that works with a transparent proxy or with authentication. We will approach the two cases:

6.2.1 Proxy with Authentication

In proxy use with authentication, works with cache and access control, having the possibility of restrictions by user.

For proxy use with authentication it's necessary to configure it in each station browser.

6.2.2 Transparent Proxy

Transparent use of proxy just works with cache, with no restrictions possibility to users.

In Transparent Proxy case it's necessary that a Firewall additional rule is created. It will be responsible for traffic redirection in port 80 to Proxy port 3128 (object squid) by default.

Rule: Transparent Proxy			
Source	Destiny	Destiny serv.	Action
Intranet	Any	http	Redirect to localhost:3128

Table 6.3: Transparent Proxy Redirection

6.2.3 General Settings

To access the proxy general settings screen access: **Proxy > Settings > General Settings**. Follows a description of settings screen fields:

- Port: port in which will work Proxy service. Example: 3128 (default);
- Cache Size: Size of the cache in MB. Example: 1000;
- Main Memory Size: amount of RAM memory (in MB) that will be used to store frequently accessed objects. Example: 100; It can be made a 10% calculation of machine RAM memory for this setting in case Nettion it's also used as Firewall, VPN, E-mail, etc. In case Nettion is just used for Proxy purpose, we can get larger values, as 60 to 70% of the available RAM. The objects storage in RAM memory

accelerates the navigation due to larger access speed compared to the hard disk access;

- Maximum object size in disk: until which size (in MB) an object is stored in cache. Example: 64;
- Default policy: standard politics to be used. Example: To deny any access. The ideal pattern is to deny access and that you create rules liberating what is necessary;
- Error messages: determines in which language the error messages will appear to users;
- Basic Authentication Processes: determines how many processes Nettion® should maintain open to make users' authentication. Varies in agreement with people's number that will access Internet simultaneously;
- NTLM Authentication Processes: determines how many NTLM authentications processes Nettion® should maintain open to accomplish the users' authentication. This number varies with the proxy users' amount through NTLM authentication. The default is 20 processes, however, in some networks with many users and many simultaneous authentications, can be necessary to increase this number;
- Company (for the error messages): Allows specifying the company's name, which will be exhibited in proxy error messages.

The illustration 6.1 displays an example of Proxy Settings.

Setting	Value
Port	3128
Cache size	1024 Mb
Main Memory Size	64 Mb
Maximum object size in disk	8 Mb
Default policy	Deny any access
Transparent proxy	No
Error messages	English
Basic Authentication Processes	20
NTLM Authentication Processes	20
Company (for the error messages)	Your Company Inc.

Figure 6.1: Proxy Settings

6.2.4 Error Messages

In Nettion®, all Proxy error messages can be edited, allowing setting flexibility. To edit Proxy messages access: **Proxy > Settings > Error Messages**. The Illustration 6.2 exhibits the Proxy error messages screen.

Error	Portuguese Message	English Message
err_access_denied	Acesso negado	Access denied
err_cache_access_denied	Acesso negado	Access denied
err_cache_mgr_access_denied	Acesso negado	Access denied
err_cannot_forward	A requisição não pôde ser encaminhada para o servidor de origem	Unable to forward the request at this time.
err_connect_fail	Falha na conexão	Connection Failed
err_dns_fail	Falha na resolução de DNS	DNS Failed
err_dom_denied	Domínio não permitido	Access denied to this domain
err_exp_denied	Url contém palavra ou expressão não permitida	URL contains forbidden word or expression
err_forwarding_denied	Forwarding negado pelo cache	Forwarding Denied
err_invalid_req	Requisição inválida	Invalid Request

Figure 6.2: Listing of Proxy error messages

To edit a message, select it and click in “Edit” button. In the screen that will be exhibited, alter the message content according to your need; however without leave message’s real reason. Notice that the message should also be transcribed in the English language. To finish, click in **Save Settings** button, as display the illustration 6.3 bellow.

err_dns_fail

Portuguese Message

Falha na resolução de DNS

English Message

DNS Failed

Save settings

Figure 6.3: Edition of Proxy Error Messages

6.3 Rules

The proxy rules can be interpreted as sentences (see illustration 6.4), it’s of administrator’s responsibility to build those that should be applied in access control. For rules formation, previously registered information is used. See reference in Chapter 4 (Objects) and in Chapter 5 (Users and Groups).

The administrator should elaborate the administration rules of access.

Pos	Description	Schedule	Apply to	Status
1	Allow domains NoAuthentication			
2	Allow domains Governmental			
3	Allow domains MSN			
4	Allow any domain with MSN			
5	Deny any domain with Downloads			
6	Deny domains Pornographics			
7	Deny any domain with Pornography			
8	Allow domains Prohibited			
9	Allow any domain			

Page 1 of 1 Go to ... 9 record(s)

Back Add Edit Items Del

Figure 6.4: Listing of Proxy rules

6.4 Composition of Proxy Rules

The Proxy rules creation/edition is made through a Wizard that will guide you in access filters composition. Each rule allows application of filters by domain, regular expressions, schedule and IP that are applied to Users and/or Users' Groups. The rules are analyzed one by one in agreement with its position, beginning by rule number 1, settling down a priority order. This way, it's important that most specific rules are above the most generic rules.

6.4.1 Screen 1 – Rule Definition

- Action: action of the rule, Allow or Deny.
- Domains: indicate “Any” in case you doesn't want to restrict by domain in this rule or indicate “Belong to group” and select an object of domains to apply the rule to the domains of the group or, still, Not indicate “belonging to the group” and select an object of domains to apply the rule to domains that are not part of selected group.
- Filter: use here same logic applied to domains, applied this time to objects of Expressions;
- Position: position of rule in table. Determine priority of rules interpretation;
- Status: rule status. Indicates if a rule is Active or Inactive. Options: **Activate** or **Inactive**

Important: In case you select domain filter and expression filter in a same rule, Netition will apply the rule **only if** URL accessed satisfies demands of domain and expressions filters of selected groups (logic “and”). The criterion for positioning the rules will vary in agreement with implemented safety's politics. We suggest, however, some concepts that can be observed in that way. Permission rules that don't request authentication should be in first positions.

Figure 6.5: Rule Definition

RULES

1. Allow the domains without authentication of commercial schedule for any user.
2. Permission rules that request **selected users**' authentication should be positioned below the rules that don't request authentication. Example: Allow any domain in any schedule for users of Management group.
3. Permission rules that request authentication for **valid users** should be positioned below the referring rules to "selected users". Example: Allow any domain, without forbidden words in any schedule, for valid users.
4. Rule regarding standard politics selected in proxy settings will be implicit and it will be written after the last rule registered by user. Like this, the standard politics will only be interpreted by proxy case requested access doesn't fit in none of previous rules.

6.4.2 Screen 2 – Schedule

It determines schedule for action. Defines the schedule in which the rule will act with base in one schedule previously registered.

Options: "Any", "Inside of the schedule" or "Out of the schedule". The "Any" pattern will be used when administrator doesn't specify a relation schedule during rule elaboration. To specify a relation schedule, the administrator should select an different option from "Any" so that registered schedules list is exhibited and which of those will select the wanted schedule, that will be exhibited in yellow, in other words, the schedule in which rule will act.

See schedules selection screen in the illustration 6.6 ahead.



Figure 6.6: Schedule Selection for Rule Application

6.4.3 Screen 3 – Apply for:

To conclude, determine for who the rule should be applied.

- **Host/Network:** host or net definition that will be treated by this rule, with base in host/network previously registered. Options: **Any**, **Equal to** ou **Different from**. The **Any** pattern will be used when administrator doesn't specify a relationship with host/network during rule elaboration. To specify a relation with host/network, the administrator should select an option different from "Any" so that registered hosts/nets list in which administrator will choose the wanted host/network.
- **Groups/Users:** The users' that will be treated by this rule considering groups and users previously registered or synchronized with an external base. Options:
 - **Any** - the rule will be applied any user, authenticated or not;
 - **Valid users** - the rule will only be applied to valid users, in other words, authenticated users. For that, if user has not still been authenticated, Proxy will request it¹;
 - **Only selected** - the rule will be applied to authenticated users that be selected in Groups and Users boxes. Therefore, choosing this option the selection boxes will be qualified. Select for the left box the Groups and/or Users wanted.

Observation: To optimize users' and groups time load Netition carries only first 100 registrations of each selection box. On list's end possesses an option called "more...". Click twice in it and will open 100 next registers. Case you prefers, you will also be able to use search field that is above the boxes.

¹In case Netition® to be using the NTLM Integrated Authentication, the authentication has already been negotiated and the authentication box will not appear asking for it again.

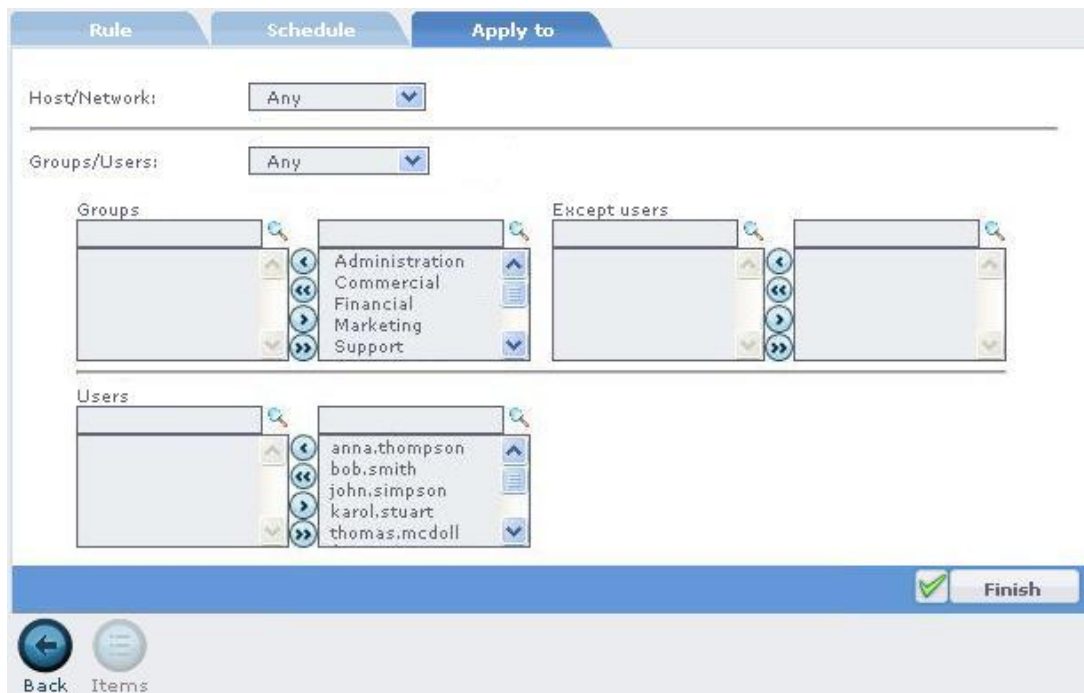


Figure 6.7: Objects Selection (Users/Hosts) of the Rule

6.5 Reports

Nettion® turn available to administrator referring managerial reports to accesses through Proxy. When authentications are used, it's possible to administrator filter the referring accesses to each user.

6.5.1 Default

This report makes possible to Nettion administrator to generate analytic reports of accessed sites, specific in a certain period. In case fields are not filled out, the report will be general.

The fields for composition of reports are:

- **User:** selects on which user the report will be demonstrated. Example: Sophia. Will bring all accomplished accesses by user Sophia on specified period in fields SINCE (DATE) and TO (DATE).
- **Host:** Specifies of which machine broke internet access. Example: 10.0.0.36. It will bring all accomplished accesses starting from the machine 10.0.0.36 in the specified period.
- **URL:** complete address or space of an address that are wanted to know who accessed it in the specified period. Example: www.nettion.com.br. Will bring a list with all users that accessed to this site: www.nettion.com.br. Example: Nettion. Will bring a list with all users that accessed some site (URL) that contains “Nettion” word.

6.5.2 By Domain

This report makes possible to Nettion® administrator generate access reports in a certain period grouped by domains, according to fields SINCE (DATE) and TO (DATE). Administrator can select a specific group for which the report will be exhibited or just specify one user.

- Clicking in “hits” column, the administrator will visualize detailed report regarding the domain.
- Group: Specifies on which group the report will be demonstrated. Example: Development. Will exhibit all accesses accomplished by the development group in specified period in fields SINCE (DATE) and TO (DATE).
- User: To specify on which user report will be demonstrated. Example: Sophia. Will exhibit all accesses accomplished by Sophia in specified period in fields SINCE (DATE) and TO (DATE).

6.5.3 Top

This report makes possible to Nettion® administrator to identify which were the Top accesses through three different reports. By User, Domain or Host. Top Users still allows the selection of three measure units, could be for Traffic (amount of bytes transferred), by Hits (amount of done accesses – each item of a site represents a hit) or for access time (it considers the sites’ load time / web files, in other words, the time that user really used Proxy).

6.5.4 Blocked Accesses

This report makes possible that Nettion®’s administrator generates analytic reports of accessed sites and that they are blocked for respective user in a certain period, for simple identification of unauthorized attempt access. Case the fields are not filled out, the report will be general.

6.5.5 On-line

This report makes possible that Nettion’s administrator makes online accompaniment of sites that are being accessed. To begin accompaniment, the administrator should click in the button “Start” and to interrupt should click the button “Stop”.

6.6 Graphics

Besides the reports, Nettion also make available graphic in *real time* of users’ accesses or net hosts. Through them administrator will graphically be able to analyze the accesses of all or of a specific user inside of a chosen period. Two options of graphs are available, could be by user or host.

To have access to Graphics, access the menu Proxy -> Graphics -> Users or Hosts. The graphics are initially loaded with all users' data or hosts, according to example in illustration 6.8.

Use selection in graphic's upper part, to visualize a user's graph or specific host.

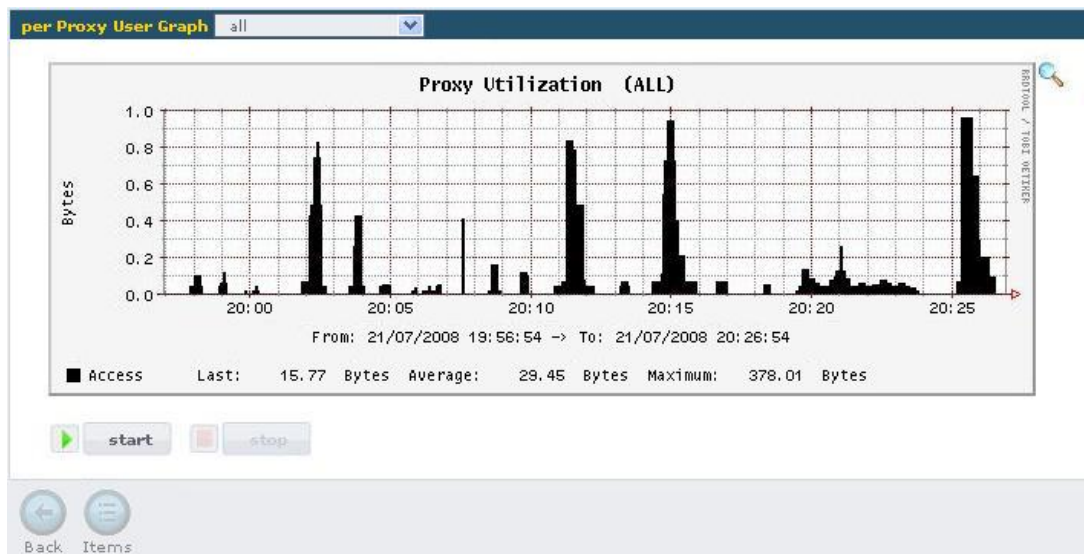


Figure 6.8: Users' Graph

6.6.1 Selecting a Period

To select a specific period for graphic visualization, click in magnifying glass that is in the superior right part of the graph. In next screen you will have two selection options of the period. The first of them is through the selection box in graphics base that allows the selection of the periods of 30 minutes to 1 year. The second option is using the mouse. Click with left button in a graphics' position and drag, making an area selection. After that, the graph will be recharged with selected period.

6.6.2 Visualizing Accesses Starting from the Graph

It is also possible to visualize the user's accesses starting from a selected graph area. For that, after selecting a period, click on icon that's in superior right part of graph.

6.6.3 Realtime Monitoring

Once selected wanted user, click "Monitor" button to accompany graphics' formation as long user makes accesses. To stop the monitoring, click in "Stop" button.

6.7 Configuring Net Stations

So that net stations use Nettion's Proxy (in way **non** transparent) it is necessary that Proxy Settings of your navigators are pointing for IP and port of Nettion. This setting

can vary in agreement with the used navigator. We listed the necessary setting below in more popular and used:

- Firefox (version 2.0)
 - With the navigator open, click in menu “Tools → Options...”;
 - In the following screen, click in “Advanced” option;
 - Now click in the brim “Net” and later in the button “Settings...”;
 - In the following screen, select the “Proxy Manual Setting” option and fill out the HTTP information with Nettion’s IP access and the Proxy port, by default is port 3128;
 - In this same screen, in “Without Proxy for” option: also indicates Nettion’s IP
 - that will avoid that accesses to Nettion are made through Proxy;
 - Later click in “OK” and the navigator will be configured.
- Internet Explorer (version 7.0)
 - With the open navigator, click in the menu “Tools → Internet Options...”;
 - Click in the brim “Connections” and later in “LAN Setting” button;
 - In the following screen, select option “Use a Proxy Server...” and indicate IP and access port to Nettion. Default Nettion’s port is 3128;
 - In Advanced Options, type Nettion’s IP in Exceptions to avoid that access to own Nettion is made through proxy;
 - Click in “OK” and the navigator will be configured.

Chapter 7

Bandwidth Control

The Nettion®'s band administration has objective of optimizing the links use through Reprioritizing packages of data. With it is possible to allocate a larger band amount of link for services or more important machines of your net. Besides, the control has flexibility of doing the allocation in a dynamic way, what allows that not used band and allocated band can be consumed by another service in an automatic way.

To make clear the Bandwidth Control concept, its necessary we understand packages reprioritization concepts and of Dynamic Band Redistribution.

7.1 Reprioritizing packages

Reprioritization acts on packages delivery, making a decrease of packages delivery speed or making a larger liberation of band according with established rules. For instance, imagine that you are receiving your e-mails of an external provider of your organization. See illustration 7.1 ahead.

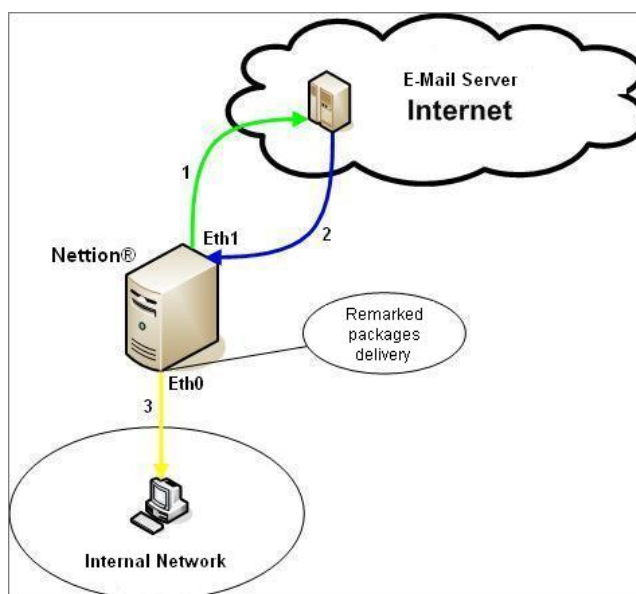


Figure 7.1: Scenery Controls Band

The line 1 (green) of image indicates the sense of your solicitation to the provider in port 110 (POP3 account) and the line 2 (blue) indicates the data packages (your e-mails) leaving the server of E-mails and going in machine direction. Arriving to Nettion, that makes connection intermediation they will enter for the net interface Eth1, and they will leave in direction your machine, line 3 (yellow), through the interface Eth0. At the delivery time, Nettion will make packages reprioritization, restricting or liberating more bands for connection.

What if we wanted for this scenery, for instance, restrict the band for e-mails obtaining, we would apply a rule in Eth0 interface (interface of delivery of the data), restricting traffic originated in port 110 destined for internal net or some specific machine. We will see more creation rules.

7.2 Dynamic Band Redistribution

Second concept, not less important, it's of dynamic band redistribution. It will allow that an allocated band for certain service or host/network it is consumed by other service, when idle.

To be clear, imagine a situation where you allocated a part of your band (300Kbits) for a certain host of your net, however, you want that, when idle, this band is distributed for other net machines. For that, we use minimum speed and maximum speed concept, where the minimum speed will be what it will be reserved, in other words, it won't be shared, and maximum speed, will be band that can be used in case idle band exists.

This whole control is made through Classes, which represent band reservations, and its Rules. In next section you will learn how classes' settings and rules are made.

7.3 Settings

To configure Nettion® Bandwidth Control, you should access menu **Bandwidth Control > Settings**. In screen that will be exhibited, they will be available all existent net interfaces of system, as display illustration 7.2 bellow.

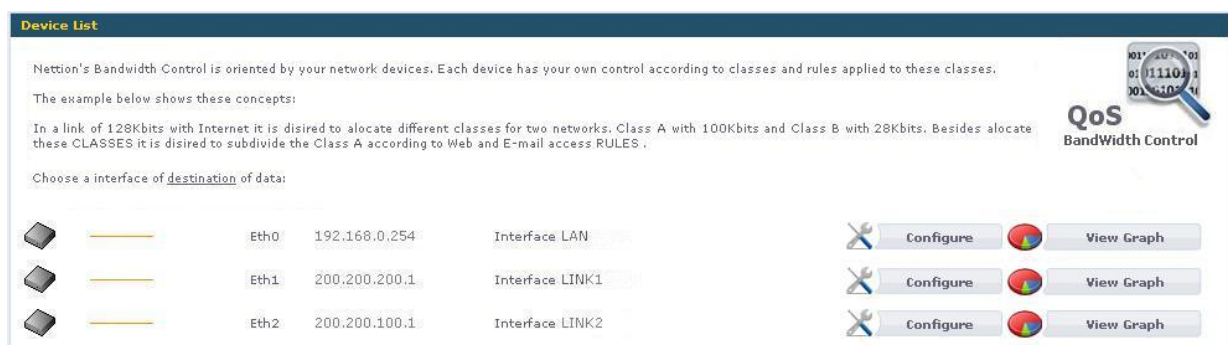


Figure 7.2: List of available net interfaces

7.3.1 Network Interface Definition

Before beginning Bandwidth Control Setting, it's necessary that you make scenery's evaluation and indicate origin and destiny of **data** that should be controlled. After identifying from where data starts and where it goes, you will identify in which interface control will be made, which is that makes data delivery directly to who requested them.

7.3.2 Classes

The first step will be to do a class creation, which means to create a band reservation of your link. At this time still we won't say to who (host or service) this reservation is destined. That will be made in rules creation.

Besides classes created by Nettion's administrator, also exists *default class concept*. The *default class* represents remaining of available band in net device, in other words, that was not still allocated in any class and that will be used by any traffic that has not been classified in any rule. The device's total band is defined in net interface setting, in menu Settings -> Net -> Interfaces.

We'll use the presented scenery, of E-mails delivery, for that concept is clearer. Imagine on that environment, we have a band of 1Mbit with internet and our need is to restrict band of e-mails download, preventing that this traffic disturbs other services.

Once defined net interface (see section 7.3.1), the next step is to do class creation in agreement with steps to proceed:

1. Click in menu Bandwidth Control -> Settings;
2. Click in button "Configure" of defined interface in section 7.3.1;
3. Next screen will show a Classes listing. Click in "Inclusion" button;
4. Fill out the fields:
 - Name: Name of Class. Example: Class 1;
 - Description: Description of Class. Example: Class 1;
 - Min. Vel.: insert reserved band for this class. For our example it will be of 1 Mbit;
 - Max. Vel.: insert maximum band allowed for the class. For our example it will be of 1 Mbit;
5. Click in "Save Settings" button.

give an idea of your current setting, Nettion offers a graphic that shows Interface and its Classes and Objects divisions. To visualize it:

1. Click in menu Bandwidth Control -> Settings;
2. Click in "Visualize Graphic" button of wanted interface.

Observing the image, the orange circle represents net Interface, the blue circles represents the classes. Positioning mouse on circles you will have larger information about your band settings, as shown in illustration 7.3 bellow.

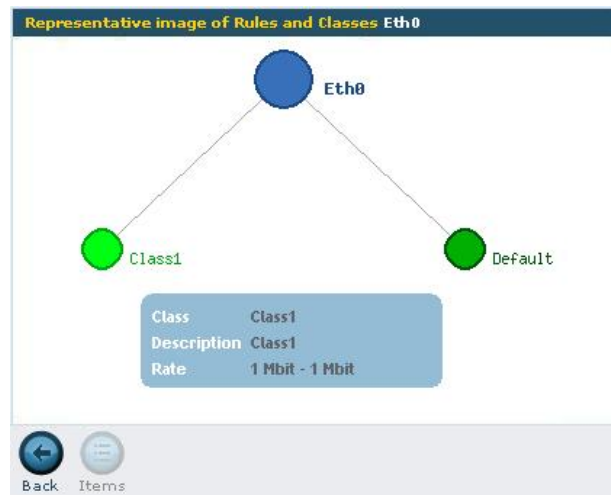


Figure 7.3: Interface Eth0 Graphic

Once Class is created, next step will be to create rules, as we will see in the next section.

7.3.3 Rules

The rules, which will always be linked to a class, will identify traffic to which control will be applied. On it we will indicate origin (from where they data start), the destiny (where data arrive) and minimum and maximum bands. The minimum band (reserve) and band maximum concepts are equivalent to seen in Classes.

Following our example, supposing that limit to be established for traffic comes from Internet (any origin) in port 110 with net intern machines destiny is 100Kbits. Follow steps to proceed for rule creation:

- Click in menu Bandwidth Control -> Settings;
- Click in “Configure” button of Eth0 interface;
- Select “Class 1” class and click in “Items” button;
- In following screen, of rules listing, click in “Inclusion” button;
- Insert rule information now. See illustration 7.4 (page 65).
 - Name: rule name. Example: POP3. Note: Is not allowed spaces in rule name;
 - Description: Insert a description. Example: POP3 Band;
 - Object of Origin: insert object from where data start. In this case selects the Any object, meaning any origin host;
 - Object of Destiny: insert destiny’s object of data. In this case selects object Internal Net, previously created;
 - Port of Origin: insert origin port of data. In this case inserts 110;
 - Port of Destiny: insert destiny port of data. In this case selects “Any” clicking in side box;
 - Minimum Speed: insert reserved band. In this case inserts 100 Kbits;
 - Maximum Speed: insert allowed maximum band. This field defines until how many of idle band can be used for this rule. In this case, as we want to restrict it inserts value 100 Kbits;

- Priority: defines the priority of this rule in relation to others. In this example it selects value 1.

Figure 7.4: POP3 Rule

Again, access Eth0 Interface graphic to visualize how Bandwidth Control is being applied. Observe that now a white circle appeared representing the created rule. See in the illustration 7.5 (page 65).

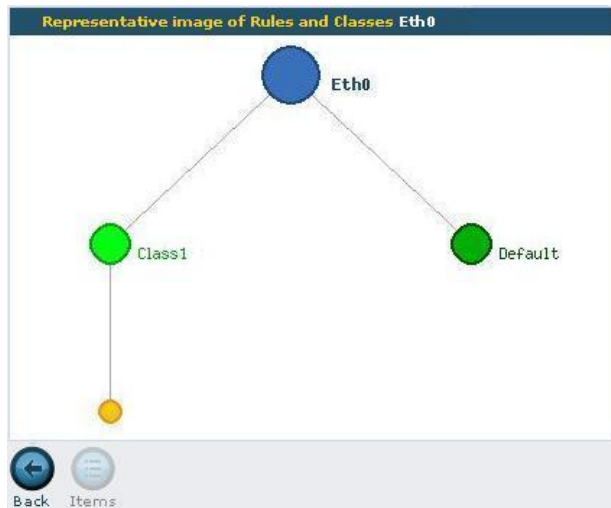


Figure 7.5: Eth0 Interface New Graphic

7.4 Activating Bandwidth Control Service

After these Settings, it is necessary that service is activated. For that, click in menu **System > Services**. Then click in “Start” button regarding the Bandwidth Control service.

To activate automatically the service when Netion starts, mark the option “Auto” of service and click in “Activate changes for selected” button them accordingly illustration 7.6 bellow.



Figure 7.6: Activation of Bandwidth Control Service

Chapter 8

Firewall

Firewall is a resource of safety that makes control of what is allowed or not to pass through Nettion®, for instance, between your net and internet. It works as a filter, avoiding that improper services are accessed, reducing the risks of exhibition of your network on internet.

The simple fact of having a Firewall in local net doesn't mean that he is being useful. For that, is necessary that it is well configured and tuned in with the safety politics needs of your organization.

Nettion® uses advanced technologies of Firewall available for Linux operating system through IPTables and Kernel 2.6, and, ally to that, also offers a quite simple interface of inclusion and rules maintenance, avoiding that in little time, administrator already gets lost with so many rules maid.

8.1 Settings

In **Firewall > Settings**, administrator will define standard access politics that will be used by Nettion's firewall. The standard politics establishes actions that will be taken on any access that has not been liberated by administrator through rules. The ideal is that standard politics is configured "Deny everything". Attention however. Before doing this setting, some basic rules should be created, as ones that they liberate the Nettion own access.

The standard politics access can be:

- **Drop All**, obstructing any access not liberated in rules;
- **Accept All**, obstructing only what was defined in rules. Originally politics is defined as **Accept All**, so that user has access to Nettion and can register the necessary rules to your accesses. Only after making that process, and that you should alter the standard politics to **Drop All**:



Figure 8.1: Firewall Standard Politics Setting

8.2 Rules

Each package¹ that traffics through Nettion® is analyzed by packages filter that opens and extracts information like origin IP, package destiny, ports, etc., verifying if these information hit with some registered rule in firewall. In case yes, the firewall takes the action that rule says (blocks, accepts or audits). In case there is not a specific rule in firewall that treats this package, the standard politics will be used defined in Nettion's firewall, which can be **Accept All** or **Drop All**.

8.2.1 Including a New Rule

So that user can add rules on Nettion® firewall, is necessary that objects that will be used are previously registered. It's recommended that plans a rules sketch of which will be registered. Nettion already makes available great majority of services that you will need in firewall setting, but you also have option to add new ones, in case it's necessary. To make a rule inclusion, click in the **Inclusion** button, in the menu **Firewall > Rules**, and fill out the requested fields:

Basic Rule definitions

- **Description:** description of rule, for instance: Access VNC to Machine01;
- **Action:** indicates actions that firewall will take on packages treated by this rule, which can be:
 - **Allow** - Liberates traffic;
 - **Deny** - Blocks traffic;
 - **Log** - Generates registrations on treated connections by rule. It is especially useful when you want to discover the ports used by a certain service. The whole traffic audited can be seen through the Firewall Report.
- **Pos:** Position in rules list. The rules are processed in sequential order and that order is important, because once a package is embraced by a rule, the action of this is taken and it are not more processed by following rules²;

¹The data in a IP net are sent in blocks referred as packages or datagrams (the terms are basically synonymous in IP, being used for data, in different places in IP layers)

²In case some package is treated by a rule whose action is to Audit, it continues until that is treated by some other rule to Allow or Deny or for standard politics.

- Status: Defines rule status as active or inactive.

Rule Schedule Apply to Advanced

Description: VNC Access to PC01

Action: Accept

Pos: 1

Status: Active

Finish

Back Items

Figure 8.2: Basic Definitions of Firewall Rule

After filling out that form, click in Next and choose the schedules in which this rule should act, as shown in illustration 8.2 above:

Schedules

If you want a rule to act always, choose **Any** (default option). You can also use objects of “schedule” type to determine when rule should act. Defined when rule should act, click in Next and you will configure the rule properly said.

Rule Schedule Apply to Advanced

Schedule: Any

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
SUN																									
MON																									
TUE																									
WED																									
THU																									
FRI																									
SAT																									

Finish

Back Items

Figure 8.3: Schedule Definition of Rule Application

Objects Selection for Rule Application

In “**Source Filters > Hosts**”, you will define starting from which host(s) or net(s) the connection will begin. To do selection, mark the selection box’s wanted objects on right

(objects list of Hosts and Nets previously cadastre), transferring them for left box. The transfer can be made by clicking twice in wanted object or using controls between the boxes.

To specify that doesn't matter the packages origin, in other words, of any origin Host/Network, leave left selection box empty.

To specify that is Nettion, use special object called "localhost".

TIP: In case you are using Mozilla Firefox Browser, it is possible to obtain larger objects information during rule creation. For that, it is enough to position mouse on wanted object, as shown in illustration 8.4.

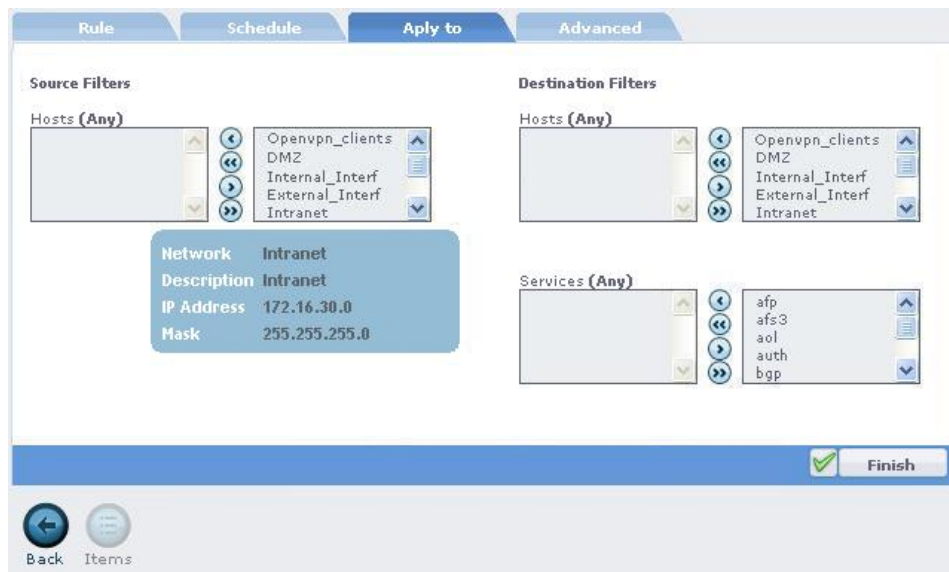


Figure 8.4: Objects Information

In “**Destination Filters > Hosts**” you will select destiny hosts or networks of connection, in other words, those that will receive the connection.

To specify that it does not matter the packages' destinies leave the left selection box empty.

To specify that is Nettion, use special object called "localhost".

In “**Destination Filters > Services**” you will select which service(s) will be accessed in connection's destiny. For default Nettion offers a list of services previously defined with principal services, but you can create your own in menu **Objects > Services > Personalized**.

See the illustration ahead.

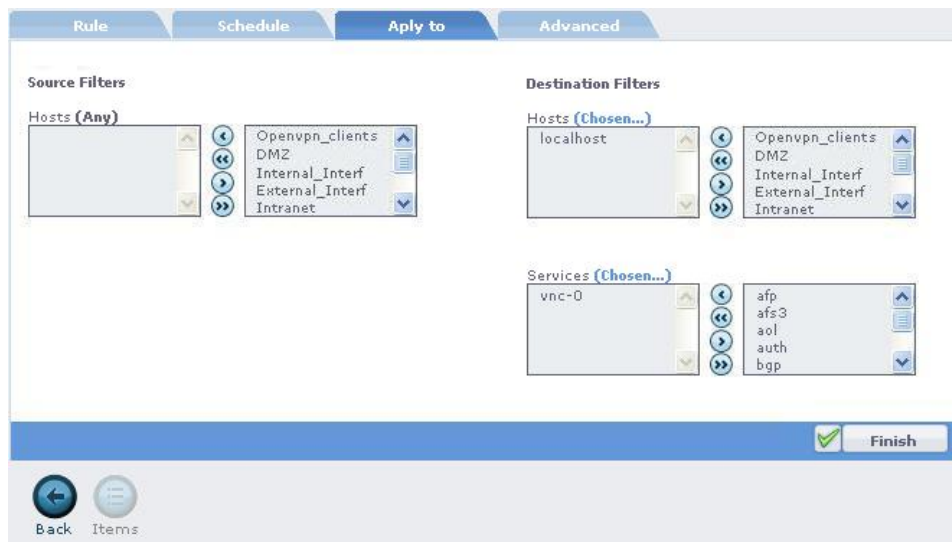


Figure 8.5: Objects Selection for Rule Application

Advanced Settings

In case you are making a packages redirection rule or want to apply other settings to rule, before “Finish” click in “Advanced” button.

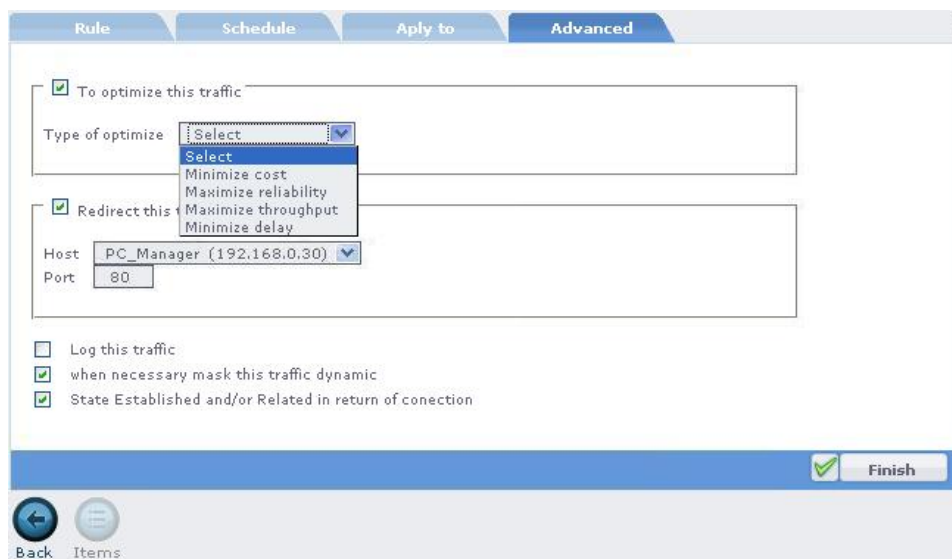


Figure 8.6: Rule's Advanced Settings

In this section, you will be able to:

- **To optimize this traffic:** This option allows that traffic treated by this rule is optimized. The optimization is made through special packages header setting (TOS - *Type of Service*) that has the function of specifying one of following settings:
 - Minimize cost
 - Maximize reliability
 - Maximize throughput

– Minimize delay

- **Redirect this traffic for other host:** use this option when you are creating a redirection packages rule, for instance, redirecting VNC connections that arrive to Nettion for a specific host of your net. Important observation: In case your intention is to do redirection services that arrive to Nettion for another host, without altering destiny Ports, leave the Port field empty. In case not, indicate number of a different port.
- **Log this traffic:** Allows that traffic treated by this rule it is logged. That will do that Nettion generates Logs registrations of connections that can be accessed through Firewall Reports.
- **When necessary mask this traffic dynamic:** this option does with that Nettion applies NAT (*Network Address Translation*) in packages treated by this rule, when necessary. That happens, for instance, when a host of local net, with a private IP, needs to access a service directly in Internet.
- **State established and/or Related in return of connection:** This option allows treat the connection state (*Stateful Firewall*). When marked, it will allow only origin hosts to begin connection in direction to destination hosts of rule. When there is need to leave that both sides (Source and Destination) originate the connection, as between two nets of a VPN, unmark this option.

TIP: during rules inclusion, it's important that you evaluate if new rule fits with some already maid. In case yes, It's enough you to edit the existent rule and add desired objects. This will do with that Firewall be more organized, facilitating your maintenance.

8.3 Firewall Basic Rules

The Firewall Setting requests detailed environment analysis so that whole necessary traffic is contemplated through rules. Follow some basic rules, which are useful in most of environments.

8.3.1 Access to Nettion

It is necessary that you create a rule that allows you to access Nettion administration interface. Liberation of this rule can be just made for a fixed IP in net, the administrator's machine or for whole local net destined for Nettion. Rule summary to be created follows in table 8.1 (page 72).

Rule: Nettion Administration			
Source	Destiny	Destiny serv.	Action
Host Administrator	localhost	http https ssh	Accept

Table 8.1: Liberation of Nettion Access

Note: as commented previously, special object “localhost” references own Nettion.

8.3.2 Access Nettion -> Internet

In most of cases, Nettion is used with the function of Net Proxy. That requests that Nettion accesses some services in Internet, as DNS, HTTP and HTTPS. See a rule summary to be created below in table 8.2 bellow.

Rule: Nettion -> Internet			
Source	Destiny	Destiny serv.	Action
localhost	any	http https dns	Accept

Table 8.2: Nettion -> Internet Access

8.3.3 Local Network Names Resolution

Most of time, Nettion is responsible for names resolution in Internet for machines of local net. For that, follows the rule summary to be created in table 8.3.

Rule: DNS for Internet			
Source	Destiny	Destiny serv.	Action
Internal Net	localhost	dns	Accept

Table 8.3: Liberation of DNS for Internal Net

OBS.: We remind that these are tips of firewall basic rules, that can and they should be complemented, however, they still exist many other rules that should be created to really turn your firewall efficient. Such rules depend on some factors as:

- Company's Politics of Safety;
- Services and Used External Applications;
- Services and Internal Applications Externally Accessed;
- Etc.

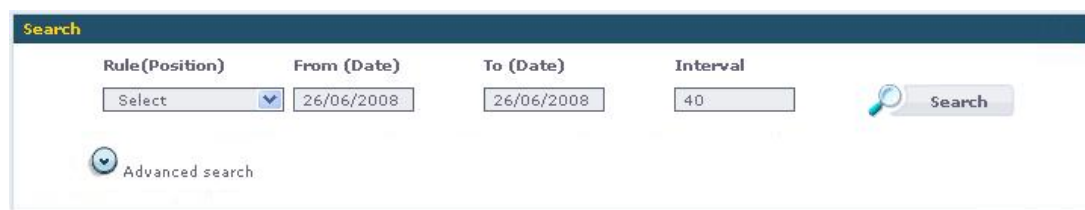
Examples of other rules can be found in this document in other modules settings of Nettion, like Proxy and VPN.

8.4 Reports

Through Firewall report you will have access to generated registers by Log rules of your Firewall.

The research filters allow you to filter for a specific log rule as for an advanced hosts and services selection.

See the illustration 8.7 that follows:



The screenshot shows a search interface for Firewall Reports. It features a dark blue header with the word "Search" in yellow. Below the header, there are four input fields: "Rule(Position)" with a dropdown menu showing "Select", "From (Date)" with the value "26/06/2008", "To (Date)" with the value "26/06/2008", and "Interval" with the value "40". To the right of these fields is a magnifying glass icon and a "Search" button. Below the input fields, there is a link labeled "Advanced search" with a small circular icon to its left.

Figure 8.7: Firewall Reports

Chapter 9

VPN

VPN (Virtual Private Network or Virtual Net) involves use of internet as safe communication middle between two points. To guarantee traffic safety of information for public middle that internet represents, Nettion, through your VPN functionality, creates a communication tunnel among two points for which the traffic data is cryptographed. That means that only these two points will have uncryptography key and of interpretation of data received.

Nettion® possesses four types of VPN:

- PPTP
- IPSec Public Key RSA
- IPSec Shared Key PSK
- OpenVPN (Plugin)

9.1 VPN PPTP

The PPTP protocol allows establishing connection of a belonging internet host to local net controlled by Nettion. Your cryptography is medium or lower, depending on client used. In operating systems Windows, with version same or subsequent to 2000, settle down connections of 128 bits medium cryptography. In Windows 98 clients, settle down connections with 40 bits cryptography.

A common use case comes when user wants to have access company's net, controlled by Nettion, starting from a dialed connection (DialUP) or ADSL.

Attention: for VPN-PPTP use, it is necessary that administrator add in firewall rules to foresee access. Make use of predefined pptp object. A summary of necessary rule follows in table 9.1.

Rule: VPN PPTP Liberation			
Source	Destiny	Destiny serv.	Action
Any	localhost	pptp	Accept

Table 9.1: Liberating VPN PPTP

9.1.1 Settings

To configure VPN - PPTP server, access **VPN > PPTP > Settings**. The settings screen will be exhibited, as display illustration 9.1 below.

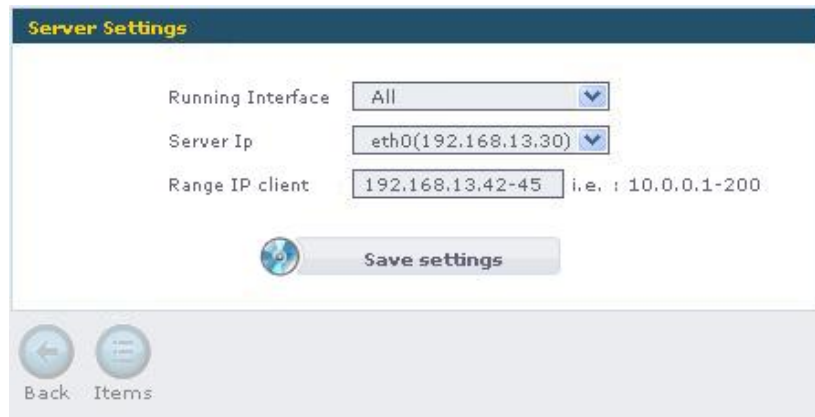


Figure 9.1: Settings of VPN PPTP

- **Running Interface:** Indicates net interface for which server will answer for PPTP requisitions. It will usually be net interface that Internet is connected (with public IP) or All, for any interface. Example: eth0 (200.200.200.200);
- **Server IP:** IP that will be PPTP client's Gateway after the connection. Example: 128.0.0.1;
- **Range IP Client:** IP's Range that will be supplied to VPN clients. Example: 128.0.0.11-20. Administrator should cadastre users that will use VPN PPTP, which we will call **Clients**, could attribute to client an IP, which will be selected for ones with differentiated treatment needs with firewall to each connection. Or, can allow PPTP server to attribute one of IPs inside of range, informed in available server setting in moment of connection.

Important: So that PPTP clients can access your net and so that they can also be accessed, it's necessary that is made a traffic liberation rule. See rule summary for an example where VPN net and local net are in 128.0.0.0/24 in table 9.2 (page 77), considering that:

- **Local Net:** Object of Host/Network configured for 128.0.0.0/24;
- **Any:** Any service which can be accessed between nets. Choose specific services case it's necessary.

Note: To allow that connection can be initiated from both sides, unmark option **Established Service and/or Related on Connection's Return** in advanced settings of this rule.

The exhibition of registered clients list can be ordered by column: **Login** or **Name** or **Description**. The clients should click on specific column for system to alternate exhibition and items ordination on table. It will be possible to use scroll bar to navigate between table items.

Rule: VPN PPTP Liberation			
Source	Destiny	Destiny serv.	Action
Internal Net	Internal Net	Any	Accept

Table 9.2: Liberating Traffic Internal Net ↔ VPN Net

9.1.2 Support of clients' cadastre for VPN PPTP

The support of clients' cadastre PPTP proceeds previously established pattern.

For PPTP clients following fields should be filled out:

Figure 9.2: Adding/Editing PPTP Users

- User: user's login. Example: John;
- Password: password authentication. Example: passwordpptp
- Confirmation: confirmation of password. Former.: passwordpptp
- IP: IP that client will receive when closing VPN connection with Nettion. In case this field is filled out with an asterisk (*), the client will receive one of existent IPs inside of range make available by Server. In case an IP is specified, this client will always receive this IP when connecting. For a larger safety suggest a static IP. Example 1: * Example 2: 128.0.0.11

Active connections

Nettion® makes possible that administrator has knowledge on which connections are active in consultation's moment. This information will be available in subsequent reports.

Reports

In this section, administrator can visualize reports on PPTP accomplished connections.

Search								
User	From (Date)	To (Date)	Host	Interval				
All	22/04/2008	22/04/2008		40	Search			
User	Start Date	Start Time	Stop Date	Stop Time	Rate	Device	IP	End Type
anna.simpson	22/04/2008	09:32:05	22/04/2008	09:32:09	115200	ppp5	192.168.224.10	Normal
george.thompson	22/04/2008	09:30:34	22/04/2008	09:30:38	115200	ppp5	192.168.224.34	Normal
john.stuart	22/04/2008	09:22:30	22/04/2008	10:33:57	115200	ppp1	192.168.224.83	Normal
karol.mcdowell	22/04/2008	08:53:52	22/04/2008	09:10:50	115200	ppp1	192.168.224.92	Normal
phillipe.smith	22/04/2008	08:33:27	22/04/2008	08:52:43	115200	ppp4	192.168.224.20	Normal
eduard.jackson	22/04/2008	08:33:22	22/04/2008	08:33:25	115200	ppp4	192.168.224.210	Multilagon block
Previous (1...40 of 431) Next								

Figure 9.3: Report of Accomplished Connections.

Connections Administrator can follow-up accesses done through PPTP, facilitating net's administration. It's also possible that administrator disconnects a connected user manually clicking in "Stop" button, as shown in illustration 9.4 bellow.

User	Start Date	Start Time	Rate	Device	IP	Action
john.simpson	22/04/2008	09:02:56	115200	ppp4	192.100.10.190	Stop
george.thompson	22/04/2008	09:22:30	115200	ppp1	192.100.10.212	Stop
hellen.morison	22/04/2008	07:56:11	115200	ppp3	192.100.10.193	Stop
tom.mcdolle	22/04/2008	08:55:11	115200	ppp2	192.100.10.221	Stop

Page 1 of 1 Go to .. 4 record(s)

Back Items

Figure 9.4: Listing of Active Connections

9.2 VPN IPsec

IPSec is one of safest protocols that exist for VPN's establishment through public communication nets. This happen because it uses a strongest public algorithms of cryptography, with safety levels configured by administrator.

Attention: for VPN-IPSec use it is necessary that administrator add in firewall rules to foresee your access. Follows a summary of rule to be created in table 9.3 (page 78).

Rule: IPsec Liberation			
Source	Destiny	Destiny serv.	Action
Localhost	Any	ipsec	Accept

Table 9.3: Liberating IPsec

Besides this rule, it is necessary to make a rule that liberates traffic among connected nets by IPsec. Follows a rule summary of the rule to be created in table 9.4 considering that:

- Local net: Object of Host/Net previously configured with IP of your local net;
- Remote net: Object of Host/Net previously configured with IP of remote net;
- Any Service: considering that any service will be available among the nets. Choose specific services case it's necessary.

Note: To allow connection be initiated starting from both sides (local net and remote net), unmark the option **Established State and/or Related on Connection's Return** in rule's advanced settings.

Rule: Liberating traffic inside of VPN			
Source	Destiny	Destiny serv.	Action
Local Net	Remote Net	Any	Accept

Table 9.4: Liberating Traffic Inside of VPN

9.2.1 Settings

Authentication Keys and Cryptography

That exist 2 possible types of key:

TIP: in case you are using 2 Nettions® to establish VPN, open a browser window through secure connection with each one of sides. This way, it is easier to configure your VPN.

PSK Key The authentication system under PSK key consists of an only key, shared among 2 VPN sides, that promotes system's cryptography, un cryptography and authentication.

Advantages:

- To use IPsec protocol, specifically projected for information safe traffic through TCP/IP protocol, Nettion VPN IPsec becomes one of the safest choices for information traffic;
- The PSK system is simpler of being configured that of double key RSA. However, the cryptography level and safety is lower;
- Total compatibility with other VPN PSK systems, as Symantec® Raptor®.

Disadvantages:

- Does not support NAT;
- Less safe than RSA system.

Precautions:

- Do not use humanly comprehensible keys;

- Do not give your key for VPN other side for e-mail, instant messages or other public means of communication. Use SSH, HTTPS or other safe way of messages transfer. In case you use diskette or CDROM for key transport, destroy it;
- Don't reveal your key for anyone;
- Generate safe keys, with more than 128bits.

Key RSA The authentication system under RSA keys consists in 2 keys, a public one and a private one, that makes cryptography system, un cryptography and authentication. This setting request the secret key generation that Netion can supply. The secret key possesses a high cryptography level (Example: 2048bits or 4096bits), configurable by administrator, that guarantees a high level of safety in transactions.

Advantages:

- To use IPSec protocol, specifically projected for information safe traffic through TCP/IP protocol, VPN IPSec becomes one of the safest choices for information traffic;
- RSA system is extremely safe;
- Trusted system has many years, with a test solid base of safety and usability.

Disadvantages:

- Does not support NAT;

Precautions:

- Do not give your key for VPN other side for e-mail, instant messages or other public means of communication. Use SSH, HTTPS or other safe way of messages transfer. In case you use diskette or CDROM for key transport, destroy it;
- Do not reveal your key for anyone.

General Settings

To configure VPN-IPSec server, access **VPN > IPSEC > Settings**. The settings screen will be exhibited, as display illustration 9.5.

- Running Interface: Interface for which server will connect. Usually will be net interface that connects to internet (with public IP). Use option "Default Route" case your Internet Link possesses a dynamic public IP (variable).
- Type: key type that will be used for encryption: 3des, 3desmd5-96 or 3des-sha1-96 Example: 3des-md5-96;
- Re-create Secret Key (only RSA): marking **YES** field will recreate the encryption key demonstrated in **Public Key** field. **Size** field will be activated, in which administrator can specify key size that wants to use in bits (512, 1024, 2048, etc.).
- Public Key (only RSA): key generated by Netion for this server.

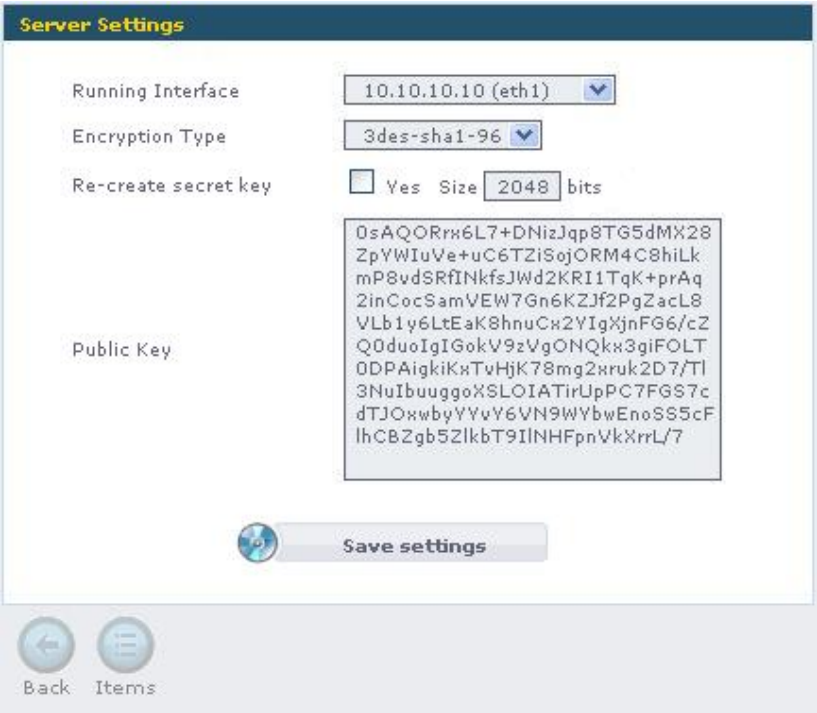


Figure 9.5: IPSEC Server Settings

9.2.2 Connections

In this module, administrator will register and control VPN-IPSec connections. It’s presented to administrator a list of connections already registered. For each listed connection, there is a status indicator that can be green (active) or red (inactive), in agreement with connection state and **Start or Stop** button, which should be pressed to begin or stop the connection in agreement with your state. Are listed in each connection: your name, net A and your Gateway, net B and your Gateway, Connection Status and **Action** (Start or Stop) button.

Attention: before beginning your connection, be certified that the VPN IPSec service in menu System -> Services is marked as “Auto” for Nettion to begin service in machine’s boot.



Figure 9.6: Listing of IPSEC connections

The exhibition of registered connections list can be ordered by any of exhibited columns. For system to alternate exhibition and ordination of table items the user should click on specific column. Scroll bar can be used to navigate among these items.

Maintenance of connections cadastre

The connections maintenance cadastre proceeds like previously established pattern. For new connections, the following fields should be filled out. To facilitate understanding, we identify as “A” and “B” the two sides that will close VPN.

- Name: indicate a name with which you want to identify connection. Example: Store 1.
- GATEWAY A: IP Address of machine that will serve as gateway, in other words, the machine that will connect with other net. Example: 200.253.5.10 (Usually Netition® Itself). Administrator has 3 options in this item: IP/Hostname, Any, Default Route. IP/Hostname: when Netition possesses a **Valid and Fixed** IP of exit. Example(for Brazil): TELEMAR LINK IP, LINK EMBRATEL; Any: when on side (A) of VPN, in this same position, the option is registered as Default Route on side (B) of VPN Any will be registered. Example: connection between a Netition with static IP accepting a connection with a dynamic IP Netition. Default Route: when administrator makes a VPN setting using a dynamic IP link, it's impossible to determine which will be Netition's IP and, consequently, it's Gateway. In this case, mark the Default Route option. Example: Setting of VPN using ADSL or Cable.
- Network A: net that will be connection's part and that, therefore, will be accessible by other side (Net B). Example: 128.0.0.0/16.
- Next Hop A: Standard exit of Netition that acts like Gateway A. Example: 200.253.5.9 (Netition's gateway). In case you are registering data of a VPN that uses dynamic IP, this option will be disabled, because it would be impossible to determine Netition's Gateway in a static way.
- Gateway A key: communication key of Gateway A.
Example:

0sAQ07tMehTP69r+Pr4PSTUmiYMDLQ4Lf70kWBgbhf+hhBKuh7Dk4XRNZcn8AYL15Pmig
hjuUoAhJEQWW1VzsdzmQosWAh6URQpQmYQ+bwymJpFAVTBFEgaJo6r+vP0Irn7/FhI41I
tnioJ7rCpEKtq41fDEeOK5MDeNK6za+Rx4WE08Dr8kjR0ePK9uPzb1xEwEizrIBUZfm4h
BXVI/7LKXZG1Hf90uc6RKhPX1N/HkhIC2s0m61TIwTzqHwx+Qd48B7oITZslcms0kK2Wl
JjZgq+5dPZQnHjoXsAuNJaNVXkQZFmNQziwznFJ7D2D1qfuVizeVYgLso6yBJgW+QG7ush
- Gateway B: IP Address of machine that will serve as gateway, in other words, inter-connection with other net. Example: 200.195.152.2.
- Network B: net that will be connection's part and that, therefore, will be accessible by other side (Net A). Example: 192.168.1.0/24.
- Next Hop B: Standard exit of Netition that acts like Gateway B. Example: 200.195.152.1. See item NextHop A.

- Gateway B key: communication key of Gateway B.
Example:

```
0sAQPZfUID9sYTuasmkJYfU8JmpKwphyfxT0NtUmzTT6S58FX1a6qEFJrv9JgIHFtp8D1
h6wHa6a9069bHg+MZX3GLtb4ynGaFtVsquvNx9aVgnuliunxaXwsq2zShTBBgrCTed5o9
YBMms1It dxI6Pu5oeD1JrzQkI5J0b0qo3ukx07nqwUmDJRVHfL1zgbVeeTmn86LmhuMYp
zwcBdBB5RZae8xnL0roUN7XUnj0g2VeHWVUk9giwS628KKLbclWIBcl8hIn1xc30qzrjl
vqPAZggNGNt3w85925oxPRn+UvXNkadx0xKeoF8DyLsrbvl61RAq7erQWyNVUvCz
```

- Connection: if connection will be activated manually or automatically. Configure this option for “Auto” for VPN it is always restarted automatically. Example: Auto.
- Connection Status: if connection is active or not.

Note: the Administrator can import Nettion’s key that being configured giving a click in **Import my public key** button.

TIPs of settings:

- 1. When configuring a VPN among 2 Nettions, open a browser window for each one of them;
- 2. Settings on 2 sides will be totally IDENTICAL, except in cases of dynamic IPs use. This means that, if administrator registers data of Nettion 1 as being Nettion (A) of the setting, when you will accomplish the setting of Nettion 2, the information will be identical, including in positioning, Nettion 1 as being the side (A);
- 3. In settings being **Nettion 1, Side (A), Static IP** and **Nettion 2, Side (B), Dynamic IP**, obligatorily (B) side will have as gateway the item **Default Route** marked. Following the previous item tip, administrator is taken to configure same item, in same position, in each one of Nettion. However, this is the only rule exception. Observing Nettion 2, in setting items on side (B), administrator will configure the **Default Route** item. To see this same setting, in same position, on side (A), administrator will have to configure the **Any** item. Note: whenever there is a VPN setting between a static IP and a dynamic IP, the fields corresponding to static IP will be identical in both Nettions. However, the corresponding setting fields beside dynamic IP will be different: in Nettion with dynamic IP, we will see marked the **Default Route** item, and in Nettion with Static IP, we will see marked the **Any** item;
- 4. Nettion makes possible that both connections (Nettion A and Nettion B) possess Dynamic IPs, of ADSL type, for instance. For that it is necessary to do settings using host name and not the Host IP. As IP is dynamic, use Nettion dynamic DNS service and for each Nettion associates a DNS name. Once made settings, Nettion maintain the connection activate even if IPs vary.

See the illustration 9.7 below:

The screenshot shows the 'USA-Brazil Connection' configuration window. It contains the following fields and options:

- Name:** USA-Brazil
- Gateway A:** ☒ IP/Hostname ☐ Any ☐ Default Route. Value: 200.200.200.1
- Network A:** 192.168.0.1/24 i.e.: 10.0.0.0/24
- Next Hop A:** 200.200.200.254
- Gateway A ID:** @host1.yourcompany i.e.: @host1.domain.com
- Gateway A key:** ☒ Public Key RSA ☐ Shared Key PSK. Value: 0sAQORw6L7+DNizJqp8TG5dMX282
- Import my public key:** (button)
- Gateway B:** ☒ IP/Hostname ☐ Any ☐ Default Route. Value: 20.250.130.1
- Network B:** 172.16.0.0/16 i.e.: 192.168.0.0/16
- Next Hop B:** 20.250.130.254
- Gateway B ID:** @host2.yourcompany i.e.: @host2.domain.com
- Gateway B key:** ☒ Public Key RSA ☐ Shared Key PSK. Value: Js0yvFrSDWmwL8IoRPWn+izJqp8TG0
- Import my public key:** (button)
- PSK Key:** (empty field)
- Use an alternative DNS Server:** (empty field) i.e.: nf1.no-ip.com; nf2.no-ip.com (opt.)
- Connection:** ☐ Manual ☒ Auto
- Connection Status:** ☐ Active ☒ Inactive
- Save settings:** (button)

At the bottom, there are navigation buttons: Back, Items, and Del.

Figure 9.7: Add/Edit of IPSEC Connection

9.3 OpenVPN

NettionPlug OpenVPN's documentation is in item 15.5 of Chapter 15 about **Nettion-Plugs**, in page 138. Also read about NettionPlugs in Chapter 15 in page 127.

Chapter 10

NIDS

The Network Intrusion Detection System of Nettion® works investigating if there is someone trying to apply some of more than 1.600 types of invasion attempts classified in Nettion, through your connection. Once attempt is detected, Nettion will send an e-mail to administrator giving notice of event and it will register the fact in a log regarding NIDS.

10.1 Settings

Defines referring information to detection system, which can be:

- Interface, used to monitor traffic;
- IPs and networks that are monitored by attacks;
- Signature Filters, etc.

The signatures update is made through the updating system of Nettion. Verify new versions of software in system module.

10.1.1 Interfaces Selection

The administrator can select which interface wants to monitor regarding invasion detection attempts. In case you want to monitor all, won't be necessary to click individually in each one of them. It is enough to click in "All" option, as display the illustration below.

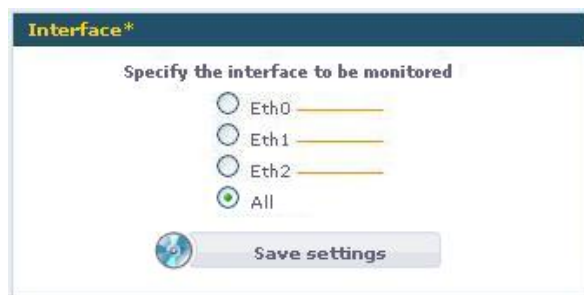
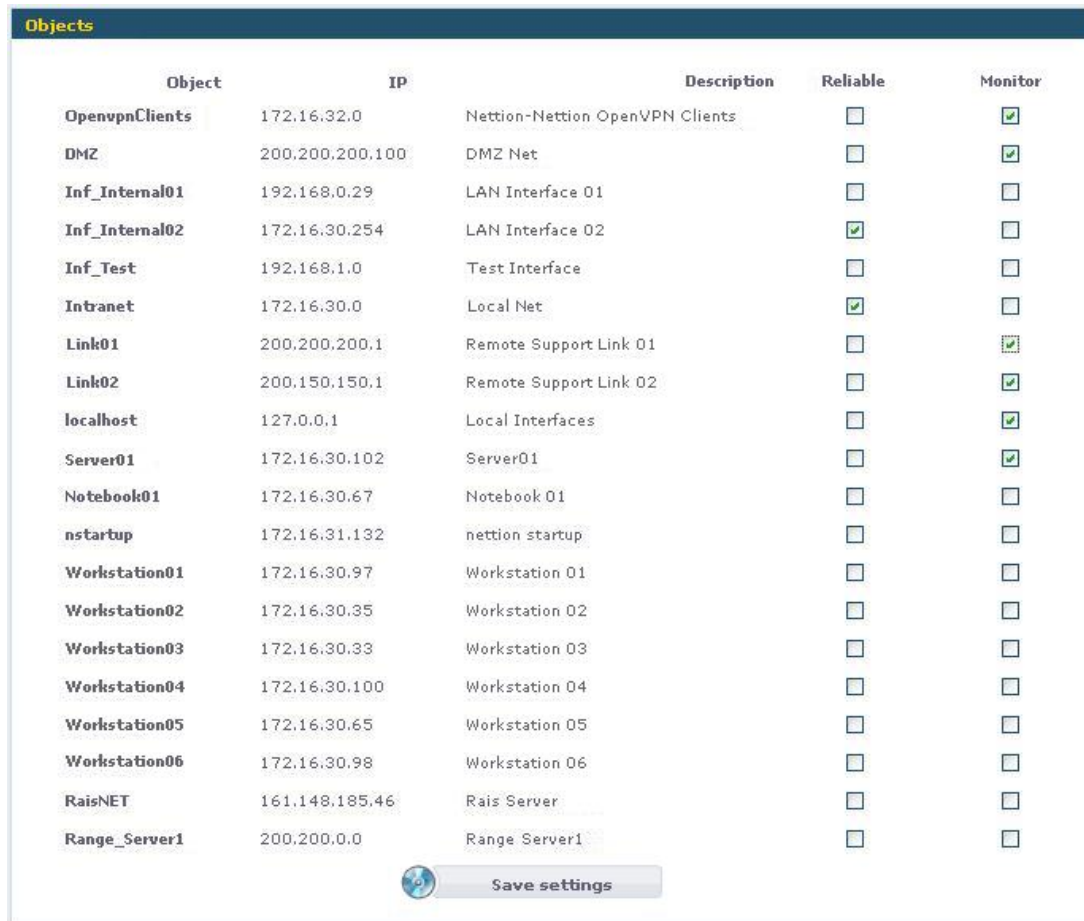


Figure 10.1: Selection of NIDS Interfaces

10.1.2 Objects

An objects list is presented in Nettion for administrator to classify which are reliable and which will be monitored. When selecting an object to be monitored whole traffic regarding chosen item will be analyzed. After make wanted alterations, it is necessary to click in “Save Settings” button for these take effect.



Object	IP	Description	Reliable	Monitor
OpenvpnClients	172.16.32.0	Nettion-Nettion OpenVPN Clients	<input type="checkbox"/>	<input checked="" type="checkbox"/>
DMZ	200.200.200.100	DMZ Net	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Inf_Internal01	192.168.0.29	LAN Interface 01	<input type="checkbox"/>	<input type="checkbox"/>
Inf_Internal02	172.16.30.254	LAN Interface 02	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Inf_Test	192.168.1.0	Test Interface	<input type="checkbox"/>	<input type="checkbox"/>
Intranet	172.16.30.0	Local Net	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Link01	200.200.200.1	Remote Support Link 01	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Link02	200.150.150.1	Remote Support Link 02	<input type="checkbox"/>	<input checked="" type="checkbox"/>
localhost	127.0.0.1	Local Interfaces	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Server01	172.16.30.102	Server01	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Notebook01	172.16.30.67	Notebook 01	<input type="checkbox"/>	<input type="checkbox"/>
nstartup	172.16.31.132	nettion startup	<input type="checkbox"/>	<input type="checkbox"/>
Workstation01	172.16.30.97	Workstation 01	<input type="checkbox"/>	<input type="checkbox"/>
Workstation02	172.16.30.35	Workstation 02	<input type="checkbox"/>	<input type="checkbox"/>
Workstation03	172.16.30.33	Workstation 03	<input type="checkbox"/>	<input type="checkbox"/>
Workstation04	172.16.30.100	Workstation 04	<input type="checkbox"/>	<input type="checkbox"/>
Workstation05	172.16.30.65	Workstation 05	<input type="checkbox"/>	<input type="checkbox"/>
Workstation06	172.16.30.98	Workstation 06	<input type="checkbox"/>	<input type="checkbox"/>
RaisNET	161.148.185.46	Rais Server	<input type="checkbox"/>	<input type="checkbox"/>
Range_Server1	200.200.0.0	Range Server1	<input type="checkbox"/>	<input type="checkbox"/>


 **Save settings**

Figure 10.2: Objects Selection to be Monitored

10.1.3 PortScan Settings

Administrator should specify number of ports and interval of time necessary here to consider a portscan coming of a same machine. These settings are valid even to UDP or TCP packages.

Standard value is four ports detection in an interval of three seconds, for portscan characterization. Here, administrator can increase or reduce the NIDS sensibility for invasion attempts detection. To increase sensibility, it is enough to reduce the number of ports for interval of time. To decrease, increase the number of ports for interval of time, as displays illustration 10.3. Soon after, click in “**Save Settings**” button.

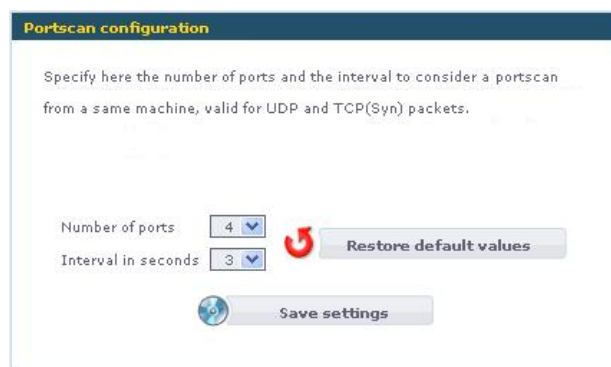


Figure 10.3: NIDS PortScan Settings

10.1.4 Detection of Signatures

Nettition® possesses registered more than 1.600 types of invasion attempts, that are differentiated by type and they are exhibited when administrator clicks in “Signature Type” field. As some examples of signature types, we can mention: Backdoors, DOS, Exploit, WEB IIS etc.

When you click in one of these signature types, the “Enable/Disable Signatures” button will be activated. When clicking in this button, a list of signatures will be presented, referring to selected item (Example: “WEB IIS”), to administrator. This will select the signatures that administrator consider important for NIDS to monitor. As shown in illustration 10.4.



Figure 10.4: Selection of NIDS Signatures

At lists’ end, there is a button that selects all referring signatures to item (Example: WEB IIS). Therefore, in case you want to mark all, it is not necessary to select one by one.

This configuration influences the performance directly for that it should be done with very care and conscience.

10.1.5 E-mail alert

Specify the interval of time in case you want to receive alert notifications by e-mail. To disable that option, specify sending frequency for “None” and save settings.

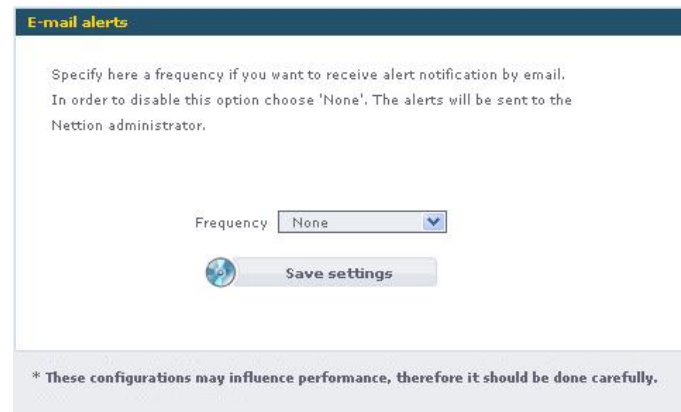


Figure 10.5: Alert through E-mail Settings

10.1.6 Reports

Exhibits alert reports and invasion attempts with details on captured packages: Origin and destiny IPs, protocol, ports etc.

10.1.7 Alerts

Administrator can visualize last detected signatures and also portscans accomplished.

List of general information regarding NIDS configuration:

- Active signatures: informs the amount of active rules and total of existent rules. Example: 721 of 1601
- Detected signatures: exhibits the amount of active signatures that were detected by NIDS in your connection. Example: 101
- Detected PortScans: number of portscan that were detected by NIDS. Example: 247
- Last Alert Date: dates and hour in which was generated the last alert. Example: 21/12/2002 - 14:27:13

10.1.8 Last Signatures

Here administrator visualizes, page by page, last signatures alert, specifying the following fields:

- Signature: signature in which alert makes reference. Example: WEB-PHP content-disposition
- Source IP: IP that originated the alert. Example: 10.0.3.30
- SP: machine's source port from where it starts access attempt. Example: 6040 IP
- Destination IP: IP that connection is destined. Example: 10.0.3.12
- DP: destination port for which destiny access was addressed. Example: 80
- Protocol: type of protocol used for access. Example: TCP

Signature by Alerts						
Signature	Source IP	SP	Destination IP	DP	Protocol	Time & Date
(spp_stream4) possible EVASIVE RST detection	201.255.147.64	56806	200.200.200.1	25	TCP	16:36:17 17-4-08
(spp_stream4) possible EVASIVE RST detection	201.255.147.64	56806	200.200.200.1	25	TCP	16:36:17 17-4-08
(spp_stream4) possible EVASIVE RST detection	201.9.11.70	60243	200.200.200.3	80	TCP	16:36:16 17-4-08
(spp_stream4) possible EVASIVE RST detection	201.9.11.70	60243	200.200.200.5	80	TCP	16:36:16 17-4-08
(spp_stream4) possible EVASIVE RST detection	70.239.136.121	54422	200.200.200.1	25	TCP	16:36:12 17-4-08
(spp_stream4) possible EVASIVE RST detection	70.239.136.121	54406	200.200.200.5	25	TCP	16:36:12 17-4-08
(spp_stream4) possible EVASIVE RST detection	10.1.1.20	9003	200.200.200.5	4949	TCP	16:36:10 17-4-08
(spp_stream4) possible EVASIVE RST detection	10.1.1.20	9003	189.66.22.83	29328	TCP	16:36:09 17-4-08
(spp_stream4) possible EVASIVE RST detection	200.183.3.130	36341	200.200.200.3	25	TCP	16:36:06 17-4-08

Previous (1...15 of 368203) Next

List with interval of 15 alerts ▼

Back Items

Figure 10.6: Report of Detected Signatures

- Time and Date: hour and date in which NIDS registered alert. Example: 16:20:47 07-04-2003

The administrator can select the amount of alert that wants to visualize for page through alteration of field “List with interval of 15 alerts”, that for default presents 15 alerts. In case administrator wants to add one of presented IPs in list to blocked IP, he should click on wanted IP and confirm the blockade in picture that will request confirmation.

Last PortScans

This report shows specifications on accomplished portscans: Source IP, amount of connections by host, used protocols and date/hour of portscan. Clicking in one of list items, it will be requested to administrator the inclusion confirmation of portscan source IP in list of blocked IPs, as displays illustration 10.7.

Portscans	
Alert Description	Time & Date
End of portscan from 189.40.142.219: TOTAL time(0s) hosts(1) TCP(1) UDP(0) STEALTH	17:19:44 17-4-08
portscan status from 189.40.142.219: 1 connections across 1 hosts: TCP(1), UDP(0) STEALTH	17:19:40 17-4-08
PORTSCAN DETECTED to port 9003 from 189.40.142.219 (STEALTH)	17:19:34 17-4-08
End of portscan from 189.40.67.119: TOTAL time(7s) hosts(2) TCP(3) UDP(0) STEALTH	17:14:39 17-4-08
portscan status from 189.40.96.30: 1 connections across 1 hosts: TCP(1), UDP(0) STEALTH	17:10:01 17-4-08
PORTSCAN DETECTED to port 9003 from 189.67.252.153 (STEALTH)	17:10:00 17-4-08
PORTSCAN DETECTED to port 9003 from 189.40.96.30 (STEALTH)	17:09:57 17-4-08

Previous (1...40 of 78416) Next

Back Items

Figure 10.7: Report of Detected PortScans

10.1.9 Blocked IPs

Exhibits a list with IPs blocked through NIDS web interface. IPs contained in this list won't have any access to Nettion, in any direction, going by any interface. Through this

list, it is also possible the removal of IPs blocked.

Note: IPs will only be blocked if Firewall is active.

List of IP blocked by inclusion date (Illustration 10.8):






Ordered by inclusion date			
IP address	Reason	Time & Date	
201.19.221.158	(spp_stream4) possible EVASIVE RST detection	23:08:37 10-9-05	 Remove
10.16.0.123	(spp_stream4) STEALTH ACTIVITY (Vecna scan) detection	15:23:19 18-9-03	 Remove
60.36.140.143	Portscan	15:11:15 13-9-04	 Remove
82.224.133.3	Portscan	15:07:23 13-9-04	 Remove
200.164.242.201	BAD TRAFFIC udp port 0 traffic	08:02:06 19-1-04	 Remove
Total of Blocked IPs = 5			

Figure 10.8: Report of Blocked IPs

Chapter 11

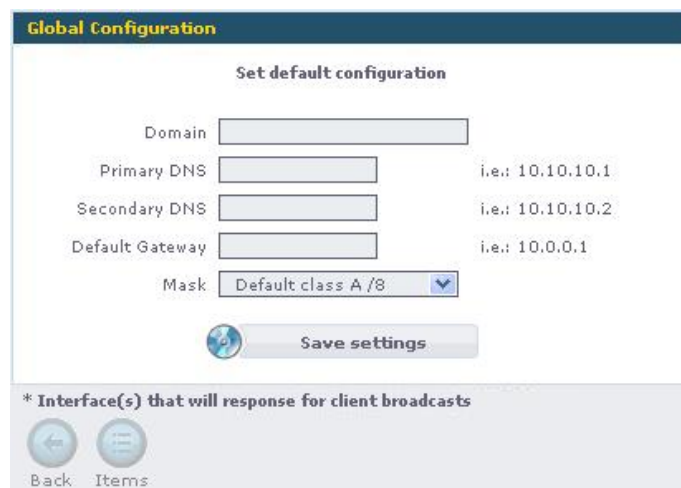
DHCP

Nettion® DHCP server can be configured to distribute IP addresses of the stations of one or more linked networks to product, allowing treating in a different way each one of them.

11.1 Settings

11.1.1 Global Settings

To configure Nettion DHCP server, access **DHCP > Settings**. In screen that will be exhibited the fields should be filled out according to description below:



Global Configuration

Set default configuration


Domain

Primary DNS i.e.: 10.10.10.1



Secondary DNS i.e.: 10.10.10.2

Default Gateway i.e.: 10.0.0.1

Mask

 Save settings

* Interface(s) that will response for client broadcasts

Back Items

Figure 11.1: Global Settings of DHCP Server

- Domain: specify domain which will answer to DHCP. Example: fictitious.com
- Primary DNS: primary name server. Example: 128.0.0.1
- Secondary DNS: secondary name server. Example: 128.0.0.2
- Default Gateway: exit machine of net. Example: 128.0.0.1
- Mask: net mask which IP of DHCP server belongs. Example: Class B default /16.

11.1.2 Interface

Still in global configurations screen, select the interfaces that will answer for DHCP requisitions in your net, according to following illustration 11.2.



Figure 11.2: Selection of DHCP operation Interface

11.2 Hosts

This section allows administrator to associate IP addresses with net *MAC addresses*, doing with that certain machines always receive a static IP. It is especially useful when we want to do specific rules for some net IPs.

The exhibition of registered hosts list can be ordered by column: “host” or “IP address”. For that the system alternates exhibition and ordination of table items, being necessary for that, the user clicks on specific column. The user can use scroll bar to navigate between items table.

11.2.1 Support for Hosts Cadastre

The hosts’ maintenance cadastre proceeds like previously established default. For hosts, the following fields should be filled out:

Figure 11.3: Inclusion of New Host

- Host Name: description of host. Example: Machine of John;
- MAC Address: specification of network adapter physical address (Mac-Address). Example: 00:E0:7D:00:E3:23;
- IP Address: IP Address to be supplied;
- Network: net of which host will be part. Example: 128.0.0.0.

11.3 Networks

DHCP Server will attribute IPs inside of specified networks for the interface which be addressed.

The exhibition of registered nets list can be ordered by column: “network” or “mask”. For that, administrator should click on specific column. That will do with that system alternates the exhibition and ordination of table items. Administrator can use scroll bar to navigate between items of table.

11.3.1 Support for Networks Cadastre

The cadastre maintenance of networks follows previously established pattern. For networks, following fields should be filled out:

New Network

Network IP*

Mask* ▼

IP range

Begin* i.e.: 10.0.0.1

End* i.e.: 10.255.255.254

Interface* ▼

Keep this fields blank to use global settings


Domain

Primary DNS i.e.: 10.10.10.1

Secondary DNS i.e.: 10.10.10.2

Default Gateway i.e.: 10.0.0.1

Allow only configured MACs ☐

 **Save settings**

* Required fields



  Back Items

Figure 11.4: Specification of Network DHCP

- Network IP: IP of network. Example: 128.0.0.0
- Mask: New network mask. Example: Class B pattern /16
- IP Range: Range of IPs that will be supplied by Netition;
- Begin: Initial IP of IP Range. Example: 128.0.0.21
- End: Last IP of IP Range. Example: 128.0.0.50
- Interface: Interface that will answer for network requisitions.

In case you want to work with registries in DHCP Global Settings, other fields are not necessary. Otherwise, they should be filled out.

Chapter 12

E-mail

12.1 Settings

Nettion® can also be used as your e-mail server, doing all administration work of multiple domains and users, integrated with a quite robust system of antivirus (updated daily) and anti-spam with learning system and quarantine.

As base for this function, Nettion uses a Linux e-mail server called **Qmail**, plenty known by your safety and stability in administration of a great number of accounts.

Besides this function, Nettion offers: integrated authentication, quote system by user, blockade system of e-mails attachments by size and extension, report system, queue control (makes possible administrator to follow if a message was not still delivered, the reason and even your exclusion), logs system and quarantine, that makes possible following the e-mails that were blocked by containing virus, and several other functions that are decisive in monitoring of your e-mail server.

To e-mails reception, users have possibility to use following kinds of accounts: POP3, POP3s, IMAP or IMAPs or even a webmail that is available by Nettion®.

12.1.1 Authentication

This option doesn't refer to authentication way, since it was previously defined in chapter regarding Users and Groups, but to maximum number of allowed simultaneous authentications. That will depend on the system users' number. As large the number of users, larger will be simultaneous authentication number. Twenty (20) are an ideal value.

However, administrator can increase it, when noticing that your users need to do several authentication attempts on e-mail client to conclude operation, or reduce it, so that memory is not used without need in server.

Global Settings

Simultaneous authentications allowed: 20

Max attachment size allowed: 10 Mb

Port SMTP: 25

Block hosts without reverse DNS: ☒

Notices (Failures/Warnings)

Sender: "Mail Delivery System" <postmaster@>

Subject: Undelivered Mail Returned to Sender

Message: I'm sorry to have to inform you that your message could not be delivered to one or more recipients.

☐ Enable purge of mailbox messages in server

Trash: 7 Day(s)

Sent mails: 30 Day(s)

[Save settings](#)

[Back](#) [Items](#)

Figure 12.1: E-mail - Authentication

12.1.2 Relay

It is important not to allow that e-mail server is used improperly to send useless messages, unpleasant and almost always undesirable –spams, what is usually made by some user that is not part of your network. Netition allows administrator to define which networks or hosts will have access of sending e-mail through your server. Technically, that permission calls itself relay. To open the relay for somebody means to allow that certain host or network send e-mails through your server. A system well administered, certainly, it will only allow access for those that are right to do it. Therefore, it is necessary to maintain a closed relay against intruders.

Name	Description	IP	Mask
Intranet	Internal Network (Company)	192.168.1.0	255.255.255.0
Filial	Internal Network (Filial)	10.10.0.0	255.255.0.0

Page 1 of 1 Go to .. 1 record(s)

[Back](#) [Add](#) [Items](#) [Del](#)

Figure 12.2: E-mails Server Relay

We have here a hosts/networks list with clearance to use server for send messages. The

liberation cadastre it is very simple, taking in consideration the previously registered objects and filling out a form as following:

In the left box are hosts/networks that have permission and in right box are all objects inserted in Nettion. Using the buttons between two windows, of intuitive characteristics, it can be added or excluded those that will be clearance of sending messages through this server. It's enough, at all alterations end, click on "Saving Settings" to finish.



Figure 12.3: Relays Administration

12.1.3 Webmail

Nettion offers a Webmail system with Send/Receive e-mails option through Web being just necessary for this the identification, with a combination of complete e-mail and user's password. Nettion Webmail can be accessed through your **IP** followed by webmail, for example: <http://200.200.200.200/webmail>.

Some characteristics are configurable to personalize Nettion® webmail as webmail standard language, the icon that appears in login screen (which needs to contain an absolute address as the default example) and the folder (directory) name that will keep the trash messages, sent messages and draft e-mail.

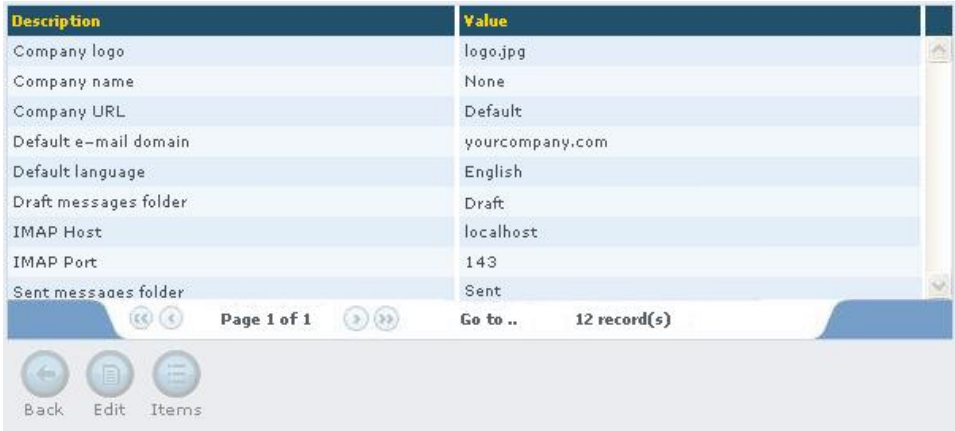


Figure 12.4: Webmail Settings

12.1.4 Messages

In this section administrator can edit the three following messages:

- Returned message for remittent that try to send e-mail for invalid user;
- Message informing that share limit is about to be reached;
- Message returned for remittent when his e-mail exceeded limit quote;



Figure 12.5: Messages Setting of E-mails Server

12.1.5 Extensions

Initially, antivirus should maintain away files that easily are infected and that can carry virus for e-mail clients. Some extensions, already classic, they can carry virus. In general terms, the self executed files as “.exe” and “.com” extension are the most frequently infected. Due to larger virus incidence and larger infection probability in files with certain extensions, Netteion blocks the delivery or exit of e-mails that contains attachments with such extensions.



Figure 12.6: List of Blocked Extensions

The Add or Edit screen is simple and intuitive where it is just necessary to register extension and a small description, as shown in following illustration:

Figure 12.7: Add/Edit of Blocked Extensions

12.2 Domains

In this section administrator will control e-mails domains. It is possible to create and remove domains, as well as to add or remove users of such domains.

Domains	Nº users	Quota	Nº messages	Autenticacion
domain01.com	35	10,00 MBytes	Unlimited	Local
domain02.com	22	10,00 MBytes	Unlimited	Nettion

Page 1 of 1 Go to .. 2 record(s)

Back Add Edit Items Del

Figure 12.8: Listing of E-mail Domains

Observe: To your e-mail domain works perfectly in Internet, it is necessary that DNS of domain is properly configured and saying that Nettion will be responsible for e-mails.

12.2.1 Including a Domain

In case you want to add a domain, click in **Add** button and fill out the fields according to descriptions below:

- Domain: name of domain to be added. Example: **nettion.com.br**;
 - Quota: maximum disk space that each account can occupy;
 - Max number of messages: quota for message. Number of messages by account;
 - Administrator password (postmaster): Administrator of domain password;
- In case you want to redirect invalid messages (sent to inexistent addressees) for another e-mail account, mark the *checkbox* **Redirect invalid e-mail** and type an e-mail account in the field below. The standard procedure would be to send a message to remittent informing that destiny account does not exist.
 - In case you want to **use Nettion authentication**, mark this *checkbox* and choose groups to import users. It is possible to import users of all groups or of some specific group.

See illustration 12.9 that follows.

Domain Edit

Domain:

Quota: MBytes ☐ Unlimited

Max number of messages:

Administrator Password (postmaster):

Password Retype:

☐ Redirect invalid e-mail

Redirect to:

☐ Use Netition authentication

Import user's group:

Start sychronization:

Figure 12.9: Add/Edit of Domains

12.3 Users

In this section administrator can search and edit users, besides of create them.

12.3.1 Searching Users

To visualize existent users (e-mail accounts) in the system, access **E-mail > Users**.

Users Search

Login: Domain: Name:

Login	Name	Quota	N° messages	Aliases
anna.thompson@yourcompany.com	Anna Thompson	250,00 MBytes	10000	1
bernard.watson@yourcompany.com	Bernard Watson	250,00 MBytes	10000	0
dennis.smith@yourcompany.com	Dennis Smith	250,00 MBytes	10000	0
john.simpson@yourcompany.com	John Simpson	Ilimitada	10000	3
george.lopez@yourcompany.com	George Lopez	250,00 MBytes	10000	3
phillipe.stuart@yourcompany.com	Phillipe Stuart	250,00 MBytes	10000	2
tom.madson@yourcompany.com	Tom Madson	250,00 MBytes	10000	1

Page 1 of 1 Go to .. 14 record(s)

Figure 12.10: Users' Management

In the screen that will be exhibited, all users will be shown, of all existent domains in e-mail server and in alphabetical order. However, exhibition order can be altered, being

enough for that to click in the corresponding header of wanted order. To facilitate search, Users search which is located above users' screen can be used.

12.3.2 Editing Users

When making the search, you can edit account clicking in **Editor** button. The following screen will appear:

Figure 12.11: User Edit

The fields **Name**, **Quota** e **Max. number of messages** can be edited. Alter them according with your need.

In case you want to use **Forward to other e-mails** (this option send copies of e-mails received for another account) resource mark this option and fill out the following field with account for which will be send a copy. If you want to direct for more than one account, separate them with **semicolon (;)**.

Don't forget to **Save Settings**, in case you set some changes.

12.3.3 Inserting Users

When clicking in add button, following screen will appear and it will allow a new e-mail user's addition:

- Login: The first part of e-mail address, the one that appears before strudel (@). Example: George;

- Domain: The existent domains will be listed in a combo box. You should choose the domain for which is creating a new account;
 - Name: The user's name. Example: George Thompson;
 - Quota: maximum disk space that an account can occupy;
 - Max. number of messages: quota by number of messages;
 - Password: user's password;
- In case you want to forward a copy of received messages for another e-mail, mark **Forward to others e-mails** option and fills out the following field with one or more accounts where new messages should be directed. Remember to separate them with **semicolon (;)**.

Figure 12.12: Add/Edit E-mail Users

12.4 Aliases

In this section administrator can define **Aliases**, a kind of nickname, another name for which one or some accounts should be known.

12.4.1 Creating a Alias

In **Aliases** section, click in **Add** and the following screen will appear:

In this example, was created a **george.thompson@default.com** alias. This address is an alias for the e-mail **george@default.com**.

Therefore, send a message for **george.thompson@default.com** is the same as send a message for **george@default.com**.

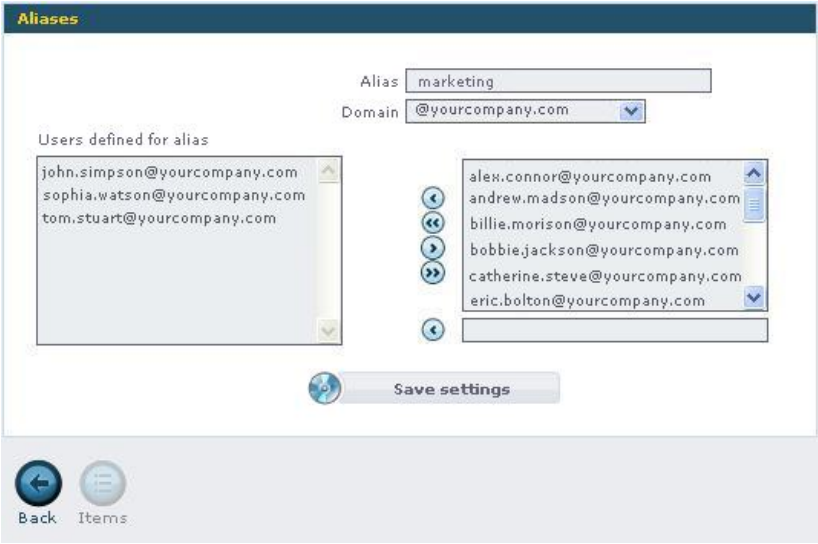


Figure 12.13: Add a E-mail Alias

- Alias: Alias name. In this example, **george.thompson;**
- Domain: select in the list a domain for which you are creating an alias. In this example, *default.com*;
- Defined Users to Alias: Define the users for which the alias will refer; in the example, **george@default.com**.

12.5 Antivirus

Every day, people with bad purposes create viruses to harm and to infect systems and computers. It would be of little usefulness an antivirus that blocks all suspicious files, but didn't contain an updated list of virus in your database. This way, a good tool should supply an instantaneous and configurable updating system.

12.5.1 Updating

That is first way of Nettleion® to update, done in an immediately, when it goes more appropriate to administrator. Nettleion makes a search for more updated base and synchronizes with local base, maintaining system stronger.

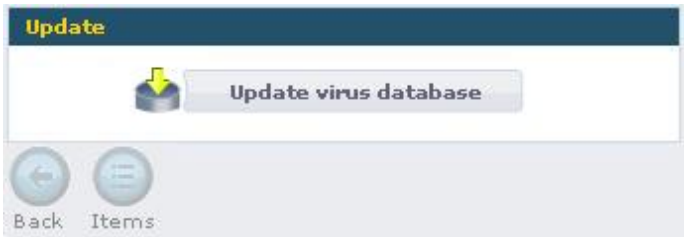


Figure 12.14: Antivirus Update

12.5.2 Scheduling

It is also possible to define an ideal moment at administrator’s criterion for Nettleon to do update in virus base. For that, define day/schedule for updating to happen, filling out the form below and then, save settings.

The screenshot shows a web interface titled "Schedule". It contains three configuration fields: "Frequency" with a "Select..." dropdown, "Day" with a "Not applicable" dropdown, and "Time range" with two "00" dropdowns separated by a colon. Below these fields is a "Save settings" button with a floppy disk icon. At the bottom of the window are "Back" and "Items" navigation buttons.

Figure 12.15: Antivirus Update Scheduling

12.5.3 Historical

Nettione® allows a direct accompaniment on report of database updating. There are three possible states for each updating:

- Successful with updates - when Nettione® search for updates in database and becomes necessary to update the local base;
- Successful without updates - when Nettione® search for updates in database but local base is already updated;
- Unsuccessful - when Nettione® can not connect with the remote bases.

The screenshot shows a web interface titled "History" displaying a table of update events. The table has four columns: "Date", "File", "New signatures", and "Status". Each row represents an update event, with dates ranging from 01/04/2008 to 10/04/2008. The "Status" column shows green circular icons, indicating successful updates. Below the table is a pagination control "Previous (1...10 of 48) Next". At the bottom of the window are "Back" and "Items" navigation buttons.

Date	File	New signatures	Status
10/04/2008	main.cvd	2062	●
09/04/2008	main.cvd	1891	●
08/04/2008	main.cvd	337	●
07/04/2008	main.cvd	388	●
06/04/2008	main.cvd	443	●
05/04/2008	main.cvd	1393	●
04/04/2008	main.cvd	631	●
03/04/2008	main.cvd	521	●
02/04/2008	main.cvd	359	●
01/04/2008	main.cvd	1395	●

Figure 12.16: Update History

12.6 Antispam

Nettion® antispam is a functionality that controls undesirable messages. Even if e-mails server relay of Nettion is closed, in some places, there are administrators that don't have due concern with closing of relay. The spammers, those that send hundreds or even thousands of not requested messages; they take advantage of this fragility. Good administrators should worry with others' bad work done and to ensure that your users will be less affected for that problem.

An antispam is a software that is based on some characteristics of e-mails, classified as spam, like word-keys and HTML format¹

12.6.1 Settings

To each spam characteristic found in an e-mail, it receives a punctuation that depends on what was located. When this punctuation reaches a certain limit in settings sensibility, e-mail suffers an alteration. Message title identified as spam will be preceded by expression ****POSSIBLE SPAM****. Message will usually be given to client. It is not automatically deleted, because a message can possess key words and formats that identify them as undesired message (spam) but is not it really. Like this, each user must define filters, in your e-mail readers, to separate the legit messages of those undesired.

The indicative number of sensibility represents the point's limit that a message can reach until spam status is given. As **SMALLER** the number, more easily a message will be classified like this.

Figure 12.17: Antispam Settings

¹HTML - (Hypertext Markup Language). It's a language used for create web pages and e-mails with a more rich formatation, like bold format, font colors and images.

The new version of Nettleon antispam adds support to messages training in **spam** and **no-spam** mode for users. Mark the **Learn user classified messages** option in case you want to activate such resource. If you decide to use this resource, you should configure two e-mail accounts, one for messages classified as spam and other for ones that are not. In that example, the accounts will be, respectively, **spam@default.com** and **nospam@default.com**. Reminding that those accounts should be created in chosen domain as any other user account. The Nettleon antispam learning system is described below:

The antispam will work as always, marking as ****POSSIBLE SPAM**** e-mails that it considers. In case users receive SPAMS that they were not marked by antispam, they can forward that message as attachment for selected e-mail to receive spam, in case, **spam@padrao.com.br**. Works in same way with messages that are not spam's, but they were classified like SPAMS. The users have the option of forwarding them for e-mail that was selected to receive the messages that are not spams. In our example **nospam@padrao.com.br**. Periodically (by administrator scheduling), the antispam checks the two accounts and it learns as spam the messages of spam account and as non spam the messages of no-spam account. This continuous training improves the effectiveness of antispam and it allows him to reach better indexes, when classifying futures e-mails.

In case you want antispam system to execute training of spam and antispam message boxes click in **Learn** button. It is common that the administrator schedule training of antispam in next section, **Learning**.

Note1: Remember that, when forwarding e-mails for **spam@default.com** and **nospam@default.com**, accounts that should be made forwarding wanted e-mail as **attachment** and not in e-mail's body. Example: You received an e-mail marked as *****POSSIBLE SPAM*****, and you verified that this e-mail is really a **SPAM** and wants to send it for Nettleon to learn this e-mail like a **SPAM**. Then, click in e-mail with right button (*in case of Outlook Express*), and select option "forward as attachment". Soon after it continues with normal e-mail sending procedure;

Note2: Sees in your e-mail client how to forward an e-mail as attachment.

12.6.2 Learning

In this section, administrator will configure training system schedule of Nettleon antispam and will have information regarding such trainings.

Scheduling

Here, administrator is going to schedule antispam system training, defining in which period it will be executed. The available options are:

- Daily: daily training, administrator defines training schedule;

- Weekly: weekly training, administrator defines day of the week in which the training will be accomplished, besides the schedule;
- Monthly: monthly training, administrator defines the day of the month in which the training will be accomplished, besides the schedule.

Schedule

Frequency: Select...
 Day: Not applicable
 Time range: 00 : 00

Save settings

Back Items

Figure 12.18: Learning Schedule

Historical

In this section, administrator will obtain an accomplished trainings report by antispam system, with information such as:

History

Date	E-Mail	Total	New	Status
09/04/2008	No spam	100	90	
09/04/2008	Spam	10	8	
08/04/2008	No spam	2	1	
08/04/2008	Spam	10	9	
07/04/2008	No spam	0	0	
07/04/2008	Spam	22	22	
06/04/2008	No spam	0	0	
06/04/2008	Spam	0	0	
05/04/2008	No spam	1	1	
05/04/2008	Spam	0	0	

Previous (1...10 of 14) Next

Back Items

Figure 12.19: Historical of trainings accomplished

- spams' number and no-spams trained;
- amount of new spams and antispams;
- training status, if successful or unsuccessful.

12.6.3 Whitelist

There is also a possibility to define a list of users called reliable, that can send messages that overcome sensibility limit and even so don't be classified as spam. This is system whitelist.



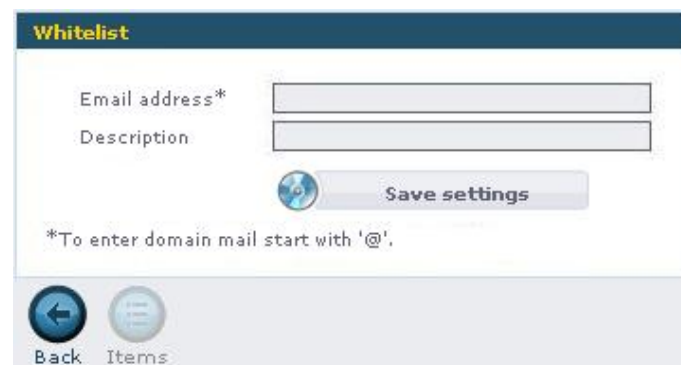
Mail address	Description
commercial@yourpartner.com	Commercial Department of your Partner
marketing@yourpartner.com	Marketing Department of your Partner
@yourcustomer.com	Domain of your Customer

Page 1 of 1 Go to .. 3 record(s)

Back Add Edit Items Del

Figure 12.20: Antispam Whitelist


To add an e-mail in *WhiteList*, click in **Add** button. In the screen that will be exhibited, type the complete e-mail address and without errors and a description that defines what refers this e-mail. At the end clicks in **Save Settings** button as display illustration 12.21.





Whitelist

Email address*

Description

 **Save settings**

*To enter domain mail start with '@'.

Back Items

Figure 12.21: E-mail Inclusion in Antispam Whitelist

12.7 Reports

12.7.1 Queue

All messages that were sent for Nettion e-mail users go by a queue to be processed and, definitively, transmitted to your addresses. While they wait processing, these messages are in a queue that is accessible so administrator can verify it, according to illustration. It is possible apply filters to queue search, and with that to obtain origin and destiny of e-mail, the number of delivery attempts, size and time that e-mail entered in line.

Emails Queue

Source:

Destination:

Attempts:

Size bigger than: KBytes

Date: 19/06/2008 19/06/2008 (dd/mm/yyyy)

Search

Source	Destination	Attempts	Size	Time
john@yourcompany.com	patynha400@hotmail.com	1	1,048,00 KBytes	10/04/2008 09:55:21
anna@yourcompany.com	patti97@donin.com	10	2,13 KBytes	10/04/2008 07:25:45
bruce@yourcompany.com	panoramictubo@iifl.org	3	2,15 KBytes	10/04/2008 15:57:30
richard@yourcompany.com	oycioyak_1992@STUDIOART-C.RU	12	1,89 KBytes	10/04/2008 02:29:45
joseph@yourcompany.com	ricardo.wrf@hotmail.com	1	1,048,00 KBytes	10/04/2008 09:55:21
george@yourcompany.com	comercial@empresaooff.com	1	453,09 KBytes	10/04/2008 07:27:13

<< < > >>

Page 1 of 1

Go to ..

6 record(s)

Back

Edit

Items

Del

Figure 12.22: E-mail Log Registers

12.7.2 Logs

After processing of a queue message, it is made a register of what happened with it. In the screen above, the message status is seen, if it was given with success or if there was some problem in the delivery.

12.7.3 Auditing

In auditing, there is a list of all messages that went by server. The auditing option makes possible that administrator visualizes a copy of each processed message.

Auditing emails

Source:

Destiny:

Date: 17/06/2008 17/06/2008 (dd/mm/yyyy)

Search

Source	Destiny	Time
john@yourcompany.com	alexander@yourcompany.com	09/04/2008 07:06:26
mary@yourcompany.com	alfred@yourcompany.com	09/04/2008 04:50:30
joseph@yourcompany.com	washington@yourcompany.com	08/04/2008 22:40:15
phillip@hotmail.com	gerald@yourcompany.com	09/04/2008 06:59:01
freddy@yourcompany.com	mary.d@yahoo.com	08/04/2008 22:31:43

<< < > >>

Page 1 of 558

Go to ..

27894 record(s)

Back

Edit

Items

Del

Figure 12.23: Messages Auditing

12.7.4 Quarantine

The quarantine works in a similar way of auditing, keeping all e-mails that are contaminated with virus. It is also allowed that administrator visualize a copy of each quarantine message.

It is also possible manage quarantine, excluding or liberating captured e-mails. For that, in exhibited report of illustration 12.24, select e-mail which you want to Del or to liberate and click in **Edit** button. The retained e-mail will be exhibited.

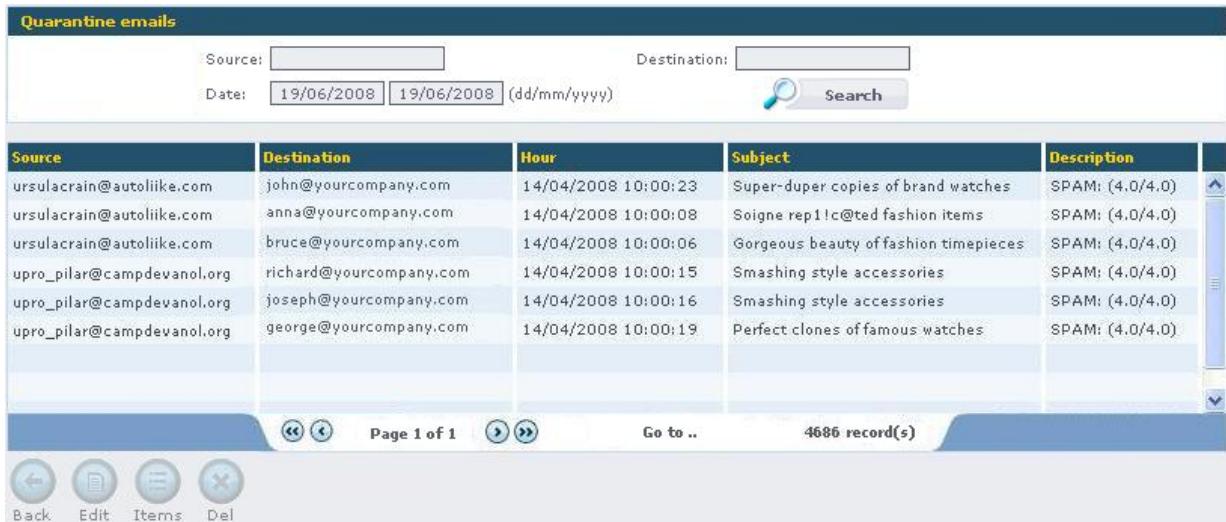


Figure 12.24: Quarantine of Messages with Virus

Below, the text of retained e-mail as displays illustration 12.25. In this screen, it is possible to see retained e-mail and decide for deleting or liberate it to be delivered to your address through the buttons “**Delete**” ou “**Liberate**”.



Figure 12.25: Liberate/Delete of Retained E-mail in Quarantine

Click in “**Delete**” button to exclude message of quarantine definitively or in “**Liberate**” button to remove the message of the quarantine and to deliver it to your address.

Note: To exclude message from quarantine, it is not necessary to edit it, because “Delete” button is also available in quarantine screen as displays illustration 12.24.

12.7.5 Top Mail

The access graphics in E-mail module can be visualized. With that, administrator follows which user sends more e-mails and which generates more traffic in e-mail server. See in illustration 12.26 that follows:



Figure 12.26: Top Mail Graphic

Chapter 13

Tools

All the tools possess a same interface, but each service is applied by your defined functions, as following described:

13.1 Reverse

This option exists to identify which domain refers an IP or which IP refers to a specific domain.

In case administrator fills out “IP/HOST” field with an IP, the result will be your equivalent domain.

- Example.1: IP/HOST: 200.200.200.1. Return: 200.200.200.1 -> www.test.com
- Example.2: IP/HOST: www.test.com. Return: www.test.com -> 200.200.200.1



Figure 13.1: Names Resolution

13.2 Whois

Whois will give you the cadastre report of a respective IP or domain in FAPESP. This report can also be printed.

13.3 Ping

The ping is used to check if a certain machine it is connected and linked. This process, as others of this section, is quite simple: fill out the field IP/HOST with IP to be tested.

13.4 Route Trace

To know which is path for a certain machine (IP), fill out IP/HOST field and wait the report of route traveled to reach it.

13.5 DNS Diagnosis

In this section, administrator can execute a DNS diagnosis that will show information regarding SMTP servers, list of names and IPs, nameservers list and host authority. The consultation can be made using Host IP address or its name.

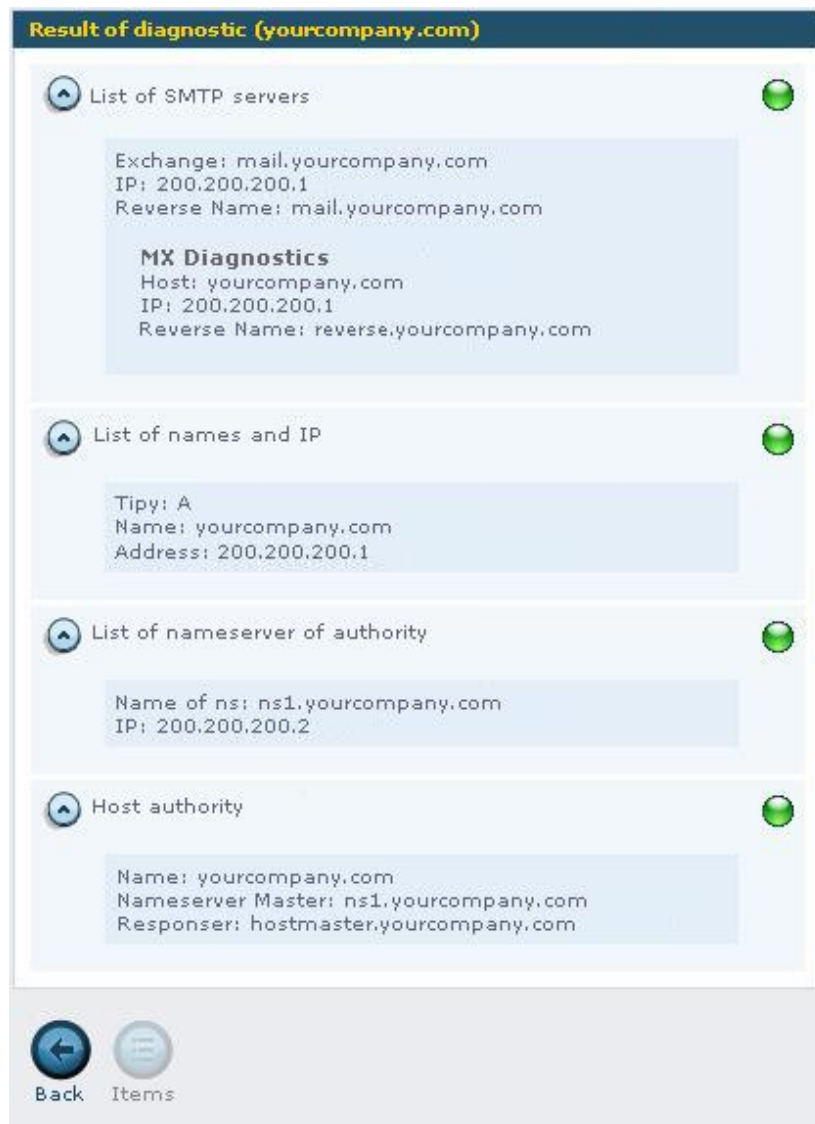


Figure 13.2: DNS Diagnosis

Chapter 14

System

14.1 Services

Through this option it is possible to visualize in one screen the **current state** (*status*) of all services supplied by Nettion, it is also possible to begin or stop any service. For that, click in the option **System** → **Services** to have access Nettion services list. Will be exhibited the *current status* of each service (if Started or Stopped), and option of alteration of its status.

There is also the possibility of making it start with Nettion through “Auto” option. See illustration 14.1.



Figure 14.1: Services List

The **Action** column will present three buttons for each service: *Start*, *Stop* and *Restart*, with which administrator can initialize, stop or restart the respective service. In case a service is in operation, will appear activated the buttons **Stop** and **Restart**. In case it is stopped, only **Start** button will appear active. Remember to click in **Apply changes to selected items** button if you had change the checkbox in “Auto” column .

14.2 Plugins

For more detailed information on *NettionPlugs*, see Chapter 15.

14.3 Backup

Nettion® is a system that provides many services, of which some are plenty critical. Such services require a great amount of information and settings. The damages caused by possible loss of such information can be, depending on the case, incalculable.

This way, reinstall and reconfigure everything, in an emergency moment, would be a plenty harmful process. Being considered this factor, was created a form of system backup that makes possible the immediate restoration of all information and existent configurations in Nettion and the return to its normal operation.

The process consists in the creating of a compacted file containing system data, as well the capability of sending a backup copy for a machine of your net through a shared Windows network. Administrator can configure the backup file content, which can contain Nettion logs, e-mails, besides your configurations.

The backup is automatic in agreement with the periodicity previously configured by Administrator. Still are possible to make a manual backup.

14.3.1 Settings

Modules

To access Nettion Backup service, access menu **System > Backup > Settings > Modules**.

In the screen that will be exhibited, it is possible to select wanted modules which will enter in backup file. To end, click in **Save Settings** button.

Remember that, as more modules you select, as space in disk will be necessary, mainly when selecting e-mail modules and some types of system logs.

The illustration 14.2 to proceed, exhibits the screen of Nettion backup modules selection.

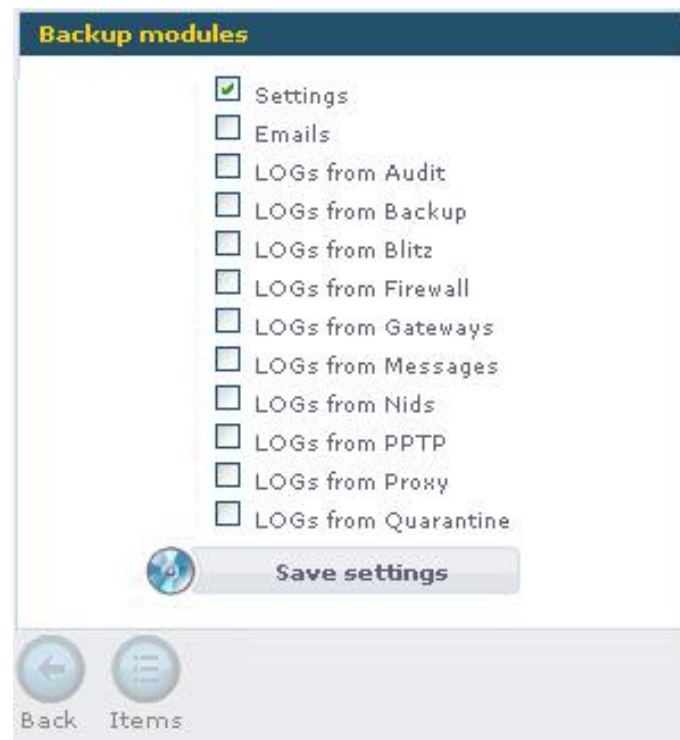


Figure 14.2: Modules for backup

Storage

Besides the Nettion backup file, it is also important to create a copy of this file in another machine of your net, because the backup can be easily stored like this in digital media, creating backup packs. For that, click in **Storage** option and fill out the fields as presented description below:



Figure 14.3: Windows Shared Network

- Host: machine name on network where file copies will be made. Example: backup
- IP: Corresponding IP of “backup” machine. Example: 128.0.0.21
- Shared Folder: shared folder name of machine. Example: bkpnettion
- User¹: user’s login with permission to write in these directories. Example: Backup.

- Password: password to accomplish shared access. Example: password. Note: The password appears under mask (*****)

At the end, click in **Save Settings** button, as display the illustration 14.3.

Schedule

In illustration 14.4 ahead, the screen is exhibited where you define the interval with that the backups will be accomplished, specifying:

- Frequency: interval of backup accomplishment: daily, weekly or monthly. Example: weekly
- Day: week day or of the month in that backup will be accomplished. In case chosen interval has been “weekly”, will be shown week days (Sunday, Monday, Tuesday, [...], Saturday) in this option. In case it is “monthly”, it will presented the days of month (1, 2, 3, [...], 31). If chosen interval it has been “daily”, this option will be disabled. Example: Monday
- Schedule: schedule in that safety copy will be accomplished. Example: 01:00 A.M.



Figure 14.4: Configuring the interval with that backup will be made

To finish, click in **Saving Settings**.

14.3.2 Manual

We will imagine a case in that, after added configurations to product, administrator wants to accomplish a backup copy immediately, instead of wait for copy to be accomplished by schedule.

So, Select modules and begin backup clicking in **Start Backup** button.

¹In case Nettion is synchronized with a Windows Domain, indicate a valid user/password for the domain e ensure yourself that this user has writing privileges in the selected network share.

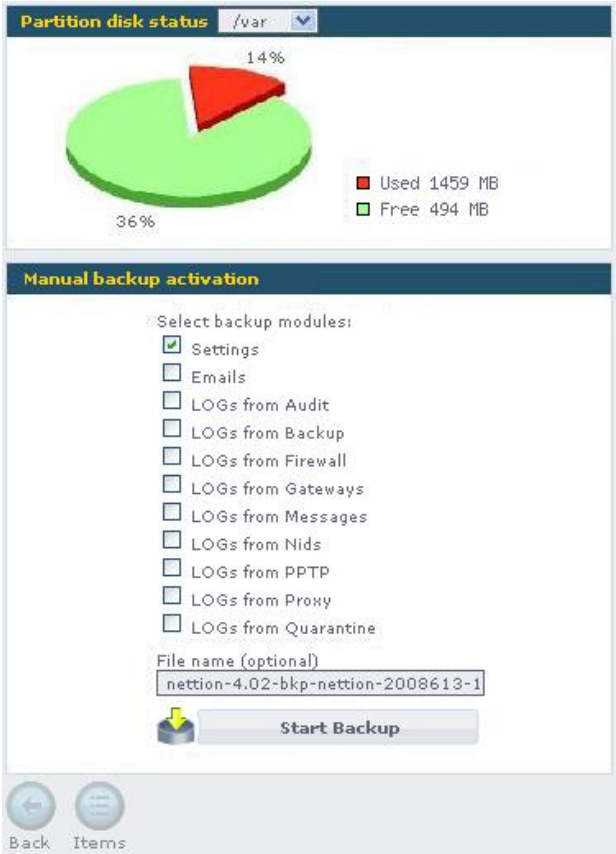


Figure 14.5: Manual Backup

14.3.3 Reports

History

The backup history will be exhibited with the following information: date, hour, file and status. The status can have a green or red light. The first, signaling that backup was successfully accomplished and the last, signaling that file writing was not successfully. If some problem happens with the backup, Nettleon will send an e-mail automatically to Administrator defined on product’s settings.

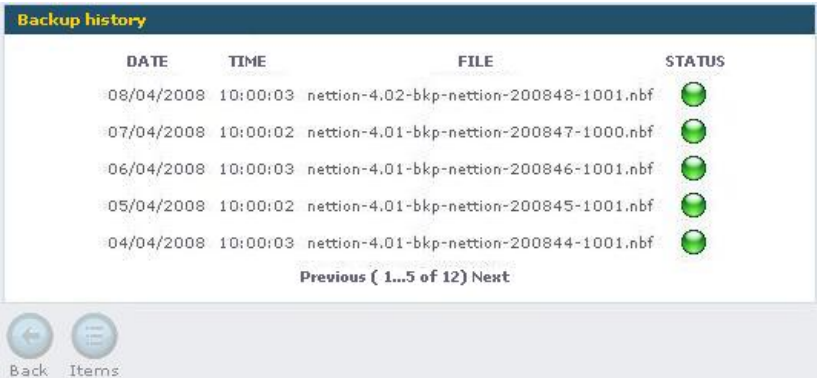


Figure 14.6: Backups History

14.4 Restore

The restoration process of a backup is quite simple. First, select backup file and click in **Upload** button. It is possible to select file, through **Search...** button, that will open a navigation window in folder, or to click in **Select File** button, that will present a list of safety copies available for restoration.

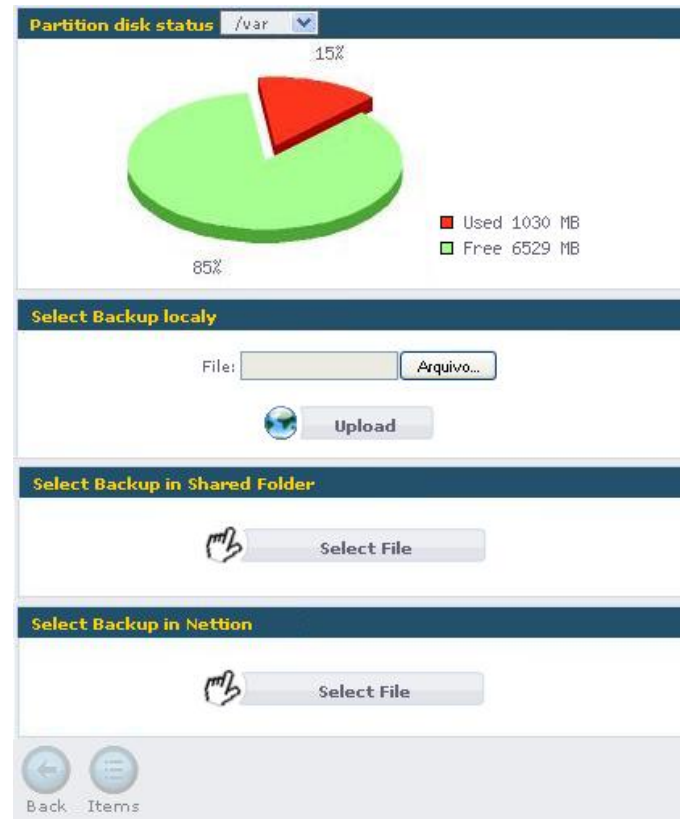


Figure 14.7: Restore

The administrator should select the wanted backup file and click in **Select** button.

Observation: Backup file should be in the same version of installed Nettion.

After file selection, for one of mentioned means, select between modules contained in backup which will be restored and, soon after, click in **Select modules**. Don't forget that the selected module(s) will be uncompressed and saved on machine overwriting current data existent for corresponding module.

ATTENTION: This is a very simple process, however, extremely critical, because, when recovering a backup, depending on the case, we will be overwriting the current system settings.

14.5 Pruning

The several services which run in Nettion constantly realize the activity registration, called *logs*. The size of log file(s) varies depending on users' amount, access permission and of amount of active services. With intention of liberating disk space, the oldest logs should be gradually deleted. This process receives the name of **Pruning**.

14.5.1 Settings

Disk Status by Partition

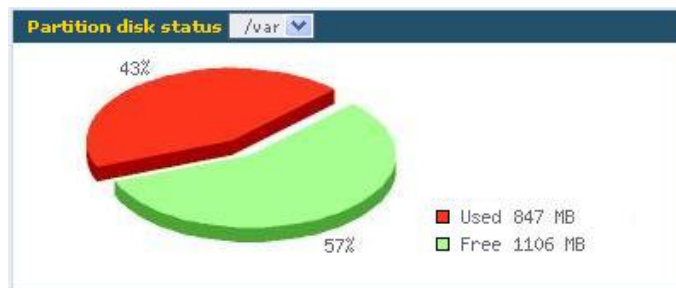


Figure 14.8: Disk Status by Partition

The picture shows a graphic by partition that presents:

1. In red, the disk used space;
2. In yellow, the free space for the use with your respective percentile.



Figure 14.9: Pruning Frequency Configuration

To configure automatic pruning, you should fill out the logs minimum interval that will be maintained and the modules whose logs you want to delete. After that, click in **“Start Pruning”** button and click on **“Start Pruning”** button. The pruning process will be started. The frequency choice depends on the accesses amount that company accomplishes and of used disk space.

14.5.2 Manual

Administrator can make, any time, a pruning differentiated of automatic pruning configured being enough to inform which are minimum interval for the logs that will be maintained and modules whose logs is wanted to delete. Soon after, click in **“Start Pruning”** button, to begin the pruning process.



Figure 14.10: Form of Manual Pruning Configuration

14.6 Update

For being a solution based on software, Nettion is in constant evolution. Consequently, new system versions are released, making available to administrator new tools that give more functionality to Nettion solution. Notification of updates is sent by e-mail to Nettion customers and they are also notified through superior bar of own software, that shows a message indicating the existence of a new available version for update.

Through update (menu System → Update), administrator checks the innovations of version released in relation to installed previous version. Learn how to Update your Nettion.

In update screen, we have two pictures: **Step 1 – Update Verify and Download** and **Step 2 - Select File for Update**. Clicking in **Check Updates** button, in following illustration, Nettion will check the existence of a newer version. In case there are not updates, the message **Without updating at the moment!** will be exhibited.

Otherwise, the most recent versions than will be listed, including the detailed information of each one of them.

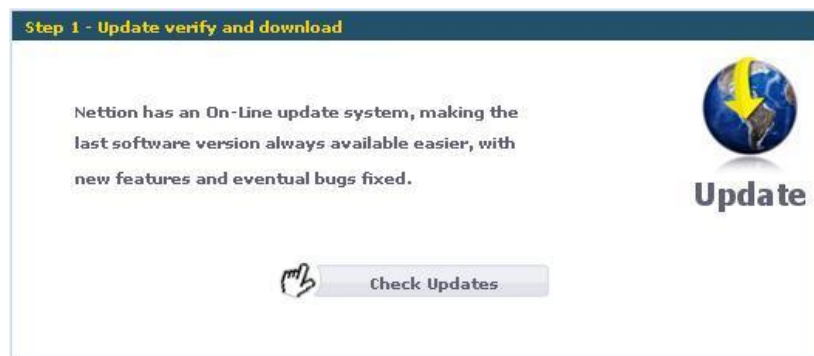


Figure 14.11: Check for Updates

The next step is to download the update file. For that, click in “Download” button. At this time, in agreement with your contract conditions, the update file will be supplied.

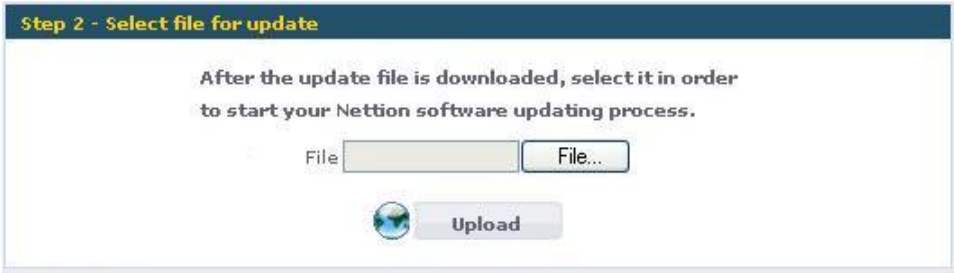


Figure 14.12: Update File’s Upload

Finished, return to previous page and begin the update selecting the new version file, through **Search...** button. After selecting it, click in **Upload!** and in the following screen in **Update** to begin it. The existent system settings will be maintained, in other words, all objects, groups, rules and other information will stay as previously. In case some consequence for the update exists, this will be informed with update on its information.

14.7 Graphs

Nettion offers graphs of your equipment resources consumption that are useful for evaluation of a possible machine overload. See the following graphics CPUs usage, Memory and Disks.

14.7.1 CPUs

In the CPU usage graphic, you can obtain a CPU usage history for “user” and for “system” inside of a time period, being also possible the accompaniment in real time clicking in “Start” button.

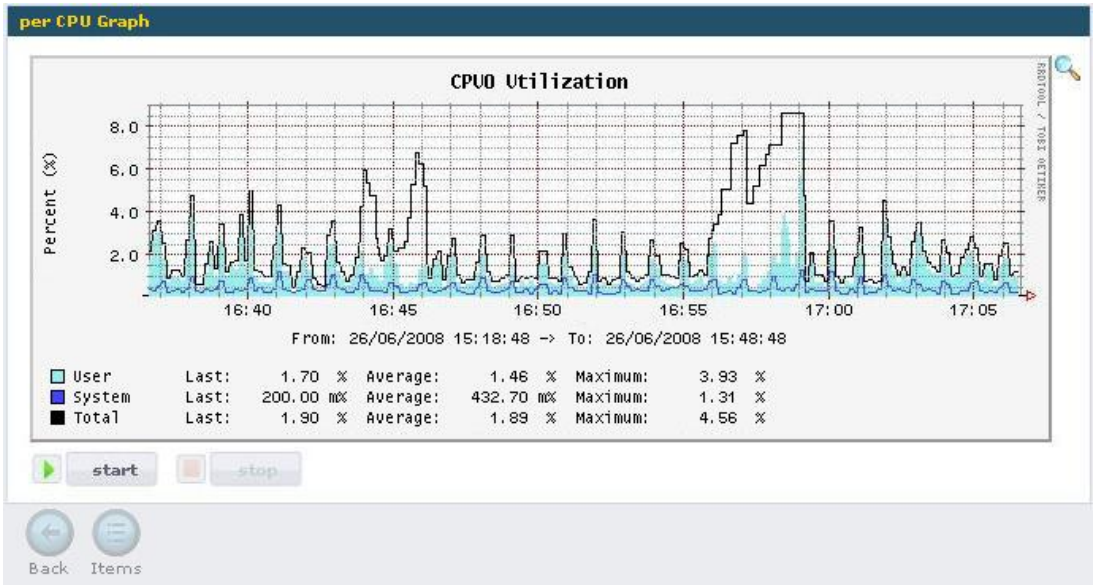


Figure 14.13: CPU Usage Graph

14.7.2 Memory

In memory consumption graph, you can obtain a consumption history so much of main memory as of SWAP memory inside of a time period, being also possible realtime accompaniment, for that click in “**Start**” button.

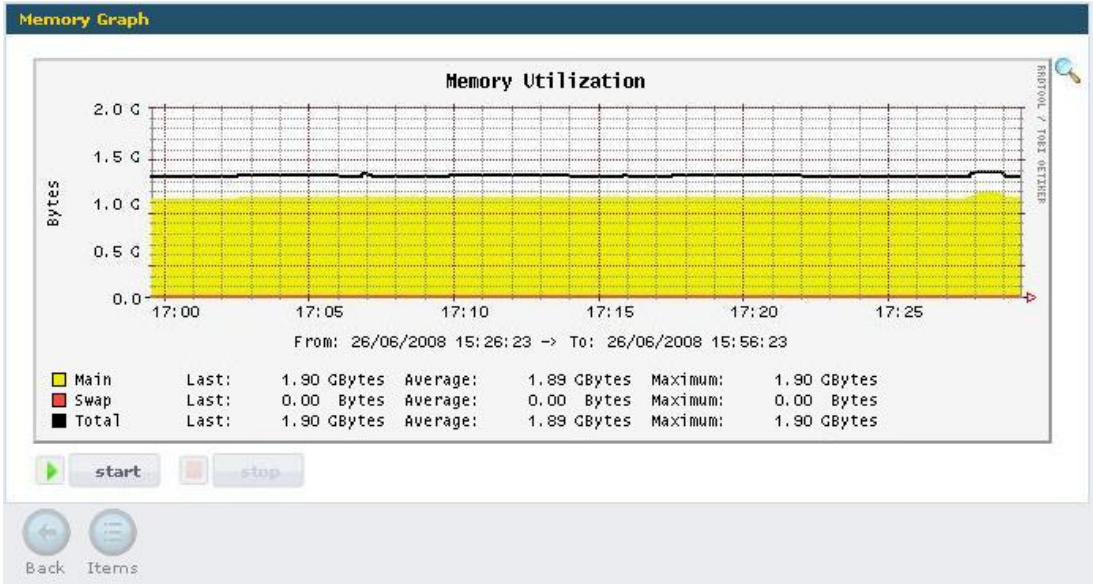


Figure 14.14: Memory Consumption Graph

14.7.3 Disks

In disk consumption graph, you can obtain a report of all read and written data inside of a time period, to see in real time, click in the “**Start**” button.

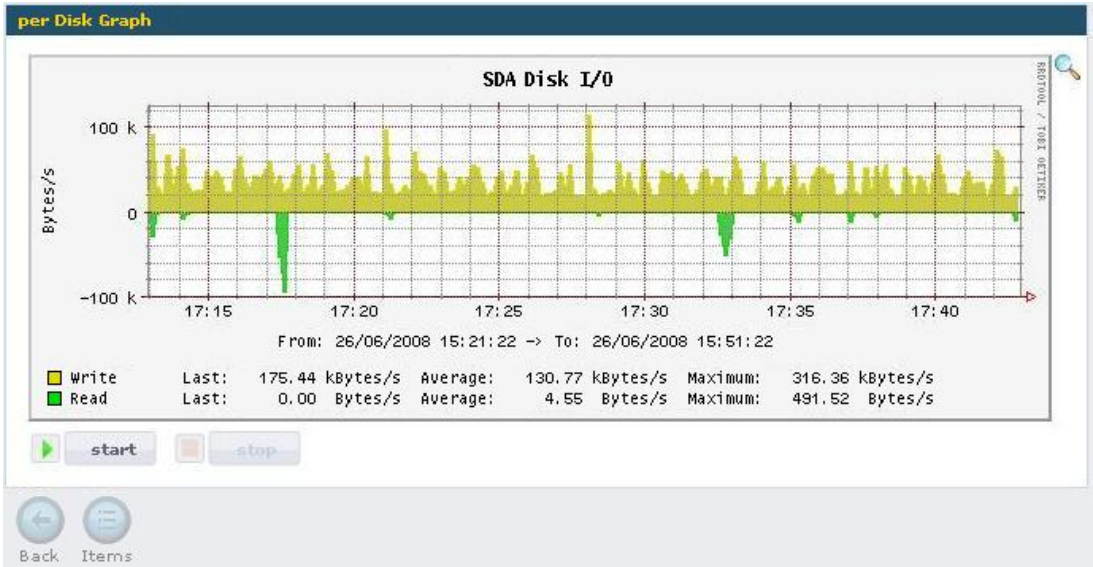


Figure 14.15: Disk Consumption Graph

14.8 About

Administrator will have access, in this section, to data referring Nettion’s license and version.



Figure 14.16: Nettion’s License Data

14.9 Audit

Daily, several operations are accomplished in **Nettion® Security Software** such as object changes, firewall and proxy rules, between others. To visualize and follow all the actions accomplished in Nettion, you can use audit service. It informs alteration date, module and sub-module that was altered, which action was accomplished, user and IP. Access Audit menu through “**System > Audit**”, according to illustration 14.17 bellow.

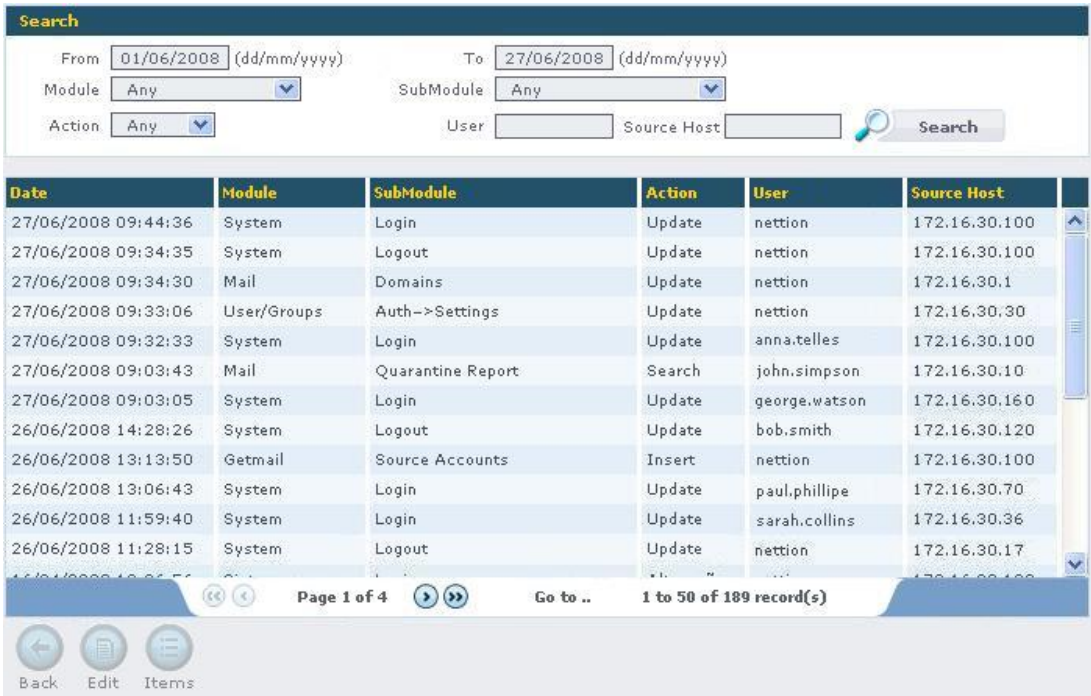


Figure 14.17: Audit of Interventions Accomplished in Nettion

Clue! Configure user's accounts so that system administrator has an own user account for product administration. Like this, the standard “**nettion**” user will be used exclusively by support team.

14.10 On/Off

In case there is need, administrator can restart or even turn off Nettion, selecting one of buttons of this topic.



Figure 14.18: Restart or Shut Down of Nettion

Chapter 15

NettionPlugs

15.1 What's NettionPlugs?

NettionPlugs® are additional functionalities (plugins) that NIS (Nettion Information Security) developed thinking about each customer's specific needs. Each NettionPlug has a different application. This way, you decide which plugin is most adequate for your business. Each plugin can be installed for evaluation by 15 days. After this period contact your Nettion reseller to acquire it.

The acquisition of NettionPlugs® is very easy. If your company already has Nettion®, it is enough to access "Systems" menu, to select "Plugins" option and install wanted functionalities. You still have **fifteen days totally free** to test applications efficiency.

15.2 Installing a NettionPlug

To do installation of NettionPlugs in your Nettion, access menu **System > Plugins**, according to displayed illustration 15.1 below and follow the steps:

Name	Description	Version needed of Nettion	Status	Action
Chat Server	Chat Server	3.85		 Install
Blitz	MSN Control	3.85		 Uninstall
OpenVPN	OpenVPN	3.88		 Uninstall
GetMail	GetMail	3.87		 Install
DNS	DNS Server	3.92		 Uninstall

Page 1 of 1 Go to .. 5 record(s)

Back Items

Figure 15.1: NettionPlugs Installation

- In the listing that will be exhibited, Nettion will show all available NettionPlugs by NIS;

- Click in “Install” button of wanted plugin. Observe that if your version is previous than requested for plugin, this option will be disabled. In this case will be necessary to update your Nettion before;
- After installation, the status will assume green color case your company has already acquired plugin license, or will assume orange color in case of an installation for evaluation.

Once installed, the plugin will totally work integrated with Nettion and will be available in menu, as well as other functionalities.

15.3 Chat Server

Chat Server® it's a NettionPlug developed by NIS to be the instant messenger (IM) of your company. The program uses **Jabber** as bases, known as the best system of IM for Linux.

Created in agreement of NIS quality, Chat Server possesses a dedicated server to send and receive internal messages. With that, you prevent the external users' addition and improve productivity in your company.

NettionPlug also allow communication with other networks of a same company. Besides saving phone bills you still guarantee the safety of messages sent and received, therefore application is not subject to virus infection and other common threats in internet.

15.3.1 Settings

Chat Server configuration is quite simple once your users and your authentication are totally integrated Nettion. With that, your organization Chat integration becomes still simpler and faster.

To configure it, access menu **Chat Server > Settings** of your Nettion. In following screen fill out the data, as shown below in illustration 15.2.



Configurations	
Domain	yourcompany.com
E-mail of administrator	admin@yourcompany.com
Interdace of working	All
 Save settings	

Figure 15.2: Chat Server Settings

- **Domain:** Your company's internet domain. This domain will be part of user's identification for Chat Server;
- **E-mail of administrator:** Administrator's E-mail in Chat Server;

- **Interface of working:** Indicate Nettion network interface that will receive connections. It is important to say that, if you select only your local interface, only machines of your local net will connect to Chat server. Therefore, if you select only your remote interface (interface connected to internet), just machines in internet will have access to Chat Server. Selecting All, both (local and remote) machines will get connected to Chat Server.

15.3.2 Client Software (Stations)

For that users access Chat, is necessary the use of some compatible software with *Jabber* protocol installed in your stations. The software to proceed is the most known and used for this:

- **Windows**
 - Pandion
 - Exodus
- **Linux**
 - Kopete
 - Gaim

Client software configuration

In client software configurations, insert internal IP of Nettion as being server and to user authentication make use of **username+@yourcompany.com**, where *yourcompany.com* is the used domain in server settings (see section 15.3.1). Ex: john@yourcompany.com. The password will be in agreement with Nettion integrated authentication, could be in own Nettion, in Windows Active Directory or a NIS server (Linux).

15.3.3 Firewall

So that net stations have access to server, it is necessary that you authorize it in Nettion Firewall. The port to be liberated, for default, is **5222** of **TCP** protocol. A summary of Firewall rule to be created follows below in table 15.1.

Rule: Internet → Nettion			
Source	Destiny	Destiny serv.	Action
Intranet	localhost	Chat Server ¹	Accept

Table 15.1: Chat Server Rule

Observe that this rule is contemplating access of internal net object to Nettion Chat Server. add other nets if necessary.

¹Create a service object to this port called “Chat Server” with port TCP 5222 – see Chapter 4 - Objects.

15.3.4 Launching the ChatSever Service

To start service, click in menu **System > Services**. Then click in “Start” button regarding “Chat Server” service. To maintain service always active in Nettion boot, mark “Auto” box and click in “Apply changes to selected items”.

15.3.5 More Information

You can also access Step by Step tutorial available in Nettion’s site (*www.nettion.com.br*) for more information of how to configure plugin server and clients.

15.4 Blitz

Blitz® is NettionPlug responsible for administration and control of MSN use in companies. It was developed for organizations that need to use IM for commercial contacts.

Besides controlling MSN permission levels for user or users’ groups, Blitz makes possible the contact list administration. This way, if your company needs to use IM to communicate with external contacts, with NettionPlug you guarantees that communication is established for appropriate ends.

Blitz is totally a web plugin (integrated with Nettion), in other words, it is not necessary a new hardware acquisition for your installation. Easily acquired, the application has an intuitive interface of simple administration through *wizard*.

The functionality was developed by NIS, seeking increase productivity of your business, as well as the reduction of band consumption and phone bills.

15.4.1 How It works?

Blitz works as a type of Proxy server (*Socks5*) that has the function of control MSN access of your net, making the whole access filtering. It is possible to establish, through its rules, which users will have access to MSN and even with which contacts they can communicate, besides the chats audit.

For that, it is necessary to block any other form of MSN access and to configure in stations (*MSN Settings*) Nettion as Socks server and Proxy obligatorily.

See how to avoid the MSN direct access.

15.4.2 Blocking MSN Direct Access

For default MSN software seeks several communication alternatives with your server in Internet, and to force your exit only by Blitz, it is necessary to block such alternatives of direct access.

In case the stations of your network are using Nettion Proxy, some settings should be made:

1. Block expression “*gateway.dll*”, and to do so follow these steps:

- Create an expressions objects group called “Block MSN”. Any doubt regarding how to configure expression objects, see Chapter 4 - **Objects**.
 - Add in this group the “*gateway.dll*” term as being of “word”, “no” to whole word, “any” position.
2. To create a Proxy rule blocking expressions group created above. Apply this rule to all users or to users that you want to block MSN direct access. Create this rule in first position to avoid that other more generic rule liberates access. Any doubt on Proxy rules, access Chapter 6 - Proxy. 6 - Proxy.
3. To liberate some URLs that MSN uses to do user’s authentication in your server. In the same way, create an expressions group called “Liberate MSN logon” and in it add the following terms as being of “regular expression” type:

- nexus.passport.com:443
- login.live.com:443
- loginnet.passport.com:443
- omega.contacts.msn.com:443
- storage.msn.com:443
- Install_Messenger.exe

4. To create other rule in Proxy liberating this expressions group. You can Allow for any user once the control will be in own Blitz. Create this rule in position 2, after “Block MSN” rule. Any doubt on Proxy rules, access Chapter 6 - Proxy.

It is also necessary create rules in firewall that blocks any access attempt to MSN through a possible net masking. For that, you should create in firewall a rule blocking the access of whole intranet (or at least of users’ IPs that should access through Blitz) to Microsoft networks (65.52.0.0/14 and 207.46.0.0/16) in ports 1863/TCP, 80/TCP and 443/TCP. This rule should be in upper positions, assuring that it stay above of any net masking (except for users’ masking that, by chance, don’t access MSN through Blitz) as display table 15.2.

Rule: Intranet -> Microsoft			
Source	Destiny	Destiny serv.	Action
Internal Net	Range MS1/Range MS2	msn/http/https	Drop

Table 15.2: Blocking the access to MSN through Masking

Note1: Before creating the rule, create “Hosts and Nets” objects containing the Microsoft ranges mentioned (for example **RangeMS1** and **RangeMS2**). For larger information on how to create “Hosts and Nets” objects, see the Chapter 4 – Objects.

Note2: Also create a service object with the door 1863/TCP called **msn**. For larger information on how to create objects of services, see the Chapter 4 – Objects.

Note3: **Http** and **Https** services should also be added in the blockade rule. See the summary rule in table 15.2.

15.4.3 Audit

All the chats accomplished through Blitz are audited. To accompany chats, click in menu “**Blitz > Audit**”, all chats will be exhibited by date. To visualize its content, select it and click in “**items**” button, as displays the illustration 15.3.

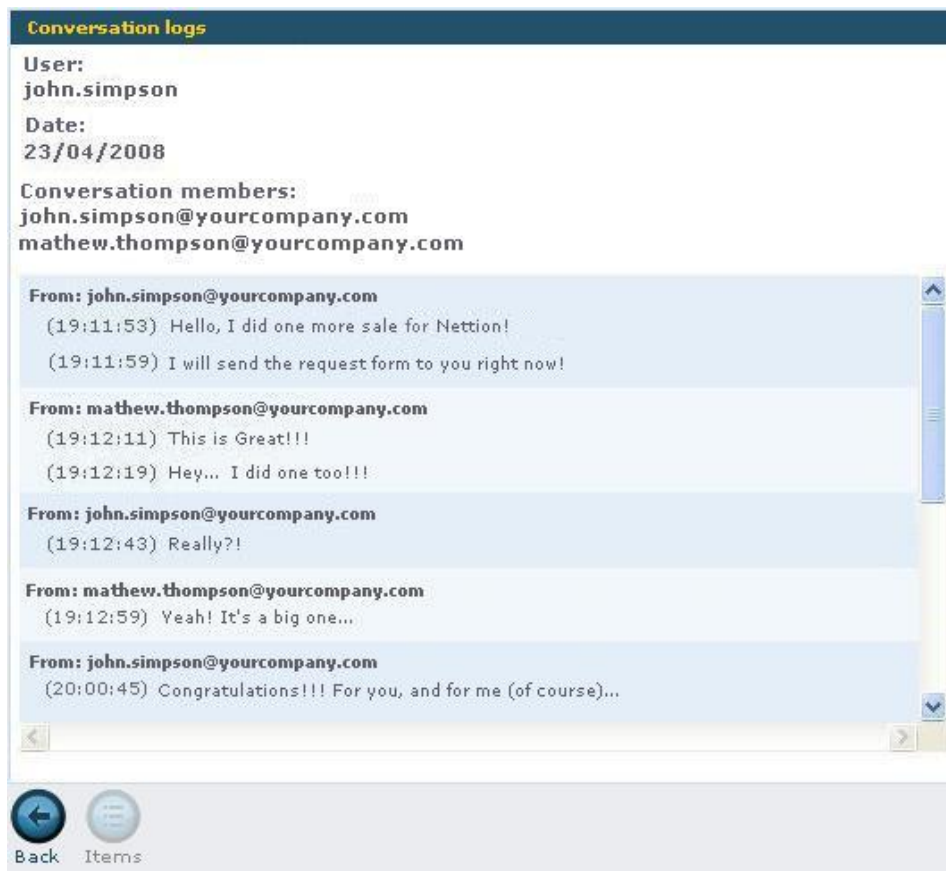


Figure 15.3: Chats Audit of Blitz

15.4.4 Firewall

Now it is necessary allow that own Nettion makes connections starting from Blitz service. For that it is necessary to create a rule liberating traffic starting on Nettion with destiny to port 1863/TCP, as it proceeds in summary rule in table 15.3.

Rule: Blitz -> Internet			
Source	Destiny	Destiny serv.	Action
localhost	Any	msn	Accept

Table 15.3: Liberating Blitz service

Note: before creating the rule, verify the existence of some rule that already contemplates this liberation, otherwise, create a service object with port 1863/TCP called msn before creating suggested rule. For larger information on how to create services objects, see Chapter 4 - Objects.

Besides this rule, it is necessary to liberate local net access to Blitz service, which works for default in **TCP 1080** port. See summary rule in table 15.4.

Rule: Intranet -> Blitz			
Source	Destiny	Destiny serv.	Action
Internal Net	localhost	blitz	Accept

Table 15.4: Liberating Access to Blitz

Note: before creating the rule, verify the existence of some rule that already contemplates this liberation, otherwise, create a service object with port 1080/TCP called blitz before creating suggested rule. For larger information on how to create services objects, see Chapter 4 - Objects.

15.4.5 Settings

As well as Nettion Proxy and Firewall, Blitz also possesses a default access politics. It will define what will be made in case user it is not inserted in some access rule, which will be seen more ahead.

Default politics is configured through menu “**Blitz > Settings**”. In this menu, it is also possible define if users will be informed that your chats are being audited and recorded. For that, mark option “**Apply notification in the beginning of the session**” as display illustration 15.4.



Figure 15.4: Basic Blitz Settings

The default politics is usually defined as “**Deny any access**” and through rules only users that really have to access MSN are allowed, as well as contacts with whom can communicate.

15.4.6 Automatic Cataloguing of Contacts

Through menus **Contacts** and **Groups** of Blitz you can manually insert contacts with whom your users will be able to communicate as display illustration 15.5.

Figure 15.5: Manual Inclusion of a Contact

However, Blitz offers an automatic way of cataloguing these contacts, which occurs when user makes your first¹ connection through Blitz.

This process makes easier the rules maintenance, as it will be seen more ahead.

In “*User Passports*” guide, it is possible see organized contacts for each *passport*. To see contacts of a passport, select it and click in “Items” button as display illustration 15.6.

Login	Name	Passports
john.simpson	John Simpson	john.simpson@yourcompany.com
kelly.watson	Kelly Watson	kelly.watson@yourcompany.com
mel.phillipe	Mel Phillipe	mel.phillipe@yourcompany.com
newton.smith	Newton Smith	newton.smith@yourcompany.com newtonbsmith@hotmail.com

Page 1 of 1 Go to .. 12 record(s)

Back Edit **Items** Del

Figure 15.6: Passport Contacts

15.4.7 Rules

Blitz wizard of rule creation is very similar to other Nettion services, like Firewall and Proxy. To create rules in Blitz, click in menu “**Blitz > Rules**” and follow these steps:

¹On next login Blitz makes only the maintenance of these contacts, adding or deleting, as necessary.

Step 1:

In list of rules screen, click in “Add” button, as exhibited in illustration 15.7.



Figure 15.7: List/Add Rules of Blitz

Step 2:

In Wizard first screen, define a description for the rule, an action, and a position (defines the rule priority order) and, finally, select the rule status, as exhibited in illustration 15.8 that follows.

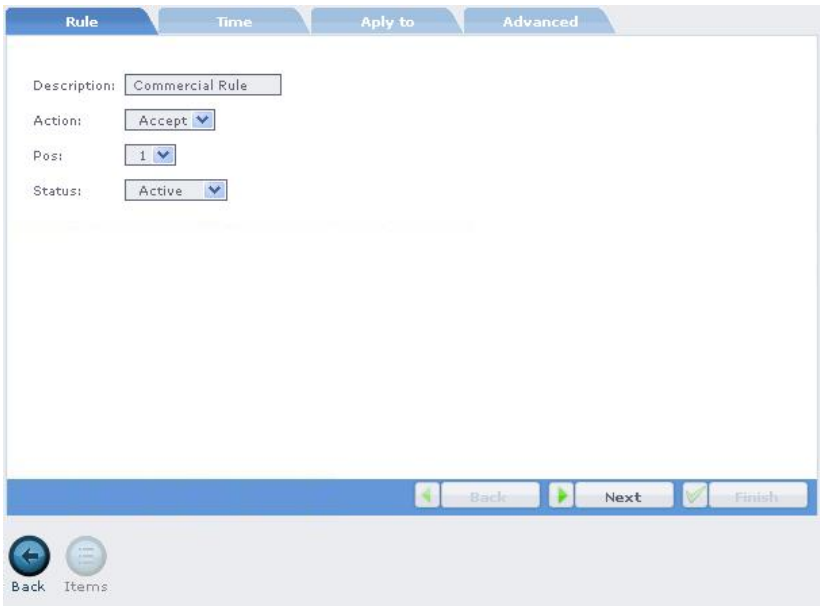


Figure 15.8: Rule Description of Blitz

Step 3:

In following screen, select schedule in that the rule will be applied, in agreement with schedules objects previously defined.

See illustration 15.9 below.

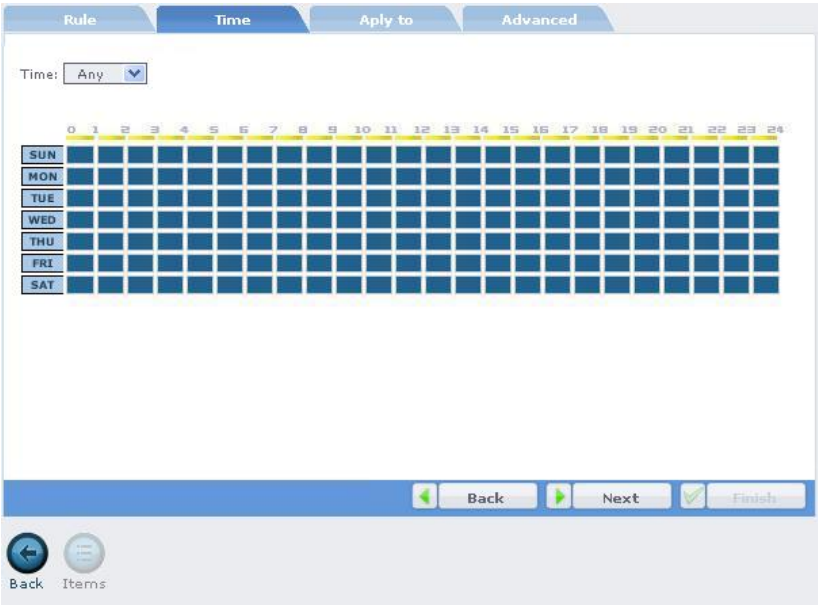


Figure 15.9: Selection of Schedule for Rule in Blitz

Step 4:

In this screen you had defined with which contacts the users can communicate. In “Source Filters” select the user(s), and in “Destination Filters” select the contact(s) allowed for that user(s). See illustration 15.10.

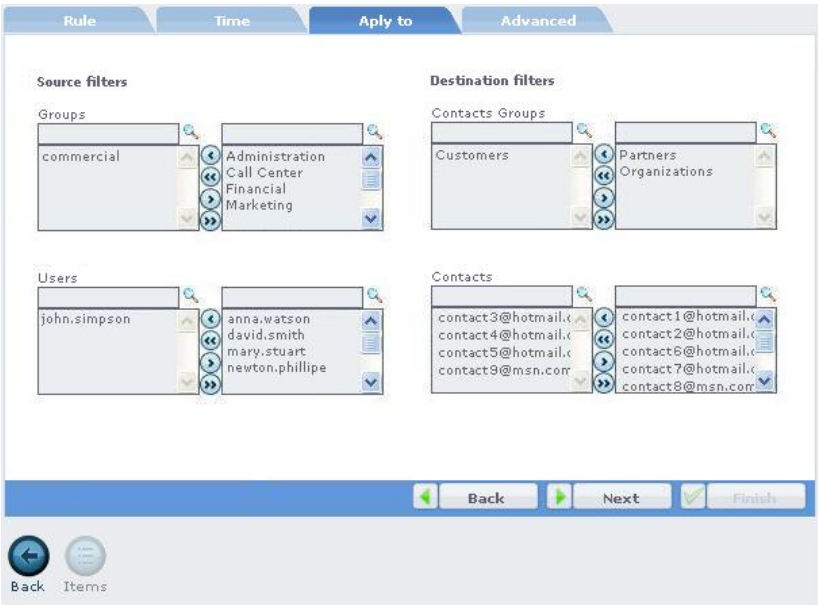


Figure 15.10: Users' Selection and Passports of the Rule

Step 5:

In last screen of Wizard, you define if will be allowed for the rule user(s) chat and/or transfer files with the selected contact(s). To create the rule click in “**Finish**” button. See illustration 15.11.

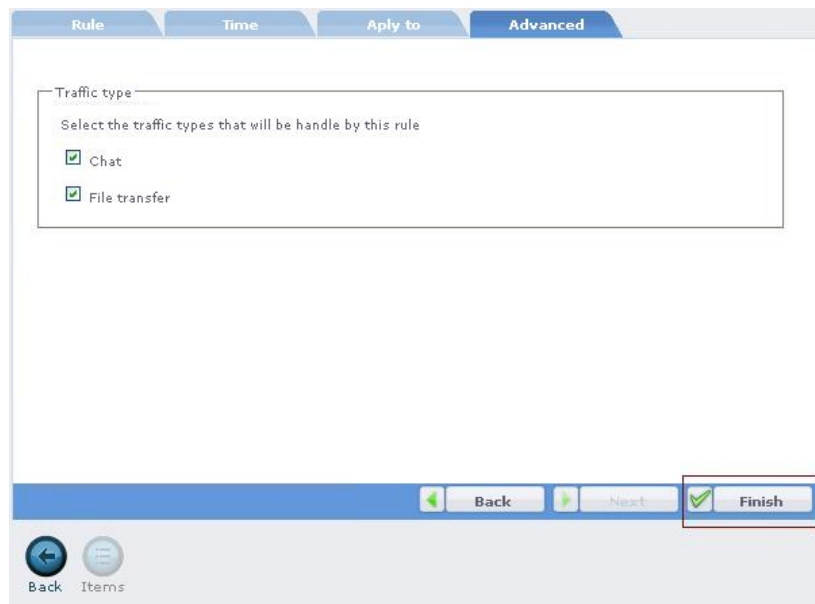


Figure 15.11: Definition of Activities Allowed through Blitz

15.4.8 Beginning the Blitz Service

To begin the service, click in menu “**System > Services**”. Later click in “Start” button regarding “Blitz” service.

To always maintain the service active in Nettion’s boot, mark box “Auto” and click in “Apply changes to selected items”.

15.4.9 Configuring the Stations

Now it is necessary to do stations settings, pointing in MSN the Nettion Blitz IP. Depending on MSN version, the place of configuration can change.

However, in a general way, you should indicate the **socks** and **http** server of your MSN. Normally the path is “**Tools > Options > Connection**”.

Point to Nettion’s IP the socks service and http proxy. It is necessary that you also indicate the user’s information authentication (user and password).

Note: Remember that the information about the configuration of your Proxy Server comes from “*Internet Explorer*”, this way, you can not put it here manually. You must put it in the Internet Explorer configuration, then it will appear in the MSN configuration.

This way, you must specify only the username/password for the Http Proxy.

See illustration 15.12 ahead.

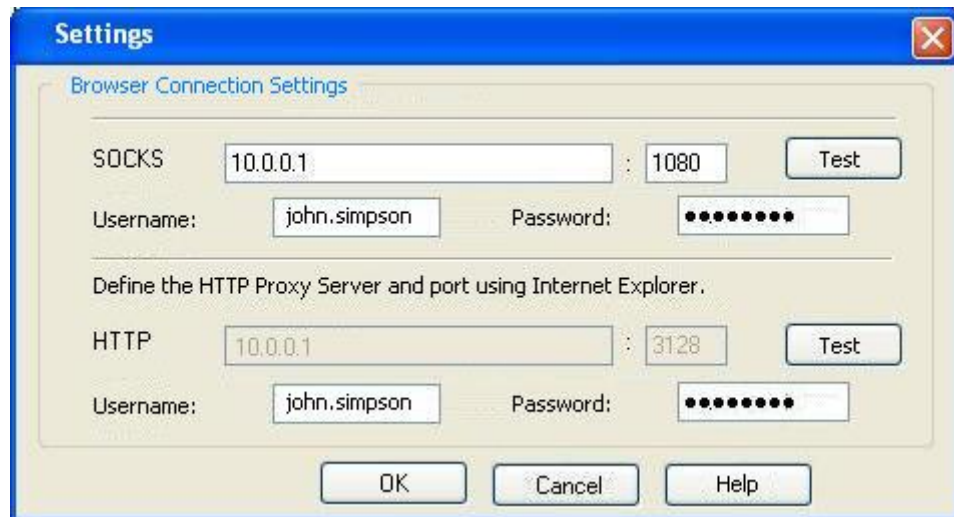


Figure 15.12: Settings of MSN Connection through Blitz

15.4.10 More Information

You can also access Step by Step tutorial available in Nettion's site (www.nettion.com.br) for more information of how to configure plugin server and clients.

15.5 OpenVPN

OpenVPN is one more form of VPN offered by Nettion. Through this resource you can interconnect nets between head office and other stores, or allow an external user to access the net in a simple and safe way. A great differential of OpenVPN is your possibility to operate even on internet with mask (NAT), as in nets of hotels, cyber-coffees or airports.

After installation (see topic 15.2 of this chapter), you access this plugin through the menu **"VPN > OpenVPN"** of your Nettion. It offers two types of connections as will be shown:

15.5.1 Nettion-Nettion

This option allows interconnect two or more networks through VPN (as interconnect subsidiary to head office). Each one with Nettion and OpenVPN Plugin installed. In this case, one of Nettions will be VPN server and the other will be client.

15.5.2 Configuring OpenVPN Server

To configure a Nettion-Nettion OpenVPN connections access the menu **"VPN > OpenVPN > Nettion-Nettion > Connections"**. The following screen will be exhibited:

Name	Local nets	Local IP	Type	Remote IP	Remote nets	Status	Action
Nettton Server	172.16.0.0	200.200.200.1		200.253.200.200	10.0.0.0 192.168.1.0		

Page 1 of 1 Go to .. 1 record(s)

Back Add Edit Items Del Reload

Figure 15.13: Listing of OpenVPN connections

To create a new connection, click in “**Add**” button. The following steps should be followed:

Step 1:

In the first page of Wizard define the following fields:

- Type: Server;
- Name: identify connections name;
- Status: Active;
- Port: Nettion already offers automatically a port suggestion. Each OpenVPN tunnel will work in a different port - remember to create a firewall rule that corresponds to this port to liberate VPN connection;
- Protocol: UDP (default);
- LZO Compression: apply to optimize traffic inside VPN with data compression.

See the following illustration:

Type of the tunnel

Net

Type:
Name:
Status:
Port:
Proto:
LZO compress:

Figure 15.14: Creation of OpenVPN Rule

Step 2:

In the following page defines:

- Local
 - IP: indicate IP/Hostname for which Nettion client(s) will find this Nettion;
 - Virtual IP: indicate a virtual IP for connection between Nettions after VPN establishment. Example: 192.168.200.1;
 - Nets: indicate the local net(s) that will connect with the remote net(s).
- Remote
 - IP: indicate the Nettion client's IP. In case it doesn't possess a static IP, leave this field in blank;
 - Virtual IP: this field will be filled out automatically;
 - Nets: indicate the remote net(s) that will connect with the local net(s).
- Click in **“Finish”** button to create the connection.

See the following illustration:

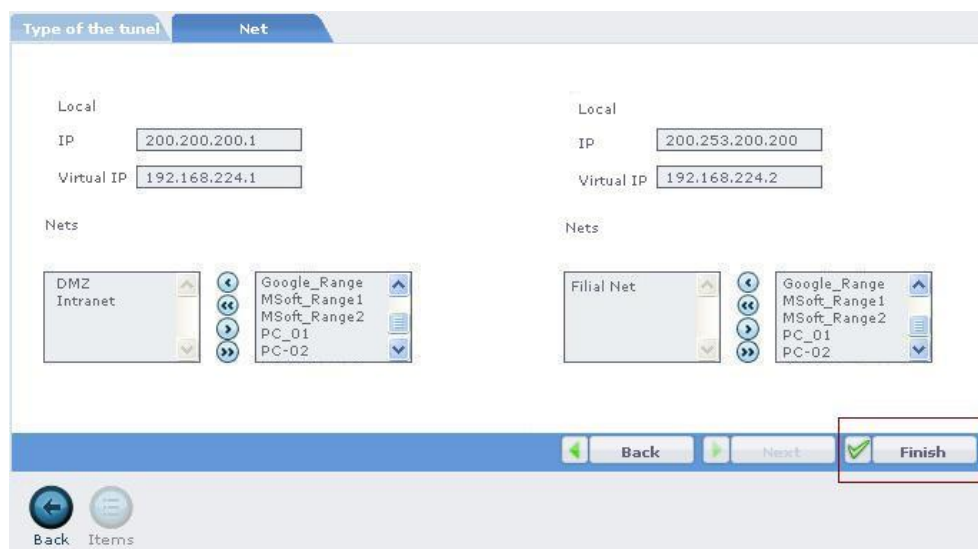


Figure 15.15: Definition of OpenVPN Connection Nets

Configuring the OpenVPN Client

Now that server is created, it is time to configure the Nettion client(s). To make this task easier, the Nettion server of VPN offers the file export that makes the entire client configuration.

To export the file, access Nettion OpenVPN Server, on connections listing and click twice in connection server that you just created. In the following screen, in “Export settings to Nettion clients”, define a safety password for the file and click in **“Export”** button. Soon after, save the file so that can be used in Nettion client configuration. See the following image:

Figure 15.16: Export of Nettion OpenVPN Client Settings

Now, access the Nettion OpenVPN Client and follow these steps:

- Access the menu “**VPN > OpenVPN > Nettion-Nettion > Connections**”;
- In the following screen, of connections listing, click in “**Add**” button;
- In the first page of Wizard define the following fields:
 - Type: select the “Client” type now;
 - Name: indicate a name for the connection;
 - In “Import Settings”, select the file exported by server, insert the file safety password and click in “Import”. At this time Nettion will import all necessary configuration of connection.
 - Click in “**Finish**” button accordingly to the illustration.

Figure 15.17: Import OpenVPN Configuration File

Firewall

As commented previously, each OpenVPN tunnel works in a different port, in agreement with your setting in the moment of creating the server tunnel. For the connection establishment, liberate in your Firewall the connection between the servers in the used ports.

Supposing that server is configured for port 1184/UDP, create a service object with this port and create a Firewall rule as shown in table 15.5:

Rule: Liberating OpenVPN server			
Source	Destiny	Destiny serv.	Action
OpenVPN Client	localhost	openvpn1	Accept

Table 15.5: Access OpenVPN server

In this case, we are just liberating for ClientOpenVPn object to connect the server. In case it is not possible to identify the connection origin, leave the source in “Any”.

Besides the rule to allow the interconnection between Nettions, it is also necessary to liberate the traffic between VPN nets in agreement with your needs. See summary of necessary rule in table 15.6.

Rule: Liberating Traffic on VPN			
Source	Destiny	Destiny serv.	Action
Local Net	Remote Net	Any	Accept

Table 15.6: Liberating Traffic Inside of VPN

Launching OpenVPN Service

Now that server and client are properly configured, launch OpenVPN service in each Nettion (server and client) in menu “**System > Services**”.

At Last, launch the tunnel. Through connection listing screen click in “Start” button correspondent to the created connection to begin the tunnel between Nettions (See topic 15.5.2). At this time connection indicative status should be green and the net stations can already communicate to each other. In case not, verify if you didn’t forget some step above.

15.5.3 Nettion-Users

This OpenVPN modality allows safe connection of external users to your organization. Through the established tunnel the users can have access to net resources as share, systems, printers, in agreement with adopted safety’s politics, as if they were locally connected to the net.

As commented previously, one thing that differentiates this plugin is its possibility to operate even in internet atmospheres with net masking (NAT), as in nets of hotels, cyber coffees or airports. Other important characteristics are its configuration easiness, as much server as clients, flexibility to users’ authentication, which operates together with Nettion centralized authentication.

15.5.4 Settings

To configure OpenVPN server access the menu “VPN > OpenVPN > Nettion-users > Settings ” and follow these steps:

Step 1: In the first page of setting screen configure the following items:

- Status: indicate the server status - Active;
- Connection name: indicates a connection name - Nettion will already make a suggestion;
- Default interface: here you can choose a specific interface (the one that possesses public IP) or “All” to wait for connections in any interface;
- Server IP: indicate IP through which your Nettion will be found by clients. It will usually be your Nettion public IP, but in situations where Nettion is being masked (NAT) for a router, for instance, indicate router’s public IP;
- Virtual network - Net that will be created between Nettion and connected users.
 - Network: will be the virtual network - Nettion will already making an automatic indication;
 - Mask: indicate the net mask - Nettion will also indicate;
 - Server IP: will be inside Nettion’s IP on virtual net;
 - Clients IP: it will be IPs’ interval that will be supplied by VPN clients.
- Nets accessed by users - Nets in which Nettion supplies access for connected users;
 - Select for the left column the local nets that will be offered to VPN users;

See the following illustration:

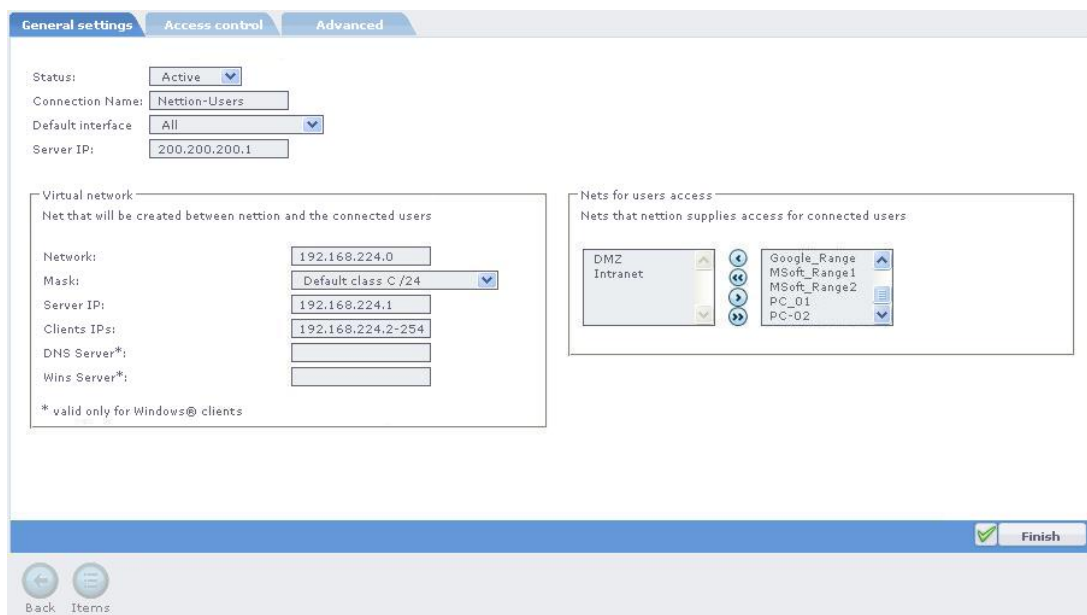


Figure 15.18: Nettion-User Connection Settings

Step 2: In Access Control indicate:

- By default net valid users (authenticated) will have access. But it is possible to specify which users will have access. For that, select the option “Allow only selected users”;
- In Users/Groups, specify which groups and/or users will have access permission. As said previously, the users will be authenticated, in the moment of connection, in indicated base in Nettion Centralized Authentication System.

Note1: To create a user and give OpenVPN access, it has to be created before the creation of Open VPN rule. For that see how to proceed to create user on Chapter 5 of this manual;

Note2: It's recommended that be selected ONLY users which must have access to VPN to avoid users' malicious intentions;

Note3: We recommend the use of 'strong' passwords, in other words, passwords that contains letters (majuscule and minuscule), numbers and special characters.

See the following illustration:

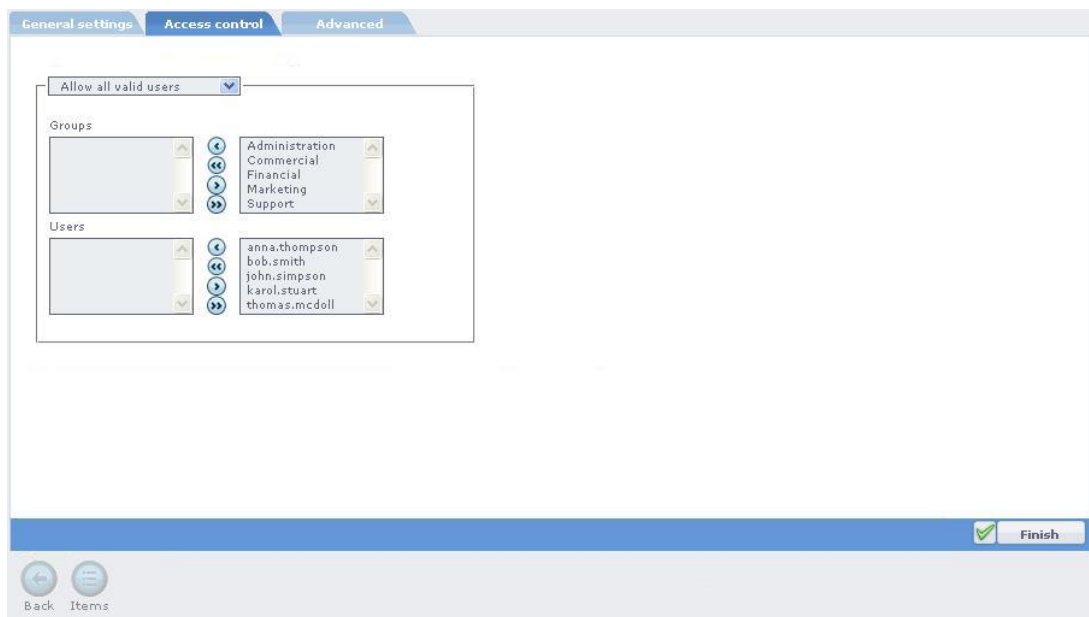


Figure 15.19: Selection of Users for Access Through OpenVPN

Step 3: In Advanced indicate:

- Port: Nettion already suggests the connection port;
- Protocol: default protocol is UDP;
- LZO Compress: use compression to optimize traffic inside of tunnel;

- Type of Server: use Tunnel option for point-to-point (default) or Ethernet for connection similar to a common net;
- Accept Connects: by defaults the connection between clients it's allowed (YES).

See the following illustration:

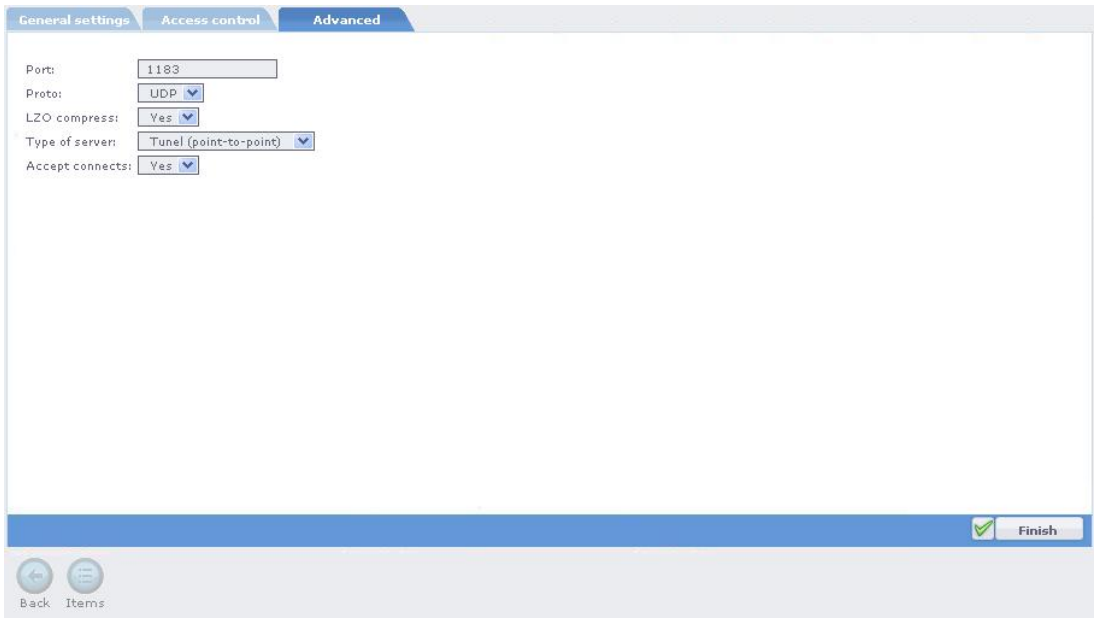


Figure 15.20: Advanced Specifications of OpenVPN

15.5.5 Active Connections

In active connections will be listed VPN connections now established to Nettion. In listing it is possible to identify user's name, date and time in that connection was established and it is also possible to disconnect user through the button "Stop". See Illustration 15.21.

User	Start Date	Start Time	Action
 john.simpson	22-04-2008	09:17:45	
 karol.smith	22-04-2008	08:10:55	

Page 1 of 1Go to ..2 record(s)

BackItems

Figure 15.21: Active Users List

Reports

Em “VPN > OpenVPN > Nettion-Users > Reports > Connections” you have access to connections report history made to OpenVPN server. Through filter it is possible to do detailed searches on done accesses, as shows the following illustration 15.22.


Search						
User	From (Date)	To (Date)	Virtual IP	Remote IP	Interval	
<input type="text"/>	<input type="text" value="01/04/2008"/>	<input type="text" value="22/04/2008"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="40"/>	 <input type="button" value="Search"/>
User	Start Date	Start Time	Stop Date	Stop Time	Remote IP	Virtual IP
User01	21/04/2008	19:31:51	21/04/2008	22:27:11	200.200.200.1	172.16.32.18
User02	19/04/2008	14:25:56	19/04/2008	16:03:57	200.200.200.54	172.16.32.2
User03	18/04/2008	16:45:54	18/04/2008	17:09:16	200.253.177.130	172.16.32.6
User04	16/04/2008	09:31:59	16/04/2008	09:52:07	200.200.253.200	172.16.32.2
User05	15/04/2008	04:14:23	15/04/2008	04:23:36	200.200.200.89	172.16.32.2
User06	03/04/2008	21:51:18	03/04/2008	22:17:35	200.200.200.198	172.16.32.6
Previous (1...36 of 36) Next						

Figure 15.22: VPN Access Report

Firewall

So that external users can be connected to Nettion its necessary to allow it in Nettion Firewall. Create a rule allowing access for Any host (Internet) in Nettion’s direction in the established server port.

Supposing that server is configured for default port, 1183/UDP, create a service object with this port called openvpn-clients, and create a Firewall rule as shown in table 15.7:

Rule: Liberating OpenVPN Server			
Source	Destiny	Destiny serv.	Action
Any	localhost	openvpn-clients	Accept

Table 15.7: Access to OpenVPN Server

Besides the rule to allow clients interconnection to Nettion, it is also necessary to liberate traffic between allowed local nets and the configured virtual net. See summary of necessary rule in table 15.8.

Rule: Liberating Traffic Inside VPN			
Source	Destiny	Destiny serv.	Action
Local Net	Virtual Net	Any	Accept

Table 15.8: Liberating Traffic inside VPN

Note: “Virtual Net” object corresponds to IP established in OpenVPN server settings – see section 15.5.4.

Starting OpenVPN Service

Open OpenVPN server through menu “**System > Services**”. To obtain more information about how to start Netion services, see topic 14.1.

Clients' Settings

In Windows client stations, download and install “OpenVPN Client” software. Installation in stations is quite simple and follows installing software pattern for this platform.

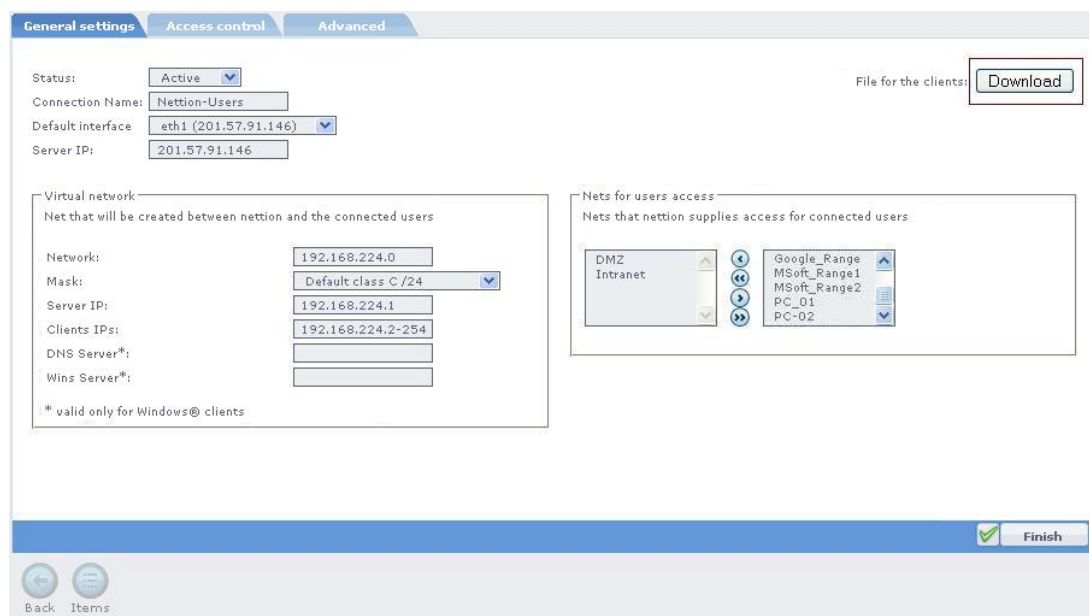


Figure 15.23: Export Settings for OpenVPN Client

Once installed, it's time to do proper settings. To make this task easier, Netion VPN server offers the file export that makes all settings of clients. See illustration above.

To export this file, enter again in OpenVPN Netion-users' settings and click in “download” option. If this option is not still available it's because server configuration was not still made.

Now, in Windows station, with *OpenVPN Client* installed, click with the right button in OpenVPN Client icon and choose “New Connection (Nettion)” option. In following window, select exported file by Nettion. With that settings will be concluded.

Note: After installation, see that a new icon will appear on windows clocks left side on Start menu.

See the following illustration that shows how to import the configuration file:

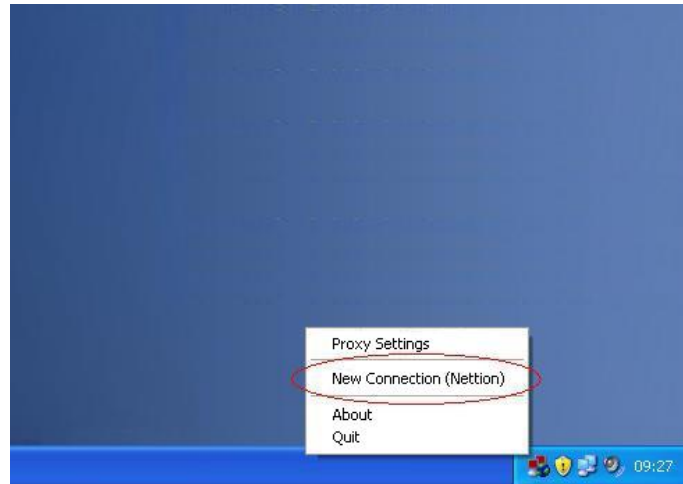


Figure 15.24: Setting File Import in OpenVPN Client

Now it is time of connecting, for that, click again with right button in OpenVPN Client icon and chooses the “Connect” option.

At this time will appear a screen requesting your username and password for Nettion authentication. Reminding that, this authentication is made in agreement with centralized authentication configured in your Nettion.

After the connection, access your net as always.

15.5.6 More Information

You can also access Step by Step tutorial available in Nettion’s site (www.nettion.com.br) for more information of how to configure plugin server and clients.

15.6 DNS

DNS is NettionPlug responsible for names (direct and reverse) resolutions.

DNS is a hierarchical system. The highest level is represented for “.” and denominated “root”. Under “.” there are several “High Level Domains” (TLDs), being ORG, COM, EDU and NET the more acquaintances.

There are 13 root DNS servers in the whole world and without them Internet would not work. Of these, ten are located in United States of America, one in Asia and two in Europe.

To Increase the installed base of these servers, “Replicas” were created in whole world, including in Brazil since 2003. In other words, the directories servers responsible for providing information like names and addresses of machines are usually called names servers. In Internet, the names service used is DNS, that presents an architecture client/server, could involve several DNS servers during the answer to a consultation.

15.6.1 How it Works?

The DNS service architecture is distributed in Masters and Slaves. The first is the responsible and it should be altered initially. It is that server who notifies other servers, where are the replicas of the information. Those are called Slaves, because they just receive Master's information.

There are two types of resolutions: a direct, when we want to find an IP of a name, and other when we have an IP and we want to know its name. This second form has a differentiated organization and it guarantees that a certain IP is of a known net. For instance, an E-mail server (SMTP) receives a connection of source host recognized by 192.168.5.4. For this IP to send e-mails, it has to have the configured reverse. It's done this way to prevent a possible fraud. The reverse domains are in path 'in-addr.arpa'. This path is not open to public access. Therefore, it is reliable. In the previous example above the reverse IP would be 4.5.168.192.in-addr.arpa.

After the installation, you access this plugin through the menu **“DNS > Domains”**.

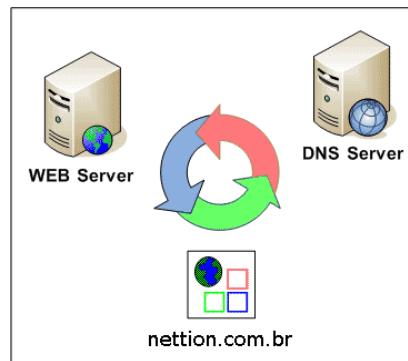


Figure 15.25: DNS Demonstrative Scheme

15.6.2 Master Domains

This modality allows that you create and manage your Masters domains. There are two fields that only appear in domain creation: NS and SOA, necessary items to any DNS. The SOA (Start Of Authority) it is the initial server of consultation. It is him who will determine the other domain names. The NS is the domain authority, it can be used to resolve the domain names, but it is usually used when SOA is “overloaded”.

To configure a domain, access in menu **“DNS > Domains”** and click in “Add” button. In the first screen of add wizard, configure:

- Name: Domain name that you will create;
- Description: Domain description which you will manage;
- Type: The domain type that you will create. In this case Master;
- Status: Active;
- SOA: Start of domain authority (Only in creation of master);
- NS: NS of domain master.

As displays following illustration.

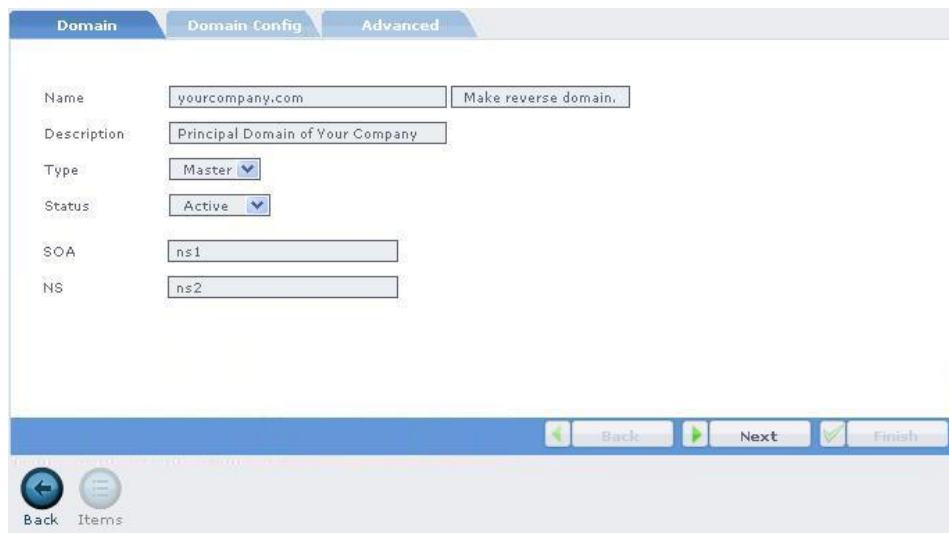


Figure 15.26: DNS Domain Settings

In the second wizard screen, select the slave servers that will be notified by master, reminding that to whole list of Items of NS type will also be notified.

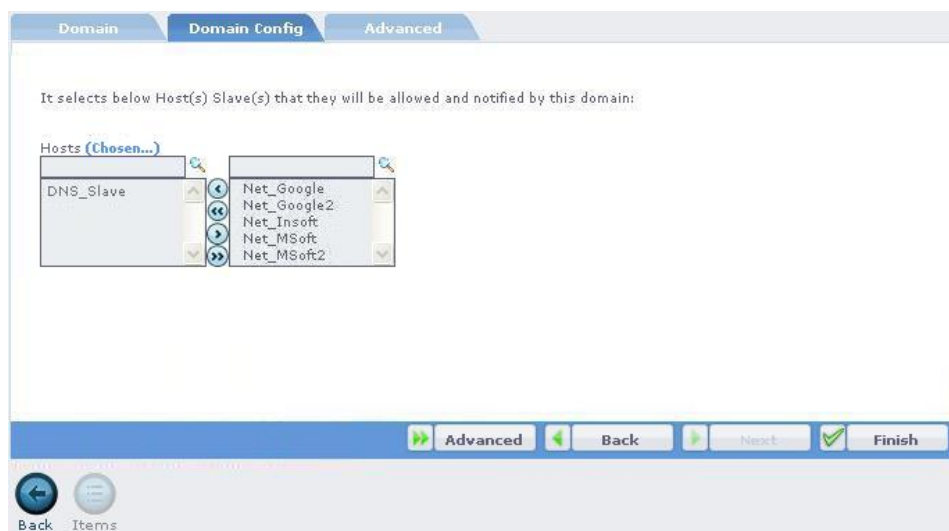


Figure 15.27: DNS Slaves Selection

In third wizard screen (Advanced Button), that it is optional, configure:

- TTL: Time of validity of cache information in other servers;
- Expire in: Total time of updating attempts;
- Refresh in: Time requested for the updating;
- Retry in: Time of retries in case of updating flaws;
- Postmaster: The administrator's of the domain e-mail.

See the illustration.

Figure 15.28: Advanced Settings of DNS Domain

15.6.3 Master Domain Items

To access this modality, select domain to which one you want to add the items and click in **“Items”** button, on inferior right side of screen. Click in **“Add”** button in the following window. In the screen that will be exhibited, report:

- In Type field: To define type of item. There are 6 types of items:
 - SOA: Start of Authority, marks the beginning of zone data and defines parameters that affect the entire zone.
 - NS: Identifies the names server of a domain.
 - MX: Mail eXchange, List of e-mail servers for delivery (SMTP).
 - A: Direct resolution of a name for an IP.
 - CNAME: Defines an alias for a hostname.
 - PTR: Maps an address for a hostname.
 - TXT: Allows the creation of registries SPF, DKIM (*DomainKeys*) and supply of additional information.
- * Example:


```
SPF: example.net. IN TXT "v=spf1 a mx ip4:192.0.2.32/27 -all"
DKIM: mail._domainkey.example.net. IN TXT "g=\; k=rsa\; t=y\; p=MF...XYZ"
INFO: example.net. IN TXT "in case of problem call (85)3878-1900"
```
- Field Description: Description for items management;
- Field Priority: Define server MX'S priority;
- Field IP/Host: To define resolutions hosts to the types PTR, A and CNAME;
- Field Resolve in: Used to determine resolution of name or type;
- Field Status: To define the item's status.

Items of "yourcompany.com"

Type: A

Description: Web Service

Name of Host: www

IP of Host: 200.200.200.1

Status: Active

Save settings

Back Items Del

Figure 15.29: Add Items in the DNS Domain

15.6.4 Slave Domains

This modality allows you to create and manage Slave domains. For that, access menu **“DNS > Domains”** and click in **“Add”** button. In the first screen of add wizard, configure:

- Name: Name of the domain that you will create;
- Description: Description of the domain which you will manage;
- Type: The domain type that you will create. In this case Slave;
- Status: Active.

Domain Domain Config Advanced

Name: yourcompany.com Make reverse domain.

Description: Principal Domain of Your Company

Type: Slave

Status: Active

Back Next Finish

Back Items

Figure 15.30: Add a Slave Domain in DNS

In the second wizard screen, select the Master servers that it should synchronize. It must be selected, obligatorily, a server¹, as display illustration below.

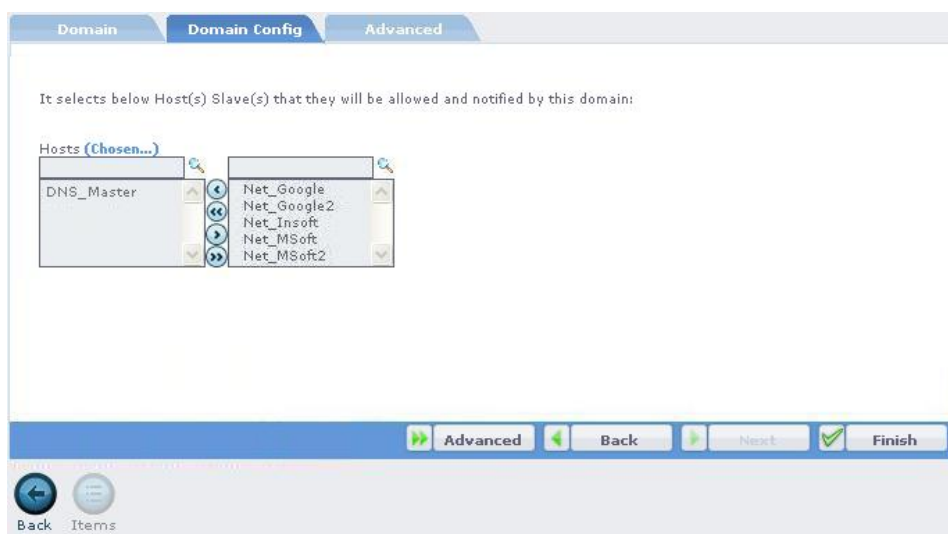


Figure 15.31: Masters DNS Selection

15.6.5 Slave Domain Items

- The items of Slave domain will be all imported items of the Master domain.

15.6.6 Reverse Domains

The reverse domains are special types. Its syntax is in-addr.arpa. They proceed at NAME field side;

There are a button called GENERATE THE REVERSE, in the creation wizard that will make the work easier. When clicked, it will request the ip/mask in xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy format.

This way, the name will be changed for the correct format.

15.6.7 Starting DNS Service

Begin DNS server through menu “**System > Services > Server of Names**”. To obtain more information on how to start Netion services, see topic 14.1.

15.6.8 Firewall with DNS

So that external users can be connected to Netion it is necessary to do Netion Firewall liberation. For that, create a rule allowing the access of any host (Internet) in direction to Netion, in the established port for the server.

Supposing that the server is configured for the default port, 53/UDP 53/TCP, use the predefined DNS service and create a Firewall rule, as shown in table 15.9:

¹Create an object with the Server name and its associated IP. See Chapter 4 - Objects

Rule: Liberating DNS Server			
Source	Destiny	Destiny serv.	Action
Any	localhost	DNS	Accept

Table 15.9: DNS Server Access

15.6.9 More Information

For larger information about the settings of this plugin, also access the Step by Step tutorial available in Nettion's site (www.nettion.com.br).

15.7 GetMail

The GetMail NettionPlug works as an e-mail messages receiver of remote servers (POP or IMAP) and direct them to an only e-mail server (usually the default e-mails server of the company), facilitating the messages management that concern the company's business. With GetMail the users don't need to access e-mails accounts of other people, nor webmails, and they still count with antivirus and antispam safety to filter the downloaded messages, in case the company's e-mails server it is own Nettion (local accounts). In that way, you reduce the risks of being virus infected and guarantee a larger productivity of your collaborators.

15.7.1 Advantages

GetMail NettionPlug provides the following advantages:

- Speed and safety in the emails access;
- Virus and spam control accessing external providers' messages;
- Better resources management;
- Compatibility with the messages solution used in your company, being capable for any network environment;
- Search of messages in several servers of -mail, independent of the provider;
- Creation of access permission, determining which external accounts can be accessed.

15.7.2 Settings

To configure GetMail, access menu **"GetMail > Settings"**. In the screen that will be exhibited, report:

- Verification interval: Time Interval (in seconds) in which verifications for new e-mails will be made;
- Destination Server (SMTP): Server that will be used for sending of the messages (usually own Nettion).

Then, click in “**Save Settings**” button as display illustration 15.32 abaixo.



Figure 15.32: GetMail Basic Settings

15.7.3 Source Accounts

To begin the GetMail rules creation, firstly we need to register the source accounts, in other words, the accounts of which we want to obtain e-mails. To add these accounts, click in “Add” button as shown in illustration 15.33.



Figure 15.33: Created Source Account List

In the screen that will be exhibited, report:

- Source Server: the name/IP of source accounts POP/POP3 server. Example: pop3.yourprovider.co
- User: the account user of access;
- Password: the password used for login;
- Confirmation: retype the password for login.

The above information should be typed correctly so that GetMail access in the account can be successfully accomplished. Such information should be obtained directly with the users of each registered source account. See illustration 15.34.

Figure 15.34: Source Account Creation

15.7.4 Rules

The rule creation process in GetMail is quite simple. Basically, it consists of to specify one or more source accounts and specify a destiny account, that can be local (accounts in own Nettion) or remote (accounts in other servers). For that, follow these steps:

Step 1:

To create a GetMail rule, access “**Getmail > Rules**”. In the screen that will be exhibited, report:

- Description: resumed rule description;
- Protocol: Select the protocol to be used POP or IMAP;
- Status: active, to make the rule enters in effect immediately.

See the illustration 15.35 to proceed.

Figure 15.35: GetMail Rule Creation

Step 2:

In the following screen, specify in “Source Accounts” the accounts of which you want to obtain the e-mails (Remembers that they should previously be created). In “Destination Accounts”, specify if destination account is **Local** or **Remote**. For Local, select the local e-mail account for which e-mails will be directed. For Remote, type the electronic address of e-mail account of remote server. Also select below one of the three options:

- Get seen emails too: specifies that GetMail should also bring e-mails that have already been read;
- Keep messages in server: specifies if will be left in source server copies of the messages that are being obtained;
- Use safe connection (TLS): Marks this option if source server demands safe authentication.

See illustration 15.36.

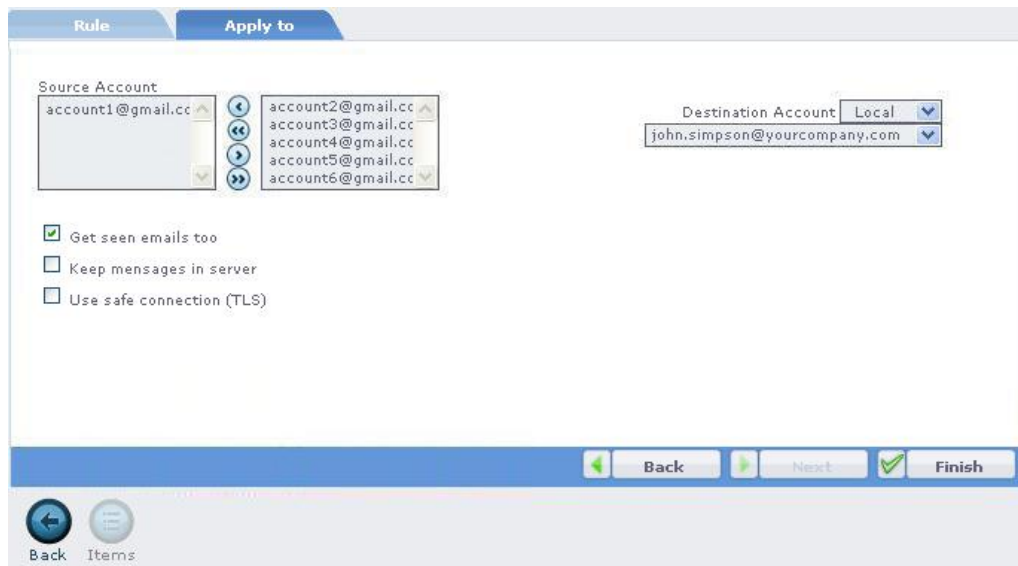


Figure 15.36: Source/Destination Accounts Selection

At the end click in “**Finish**” button for rule creation to conclude.

15.7.5 Starting GetMail Service

Start GetMail through menu “**System > Services > Getmail**”. To obtain more information on how to begin services in Nettion, see topic 14.1.

15.7.6 More Information

For larger information about the settings of this plugin, also access the site in (www.nettion.com.br).

A product by

Nettion[®]

Information Security

Northeast Brazil

Fortaleza City - Factory - Phone: 55 85 3878.1900 - Fax: 55 85 3878.1920 - Oliveira Paiva Avenue, 941 - Cidade dos Funcionários - ZIP Code: 60822-130

Fortaleza City - Administration - Phone: 55 85 3878.1900 - Fax: 55 85 3878.1920 - Antônio Fortes Street, 330 - Água Fria - ZIP Code: 60813-630

Southeast Brazil

São Paulo City - Phone: 55 11 3013.3010 - Cincinato Braga Street, 59 Cj 5-B1 - Bela Vista - ZIP Code: 01333-010

comercial@nettion.com.br

nettion.com.br