



# **Pare-Feu NETASQ au CGS**

---

A. CLEMENT & N. MAHR

présentation au groupe Xstra du 6 décembre 2002



# Pourquoi ?

---

## **mise en sécurité du réseau informatique**

- protéger le réseau interne des attaques
- palier à l'impossibilité de mettre à jour chaque poste
- mettre à part les serveurs visibles du monde extérieur



# Que choisir ?

---

- kit proposé par le CRC
- solution de type pont filtrant inclus dans Linux
- solution logicielle (Sygate, Norton, ZoneAlarm ...)
- solution matérielle (Arkoon, NetAsq)



# **solution retenue**

---

## **le Pare-Feu de NetAsq (F100B-3)**

- réponse aux besoins du laboratoire
- intégration aisée au réseau existant
- facilité d'administration et de surveillance
- support et maintenance

... pour un minimum de temps à investir dans l'installation et le suivi du pare-feu



# principe du pare-feu NetAsq

---

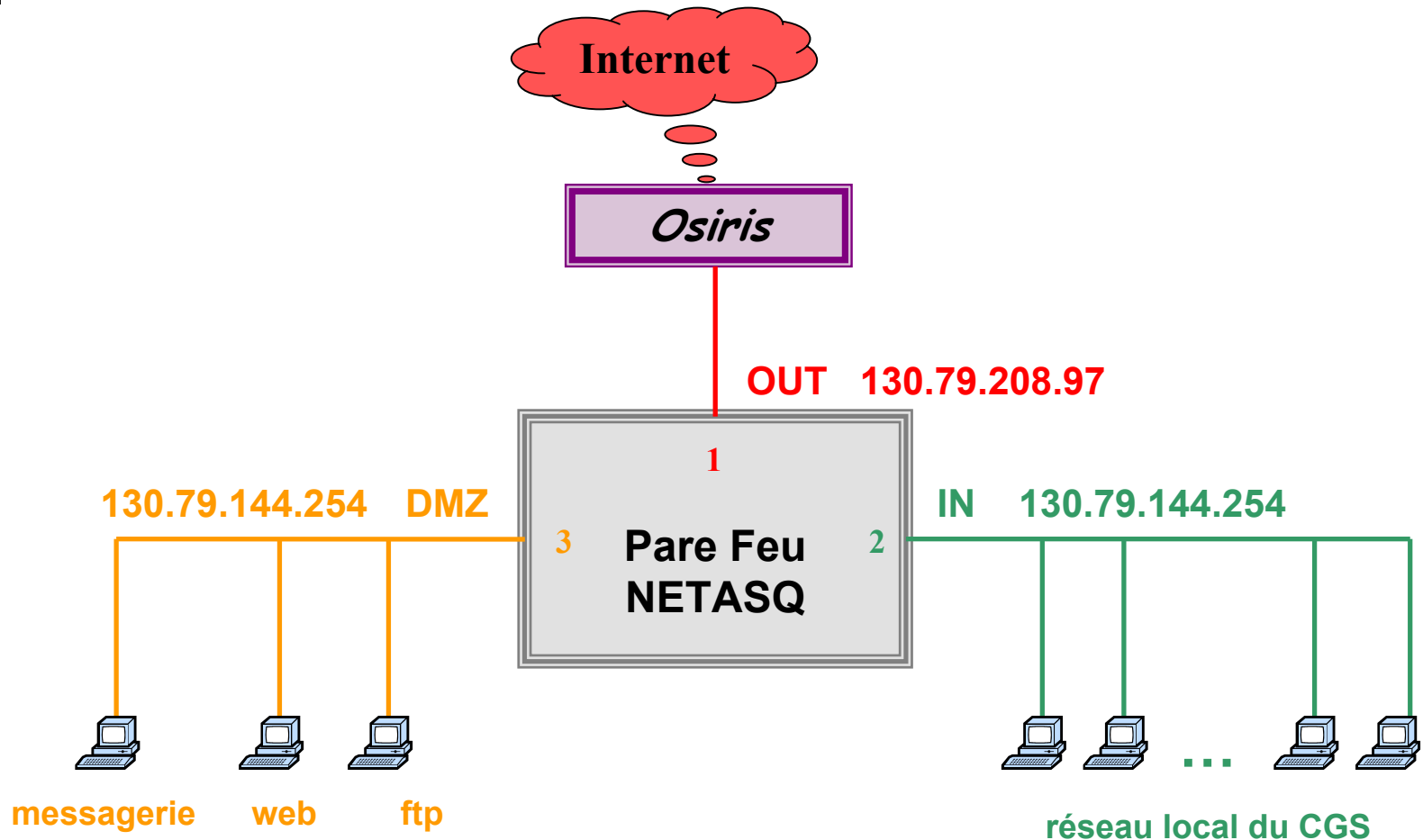
- détection et blocage en temps réel d'attaques informatiques : *paquets illégaux, tentatives de deny de service, anomalies dans une connexion, s de ports ...*

entrant ou sortant selon des règles pré-définies

nisme de filtrage de paquets évolués

isme de filtrage de paquets évolués  
chnologie NetAsq)

# schéma structurel





# spécifications matérielles

---

- 3 interfaces 100Mbits/sec
- processeur : Céléron 633 MHz
- mémoire : 64 Mo
- disque dur : 10Go
- OS : FreeBSD v4.5 allégé et sécurisé
- standards supportés : IP, ARP, TCP, UDP, ICMP, HTTP, IP-sec .....




# fonctionnalités

---

- de sécurité étendue : « stateful » inspection et détection d'attaques
- de routage
- de translation d'adresse
- de filtrages (adresses IP, protocoles, services ...)
- de traçabilité des logs
- de remontée des alarmes
- de passerelle VPN (tunnel chiffré)



# matrice des flux du CGS

 sens du filtrage	ZC	I	DMZ
ZC		web connexion cryptée échange de fichiers	web connexion cryptée échange de fichiers messagerie
I	accès interdit		web connexion cryptée échange de fichiers messagerie
DMZ	accès interdit	web connexion cryptée échange de fichiers messagerie	



# configuration du pare-feu

---

## 1- partie réseau (stateful)

- route statique : 130.79.208.102 (commutateur Osiris)
- interfaces en mode hybride
  - bridge** entre **IN** et **DMZ** : 130.79.144.254  
255.255.255.0
  - OUT** : 130.79.208.97  
255.255.255.248 (masque 29)



# configuration du pare-feu

---

## 2- déclaration d'objets

- machines : serveur\_web 130.79.144.5  
mesolite 130.79.144.95
- réseaux : Network\_bridge 130.79.144.0 255.255.255.0  
Network\_out 130.79.208.96 255.255.255.248  
Network\_crc 130.79.200.0 255.255.255.0
- services : http tcp 80  
x11 tcp 6000:6063
- protocoles : tcp 6  
udp 17
- groupes d'objets ( groupes de machines, groupes de services, ...)



# configuration du pare-feu

---

## 2- déclaration d'objets

- utilisateurs : authentification des utilisateurs pour des connexions entrantes (provenant de l'Internet) et autorisation d'accès à certains services hébergés sur votre réseau interne à certains utilisateurs de l'Internet

... à tester ...

# définition des règles (slots)

## 1- règles de filtrage

### 01-block all (08/04/2002) - NE JAMAIS Y TOUCHER -

<i>états</i>	<i>protocole</i>	<i>source</i>	<i>destination</i>	<i>service</i>	<i>action</i>
<b>Off</b>	all	<Any>	<Any>	<b>█</b> <Any>	<b>B</b> loquer

### 02-standard (22/10/2002)

<i>états</i>	<i>protocole</i>	<i>source</i>	<i>destination</i>	<i>service</i>	<i>action</i>
<b>On</b>	icmp	Serveurs_DMZ	<Any>	<b>█</b> <Any>	Passer
<b>On</b>	all	Serveurs_DMZ	<b>Network_bridge</b>	<b>█</b> <Any>	<b>B</b> loquer
<b>On</b>	all	<b>Network_bridge</b>	<Any>	<b>█</b> <Any>	Passer
<b>On</b>	group	<Any>	Serveurs_DMZ	full	Passer
<b>On</b>	icmp	Network_CRC	<Any>	<b>█</b> <Any>	Passer
<b>On</b>	all	<Any>	<Any>	<b>█</b> <Any>	<b>B</b> loquer

### 10-pass all (08/04/2002) - NE JAMAIS Y TOUCHER -

<i>états</i>	<i>protocole</i>	<i>source</i>	<i>destination</i>	<i>service</i>	<i>action</i>
<b>On</b>	all	<Any>	<Any>	<b>█</b> <Any>	Passer

# définition des règles (slots)

## 1- règles de filtrage ... suite

04-règle en cours (31/10/2002)

<i>états</i>	<i>protocole</i>	<i>source</i>	<i>destination</i>	<i>service</i>	<i>action</i>
On	all	alien	<Any>	=<Any>	<b>B</b> loquer
On	icmp	Serveurs_DMZ	<Any>	=<Any>	Passer
On	tcp	Serveurs_DMZ	<b>Network_bridge</b>	=auth	Passer
On	tcp	<b>Network_bridge</b>	<b>Serveur_Illite</b>	=ftp	Passer
On	tcp	<Any>	<b>Serveur_Illite</b>	=ftp	<b>B</b> loquer
On	group	<b>Serveur_Tropos2</b>	postes_X11	protocole_x11	Passer
On	all	<b>Serveur_DMZ</b>	<b>Network_bridge</b>	=<Any>	<b>B</b> loquer
On	all	<b>Network_bridge</b>	<Any>	=<Any>	Passer
On	group	<Any>	<b>Serveur_DMZ</b>	full	Passer
On	icmp	<b>Network_CRC</b>	<Any>	=<Any>	Passer
On	tcp	<b>Network_CRC_IN</b>	<b>Xylan_Alcatel</b>	=telnet	Passer
On	all	<Any>	<Any>	=<Any>	<b>B</b> loquer



# définition des règles (slots)

---

## **2-règle de translation d'adresse**

- non appliquée pour l'instant

## **3- tunnel VPN**

- pourra convenir pour les postes nomades

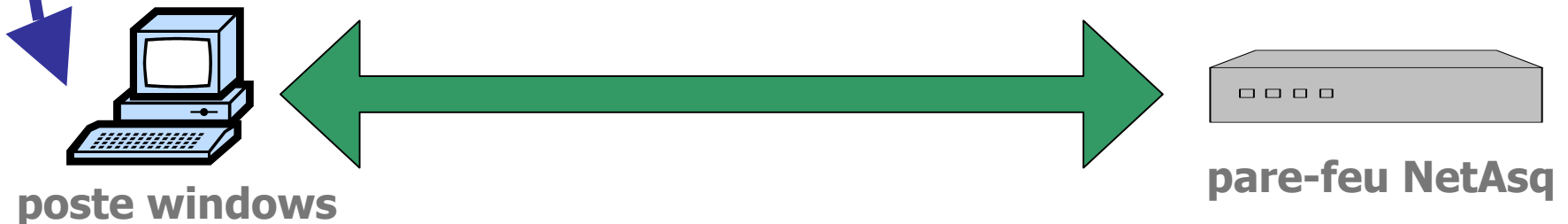
## **4- url web**

- non livré en standard

# outils de gestion

- **Firewall Manager** : outil d'administration
- **Firewall Reporter** : outil de visualisation et d'analyse des traces et statistiques
- **Firewall Monitor** : moniteur d'alarmes en temps réel visualisant l'activité du pare-feu

SRP (authentication et chiffrement) via le port 1300







# Firewall Manager

---

- logiciel graphique développé par la société NETASQ
- permet de configurer entièrement le pare-feu depuis un poste Windows(NT-2000-XP)

en cas de plantage du pare-feu , possibilité de s'y connecter en mode console

# Firewall Manager

The screenshot displays the Firewall Manager application window. At the top, there are three icons: Firewall Manager, Firewall Monitor, and Firewall Reporter. The main window has a menu bar with 'Fichier', 'Configuration', 'Authentification', and 'Firewall'. On the left, there is a sidebar with 'Firewall' and 'Configuration' sections, and a vertical menu with 'Réseau', 'Objets', 'Alarmes', and 'Certificats externes'. The 'Objets' section is active, showing a list of objects with columns for 'Nom', 'Protocole', and 'Port'. Below this list, there are several categories: 'Groupes d'utilisateurs', 'Groupes de machines', 'Groupes de réseaux', and 'Groupes de services'. The 'Edition des objets' dialog box is open, showing a list of objects with columns for 'Nom' and 'Commentaire'. The 'full' object group is selected, showing a list of protocols and ports. The 'full' group contains the following objects:

Nom	Commentaire
domain_udp	Domain Name Server
ftp	Service réservé pour l'accès
http	World Wide Web
https	
imap	Internet Message Access F
pop3	Post Office Protocol - Versi
smtp	Simple Mail Transfer Protoc
ssh	Réservé pour l'accès au fir
auth	Identification Protocol

The 'mail' group contains:

Nom	Commentaire
imap	Internet Message Access F
pop3	Post Office Protocol - Versi
smtp	Simple Mail Transfer Protoc

The 'web' group contains:

Nom	Commentaire
domain_udp	Domain Name Server
http	World Wide Web
https	

The 'protocole\_x11' group contains:

Nom	Commentaire
x11	X Window System
x11_udp	X Window System

At the bottom of the dialog box, there are buttons for 'Ajouter', 'Supprimer', 'Envoyer', and 'Annuler'. The status bar at the bottom shows the user 'admin@130.79.144.' and the command 'A B L F V U P O W T'. The system tray at the bottom right shows the date and time '15:21'.

# Firewall Manager

**Édition des objets**

Objets

- Utilisateurs
- Machines
- Réseaux
- Services
- Protocoles

Nom	IP	Commentaire
Firewall_dialup	0.0.0.0	
Firewall_altdialup	0.0.0.0	
Firewall_bridge	130.79.144.254	
Firewall_out	130.79.208.97	
Serveur_illite	130.79.144.2	
Serveur_Talc	130.79.144.5	
Serveur_Tropos2	130.79.144.11	
edenite	130.79.144.12	
atmosbond	130.79.144.236	
xylan_alcatel	130.79.144.245	
alien	172.16.1.12	

Objets disponibles: Ajouter, Supprimer, Importer...

Envoyer / Annuler

Firewall Manager

Sélection de slot de filtrage

Nom	Heure	Dernière modification
01-block all	Aucun	08/04/2002 08:56:10
02-standard	Aucun	22/10/2002 18:26:12
03-Appliqué	Aucun	23/10/2002 14:49:26
04-test en cours	Aucun	31/10/2002 09:14:58
05-vide	Aucun	
06-vide	Aucun	
07-vide	Aucun	
08-vide	Aucun	
09-vide	Aucun	
10-pass all	Aucun	08/04/2002 08:56:25

Édition des règles de filtrage

Etats	Protocole	Source	Destination	Service	Action	Log	Commentaire
1 On	all	alien	<Any>	<Any>	Bloquer		
2 On	icmp	Serveurs_DMZ	<Any>	<Any>	Passer		ping possible depuis
3 On	tcp	Serveurs_DMZ	Network_bridge	auth	Passer		113 possible depuis
4 On	tcp	Network_bridge	Serveur_illite	ftp	Passer		ftp OK depuis réseau
5 On	tcp	<Any>	Serveur_illite	ftp	Bloquer		ftp KO depuis tout ven
6 On	group	Serveur_Tropos2	postes_X11	protocole_x11	Passer		X11 OK vers certaines
7 On	all	Serveurs_DMZ	Network_bridge	<Any>	Bloquer		toute connexion KO di
8 On	all	Network_bridge	<Any>	<Any>	Passer		toute connexion OK di
9 On	group	<Any>	Serveurs_DMZ	full	Passer		connexions standard:
10 On	icmp	Network_CRC	<Any>	<Any>	Passer		ping OK depuis CRC
11 On	tcp	Network_CRC_IN	xylan_alcatel	telnet	Passer		
12 On	all	<Any>	<Any>	<Any>	Bloquer		par précaution tout es

Mode avancé

Nom du Slot : test en cours

Envoyer / Annuler

admin@130.79.144. A B L F V U P O W T 130.79.144.254@Port:1300

Démarrer | Eudora | Microsoft P... | Firewall M... | ilite.u-str... | Document... | 15:25



# Firewall Reporter

---

- logiciel de visualisation des informations de logs générées par le pare-feu NetAsq
  - analyse l'activité du réseau, des accès aux ressources informatiques, de l'utilisation d'Internet, de la messagerie ...
  - diagnostique les attaques informatiques repérées et rejetées par le pare-feu.

# Firewall Reporter

## vue sur le fichier des connexions

The screenshot displays the Firewall Reporter application window. The title bar reads "Firewall Reporter - [Directement connecté sur le firewall F1003D009330100601]". The interface includes a menu bar with "Fichier", "Fenêtres", and "?". Below the menu is a "Sélection" section with date and time filters for "Aujourd'hui", "14/11/2002", and "00:00:00" to "23:59:59". A navigation bar contains tabs for "Filtres", "Alarmes", "Connexions" (selected), "Internet", "Emails", and "Fichier WELF importé". A sidebar on the left lists "Reporter", "Fichiers", "Graphiques", "Statistiques", and "Divers". The main area shows a table of connections with columns for "Line - date", "Protocol", "Source", "Destination", and "Volume".

Line - date		Protocol	Source			Destination		Volume		
Date-Heure	Règle Id	Protocole Internet	Utilisateur	Nom Source	Nom Port Source	Nom Destination	Nom Port Destination	Envoyé	Reçu	Durée
14/11/2002 16:	8	udp		130.79.144.80	32768	ns1.u-strasbg.fr	domain_udp	37	165	1 ms
14/11/2002 16:	8	tcp		melanite.u-strasbg.	2303	logc1.xiti.com	http	401	365	3 s
14/11/2002 16:	8	tcp		epidote.u-strasbg.fr	3272	Serveur_illite	pop3	39	216	127 ms
14/11/2002 16:	8	tcp		atmosemi.u-strasbg	4448	ads.ix.com	http	342	13 KB	101 ms
14/11/2002 16:	8	tcp		atmosemi.u-strasbg	4446	ads.ix.com	http	555	523	318 ms
14/11/2002 16:	8	tcp		franceville.u-strasb	ephemeral_fw	www.photoways.com	http	2 KB	3 KB	6 m 8 s
14/11/2002 16:	8	tcp		franceville.u-strasb	ephemeral_fw	www.photoways.com	http	2 KB	6 KB	6 m 8 s
14/11/2002 16:	8	tcp		franceville.u-strasb	ephemeral_fw	www.photoways.com	http	2 KB	9 KB	6 m 8 s
14/11/2002 16:	8	tcp		franceville.u-strasb	ephemeral_fw	www.photoways.com	http	1 KB	2 KB	6 m 6 s
14/11/2002 16:	8	tcp		franceville.u-strasb	ephemeral_fw	www.photoways.com	http	689	5 KB	6 m 6 s
14/11/2002 16:	8	tcp		franceville.u-strasb	ephemeral_fw	www.photoways.com	http	12 KB	105 KB	6 m 11 s
14/11/2002 16:	8	tcp		franceville.u-strasb	ephemeral_fw	www.photoways.com	http	2 KB	24 KB	6 m 8 s
14/11/2002 16:	8	tcp		franceville.u-strasb	ephemeral_fw	www.photoways.com	http	1 KB	34 KB	6 m 8 s
14/11/2002 16:	8	tcp		130.79.144.80	2048	Serveur_illite	pop3	59	1 KB	5 s
14/11/2002 16:	8	tcp		mesolite.u-strasbg.l	1870	Serveur_illite	pop3	37	212	95 ms
14/11/2002 16:	8	tcp		silice.u-strasbg.fr	1501	Serveur_illite	pop3	38	214	132 ms
14/11/2002 16:	8	tcp		kenyaite.u-strasbg.	ephemeral_fw	Serveur_illite	pop3	61	714	1 s
14/11/2002 16:	8	tcp		atmosemi.u-strasbg	4447	www.topachat.com	http	4 KB	73 KB	43 s
14/11/2002 16:	8	tcp		atmosemi.u-strasbg	4449	ads.ix.com	http	555	522	401 ms
14/11/2002 16:	8	tcp		atmosemi.u-strasbg	4450	ads.ix.com	http	341	12 KB	114 ms
14/11/2002 16:	8	tcp		atmosjlc.u-strasbg.l	2765	Serveur_illite	pop3	46	421	424 ms
14/11/2002 16:	8	tcp		larnite.u-strasbg.fr	1508	east.u-strasbg.fr	http	348	11 KB	1 s
14/11/2002 16:	8	tcp		melanite.u-strasbg.	2302	memorix.sdv.fr	http	375	2 KB	92 ms
14/11/2002 16:	8	tcp		atmosemi2.u-strast	4144	Serveur_illite	pop3	49	423	378 ms

At the bottom, there are buttons for "Recherche", "Filtre", "Colonnes", "Imprimer", "Exporter...", and "Importer un fichier WELF". A status bar at the very bottom indicates "Fin de transformation des logs. Sélection de 65365 lignes. (Temps: 137 secondes)".

# Firewall Reporter

## vue sur le fichier des alarmes

The screenshot displays the Firewall Reporter application window. The title bar reads "Firewall Reporter - [Directement connecté sur le firewall F1003D009330100601]". The interface includes a menu bar with "Firewall", "Fenêtres", and "?". Below the menu bar is a "Sélection" section with a dropdown menu set to "Aujourd'hui", a date field for "14/11/2002", a time field for "00:00:00", and another date field for "14/11/2002" with a time field for "23:59:59".

The main area is divided into a left sidebar and a central table. The sidebar contains a "Reporter" section with icons for "Fichiers", "Graphiques", "Statistiques", and "Divers". The central table is titled "Filtres" and "Alarmes" and contains a list of firewall alerts. The table has columns for "Line - date", "Règle Id", "Priorité", "Interface", "Nom Interface Source", "Protocole Internet", "Utilisateur", "Source", "Nom Port Source", "Destination", "Nom Port Destination", "Action", and "Message".

Line - date	Règle Id	Priorité	Interface	Nom Interface Source	Protocole Internet	Utilisateur	Source	Nom Port Source	Destination	Nom Port Destination	Action	Message
14/11/2002 13:		Minor	out		icmp (8 8)		212.155.111		melanite.u-strast		block	Firewall policy
14/11/2002 13:		Minor	out		icmp (8 8)		212.155.111		melanite.u-strast		block	Firewall policy
14/11/2002 13:		Minor	out		icmp (8 8)		212.155.111		melanite.u-strast		block	Firewall policy
14/11/2002 13:		Minor	out		icmp (8 8)		212.155.111		melanite.u-strast		block	Firewall policy
14/11/2002 13:		Minor	out		icmp (8 8)		212.155.111		melanite.u-strast		block	Firewall policy
14/11/2002 13:		Minor	out		icmp (8 8)		212.155.111		melanite.u-strast		block	Firewall policy
14/11/2002 14:		Minor	out		tcp		www.meteo	http	atmospops.u-str.	2621	block	nmap OS prot
14/11/2002 14:		Minor	out		tcp		www.meteo	http	atmospops.u-str.	2631	block	nmap OS prot
14/11/2002 14:		Minor	out		tcp		www.meteo	http	atmospops.u-str.	2618	block	nmap OS prot
14/11/2002 14:		Minor	out		tcp		www.meteo	http	atmospops.u-str.	2641	block	nmap OS prot
14/11/2002 14:		Minor	out		tcp		www.meteo	http	atmospops.u-str.	2684	block	nmap OS prot
14/11/2002 14:		Minor	out		tcp		www.meteo	http	atmospops.u-str.	2686	block	nmap OS prot
14/11/2002 14:		Minor	out		tcp		www.meteo	http	atmospops.u-str.	2685	block	nmap OS prot
14/11/2002 14:		Minor	out		tcp		www.meteo	http	atmospops.u-str.	2690	block	nmap OS prot
14/11/2002 14:		Major	in		tcp		130.79.231.	1624	130.79.231.179	netbios-ssn	block	IP address sp
14/11/2002 14:		Minor	out		tcp		www.meteo	http	atmospops.u-str.	2989	block	nmap OS prot
14/11/2002 14:		Minor	out		tcp		www.meteo	http	atmospops.u-str.	2990	block	nmap OS prot
14/11/2002 14:		Minor	out		tcp		www.meteo	http	atmospops.u-str.	2992	block	nmap OS prot
14/11/2002 14:		Minor	out		tcp		www.meteo	http	atmospops.u-str.	3012	block	nmap OS prot
14/11/2002 14:		Minor	out		tcp		www.meteo	http	atmospops.u-str.	3039	block	nmap OS prot
14/11/2002 14:		Minor	out		tcp		www.meteo	http	atmospops.u-str.	3070	block	nmap OS prot
14/11/2002 14:		Minor	out		tcp		www.meteo	http	atmospops.u-str.	3067	block	nmap OS prot

At the bottom of the window, there is a status bar with the text "Fin de transformation des logs. Sélection de 198 lignes. (Temps: 1 secondes)". To the right of the status bar is a green button labeled "Prêt !".

# Firewall Reporter

les alarmes majeures sont remontées via la messagerie

The screenshot shows the Eudora email client interface. The main window displays an email with the following details:

**Subject:** Alarm report for NETASQ Firewall [1]

**Date:** Thu, 14 Nov 2002 15:37:32 GMT

**From:** F1003D009330100601@u-strasbg.fr

**Subject:** Alarm report for NETASQ Firewall [1]

**Sender:** F1003D009330100601@u-strasbg.fr

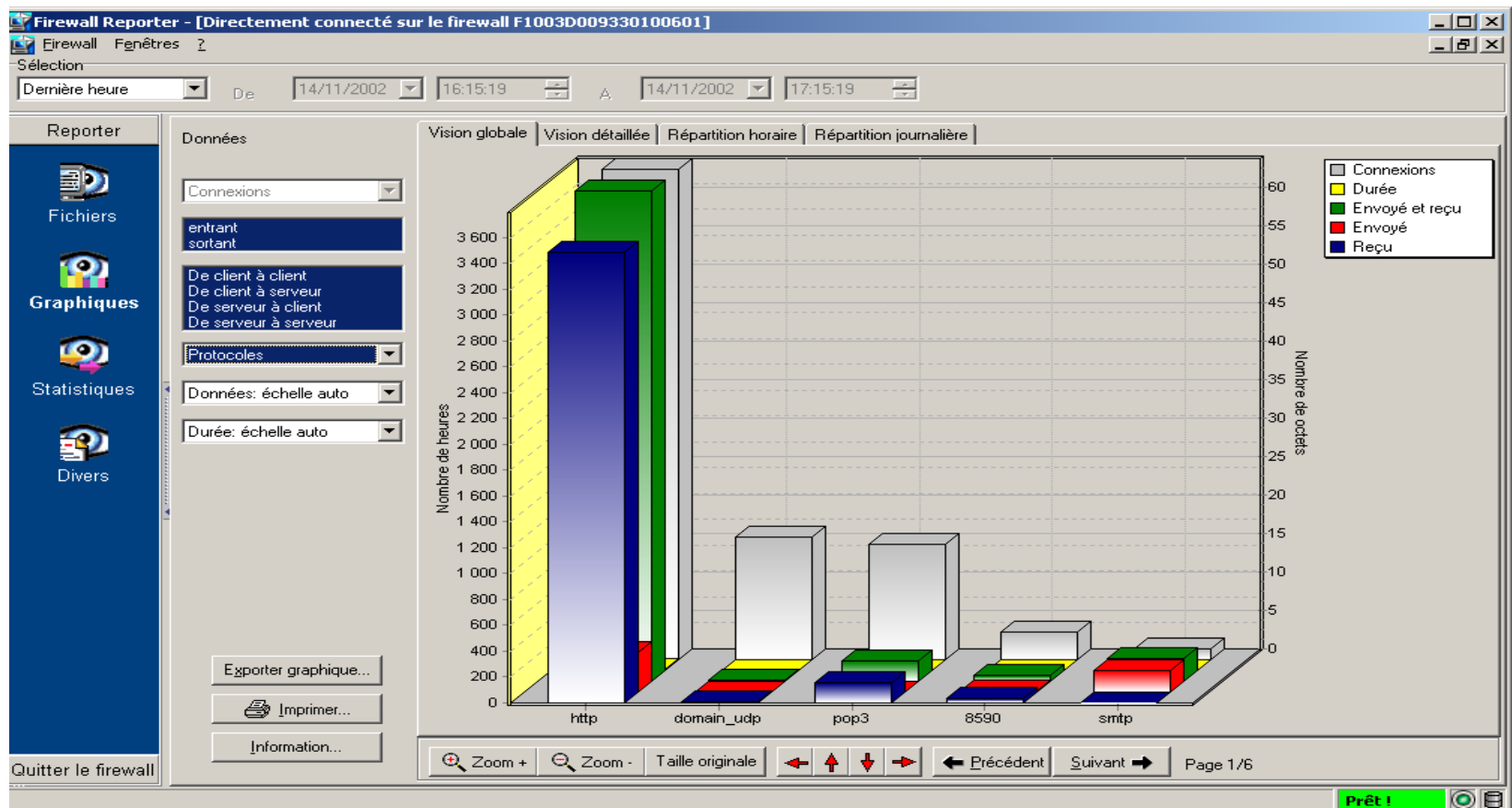
**To:** nmahr@illite.u-strasbg.fr, aclement@illite.u-strasbg.fr, nmahr@illite.u-strasbg.fr

Type	Date	Interface	Protocol	Source	Destination	Description
major	2002/11/14 14:24:00	in	tcp	130.79.231.188,1624	130.79.231.179,139	IP address spoofing

The interface also shows a taskbar with 'Fw-cgs' and 'F1003D009330100...' open, and a 'QUALCOMM' logo in the bottom right corner.

# Firewall Reporter

## vue graphique sur les protocoles







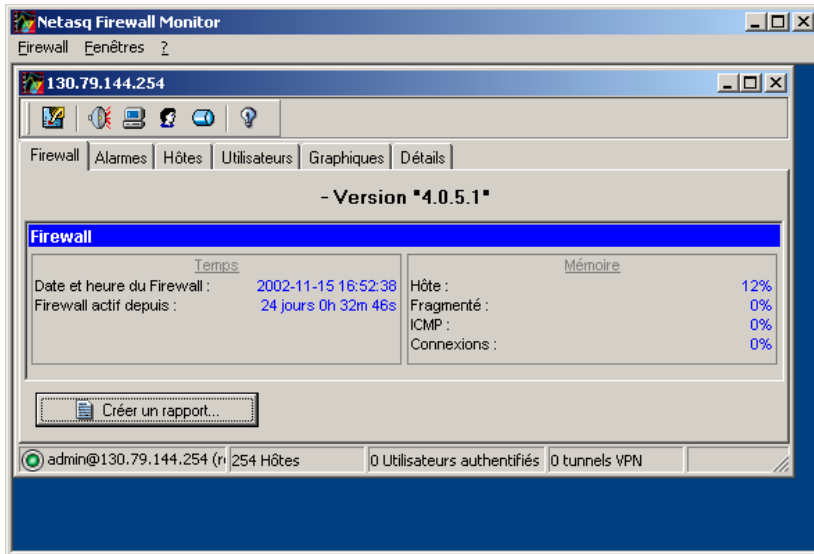
# Firewall Monitor

---

- logiciel de visualisation en temps réel de l'activité du pare-feu
  - utilisation des ressources internes du pare-feu (mémoire, CPU ...)
  - liste des machines et utilisateurs connectés
  - alarmes remontées en temps réel
  - nombre de connexions, utilisation de la bande passante, débit
  - informations sur l'état des interfaces et des tunnels VPN

# Firewall Monitor

états internes des ressources  
du pare-feu



Netasq Firewall Monitor  
130.79.144.254

Firewall Alarmes Hôtes Utilisateurs Graphiques Détails

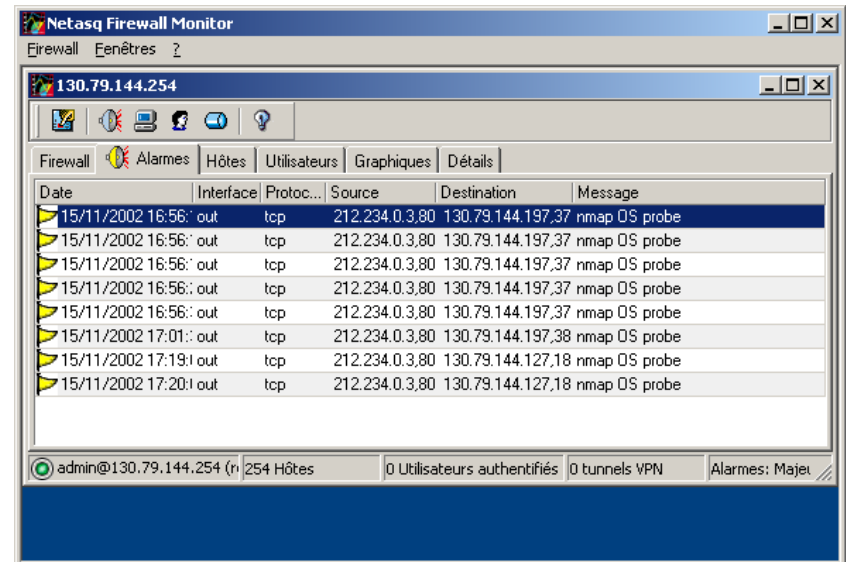
- Version "4.0.5.1"

Temps		Mémoire	
Date et heure du Firewall :	2002-11-15 16:52:38	Hôte :	12%
Firewall actif depuis :	24 jours 0h 32m 46s	Fragmenté :	0%
		ICMP :	0%
		Connexions :	0%

Créer un rapport...

admin@130.79.144.254 (r) 254 Hôtes 0 Utilisateurs authentifiés 0 tunnels VPN

suivi des alarmes en temps réel



Netasq Firewall Monitor  
130.79.144.254

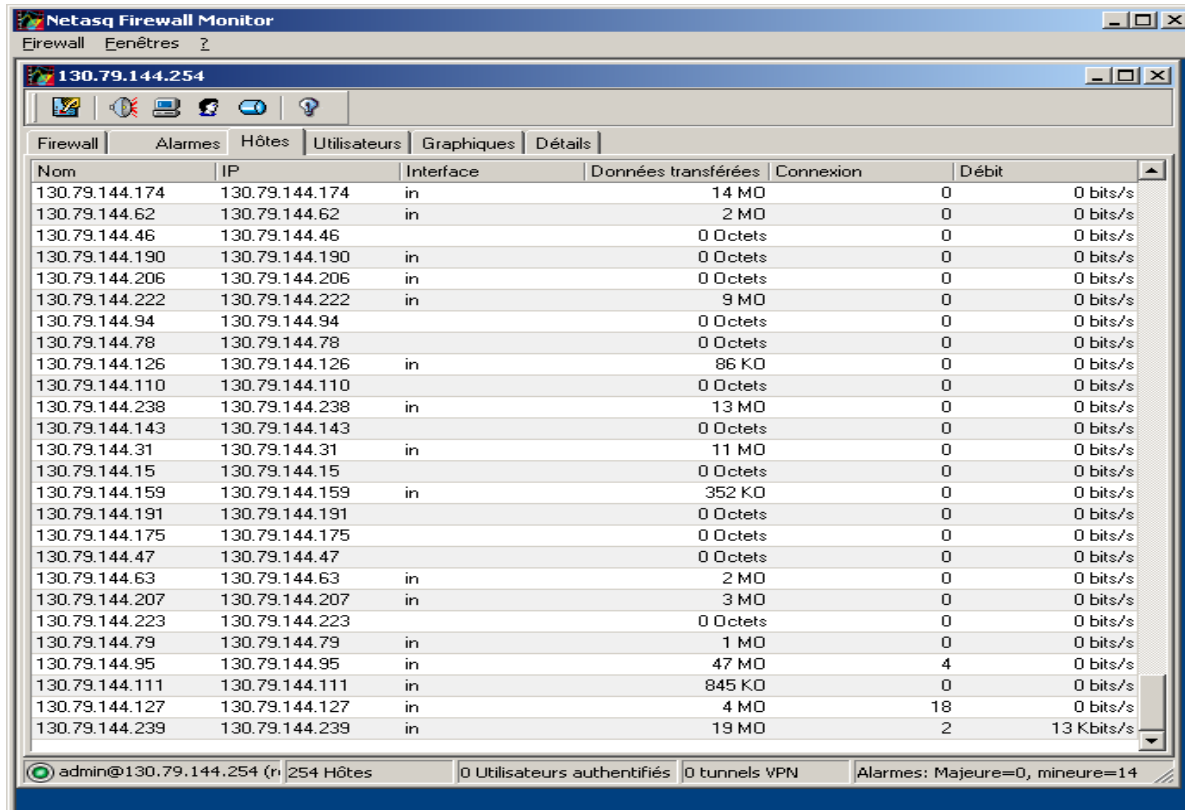
Firewall Alarmes Hôtes Utilisateurs Graphiques Détails

Date	Interface	Protoc...	Source	Destination	Message
15/11/2002 16:56:	out	tcp	212.234.0.3.80	130.79.144.197,37	nmap OS probe
15/11/2002 16:56:	out	tcp	212.234.0.3.80	130.79.144.197,37	nmap OS probe
15/11/2002 16:56:	out	tcp	212.234.0.3.80	130.79.144.197,37	nmap OS probe
15/11/2002 16:56:	out	tcp	212.234.0.3.80	130.79.144.197,37	nmap OS probe
15/11/2002 17:01:	out	tcp	212.234.0.3.80	130.79.144.197,38	nmap OS probe
15/11/2002 17:19:	out	tcp	212.234.0.3.80	130.79.144.127,18	nmap OS probe
15/11/2002 17:20:	out	tcp	212.234.0.3.80	130.79.144.127,18	nmap OS probe

admin@130.79.144.254 (r) 254 Hôtes 0 Utilisateurs authentifiés 0 tunnels VPN Alarmes: Majes

# Firewall Monitor

informations des machines hôtes



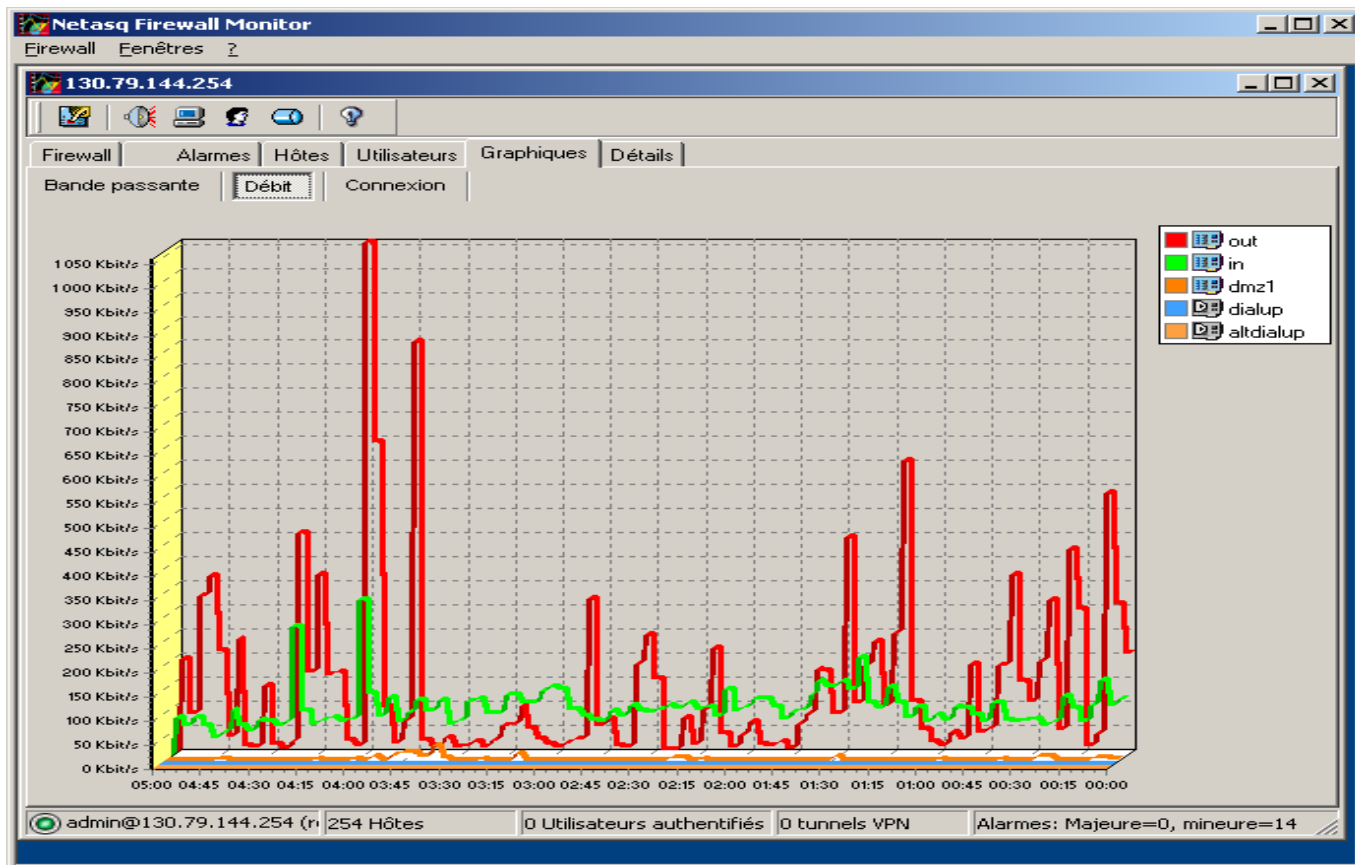
The screenshot shows the Netasq Firewall Monitor application window. The title bar reads "Netasq Firewall Monitor". Below the title bar, there are menu options: "Firewall", "Fenêtres", and "?". The main window has a sub-title bar with the IP address "130.79.144.254" and a toolbar with icons for home, refresh, help, and search. Below the toolbar, there are tabs: "Firewall", "Alarmes", "Hôtes", "Utilisateurs", "Graphiques", and "Détails". The "Hôtes" tab is selected, displaying a table of host information. The table has columns for "Nom", "IP", "Interface", "Données transférées", "Connexion", and "Débit". The data is as follows:

Nom	IP	Interface	Données transférées	Connexion	Débit
130.79.144.174	130.79.144.174	in	14 MO	0	0 bits/s
130.79.144.62	130.79.144.62	in	2 MO	0	0 bits/s
130.79.144.46	130.79.144.46		0 Octets	0	0 bits/s
130.79.144.190	130.79.144.190	in	0 Octets	0	0 bits/s
130.79.144.206	130.79.144.206	in	0 Octets	0	0 bits/s
130.79.144.222	130.79.144.222	in	9 MO	0	0 bits/s
130.79.144.94	130.79.144.94		0 Octets	0	0 bits/s
130.79.144.78	130.79.144.78		0 Octets	0	0 bits/s
130.79.144.126	130.79.144.126	in	86 KO	0	0 bits/s
130.79.144.110	130.79.144.110		0 Octets	0	0 bits/s
130.79.144.238	130.79.144.238	in	13 MO	0	0 bits/s
130.79.144.143	130.79.144.143		0 Octets	0	0 bits/s
130.79.144.31	130.79.144.31	in	11 MO	0	0 bits/s
130.79.144.15	130.79.144.15		0 Octets	0	0 bits/s
130.79.144.159	130.79.144.159	in	352 KO	0	0 bits/s
130.79.144.191	130.79.144.191		0 Octets	0	0 bits/s
130.79.144.175	130.79.144.175		0 Octets	0	0 bits/s
130.79.144.47	130.79.144.47		0 Octets	0	0 bits/s
130.79.144.63	130.79.144.63	in	2 MO	0	0 bits/s
130.79.144.207	130.79.144.207	in	3 MO	0	0 bits/s
130.79.144.223	130.79.144.223		0 Octets	0	0 bits/s
130.79.144.79	130.79.144.79	in	1 MO	0	0 bits/s
130.79.144.95	130.79.144.95	in	47 MO	4	0 bits/s
130.79.144.111	130.79.144.111	in	845 KO	0	0 bits/s
130.79.144.127	130.79.144.127	in	4 MO	18	0 bits/s
130.79.144.239	130.79.144.239	in	19 MO	2	13 Kbits/s

At the bottom of the window, there is a status bar with the following information: "admin@130.79.144.254 (r) 254 Hôtes", "0 Utilisateurs authentifiés", "0 tunnels VPN", and "Alarmes: Majeure=0, mineure=14".

# Firewall Monitor

graphique du débit en temps réel





# conclusion 1

---

- bon niveau de sécurité
- performances réseau maintenues
- insertion facile à l'existant
- règles de sécurité acceptées par les utilisateurs
- remontée des alarmes
- suivi des logs
- remise en état sous 48 h en cas de panne

... pour un coût financier de 6000 €



## conclusion 2

---

- mise à jour de l'infrastructure déployée
- mise à jour et sécurisation des OS
- vérification de la cohérence des règles de sécurité

... avec une veille technologique régulière