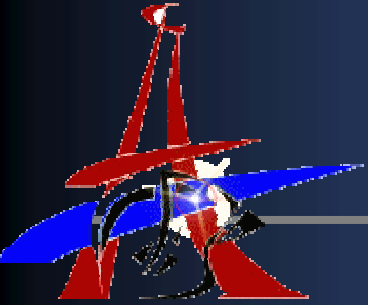
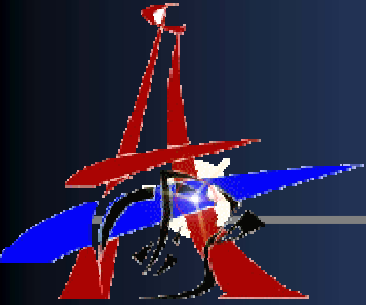


Retour d'expérience Produits Matranet



Sommaire

- 1 - Présentation générale
- 3 - Démarche
- 4 - Schématisation
- 5 - Mise en œuvre
- 7 - Exploitation
- 8 - Conclusion



Présentation générale

Mise en œuvre d'une solution Matranet
FireWall, M>Manager, Sémantica
Intégrateur Matranet

ISP Easynet connection adsl 256k
Routeur atm 1401

Hébergement messagerie @pompiersparis.fr



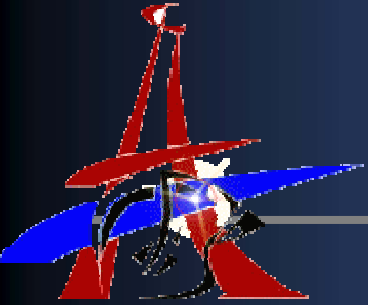
Démarche

Analyse technique

Politique de mise en oeuvre

Pré installation

Intervention Matranet 5j Installation Tests

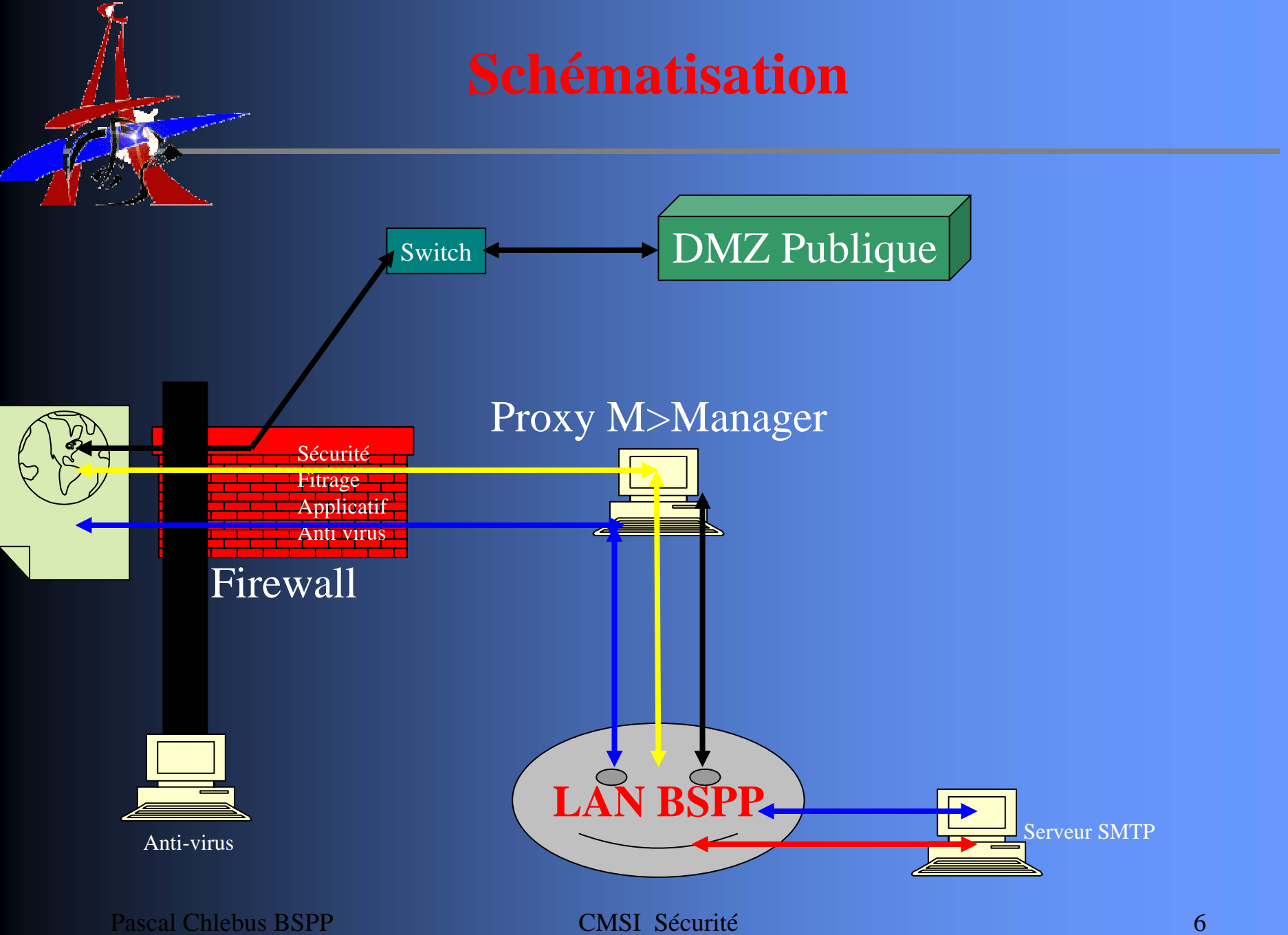


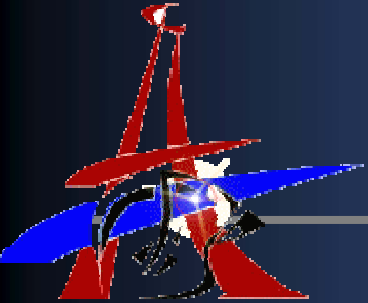
Démarche: choix technique

FireWall : Compaq proliant 3000 bi-proc 512MO Ram Raid5
Se BSD 4.1

M>Manager : Compaq proliant ML530 1GO RAM Raid5
Se W2K Serveur Active directory

Schématisation





Mise en oeuvre: pré-installation

Installation M>Manager suivant guide d'installation

Version 2.1 (CD évaluation nouvelle version)

Configuration des comptes utilisateurs non liés

Mise en place stratégie globale

Tests et suppression ancien proxy

3 Jours

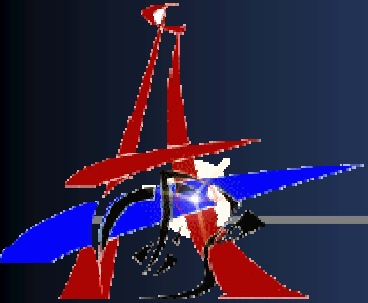
Problème rencontré : pas d'image lors du chargement, il faut rafraichir

Solution : Contact support technique Matranet

Changement de config : sans résultat 1 jour

Installation d'une dll + executable 4 Jours

En service depuis 2 mois sans problème



Exploitation: Qui, Comment?

Proxy autorisation

M>Manager gestion droit stratégie

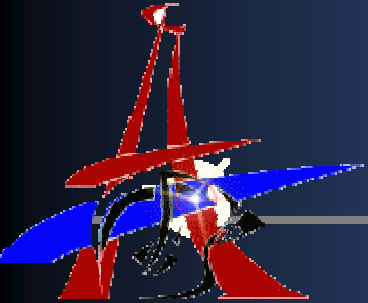
Sémantica (référentiel, catégorisation)

FireWall

Madmin 3.1 Java

Madmin 3.1 Java
Mnet-setup

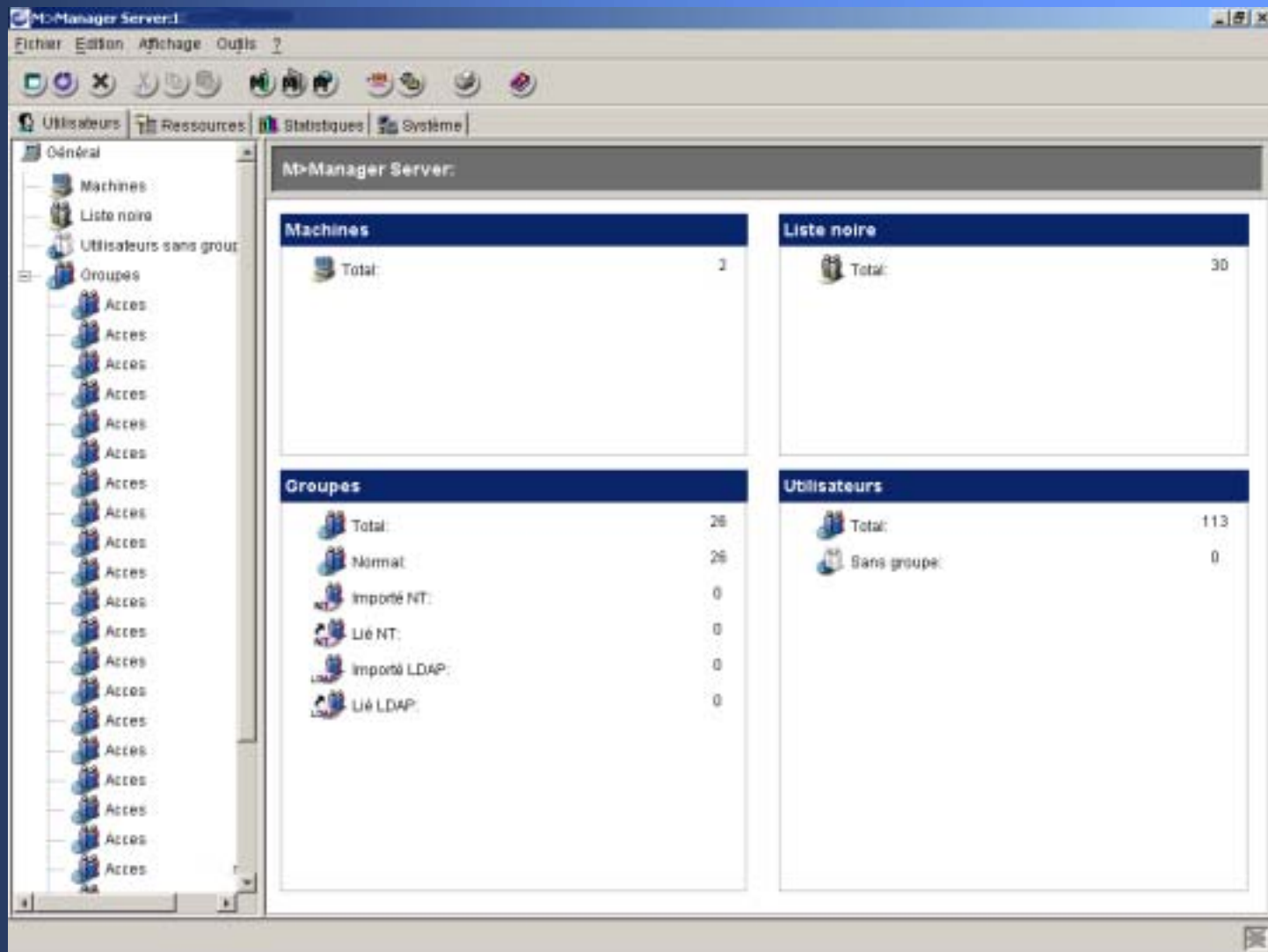
Exploitation



The screenshot shows a web browser window titled "M-Admin" with a MATRA net logo on the left. The main content area displays a table with the following columns: Etat, Adresse IP, Port, URL, and Description. A single row is visible, containing a yellow warning icon in the 'Etat' column, a computer icon in the 'Adresse IP' column, and the number '6661' in the 'Port' column. A tooltip message is shown over the table row: "Vous n'êtes pas authentifié auprès de cette machine (problème de connectivité réseau ?)..."

Etat	Adresse IP	Port	URL	Description
		6661		

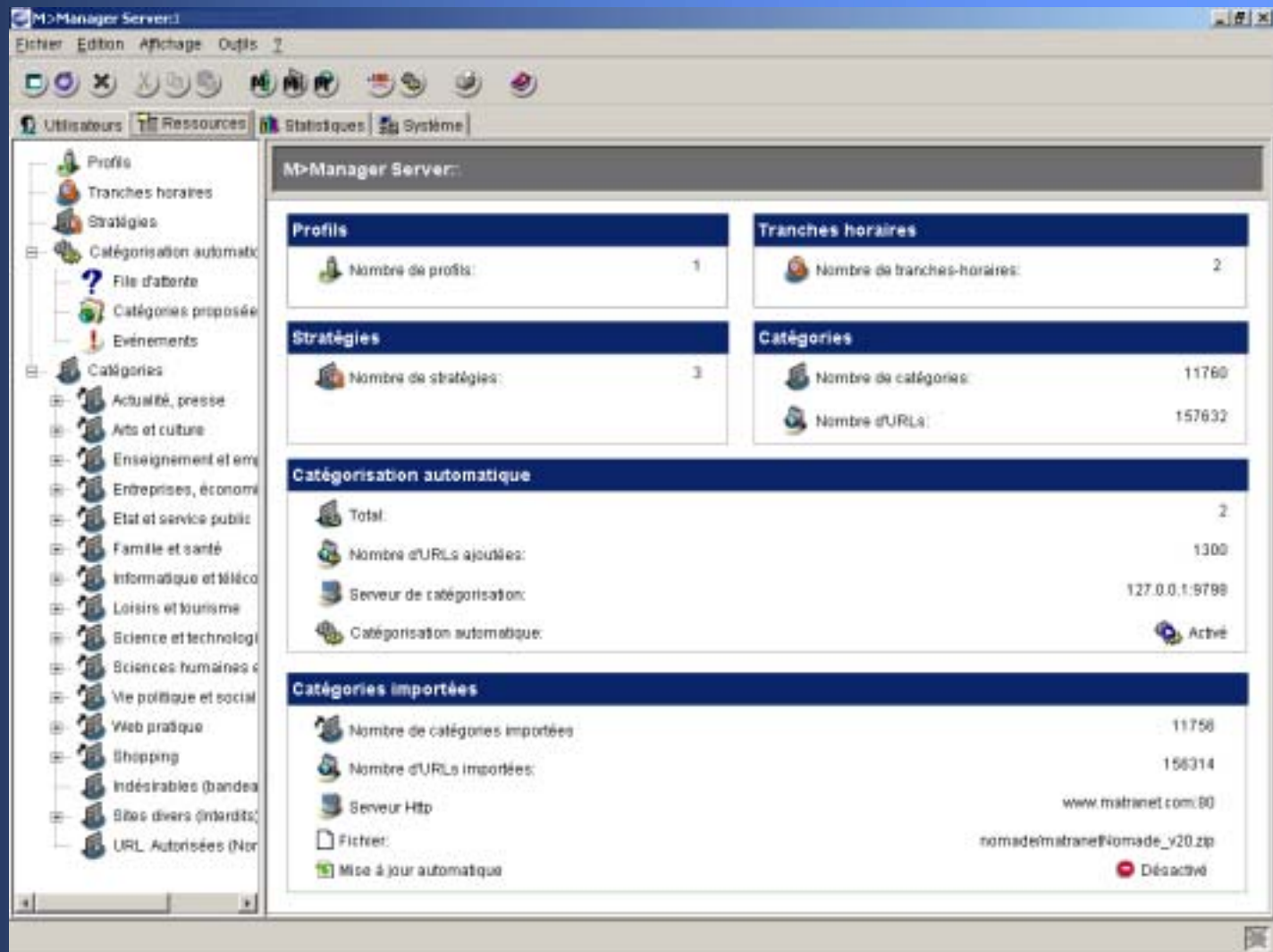
Exploitation



The screenshot displays the Mb-Manager Server interface. On the left is a navigation tree with categories like 'Général', 'Machines', 'Liste noire', 'Utilisateurs sans groupe', and 'Groupes'. The main area contains four summary panels:

- Machines:** Total: 2
- Liste noire:** Total: 30
- Groupes:** Total: 26, Normal: 26, Importé NT: 0, Lié NT: 0, Importé LDAP: 0, Lié LDAP: 0
- Utilisateurs:** Total: 113, Sans groupe: 0

Exploitation



The screenshot displays the M-Manager Server interface. On the left is a tree view of categories, and the main area shows several summary panels.

Profil

- Nombre de profils: 1

Tranches horaires

- Nombre de tranches horaires: 2

Stratégies

- Nombre de stratégies: 3

Catégories

- Nombre de catégories: 11760
- Nombre d'URLs: 157632

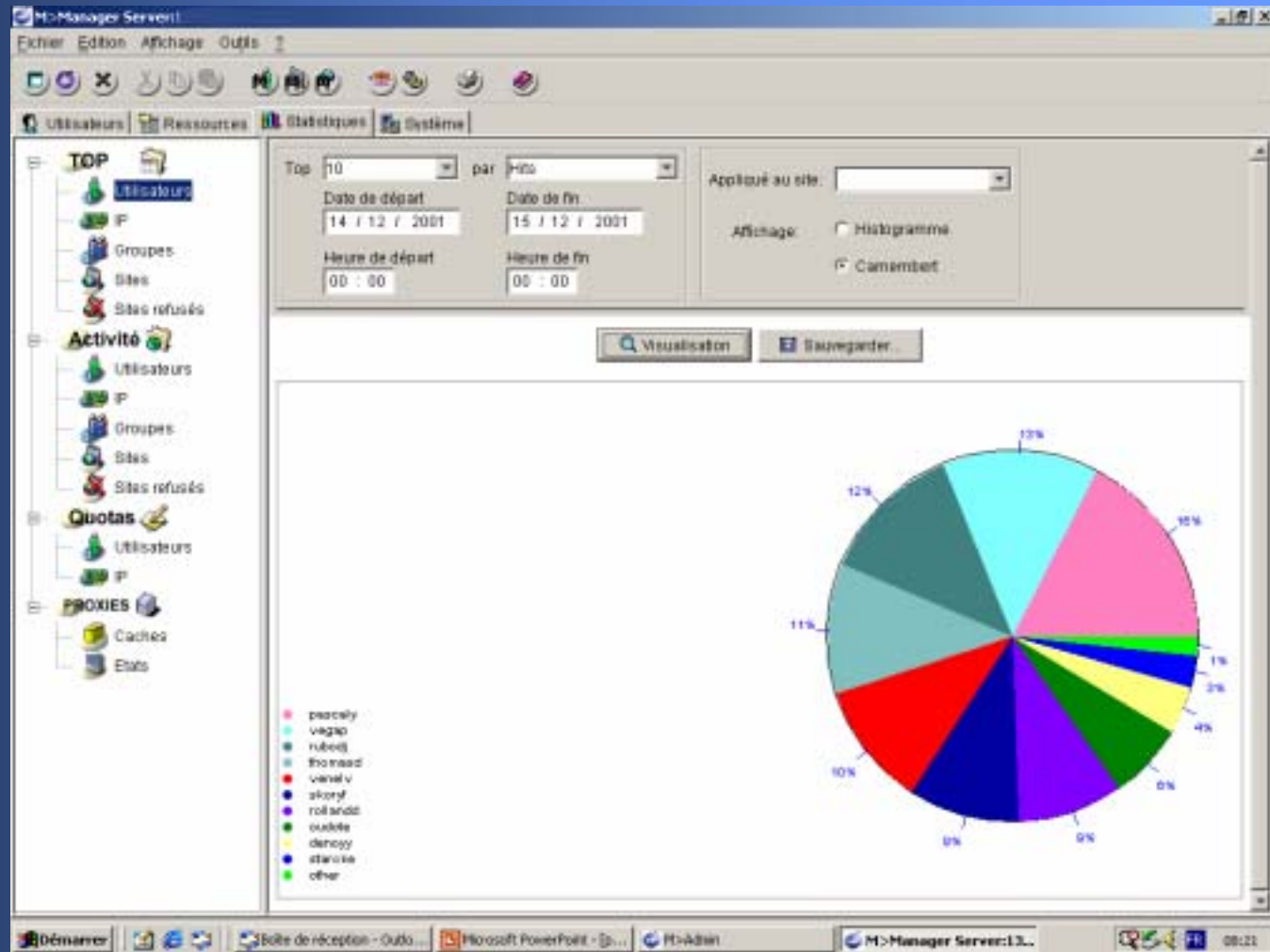
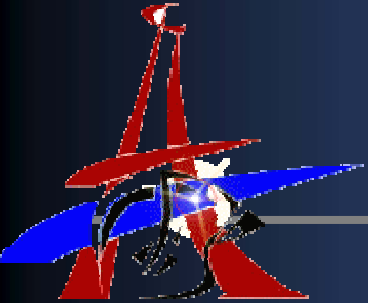
Catégorisation automatique

- Total: 2
- Nombre d'URLs ajoutées: 1300
- Serveur de catégorisation: 127.0.0.1:9799
- Catégorisation automatique: Activé

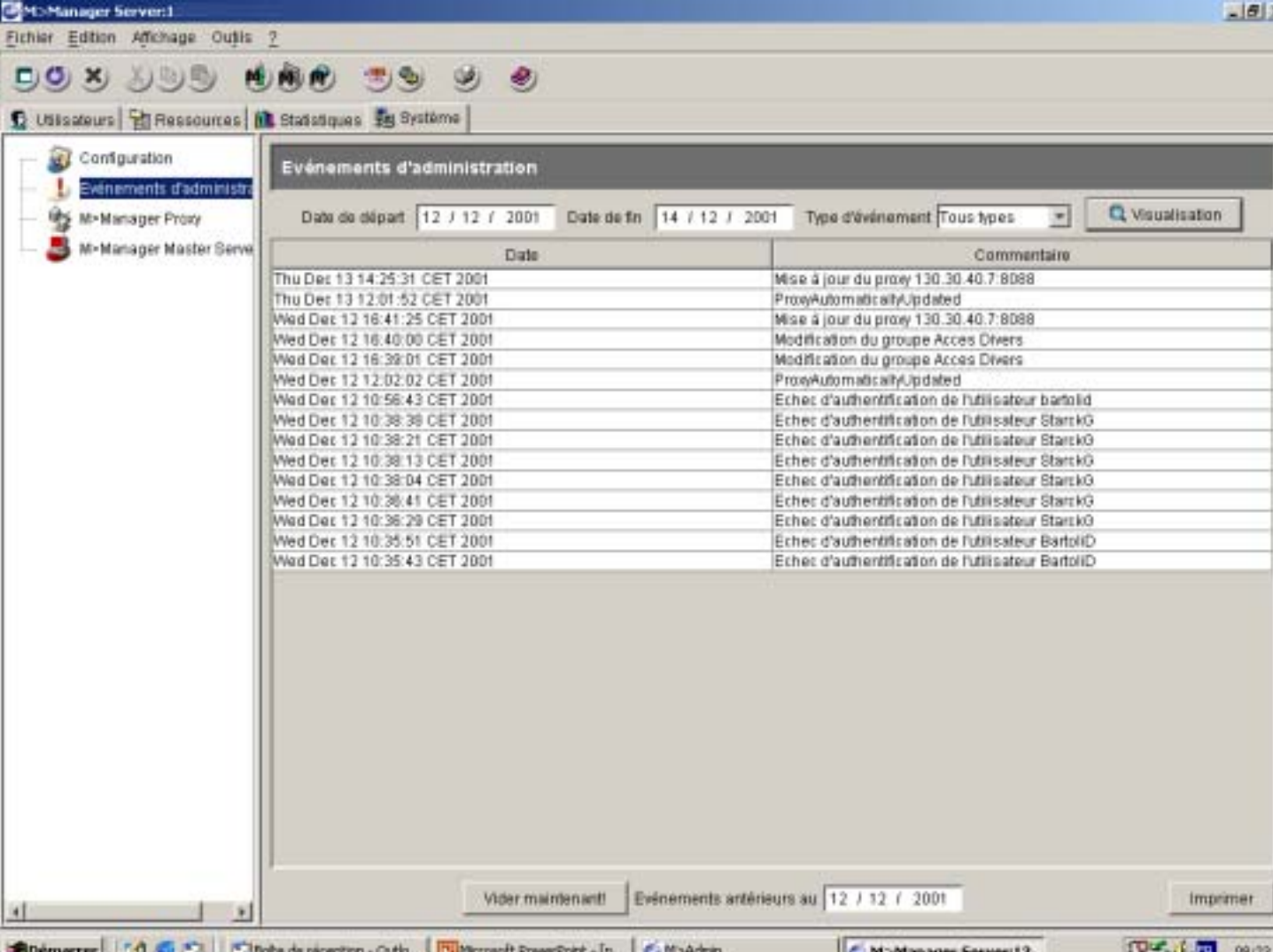
Catégories importées

- Nombre de catégories importées: 11758
- Nombre d'URLs importées: 156314
- Serveur HTTP: www.matranet.com:80
- Fichier: nomade/matrane/nomade_y20.zip
- Mise à jour automatique: Déactivé

Exploitation



Exploitation



The screenshot displays the M-Manager Server 1 administration console. The interface includes a menu bar (Fichier, Edition, Affichage, Outils, ?), a toolbar with various icons, and a navigation pane on the left with options like Configuration, Evénements d'administration, M-Manager Proxy, and M-Manager Master Serveur. The main area shows a table of administrative events with columns for Date and Commentaire. The table is filtered for the period from 12/12/2001 to 14/12/2001. The events list includes proxy updates, group modifications, and multiple authentication failures for users such as barfoiD, StarckO, and BartoiD.

Date	Commentaire
Thu Dec 13 14:25:31 CET 2001	Mise à jour du proxy 130.30.40.7:8088
Thu Dec 13 12:01:52 CET 2001	ProxyAutomaticallyUpdated
Wed Dec 12 16:41:25 CET 2001	Mise à jour du proxy 130.30.40.7:8088
Wed Dec 12 16:40:00 CET 2001	Modification du groupe Acces Divers
Wed Dec 12 16:39:01 CET 2001	Modification du groupe Acces Divers
Wed Dec 12 12:02:02 CET 2001	ProxyAutomaticallyUpdated
Wed Dec 12 10:58:43 CET 2001	Echec d'authentification de l'utilisateur barfoiD
Wed Dec 12 10:38:38 CET 2001	Echec d'authentification de l'utilisateur StarckO
Wed Dec 12 10:38:21 CET 2001	Echec d'authentification de l'utilisateur StarckO
Wed Dec 12 10:38:13 CET 2001	Echec d'authentification de l'utilisateur StarckO
Wed Dec 12 10:38:04 CET 2001	Echec d'authentification de l'utilisateur StarckO
Wed Dec 12 10:38:41 CET 2001	Echec d'authentification de l'utilisateur StarckO
Wed Dec 12 10:38:29 CET 2001	Echec d'authentification de l'utilisateur StarckO
Wed Dec 12 10:35:51 CET 2001	Echec d'authentification de l'utilisateur BartoiD
Wed Dec 12 10:35:43 CET 2001	Echec d'authentification de l'utilisateur BartoiD

Exploitation

MATRA not

M-WallM-Tunnel

Etat	Adresse IP	Port	URL	Description
	130.30.40.15	8881		

130.

Ip: 130.

Port: 8881

URL de service:

Description:

Paramétrage...

Exploitation...

Utilisateurs...

Modifier...

Supprimer

Déconnexion...

Démarrer

Microsoft PowerPoint - [p...]

M-Admin

09:24

Exploitation



vue temps-réel de la machine

Fichier Edition Journaux Statistiques Affichage ?

Vue temps-réel Services actifs Statistiques réseau

Charge CPU:

Utilisation des disques:

/	8%
/usr	10%
/var	4%

Statistiques de collision:

eb2	
eb3	
eb0	
eb1	
eb4	

Informations générales:

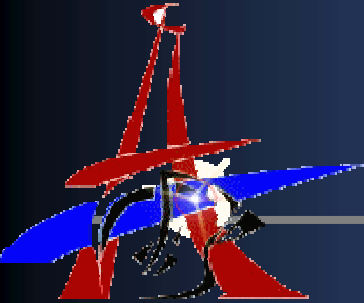
Sessions locales	0
Démarré depuis:	9 days 3:12

Usage mémoire:

Processing rule 1
Reading log files
Switching to real time logs

```
14/12 08:27:34 spfw admhttp-gw[10217]: connection from
14/12 08:27:34 spfw admhttp-gw[10217]: connection from
14/12 08:27:34 spfw admhttp-gw[16869]: daemon port 888
14/12 08:27:34 spfw admhttp-gw[16870]: daemon port 888
14/12 08:27:34 spfw mwadmd[10207]: fwadmin is authenti
14/12 08:27:34 spfw mwadmd[16873]: executing /matranet
14/12 08:27:35 spfw http.80[16096]: permit host=nodnsqu
14/12 08:27:35 spfw http.80[16096]: permit host=nodnsqu
14/12 08:27:35 spfw http.80[16096]: log host=nodnsquery
14/12 08:27:35 spfw http.80[16096]: permit host=nodnsqu
14/12 08:27:35 spfw http.80[16096]: permit host=nodnsqu
14/12 08:27:35 spfw http.80[16096]: log host=nodnsquery
14/12 08:27:36 spfw http.80[16096]: exit host=nodnsquery
14/12 08:27:36 spfw http.80[16096]: exit host=nodnsquery
14/12 08:27:36 spfw http.80[16096]: permit host=nodnsqu
```

Exploitation




Configuration de la machine

Fichier Edition ?

MATRAnet

- Systeme
- DNS
- SMTP
- Routes
- Accès local
- Configuration réseau
 - Noms de réseaux
 - Interfaces réseau
- Services
 - Activation des services
 - Groupes de services
 - Politiques
 - Authentification
- Sécurité
 - Filtre de paquets
 - NAT
 - Règles de sécurité

Systeme



Système d'exploitation: UNIX/BSD-OS/386

Configuration machine

Nom de machine:

Nom de domaine:

LICENCE LOGICIELLE

Produits MATRAnet installés: MWALL

Adresse MAC:

Type de licence: LICENSE (100 utilisateurs) (P2537)

Certificat délivré à: SAPEUR POMPIER DE PARIS

Validité du certificat: lundi 26 novembre 2001 12:00 - vendredi 13 avril 2029 12:00

Logiciels additionnels:

Restriction d'utilisation: FRANCE

Sauvegarder et quitter... Sauvegarder Quitter

Exploitation



The screenshot shows the MATRA net network configuration window. The title bar reads "Configuration de la machine". The window title is "Interfaces réseaux" with the subtitle "Configuration réseau". The left sidebar contains a tree view with categories: Système (DNS, BMT, Routes, Accès locaux), Configuration réseau (Noms de réseaux, Interfaces réseau), Services (Activation des services, Groupes de services, Politiques, Authentification), and Sécurité (Filtre de paquets, NAT, Règles de sécurité). The main area displays a table of network interfaces.

Etat	Nom commun	Couleur	Interface	Adresse IP	Masque	Média actif
⊖	I-Invalde (eb0)		eb0		255.255.0.0	auto
⊕	dmz (eb1)	Green	eb1		255.255.255.0	auto
⊕	AntiVirus (eb2)	Yellow	eb2		255.255.255.0	auto
⊕	I-Externe (eb3)	Red	eb3		255.255.0.0	auto
⊕	Ian (eb4)	Cyan	eb4		255.255.0.0	auto

Buttons at the bottom right: "Modifier..." and "Imprimer...".

Antispoofing et transparence

Exploitation

The screenshot displays the MATRA net network configuration interface. The main window is titled 'Interfaces réseaux' and shows a table of network interfaces. A dialog box titled 'Configurer une carte réseau...' is open, allowing configuration for a specific interface.

Table: Interfaces réseau

Etat	Nom commun	Couleur	Interface	Adresse IP	Masque	Média actif
Invalide (eb0)			eb0		255.255.0.0	auto
						auto
						auto
						auto
						auto

Configurer une carte réseau...

Nom commun: Antivirus (eb2)

Interface physique: eb2

Options d'interface réseau:

- Adresse IP: []
- Masque de réseau: 255.255.255.0
- Drapeaux optionnels: []
- Type de média: auto

Couleur associée avec l'interface: [orange]

Ensembles de réseaux autorisés:

- Réseaux autorisés: []

Utiliser l'antispoofing:

Utiliser la transparence:


Moins d'informations sur la carte...

Informations sur la carte:

- Adresse MAC: []
- Type de carte: Ethernet
- Nom de la carte: com Ethernet 10/100base
- Vitesse de la carte: 100Mbps
- Statut de la carte: UP

Buttons: Sauvegarder et quitter, Ok, Annuler, Imprimer...

Exploitation



Configuration de la machine

Fichier Edition ?

Noms de réseau
Configuration réseau

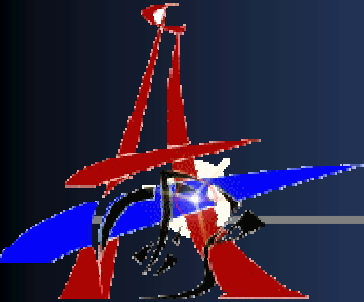
Noms de réseaux

Nom de réseaux	Adresses IP
Internet	
LAN	132.174.255.255
Anti-Virus	11.11.11.11
DMZ	11.11.11.11
DNS externe	21.11.11.11
MManager	12.11.11.11
Brv messagerie interne	13.11.11.11
DNS interne	14.11.11.11
BRV SMTP externe	21.11.11.11
FW	15.11.11.11
LAN-CMSI	12.11.11.11
LAN-PORTABLE	13.11.11.11
LAN-BPF	11.11.11.11
Acces FTP	13.11.11.11

Recherche... Modifier... Ajouter... Supprimer... Imprimer...

Sauvegarder et quitter... Sauvegarder... Quitter

Exploitation



Configuration de la machine

Echier Edition ?

MATRA net

Système
DNS
BMP
Routes
Accès locaux
Configuration réseau
Noms de réseaux
Interfaces réseau
Services
Activation des services
Groupes de services
Politiques
Authentification
Sécurité
Filtre de paquets
NAT
Règles de sécurité

Filtre de paquets

Sécurité

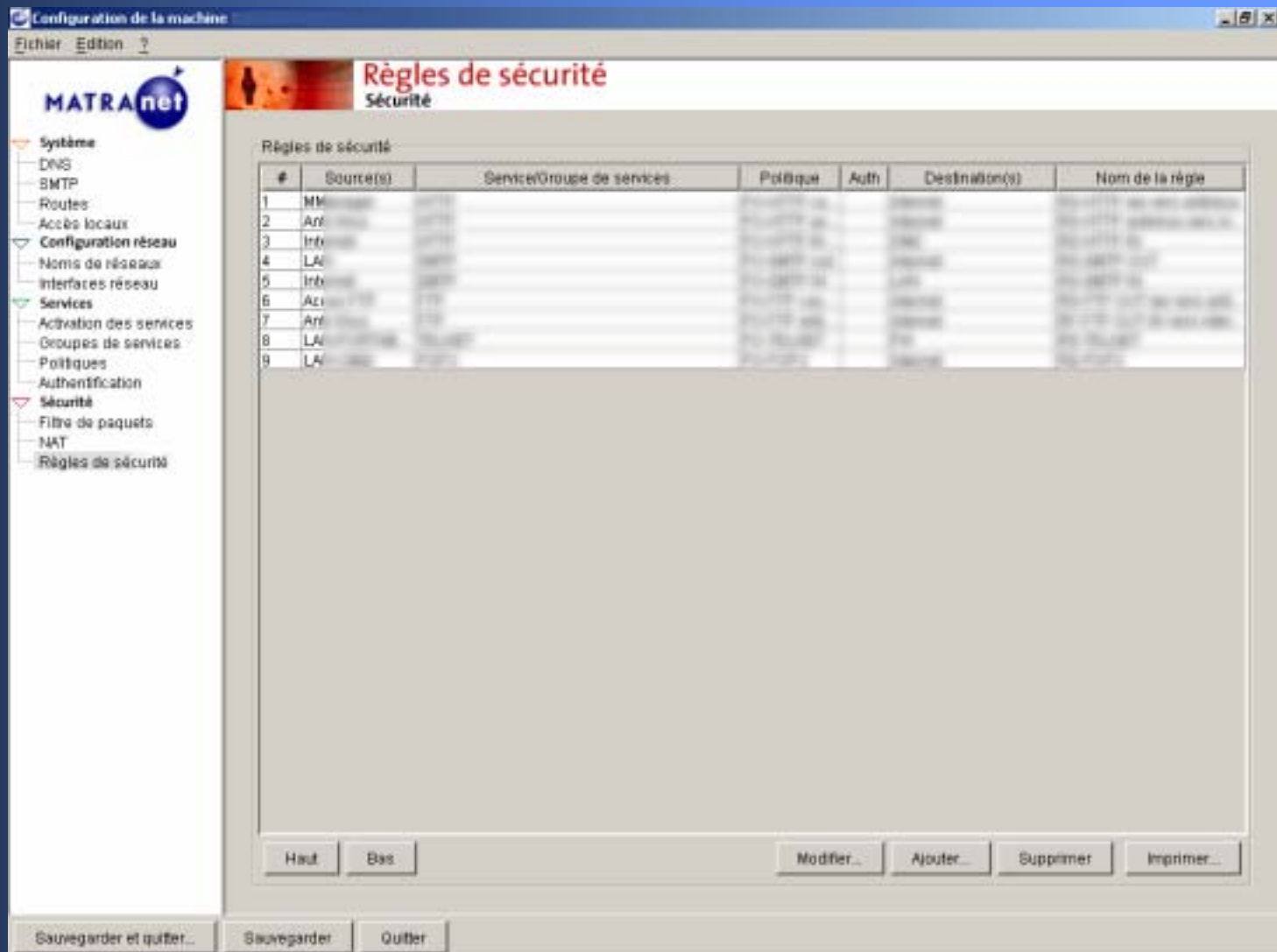
Règles de filtre de paquets

#	Nom de la règle	Type de règle	Adresse source	Port source	Adresse de destination	Port de destination	Accès	Protocole
1	RF1-DNS	Statique						
2	RF2-DNS	Statique						
3	RF3-DNS	Statique						
4	RF1-FTP OUT	Statique						
5	RF2-FTP OUT	Statique						
6	RF3 bis-FTP OUT	Statique						
7	RF3-FTP OUT	Statique						
8	RF4-FTP OUT	Statique						
9	RF1-HTTP OUT	Statique						
10	RF2-HTTP OUT	Statique						
11	RF3-HTTP OUT	Statique						
12	RF3 bis-HTTP OUT	Statique						
13	RF4-HTTP OUT	Statique						
14	RF1-HTTP IN	Statique						
15	RF3-HTTP IN at...	Statique						
16	RF1-SMTP OUT	Statique						
17	RF1 bis-SMTP OUT	Statique						
18	RF2-SMTP OUT	Statique						
19	RF1-SMTP IN	Statique						
20	RF2-SMTP IN	Statique						
21	RF2-SMTP IN	Statique						
22	RF4-SMTP IN	Statique						
23	RF5-SMTP IN	Statique						
24	RF1-TELNET sur	Statique						
25	RF1-BUL-SMBOW	Statique						
26	RF1-TELNET sur	Statique						
27	RF1-POP3	Statique						
28	RF1 bis-POP3	Statique						
29	RF2-POP3	Statique						

Haut Bas Recherche... Modifier... Ajouter... Supprimer Imprimer...

Sauvegarder et quitter... Sauvegarder Quitter

Exploitation



The screenshot displays the MATRANet configuration window for security rules. The interface includes a navigation tree on the left, a main table of rules, and control buttons at the bottom.

Configuration de la machine
Fichier Edition ?

MATRANet

Règles de sécurité
Sécurité

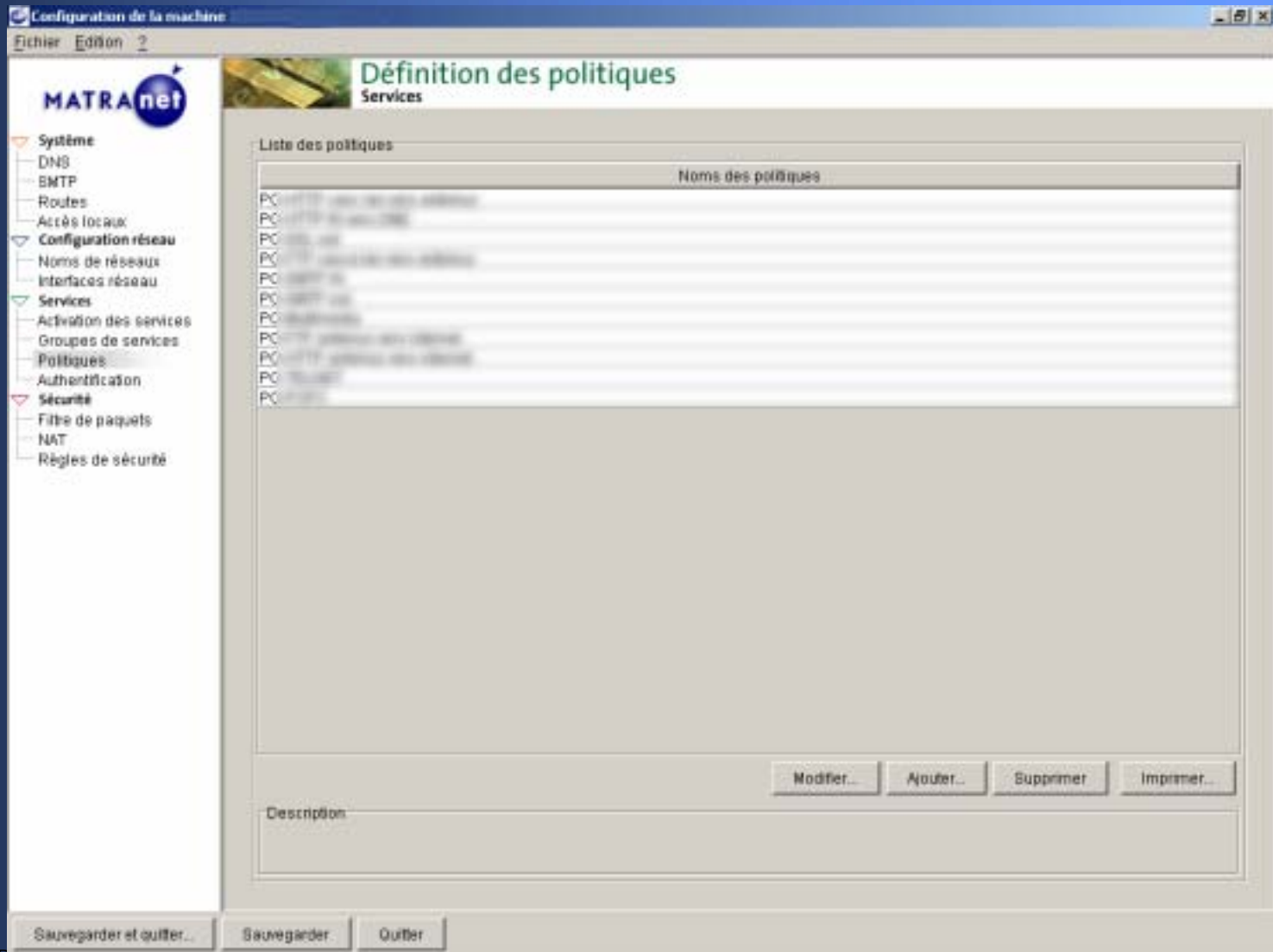
Règles de sécurité

#	Source(s)	Service/Groupe de services	Politique	Auth	Destination(s)	Nom de la règle
1	MM					
2	Ant					
3	Int					
4	LA					
5	Int					
6	Azi					
7	Ant					
8	LA					
9	LA					

Haut Bas Modifier... Ajouter... Supprimer... Imprimer...

Sauvegarder et quitter... Sauvegarder Quitter

Exploitation



The screenshot shows the MATRA net configuration interface. The main window is titled "Définition des politiques" (Policy Definition) under the "Services" category. The left sidebar contains a tree view with the following items:

- Systeme
 - DNS
 - BMP
 - Routes
 - Accès locaux
- Configuration réseau
 - Noms de réseaux
 - Interfaces réseau
- Services
 - Activation des services
 - Groupes de services
 - Politiques
 - Authentification
- Sécurité
 - Filtre de paquets
 - NAT
 - Règles de sécurité

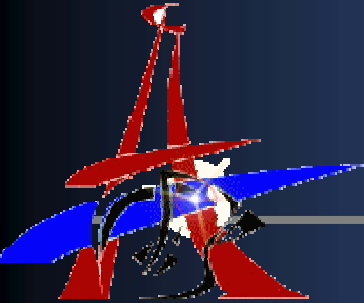
The main area displays a table titled "Liste des politiques" (List of policies) with the following columns:

Noms des politiques
PC-1111 - accès des réseaux
PC-1112 - accès des réseaux
PC-1113 - accès des réseaux
PC-1114 - accès des réseaux
PC-1115 - accès des réseaux
PC-1116 - accès des réseaux
PC-1117 - accès des réseaux
PC-1118 - accès des réseaux
PC-1119 - accès des réseaux
PC-1120 - accès des réseaux
PC-1121 - accès des réseaux
PC-1122 - accès des réseaux
PC-1123 - accès des réseaux
PC-1124 - accès des réseaux
PC-1125 - accès des réseaux
PC-1126 - accès des réseaux
PC-1127 - accès des réseaux
PC-1128 - accès des réseaux
PC-1129 - accès des réseaux
PC-1130 - accès des réseaux

At the bottom of the window, there are buttons for "Modifier..." (Modify...), "Ajouter..." (Add...), "Supprimer" (Delete), and "Imprimer..." (Print...). Below the table is a "Description" field.

At the bottom of the application window, there are buttons for "Sauvegarder et quitter..." (Save and quit...), "Sauvegarder" (Save), and "Quitter" (Quit).

Exploitation



Configuration de la machine

Fichier Edition ?

MATRAnet

- Systeme
 - DNS
 - SMTP
 - Routes
 - Accès local
- Configuration réseau
 - Noms de réseaux
 - Interfaces réseau
- Services
 - Activation des services
 - Groupes de services
 - Politiques
 - Authentification
- Sécurité
 - Filtre de paquets
 - NAT
 - Règles de sécurité

Activation des services

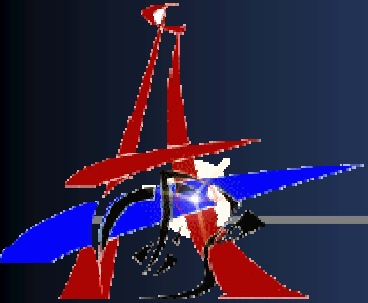
Services

Activation des services

Etat	Noms des services	Type	Port
	H...		
	B...		
	M...		
	F...		
	S...		
	T...		
	P...		

Modifier... Ajouter... Supprimer Imprimer...

Démarrer [Taskbar icons] Microsoft PowerPoint - [p...] M>Admin Configuration de la ma... 09:50



Exploitation

Sauvegarde

Rapport1 par messagerie

Rapport2 par messagerie



Conclusion

Les plus
Produit stable
Support technique très efficace

Les moins
Bug madmin
Stratégie groupe nb de connexion maxi
Statistiques pas de zoom
Sémantica gourmand mémoire