Network Systems®

# Les Fonctions de Sécurité Network Systems®

Network Systems®


# Robert Bugnet

**Ingenieur Avant-Vente**

**Network Systems France**

robert.bugnet@network.com

Tel: (33) 1 46 43 70 00

# Claude Piovant

**Directeur Commercial vente Indirect**

**Network Systems France**

piovac@network.com

# Bernard Zeutzius

**Internetworking Product Marketing Manager**

**Network Systems Europe**

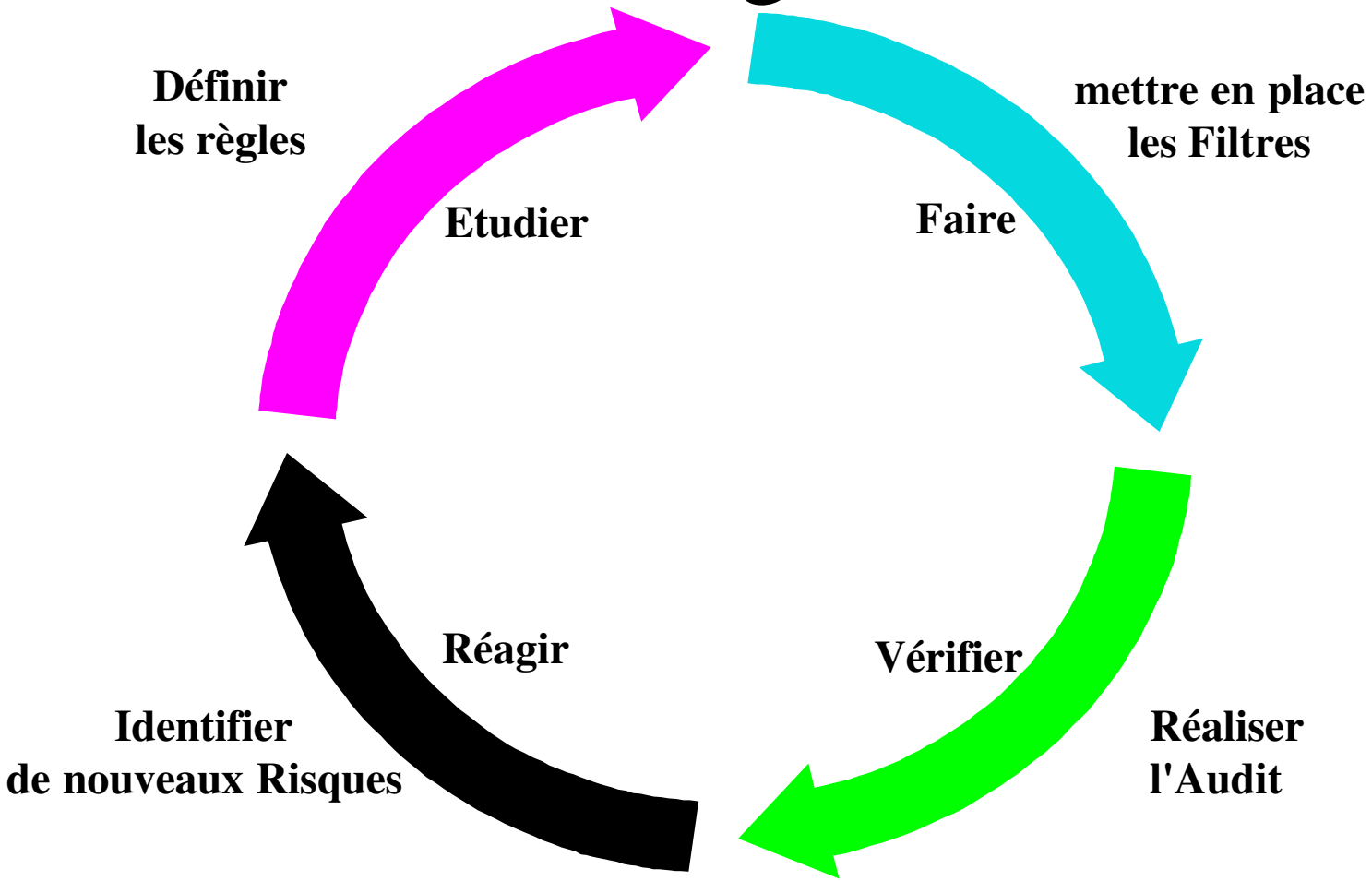
bernard.zeutzius@network.com

Network Systems®

# Agenda

- Définition des règles de Sécurité
- Sécurité par Filtrage
- Sécurité par les réseaux virtuels
- Sécurité par le chiffrement
- Optimisation des Lignes PTT
- Sécurité par les protections physiques du réseau
- Administration et outils
- Evolutions

# Définir les règles de Sécurité



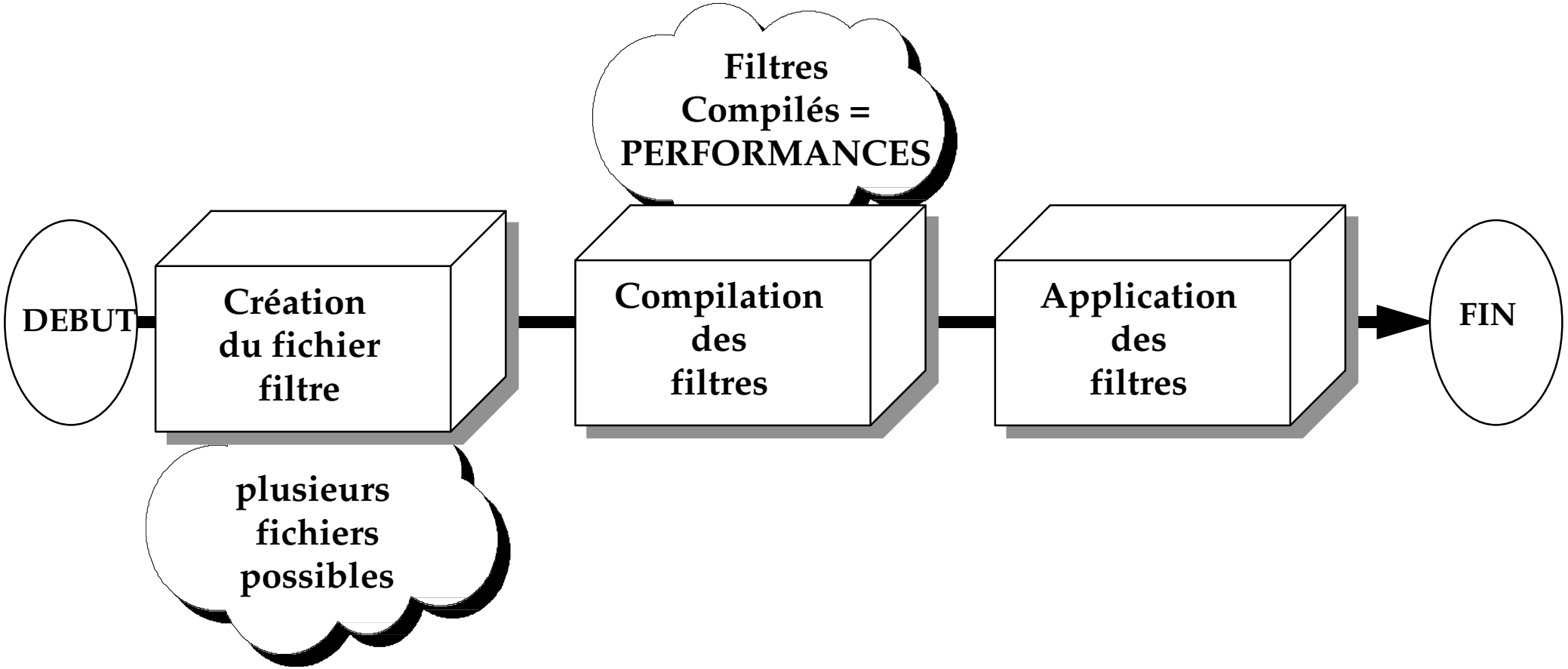
Network Systems®

# La sécurité par Filtrage avec *NETSENTRY*

- Filtrage d'après les en-têtes des paquets
  - Autoriser/Interdire l'accès
  - Modifier les datagrammes
  - Chiffrement
- Filtrage sur différents niveaux d'accès
  - Couche Liaison - Addresse physique
  - Couche Réseau - Réseau logique
  - Couche Transport - Type d'application
  - Couche hautes - Commandes particuliéres
- Modification dynamique des filtres sans perte de donnée

Network Systems®

# Règles de filtrage



# Syntaxe *NetSentry*

Les Filtres sont composés de trois éléments:

- **Patterns**
  - »Que cherchons nous dans ce message?
- **Actions**
  - »Que faisons nous si nous le trouvons?
- **Dispositions**
  - »Que faisons nous du message lui-même?

Network Systems®

# Exemple de filtre *NetSentry (1)*...

## La création d'un filtre

```
FILTER      telnet_only                          * Nom du filtre

            TCP_SP in (23)                       * Pattern:Teste le port source 23 (telnet)
            BREAK;                               * Disposition : laisse passer

            TCP_DP in (23)                        * Pattern : Teste le port destination 23
            BREAK;                               *  Disposition : Laisse passer

            ANY                                  * Pattern : Tout le reste
            COPY_TO 129.210.1.64   1781           * Action : copie la trame
            FAIL;                                * Disposition : détruit

            END                                  * FIN
```

Network Systems®

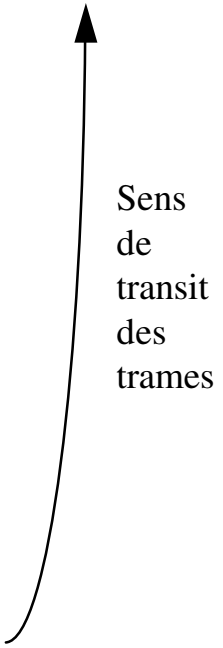
# Exemple de filtre *NetSentry (2)*...

**La mise en place :**

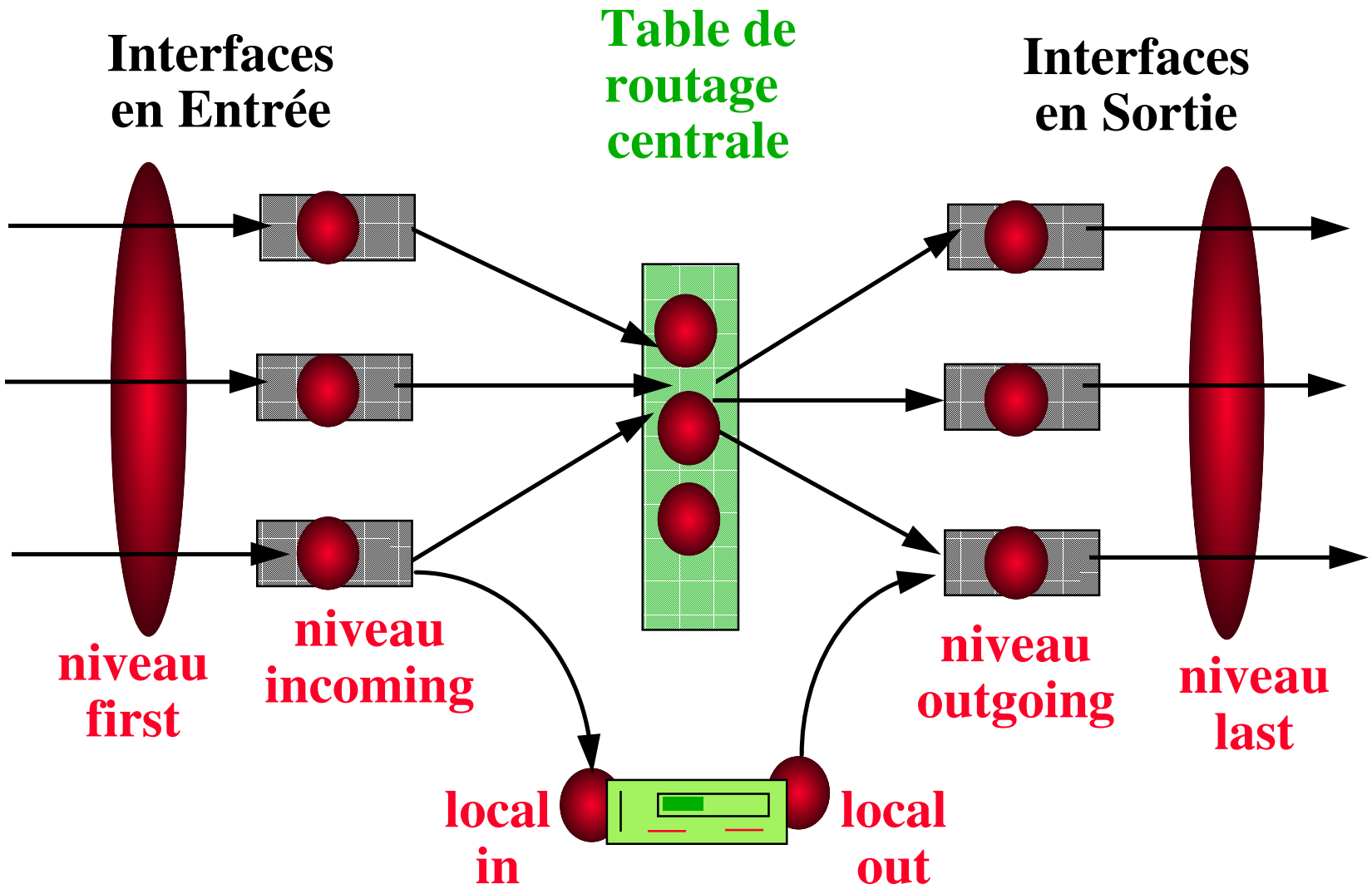
**APPLY** bad on * tofrom *
**APPLY** telnet-only on 129.210.1.* to *
**APPLY** telnet-only on 129.210.1.1 from 12.*.*.*
**APPLY** telnet-only on 129.210.1.2 tofrom 12.3.1.6
**APPLY** telnet-only on 129.210.1.32 tofrom *

.....

.....



# *NetSentry:* Les 5 niveaux d'application des filtres...



Network Systems®

# Pattern Recherche sur messages IP

## Sur champs particuliers :

*Niveau MAC*

**Multicast**
**Mac Source,dest (masque)**
**DSAP ,SSAP ,SNAP**
**Longueur du datagramme**
**En-tête Token ring**
**Paquet type**
**1, 2, 4 octets particuliers (masque)**
**Recherche de domaines**

*Niveau Transport*

**TCP bit Syn ou Ack**
**Port TCP/UDP source ou dest**
**1, 2, 4 octets particuliers (masque)**

*Niveau IP*

**Broadcast IP**
**IP source, destination (masque)**
**Type de protocole (TCP,UDP,ICMP etc...)**
**Longueur du datagramme**
**N° de fragment**
**Option particulière (Ripso DNSIX)**
**T.O.S**
**Time to live**
**Prochain routeur**
**1, 2, 4 octets particuliers (masque)**

*Niveau Supérieur*

**1, 2, 4 octets particuliers (masque)**

## Sur événement :

**Dates et heures**
**Réponse à ping**
**Verification IP-->MAC**

Network Systems®

# Pattern Recherche sur messages Decnet

## Sur champs particuliers :

*Niveau MAC*

**Multicast**
**Mac Source,dest (masque)**
**DSAP ,SSAP ,SNAP**
**Longueur du datagramme**
**En-tête Token ring**
**Paquet type**
**1, 2, 4 octets particuliers (masque)**
**Recherche de domaines**

*Niveau Decnet*

**Decnet source, destination**
**1, 2, 4 octets particuliers (masque)**

*Niveau Supérieur*

**1, 2, 4 octets particuliers (masque)**

## Sur événement :

**Dates et heures**

Network Systems®

# Pattern Recherche sur messages IPX

## Sur champs particuliers :

*Niveau MAC*

**Multicast**
**Mac Source,dest (masque)**
**DSAP ,SSAP ,SNAP**
**Longueur du datagramme**
**En-tête Token ring**
**Paquet type**
**1, 2, 4 octets particuliers (masque)**
**Recherche de domaines**

*Niveau IPX*

**IPX source, destination host**
**IPX source, destination réseau**
**IPX source, destination socket**
**1, 2, 4 octets particuliers (masque)**

*Niveau Supérieur*

**1, 2, 4 octets particuliers (masque)**

## Sur événement :

**Dates et heures**

Network Systems®

# Pattern Recherche sur messages Appletalk*

## Sur champs particuliers :

*Niveau MAC*

**Multicast**
**Mac Source,dest (masque)**
**DSAP ,SSAP ,SNAP**
**Longueur du datagramme**
**En-tête Token ring**
**Paquet type**
**1, 2, 4 octets particuliers (masque)**
**Recherche de domaines**

*Niveau Appletalk*

**Appletalk source, destination host**
**Appletalk source, destination socket**
**1, 2, 4 octets particuliers (masque)**

*Niveau Supérieur*

**1, 2, 4 octets particuliers (masque)**

## Sur événement :

**Dates et heures**

* Disponible fin 95

Network Systems®

# Pattern Recherche sur messages Pontés

## Sur champs particuliers :

*Niveau MAC*

**Multicast**
**Mac Source,dest (masque)**
**DSAP ,SSAP ,SNAP**
**Longueur du datagramme**
**En-tête Token ring**
**Paquet type**
**1, 2, 4 octets particuliers (masque)**
**Recherche de domaines**

*Niveau Transport*

**TCP bit Syn ou Ack**
**Port TCP/UDP source ou dest**
**1, 2, 4 octets particuliers (masque)**

*Niveau Supérieur*

**1, 2, 4 octets particuliers (masque)**

*Niveau Routage: IP*

**Broadcast IP**
**IP source, destination (masque)**
**Type de protocole (TCP,UDP,ICMP etc...)**
**Longueur du datagramme**
**N° de fragment**
**Option particulière (Ripso DNSIX)**
**T.O.S**
**Time to live**
**Prochain routeur**
**1, 2, 4 octets particuliers (masque)**

*: Decnet*

**Decnet source, destination**

*: IPX*

**IPX source, destination host**
**IPX source, destination réseau**
**IPX source, destination socket**

*: Appletalk*

**Appletalk source, destination host**
**Appletalk source, destination socket**

## Sur événement :

**Dates et heures**

Network Systems®

# Action

## Pour IP

**Statistiques**
**2 compteurs**
**Icmp_unreachable**
**Translation d'adresse IP source ou dest**
**Reroutage**
**Rajout d'option (RIPSO,DNSIX)**
**Retrait d'option**
**Chiffrement**

## En Général

**Alarmes (locales ou distantes)**
**copie de message**
**Prioritisation**

# Disposition

- **4 dispositions permettent aux messages de:**
  - »Sortir du routeur directement
  - »Sortir du filtre pour aller au niveau d'application suivant (Ex:First --->Incoming)
  - »Continuer le traitement dans le filtre lui-même
  - »Etre détruit

Network Systems®

# *Application*: Comptabilité IP

- Matrice de couple d'adresse IP
- Selection sur tout type de champ ou par interface
- Comptage Octets et Trames dans chaque sens

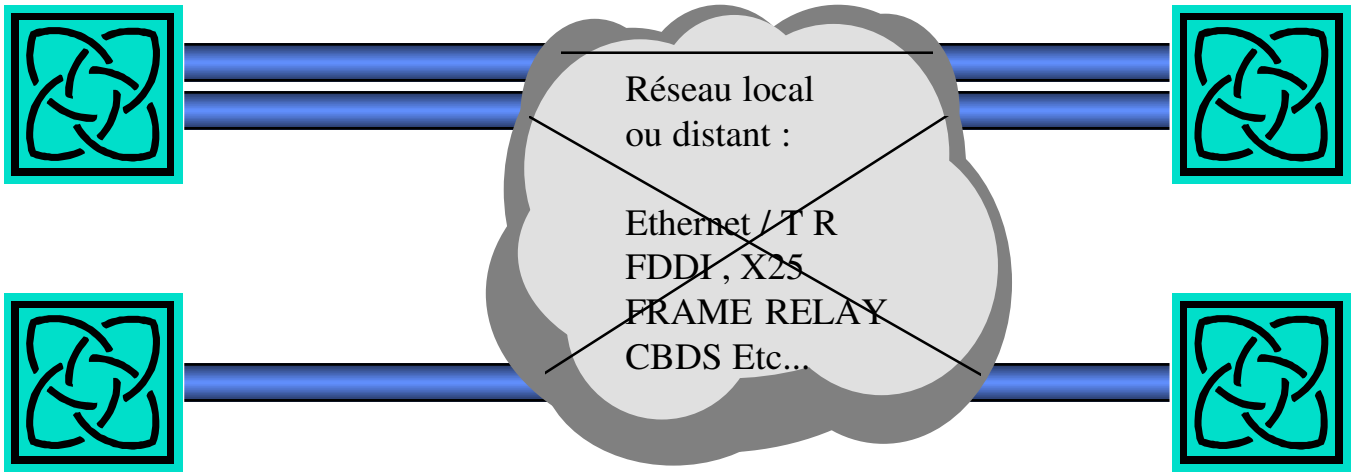
Network Systems®

# *Application*: La sécurité par les Réseaux virtuels

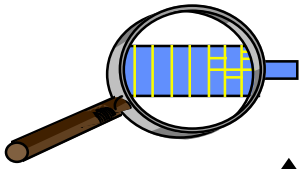
- La notion de Domaine offerte par NetSentry permet de scinder votre réseau en un ensemble de réseaux indépendants tout en utilisant un backbone commun (Méthode Tagging).
- Les domaines peuvent etre Définis à partir de tout type de pattern.
- Les ponts supportent un STP différent par domaine.

# Le chiffrement par DPF

- Encapsulation sous IP de messages IP chiffrés
- Plusieurs sessions sécurisées possibles vers différents sites avec différents paramètres de chiffrement
- Tout type de paramétrage est possible




Reseau privé , Internet , Renater , Transpac , Numéris etc....



# Le chiffrement par DPF

- *<u>Privatisation</u> avec DES ,IDEA ,NSC1*
  - Personne ne peut déterminer le contenu de vos communications en examinant les données.

- *<u>Authentification</u> par RSA et Diffie-Hellman*
  - Le message provient d'une source authentique, et n'a pas été crée par une personne externe malveillante.
  - Des clés sont échangées confidentiellement et changées régulièrement avec le flux de données.

- *<u>Integrité des données</u>(Signature Digitale) par MD5*
  - Le contenu de vos messages n'as pas été changé durant la transmission

- *<u>Non-répudiation</u>*
  - Tous les messages doivent étre déchiffré pour garder un dialogue continu entre les deux parties.

Network Systems®

# Optimisation des lignes PTT

- Compression des données par *ALDC* (source IBM)
- Prioritisation du traffic le plus important sur une ligne congestionnée
- Selection basée sur les filtres NetSentry
  - Adresse, application
  - Interface, plage horaire, table de routage
- 255 niveaux de priorité

Network Systems®

# La sécurité au niveau physique

- Sécurité par les hubs Network Systems (Bytex)
  - Gestion des Adresses MAC
  - Controle d'intrusion
- Brouillage des données (Eavesdropping)
- Controle d'adresses IP/MAC par *NetSentry*
  - Comparaison adresse MAC / Adresse IP (HSA_OKAY)

Network Systems®

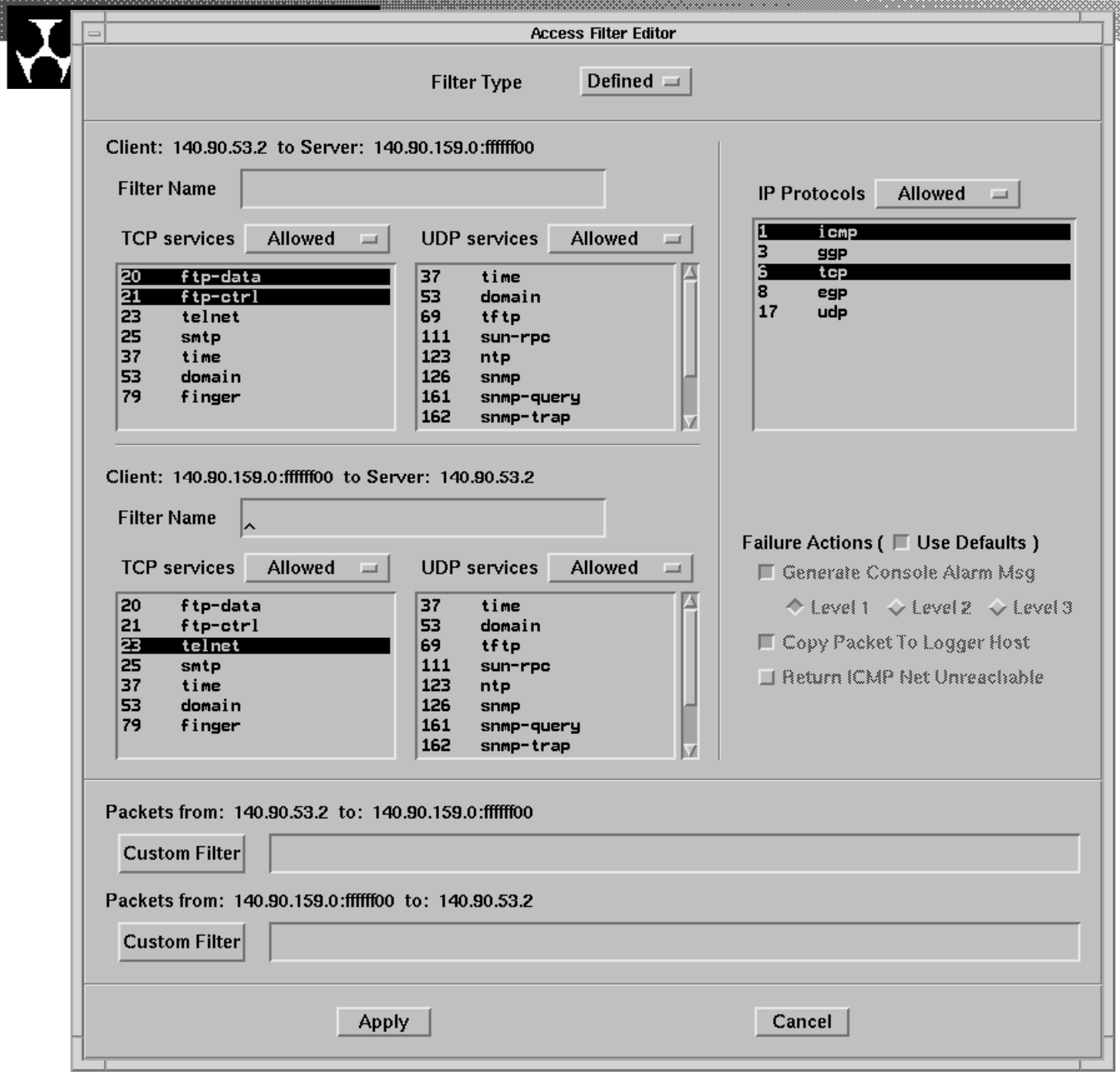
# Les outils d'administration de la sécurité

- *PCF Tools* crée et gère les Filtres
- *PCF Logger* crée et gère les événements
- *NetStalker* réalise l'audit des événements

Network Systems®

# *PCF Tools* Crée et gère les Filtres

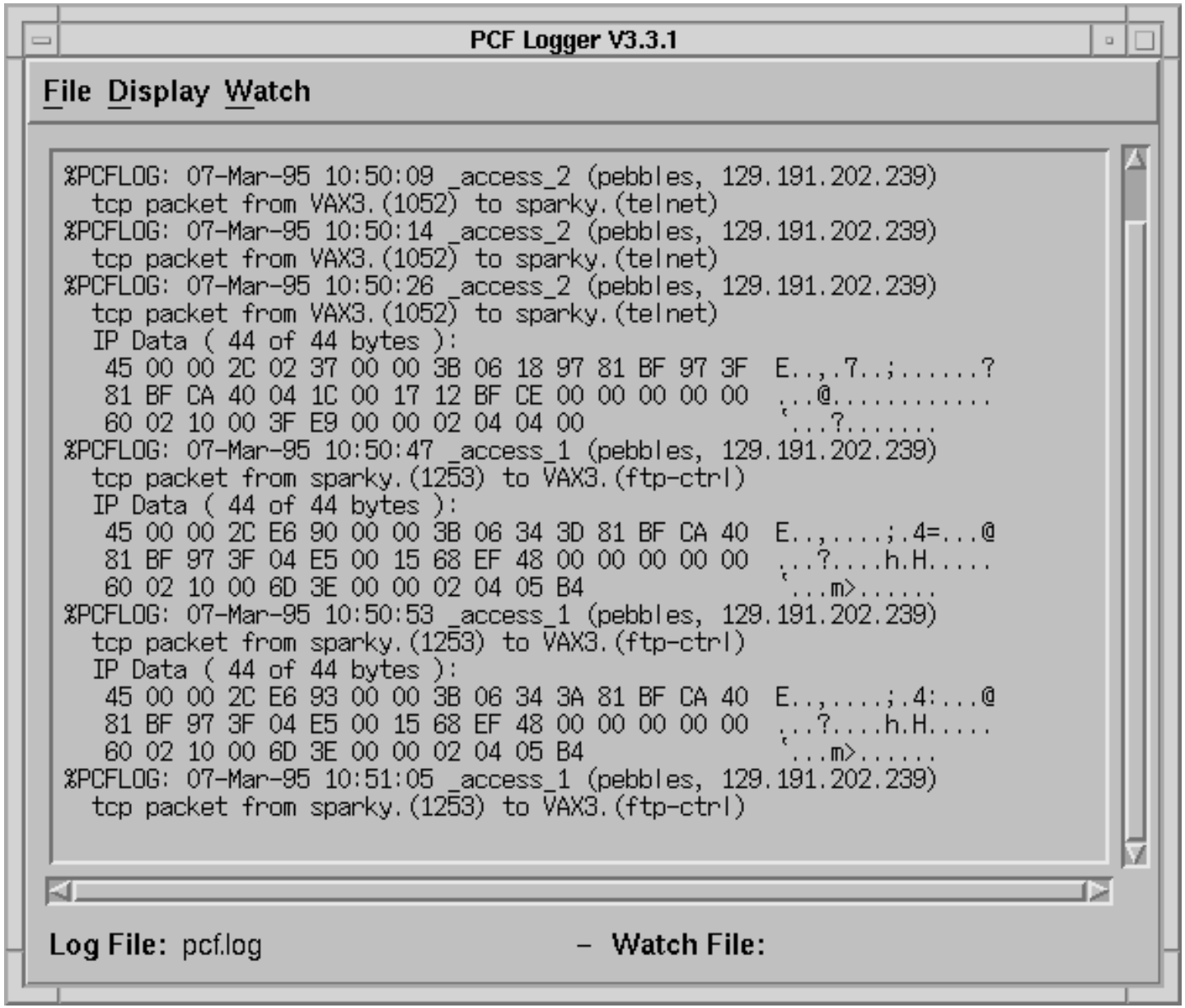
- L'interface utilisateur X-Windows OSF/Motif permet  la création et l'administration facile des filtres .
- Les configurations des routeurs sont archivées et gérées depuis un seul point.
- Supervision centrale possible de centaines de routeurs.
- Librairie de filtres classiques fournie avec *PCF Tools* + filtres spécifiques crées par le gestionnaire.


Access Filter Editor
Filter Type
Defined
Client: 140.90.53.2 to Server: 140.90.159.0:ffffff00
Filter Name
TCP services
Allowed
UDP services
Allowed
20 ftp-data
21 ftp-ctrl
23 telnet
25 smtp
37 time
53 domain
79 finger
37 time
53 domain
69 tftp
111 sun-rpc
123 ntp
126 snmp
161 snmp-query
162 snmp-trap
IP Protocols
Allowed
1 icmp
3 ggp
6 tcp
8 egp
17 udp
Client: 140.90.159.0:ffffff00 to Server: 140.90.53.2
Filter Name
TCP services
Allowed
UDP services
Allowed
20 ftp-data
21 ftp-ctrl
23 telnet
25 smtp
37 time
53 domain
79 finger
37 time
53 domain
69 tftp
111 sun-rpc
123 ntp
126 snmp
161 snmp-query
162 snmp-trap
Failure Actions ( Use Defaults )
Generate Console Alarm Msg
Level 1 Level 2 Level 3
Copy Packet To Logger Host
Return ICMP Net Unreachable
Packets from: 140.90.53.2 to: 140.90.159.0:ffffff00
Custom Filter
Packets from: 140.90.159.0:ffffff00 to: 140.90.53.2
Custom Filter
Apply
Cancel

Network Systems®

# *PCF Logger* crée et gère les événements

- **Le Client** *PCF Logger* réside sur une station Unix de surveillance de type SUN
  - ☆ Interface utilisateur X-Windows
  - ☆ Des commandes UNIX peuvent ètre déclenchées sur événement.
- **L'agent** *PCF Logger* est une fonction du routeur qui envoie des copies de datagramme (choisis par filtrage) sur le client.
- **Les notifications donnent différentes informations:**
  - ☆ Date et Heure
  - ☆ Quel routeur et quel filtre génère l'événement
  - ☆ Addresses et ports source et destination IP , TCP/UDP
  - ☆ Paquet entier (Option)


PCF Logger V3.3.1
File Display Watch
%PCFLOG: 07-Mar-95 10:50:09 _access_2 (pebbles, 129.191.202.239)
tcp packet from VAX3.(1052) to sparky.(telnet)
%PCFLOG: 07-Mar-95 10:50:14 _access_2 (pebbles, 129.191.202.239)
tcp packet from VAX3.(1052) to sparky.(telnet)
%PCFLOG: 07-Mar-95 10:50:26 _access_2 (pebbles, 129.191.202.239)
tcp packet from VAX3.(1052) to sparky.(telnet)
IP Data ( 44 of 44 bytes ):
45 00 00 2C 02 37 00 00 3B 06 18 97 81 BF 97 3F E..,.7..;.....?
81 BF CA 40 04 1C 00 17 12 BF CE 00 00 00 00 00 ...@.....
60 02 10 00 3F E9 00 00 02 04 04 00 `...?.....
%PCFLOG: 07-Mar-95 10:50:47 _access_1 (pebbles, 129.191.202.239)
tcp packet from sparky.(1253) to VAX3.(ftp-ctrl)
IP Data ( 44 of 44 bytes ):
45 00 00 2C E6 90 00 00 3B 06 34 3D 81 BF CA 40 E..,....;.4=...@
81 BF 97 3F 04 E5 00 15 68 EF 48 00 00 00 00 00 ...?....h.H.....
60 02 10 00 6D 3E 00 00 02 04 05 B4 `...m>.....
%PCFLOG: 07-Mar-95 10:50:53 _access_1 (pebbles, 129.191.202.239)
tcp packet from sparky.(1253) to VAX3.(ftp-ctrl)
IP Data ( 44 of 44 bytes ):
45 00 00 2C E6 93 00 00 3B 06 34 3A 81 BF CA 40 E..,....;.4:...@
81 BF 97 3F 04 E5 00 15 68 EF 48 00 00 00 00 00 ...?....h.H.....
60 02 10 00 6D 3E 00 00 02 04 05 B4 `...m>.....
%PCFLOG: 07-Mar-95 10:51:05 _access_1 (pebbles, 129.191.202.239)
tcp packet from sparky.(1253) to VAX3.(ftp-ctrl)
Log File: pcf.log
– Watch File:

Network Systems®

# Audit

- 2 fonctions:
  - Vérifier que tout fonctionne
  - Contrôle des connexions
- Regarder tous les événements peut ètre fastidieux
- Un outil logiciel est important pour déterminer une réelle attaque
- Audit à partir des informations de *PCF Logger*
- L'audit fournit des informations tel que:
  - Tentatives de connection erronées
  - Connections habituelles
  - Attaques délibérées

Network Systems®

# L'Audit par *NetStalker*™

- *Stalker* est considéré comme le meilleur programme d'audit mondial.
  - Rapide
  - Facile à utiliser
  - Minimise le nombre d'Alarme
- Conçu pour l'analyse des "logs" UNIX .
- Supporte désormais NetSentry et PCF.
  - *Stalker for Networks*
  - Arrangement Exclusif avec NSC - Seul routeur supporté
- Signale lorsque vous êtes soumis à une attaque

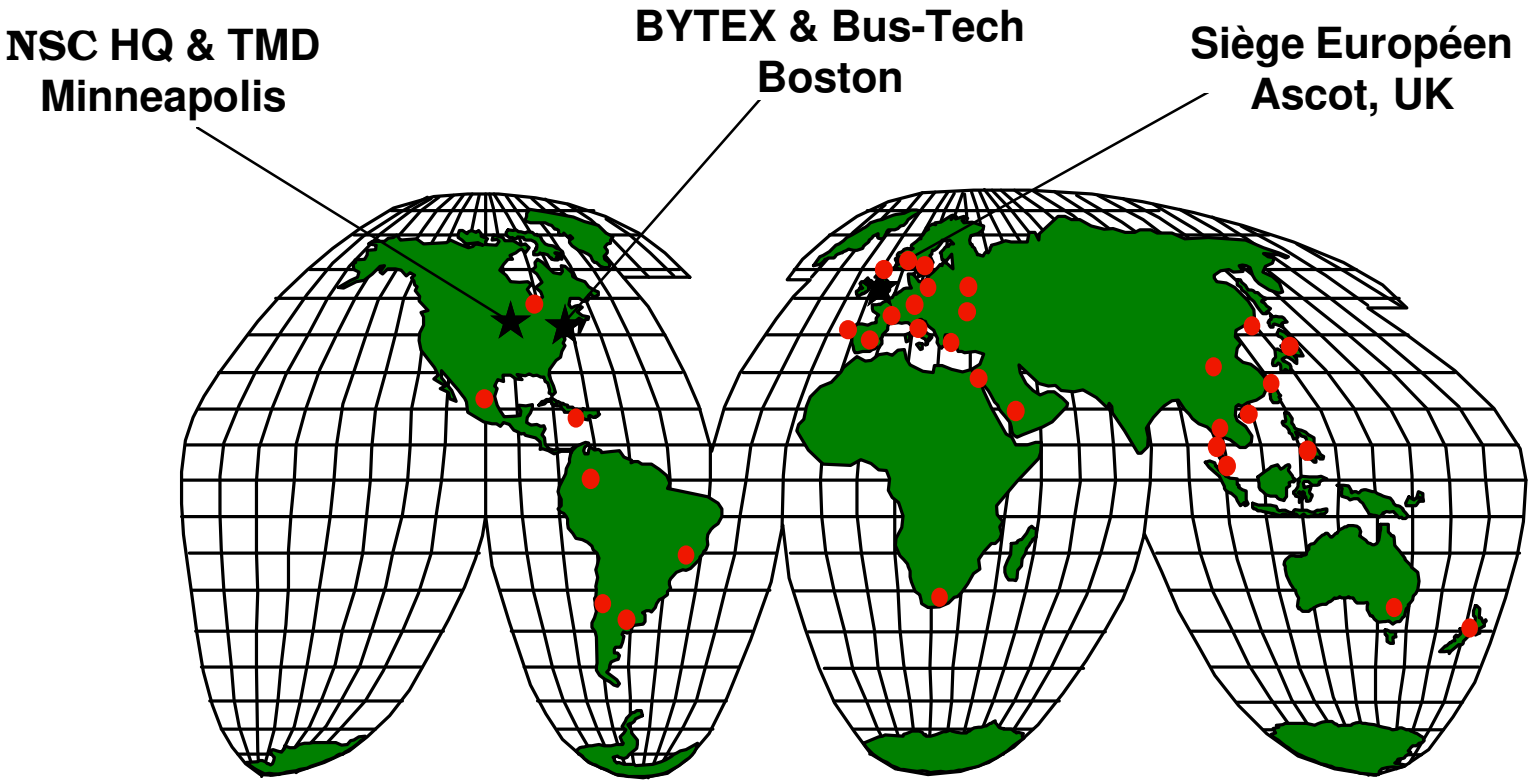
Network Systems®

# Evolutions

- Chiffrement de tout protocoles sous DPF (sous IP)
- Chiffrement de tout protocoles sous DPF (sous autres protocole + pontage)
- Mémorisation d'informations d'état (Port tcp , logging etc...)

Network Systems®

# Qui est NSC

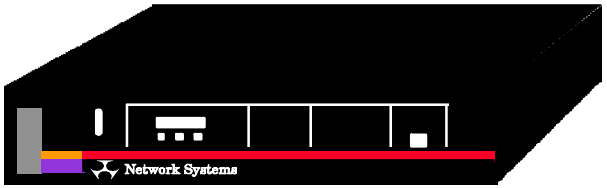



- 1100 Employers
- 11 Filiales Internationales
- 5000+ Installations
- •Ventes , Services et Support mondial
- $231M Revenue

Network Systems®

# Les produits (1)

## *The Security Router*




| ID | Description |
|---|---|
| SR04 | 4 Ethernets |
| SR07 | 2 Ethernets, 2 Lignes Série |
| SR14 | FDDI, 4 Ethernets |
| SR17 | FDDI, 2 Ethernets, 2 Lignes Séries |
| SR19 | FDDI, 4 lignes Séries |

Network Systems®

# Les produits (2)

## *The Border Guard*

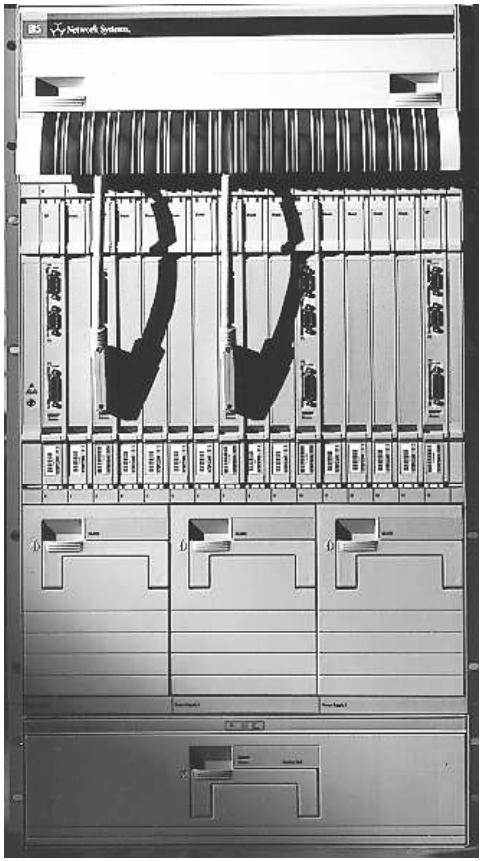
1 Ethernet
1 à 3 lignes séries (Option)

Network Systems®

# Les produits (3)

## ERS

Modulaire
84 Ethernets
56 Token Ring
14 FDDI
42 ATM OC3/DS3
112 Lignes Séries
4 G703 (voix)



Network Systems®

# Disponibilités

| | *PCF/BCF* | *Netsentry* | *DPF* |
|---|---|---|---|
| *The Security Router* | X | SEPT 95 | X |
| *The Border Guard* | X | SEPT 95 | 96 |
| ERS | X | X | 96 |

X : Disponible

Network Systems®

# WINNER

**Data Communications LAN Times**

# BEST

**OF SHOW 1995**

**NETWORLD + INTEROP '95**

**LAS VEGAS**

## PRIX 1995

## NETWORLD + INTEROP '95

# The Security Router

Selectionné par Data Communications et LAN Times comme apportant une signifiante contribution à l'avancement des technologies ,produits ,et services internetworking