HARRIS
COMPUTER SYSTEMS CORPORATION

HARRIS ET LA SECUR

SYSTEME D'EXPLOITATION SECURISE

CX/SX LAN/SX B1

Secure/Power UNIX B2

LE SYSTEME GARDE-BARRIERE

NetGuard (logiciel Firewall)

Le produit CyberGuard

HARRIS
COMPUTER SYSTEMS CORPORATION

Systèmes d'Exploitation HARRIS

Conçus pour multi-processeur symétrique

Temps-Réel

CX/UX 6.2

CX/UX 7.1

Temps-Réel + Sécurité

CX/SX + LAN/SX 6.2 Certifié B1

sur NH 4000 (MC 88100)
NH 5000 (MC 88110)

CX/SX + Netguard

Evaluation FB1/E3 UK

Points communs entre CX/UX et CX/SX

- **Interface de programmation standard**
  SYSTEM V R4 (SVID Issue 3)
- **Mêmes mécanismes temps-réel**
  POSIX 1003.1b
- **Evolution parallèle des souches**
- **Continuité et homgénéité :**
  - **Compatibilité ascendante des interfaces**
  - **Même chaine de compilateurs**

HARRIS
COMPUTER SYSTEMS CORPORATION

Systèmes d'Exploitation HARRIS
Nouvelle Génération d'OS

Temps-Réel

Real-Time / Power UNIX

- NH 6000

Power Hawk
Cartes Power PC604

Sécurité B2

Secure/Power UNIX (+ Power LAN)

- NH 6000

Power Hawk

Evaluation B2 au NCSC

Evaluation FB2/E3 UK
FB2/E3-E4 CELAR

Souche Commune : SYSTEM V R 4.2 (ES/MP)

. **Interface en compatibilité ascendante avec CX/UX CX/SX**

. **Principales Nouveautés :**

- **Installation et Paramétrage du Système**
- **Administration et Sécurité**
- **Internationalisation**
- **Drivers "Streams" - "Fonction Streams**
- **Modules changeables dynamiquement**
- **Threads (LWP)**

Les Applications sur CX/SX + LAN/SX

Evolution dans le temps

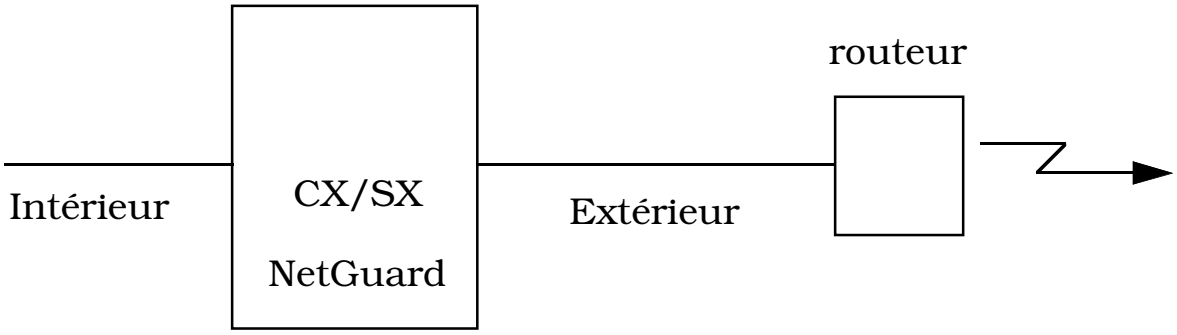
- Applications multiniveau
    - Bases de données
    - Centres d'Essais (Télémesure)
    - Simulateurs
- Serveurs sécurisés
- Frontaux de réseau
    - Passerelles sécurisées en tous genres
        . Contexte technique ou militaire
        . Contexte " tertiaire "
- Définition d'un noyau de "FIREWALL"
    Netguard 1.0 (sans Proxies)
    Netguard 2.0 (avec Proxies)

PRINCIPALES CARACTERISTIQUES DE NetGuard 2.0

.**Netguard** : option logicielle sur CX/SX Night Hawk

.**CyberGuard** : paquetage complet matériel + logiciel

"Firewall" d'architecture "dual home" pour réseau TCP/IP



.Filtre de paquets IP intelligent (au niveau noyau)

.Proxies pour Telnet, Ftp, Smtp, http, nntp ...
(au niveau demon)

.Système d'audit dérivé de CX/SX

.Système d'alarmes

.Traduction d'adresses IP

.Dual DNS

.Statistiques

.Option : Réseau Privé

. Support de systèmes d'authentification

Le Filtre de Paquets

Critères de Filtrage

Adresse (source, destination)
Protocole de base : UDP, TCP, ICMP
Port de service

Comportement intelligent :

- Regle dynamique pour le couple de ports
- Regle dynamique pour les sessions de commandes FTP

Contrôle sur les interfaces (IP spoofing)

Interface de paramétrage

- vi sur : mls/net/netguard.conf
- /mls/bin/netguard pour analyser et valider

- utilitaire interactif /mls/bin/cyberconf

  Cet utilitaire agit sur :
  Les règles de filtrage
  Le fichier /etc/host
  Le fonctionnement des alarmes

- Le filtre s'arrête sur la première règle applicable au paquet condidéré.

Si mot clé proxy ► le paquet est remonté à l'interface proxy.

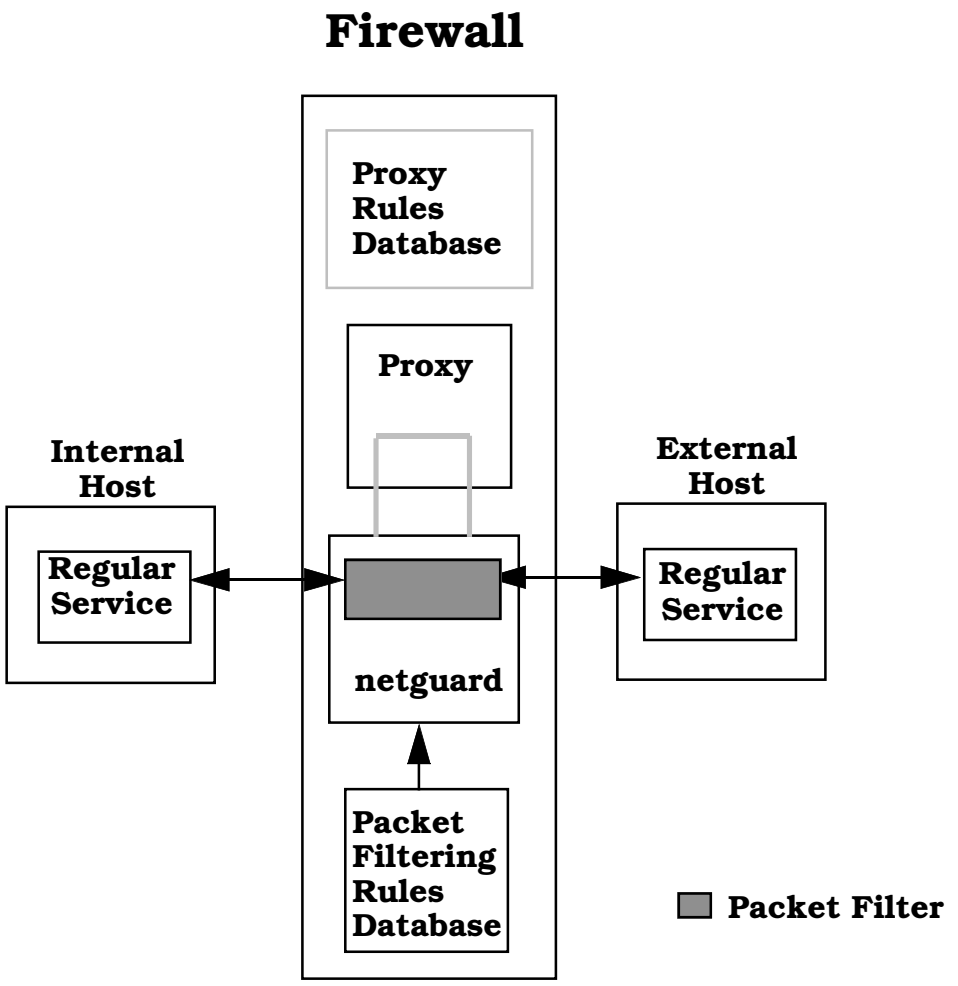
LES PROXIES

.Principe :

Le filtre de paquets détecte que le paquet relève du traitement PROXY.

Le paquet est remonté à l'interface proxy

Le demon inetd (spécial) reveille le lion démon proxy.

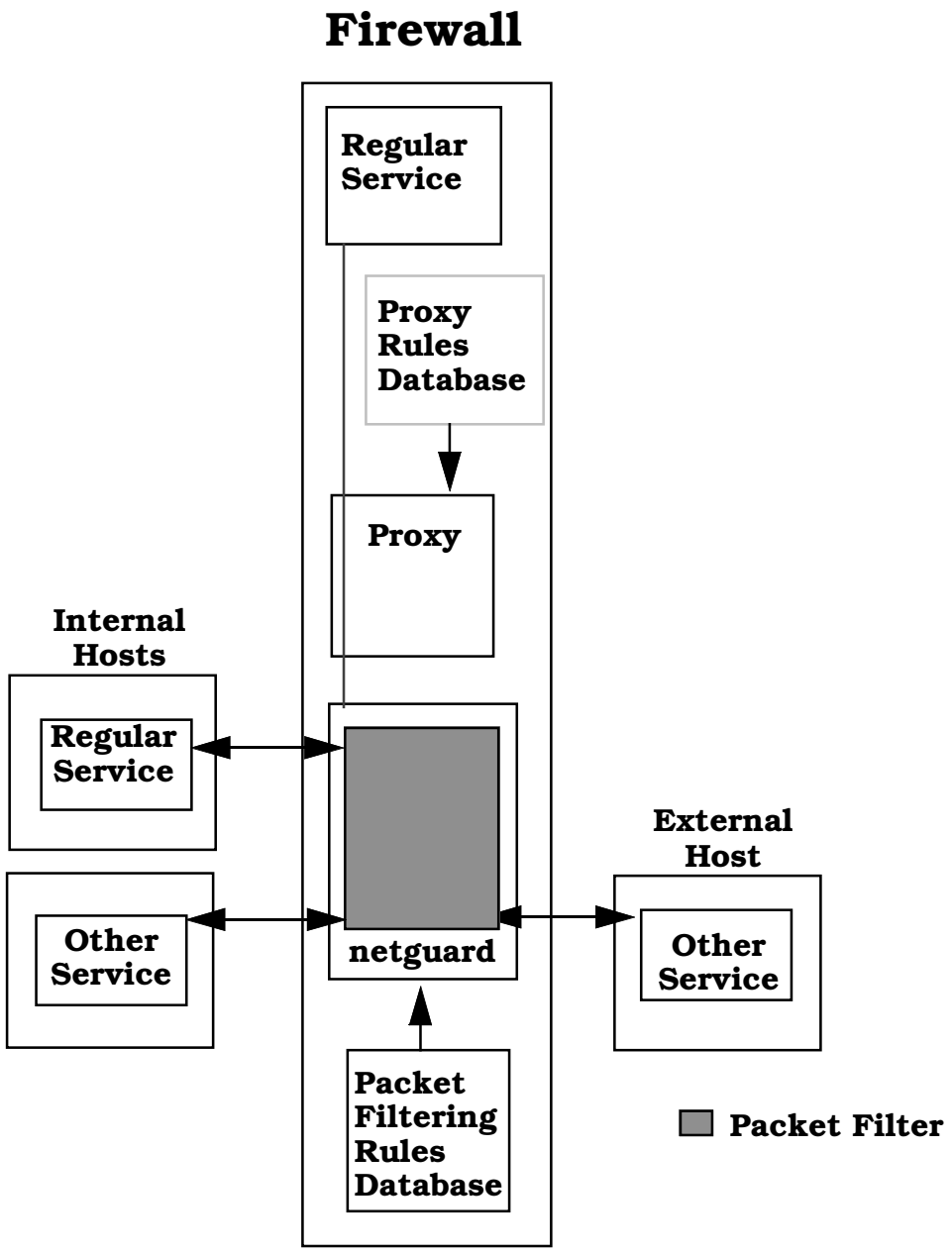


LES PROXIES suite

.Le traitement peut-être mixte.

- Proxy pour tel service dans telle direction

- Filtrage simple pour d'autres services ou le même dans l'autre l'autre direction.



PROXY TELNET

On peut invoquer :

soit directement la machine distante
soit le "firewall"

Dans les 2 cas l'authentification est faite par le proxy.

Si l'utilisateur est décrit dans la base de données
" token.conf ", l'entrée du password est remplacée par la réponse au "challenge ".

PROXY FTP

1 fichier de configuration permet de sélectionner les commandes FTP autorisées.

PROXY SMTP

Si smtp est traité en mode PROXY, le fichier /usr/lib/aliases est exploité dans le sens
Extérieur → Intérieur.

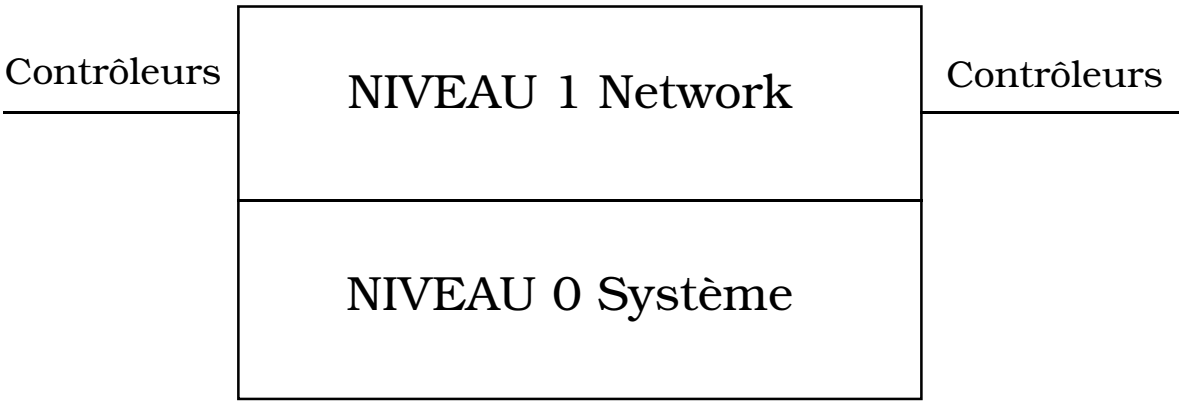
LES AVANTAGES DU MULTINIVEAU B1

Déjà un système C2 apporte plus de sécurité :

- audit sérieux
- gestion de la réutilisation des objets

Le B1 apporte le multiniveau, avantage considérable

(modèle Bell-la Padula)



Niveau 1 - Commandes réseau
- certains "proxies"

Niveau 0 - Tables du systèmes
- Filtre
- Démons de proxy

LES MESSAGES D'ALARME

L'utilitaire **cyberconf** permet de choisir le mode de traitement de l'alarme pour les thèmes suivants :

- HackFTP
- IFMACerror
- Logins
- NetguarD
- NetguardI
- NetguardM
- NetguardP
- NetguardS
- Passwd

NetguardT → Information volume
Portscan

En standard :

- Append dans 1 fichier
- mail à secadm
- message console
- pipe dans un "script" utilisateur
- OFF

HARRIS
COMPUTER SYSTEMS CORPORATION

La Module de Statistiques FW_STATS

Affichage périodique de statistiques

Issues des fichiers d'alarme
et de sorties netstat

DNS - SpLit Domain Name System

Principe :

Faire tourner 2 serveurs DNS

1 sur interface interne

1 sur interface externe

On lance 2 démons named

named -a IP_address -b bootfile

Dans bootfile on trouve le paramètre security_policy

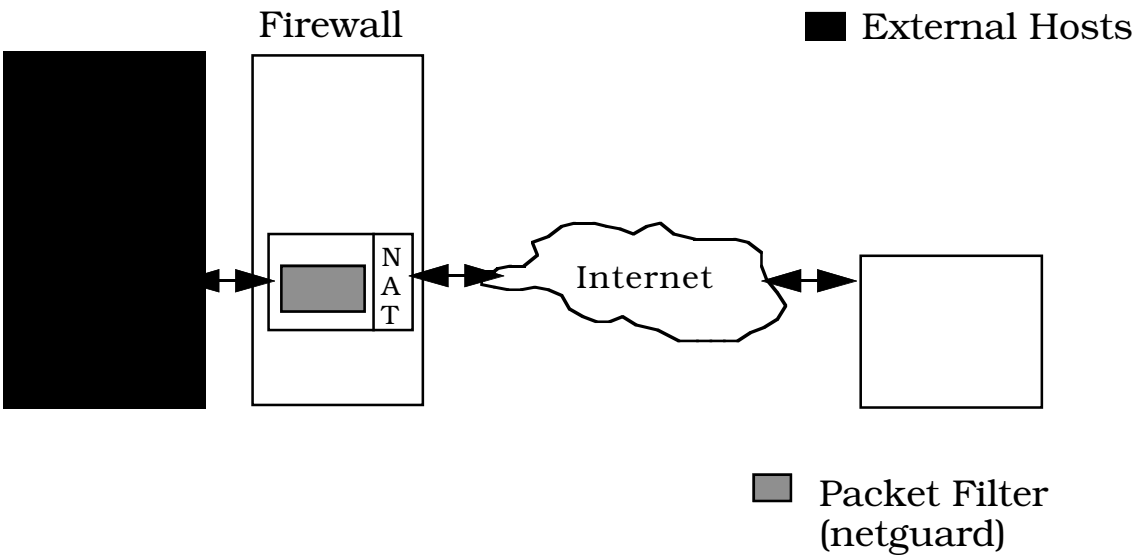
.Les règles de permissions nécessaires doivent être placées dans netguard.conf

1 dans chaque sens pour domain/udp
1 pour domain/tcp avec enable_reply

Le Manuel contient un guide détaillé inspiré de DNS and BIND Albitz and Lui

NAT Network Address Translation

Substitution de l'adresse IP du port externe à l'adresse source des machines internes



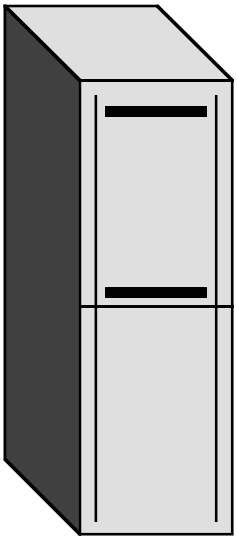
Configuration ifconfig ego addressxlate

Lancer nat -i dans /etc/rc

nat donne des statistiques

LES SOLUTIONS POSSIBLES SUR LA BASE CX/SX + NetGuard

PRODUIT CyberGuard



- **"package" matériel**
- **CPU NH 4800**
- **2 Ethernet**
- **1 disque 1 giga 1 DAT**
- **32 méga de mémoire**

=> CX/SX préconfiguré avec NetGuard

TOUTE LA GAMME NIGHT HAWK

- CX/SX + NetGuard
- Configuration extensible
- CPU, contrôleurs etc.....

LES OPTIONS

HAUTE PERFORMANCE

CPU NH 5000

CONFIGURATION REDONDANTE

Le CyberGuard est doublé

OPTION RESEAUX PRIVES

Chiffrement entre 2 CyberGuards

OPTION D'AUTHENTIFICATION

Calculette (challenge-response)

Cartes DES (génération de mots de passe à partir d'une clé)

Carte d'accès à clé négociée