Sécurité des systèmes d'information

les firewalls

© 2001 Nicolas Dubée, ndubee@secway.com

Plan

- Définition et notions générales
- L'offre Firewall actuelle
- Conception d'une architecture sécurisée par firewall
- Administration et maintenance

© 2001 Nicolas Dubée, ndubee@secway.com

Aperçu général

© 2001 Nicolas Dubée, ndubee@secway.com

Définition

- Historiquement:
  - Notion automobile, protection de l'habitacle contre l'incendie du moteur
- Informatique
  - Moyen pour appliquer des règles de sécurité entre deux entités
  - Par acceptation ou blocage de flux de données
  - Réseaux (filtres) ou applications (sandbox)

© 2001 Nicolas Dubée, ndubee@secway.com

Les firewalls étudiés ici seront les FW réseaux IP

© 2001 Nicolas Dubée, ndubee@secway.com

Présentation produit

- logiciel vendu séparément
  - À installer soi-même au dessus d'un OS classique (NT, Solaris, Linux, ...)
- « Pack » complet matériel + logiciel
  - Souvent, matériel+OS+logiciel modifié et amélioré par le constructeur

© 2001 Nicolas Dubée, ndubee@secway.com

Architecture externe

- Machine dédiée ou non
  - Dédié très recommandé
- Disposant d'au moins 2 interfaces réseau
- Branchées sur les réseaux à cloisonner

© 2001 Nicolas Dubée, ndubee@secway.com

Les technologies actuelles

© 2001 Nicolas Dubée, ndubee@secway.com

Architectures internes

- 2 grandes familles:
  - Filtres IP
  - Proxies applicatifs

  (+ hybrides des deux)
- Fonctionnalités annexes communes
  - Authentification utilisateurs
  - VPN
  - Surveillance et IDS

© 2001 Nicolas Dubée, ndubee@secway.com

Filtres IP

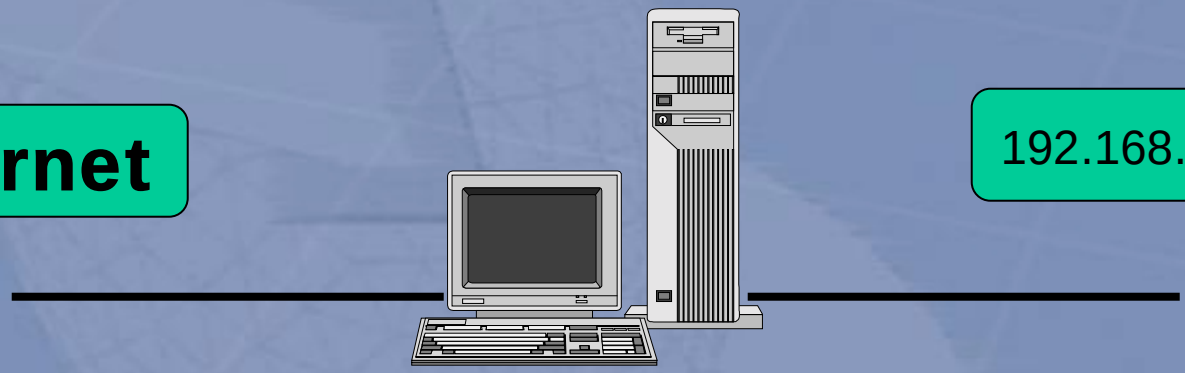
© 2001 Nicolas Dubée, ndubee@secway.com

Aperçu

- Pour chaque paquet, décision de:
  - Passage (ACCEPT, FORWARD)
  - Refus (REJECT, DENY)
  - Log
- En fonction de règles (rulebase) mettant en jeu les critères:
  - IP source
  - IP destination
  - Protocole et port

© 2001 Nicolas Dubée, ndubee@secway.com

Internet



192.168.1.0/24

```
IP src: 212.198.89.153
IP dst: 192.168.1.80
Proto: tcp
Port: 139
```

```
block in from any to 198.168.1.80 log
```


© 2001 Nicolas Dubée, ndubee@secway.com

La rulebase

- Traduction par langage dédié ou GUI des contraintes déterminées dans cahier des charges
- « Interdiction aux extérieurs de se connecter à l'intérieur, sauf serveur de mail port 25/tcp, accès complet intérieur vers extérieur, ... »

© 2001 Nicolas Dubée, ndubee@secway.com

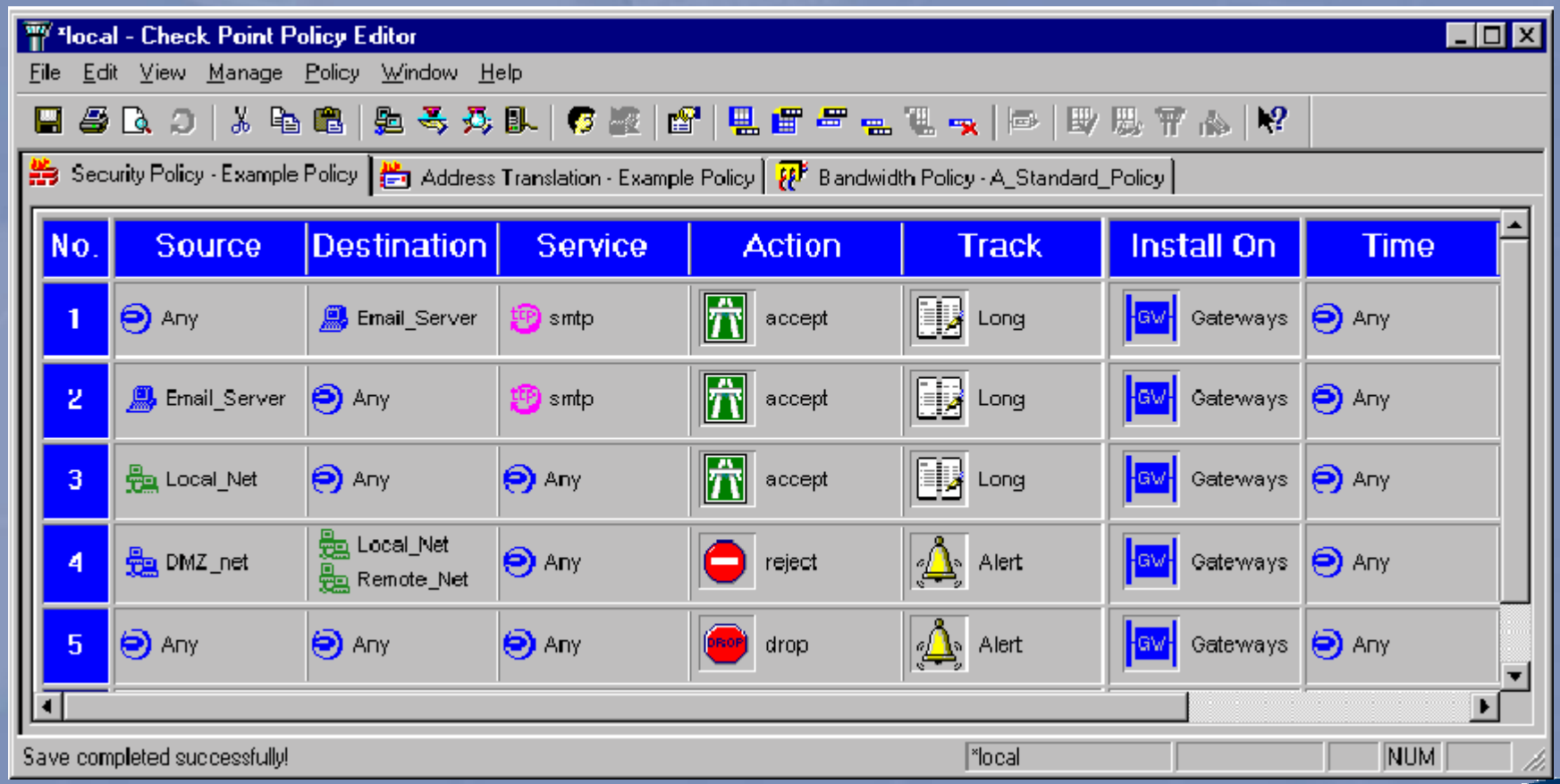
Exemple de rulebase

Ipf sous OpenBSD

```
block in from 192.168.1.0/24 to any on ne0
…
pass in proto tcp from any to 192.168.1.20 port 25
pass out proto tcp from 192.168.1.0/24 to any port 80
…
block in from any to 198.168.1.80 log
```

© 2001 Nicolas Dubée, ndubee@secway.com

Exemple d'outil d'édition de rulebase



Tiré de documentation Checkpoint FW-1

© 2001 Nicolas Dubée, ndubee@secway.com

Techniques et fonctionnalités avancées

- Masquerade ou NAT
  - traduction d'adresses IP (plages->plages, plages->single)
- Content inspection
  - analyse du contenu, couplé à un IDS
- Stateful inspection
  - suivi des connexions par table interne
- Contrôle de flux (shapping)

© 2001 Nicolas Dubée, ndubee@secway.com

Avantages / Inconvénients

- Avantages:
  - Rapidité
  - Précision des règles
  - Peuvent être complètement transparents
  - Offre importante (dont gratuits)
- Inconvénients:
  - Sécurité au mieux totalement dépendante des règles
  - Travail de conception et d'administration important pour la pérennité du système

© 2001 Nicolas Dubée, ndubee@secway.com

Offres principales (1)

- Checkpoint FW1
  - Software uniquement: NT, Solaris, ...
    - (Nokia fournit des « appliances » à base de FW1)
  - Leader mondial du marché, environ 45% (2000)
- Cisco PIX
  - Hardware
  - Performances élevées
  - Difficile à prendre en main

© 2001 Nicolas Dubée, ndubee@secway.com

Offres principales (2)

- Firewalls libres
  - Ipchains (Linux), ipfilter (BSD, Linux)
- Netasq
  - Français
  - Hardware, basé sur un noyau BSD
- Watchguard Firebox
  - Hardware, noyau Linux

© 2001 Nicolas Dubée, ndubee@secway.com

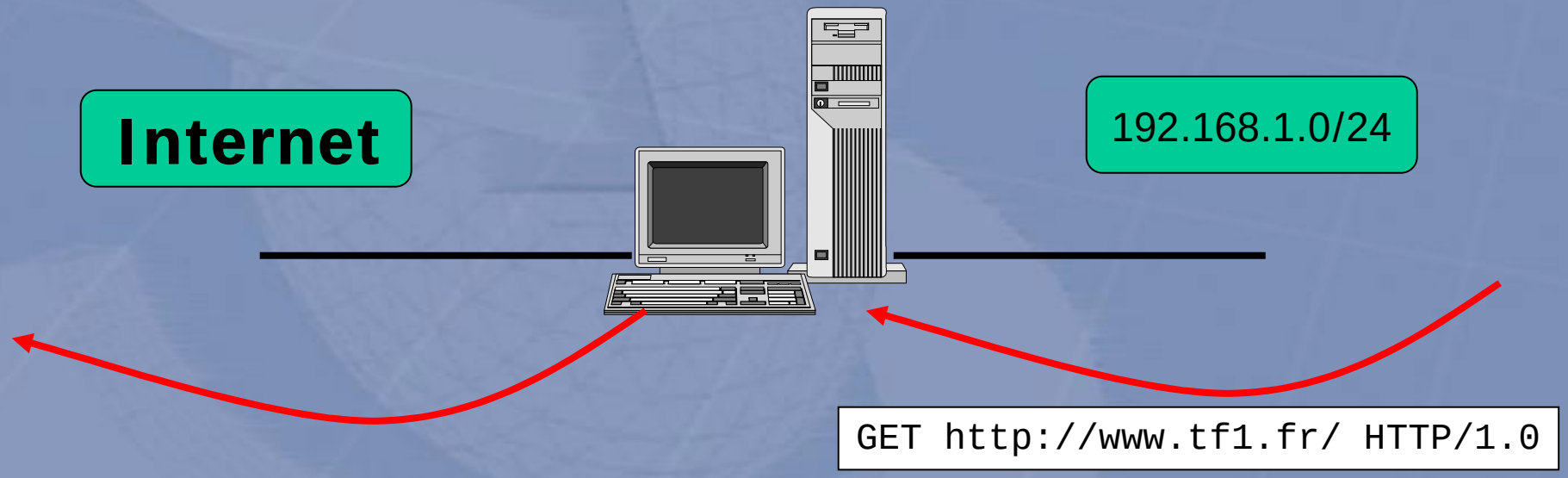
Proxies applicatifs

© 2001 Nicolas Dubée, ndubee@secway.com

Aperçu

- Passerelle niveau application entre les deux réseaux
- Pour chaque connexion d'une partie à l'autre:
  - Une connexion est établie de la source au proxy
  - Le proxy établit une connexion vers la cible
  - Le proxy fait transiter les informations entre les deux connexions

© 2001 Nicolas Dubée, ndubee@secway.com



© 2001 Nicolas Dubée, ndubee@secway.com

Techniques et fonctionnalités avancées

- Analyse de contenu haut niveau
- Méthodes d'authentification fortes (RSA SecurID, S/KEY, Alladin USB tokens)
- Proxies *transparents* génériques (TCP/UDP)
- Caches (DNS, HTTP)

© 2001 Nicolas Dubée, ndubee@secway.com

Avantages / Inconvénients

- Avantages
  - Sécurité élevée
  - Analyse de contenu (intégration avec IDS, blacklists Web, ...)
  - Orientés application
- Inconvénients
  - Lenteur
  - Difficulté à mettre en œuvre
  - Nécessite des logiciels clients

© 2001 Nicolas Dubée, ndubee@secway.com

Les offres principales (1)

- Network Associates Gauntlet 5.0
  - Software
  - Codebase originale issue de FWTK, réécriture importante
  - Utilisé par la plupart des administrations US
- MatraNet M/WALL
  - Dérivé de Gauntlet
  - Software, Français
- FWTK

© 2001 Nicolas Dubée, ndubee@secway.com

Les offres principales (2)

- SOCKS 4 et 5
  - Protocole de proxy, largement utilisé
  - Implémentation de référence disponible chez NEC
- Secure Computing SideWinder
  - Présent dans beaucoup d'administrations US

© 2001 Nicolas Dubée, ndubee@secway.com

Déploiement de firewalls

© 2001 Nicolas Dubée, ndubee@secway.com

Conception d'architectures

- Le FW est le moyen d'application de la politique de sécurité à l'accès Internet
- La conception et l'implémentation de l'architecture sont critiques
- Des architectures typiques sont disponibles

© 2001 Nicolas Dubée, ndubee@secway.com

Etapes de déploiement d'un FW

- Spécifications techniques
- Choix d'un produit, d'une architecture
- Installation, formation des administrateurs
- Test intrusif pré-prod
- Production

© 2001 Nicolas Dubée, ndubee@secway.com

Spécifications techniques

- En s'appuyant sur la politique de sécurité:
  - Définir les fonctionnalités nécessaires du FW lui-même (Authentification des utilisateurs, VPN, ...)
  - Définir les services qui seront visibles de l'extérieur
  - Et les règles d'accès à l'Internet des utilisateurs internes
  - En déduire les règles du firewall (rédigées)

© 2001 Nicolas Dubée, ndubee@secway.com

Choix d'un produit, d'une architecture

- Ce choix peut conditionner ou être conditionné par les spécifications techniques
- Architectures de bases disponibles, les utiliser de préférence !
- Facteur Prix important (FW = très cher)

© 2001 Nicolas Dubée, ndubee@secway.com

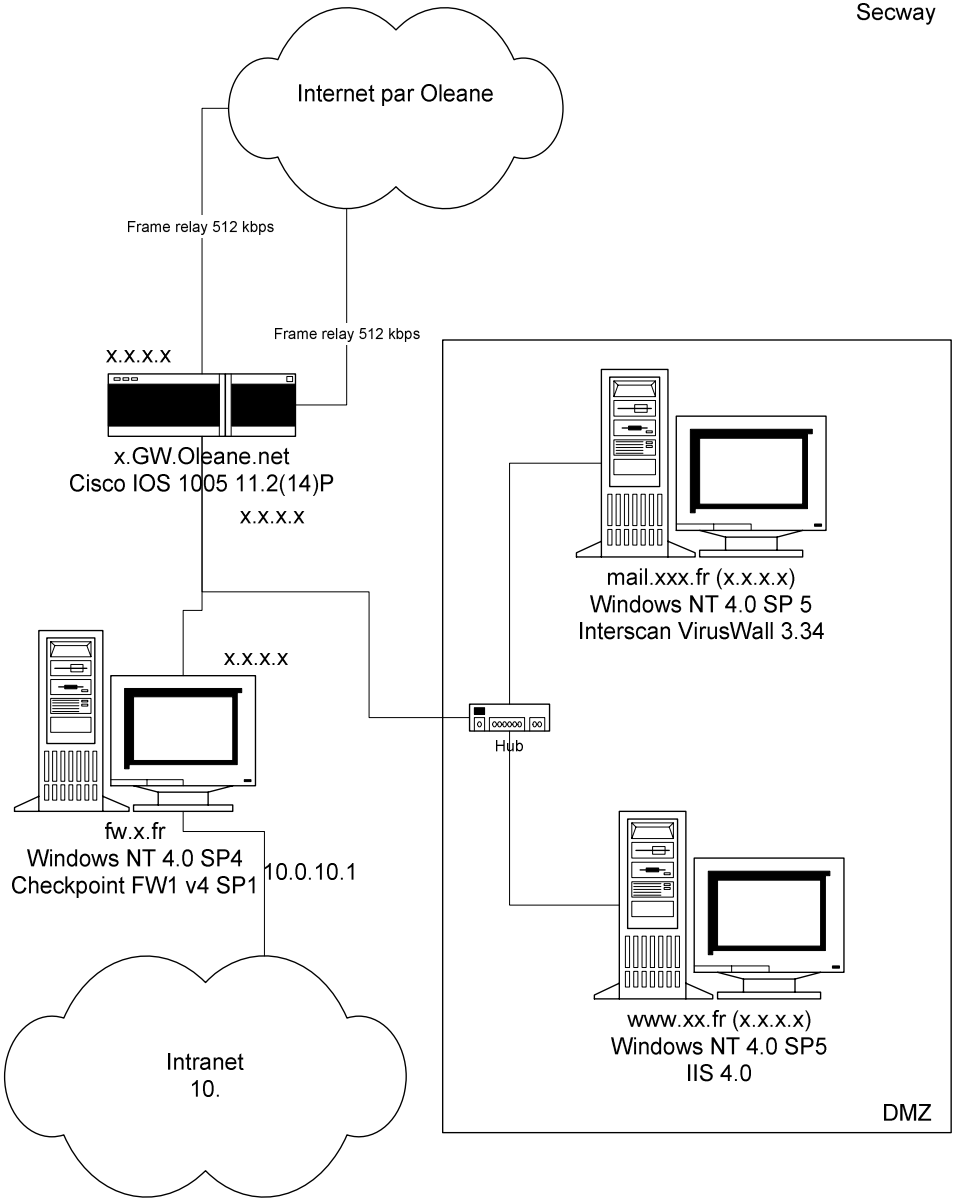
Architectures de bases

- Concept de DMZ
  - DeMilitarized Zone
  - Réseau situé côté Internet du FW, contenant tous les services (=serveurs) visibles de l'extérieur, et complètement séparé de l'intranet
    - WWW / FTP
    - Mail
    - DNS
  - Surveillance de cette zone importante

© 2001 Nicolas Dubée, ndubee@secway.com

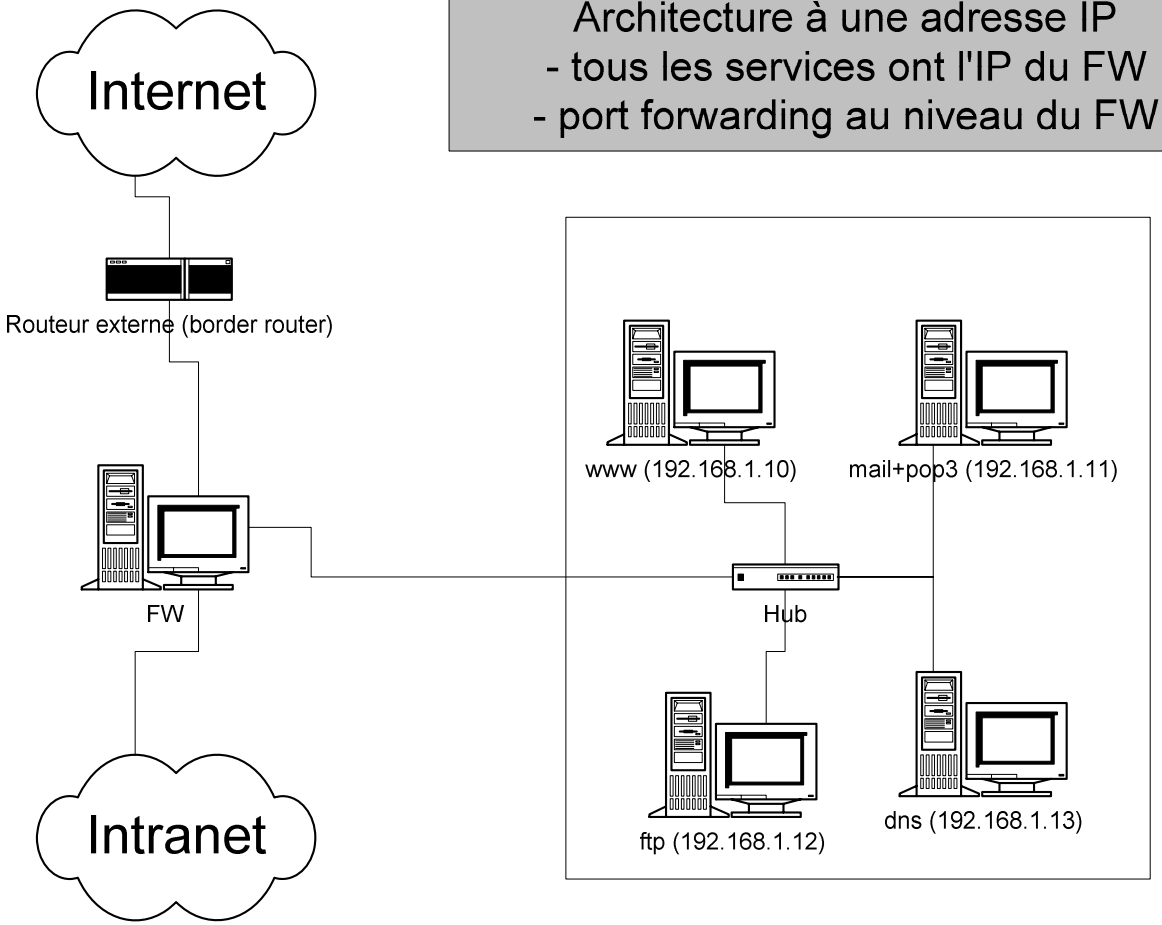
Topologie du réseau FR-XXXX (vue externe au xx/xx/2001)

N. Dubée
Secway

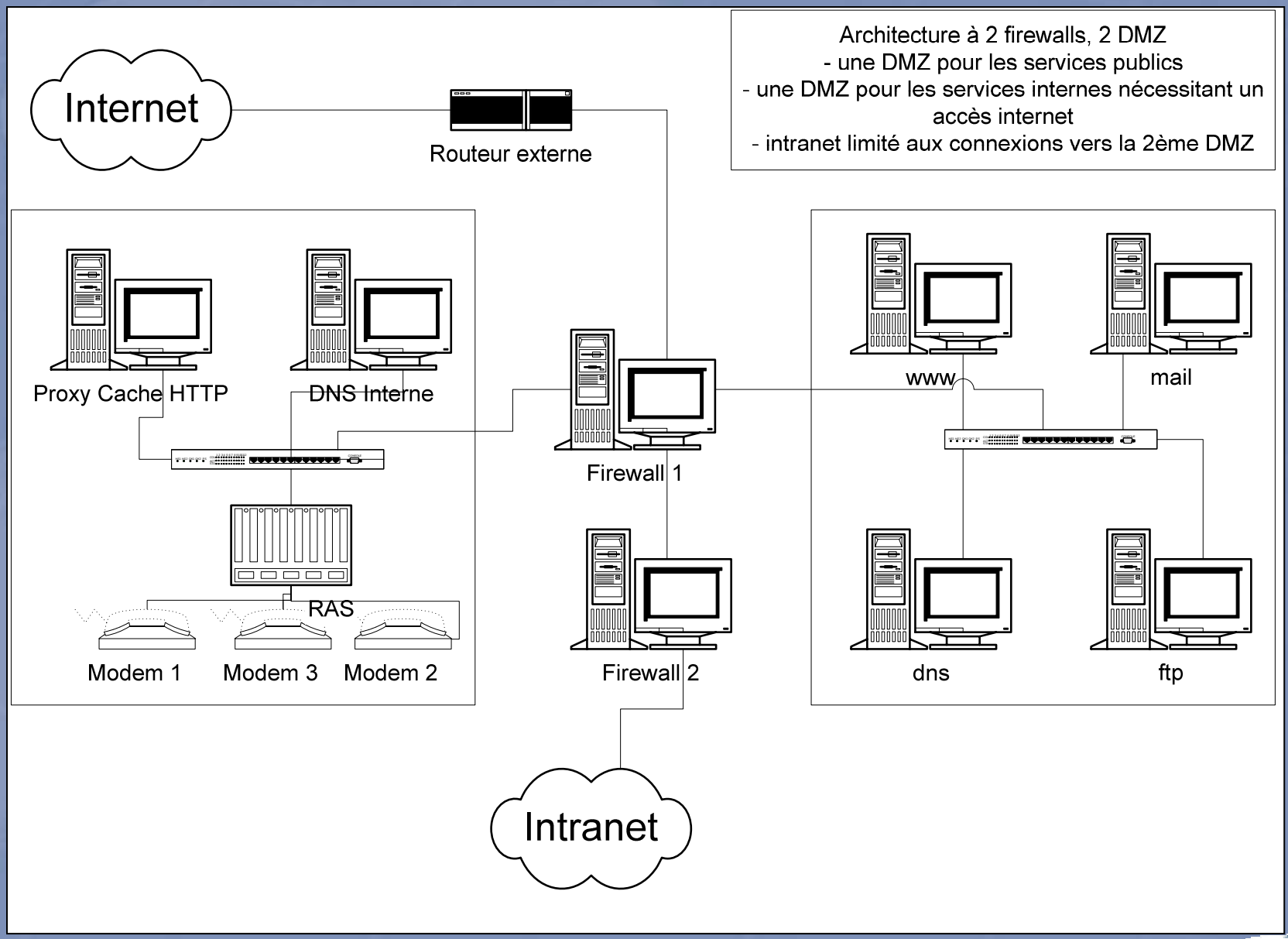


© 2001 Nicolas Dubée, ndubee@secway.com

Architecture à une adresse IP
- tous les services ont l'IP du FW
- port forwarding au niveau du FW



© 2001 Nicolas Dubée, ndubee@secway.com



© 2001 Nicolas Dubée, ndubee@secway.com

Règles pour la conception d'architectures

- Seules les connexions sortantes sont autorisées
- Aucun service public ne doit être dans l'intranet
- La DMZ doit être vue comme extérieure, aucune relation de confiance ne doit être établie avec la DMZ
- Interdire par défaut, autoriser au cas par cas

© 2001 Nicolas Dubée, ndubee@secway.com

Règles (2)

- Ne pas autoriser l'accès intranet à certaines IP externes, même « amies »
  - C'est le rôle des VPN
  - Il est très facile de changer son adresse IP
- Seules quelques stations auront l'accès au firewall (stations d'administration)
  - Ces machines doivent être sûres !!!

© 2001 Nicolas Dubée, ndubee@secway.com

Règles (3)

- Le FW peut être redondé
- Cas des débits importants
  - Voir spécifications techniques des FW dans le choix
  - Au besoin, utiliser des équilibreurs de charge

© 2001 Nicolas Dubée, ndubee@secway.com

Ajouts utiles

- Sur le FW et la DMZ
  - IDS
  - Tripwire
  - Outils de backup
- Sur le FW
  - Serveur de log sécurisé, imprimante

© 2001 Nicolas Dubée, ndubee@secway.com

Administration et maintenance

- Du firewall
- Des équipements réseaux (border routeur)
- Des machines de la DMZ

© 2001 Nicolas Dubée, ndubee@secway.com

Admin: le firewall (1)

- Le firewall, un système figé
- Ne pas oublier les patchs cependant (!)
  - Niveau OS host
  - Niveau Firewall lui-même
  - Rôles et procédures pour les patchs définis dans la politique de sécurité
- Les conditions de modification des règles doivent être bien définies et délimitées !

© 2001 Nicolas Dubée, ndubee@secway.com

Admin: le firewall (2)

- Analyse des logs
  - Très important, permet de détecter d'éventuelles failles/intrusions, ou d'établir des statistiques
  - Peut être réalisé en temps réel par des IDS
  - Ou en différé par des outils d'analyse (Webtrends)
  - Ou « à la main » en utilisant les outils du FW
- Garder les logs au minimum 2 mois
  - les archiver régulièrement en lieu sûr (CD-ROM)
  - Serviront de preuve en cas d'intrusion

© 2001 Nicolas Dubée, ndubee@secway.com

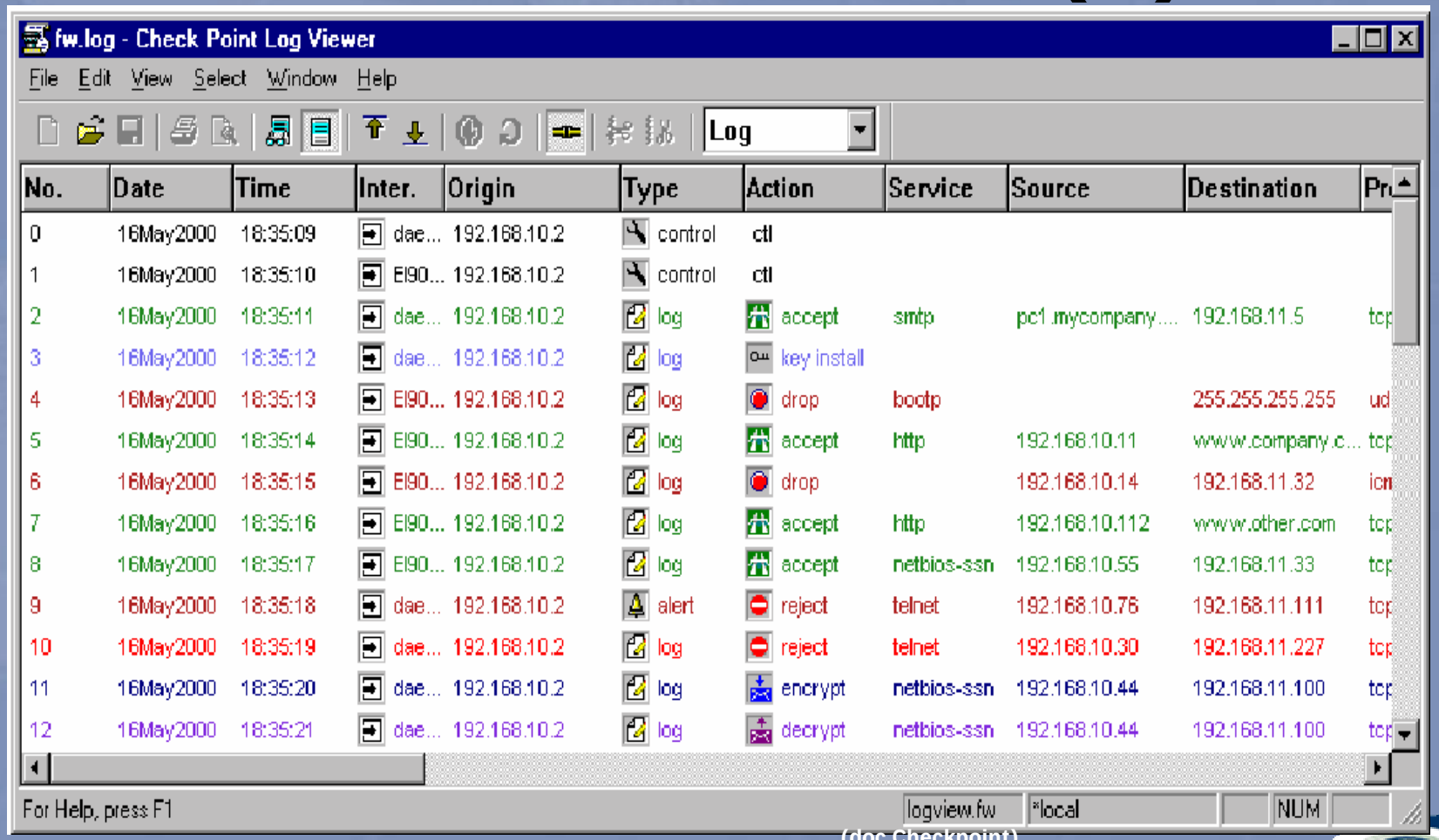
Admin: le firewall (3)

- Exemple de logs (Linux)

```
Oct 12 18:45:15 leeloo kernel: Packet log: inp DENY eth0 PROTO=1
  202.181.1.53:11 212.198.98.10:0 L=56 S=0xC0 I=48891 F=0x0000 T=237 (#25)
Oct 12 18:45:29 leeloo kernel: Packet log: inp DENY eth0 PROTO=1
  202.181.1.53:11 212.198.98.11:0 L=56 S=0xC0 I=48929 F=0x0000 T=237 (#25)
Oct 12 18:45:33 leeloo kernel: Packet log: inp DENY eth0 PROTO=1
  202.181.1.53:11 212.198.98.12:0 L=56 S=0xC0 I=48933 F=0x0000 T=237 (#25)
Oct 12 18:45:41 leeloo kernel: Packet log: inp DENY eth0 PROTO=1
  202.181.1.53:11 212.198.98.13:0 L=56 S=0xC0 I=48950 F=0x0000 T=237 (#25)
…
```

© 2001 Nicolas Dubée, ndubee@secway.com

Admin: le firewall (4)



No.	Date	Time	Inter.	Origin	Type	Action	Service	Source	Destination	Pr
0	16May2000	18:35:09	dae...	192.168.10.2	control	ctl				
1	16May2000	18:35:10	El90...	192.168.10.2	control	ctl				
2	16May2000	18:35:11	dae...	192.168.10.2	log	accept	smtp	pc1.mycompany....	192.168.11.5	tcp
3	16May2000	18:35:12	dae...	192.168.10.2	log	key install				
4	16May2000	18:35:13	El90...	192.168.10.2	log	drop	bootp		255.255.255.255	ud
5	16May2000	18:35:14	El90...	192.168.10.2	log	accept	http	192.168.10.11	www.company.c...	tcp
6	16May2000	18:35:15	El90...	192.168.10.2	log	drop		192.168.10.14	192.168.11.32	ico
7	16May2000	18:35:16	El90...	192.168.10.2	log	accept	http	192.168.10.112	www.other.com	tcp
8	16May2000	18:35:17	El90...	192.168.10.2	log	accept	netbios-ssn	192.168.10.55	192.168.11.33	tcp
9	16May2000	18:35:18	dae...	192.168.10.2	alert	reject	telnet	192.168.10.76	192.168.11.111	tcp
10	16May2000	18:35:19	dae...	192.168.10.2	log	reject	telnet	192.168.10.30	192.168.11.227	tcp
11	16May2000	18:35:20	dae...	192.168.10.2	log	encrypt	netbios-ssn	192.168.10.44	192.168.11.100	tcp
12	16May2000	18:35:21	dae...	192.168.10.2	log	decrypt	netbios-ssn	192.168.10.44	192.168.11.100	tcp

(doc Checkpoint)

© 2001 Nicolas Dubée, ndubee@secway.com

Admin: la DMZ

- Appliquer les patchs OS et services
- Examiner les logs des services
  - Logs des serveurs Web: /scripts/..%1c%c1../winnt/ etc..
  - Mails bouncés
- Les conserver au minimum 2 mois
  - Idem FW, peuvent prouver une intrusion
  - Qui ne serait pas dans les logs du FW

© 2001 Nicolas Dubée, ndubee@secway.com