EdelWeb

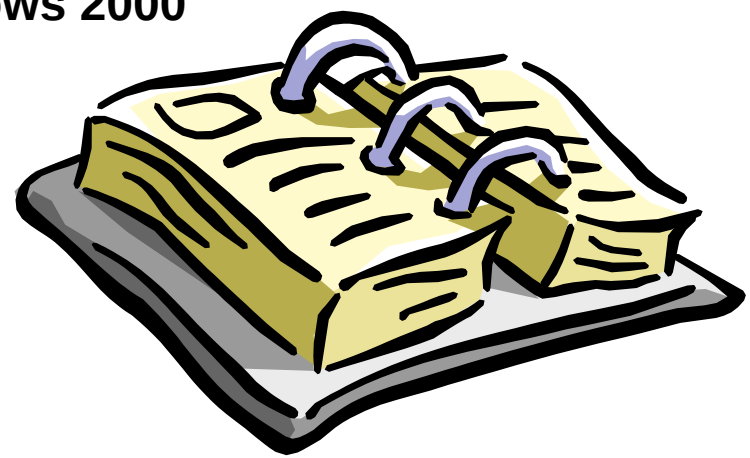
Les mécanismes de sécurité de Microsoft ISA Server

Patrick CHAMBET patrick.chambet@edelweb.fr
EdelWeb http://www.edelweb.fr

Planning

EdelWeb

- Objectifs
- Généralités
  - Principes de filtrage IP de Windows 2000
  - Familles de fonctionnalités
- Fonctions de sécurité
  - Renforcement du système
  - Fonctions de pare-feu
  - Relais SMTP
  - Réseaux privés virtuels
  - Détection d'intrusions
  - Alertes
  - Logs et reporting
- Vulnérabilités et recommandations
- Utilisations
- Conclusion



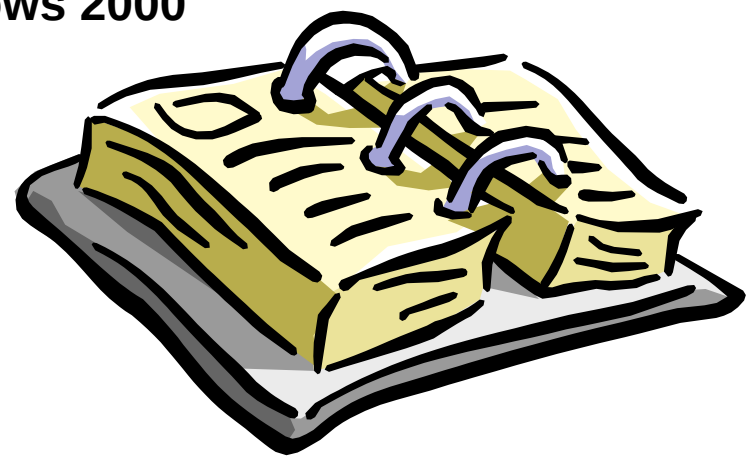
Objectifs

- Présenter les principales caractéristiques des mécanismes de sécurité d'ISA Server
- Proposer des recommandations pour améliorer la sécurité d'ISA Server
- Présenter des retours d'expérience concernant ISA Server
- Envisager des cas d'utilisations pratiques
- Conclure sur le niveau de sécurité d'ISA Server

Planning

EdelWeb

- Objectifs
- Généralités
  - Principes de filtrage IP de Windows 2000
  - Familles de fonctionnalités
- Fonctions de sécurité
  - Renforcement du système
  - Fonctions de pare-feu
  - Relais SMTP
  - Réseaux privés virtuels
  - Détection d'intrusions
  - Alertes
  - Logs et reporting
- Vulnérabilités et recommandations
- Utilisations
- Conclusion



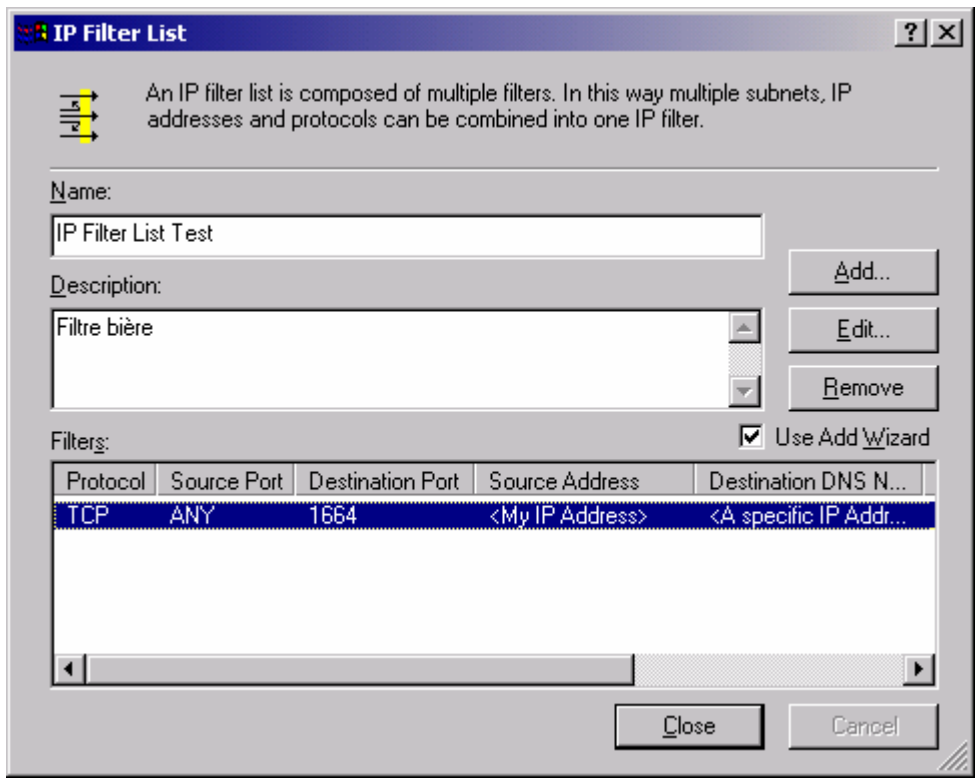
Généralités

- ISA = Internet Security and Acceleration Server
- Intégration avec Windows 2000 et Active Directory
- Basé sur le filtrage IP de la pile IP de Windows 2000
- Nécessite au moins le SP1 de Windows 2000
- Ne nécessite pas IIS 5.0
- Ensemble de services NT:
  - Microsoft Firewall Service
  - Microsoft H.323 Gatekeeper
  - Microsoft ISA Server Control Service
  - Microsoft Scheduled cache content download service
  - Microsoft Web Proxy Service

Principes de filtrage IP de Windows 2000

EdelWeb

- Le filtrage IP est supporté en standard sous Windows 2000
  - Stratégie de sécurité locale > stratégies IPSec
- Pour chaque interface, filtrage en fonction des paramètres:
  - Protocole
  - Direction
  - Adresse source
  - Port source
  - Adresse destination
  - Port destination
- ISA Server
  - Utilise des hooks
  - Offre des compléments au filtrage IP de Windows 2000



Familles de fonctionnalités

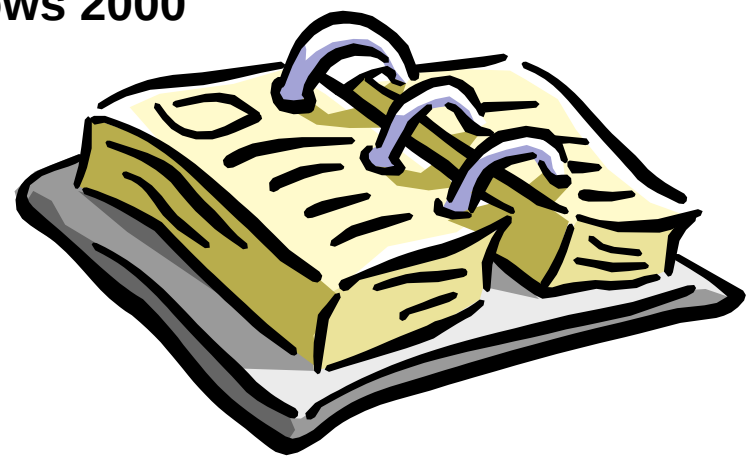
- **Sécurité réseau**
- **Publication (reverse proxy, RPC)**
- **Qualité de service (bande passante)**
- **Cache dynamique (le “A” de ISA)**
- **Gestion distribuée des accès Internet (arrays)**
- **Diffusion de flux (H.323)**

On ne s’intéressera ici qu’aux mécanismes de sécurité

Planning

EdelWeb

- Objectifs
- Généralités
  - Principes de filtrage IP de Windows 2000
  - Familles de fonctionnalités
- Fonctions de sécurité
  - Renforcement du système
  - Fonctions de pare-feu
  - Relais SMTP
  - Réseaux privés virtuels
  - Détection d'intrusions
  - Alertes
  - Logs et reporting
- Vulnérabilités et recommandations
- Utilisations
- Conclusion



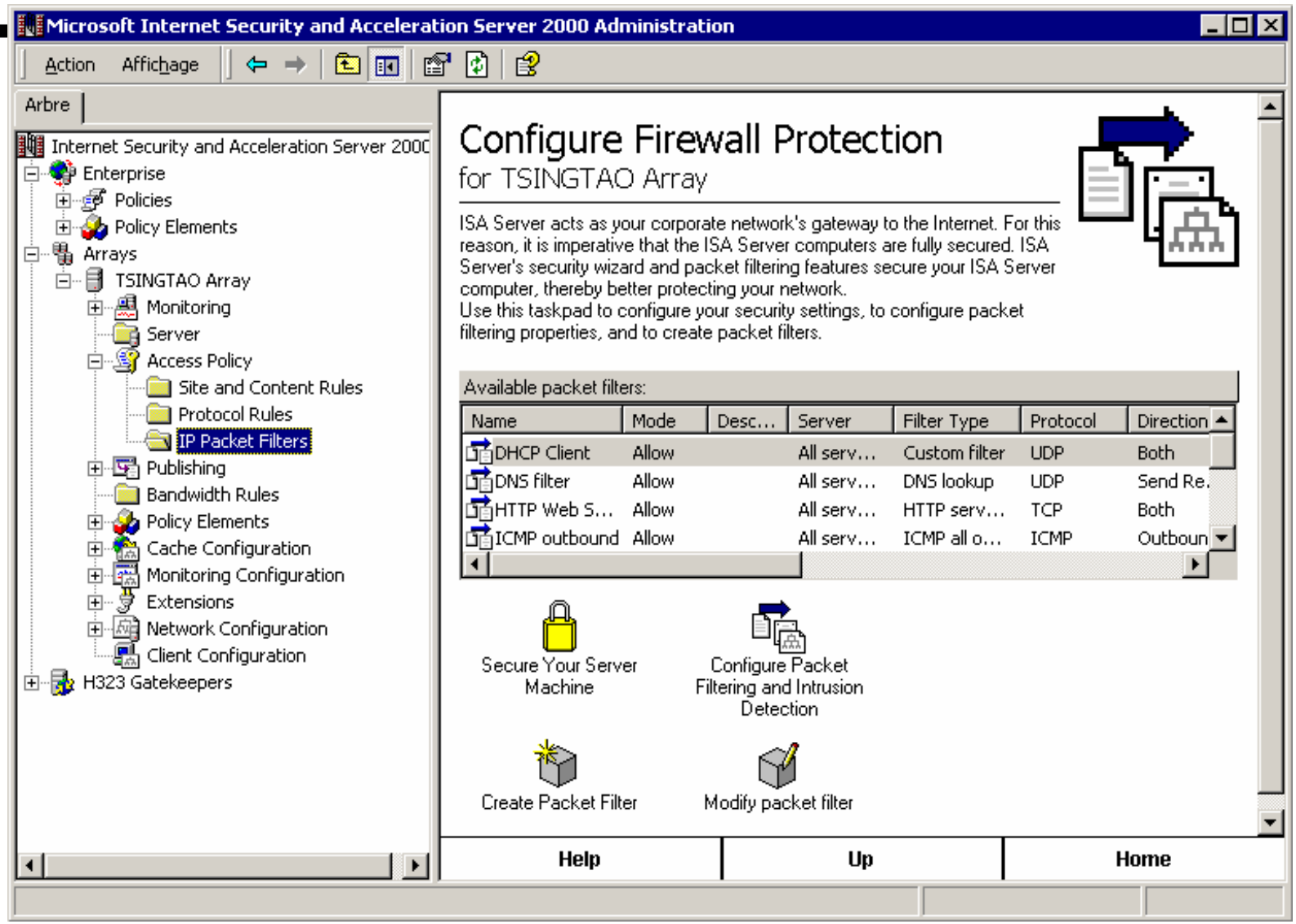
Fonctions de sécurité

EdelWeb

- Renforcement du système Windows 2000
- Pare-feu à plusieurs niveaux
  - Filtrage dynamique de paquets
  - Inspection
  - Filtres applicatifs pour un grand nombre de protocoles
  - Authentification
  - Régles détaillées pour le contrôle d'accès et le respect des stratégies
- Relais SMTP
- Réseaux privés virtuels
- Détection d'intrusions
- Alertes
- Logs et reporting

Console d'administration

EdelWeb



Renforcement du système

EdelWeb

- **3 niveaux de sécurisation proposés:**

- **Mais:**
  - **Peu d'informations sur ce qui est configuré**
  - **Long à appliquer**
  - **Pas documenté**

Fonctions de pare-feu

- **Stratégies basées sur:**
  - **Les éléments définis globalement pour tous les modules d'ISA Server:**
    - **Définitions de protocoles**
    - **Groupes d'adresses de destination**
    - **Groupes d'adresses clientes**
    - **Contenu des échanges (MIME, extensions de fichiers)**
    - **Horaires**
    - **Priorité de bande passante**
  - **Des stratégies de contrôle des flux:**
    - **Règles de protocoles (qui a le droit d'utiliser tel protocole et quand)**
    - **Règles de groupes d'adresses (qui a le droit de parler avec qui et quand)**
    - **Règles de filtrage de paquets (sur quelles interfaces les règles sont appliquées)**
  - **Les règles "Deny" l'emportent toujours**

Filtrage dynamique de paquets

EdelWeb

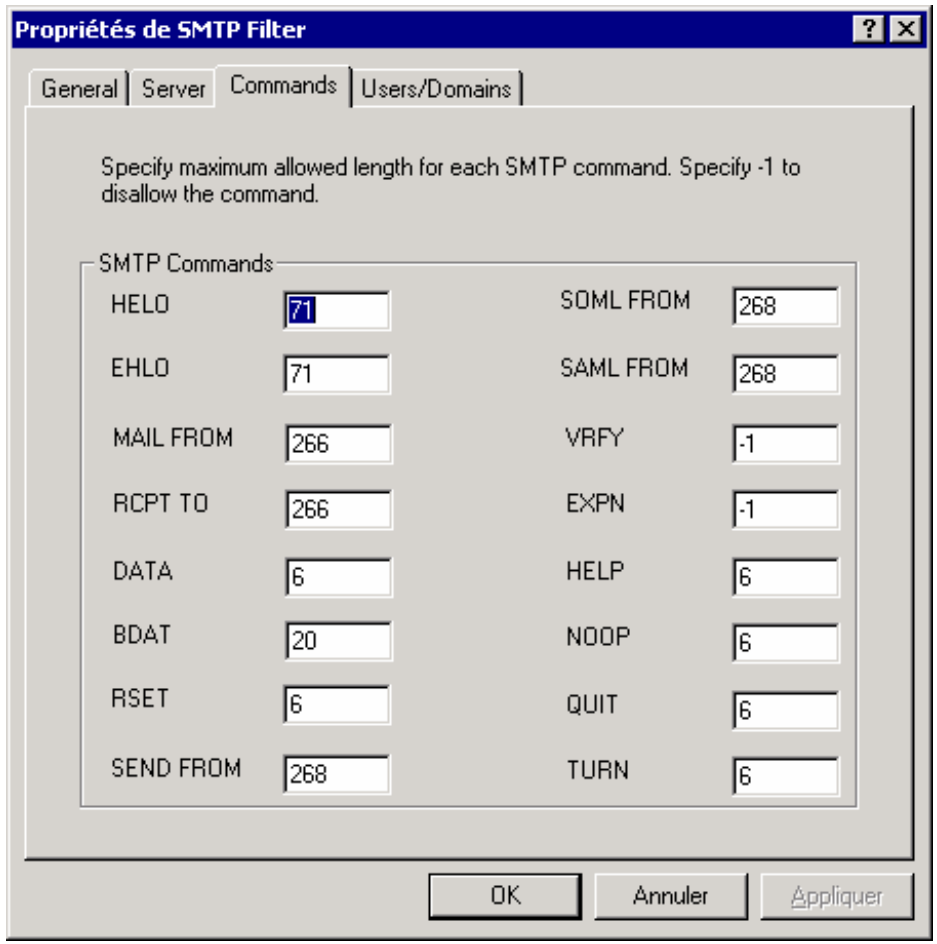
- **Globalement, les paramètres de filtrage sont donc:**
  - **Protocole**
  - **Direction**
  - **Mode (autoriser, bloquer)**
  - **Groupe d'adresses sources**
  - **Groupe d'adresses destination**
  - **Port source**
  - **Port destination**
  - **Groupe d'utilisateurs**
  - **Contenu**
  - **Horaires**
  - **Groupe de serveurs ISA**
  - **Interface du serveur ISA**

- **Possibilité de filtrer aussi:**
  - **Les paquets fragmentés**
  - **Les paquets avec options IP**

Relais SMTP

EdelWeb

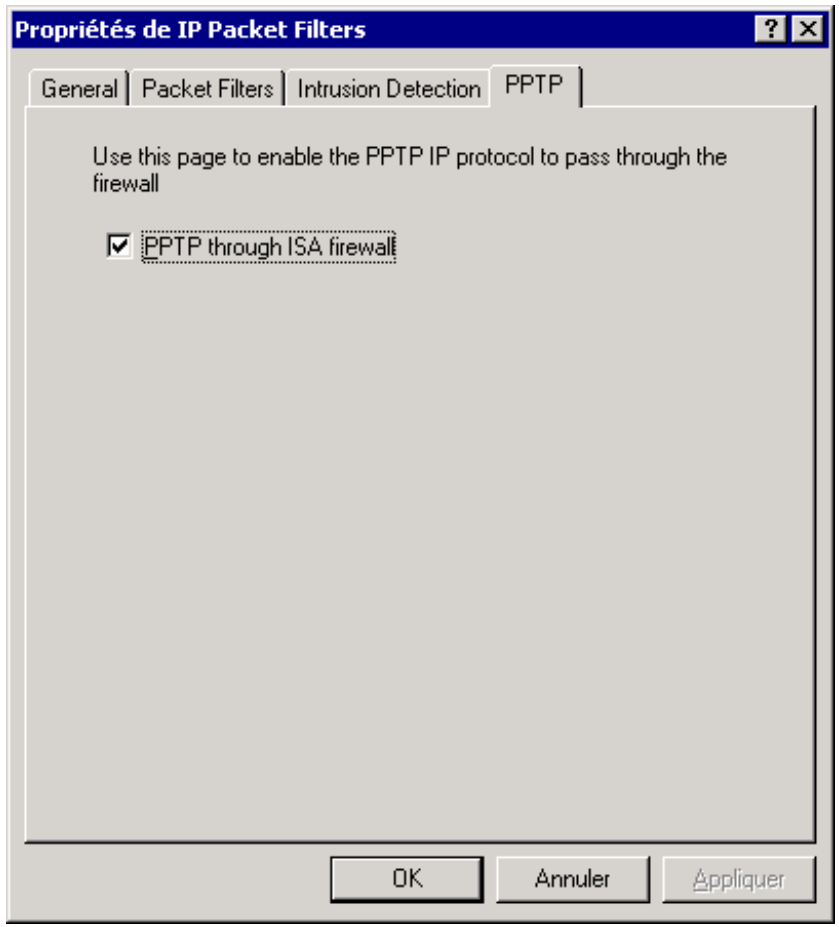
- **Permet de**
  - **Limiter la longueur des paramètres de chaque commande SMTP**
  - **Interdire certaines commandes**
  - **Rejeter certains utilisateurs**
  - **Rejeter des domaines**
  - **Filtrer en fonction de mots clés dans les headers ou le corps des messages**
  - **Filtrer en fonction des pièces attachées (type MIME, extensions de fichiers)**



Réseaux privés virtuels

EdelWeb

- Gère les VPN basés sur:
  - PPTP
  - L2TP sur IPSec
- Utilise le service RRAS



Détection d'intrusion

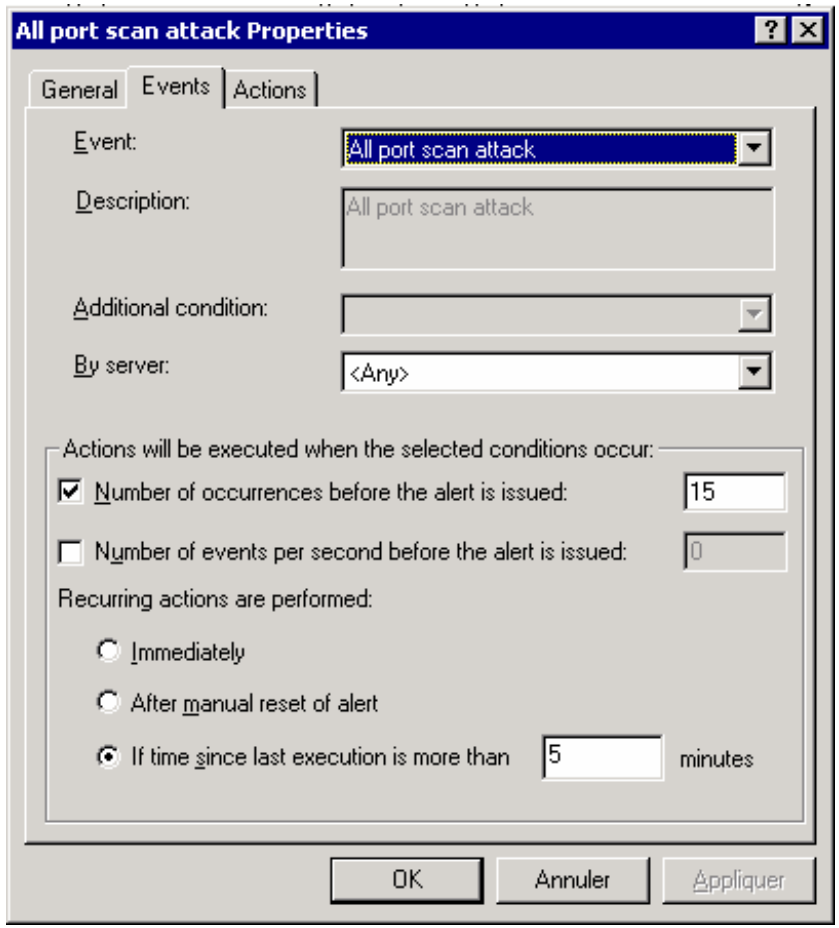
- Utilise les technologies d'ISS
- Détection d'attaques de type:
  - Windows Out of Band (WinNuke)
  - Land
  - Ping of Death
  - IP half scan
  - UDP bomb
  - Port scan
  - POP buffer overflows (extension)
  - DNS traffic (extension)
- Génération d'alertes
- Mais pas configurable finement

Alertes (1/2)

EdelWeb

- **Alertes prédéfinies:**
  - **Port scanning**
  - **Paquets droppés**
  - **Problème de logs**
  - **Attaques (Land, half scan, …)**
  - **Disque saturé**
  - **Etc…**

- **Possibilité de définir ses propres alertes**



Alertes (2/2)

- **Actions:**
  - **Envoyer un mail**
  - **Démarrer un programme**
  - **Enregistrer un événement dans un journal Windows 2000**
  - **Stopper un service d'ISA Server**
  - **Démarrer un service d'ISA Server**

- **Attention, toutes les alertes ne sont pas activées par défaut**

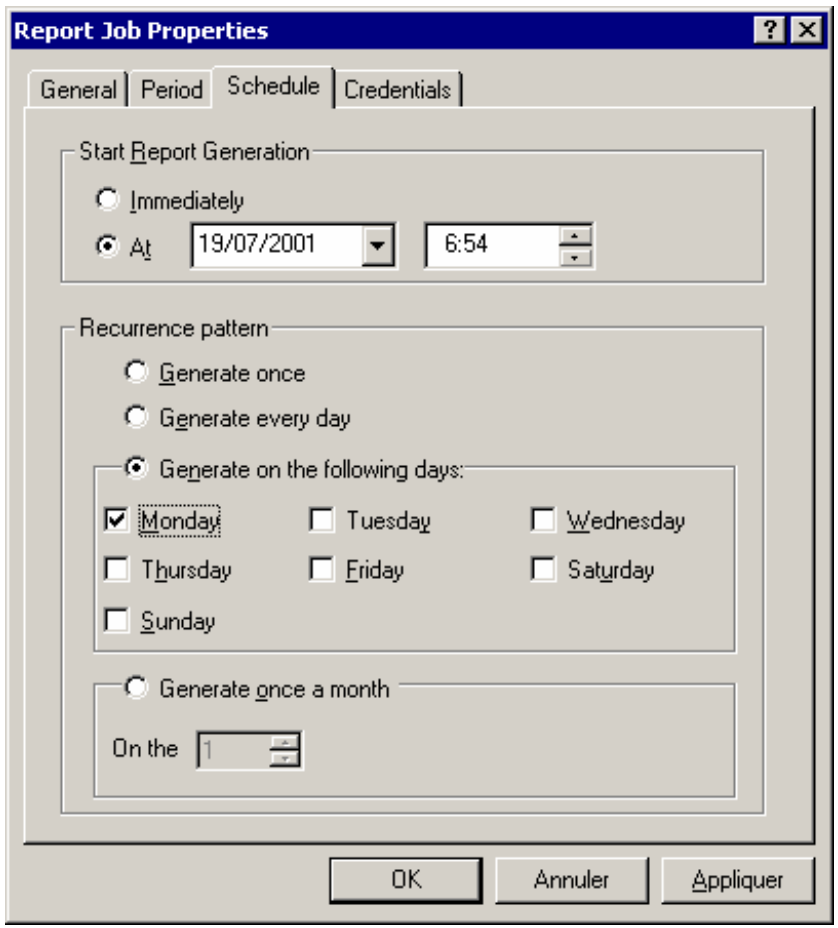
Logs et reporting (1/2)

- **Problèmes de configuration:**
  - Insecure configuration
  - Log information failure
  - Server Publishing failure
  - Undeliverable alert
- **Règles enfreintes:**
  - Rule Policy violation
  - Dropped packets
  - Protocol violation
  - RPC Filter - server is reachable
  - RPC Filter - server is unreachable
  - SMTP Filter Event
- **Attaques:**
  - Port scan attack, IP half scan attack, Land attack, Windows out-of-band attack, Ping of death attack, UDP bomb attack

Logs et reporting (2/2)

EdelWeb

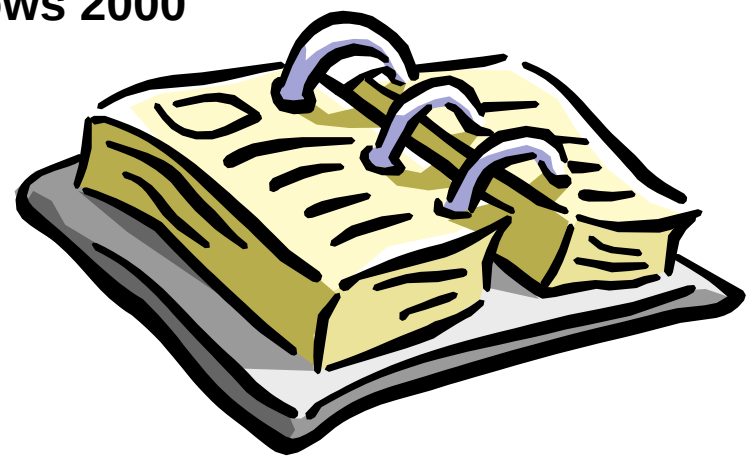
- 3 journaux d'événements:
  - Filtrage de paquets
  - Service firewall
  - Service Proxy Web
- Rapports
  - Programmés
  - Contenu paramétrable
  - Permissions d'accès pour la lecture



Planning

EdelWeb

- Objectifs
- Généralités
  - Principes de filtrage IP de Windows 2000
  - Familles de fonctionnalités
- Fonctions de sécurité
  - Renforcement du système
  - Fonctions de pare-feu
  - Relais SMTP
  - Réseaux privés virtuels
  - Détection d'intrusions
  - Alertes
  - Logs et reporting
- Vulnérabilités et recommandations
- Utilisations
- Conclusion



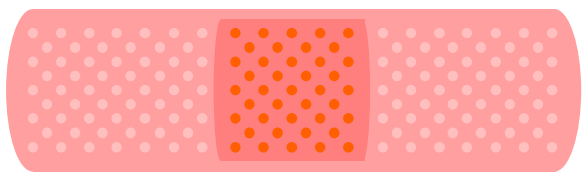
Vulnérabilités

EdelWeb

- Avis Microsoft MS01-021 du 16/04/01 (SecureXpert Labs Advisory [SX-20010320-2])
  - DoS du service Proxy

  http://www.microsoft.com /technet/security/bulletin/MS01-021.asp
  http://www.securexpert.com

- Avis Microsoft MS01-045 du16/08/01
  - H.323 Gatekeeper Memory Leak
  - DoS du service Proxy
  - Cross-site scripting



  http://www.microsoft.com/technet/security/bulletin/MS01-045.asp

- Programme de tests de vulnérabilités chez Edelweb

Recommandations (1/2)

1. Utiliser un serveur autonome
2. Installer ISA Server sur une partition séparée
3. N'installer que les modules nécessaires (pas de H.323 par ex.)
4. Utiliser le mode firewall ou le mode intégré
5. Sécuriser le serveur (fonction intégrée ISA + procédures habituelles + script NSA + à la main)
6. Contrôler les adresses définies dans la LAT
7. Supprimer le partage "mspclnt"
8. Ne pas activer le routage
9. Ne publier des serveurs que si ceux-ci sont dans une DMZ

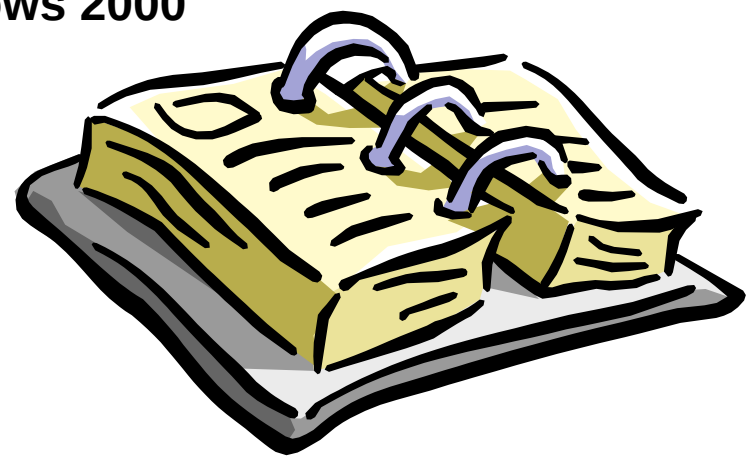
Recommandations (2/2)

1. Rester rigoureux dans la définition des stratégies
2. Respecter un ordre de création:
    1. Paramètres globaux
    2. Régles particulières
3. Activer le filtrage de paquets
4. Définir des règles de filtrage anti-spoofing
5. Activer la détection d'intrusion
6. Activer toutes les alertes et définir ses propres alertes
7. Activer les options de journalisation et loguer dans une base de données si possible
8. Attentions aux extensions (vérifier avec un scanner de ports)

Planning

EdelWeb

- Objectifs
- Généralités
  - Principes de filtrage IP de Windows 2000
  - Familles de fonctionnalités
- Fonctions de sécurité
  - Renforcement du système
  - Fonctions de pare-feu
  - Relais SMTP
  - Réseaux privés virtuels
  - Détection d'intrusions
  - Alertes
  - Logs et reporting
- Vulnérabilités et recommandations
- Utilisations
- Conclusion



Utilisations

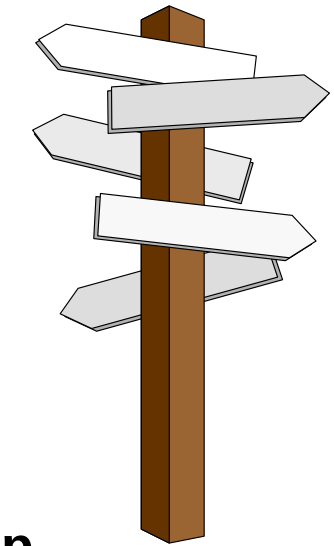
- **Grande entreprise**
  - **+ : S'interface avec Active Directory**
  - **- : Pas encore de tests à grande échelle**
- **PME**
  - **+ : Peut s'installer en mode firewall seulement ou cache seulement**
  - **- : Complexe à paramétrer**
- **Domicile**
  - **+ : Nécessite peu de ressources (Pentium, 64 Mo RAM)**
    Supporte les connexions modem
  - **- : Prix**

Conclusion

- **Bon contrôle des filtres grâce à un jeu de paramètres très complet**
- **Peu de vulnérabilités majeures découvertes à ce jour**
- **Mais encore peu de retours d'expérience de déploiement à grande échelle**

Bibliographie
Microsoft

EdelWeb



- **Microsoft :**
  - **ISA Server**
    http://www.microsoft.com/isaserver/
  - **Sécurité**
    http://www.microsoft.com/security/
  - **Knowledge Base**
    http://search.support.microsoft.com/kb/
  - **Security bulletins**
    http://www.microsoft.com/technet/security/current.asp
  - **Mises à jour**
    http://www.microsoft.com/windows2000/downloads/critical
    http://www.microsoft.com/windows2000/downloads/recommended

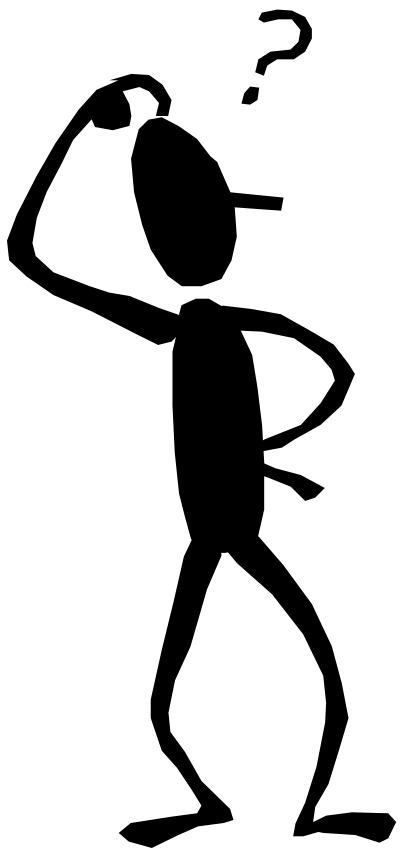
Bibliographie
Non-Microsoft

EdelWeb

- NSA
  - http://nsa2.www.conxion.com/
- Bugtraq, NTBugtraq, Security Focus
  - http://www.securityfocus.com/
- SANS (System Administration, Networking and Security)
  - http://www.sans.org/
- Windows 2000 Magazine Security News
  - http://www.ntsecurity.net/
- Security Portal
  - http://www.securityportal.com/

Questions

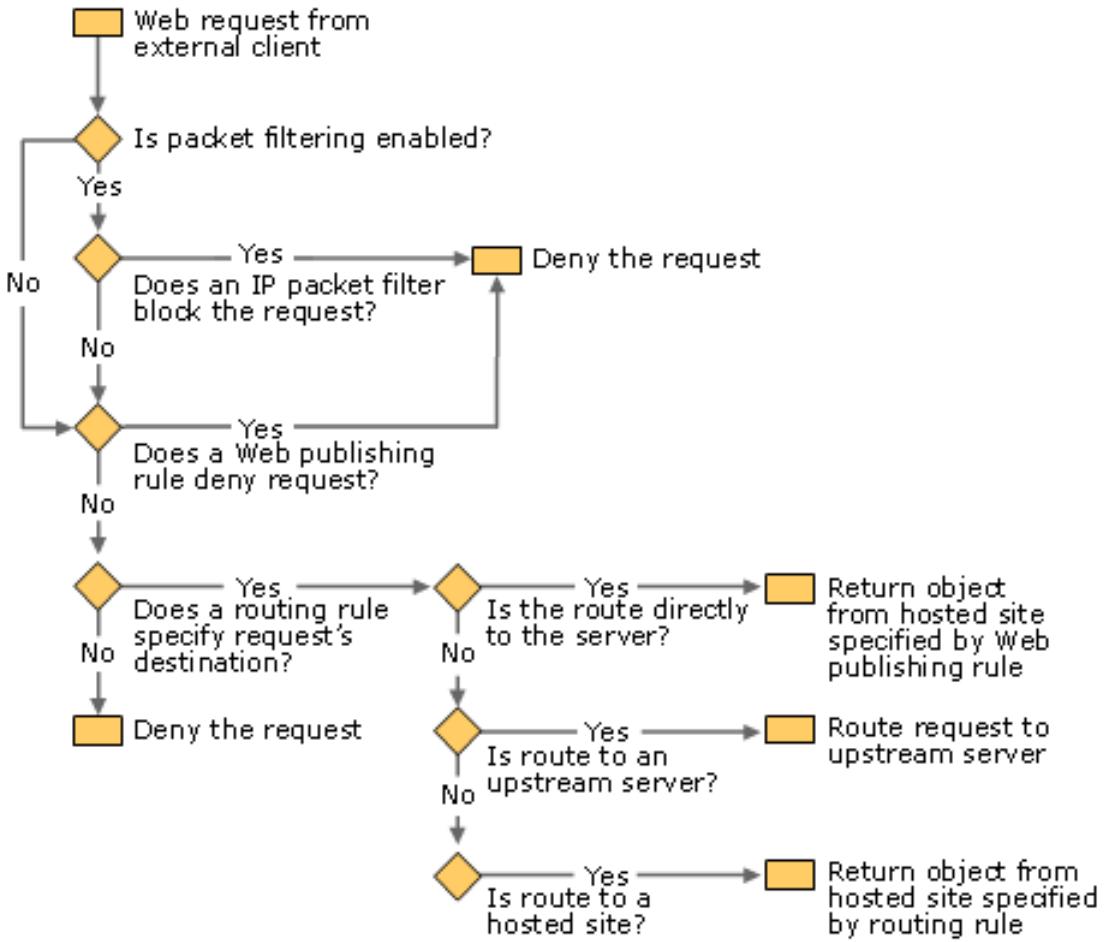
EdelWeb



Annexe: ordre d'application des règles (1/2)

EdelWeb

- **Paquet entrant:**



Annexe: ordre d'application des règles (2/2)

EdelWeb

- **Paquet sortant:**