Mise en œuvre de la sécurité de votre périmètre et de votre réseau

Benoît HAMET
Ingénieur d'étude / Formateur
MVP
Concept Réseau

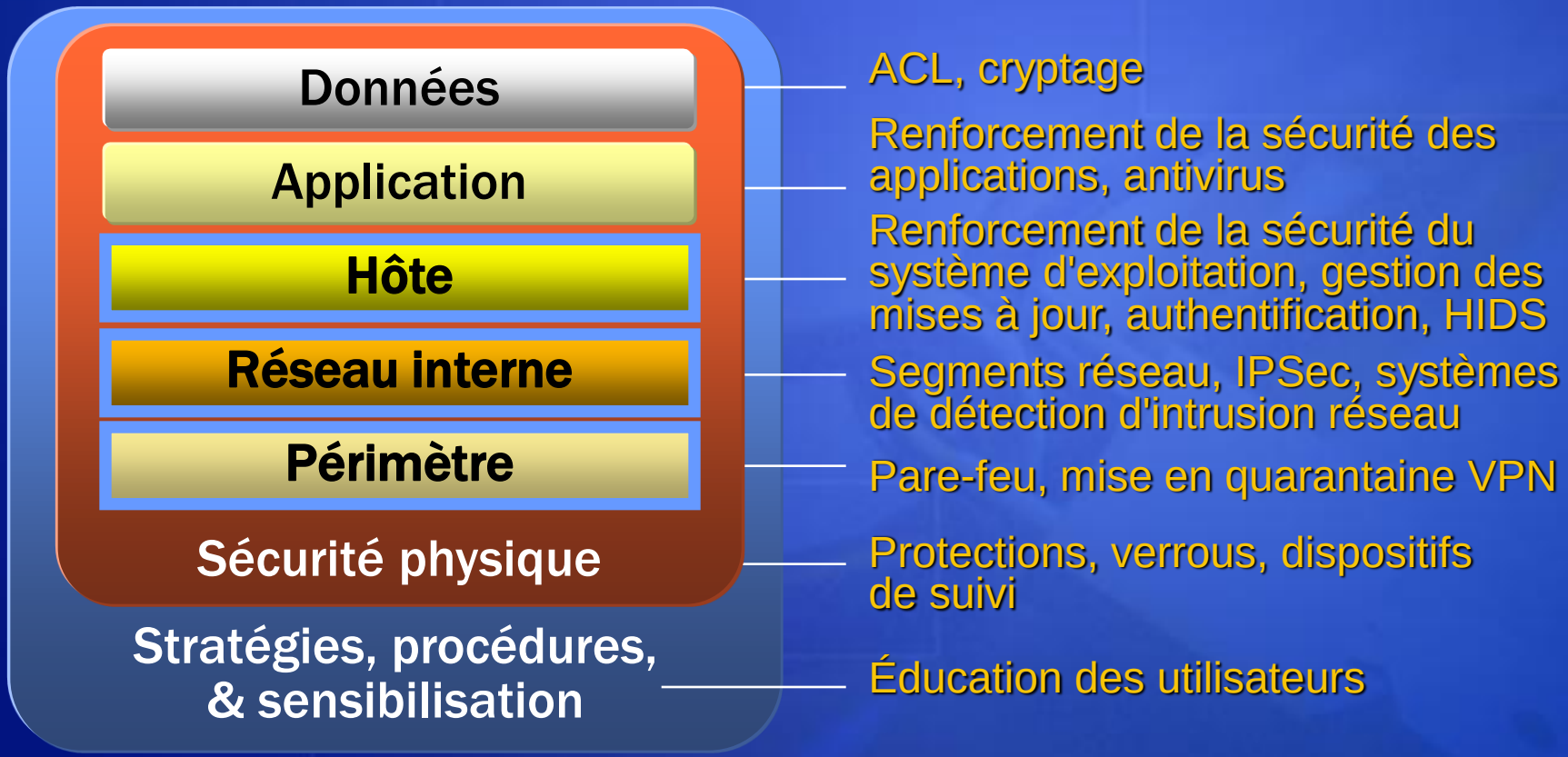
Microsoft

Programme

- Introduction
- Utilisation des défenses du périmètre
- Utilisation de Microsoft ISA (Microsoft® Internet Security and Acceleration) Server pour protéger les périmètres
- Utilisation du pare-feu Windows pour protéger les clients
- Protection des réseaux sans fil
- Protection des communications à l'aide d'IPSec

Défense en profondeur

- Utilisation d'une approche en couches :
  - Augmente la probabilité de détection d'un intrus
  - Réduit les chances de succès d'un intrus



Objectif et limitations des défenses du périmètre

- Des pare-feu et des routeurs de frontière correctement configurés sont la pierre angulaire de la sécurité du périmètre
- Internet et la mobilité augmentent les risques de sécurité
- Les réseaux privés virtuels ont assoupli le périmètre et ont fait disparaître (en association avec les réseaux sans fil) le concept traditionnel de périmètre réseau
- Les pare-feu à filtrage de paquets traditionnels bloquent uniquement les ports réseau et les adresses d'ordinateurs
- La plupart des attaques modernes se produisent au niveau de la couche Application

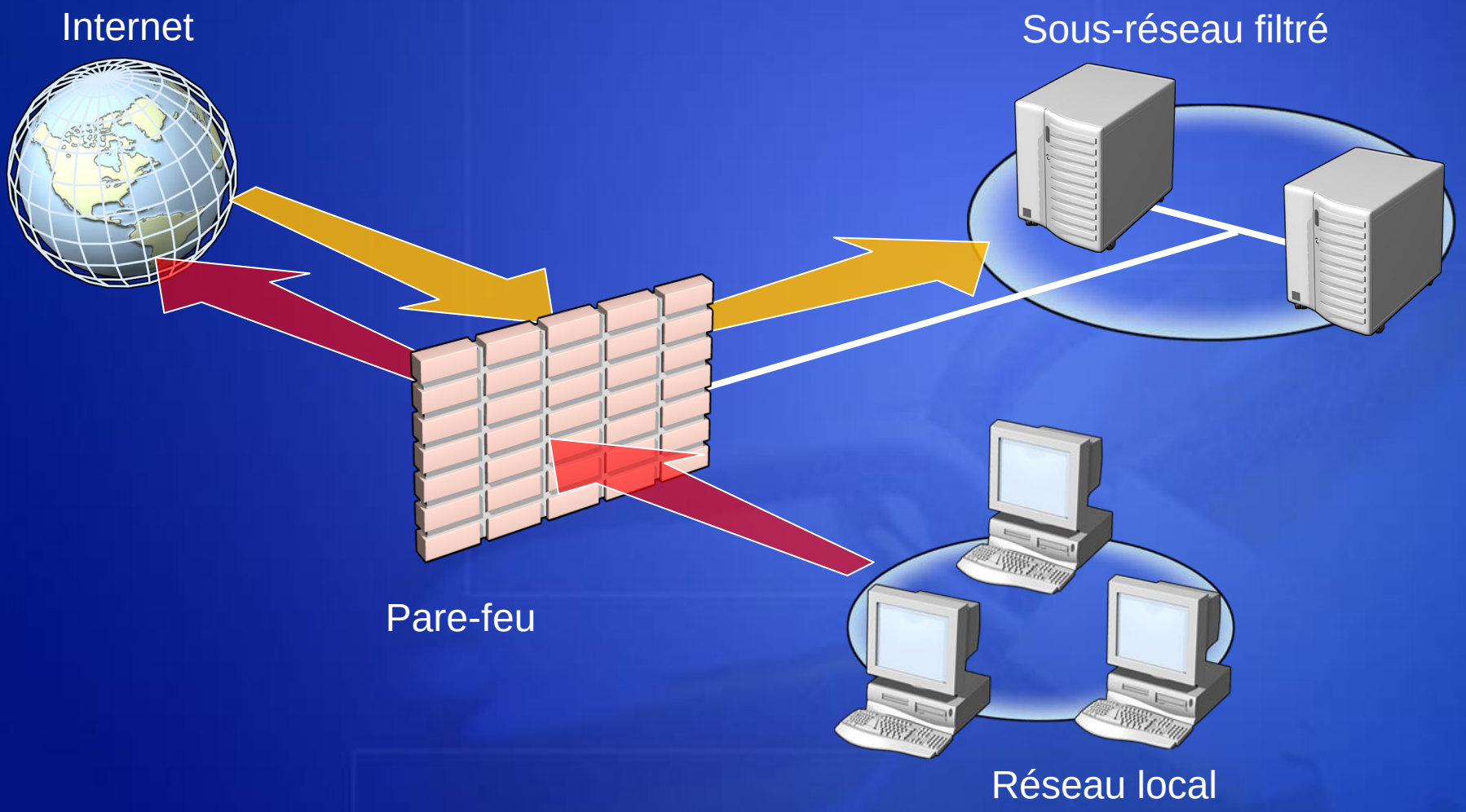
Objectif et limitations des défenses du client

- Les défenses du client bloquent les attaquent qui contournent les défenses du périmètre ou qui proviennent du réseau interne
- Les défenses du client comprennent entre autres :
  - Le renforcement du système d'exploitation
  - Un logiciel antivirus
  - Des pare-feu personnels
- Les défenses du client impliquent la configuration de nombreux ordinateurs
- Dans des environnements non managés, les utilisateurs peuvent contourner les défenses du client

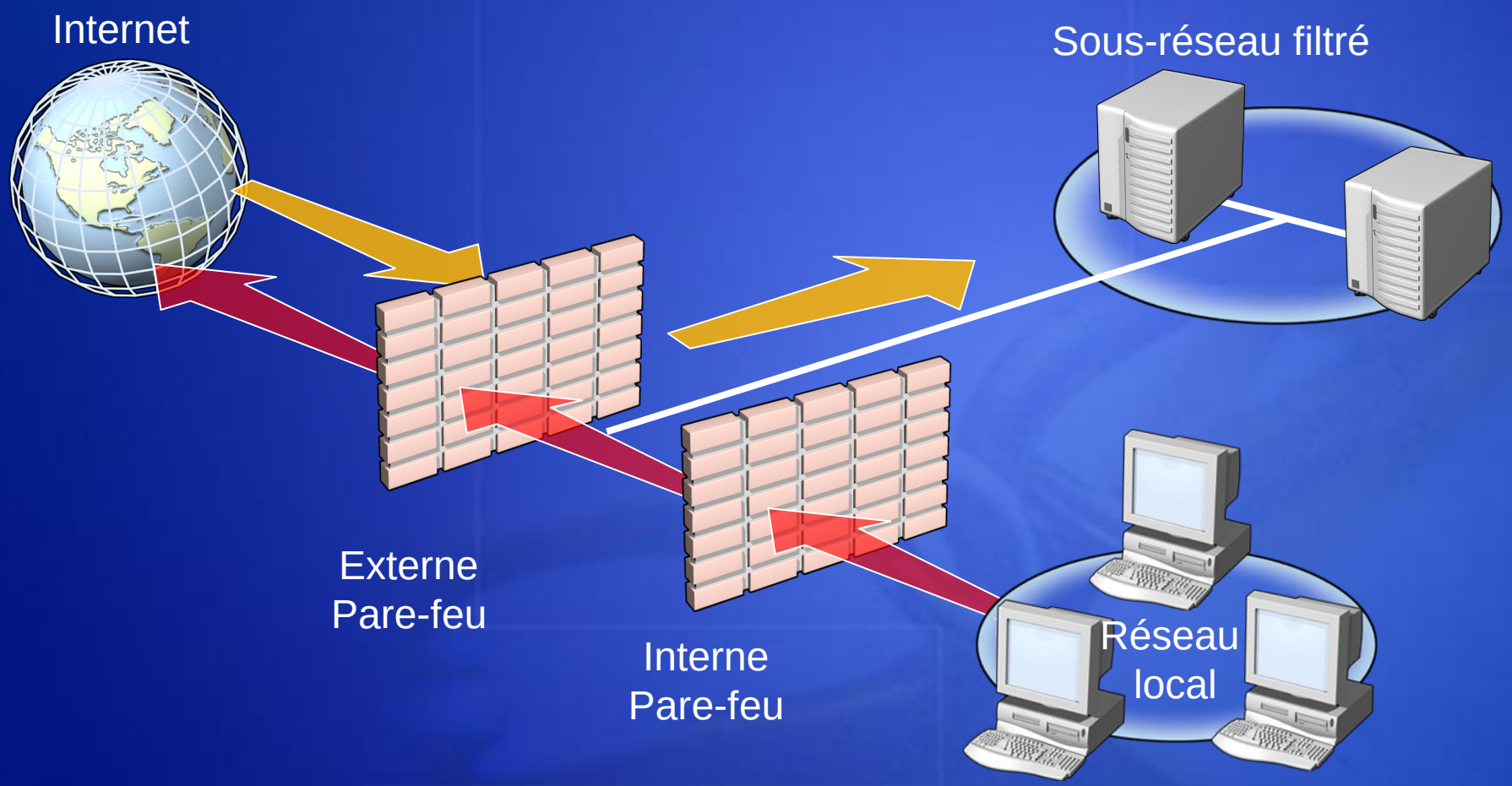
Objectif et limitations de la détection des intrusions

- Détecte le modèle des attaques courantes, enregistre le trafic suspect dans les journaux des événements et/ou avertit les administrateurs
- Les menaces et les failles de sécurité sont en constante évolution, ce qui rend les systèmes vulnérables tant qu'une nouvelle attaque n'est pas connue et une nouvelle signature créée et diffusée

Conception d'un pare-feu : trois hôtes



Conception d'un pare-feu : dos à dos

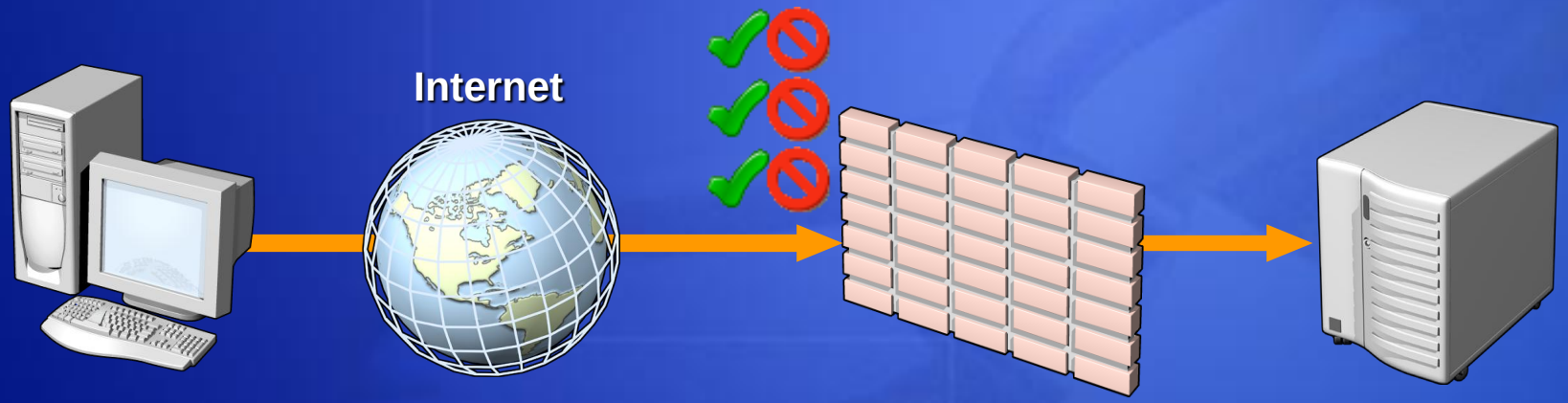


Ce contre quoi les pare-feu NE protègent PAS

- Trafic malveillant qui est passé via les ports ouverts et qui n'est pas inspecté au niveau de la couche Application par le pare-feu
- Tout le trafic qui passe via un tunnel ou une session cryptée
- Attaques une fois qu'un réseau a été pénétré
- Trafic qui semble légitime
- Utilisateurs et administrateurs qui installent des virus par accident ou intentionnellement
- Administrateurs qui utilisent des mots de passe faibles

Types de fonctions de pare-feu

- Filtrage de paquets
- Inspection avec état
- Inspection de la couche Application



Inspection de plusieurs couches
(notamment filtrage de la couche Application)

Objectifs de la sécurité réseau

	Défense du périmètre	Défense du client	Détection des intrusions	Contrôle d'accès réseau	Confiden-tialité	Accès distant sécurisé
ISA Server	✓		✓ *	✓		✓
Pare-feu Windows		✓				
802.1x / WPA				✓	✓	
IPSec		✓			✓	✓

*** Détection des intrusions de base, étendues par les partenaires**

Protection des clients

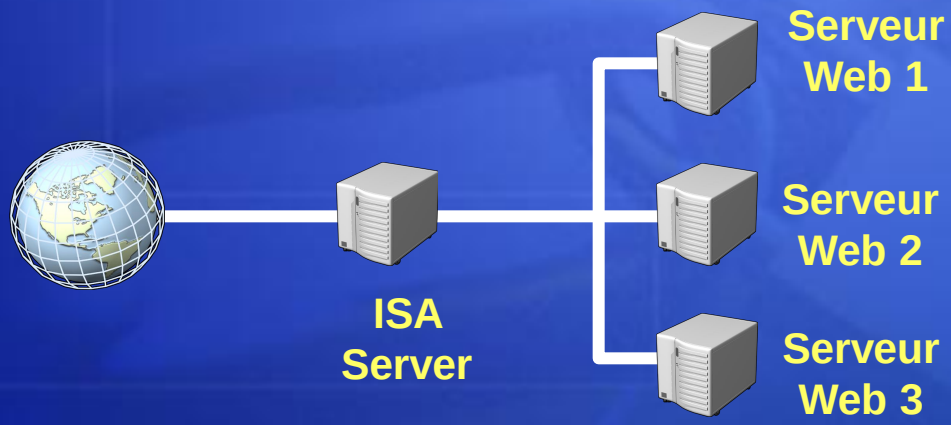
Méthode	Description
Fonctions proxy	**Traite toutes les demandes pour les clients et n'autorise jamais les connexions directes.**
Support client	**Prise en charge de tous les clients sans logiciel spécifique. L'installation du logiciel de pare-feu ISA sur les clients Windows permet des fonctionnalités supplémentaires.**
Règles	**Les règles de protocole, de contenu et de site et de publication déterminent si l'accès est autorisé.**
Compléments	**Le prix d'achat initial pour des pare-feu matériels peut être moindre. Les pare-feu logiciels tirent parti des coûts peu élevés des processeurs. Le matériel peut être facilement mis à niveau et l'ancien matériel ré attribué.**

Protection des serveurs Web

- Règles de publication Web
  - Protègent les serveurs Web situés derrière le pare-feu contre les attaques externes en inspectant le trafic HTTP et en s'assurant qu'il est formaté correctement et qu'il répond aux normes
- Inspection du trafic SSL (Secure Socket Layer)
  - Décrypte et inspecte les demandes Web cryptées entrantes pour s'assurer qu'elles correspondent au formatage et aux normes requises
  - Peut recrypter le trafic avant de l'envoyer sur le serveur Web

URLScan

- ISA Server Feature Pack 1 comprend URLScan 2.5 pour ISA Server
- Permet l'application du filtre ISAPI URLScan à la périphérie du réseau
  - Blocage général de tous les serveurs Web derrière le pare-feu
  - Blocage du périmètre contre toutes les attaques connues ou nouvellement découvertes



Protection d'Exchange Server

Méthode	Description
Assistant de publication de messages	**Configure les règles d'ISA Server pour publier de façon sécurisée les services de messagerie internes pour les utilisateurs externes**
Filtreur de messages	**Filtre les messages électroniques SMTP qui entrent sur le réseau interne**
Publication RPC	**Sécurise l'accès au protocole natif pour les clients Microsoft Outlook®**
Publication OWA	**Fournit une protection du serveur OWA principal pour les utilisateurs Outlook distants qui accèdent à Microsoft Exchange Server sur des réseaux non approuvés sans réseau privé virtuel**

Trafic qui contourne l'inspection du pare-feu

- Le trafic SSL passe à travers les pare-feu traditionnels car il est crypté, ce qui permet aux virus et aux vers de passer inaperçus et d'infecter les serveurs internes
- Le trafic VPN est crypté et ne peut pas être inspecté
- Le trafic IM (Instant Messenger) souvent n'est pas inspecté et peut être utilisé pour transférer des fichiers

Inspection SSL

- Le trafic SSL passe à travers les pare-feu traditionnels car il est crypté, ce qui permet aux virus et aux vers de passer inaperçus et d'infecter les serveurs internes
- ISA Server peut décrypter et inspecter le trafic SSL. Le trafic inspecté peut être envoyé au serveur interne crypté ou en clair

Objectifs de la sécurité réseau

	Défense du périmètre	Défense du client	Détection des intrusions	Contrôle d'accès réseau	Confiden-tialité	Accès distant sécurisé
ISA Server	✓		✓*	✓		✓
Pare-feu Windows		✓				
802.1x / WPA				✓	✓	
IPSec		✓			✓	✓

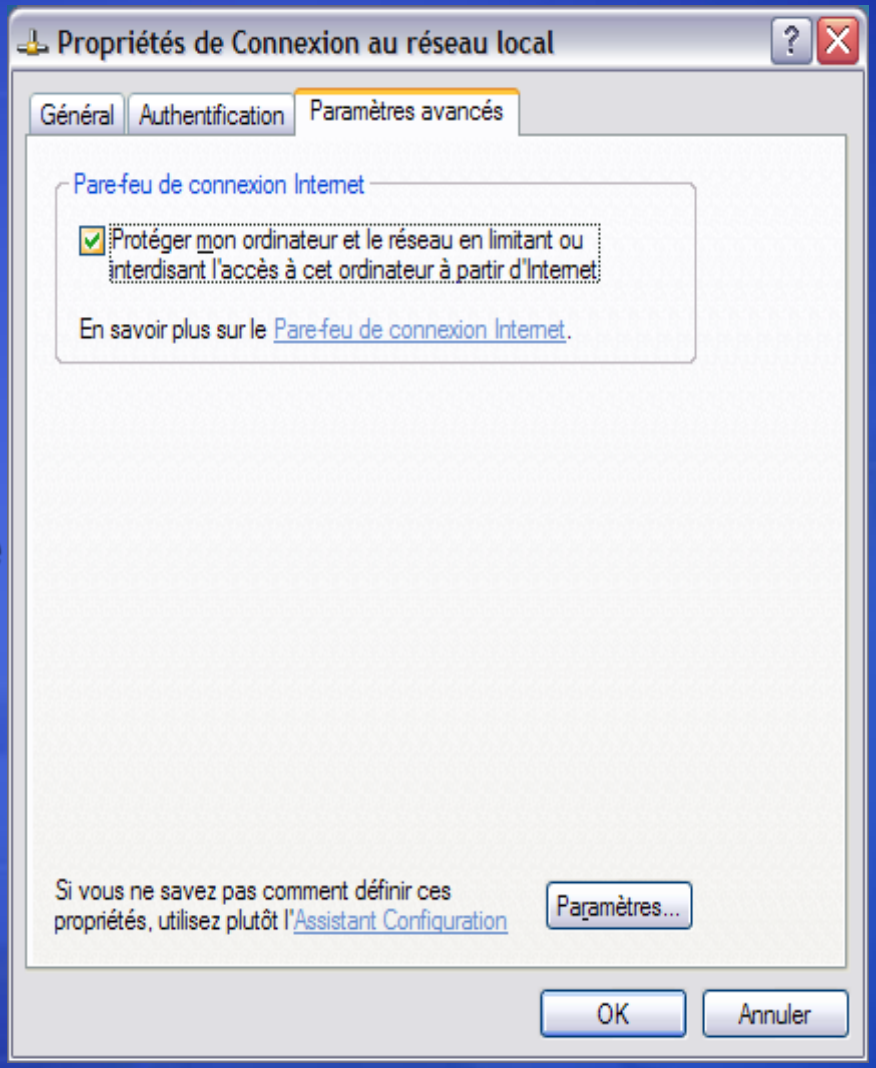
*** Détection des intrusions de base, étendues par les partenaires**

Vue d'ensemble du pare-feu Windows

Qu'est-ce ?	• Pare-feu Windows dans Microsoft Windows XP et Microsoft Windows Server 2003
À quoi sert-il ?	• Aide à arrêter les attaques qui ciblent le réseau, telles que Blaster, en bloquant tout le trafic entrant non sollicité
Fonctionnalités clés	• Des ports peuvent être ouverts pour les services qui s'exécutent sur l'ordinateur • Administration d'entreprise par stratégie de groupe

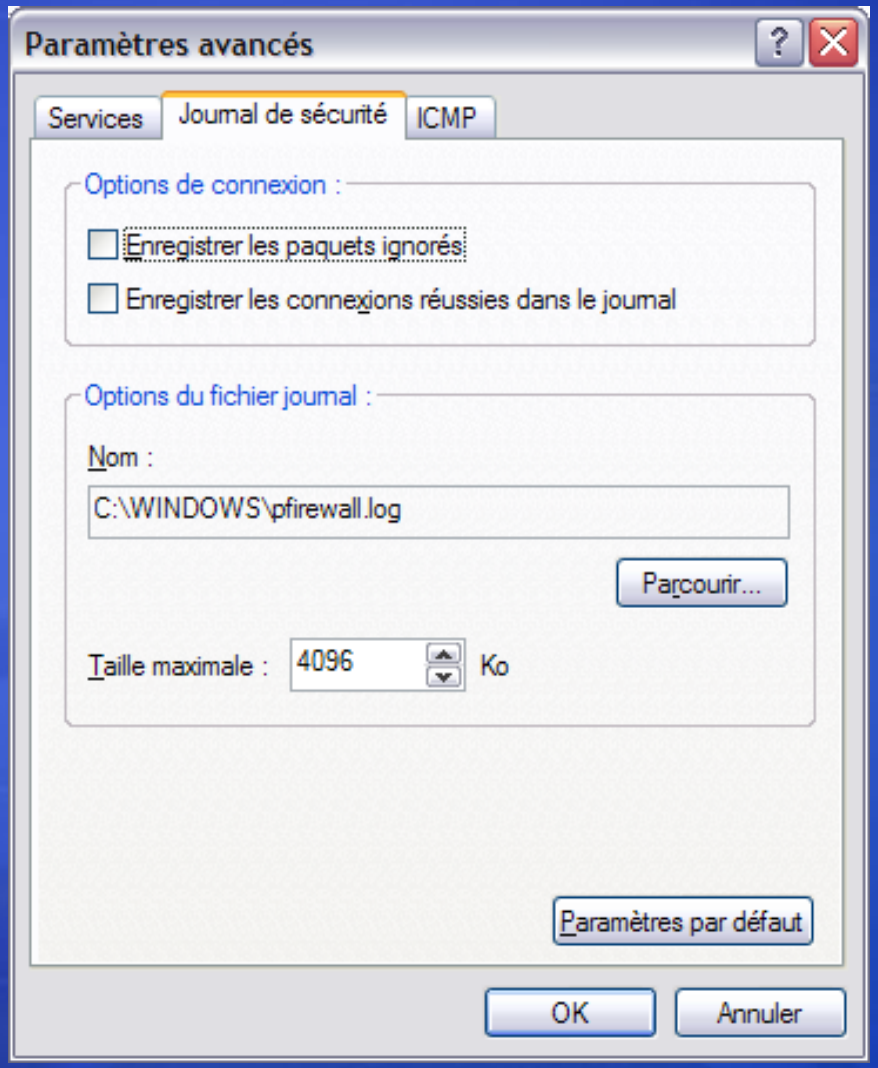
Activation du pare-feu Windows

- Activé :
  - En activant une case à cocher
  - Avec l'Assistant Configuration du réseau
  - Avec l'Assistant Nouvelle connexion
- Activé séparément pour chaque connexion réseau



Journalisation de la sécurité du pare-feu Windows

- Options de journalisation
- Options du fichier journal



Objectifs de la sécurité réseau

	Défense du périmètre	Défense du client	Détection des intrusions	Contrôle d'accès réseau	Confiden-tialité	Accès distant sécurisé
ISA Server	✓		✓*	✓		✓
Pare-feu Windows		✓				
802.1x / WPA				✓	✓	
IPSec		✓			✓	✓

*** Détection des intrusions de base, étendues par les partenaires**

Problèmes de sécurité sans fil

- Limitations de WEP (Wired Equivalent Privacy)
  - Les clés WEP statiques ne sont pas modifiées dynamiquement et sont donc vulnérables aux attaques
  - Il n'existe pas de méthode standard pour fournir des clés WEP statiques aux clients
  - Évolutivité : Compromission d'une clé WEP statique expose tout le monde
- Limitations du filtrage des adresses MAC
  - Un intrus peut usurper une adresse MAC autorisée

Solutions possibles

- Authentification de couche 2 par mot de passe
  - IEEE 802.1x PEAP/MSCHAP v2
- Authentification de couche 2 par certificat
  - IEEE 802.1x EAP-TLS
- Autres options
  - Connectivité VPN
    - L2TP/IPsec (recommandé) ou PPTP
    - N'autorise pas les utilisateurs itinérants
    - Utile lors de l'utilisation de points d'accès sans fil publics
    - Aucune authentification de l'ordinateur ou traitement des paramètres de l'ordinateur dans la stratégie de groupe
  - IPSec
    - Problèmes d'interfonctionnement

Comparaison de sécurité WLAN

Type de sécurité WLAN	Niveau de sécurité	Facilité de déploiement	Facilité d'utilisation et intégration
WEP statique	Faible	Élevé	Élevé
IEEE 802.1X PEAP	Élevé	Moyen	Élevé
IEEE 802.1x TLS	Élevé	Faible	Élevé
VPN	Élevé (L2TP/IPSec)	Moyen	Faible
IPSec	Élevé	Faible	Faible

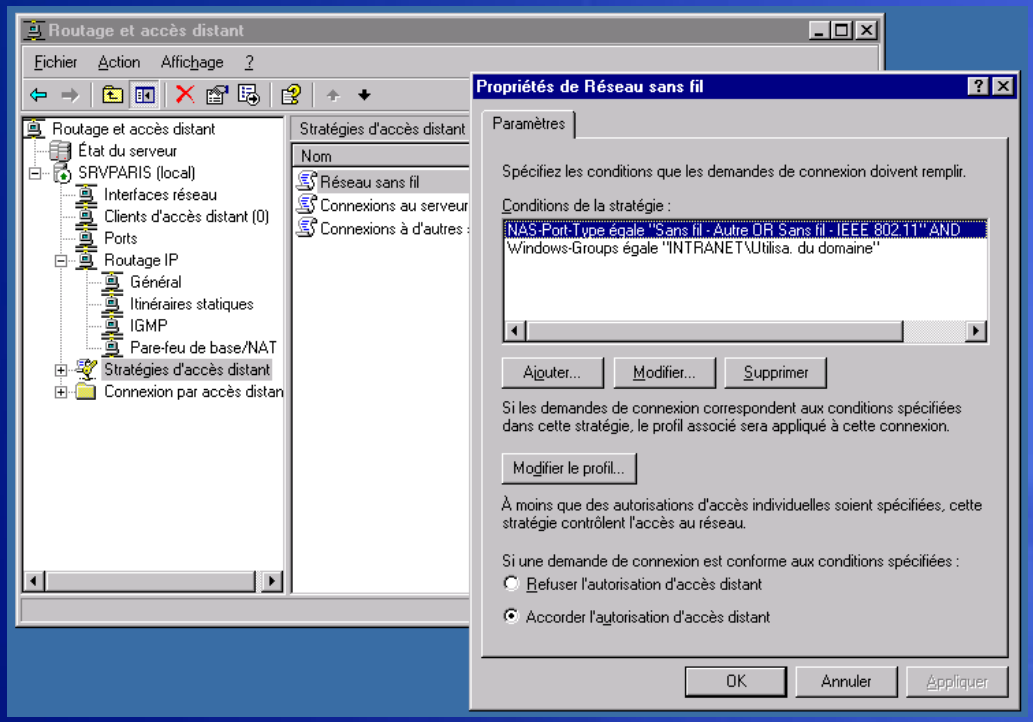
802.1x

- Définit le mécanisme de contrôle d'accès basé sur les ports
  - Fonctionne sur des réseaux avec et sans fil
  - Pas de configuration spéciale de clé de cryptage
- Permet le choix des méthodes d'authentification à l'aide du protocole EAP (Extensible Authentication Protocol)
  - Choisi par les homologues au moment de l'authentification
  - Le point d'accès ne se préoccupe pas des méthodes EAP
- Gère automatiquement les clés
  - Pas besoin de préprogrammation des clés de cryptage sans fil

Configuration requise pour 802.1x

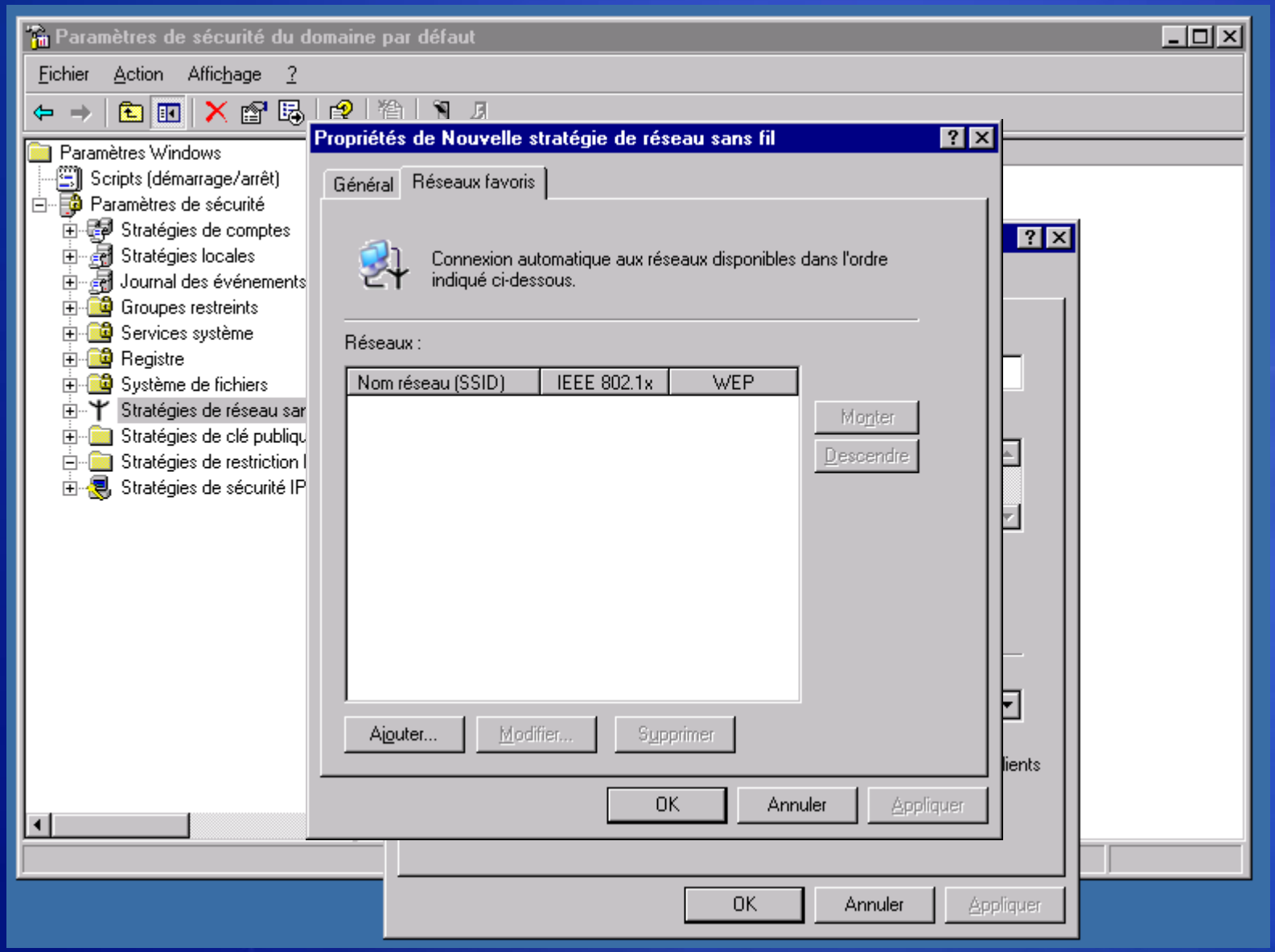
- Client : Windows XP
- Serveur : Windows Server 2003 IAS
  - Internet Authentication Service — notre serveur RADIUS
  - Certificat sur l'ordinateur IAS
- 802.1x sur Windows 2000
  - Le client et IAS doivent utiliser le SP3
  - Consultez l'article 313664 de la Base de connaissances
  - Pas de prise en charge de la configuration automatique sur le client
  - Prend en charge uniquement EAP-TLS et MS-CHAPv2
    - Les futures méthodes EAP sur Windows XP et Windows Server 2003 ne pourront pas être utilisées sur un système antérieur

Stratégies d'accès



- Conditions de stratégie
  - ***NAS-port-type correspond à Wireless IEEE 802.11 OU Wireless Other***
  - ***Groupe Windows = <certain groupe dans Active Directory>***
    - En option, permet un contrôle administratif
    - Doit contenir les comptes d'ordinateurs et d'utilisateurs

Stratégies d'accès



Accès protégé sans fil (WPA, Wireless Protected Access)

- Une spécification qui regroupe des améliorations de la sécurité basées sur des normes et qui améliore le niveau de protection des données et le contrôle d'accès pour les systèmes LAN sans fil existants et futurs
- WPA requiert l'authentification 802.1x pour l'accès réseau
- Objectifs
  - Cryptage de données amélioré
  - Fournir une authentification de l'utilisateur
  - Compatibilité ascendante avec 802.11i
  - Fournir une solution non-RADIUS pour les PME/PMI
- Wi-Fi Alliance a commencé le test de la certification pour l'interfonctionnement sur les produits WPA en février 2003

Objectifs de la sécurité réseau

	Défense du périmètre	Défense du client	Détection des intrusions	Contrôle d'accès réseau	Confiden-tialité	Accès distant sécurisé
ISA Server	✓		✓*	✓		✓
Pare-feu Windows		✓				
802.1x / WPA				✓	✓	
IPSec		✓			✓	✓

*** Détection des intrusions de base, étendues par les partenaires**

Mise en œuvre du filtrage de paquets IPSec

- Filtres pour le trafic autorisé et bloqué
- Pas de négociation d'associations de sécurité IPSec
- Filtres superposés — la correspondance la plus spécifique détermine l'action
- Ne fournit pas de filtrage avec état
- Doit définir "NoDefaultExempt = 1" pour être sécurisé

À partir d'une adresse IP	Vers une adresse IP	Protocole	Port source	Port de destination	Action
Quelconque	Mon adresse IP Internet	Quelconque	N/A	N/A	Bloquer
Quelconque	Mon adresse IP Internet	TCP	Quelconque	80	Autoriser

Le filtrage de paquets n'est pas suffisant pour protéger le serveur

- Les paquets IP usurpés qui contiennent des requêtes ou du contenu malveillant peuvent atteindre des ports ouverts via les pare-feu
- IPSec ne fournit pas une inspection avec état
- De nombreux outils de pirate utilisent les ports source 80, 88, 135, etc., pour se connecter à un port de destination

Communications internes sécurisées

- Utilisez IPSec pour fournir une authentification mutuelle des périphériques
  - Utilisez les certificats ou Kerberos
  - Une clé prépartagée ne convient que pour le test
- Utilisez AH (Authentication Header) pour garantir l'intégrité des paquets
  - AH garantit l'intégrité des paquets
  - AH ne crypte pas, ce qui permet la détection des intrusions réseau
- Utilisez ESP (Encapsulation Security Payload) pour crypter le trafic sensible
  - ESP garantit l'intégrité des paquets et la confidentialité
  - Le cryptage empêche l'inspection des paquets
- Planifiez avec soin le trafic qui doit être sécurisé

VPN sur des supports non approuvés

- VPN client
  - Utiliser L2TP/IPSec
- VPN succursale
  - Entre Windows 2000 ou Windows Server, qui exécute RRAS : Utiliser le tunnel L2TP/IPSec (facile à configurer, ressemble à une interface de routage)
  - Vers une passerelle tierce : Utiliser L2TP/ISec ou le mode tunnel IPSec pur
  - Vers une passerelle Microsoft Windows NT® 4 RRAS : Utiliser PPTP (IPSec n'est pas disponible)

Étapes suivantes

1. Être informé sur la sécurité
   - S'inscrire aux bulletins de sécurité :
     http://www.microsoft.com/france/securite/bulletins_securite/default.asp
   - Obtenir l'aide la plus récente de Microsoft sur la sécurité :
     http://www.microsoft.com/france/securite/default.asp
2. Obtenir des activités de formation supplémentaires sur la sécurité
   - Trouver des séminaires de formation :
     http://www.microsoft.com/france/events/default.asp
   - Trouver un centre de formation local agréé Microsoft (CTEC) pour des cours pratiques :
     http://www.microsoft.com/france/formation/centres/recherche.asp

Pour plus d'informations

- Site Microsoft sur la sécurité (tout public)
  - http://www.microsoft.com/france/securite/default.asp
- Site TechNet sur la sécurité (informaticiens)
  - http://www.microsoft.com/france/technet/themes/secur/default.asp
- Site MSDN sur la sécurité (développeurs)
  - http://msdn.microsoft.com/security (en anglais)
- Newsgroup
  - news://news.microsoft.com

Des questions ?

Microsoft