Protection des accès distants avec les services de quarantaine

http://www.microsoft.com/france/securite
news://microsoft.public.fr.securite

Cyril Voisin
Chef de programme Sécurité
Microsoft France

Microsoft

Sommaire

- Services de quarantaine de Windows Server 2003 SP1 (Network Access Quarantine Control)
- Les autres mécanismes de quarantaine
  - Pare-feu ISA Server 2004
  - Le futur : NAP

Quarantaine dans Windows Server 2003

Network Access Quarantine Control

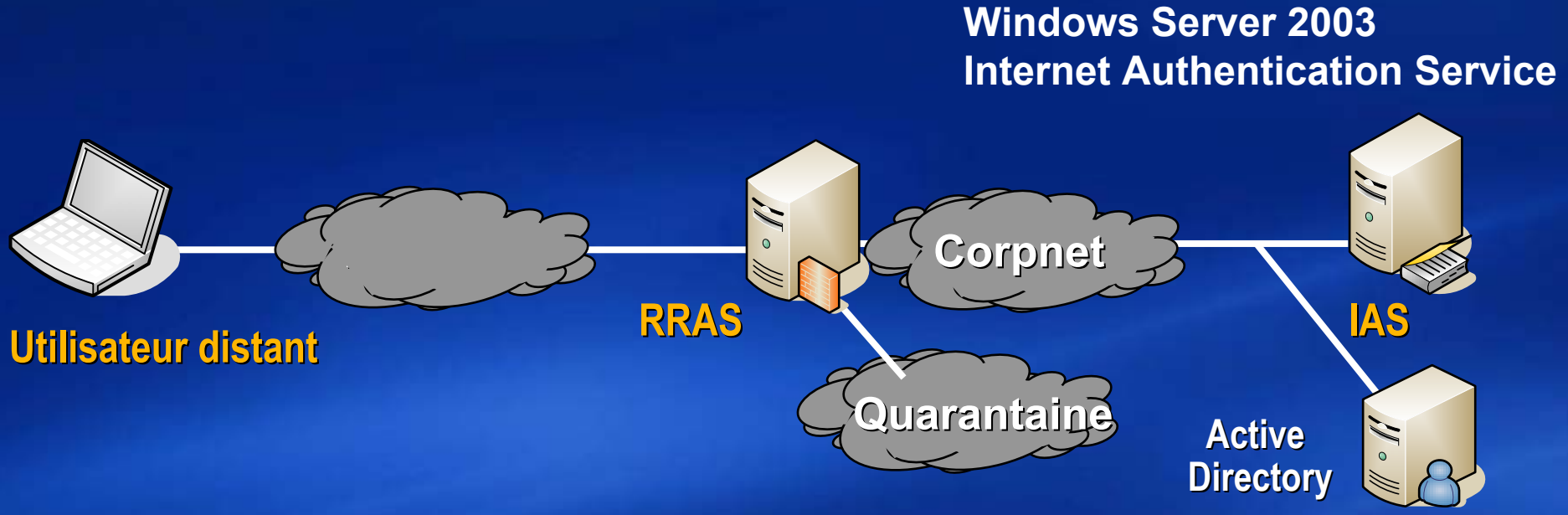
Sécurité des accès distants

- Moyens de protection classiques
  - Authentification forte
  - Chiffrement des communications
- Problématique
  - Que se passe-t-il si la machine qui se connecte
    - N'est pas saine ?
    - N'est pas à jour ? (tant au niveau des patches qu'au niveau des signatures d'antivirus ou d'antispyware ?)
    - N'a pas eu le temps de se mettre à jour ? (portable utilisant uniquement l'accès à distance par intermittence)

Quarantaine

- Solution de contrôle et de mise en conformité des postes lors des connexions distantes (portables ou machines à la maison ne présentant pas forcément toutes les garanties en termes d'application des mises à jour de sécurité, d'antivirus, d'antispyware, etc.)

VPN: Quarantaine



- Vérifie que les systèmes distants sont conformes aux standards de sécurité de l'entreprise.
- Limite le risque de défaillances de sécurité
- Limite la propagation des logiciels malveillants
  - Systèmes distants
  - Systèmes de sous-traitants ou extérieurs

Côté client

- Clients
  - Windows Server 2003
  - Windows XP Professionnel et Édition Familiale
  - Windows 2000
  - Windows Millennium Edition
  - Windows 98 Seconde Édition
- Profils CM créés avec le *Connection Manager Administration Kit* (CMAK), fourni dans Windows Server 2003 SP1
  - Une action post-connexion qui exécute un script de conformité à la stratégie d'accès
  - Un script de conformité à la stratégie d'accès
  - Un composant de notification

Notification et script

- Composant de notification
  - Le composant de notification envoie un message signalant la bonne exécution du script au serveur d'accès distant de quarantaine
  - Il est possible d'utiliser soit un composant de notification propre, soit Rqc.exe, qui est fourni dans Windows Server 2003 SP1
- Script de stratégie d'accès
  - Effectue des contrôles sur le système client distant pour vérifier sa conformité avec la stratégie d'accès. Il peut s'agir d'un fichier exécutable ou d'un simple fichier de commandes (fichier batch)

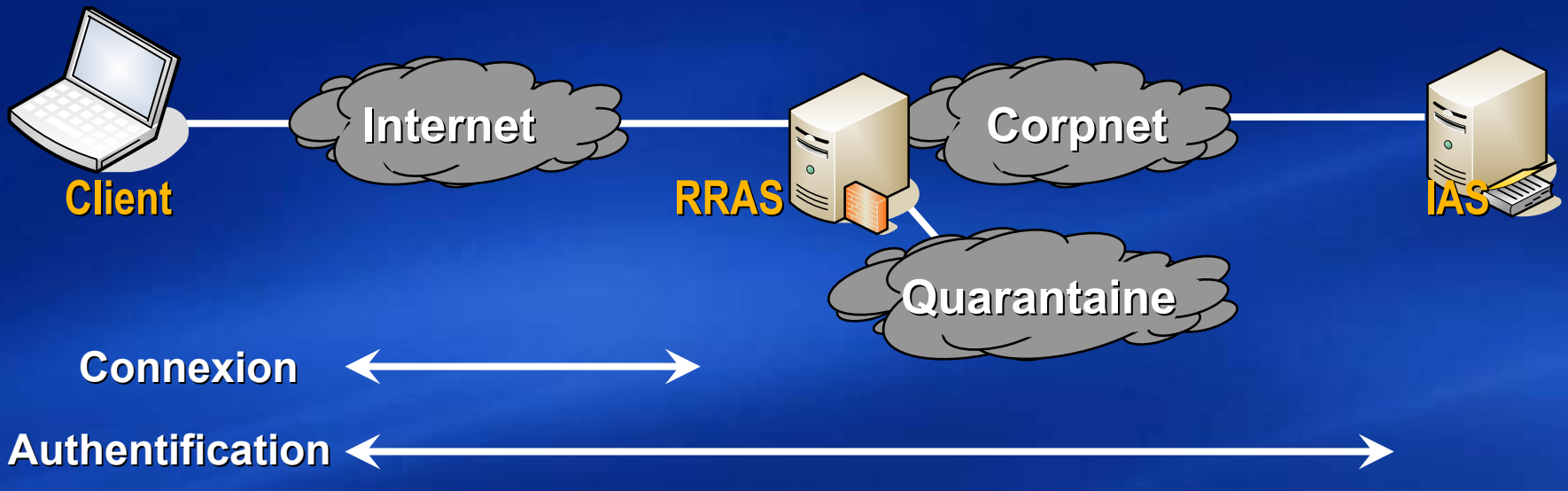
Côté serveur

- Un système exécutant l'une des versions de Windows Server 2003 et RRAS (*Routing and Remote Access*), supportant les attributs RADIUS *MS-Quarantine-IPFilter* et *MS-Quarantine-Session-Timeout* pour imposer les paramètres de quarantaine
- Un composant recevant les notifications (*listener*)

Description du fonctionnement

1. Le client distant utilise le profil CM installé pour se connecter au serveur d'accès distant
2. Le client distant fournit ses informations d'authentification au serveur d'accès distant
3. Le service *Routing and Remote Access* envoie une demande d'accès RADIUS au serveur IAS
4. Le serveur IAS valide les informations d'authentification du client distant et, si elles sont valides, vérifie sa stratégie d'accès distant. La tentative de connexion respecte les règles de quarantaine

Description du fonctionnement



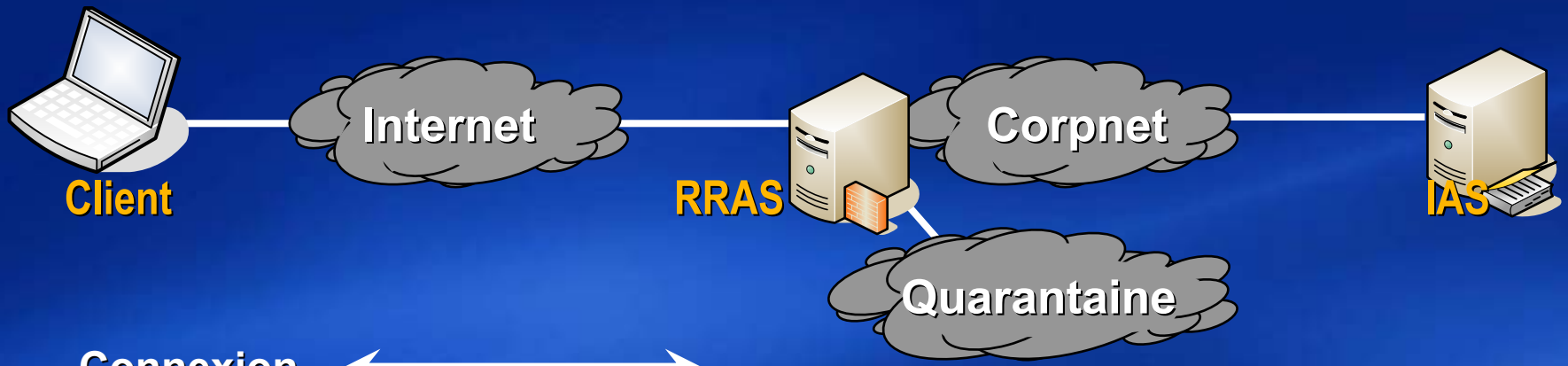
Description du fonctionnement

5. La connexion est acceptée avec les restrictions de quarantaine. Le serveur IAS envoie une autorisation d'accès RADIUS, contenant entre autres les attributs *MS-Quarantine-IPFilter* et *MS-Quarantine-Session-Timeout*
   (cet exemple suppose que les 2 attributs sont configurés dans la règle d'accès distant correspondante)
6. Le client distant et serveur d'accès complètent la connexion distante, ce qui inclut l'obtention d'une adresse IP et d'autres paramétrages

Description du fonctionnement

7. Le service *Routing and Remote Access* configure les paramètres *MS-Quarantine-IPFilter* et *MS-Quarantine-Session-Timeout* pour la connexion. A ce point, le client distant ne peut envoyer que du trafic respectant les filtres de quarantaine et dispose du nombre de secondes spécifié par *MS-Quarantine-Session-Timeout* pour notifier au serveur d'accès que le script s'est effectué avec succès
8. Le profil CM exécute le script de quarantaine comme action de post-connexion

Description du fonctionnement



Connexion

Authentification

Autorisation

VSA Quarantaine
+ Filtres normaux

Accès en
Quarantaine

Description du fonctionnement

9. Le script de quarantaine vérifie que le système du client distant est conforme à la stratégie des pré-requis de configuration. Si tous ces tests de contrôle sont réussis, le script exécute Rqc.exe avec ces paramètres de commande, dont l'un contient le libellé de la version du script de quarantaine inclus dans le profil CM
10. Rqc.exe envoie une notification au serveur d'accès distant, indiquant que le script s'est exécuté avec succès. La notification inclut le libellé de la version du script de quarantaine

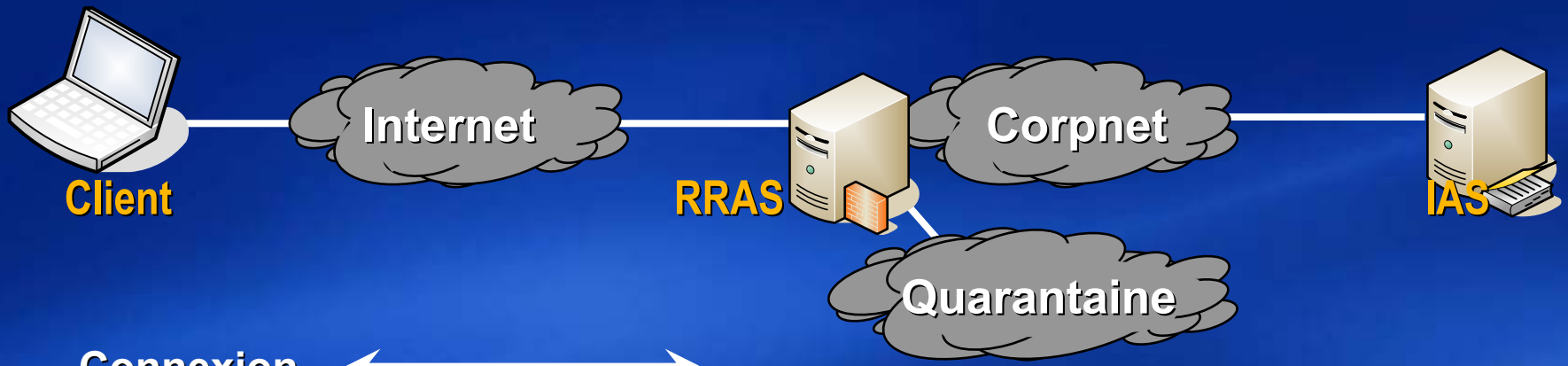
Description du fonctionnement

11. La notification est reçue par le composant *listener* (Rqs.exe). Le trafic nécessaire à la notification a été accepté car correspondant aux échanges autorisés par les filtres de quarantaine configurés par l'attribut *MS-Quarantine-IPFilter* de la règle d'accès distant correspondante
12. Le composant *listener* compare le libellé de la version du script contenu dans le message de notification avec ceux configurés dans le Registre et renvoie un message indiquant que cette version du script est soit valide, soit invalide

Description du fonctionnement

13. Si la version du script est valide, le composant *listener* invoque l'API *MprAdminConnectionRemoveQuarantine*(), qui permet au service *Routing and Remote Access* de supprimer les paramètres *MS-Quarantine-IPFilter* et *MS-Quarantine-Session-Timeout* de la connexion et configure les conditions de la connexion normale. Dés lors, le client distant dispose d'un accès normal à l'intranet
14. Le composant « *listener* » enregistre dans le journal Système un événement détaillant la connexion en quarantaine

Description du fonctionnement



Connexion

Authentification

Autorisation

VSA Quarantaine
+ Filtres normaux

Accès en
Quarantaine

Résultat de la
vérification des règles

Suppression de la quarantaine

Accès complet

Stratégie d'accès en quarantaine

- Il est possible d'utiliser l'attribut *MS-Quarantine-IPFilter* pour configurer les filtres d'entrées/sorties afin de n'autoriser que :
  - Le trafic généré par l'agent de notification. Si vous utilisez Rqc.exe et Rqs.exe avec leur port par défaut, alors le filtre des paquets entrants ne doit accepter que le trafic vers le port TCP 7250
  - Le trafic nécessaire aux messages *Dynamic Host Configuration Protocol* (DHCP) entre le client distant et le serveur d'accès
  - Le trafic nécessaire pour accéder aux ressources de quarantaine. Cela comprend des filtres permettant au client distant d'accéder à des serveurs de résolution de noms (tels des serveurs DNS), de partage de fichiers, ou de sites Web

Comment déployer le contrôle d'accès par quarantaine

- Créer des ressources de quarantaine
- Créer un script ou un programme qui valide la configuration client
- Installer Rqs.exe sur les serveurs d'accès
- Créer un nouveau profil CM de quarantaine avec CMAK de Windows Server 2003
- Distribuer le profil CM pour l'installer sur les postes distants
- Configurer la stratégie d'accès par quarantaine

Créer des ressources de Quarantaine

- Serveurs de résolution de noms (tels que des serveurs DNS et WINS [*Windows Internet Name Service*])
  - Autoriser la résolution de noms DNS ou NetBIOS pendant que le client est en quarantaine. Cela est important quand vous référencez des serveurs de fichiers, des sites Web, ou d'autres types de ressources par leur nom
- Serveurs de fichiers
  - Autoriser l'accès à des fichiers partagés, utilisés pour installer les composants nécessaires sur les clients distants, tels mises à jour de signatures de virus ou profils CM
- Serveurs Web
  - Autoriser l'accès aux pages Web contenant les instructions et les liens vers les composants à installer sur les clients distants

Où placer les ressources de quarantaine ?

- Désigner ou placer toutes les ressources de quarantaine sur un sous-réseau séparé.
  - L'avantage de cette approche est que vous n'avez qu'à configurer qu'un seul filtre d'entrée/sortie pour vos ressources de quarantaine
- Désigner différents serveurs de votre intranet en tant que ressources de quarantaine, indépendamment de leur emplacement.
  - L'avantage de cette approche est que vous pouvez utiliser des serveurs existants pour héberger les ressources de quarantaine, profitant de leur sous-utilisation

Créer un script ou un programme qui valide la configuration client

- Le script ou programme de quarantaine que vous créez peut être soit un fichier exécutable (*.exe) soit un simple fichier de commandes (*.cmd ou *.bat). Dans le script, exécuter la série de tests permettant de vérifier que le client distant est conforme aux stratégies d'accès. Si tous ces tests sont réussis, le script doit exécuter Rqc.exe avec les paramètres suivants :

```
rqc /conn %CONNNAME% /port
%PORT% /domain %DOMAIN% /user
%USERNAME% /sig %REMOVAL% /log
%RQS_LOGMESSAGE%
```

Si les tests de conformité échouent

- Le script peut diriger l'utilisateur distant vers une page Web
- La page décrit comment obtenir les composants nécessaires
- Si la réponse de notification indique une version invalide du script, le script peut proposer à l'utilisateur distant d'installer le dernier profil CM à partir d'un répertoire partagé ou d'une page Web

Restreindre l'accès au serveur VPN

- Dans le cas d'un VPN dédié, restreindre l'accès aux seuls ports nécessaires à la connexion VPN :

Src addr	Src mask	Dest addr	Dest mask	Protocol	Src port	Dest port	Description
Any	Any	Any	Any	47	Any	Any	GRE
Any	Any	Any	Any	TCP	1723	Any	PPTP Inbound
Any	Any	Any	Any	TCP	Any	1723	PPTP Outbound
Any	Any	Any	Any	UDP	500	500	ISAKMP
Any	Any	Any	Any	UDP	1701	1701	L2TP

Restreindre les droits d'utilisation VPN

- Utiliser la stratégie RAS pour accorder la connectivité VPN qu'aux utilisateurs ayant une activité professionnelle nécessitant un accès distant
- Définir les utilisateurs par « *Control access through Remote Access Policy* »
- Exploiter les notions de groupes et d'utilisateurs Windows pour faire respecter les droits d'utilisation VPN

Aperçu de stratégie d'accès

- Configuration de Domaine
  - La permission d'accès distant des propriétés du compte utilisateur est définie à **Control access through Remote Access Policy**
  - Le compte utilisateur est inclus dans le groupe *VPN_Users* de l'annuaire Active Directory
- Configuration de la stratégie d'accès distant
  - Nom de la stratégie : *Remote Access VPN Connections*
  - Méthode d'accès : *VPN*
  - Utilisateur ou Groupe : Groupe avec *EXAMPLE|VPN_Users* sélectionné
  - Méthodes d'authentification : **Extensible Authentication Protocol** avec **Smart card ou autres Certificats**, **Microsoft Encrypted Authentication version 2 (MS-CHAP v2)**, et **Microsoft Encrypted Authentication (MS-CHAP)** sélectionnés
  - Niveau de chiffrement : **Strong encryption** et **Strongest encryption** sélectionnés

Filtrage de paquets par profil RAS

- Les stratégies RAS peuvent être utilisées pour spécifier un ensemble de filtres de paquets IP, appliqués aux connexion à distance
- Elles peuvent également empêcher les clients VPN d'envoyer des paquets dont ils ne sont pas la source
  - Protection contre le risque de clients VPN agissant comme des routeurs pour des éléments non authentifiés

Un script (très) simple

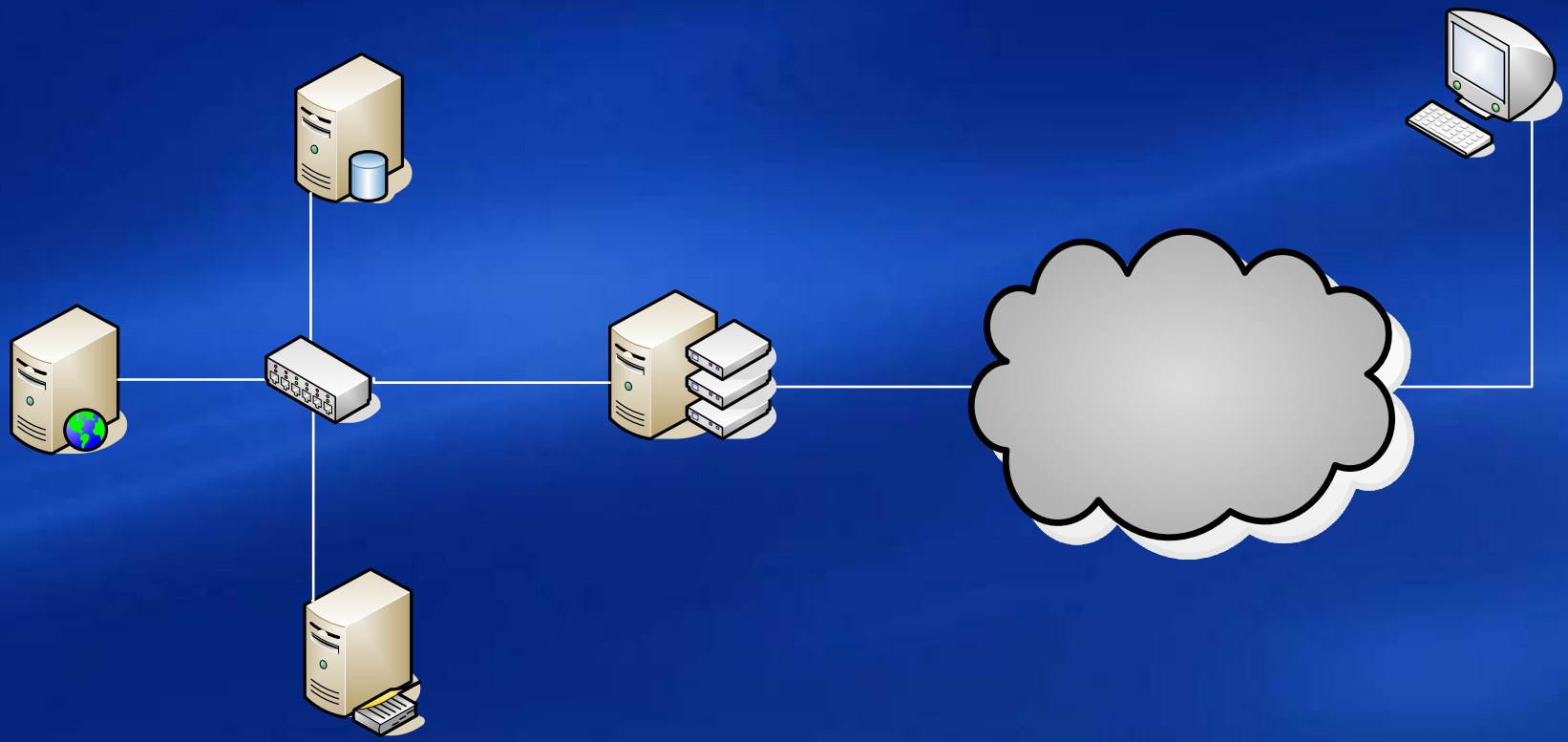
```
:INITIALIZATION
  @echo off
  @rem ***
  @rem * Define the locations for the source file (remove quarantine if
          this file exists) and
  @rem * the target file (the file to copy if the source file does not
          exist).
  @rem *
  SET SOURCE_FILE=c:\access.txt
  SET TARGET_FILE=\\ca1.contoso.com\quarantine\access.txt
  @rem Use %ServiceDir% macro to locate rqc.exe.
  SET RQCLOC=%1\rqc.exe
  @rem Use %DialRasEntry% macro.
  SET CONNNAME=%2
  @rem Use %TunnelRasEntry% macro.
  SET TUNNELCONNNAME=%3
  @rem Use %DomainName% macro.
  SET DOMAIN=%4
  @rem Use %UserName% CM macro for this value.
  SET USERNAME=%5
  SET REMOVAL=Contoso1a
  SET PORT=7250
:VALIDATION
  @rem ***
  @rem * Check whether files can be copied.
  @rem *
  echo Checking for %SOURCE_FILE%
  if exist %SOURCE_FILE% goto REMOVE_QUARANTINE
  @rem ***
  @rem * PING the resource to ensure that it is available
  @rem * before attempting to access it. (This also helps
  @rem * in case of any network delays.)
  @rem *
  ping ca1.contoso.com -n 20 -a
  if exist %TARGET_FILE% goto COPY_FILE_TO_LOCAL
  goto FILE_NOT_FOUND
:FILE_NOT_FOUND
  @rem ***
  @rem * File specified in TARGET_FILE could not be detected.
  @rem *
  echo Unable to locate %TARGET_FILE%
  goto EXIT_SCRIPT
:COPY_FILE_TO_LOCAL
  @rem ***
  @rem * The file does not exist on the local computer. The file will now be copied
  @rem * from the server, and the program will exit (leaving the user in quarantine).
  @rem *
  echo Copying %TARGET_FILE% to %SOURCE_FILE%
  copy %TARGET_FILE% %SOURCE_FILE%
  goto SHOWQUARANTINEINFO
:REMOVE_QUARANTINE
  @rem ***
  @rem * The file exists on the local computer. The client now must be removed from
  @rem * quarantine.
  @rem * Also, to demonstrate how the script works, echo
  @rem * the executable, and pause for test review before opening the
  @rem * Web site. Do not echo or pause in a production script.
  echo %SOURCE_FILE% found!
  echo Executing %RQCLOC% %CONNNAME% %TUNNELCONNNAME% %PORT% %DOMAIN%
%USERNAME% %REMOVAL%
  pause
  %RQCLOC% %CONNNAME% %TUNNELCONNNAME% %PORT% %DOMAIN% %USERNAME%
%REMOVAL%
  IF %ERRORLEVEL%==0 GOTO QUARANTINED_REMOVED
  IF %ERRORLEVEL%==1 GOTO QUARANTINED_INVALIDLOC
  IF %ERRORLEVEL%==2 GOTO QUARANTINED_INVALIDSTRING
  goto QUARANTINE_FAIL
:QUARANTINED_REMOVED
  "%ProgramFiles%\Internet Explorer\iexplore.exe" http://iis1.contoso.com/test.htm
  goto EXIT_SCRIPT
:QUARANTINED_INVALIDSTRING
  echo Invalid removal string passed. Request rejected.
  goto QUARANTINE_FAIL
:QUARANTINED_INVALIDLOC
  echo Unable to contact remote access server. (Is port %PORT% open?)
  GOTO QUARANTINE_FAIL
:QUARANTINE_FAIL
  echo Quarantine removal failed. Please disconnect, and retry the connection.
  echo If the problem persists, please contact HelpDesk at 555-0100.
:SHOWQUARANTINEINFO
  "%ProgramFiles%\Internet Explorer\iexplore.exe" http://ca1.contoso.com/quarantine.htm
  goto EXIT_SCRIPT
:EXIT_SCRIPT
  @rem ***
  @rem * Exit script.
  @rem *
  echo Script has
```

Exemples de script

- Exemples de script de vérification de la configuration client http://www.microsoft.com/downloads/details.aspx?FamilyID=a290f2ee-0b55-491e-bc4c-8161671b2462&displaylang=en

Démo

Réalisée par Arnaud Jumelet



Les limites

1. Utilisateurs malveillants
2. Intégrité du script de quarantaine
3. Systèmes Wi-Fi et 802.1x
4. Numéro de version vulnérable
5. Possibilité d'usurpation de la notification
6. *Reverse Engineering*

ISA Server 2004

La quarantaine dans ISA Server

- Vérifier lors de la connexion la conformité du poste client VPN:
  - Mécanisme d'analyse
  - Mise en quarantaine
- Limiter les accès autorisés pour les sessions VPN
  - Seules les ressources nécessaires sont accessibles
  - L'ensemble du réseau interne ne devrait pas être accessible
- Utiliser du filtrage applicatif pour analyser les communications à destination des ressources internes.
  - Possibilité de faire de l'analyse antivirale
  - Filtrage des flux RPC, http, SMTP, CIFS, DNS…

Network Access Protection (NAP)

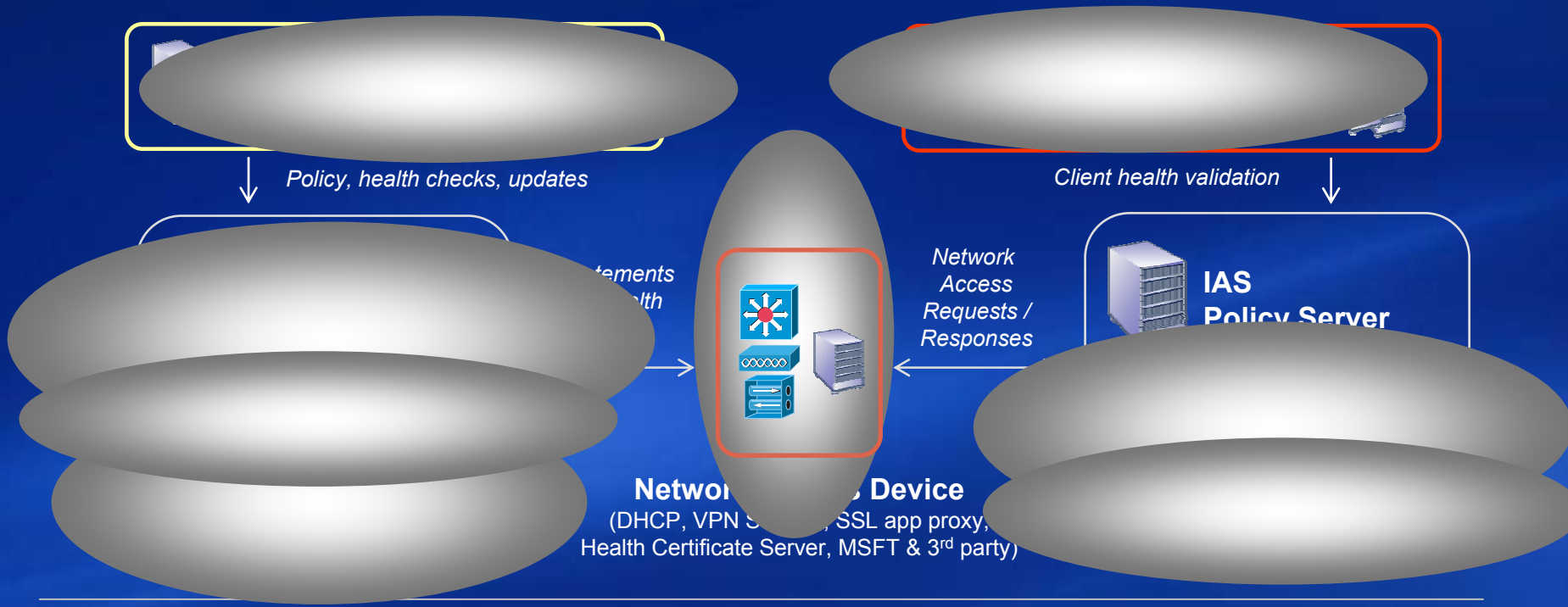
NAP

- Technologie s'appliquant à tout type de connexion réseau (distante mais aussi et surtout locale)
- 3 fonctions de base
  - Validation de la politique de conformité (*Health Policy Validation*)
  - Restriction des clients
  - Mise en conformité (*Health Remediation*)
- NAP est la surcouche santé de vos systèmes de sécurité réseau.
- Prévu pour Windows Server « Longhorn » (en 2007)

Bénéfices de NAP

- Architecture Extensible
  - Extensible via des solutions d'éditeurs tierces
  - Basée sur des standards ouverts (DHCP, IPSec, Radius, 802.1x…)
  - Possibilité d'utilisation de scripts personnalisés pour faire des tests complémentaires
- Fonctionne avec les infrastructures réseau existantes
- Réduit le risque de compromission du réseau

Network Access Protection Components



SHA	System Health Agent = Declares health (patch state, virus signature, system configuration, etc.)
SHV	System Health Validator = Certifies declarations made by health agents
QEC	Quarantine Enforcer = Negotiates access with specific network access devices
NAD	Network Access Device = Facilitates health reporting, enforces network restrictions
QA	Quarantine Agent = Reports client health status, coordinates between SHA and QES
QS	Quarantine Server = Restricts client's network access based on what SHV certifies
SHS	System Health Server = Defines health requirements for system components on the client
RS	Remediation Server = Installs necessary patches, configurations, applications; brings client to healthy state

Les partenaires NAP

http://www.microsoft.com/windowsserver2003/partners/nappartners.mspx

Ressources

- Quarantaine dans Windows Server 2003
  - http://www.microsoft.com/windowsserver2003/techinfo/overview/quarantine.mspx
- Retours d'expérience de Microsoft en tant qu'entreprise
  - www.microsoft.com/technet/itshowcase
- ISA Server 2004
  - www.microsoft.com/isaserver
  - www.microsoft.com/france/isa
- NAP
  - www.microsoft.com/nap

Rendez-vous

- Rendez-vous pour les Journées Microsoft de la Sécurité 2005
  - 17 mai à Lyon
  - 19 mai à Toulouse
  - 24 mai à Marseille
  - 26 mai à Nantes
  - 31 mai à Strasbourg
  - 14 et 15 juin à Paris