UNIL | Université de Lausanne
Centre informatique

Guide Utilisateur « **AUTHENTIC 3** »
UNIL CI, version 06.07.2011

GENERALITES

Règles génériques

Configuration du pare-feu :
- R1: Toutes les sessions sortantes sont permises.
- R2: Pour les sessions entrantes, seul crypto est autorisé comme source.

En dehors de quelques rares exceptions (par exemple le pare-feu natif de Windows XP SP1), il est possible de programmer ces règles dans la majorité des pare-feux. A titre indicatif, les chapitres ci-dessous décrivent la configuration pour les produits suivants :
- Windows Firewall de XP SP2.
- ZoneAlarm.

Au niveau de Windows :
- Activer le service « Affichage des messages » (Messenger) pour recevoir des messages importantes du CI.
- Utiliser un compte avec droits limités pour travaux courants.

Activation du service « Affichage des messages »

Par défaut, ce service est activé dans Windows 2000 et XP SP1. Pour l'activer dans Windows XP SP2 :
- Démarrer> Panneau de configuration> Performances et maintenance> Outils d'administration.
- Double-cliquer sur « Services », puis sur « Affichage des messages ».
- Choisir « Type de démarrage »=Automatique, puis cliquer sur Démarrer.

Désactivation pare-feu de Windows XP

D'une manière générale, on ne peut pas avoir plusieurs pare-feux activés simultanément. Aussi, si l'on désire utiliser un pare-feu différent de celui fourni (et activé) par défaut par Windows XP, il faut désactiver ce dernier.

Pour désactiver le pare-feu de Windows XP SP2 :
- Démarrer> Panneau de configuration> Centre de sécurité> Pare-feu Windows> Général.
- Choisir l'option « Désactivé ».

S'il s'agit de Windows XP SP1, désactiver Internet Connection Firewall (ICF) :
- Démarrer> Panneau de configuration> Connexions réseau et Internet> Connexions réseau.
- Clic droit sur icône connexion, puis Propriétés.
- Cliquer sur l'onglet « Paramètres avancés », puis désactiver « Pare-feu de connexion Internet ».
- Cliquer sur OK.

Utilisation compte avec droits limités

Si on a besoin de l'option « Applications clientes » de crypto, on doit accéder à crypto avec les privilèges d'administrateur. Depuis le compte avec droits limités :
- « Démarrer> Tous les programmes », puis SHIFT-Clic droit (Win2k) ou Clic droite (XP) sur « Internet Explorer ».
- Choisir « Exécuter en tant que... », puis entrer le nom et le mot de passe du compte administrateur.

PARE-FEU WINDOWS XP SP2

Pour utiliser l'option « Applications clientes » de crypto, on doit appliquer le correctif qui se trouve à l'emplacement suivant :

- http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=17d997d2-5034-4bbb-b74d-ad8430a1f7c8

Règle R1

Aucune configuration à faire car ce pare-feu permet toutes les sessions sortantes.

Règle R2

Pour configurer le pare-feu, il suffit d'exécuter les commandes netsh suivantes :

```
netsh fire reset
netsh fire set allow prog=%windir%\system32\sessmgr.exe mode=DISABLE prof=ALL
netsh fire set port proto=TCP port=139 scope=CUSTOM addr=130.223.2.2 prof=ALL
netsh fire set port proto=TCP port=445 scope=CUSTOM addr=130.223.2.2 prof=ALL
netsh fire set port proto=TCP port=3389 scope=CUSTOM addr=130.223.2.2 prof=ALL
netsh fire set port proto=UDP port=137 scope=CUSTOM addr=130.223.2.2 prof=ALL
netsh fire set port proto=UDP port=138 scope=CUSTOM addr=130.223.2.2 prof=ALL
netsh fire add allow prog="%systemdrive%\Program Files\Internet Explorer\iexplore.exe" name=IE
scope=CUSTOM addr=130.223.2.2 profile=ALL
```

Un fichier contenant toutes ces commandes est disponible à l'adresse ci-dessous :

- \\softboss\soft\Security\Crypto\crypto.bat

Configuration avec l'interface graphique

On peut aussi configurer la règle R2 en utilisant l'interface graphique :

Démarrer> Panneau de configuration> Centre de sécurité> Pare-feu Windows.

Pour configurer le trafic entrant:

- Choisir l'onglet "Exceptions".
- Seuls les programmes/services utiles sont activés (par exemple « Partage de fichiers et d'imprimantes ») avec Etendue=130.223.2.2
- Si on désire se connecter à un lecteur réseau via crypto, le navigateur web doit être activé avec Etendue=130.223.2.2 (voir ci-dessous pour limiter l'étendue).
- Lorsqu'un nouveau programme de type serveur s'exécute la première fois, le pare-feu affiche un message d'alerte. On peut alors choisir de cliquer sur « Débloquer », puis on configure pour ce programme Etendue=130.223.2.2

Pour limiter à crypto l'étendue (adresse IP source permise) d'un programme ou service :

- Choisir l'onglet « Exceptions », puis le programme/service.
- Cliquer sur « Modifier... », puis « Modifier l'étendue... ».
- Activer « Liste personnalisée », puis entrer 130.223.2.2 (adresse de crypto.unil.ch). Cliquer sur OK.
- Si une liste de ports est affichée, on doit cliquer sur chaque port et répéter la procédure de modification de l'étendue.

PARE-FEU ZONEALARM

Ce logiciel se trouve à :

- http://www.zonealarm.fr/security/fr/anti-virus-spyware-free-download.htm
  Télécharger « Pare-feu ZoneAlarm élémentaire ».

Menu Firewall :

- Firewall> Main> Internet Zone Security=High.
- Firewall> Main> Trusted Zone Security=Medium.
- Firewall> Main> Advanced> Block Internet servers=enable.
- Firewall> Main> Advanced> Allow Outgoing DNS/DHCP in Internet/Trusted Zone on High setting=enable.
- Firewall> Zones: à mettre dans Trusted Zone seulement *le strict minimum* (le reste se retrouve par défaut dans Internet Zone) :
  - crypto.unil.ch
  - Le subnet 130.223.21.0/24 (pour l'accès aux serveurs de distribution de logiciel du Ci)
  - Le PC lui-même (seulement si on désire se connecter à un lecteur réseau via crypto)

Menu Program Control :

- Program Control> Main> Program Control=Medium.
- A la première exécution de chaque nouveau programme de type serveur ou client, on reçoit un popup auquel il faut activer « Remember this setting », puis cliquer sur « Allow ».
- Si on désire se connecter à un lecteur réseau via crypto, le navigateur web doit avoir en plus la permission « Server Trusted »= √.

Menu Alerts & Logs :

- Alert Events Shown=off.