# Installation d'un Barracuda

Installation

## Base

1. Connectez un câble réseau, un écran et un clavier directement sur le Barracuda
2. Connectez-vous avec l'utilisateur "admin" et le mot de passe "admin"
3. Configurez l'ensemble des paramètres réseaux
4. Arrêtez le système et débranchez les câbles VGA et clavier

## Mises à jour

1. Connectez-vous avec les mêmes identifiant sur l'interface web en HTTP sur le port 80 en anglais
2. Effectuez la procédure d'enregistrement de l'appareil auprès de Barracuda Networks
3. "BASIC"
   1. "Administration"
      1. Cliquez sur "Offline"
4. "ADVANCED"
   1. "Firmware Update"
      1. Mettez à jour le firmware "Latest General Release"
5. Ouvrez les notes de mises à jour du nouveau firmware afin qu'elles n'apparaissent plus
6. Vérifiez si de nouveaux firmware sont proposés suite à la mise à jour et installez-les si possible
7. "BASIC"
   1. "Administration"
      1. Cliquez sur "Online"
8. "ADVANCED"
   1. "Energize Updates"
      1. Mettez tout à jour

Configuration

## Configuration

*Seulement les paramètres différents des valeurs par défaut sont documentés, il est par conséquent nécessaire de contrôler dans chaque onglet les valeurs proposés par Barracuda sur la colonne de droite. La documentation a été effectuée à partir d'un modèle 300. Ceci représente une configuration de base sans quarantaine qui doit être ajustée selon les besoins au cas par cas…*

1. "BASIC"
   1. "Spam checking"
      1. Spam Scoring Limits
         1. Quarantine: Enable, level 2.5
         2. Tag: Disable
      2. Outbound Spam Scoring Limits
         1. Block: Enable, level 7
      3. Spam Tag Configuration
         1. Subject Tag: [SPAM]
      4. Intent Analysis
         1. Spam: Inbound Block, Outbound Off
         2. Adult/Dating: Inbound Block, Outbound Off
         3. Political Issues & Activist Groups: Inbound Block, Outbound Off
      5. Global Bayesian Analysis
         1. Submit Email To Barracuda Central: No
   2. "Virus Checking"
      1. Barracuda Real-Time Protection
         1. Barracuda Real-Time Protection: On - Do Not Sent Virus Variants
   3. "Quarantine"
      1. Inbound Quarantine Type
         1. Quarantine Type: Per-User
      2. Global Inbound Quarantine Configuration
         1. Quarantine Delivery Address: [quarantine@domaine.ch](mailto:quarantine@domaine.ch)
         2. Quarantine Subject Text: [QUAR]
      3. Per-User Quarantine Configuration
         1. Quarantine Reply-To Address: [noreply@domaine.ch](mailto:noreply@domaine.ch)
         2. Quarantine Host: barracuda.domain.ch
         3. Link Domains: No
         4. Notification Start Time: 15:30
      4. Outbound Quarantine
         1. Notification Address: [quarantine@domaine.ch](mailto:quarantine@domaine.ch)
   4. "IP Configuration"
      1. Destination Mail Server TCP/IP Configuration
         1. Server Name/IP: IP du serveur Exchange
         2. Valid Test Email Address: [quarantine@domaine.ch](mailto:quarantine@domaine.ch)
      2. DNS Configuration
         1. Primary DNS Server: DNS du FAI
         2. Secondary DNS Server: DNS de Google
      3. Trusted Forwarder Configuration
         1. Inscrivez les adresses IP des serveurs MX secondaires, ex pour Nettica :
            1. 216.154.198.171 - 255.255.255.255 - NETTICA MAIL BACKUP 1
            2. 216.154.198.172 - 255.255.255.255 - NETTICA MAIL BACKUP 2
      4. Domain Configuration
         1. Default Host Name: barracuda
         2. Default Domain: domaine.ch
         3. Accepted Email Recipient Domain(s): tous les domaines emails
   5. "Administration"
      1. Password Change
         1. Changez le mot de passe de l'appareil
      2. Email Notifications
         1. System Alerts Email Address: [alertes@bmcssi.ch](mailto:alertes@bmcssi.ch)
         2. System Contact Email Address: [alertes@bmcssi.ch](mailto:alertes@bmcssi.ch)
         3. Send SNMP/Email notifications: No
      3. Time
         1. Time Zone: Europe: Switzerland - Zurich
      4. Default Barracuda Locale
         1. Default Language and Encoding: Français (utf-8)
      5. Web Interface Settings
         1. Session Expiration Length: 60 minutes
   6. "Outbound"
      1. Relay Using Trusted IP/Range
         1. Inscrivez l'adresse du serveur Exchange ainsi que tous les éléments du réseau qui doivent envoyer des emails sans authentification (HP Management Agents, vCenter, SAN, UPS, BlackBerry Server, …)
2. "BLOCK/ACCEPT"
   1. "Rate Control"
      1. Rate Control Exemption IP/Range
         1. Inscrivez l'adresse du serveur Exchange
   2. "IP Filters"
      1. Allowed IP/Range
         1. Inscrivez l'adresse du serveur Exchange ainsi que tous les équipements devant envoyer des alertes importantes (HP Management Agents, vCenter, SAN, UPS, …)
   3. "Attachment Filters"
      1. Attachment File Type Filters
         1. Documents - Adobe PDF Off Off Enable
         2. Documents - MS-Access Off Off Enable
         3. Documents - MS-Excel Off Off Enable
         4. Documents - MS-Powerpoint Off Off Enable
         5. Documents - MS-Word Off Off Enable
         6. Executables - Windows Executables Quarantine Off Enable
         7. Executables - Windows Scripts Quarantine Off Enable
      2. Password Protected Archive Filtering
         1. Action for Password Protected Archives: Inbound Off, Outbound Off
3. "USERS"
   1. "User Features"
      1. Mail Client Plugins
         1. Allow Users To Download Outlook Add-In: Yes
      2. Default User Features
         1. Quarantine Enable/Disable: No
         2. Spam Scan Enable/Disable: No
         3. Notification Change: Yes
         4. Whitelist/Blacklist: Yes
   2. "Retention Policies"
      1. Age Based Retention
         1. Age Limit (Days): 30
4. "DOMAINS"
   1. "Domain Manager"
      1. Supprimez le domaine d'exemple
      2. Créez les différents domaines email nécessaires
5. "ADVANCED"
   1. "Email Protocol"
      1. SMTP Configuration
         1. Maximum Message Size: 50000000
      2. SMTP over TLS/SSL
         1. Enable SMTP over TLS/SSL: Yes
   2. "Secure Administration"
      1. Web Interface HTTPS/SSL Configuration
         1. Use HTTPS Links in Emails: Yes
      2. SSL Certificate Configuration
         1. Certificate Type: Private (Self-signed)
         2. Remplissez la section "Private (Self-signed)" et indiquez dans Common Name le nom du Barracuda (barracuda.domaine.ch)
         3. Sauvegardez les changements
         4. Pour utiliser un certificat validé, cliquez sur "Certificate Signing Request (CSR): Download" puis importez la clé privée crée par la CA
   3. "Bounce/NDR Settings"
      1. Spam NDR (Bounce) Configuration
         1. NDR on Block: Inbound Yes, Outbound Yes
      2. Quarantine NDR configuration (Outbound Only)
         1. NDR on Quarantine: Yes
      3. Bounce/NDR Language and Text
         1. Default Language: Français
   4. "Backup"
      1. Automated Backups
         1. Server Type: Off

## Configuration du domaine

1. A effectuer pour chaque domaine dans "DOMAINS", "Domain Manager", "Manage Domain"
2. "USERS"
   1. "LDAP Configuration"
      1. Exchange Accelerator/LDAP Verification: Yes
      2. LDAP Server: IP du contrôleur de domaine suivi du 2ème contrôleur de domaine (séparé par un espace)
      3. LDAP Server Type: Active Directory
      4. Bind DN (Username): [ldap@domaine.ch](mailto:ldap@domaine.ch) (à créer dans l'AD)
      5. Bind Password: Mot de passe du compte LDAP
      6. Valid Email (for testing): [quarantine@domaine.ch](mailto:quarantine@domaine.ch)
   2. "Valid Recipients"
      1. Use LDAP: Yes
3. "ADVANCED"
   1. "Outbound Footers"
      1. Ajoutez un texte de bas de page si nécessaire

## Configuration du réseau

1. Créez une zone DNS "barracuda.domaine.ch" sans mises à jour dynamique avec un hôte pointant sur le Barracuda en interne
2. Créez les entrées DNS avec un MX pointant sur le Barracuda et une 2ème pointant sur une passerelle de secours, ex :
   1. domaine.ch Mail (MX) 10 barracuda.domaine.ch
   2. domaine.ch Mail (MX) 20 mail1.mailhostingservice.com
   3. domaine.ch Text (TXT) "v=spf1 mx -all"
   4. barracuda.domaine.ch Host (A) IP WAN
3. Redirigez le trafic entrant sur le port 25 du Barracuda
4. Relayez le trafic du serveur Exchange sur l'adresse IP du Barracuda sans authentification
5. N'acceptez que les emails en provenance de l'IP du Barracuda sur le connecteur Internet

## Désactivation anti-spam Outlook / Serveur Exchange

1. Désactivez par GPO le système de courrier indésirable d'Outlook
   1. Office 2007
      1. User Configuration/Policies/Administrative Templates/Classic Administrative Templates (ADM)/Microsoft Office Outlook 2007/Tools | Options…/Preferences/Junk E-mail
         1. Hide Junk Mail UI : Enabled
         2. Junk E-mail protection level : Enabled, No Protection
   2. Office 2010
      1. User Configuration/Policies/Administrative Templates/Classic Administrative Templates (ADM)/Microsoft Outlook 2010/Outlook Options/Preferences/Junk E-mail
         1. Hide Junk Mail UI : Enabled
         2. Junk E-mail protection level : Enabled, No Protection
2. Ouvrez la console "Exchange Management Console"
   1. Allez dans "Organization Configuration", "Hub Transport", "Anti-spam"
      1. Désactivez tous les composants sauf "IP Allow List"

## Installation du client Outlook pour les listes blanches / noires

1. Installez les clients Outlook "Barracuda Spam & Virus Firewall Outlook Add-In" sur tous les PC disposant d'Outlook (téléchargement depuis la page de login du Barracuda)
   1. Les utilisateurs devront marquer somme courrier indésirable ou comme bon afin de les ajouter dans leur liste noir ou blanche personnelle (peut être gérée depuis l'interface web du Barracuda)

## Installation automatique du client Outlook par GPO

1. Récupérez les fichiers MSI depuis l'interface du Barracuda (outlook\_plugin\_v2.msi) ainsi que le kit de déploiement dans "USERS/User Features/Outlook Add-In Deployment Kit"
2. Créez sur le serveur de fichiers le dossier "D:\BarracudaOutlookAddin"
3. Partagez le dossier "D:\BarracudaOutlookAddin " en "BarracudaOutlookAddin$", désactivez la mise en cache, droits à Everyone FULL CONTROL
4. Sur le dossier "D:\BarracudaOutlookAddin", cassez l'héritage, enlevez les droits aux utilisateurs puis ajoutez le droit de lecture au groupe "Domain Computers"
5. Copiez les fichiers MSI du kit ainsi que de l'interface Barracuda dans le dossier "D:\BarracudaOutlookAddin"
6. Créez les GPO suivantes selon les rapports enregistrés :
   1. Computers - Barracuda Outlook Add-in Deployment

Divers

## Procédure de réinitialisation d'usine

1. Démarrez le Barracuda avec un écran et un clavier attaché
2. Au menu de démarrage, choisissez le mode "Recovery"
3. Choisissez l'option "Perform Full System Re-image"
4. Quitter le menu puis paramétrer à nouveau l'appareil