

Dans le cadre de **SECURIDAY 2009**

SECURINETS



Présente

Atelier : ASTARO



Formateurs: 1. RHIMI BILEL
2. BEN MOUSSA RAHMA
3. GUIZANI ZEINEB
4. MHADHBI IMENE
5. DAHI NOUHA
6. JOUINI NADIA

1. Introduction :

Pour protéger leurs réseaux, les organisations utilisent souvent différentes solutions telles que des systèmes de détection d'intrusions (IDS/IPS), des routeurs VPN et des pare-feu. Cela présente deux inconvénients majeurs : d'une part, l'administrateur doit effectuer une maintenance sur chacun des produits, mais en plus, rien ne garantit que ces multiples solutions aient été intégrées de manière à protéger intégralement notre périmètre réseau.

Astaro Security Gateway élimine complètement ce genre de désagréments en proposant une solution unique, simple à installer et à administrer, intégrant de multiples fonctionnalités pour la protection de votre réseau et de vos données.

Il intègre aussi de manière unifiée toutes les fonctionnalités de filtrage Web nécessaires à l'entreprise.

De plus, il permet de vous apporter une solution unique pour lutter contre toutes ces menaces, combinant des technologies de filtrage, de chiffrement et de signature.

Astaro Security Gateway : La sécurité unifiée

Sécurité Réseau	Protection Web	Protection Email
Pare-feu Stateful Inspection Détection d'intrusions Passerelle VPN	Protection antispyware Protection antivirus Filtrage de contenu Filtrage P2P	Protection antivirus Protection antispam Protection anti phishing Chiffrement & Signature

2. Présentation :

Notre atelier a pour objectif d'installer des outils qui permettent de mettre en place la solution de sécurisation Astaro Security Gateway afin d'être capables d'empêcher les attaques de se produire dans le réseau et ainsi lutter contre le botnet qui est un réseau de machines compromises à la disposition d'un individu malveillant lui permettant de transmettre des ordres à tout ou partie des machines du botnet et de les actionner à sa guise.

Il s'agit donc :

- D'installer le serveur Astaro Security Gateway (ASG V7)
- De configurer le serveur à partir du client Admin.
- De faire différentes attaques dans le réseau afin de voir l'efficacité de l'outil de sécurité ASG .

3. Outils utilisés :

Lors de cet atelier, on a utilisé Astaro Security Gateway (ASG V7) qui fonctionne comme un appareil virtuel dans tout produit de virtualisation de VMware.

Les appareils virtuels sont téléchargeables à partir de l'un des liens suivants :

<http://www.astaro.com/vmware>.

ftp://ftp.astaro.com/pub/Astaro_Virtual_Appliance/

http://download.astaro.com/Astaro_Virtual_Appliance/

4. Installation et Configuration :

La solution de sécurité Astaro Security Gateway intègre parfaitement l'ensemble des fonctionnalités proposées, grâce à une interface web utilisateur très intuitive.

Définition simple de politiques :

Permet d'appliquer en quelques clics des fonctions de filtre paquet, d'IPS ou de chiffrement à des éléments tels que adresses IP, réseaux, utilisateurs ou groupe d'utilisateurs

Tableaux de bord en temps réel :

Permet de visualiser l'état de la sécurité de notre réseau en temps réel.

Intégration simple des utilisateurs :

Permet de créer et appliquer des profils d'accès au web à des groupes d'utilisateurs existants, directement grâce à grâce aux annuaires tels que Active Directory, LDAP ou Radius...

Rapport granulaire concernant l'usage du Web :

Des données détaillées, simples et pertinentes sont fournies en temps réel sur l'usage fait du Web au sein de votre société. Une option permet de fournir automatiquement ces rapports par e-mail.

Installation simple :

Qu'il s'agisse du routage des e-mails par utilisateur ou par domaine, du filtrage antivirus et antispam ou de la gestion de clés ; toutes les configurations sont intuitives et extrêmement simples à installer.

Un self-service pour les utilisateurs :

Astaro offre dans cette nouvelle version une grande autonomie pour les utilisateurs finaux. Ainsi ils pourront gérer eux mêmes certaines installations et aussi la quarantaine - ce qui réduit considérablement les coûts et le temps d'administration.

Les étapes d'installation et de configuration se présentent comme suit :

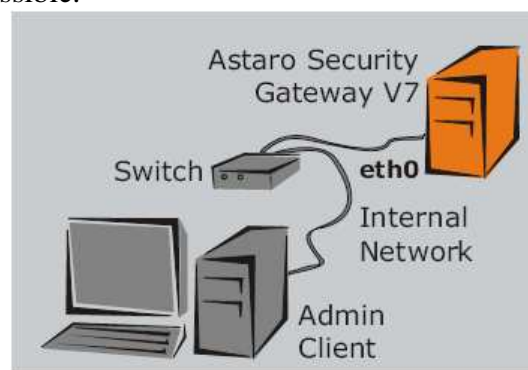
Tout d'abord, on doit avoir les caractéristiques suivantes au niveau de la machine serveur ASG et de la machine du client Admin :



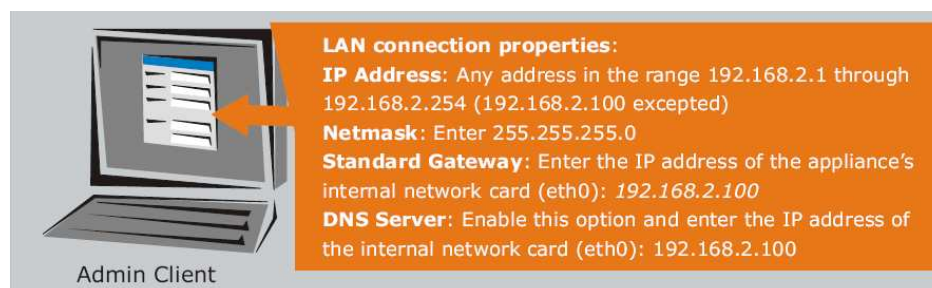
The screenshot shows the Astaro Security Gateway V7 requirements page. On the left, under 'ASG - Minimum Hardware Requirements', it lists: Pentium III (800 MHz) or compatible CPU, 512 MB RAM, 10 GB IDE or SCSI hard disk drive, and Bootable CD-ROM drive. On the right, under 'Client - Hard-/Software Requirements', it lists: 1 GHz and 512 MB RAM, Browser: Firefox recommended (with a URL) or Microsoft Internet Explorer 6 or 7, and WebAdmin is running at port 4444.

1. Installer l'outil ASG V7

Installer le logiciel ASG sur une machina à part. L'installation effacera complètement toutes les données sur le disque dur comprenant tous les programmes et le système d'exploitation. Après avoir redémarré le système de sécurité faire un ping sur l'adresse IP de l'interface eth0 pour s'assurer qu'elle est accessible.



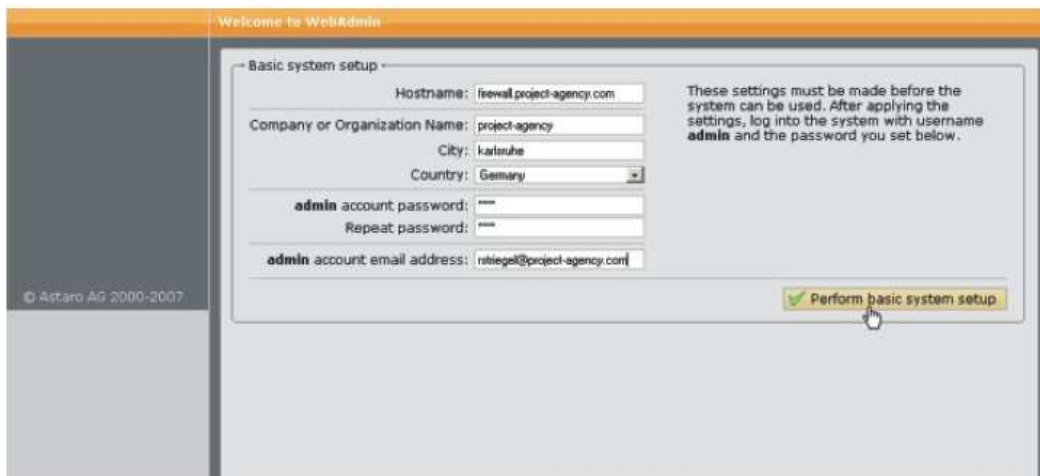
2. Lancer le browser et ouvrir l'interface graphique de l'utilisateur Admin (WebAdmin)



The screenshot shows the LAN connection properties configuration window on the Admin Client. The properties are: IP Address: Any address in the range 192.168.2.1 through 192.168.2.254 (192.168.2.100 excepted), Netmask: Enter 255.255.255.0, Standard Gateway: Enter the IP address of the appliance's internal network card (eth0): 192.168.2.100, and DNS Server: Enable this option and enter the IP address of the internal network card (eth0): 192.168.2.100.

Une fois le browser est correctement configuré, entrer l'adresse du système de sécurité (l'adresse IP interne configuré pour eth0) comme suit:
`https://IP Address:4444` (e.g., `https://192.168.2.100:4444`)

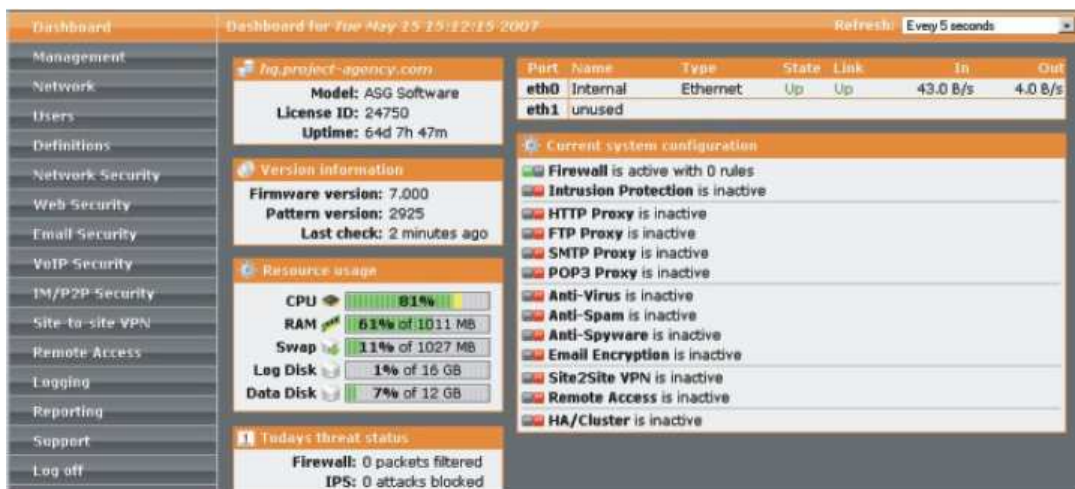
3. Écrire le contact d'administrateur et placer les mots de passe du système



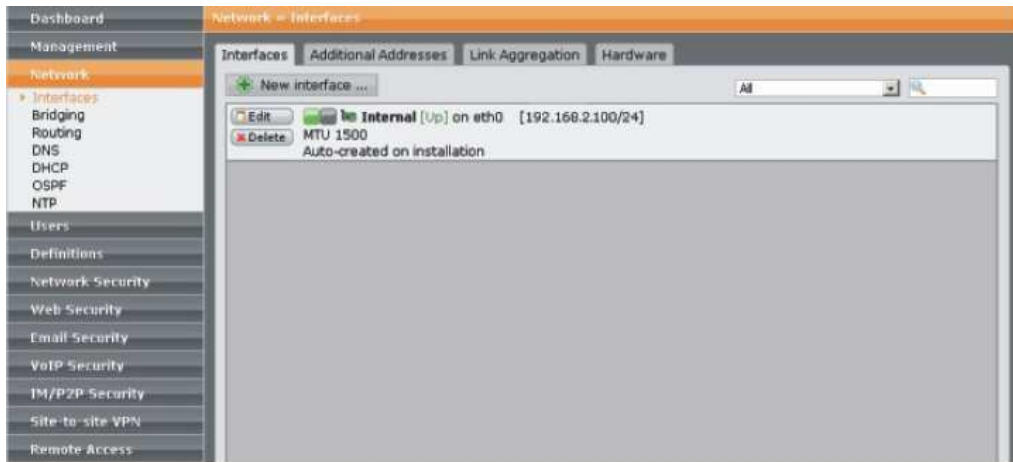
4. Procédure de connexion à l'interface graphique de l'utilisateur Admin (WebAdmin)



Ouvrir le tableau de bord



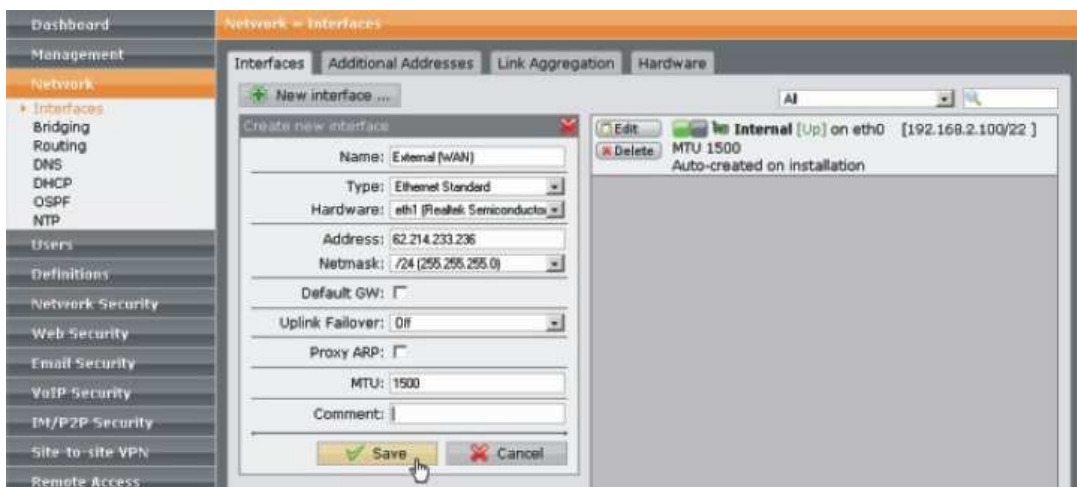
5. Contrôler l'interface du réseau interne (réseau local) (eth0)



6. Configurer le réseau local(LAN)



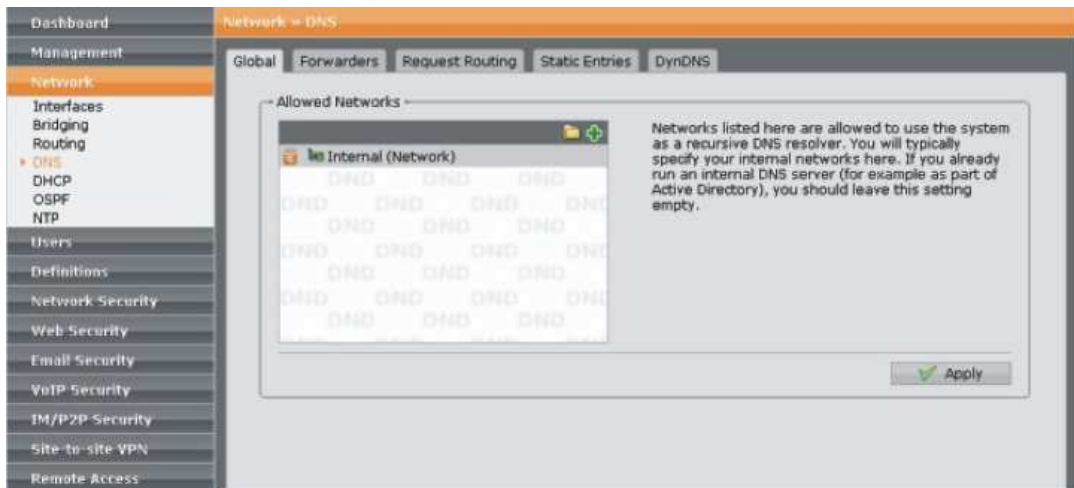
7. Configurer l'interface externe WAN (eth1)



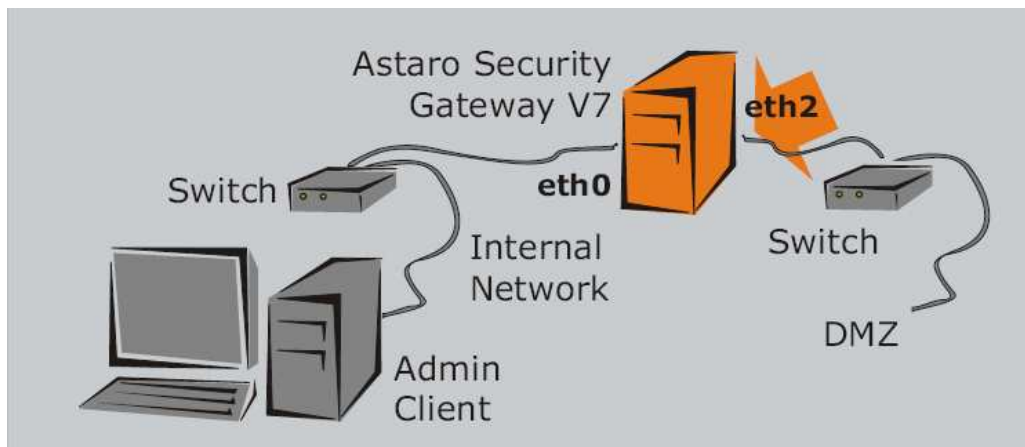
8. Définir les règles pour se connecter directement à l'internet sans proxy



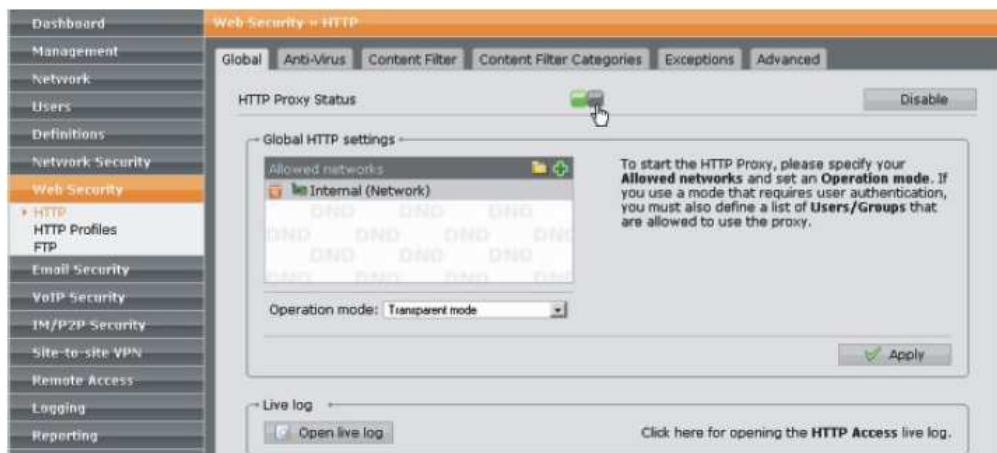
9. Configurer le proxy DNS



10. Connecter autres réseaux



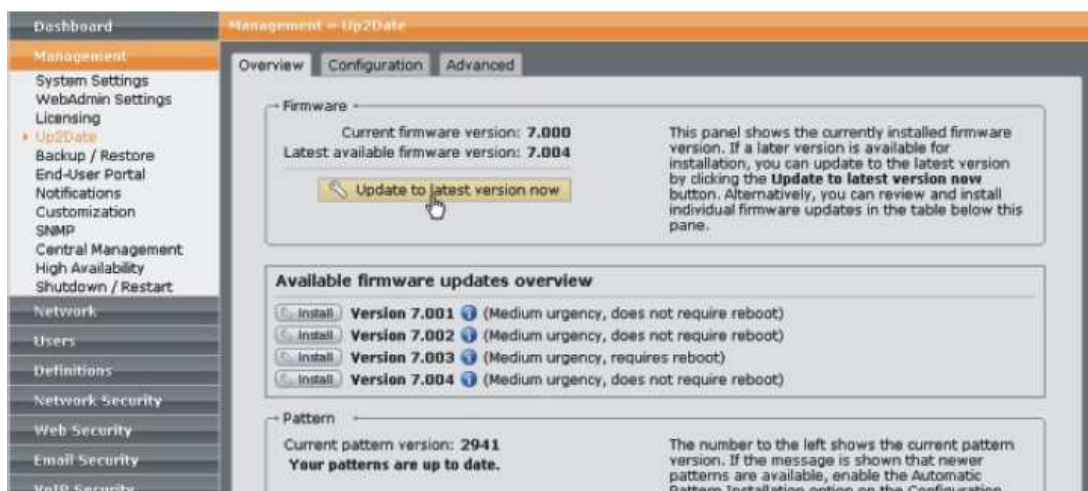
11. Configurer le proxy http (au niveau de la sécurité web)



12. Configurer le filtre des paquets



13. Installer les mises à jour du système et du scanneur de virus



5. Conclusion :

Lors de cet atelier nous nous avons installé et configuré l'outil de sécurité Astaro Security Gateway afin de rendre la sécurité du réseau plus robuste et pour lutter également contre les botnets et ceci grâce à la compatibilité de la solution ASG avec tout type de réseaux (puisqu'elle est disponible sous forme logicielle, matérielle (appliance) ou machine virtuelle).