Elastix SIP Firewall

Manuel de l'utilisateur

Droit d'auteur.

Droits sur la propriété.

Clause de non responsabilité.

Les informations contenues dans ce document sont sujettes à des modifications sans préavis et ne doivent pas être interprétées comme un engagement de la part de http://www.elastix.org, et n'assume aucune responsabilité ou garantie sur d'éventuelles erreurs. Dans ce document, Il peut apparaître des erreurs et décline toute garantie de qualité marchande ou d'adéquation à un usage particulier.

1.1. A propos de ce Manuel

Ce manuel décrit l'application du produit Elastix® et explique comment il fonctionne et comment utiliser les principales fonctions. Il sert ici comme un moyen de décrire l'interface utilisateur et la façon de l'utiliser pour accomplir des tâches communes. Ce manuel décrit également les hypothèses fondamentales, et les utilisateurs accomplissent ce modèle de données fondamentale.

1.1. Conventions du Document

Dans ce manuel, certains mots sont représentés sous différents caractères, types, tailles et poids. Cette présentation est systématique; différents mots sont représentés dans le même style pour indiquer leur appartenance à une catégorie spécifique. En outre, le présent document possède différentes stratégies pour attirer l'attention de l'utilisateur à certains éléments d'informations. Afin de mettre un accent sur le degré d'informations de votre système, ces éléments sont marqués comme une remarque, une astuce, une importance, une attention ou un avertissement.

Icon	Purpose
	**Notes**
	**Trucs et Astuces**
	**Important**
	**Prudence**
	**Attention**

- Les caractères **gras** indiquent le nom des éléments de menu, les options, les boîtes de dialogue, les fenêtres et les fonctions.
- La couleur bleu soulignée est utilisé pour indiquer une référence croisée et un hyperlien.
- La numérotation de paragraphe est utilisé pour indiquer quelle sont les tâches à effectuer. Un texte seul dans le paragraphe sans numérotation représente une fonction quelconque.
- La police de caractère « Courier » indique une séquence de commande, un type de fichier, une URL, un répertoire ou nom de fichier par exemple: http://www.elastix.org

1.2. Informations sur le support

Tous les efforts ont été faits pour assurer l'exactitude de ce document. Si vous avez des commentaires, des questions ou encore des idées concernant ce document, contactez: sales@elastix.com

Table des matières

1. Introduction

1.1 Aperçu

Ce manuel décrit les étapes impliquées dans la mise en place de l'Appliance pare-feu SIP Elastix®. Elastix® SIP Firewall est un boitier pour la VoIP incluant une solution de prévention des menaces dédiée à protéger le protocole SIP pour des IPBX / Téléphones / passerelle IP Telecom / déploiements de périphériques mobiles. L'appareil exécute le *Deep Packet Inspection* en temps réel sur le trafic SIP pour identifier les vecteurs d'attaque VoIP et empêche les menaces visant les appareils utilisant le protocole SIP. L'appareil a été créé pour s'intégrer de manière transparente avec l'infrastructure réseau existante et réduit la complexité du déploiement.
Le jeu de fonctionnalités de l'appareil comprend :

- Analyses des paquets SIP utilisant le moteur *Deep Packet Inspection* temps réel.
- La détection des anomalies de protocole SIP avec personnalisation des paramètres de détection.
- Détection et Prévention suivant les catégories d'attaques SIP.
    - Reconnaissance des attaques (SIP Devices Fingerprinting, Recherche d'utilisateurs, Tentatives de casses de mot de passe)
    - Attaques par Dos / DDos
    - Attaques basées sur le Cross-Site Scripting.
    - Attaques par débordement de Buffer
    - Attaques basées sur les anomalies SIP.
    - Vulnérabilités fournisseurs tiers.
    - Détection de fraude et prévention.
    - Protection contre les spams VoIP & War Dialing
- Réponse d'attaque, comprend l'option de rejet discret des paquets SIP malveillants, pour empêcher les attaques continues.
- Un service de mise à jour de la liste noire en cas de menaces sur VoIP, IPBX SIP ou Passerelle SIP
- Configuration possible de la Liste Noire, Blanche, et règles Firewall.
- Support de la Géolocalisation pour le blocage.
- Apporte la possibilité de sécuriser les IPBX contre leurs vulnérabilités.
- Fonctionne sur la couche Niveau II, donc transparent pour les infrastructures existantes. Aucune modification requise pour ajouter le matériel sur un réseau existant.
- Gestion du boitier accessible en Web et SSL qui permettra l'accès aux paramètres du boitier n'importe où depuis le Cloud.
- Possibilité de restreindre la gestion du boitier à un réseau IP spécifique.
- Fournit à un serveur Syslog distant, le journal d'évènements sur le statut du système et de la sécurité.
- Fournit un débit SIP jusqu'à environ 10Mb/s.

- Supporte la souscription de mise à jour de signature et le mécanisme de mise à jour automatique des signatures.
- Le boitier est prévu pour fonctionner avec la configuration par défaut, avec juste une mise sous tension de l'appareil. Aucune intervention de l'administrateur n'est nécessaire pour le faire fonctionner avec la configuration par défaut.
- Alimentation via une prise USB
- Supporte en option, le stockage du journal d'événements sur une clef USB ou autres dispositifs de stockage USB. (*Formatage ext3*)

Spécifications Techniques

Mode de fonctionnement	Firewall transparent avec le moteur SIP Deep Packet.
SIP Intrusion/Prévention	Supporte plus de 400 types de signatures d'attaques SIP.
Débit SIP	Environ 10Mb/s
Nombre de comm. simultanées	Jusqu'à 50 communications simultanées.
Journal d'événements	Console locale ou Syslog distant.
Gestion du boitier	Web GUI via Https & SSH CLI
Matériel	MIPS à base de processeur 32bits simple cœur cadencé à 300MHz.
Stockage principal	Mémoire Flash de 16 Mo
RAM	Mémoire de 64Mo
Stockage secondaire	Clef ou autres appareils de stockages USB (En Option)
Interfaces	Deux interfaces Fast Ethernet.

1.1.1. LEDs de notifications (Sur la face avant de Firewall SIP)

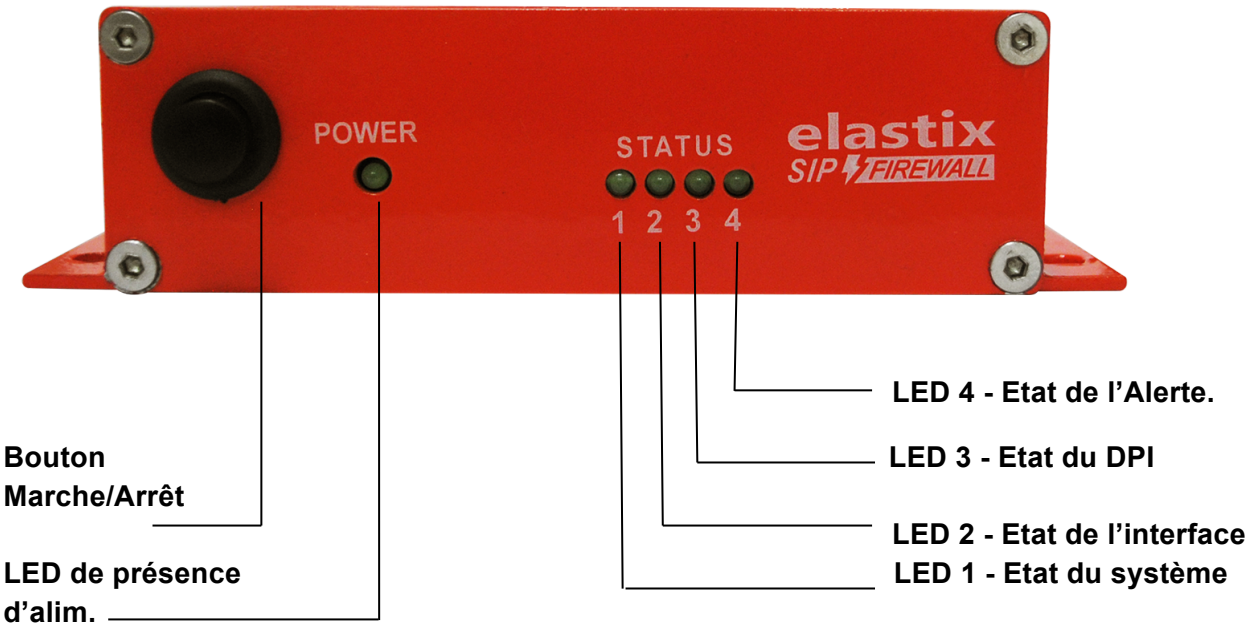

Figure 1: Etats des LEDs en face avant.

Le package du Firewall SIP inclue:

- 1 Boitier Firewall SIP
- 1 Adaptateur secteur USB
- 1 Câble série pour la console
- 2 Câbles Ethernet

1.1.2. Firewall SIP vue arrière:

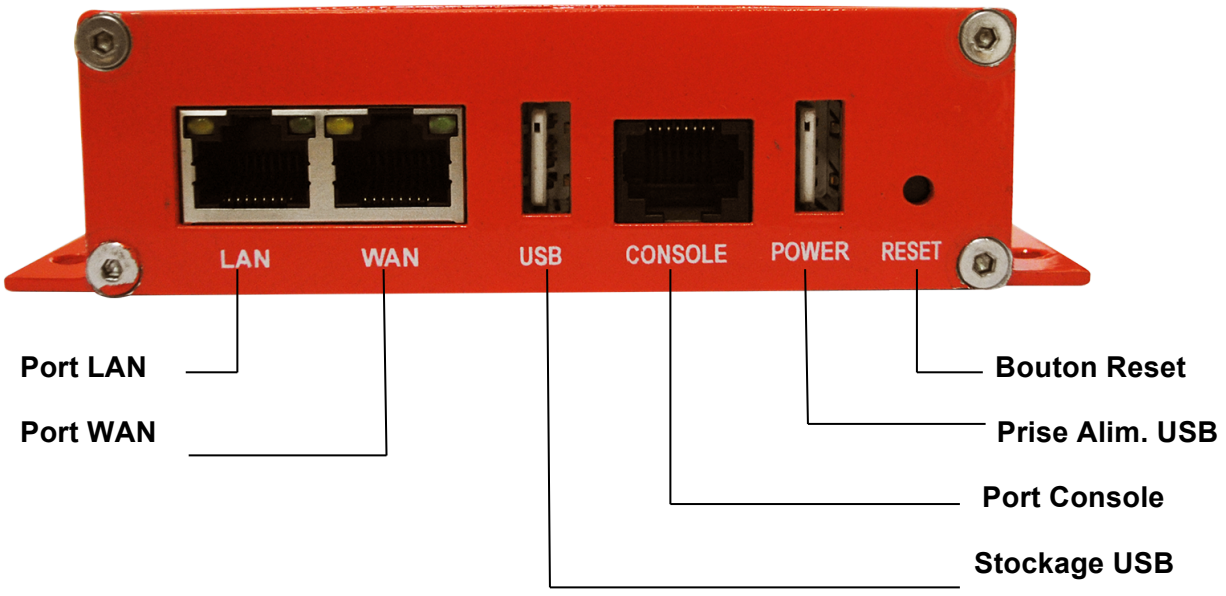

Figure 2: Firewall SIP Vue Arrière

1.1.3. Firewall SIP - Remarques à propos du déploiement.

Le Firewall SIP a été conçu pour protéger les IPBX ou Passerelles basés sur le protocole SIP contre des attaques ou anomalies SIP provenant réseaux. Par conséquent il est recommandé de déployer the pare-feu SIP en même temps que le déploiement de l'IPBX ou Passerelle, comme indiqué dans les scénarios ci-dessous, en fonction de ce qui est applicable dans la configuration de l'utilisateur.

Déploiement - Scenario 1

Figure 1: Scenario 1

Certains IPBX ou passerelles peuvent avoir une interface LAN dédiée exclusivement pour la gestion autre que l'interface de données (également nommée WAN/Public). Dans ce cas, le port LAN du pare-feu SIP devra être connecté sur l'interface de données (Interface WAN/Public).

Déploiement - Scenario 2

Dans le cas d'un IPBX déployé dans un environnement LAN, le paramétrage suivant est recommandé car il contribuera à se protéger des menaces aussi bien côté Réseau Privé que côté Réseau Public/Cloud en traversant le Firewall non SIP existant de l'entreprise.

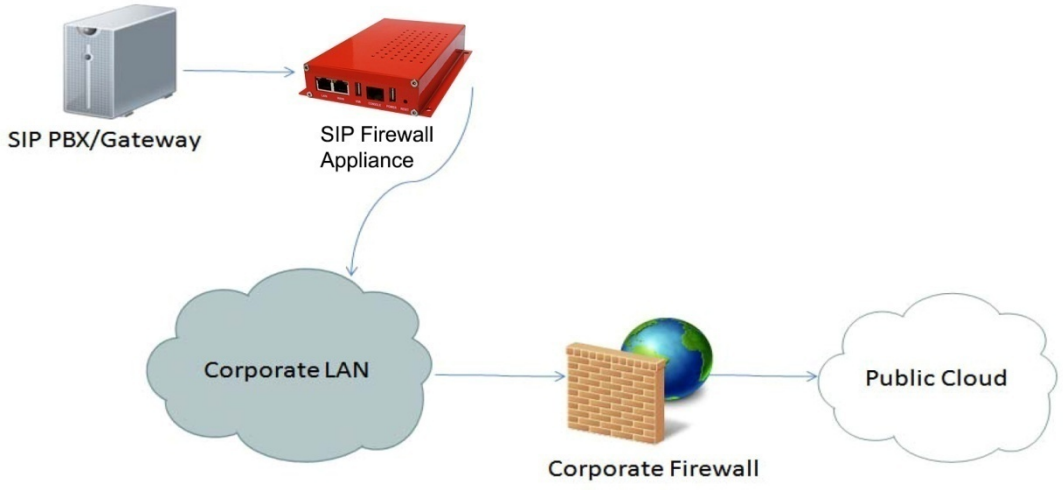

Figure 2: Scenario 2

Déploiement - Scenario 3

Dans le cas de plusieurs IPBX ou passerelles VoIP déployés dans un environnement LAN, le paramétrage suivant est recommandé car il contribuera à se protéger des menaces aussi bien côté Réseau Privé que côté Réseau Public/Cloud en traversant le Firewall non SIP existant de l'entreprise.

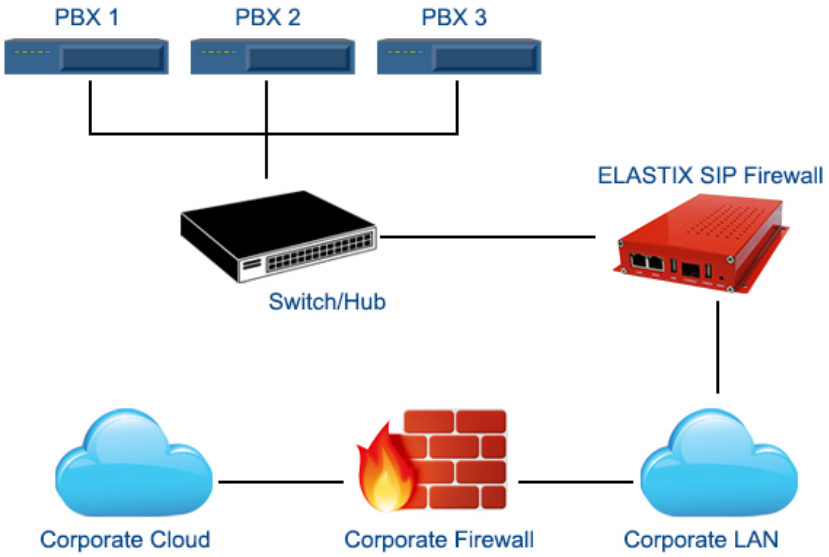

Figure 3: Scenario 3

2. Configuration initiale & Paramétrage

1. Déballage des éléments de la boite.
2. Vérifier que vous avez tous les éléments listés dans le contenu de la boite.
3. Connecter le port WAN du Firewall SIP au réseau non sécurisé ou public.
4. Connecter le port LAN du Firewall SIP à l'IPBX ou à la passerelle VoIP.
5. Connecter le boitier à la prise d'alimentation en utilisant le câble USB.
6. Le boitier devrait prendre environ une minute lors du boot et ensuite il sera entièrement fonctionnel rien qu'avec la configuration par défaut.

Certains IPBX ou passerelles peuvent avoir une interface LAN dédiée exclusivement pour la gestion autre que l'interface de données (également nommée WAN/Public). Dans ce cas, le port LAN du pare-feu SIP devra être connecté sur l'interface de données (Interface WAN/Public).

2.1 Configuration par Défaut.

Le boitier fonctionne comme un pont firewall transparent avec le Deep Packet Inspection validé sur le trafic SIP. Par défaut, le boitier a été configuré avec l'adresse IP statique suivante : 10.0.0.1/24

Le boitier a été conçu pour être entièrement fonctionnel avec la configuration par défaut. Par contre, si l'utilisateur a besoin de personnaliser la configuration du boitier et la politique du DPI, il peut le faire via l'accès à l'interface WebUI.

Le boitier dispose d'une interface d'accès en ligne de commandes via SSH, qui autorisera la configuration des paramètres basiques et d'avoir une vision sur le statut du boitier.

Accès à la Gestion	Compte et mot de passe
WebUI	admin/admin
SSH CLI	admin/stmadmin
IP Vlan Gestion	192.168.100.1/255.255.255.0
IP du boitier (défaut)	10.0.0.1/255.255.255.0

2.2. Accès au WebUI

L'utilisateur peut se connecter au boitier via le Vlan Gestion pour accéder au WebUI dès la configuration initiale. Le Vlan Gestion configuré sur le boitier est accessible via les ports LAN ou WAN et lui ait assigné l'adresse IP suivante : 192.168.100.1/24
Utiliser la procédure ci-dessous pour accéder au WebUI,

1. Connecter le port LAN du Firewall SIP a un PC.
2. Affecter l'adresse IP 192.168.100.2/24 au PC.

Maintenant vous pouvez accéder au boitier depuis votre navigateur Web en utilisant l'URL https://<192.168.100.1>
Configurer l'adresse IP du boitier Firewall SIP depuis la page "Device Settings" en conformité avec votre réseau local. Vérifier la configuration de l'adresse IP de votre boitier sur la page « Dashboard ». Une fois que l'utilisateur a réussi à affecter son adresse IP sur le boitier, Il pourra y accéder en utilisant sa nouvelle adresse.

Maintenant vous pouvez déconnecter le PC et connecter le port LAN à l'IPBX ou réseau d'IPBX que vous aurez besoin de protéger.

Le WebUI a été rendu accessible uniquement via HTTPS. Il est recommandé d'utiliser Mozilla FireFox pour accéder au WebUI.

L'interface utilisateur permet à l'administrateur de configurer l'adresse IP du Vlan Gestion. Dans le cas où l'utilisateur changerait l'adresse IP du Vlan IP Gestion, il aura besoin d'affecter une adresse correspondant au réseau de son PC pour y accéder ultérieurement.
Au lancement du WebUI du Firewall SIP, l'application Web vous demandera de vous authentifier avec le compte administrateur.

Une alternative, l'utilisateur peut accéder au boitier par l'adresse IP statique 10.0.0.1 et configurer les paramètres réseau durant la première installation. Connecter le PC au port LAN du Firewall SIP et affecter l'adresse IP 10.0.0.100/24 au PC. Maintenant vous pouvez accéder au boitier depuis votre navigateur Web à l'URL https://<10.0.0.1>

Si le boitier n'est pas accessible après avoir rentré les paramètres réseau, essayer de rebooter le boitier et vérifier le tableau de bord du firewall en y accédant via le Vlan Gestion.

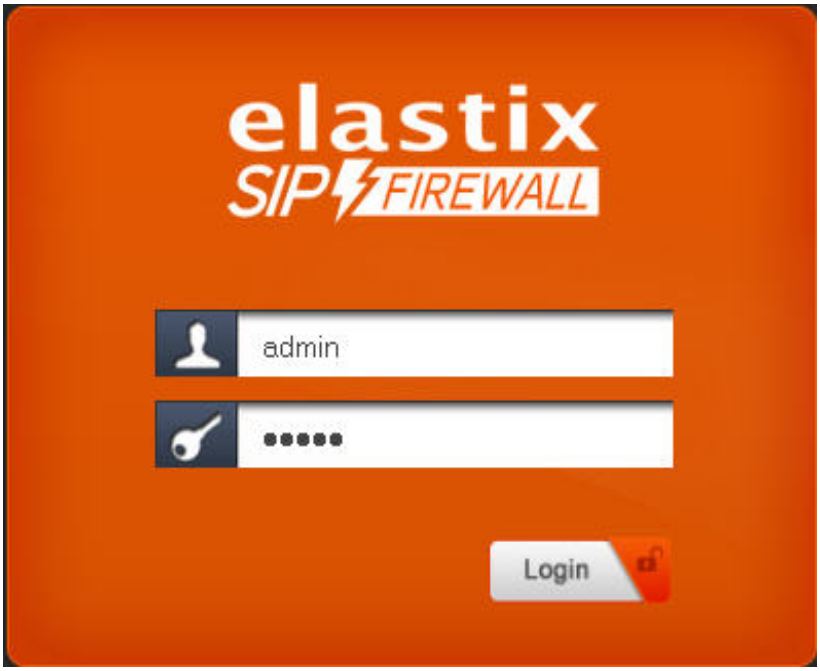

Figure 4: Page d'authentification

La session d'authentification a été créée avec un temps limité, par conséquent, si l'utilisateur n'est pas authentifié dans les 30 secondes, il sera redirigé vers une page d'informations. L'utilisateur peut cliquer sur l'hyperlien nommé 'login' qui apparait dans la page d'informations, et vous affichera la page d'authentification une nouvelle fois.

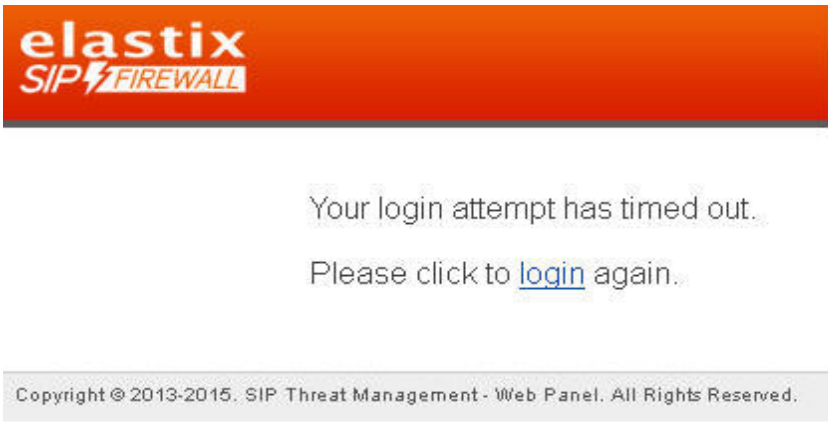

Figure 5: Message Temps dépassé

Si quelqu'un est déjà connecté à une session WebUI du Firewall SIP, une invitation à se connecter ultérieurement affichera les détails de la précédente session comme illustré ci-dessous, et demandera à l'utilisateur d'ignorer la session précédente et de continuer ou d'ignorer la tentative de connexion.

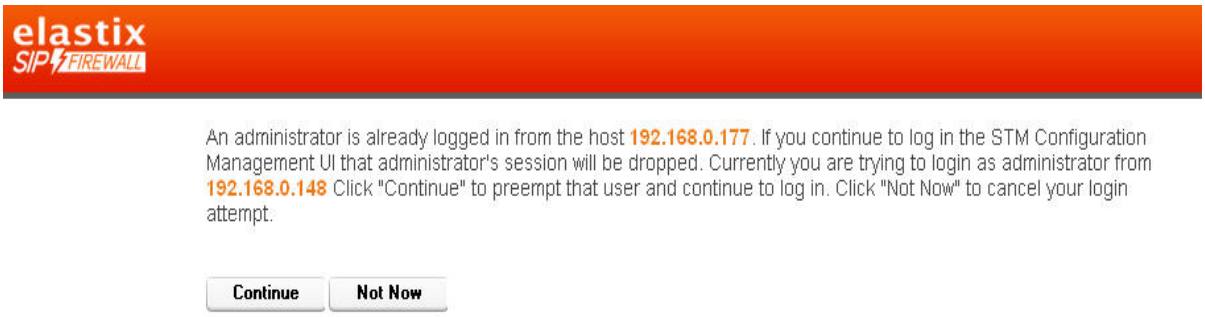

Figure 6: Sélection de la tentative de connexion

2.3 Expiration de la session WebUI

Après s'être authentifié sur le WebUI, s'il n'y a aucune activité durant une période limitée de la session WebUI (Par défaut, la session WebUI étant limitée à 900 secondes), alors la session se fermera automatiquement et le navigateur vous redirigera à nouveau sur la page d'authentification.

2.4 Configuration du WebUI

Pour modifier les paramètres de l'interface utilisateur (WebUI), cliquer sur l'icône settings qui apparait en haut à droite (en dessous du bouton « Apply Changes »). La boite de dialogue « Web Settings » s'affichera dans le navigateur web et permettra à l'administrateur de configurer la durée de la session du WebUI ainsi que le mot de passe. Pour le configurer, l'utilisateur devra saisir le mot de passe administrateur précédemment défini.

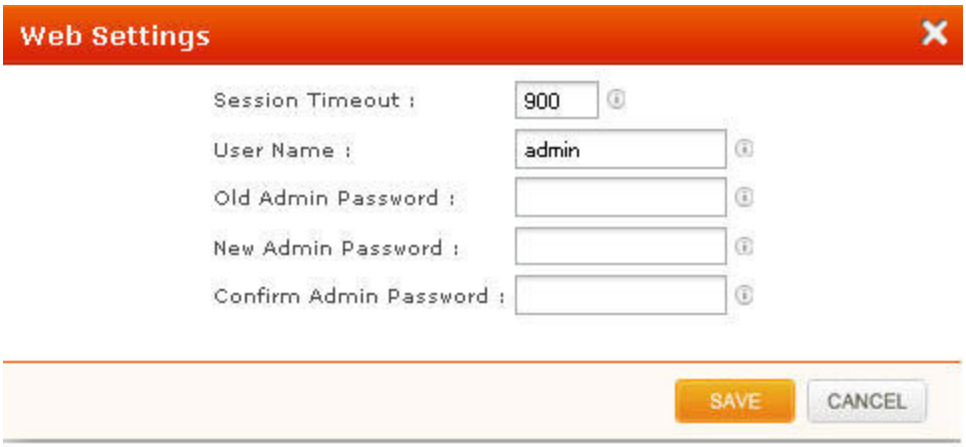

Figure 7: Configuration du WebUI

2.5 Tableau de bord

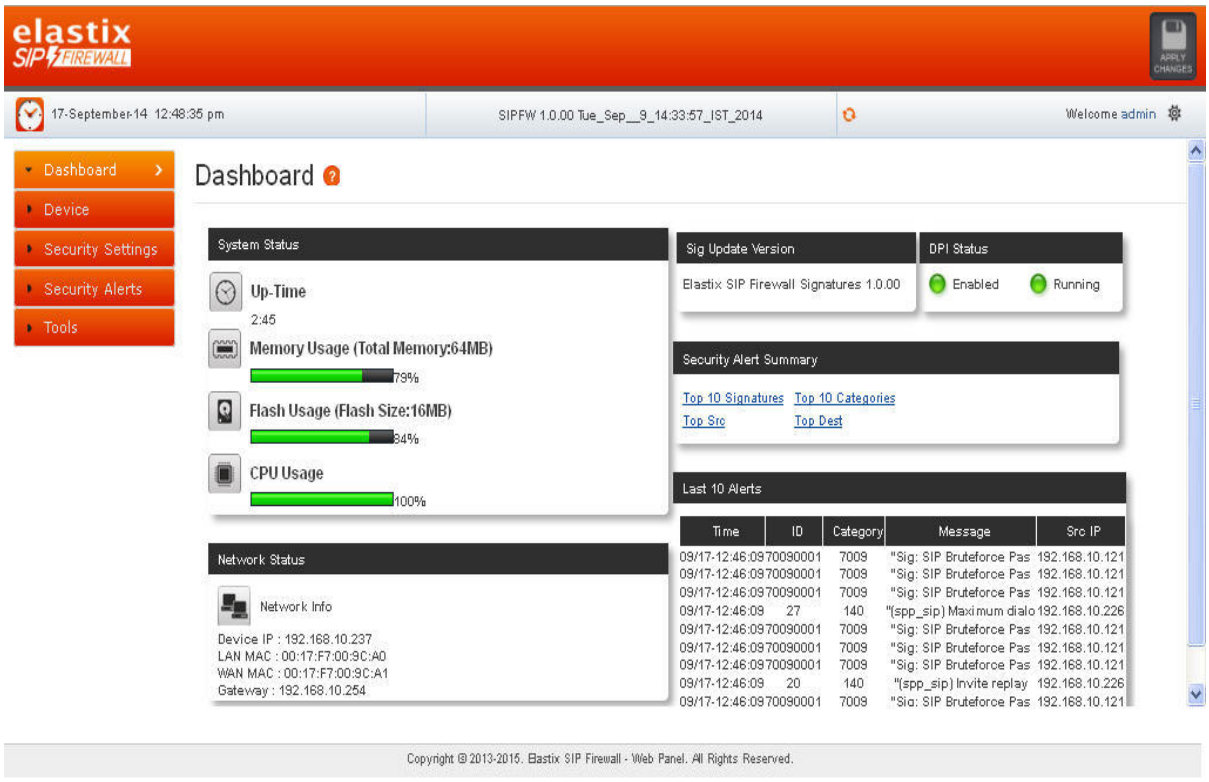

Figure 8: Tableau de bord

Une fois authentifié sur le WebUI du Firewall SIP, le tableau de bord sera affiché.

L'utilisateur peut consulter la page du tableau de bord depuis n'importe quelle page de configuration dans le WebUI du Firewall SIP, en cliquant sur l'icône du produit qui apparait en haut à gauche de la fenêtre.

Le bandeau d'état qui apparaît sous le bandeau supérieur en entête, affiche l'heure de l'appareil, la version du firmware du Firewall SIP, l'icône de rafraîchissement de la page et enfin l'icône de réglage.

En cliquant sur le bouton de rafraîchissement de la page, le contenu de la page courante dans la zone principale sera rafraîchi.

En cliquant sur l'icône de réglage, cela affiche un menu contextuel contenant les options suivantes : Paramétrage de l'interface utilisateur Web et Déconnexion.

Le cadre « System Status » montre le temps de fonctionnement du boitier, l'utilisation de la mémoire, le taux d'utilisation de la mémoire Flash et le taux d'utilisation du processeur.
Le cadre « Sig Update Version » affiche la version des signatures du Firewall et l'état de la libération.
Le cadre « Network Status » affiche l'adresse IP, l'adresse MAC LAN, l'adresse MAC WAN et la passerelle du boitier.
Le cadre « Security Alert Summary » affiche des hyperliens pour visualiser le Top 10 des signatures concernées, le Top 10 des Catégories concernées, Top des adresses IP attaquantes & Top 10 des destinations cibles.

3. Configuration du boitier.

Les pages de configurations du WebUI ont été créées pour être ludique et simple à paramétrer.

Toutes les pages de configurations ont été réalisées pour fonctionner en un modèle à deux étapes de validation.


La validation en deux étapes n'est pas applicable au paramétrage de l'heure et pour les paramètres de mise à jour des signatures. Dans ces paramètres, les changements seront appliqués en cliquant sur « Apply » dans la zone de contenu de l'éditeur de configuration.

Important. Quand l'administrateur change les paramètres dans les pages de configurations et clique sur le bouton « Save », les paramètres seront sauvegardés temporairement dans une zone tampon dans le boitier. Durant la sauvegarde des changements configurations, le bouton 'Apply Changes' apparait en haut à droite sera alors activé et le bouton 'Ignore Changes' devrait apparaitre à côté.

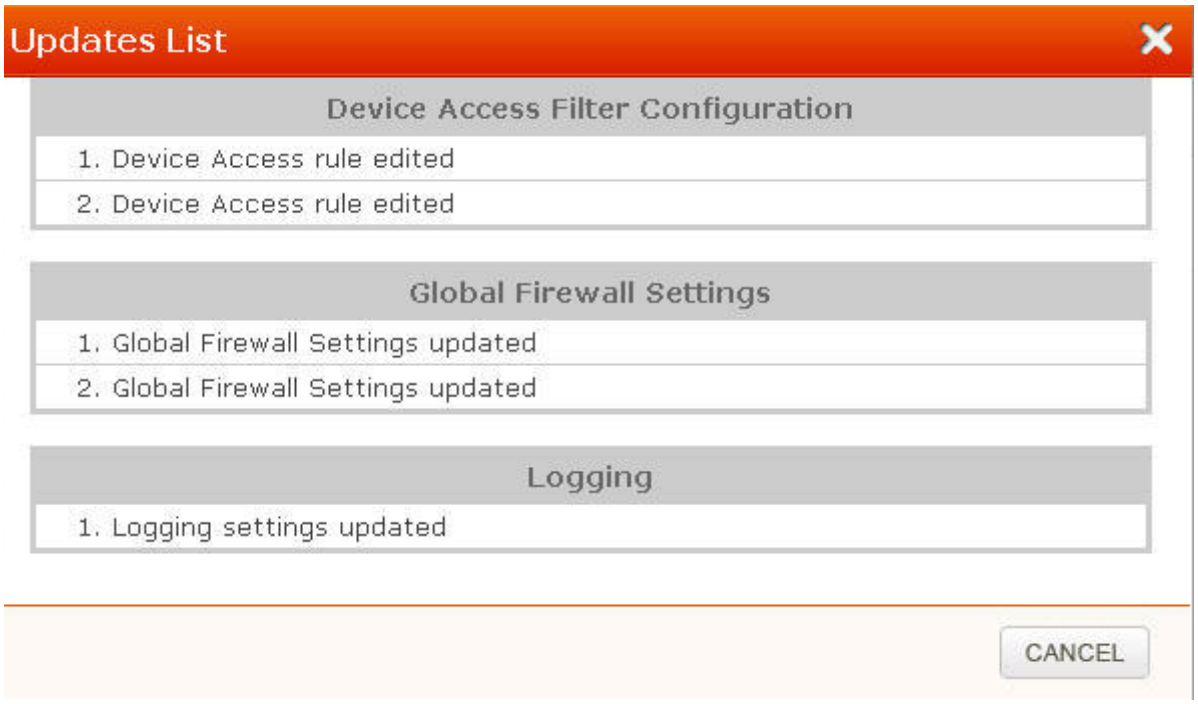

Figure 9: Configuration du boitier

Le nombre de changements de configurations apparaitra immédiatement à gauche du bouton 'Apply Changes'. Pour visualiser ces changements, l'utilisateur peut cliquer sur l'icône du nombre de changements qui les affichera sous forme de liste dans une fenêtre.

L'utilisateur peut appliquer les changements de configurations du boitier en cliquant sur le bouton « Apply Changes ». Dès le clic sur le bouton « Apply Changes », les changements de configurations seront appliqués au système et la configuration mise à jour restera en permanence dans votre boitier.
Dans le cas où l'utilisateur souhaite abandonner les modifications apportées à la configuration, il peut cliquer sur le bouton « Ignore Changes ». En cliquant sur le bouton « Ignore Changes », les changements de configurations stockés temporairement dans la zone mémoire tampon seront ignorés.

Pour appliquer les changements de configurations, le bouton 'Ignore Changes' s'affichera et il ne pourra pas y avoir de choix d'ignorer les changements de configurations. Le bouton 'Ignore Changes' sera désactivé seulement lorsqu'il y aura des changements de configurations en attente qui auront besoin d'être appliqués encore dans le boitier.

Si l'administrateur essaye de paramétrer un élément de configuration avec une valeur inappropriée, un icône tooltip apparait alors à côté de chaque élément de configurations et apportera les détails sur cette erreur.

En cliquant sur l'icône en forme de point d'interrogation qui apparait à côté du titre de la configuration sélectionnée, l'aide affichée correspondra à celle de la page de configuration courante.

3.1. Paramètres Généraux.

La page des paramètres généraux permettra la configuration des paramètres du host et du réseau du boitier Firewall SIP. Le boitier qui a été conçu pour travailler en mode pont et peut soit choisir de travailler avec une adresse IP statique, ou de travailler avec une adresse IP dynamique délivrée via un serveur DHCP.

La page permet également d'activer ou désactiver la connexion SSH sur le boitier. L'option 'Allow ICMP' devrait configurer le boitier pour qu'il réponde ou non aux messages ICMP ping envoyés au Firewall SIP.

Par défaut, l'accès SSH et le protocole ICMP, messages ping sont validés sur le boitier Firewall SIP.

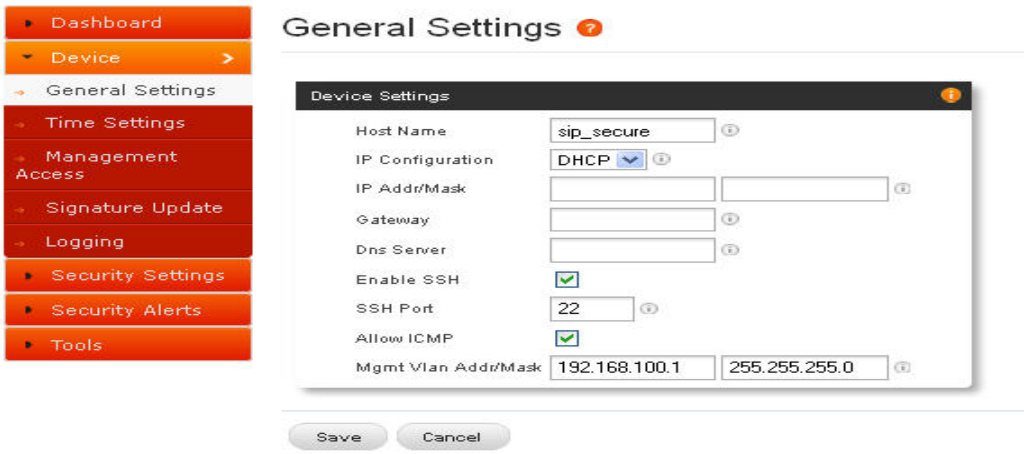

Figure 10: General Settings

3.2. Paramétrage Date / Heure

L'administrateur peut choisir de définir manuellement le réglage de l'heure sur le boitier ou de le configurer pour synchroniser l'heure venant d'un serveur NTP. Un paramétrage de l'heure et du fuseau horaire devra être correctement configuré pour un bon horodatage des logs de manière à bien afficher les alertes de sécurité SIP générées par le boitier.

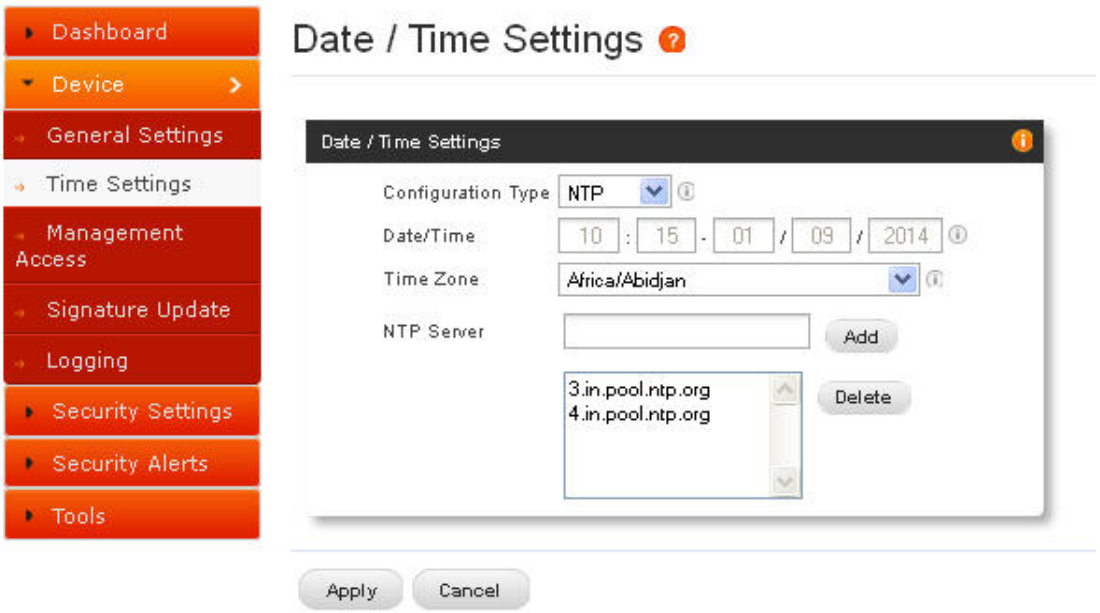

Figure 11: Paramétrage date/heure

3.3. Gestion des accès

L'accès à la gestion du boitier Firewall SIP (Accès SSH CLI / WebUI) peut être limitée avec des filtres d'accès à la gestion. Par défaut, l'accès a été autorisé globalement à toutes les adresses IP et pour la configuration du réseau Vlan Gestion du boitier. L'administrateur peut remplacer ces paramètres.

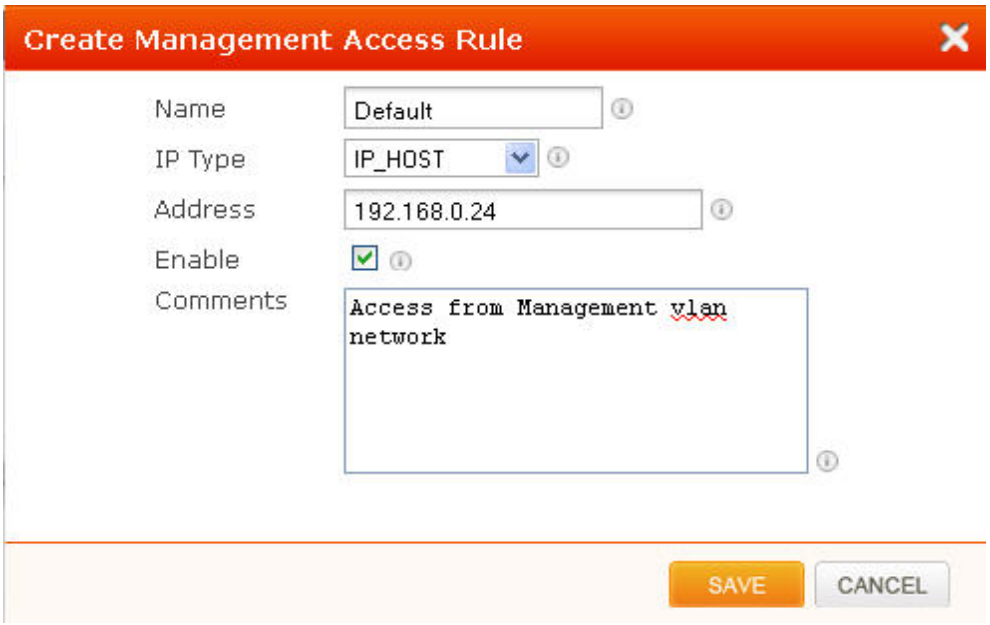

Figure 12: Création d'une règle de gestion d'accès.

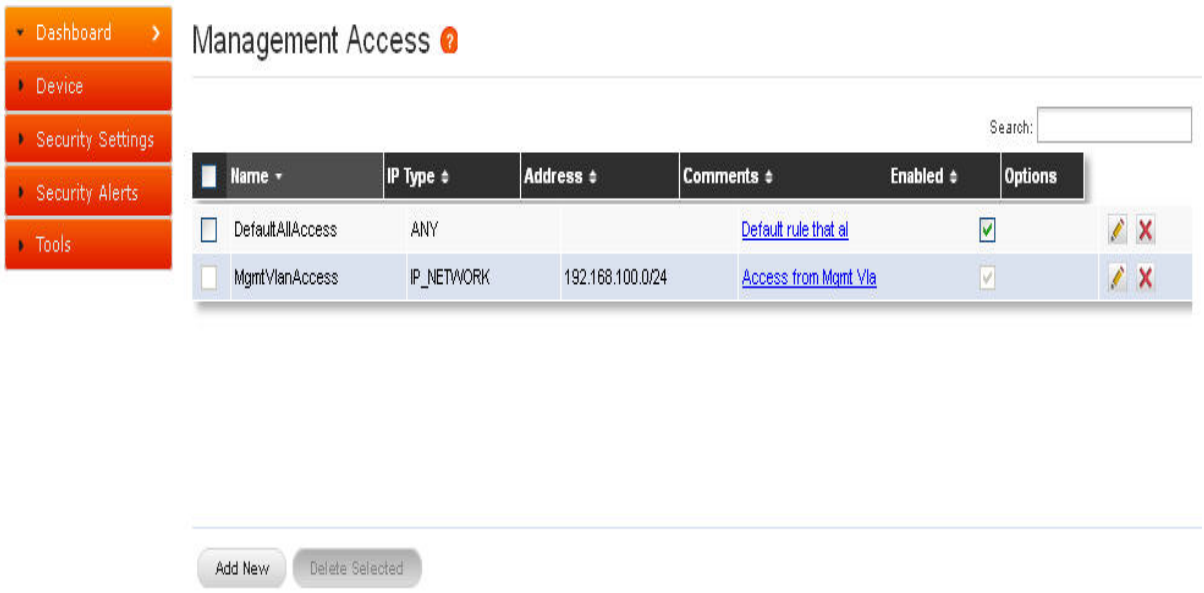

Figure 13: Gestion d'accès

L'administrateur aura besoin de configurer l'adresse IP ou le réseau IP, ou encore la plage d'adresses IP qui aura accès au boitier et devra être autorisé dans les règles de filtrage d'accès à la gestion. L'IP de type 'ANY' indique le réseau global (Tout réseau, Toute adresse IP).

L'option de recherche dans la gestion de table de filtrage d'accès aidera à les visualiser sélectivement dont les valeurs correspondent aux critères de recherche Nom / adresse.

3.4. Mise à jour des signatures.

Pour activer la mise à jour automatique des signatures, cochez la case « Enable update » sur le boitier et configurer le calendrier de mises à jour des signatures. La clé de souscription valide et une URL de mise à jour des signatures correctes doivent être configurées pour que cette mise à jour se produise.
Pour mettre à jour les signatures de l'appareil instantanément, cliquez sur le bouton «Update Signatures now ».

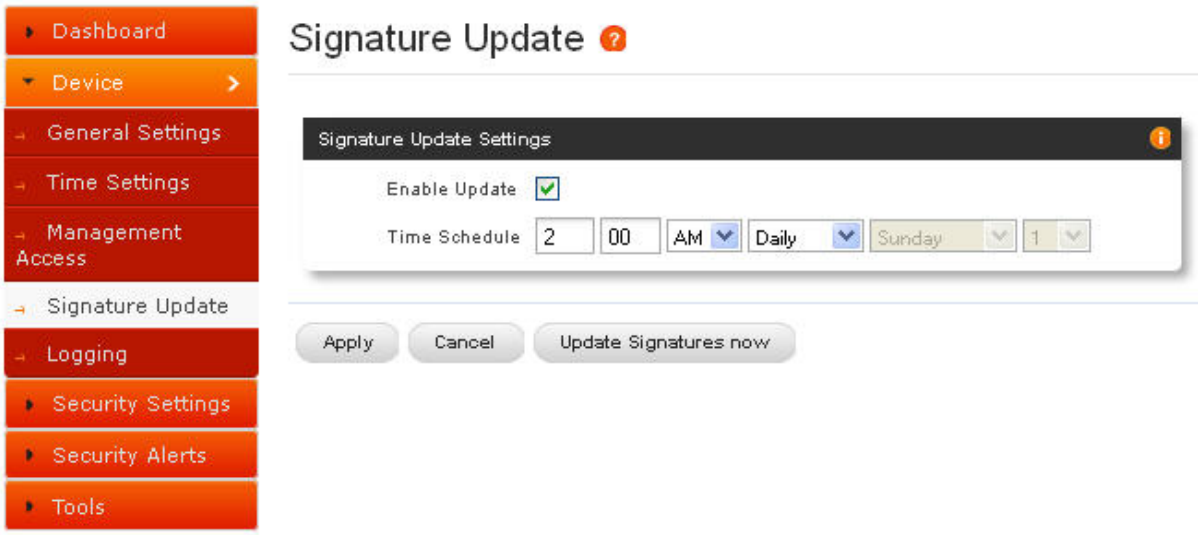

Figure 14: Mise à jour des signatures

Lorsque l'utilisateur achètera un boitier SIP Firewall, l'appareil sera livré avec des signatures SIP de base qui vous aideront dans la protection contre les attaques SIP connues à ce jour.

Toutefois, si l'utilisateur souhaite assurer son déploiement SIP et obtenir la protection contre les nouveaux vecteurs d'attaque, il est recommandé d'activer la mise à jour des signatures sur le boitier.

Vérifier s'il vous plaît au près d'un agent commercial Elastix pour obtenir les détails sur l'achat de la clé de souscription des signatures du Firewall SIP.

3.5. Enregistrement / Loggin

L'administrateur peut configurer le boitier Firewall SIP pour envoyer les alertes de sécurité générées par la détection des attaques SIP vers un serveur Syslog distant.

La page « Loggin » permettra d'activer ou de désactiver l'enregistrement distant des alertes de sécurité et l'adresse du serveur Syslog où vous voudriez transférer les alertes.

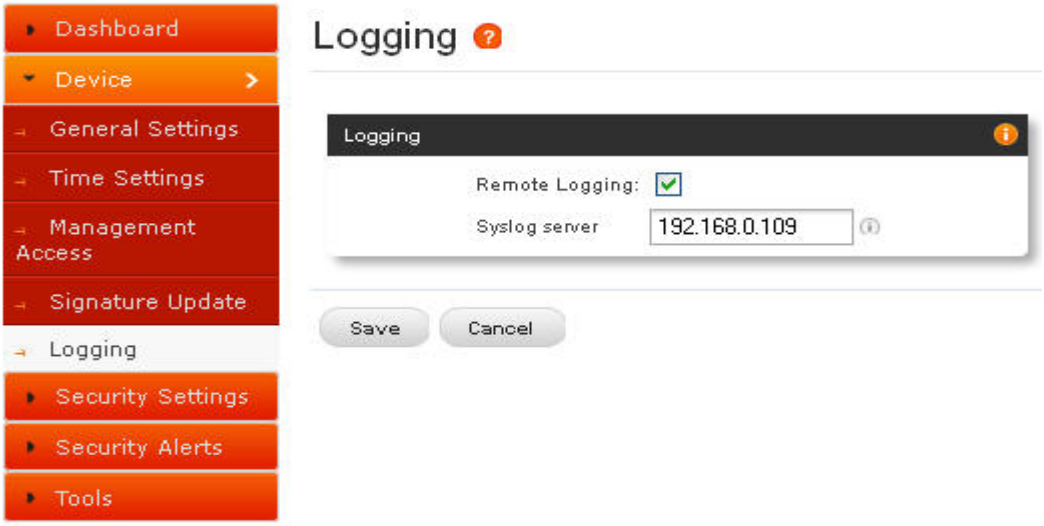

Figure 15: Enregistrement / Logging

4. Configuration Des Politiques De Sécurité SIP

4.1. Politiques de détections des attaques SIP

La page « SIP Attack Detection » permet de configurer les catégories de règles SIP « Deep packet Inspection ». L'administrateur peut activer ou désactiver l'inspection contre une certaine catégorie de règles, l'action à prendre lorsqu'il y aura détections d'attaques correspondant à ces catégories.

Les actions possibles que le pare-feu SIP soit en mesure d'exécuter sont: la journalisation d'alertes, de bloquer les paquets contenant le vecteur d'attaque, et mettre l'adresse IP de l'attaquant dans une liste noire pour une durée donnée. La durée du blocage dépendra de combien de temps l'attaquant aura besoins d'être bloqué, et est également configurée par niveau de catégorie.

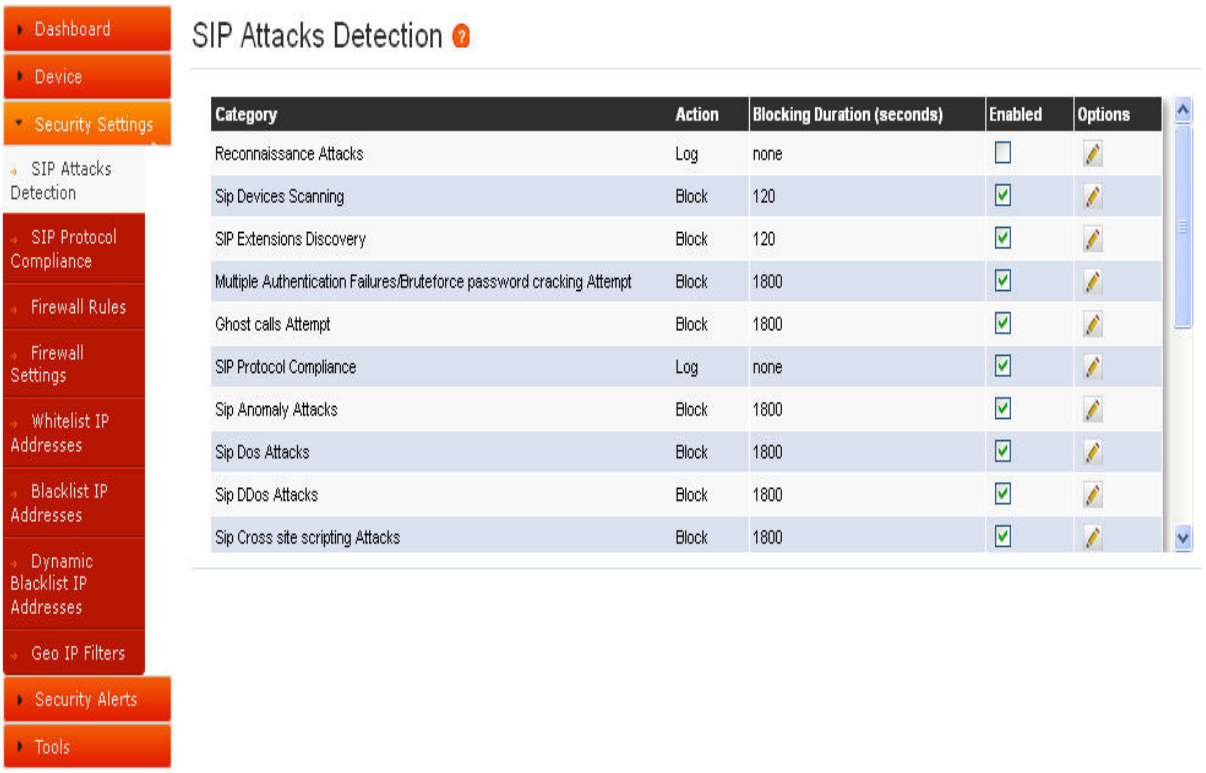

Figure 16: Détections d'attaques SIP

La table évoquée ci-dessous liste les catégories de règles SIP Deep Packet Inspection supportées dans le Firewall SIP et les paramètres de configurations pour chaque catégorie.

Catégorie	Description	Options Configurables par l'utilisateur
SIP Reconnaissance Attacks	L'intrus tente de détecter quelle version d'Asterisk vous avez. Avec cette information, il va commencer à exploiter les nombreuses failles de cette version. Le pare-feu SIP ne répondra pas à sa requête.	N/A
SIP Devices Scanning	L'intrus va scanner les ports de l'IPBX pour voir quels sont les périphériques qui y sont connectés. Avec cette information, il peut exploiter les vulnérabilités de la tierce partie. Le pare-feu SIP ne répondra pas à sa requête.	N/A
SIP Extensions Discovery	L'intrus va demander à L'IPBX de divulguer la gamme des numéros de poste. Avec cette information, il peut essayer différents mots de passe et d'en prendre le contrôle. Le pare-feu SIP ne répondra pas à cette requête.	Invalid SIP User Registration Attempts/Duration
Multiple Authentication Failures/Brute force password Attempt	L'intrus va essayer de se connecter avec différents noms d'utilisateur et mots de passe à plusieurs reprises. Une fois qu'il aura réussi, il aura le contrôle de cette extension. Le pare-feu SIP peut bloquer, enregistrer ou blacklister l'IP pour une période donnée si elle dépasse le nombre d'essais autorisés par seconde.	Failed Authentication Attempts/Duration
Ghost calls Attempt	L'intrus va générer des appels vers une extension et il va ressembler à des appels provenant de cette même extension. Son objectif est de planter l'IPBX dû à une perturbation des communications. Le pare-feu SIP peut bloquer, enregistrer ou blacklister l'IP pour une période donnée si elle dépasse le nombre d'essais autorisés par seconde.	No of Anonymous Invite Responses/Duration
SIP Dos Attacks	Tentatives de d'inondation à partir de divers messages SIP.	No of SIP Request Messages/Duration
SIP DDos Attacks	Tentatives d'inondation distribuées à l'aide de divers messages SIP.	No of SIP Response Messages/Duration

SIP Anomaly attacks	L'intrus va envoyer des paquets SIP anormaux à l'IPBX. Son objectif est de planter l'IPBX engendrant des perturbations dans les communications. Le pare-feu SIP peut bloquer, enregistrer ou blacklister l'IP pour une période donnée si elle dépasse le nombre d'essais autorisés par seconde.	N/A
SIP Buffer overflow attacks	Tentatives de débordement du Buffer qui engendre une validation incorrect des entrées de l'utilisateur.	N/A
SIP Cross site scripting	Le SIP est vulnérable aux cross-site scripting, causée par une validation incorrecte de l'entrée fournie par l'utilisateur dans une requête SIP. L'attaquant distant pourrait exploiter cette vulnérabilité pour injecter un script malveillant dans une page Web qui serait exécuté dans le navigateur Web de la victime, lorsque celle-ci aurait accédé à une page Web contenant des informations tirées de la requête SIP.	N/A
3rd Party vendor vulnerabilities	Attaques ciblées vers les appareils IPBX ou passerelle SIP exploitant leurs propres vulnérabilités.	N/A

4.2. Conformité du Protocole SIP

Le moteur SIP Deep Packet Inspection fonctionnant au cœur du boitier Firewall SIP Firewall a été conçu pour inspecté de trafique SIP en conformité des règles de sécurités embarqué dans ce moteur.

Les anomalies d'entêtes de messages SIP peuvent provoquer diverses conditions erronées, erreurs de l'analyseur SIP et paquets mal formatés qui feront de ces applications SIP d'être vulnérables aux attaques.

Les paramètres suivant seront utilisés par le moteur SIP DPI pour l'identification des différentes conditions d'anomalies de protocole et prend la mesure configuré par l'administrateur.

La configuration de valeurs inappropriées pour ces paramètres peut entraîner un effet perturbateur dans le déploiement de la VoIP. Des administrateurs avec des connaissances approfondies du protocole SIP peuvent choisir de régler ces paramètres pour leurs besoins de déploiements spécifiques. Sinon, il est recommandé d'utiliser les paramètres par défaut.

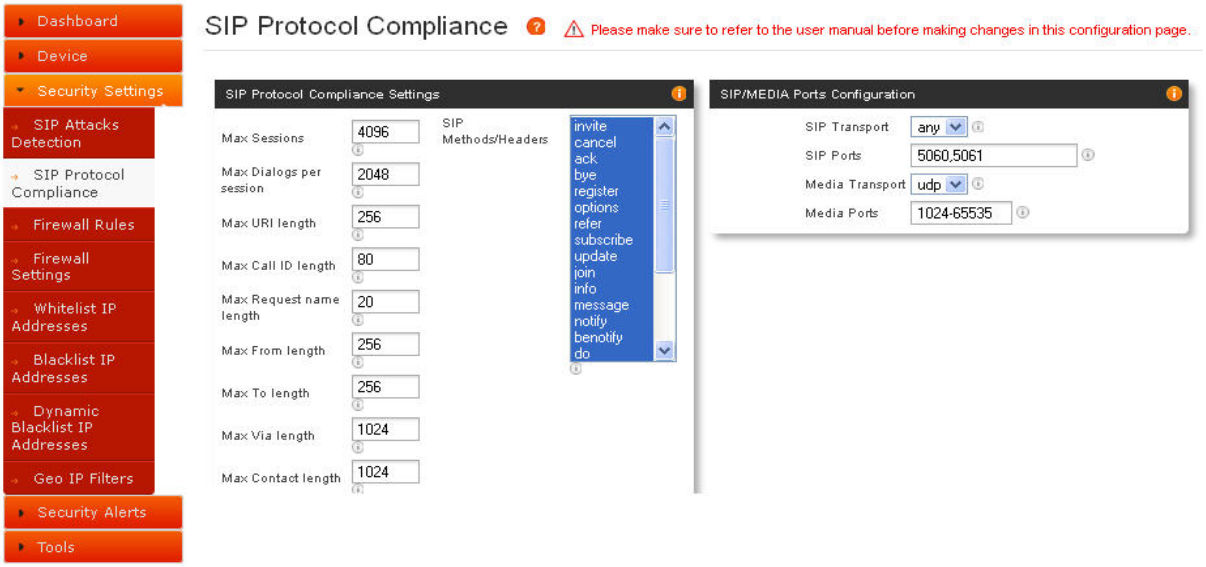

Figure 17: Conformité du Protocole SIP

Max_sessions

Une session SIP est l'application d'une configuration au niveau de la connexion créée entre le serveur et le client SIP pour s'échanger des messages audio / vidéo entre eux. Le paramètre max_sessions définie le nombre maximum de sessions que le moteur SIP DPI pourra tracer. La valeur par défaut a été fixée à 4096.

Max_Dialogs_per_session

Spécifie le nombre maximum de transactions de messages SIP pouvant circuler entre le serveur et le client SIP.

Methods

Spécifie qu'elles seront les méthodes pour vérifier les messages SIP. Les messages SIP qui pourront être identifiés par le moteur SIP DPI sont les suivants: (1) invite, (2) cancel, (3) ack, (4) bye, (5) register, (6) options, (7) refer, (8) subscribe, (9) update (10) join (11) info (12) message (13) notify (14) prack.

Max_uri_len

L'Uri identifie l'utilisateur ou le service auquel la requête SIP est adressée. Max_uri_len spécifie la taille maximale du champ URI de la demande. Par défaut la valeur est réglée à 256. La plage autorisée pour cette option va de 1 à 65535.

Max_call_id_len

Le champ d'en-tête Call-ID dans le message SIP agit comme un identifiant unique qui se rapporte à la séquence de messages échangés entre le client et le serveur SIP. Max_call_id_len spécifie la taille maximale du champ Call-ID. Par défaut la valeur est réglée à 256. La plage autorisée pour cette option va de 1 à 65535.

Max_requestName_len
Spécifie la taille maximum du nom de la requête faisant partie de CSeq ID. Par défaut la valeur est réglée à 20. La plage autorisée pour cette option va de 1 à 65535

Max_from_len
L'entête From spécifie l'identité de l'initiateur de la requête SIP. Max_from_len spécifie la taille maximum du champ From. Par défaut la valeur est réglée à 256. La plage autorisée pour cette option va de 1 à 65535.

Max_to_len
L'entête To spécifie le destinataire souhaité de la requête SIP. Max_to_len la taille maximum du champ To. Par défaut la valeur est réglée à 256. La plage autorisée pour cette option va de 1 à 65535.

Max_via_len
L'entête Via indique quel sera le transport utilisé pour la transaction SIP et identifie l'emplacement où la réponse SIP devra être envoyé.
Max_via_len spécifie la taille maximum du champ Via. Par défaut la valeur est réglée à 1024. La plage autorisée pour cette option va de 1 à 65535

Max_contact_len
Identifiant utilisé pour communiquer avec une instance spécifique client / serveur SIP pour les requêtes suivantes. Max_contact_len spécifie la taille maximale du champ contact. Le défaut est réglé à 256. La plage autorisée pour cette option va de 1 à 65535.

Max_content_len
Spécifie la longueur de la longueur maximale du corps du message. Par défaut la valeur est réglée à 1024. La plage autorisée pour cette option va de 1 à 65535.

4.3. Règles du Firewall.

La configuration des règles du pare-feu permettra à l'administrateur de paramétrer quel trafic devraient être autorisés pour protéger le réseau IPBX / Passerelle SIP à partir d'une zone non fiable Wan, outre le DPI activé, concerne le trafic SIP et RTP. L'administrateur doit spécifier les réseaux source / destination, les numéros de ports et le protocole qui seront utilisés comme les critères de correspondance dans les règles de filtrage et les mesures à prendre en adéquation avec ces règles. Les actions possibles sont de bloquer le trafic et de permettre le trafic correspondant aux règles. Leur priorité sera dans l'ordre dans laquelle elles seront configurées dans la table des règles du pare-feu.

Figure 18: Créer une règle du Firewall

4.4. Paramétrage du Firewall.

Les paramètres du pare-feu permettent à l'utilisateur de configurer le taux de Flood TCP, le TCP Flood Burst, le taux de Flood UDP, et l'UDP Flood Burst dans les paramètres globaux du Firewall.

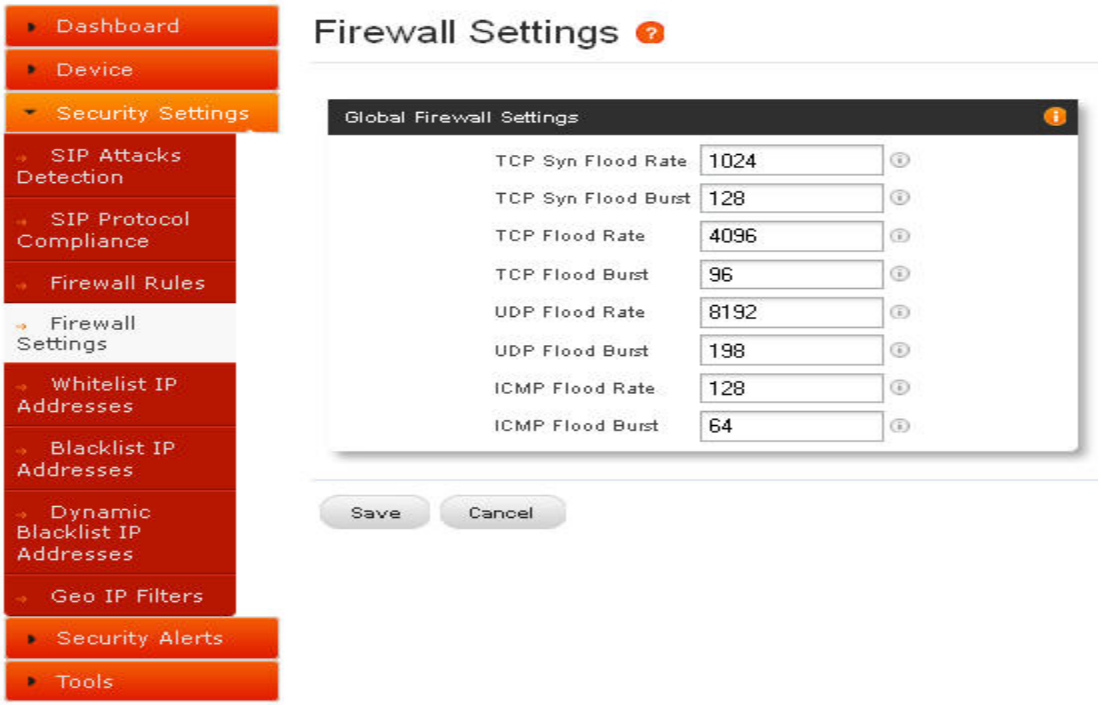

Figure 19: Paramétrages du Firewall

4.5. Les règles de Liste Blanche

Cette page permet de configurer des adresses IP de la liste blanche venant d'une zone non fiable Wan dont l'accès sera autorisé à communiquer avec le réseau SIP protégées par le pare-feu SIP.

Cette page vous permettra aussi de configurer à tout moment si les règles blanches priment sur celles de la liste noire configurés sur le boitier. (À la fois statiques et dynamiques)

Figure 20: Créer une règle Liste Blanche

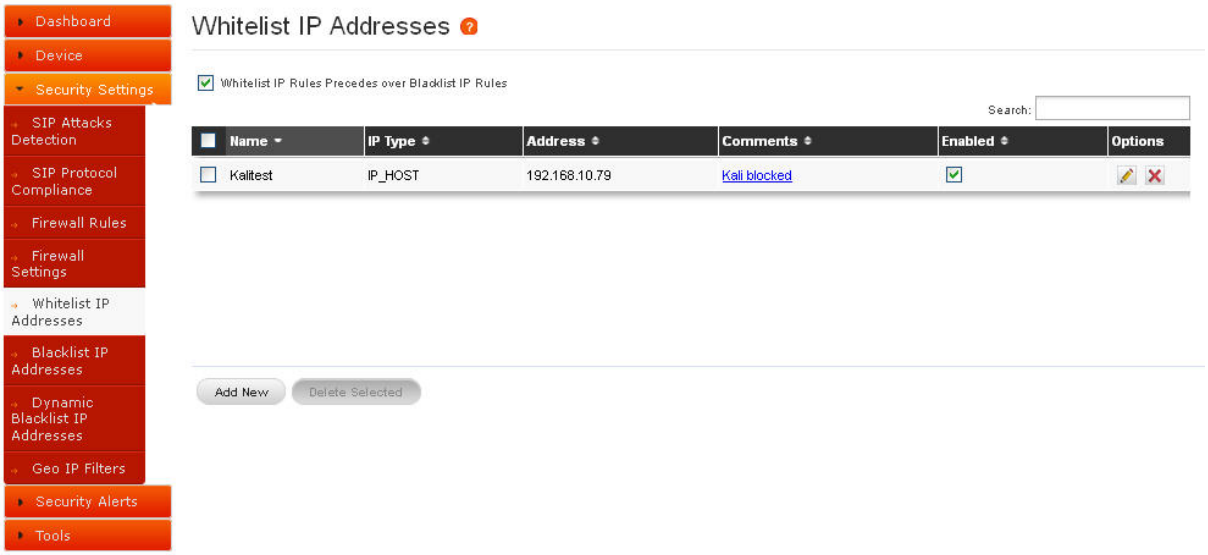

Figure 21: Adresses IP de la Liste Blanche

4.6. Règles de Liste Noire (Statique)

Cette page permet de configurer des adresses IP de la liste noire venant d'une zone non fiable Wan dont l'accès pour communiquer avec le réseau SIP sera bloqué par le Firewall SIP.

Cette page vous permettra aussi de définir à tout moment que les règles de la liste blanches priment sur celles de la liste noire) configurés sur le boitier. (À la fois statiques et dynamiques)

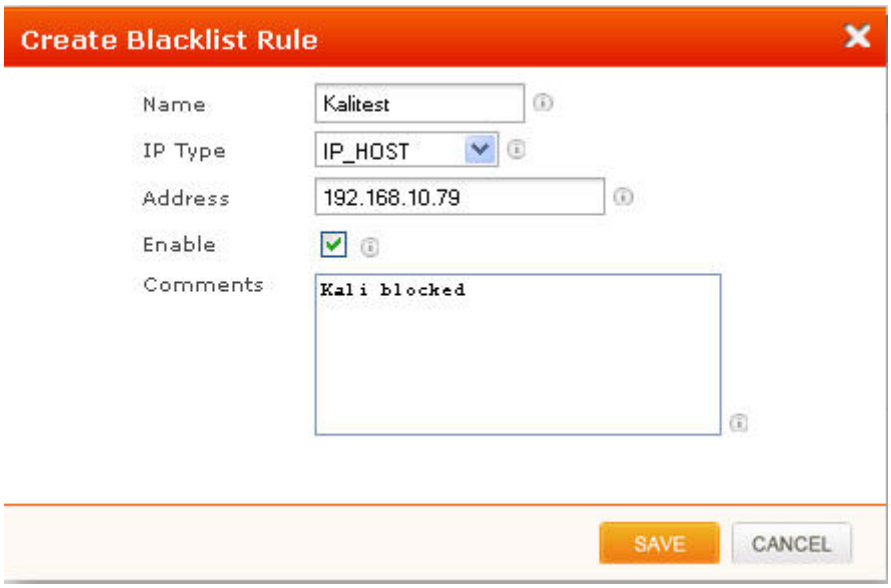

Figure 22: Créer une Liste Noire.

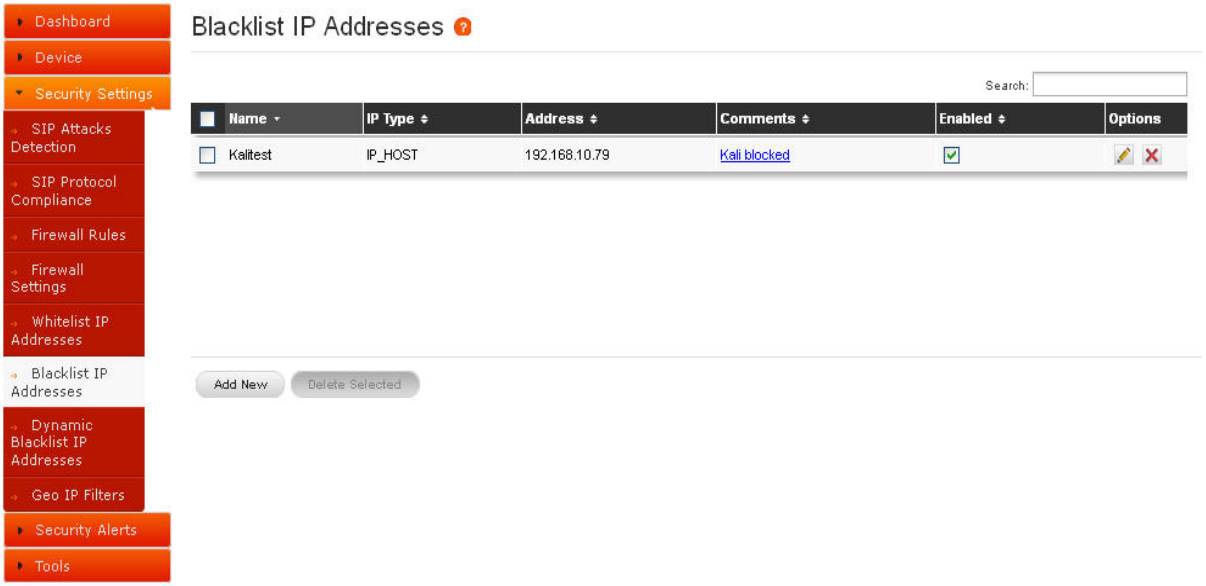

Figure 23: Adresses IP black listées

4.7. Règles de Liste Noire Dynamique.

Les règles de liste noire dynamiques sont les règles de blocages ajoutées par le moteur SIP DPI du firewall pour bloquer le trafic provenant d'adresses IP attaquantes pour une durée configurée dans la catégorie des règles, lors de la détection d'attaques.

Les règles de liste noire dynamiques permettront à l'administrateur de voir les règles actuellement configurées sur le boitier à tout instant. Dans le cas où l'administrateur veut remplacer et autoriser un trafic IP particulier sur liste noire, il pourra supprimer la règle dans la page des règles de liste noire dynamique.

Figure 24: Adresses IP Liste Noire Dynamique.

4.8. Filtres d'Adresses IP Géographiques

L'administrateur peut choisir de bloquer le trafic originaire d'un pays en particulier vers le réseau SIP protégé en configurant les règles de filtrages IP géographiques dans le Firewall SIP.

Figure 25: filtrages IP géographiques

5. Statut

5.1. Alertes de Sécurité.

La page du statut des alertes affiche à tout moment la liste des alertes relatives aux attaques SIP détectées par le moteur DIP du Firewall SIP.

L'administrateur peut choisir de définir l'intervalle de rafraichissement de la visualisation des logs dans cette page.

L'administrateur peut choisir de configurer le boitier afin qu'il notifie par mail un résumé des alertes de sécurité générées par le Firewall SIP.

Il y a également la possibilité de télécharger les alertes de sécurité au format CSV figurant sur la page.

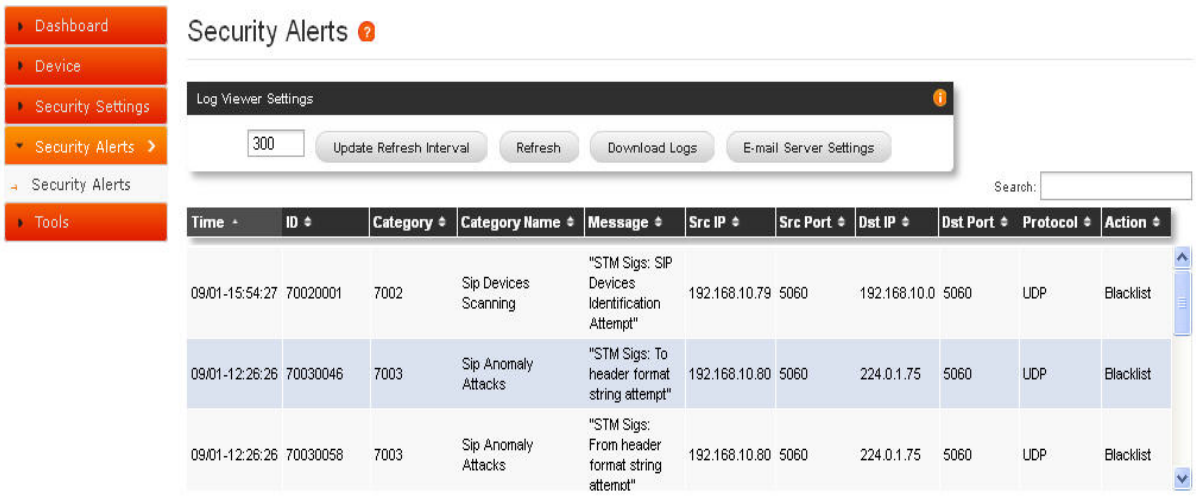

Figure 26: Alertes de Sécurité

Sauf si l'utilisateur configure la transmission des alertes de sécurité à un serveur syslog distant, les alertes de sécurité ne sont pas conservées en permanence dans le boitier. L'emplacement de la mémoire tampon de journalisation sera vidé à un intervalle prédéfini (non configurable) et une fois les critères de seuil d'enregistrement remplies. Toutefois, si l'administrateur souhaite inscrire les alertes dans un périphérique de stockage USB, ils peuvent le connecter au port de données USB du boitier Firewall SIP. La rotation des logs seront automatiquement archivés au format CSV dans le boitier.

6. Outils

6.1. Administration

La page d'interface d'Administration apporte les options pour exécuter une réinitialisation d'usine du boitier, redémarrer les services, redémarrer le boitier, arrêt du boitier, sauvegarde et restauration de la configuration.

L'exécution d'une réinitialisation d'usine nécessite un reboot et ainsi, l'administrateur sera redirigé vers une page de notification d'attente dès qu'il aura cliqué sur le bouton « Factory Reset ». Ensuite un Login s'affichera une fois que le boitier sera revenu à sa configuration par défaut.

Le boitier Firewall SIP supporte que l'on prenne une configuration sauvegardée et qu'on la restaure plus tard.

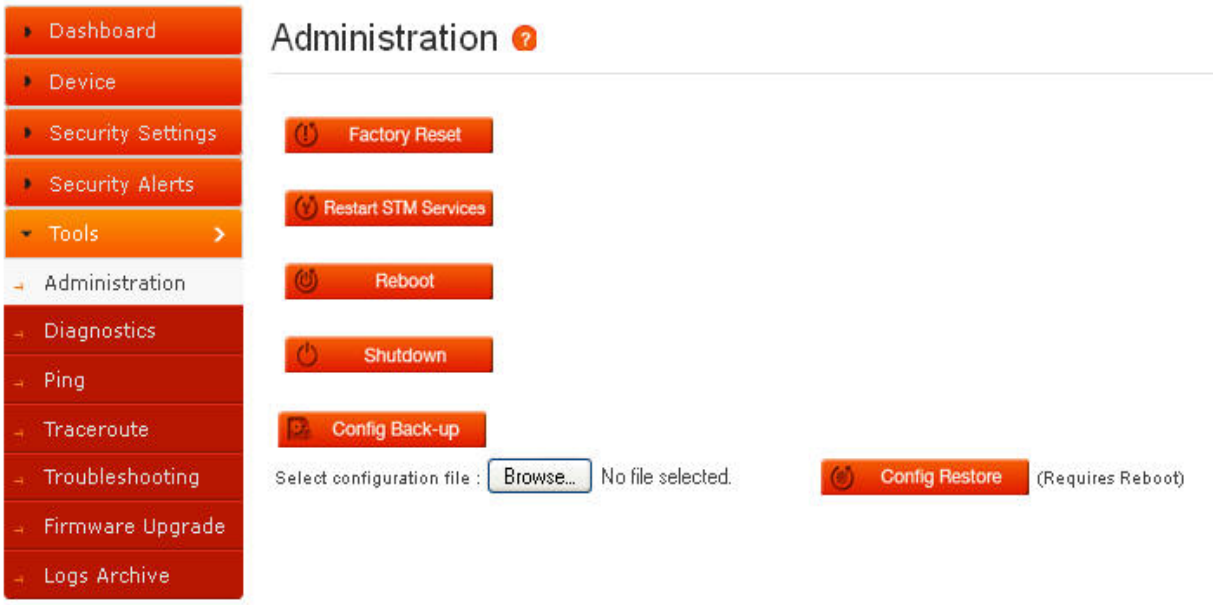

Figure 27: Administration

La sauvegarde de la configuration contiendra au final la configuration effective, s'il y a des changements transitoires qui ne sont pas encore appliqués durant la sauvegarde, ceux-là ne seront pas pris en compte lors de l'archivage de la configuration dans le fichier de sauvegarde.

6.2. Diagnostics

La page de diagnostics permettra à l'administrateur de réunir les fichiers de journalisations qui se rendront utile pour l'équipe support Elastix lors du débogage des problèmes lors d'une installation d'un déploiement du Firewall SIP.

Pour exécuter cet outil sur ce boitier, l'administrateur doit cliquer sur le bouton « Run diagnostics ». L'appareil exécutera les diagnostics en tâche de fond et affichera les résultats une fois cette tâche effectuée. L'administrateur peut télécharger les rapports en cliquant sur le bouton « Get Report » puis l'envoyer à l'équipe support d'Elastix. (**Note** : vous pouvez l'envoyer à : support@elastix.com)

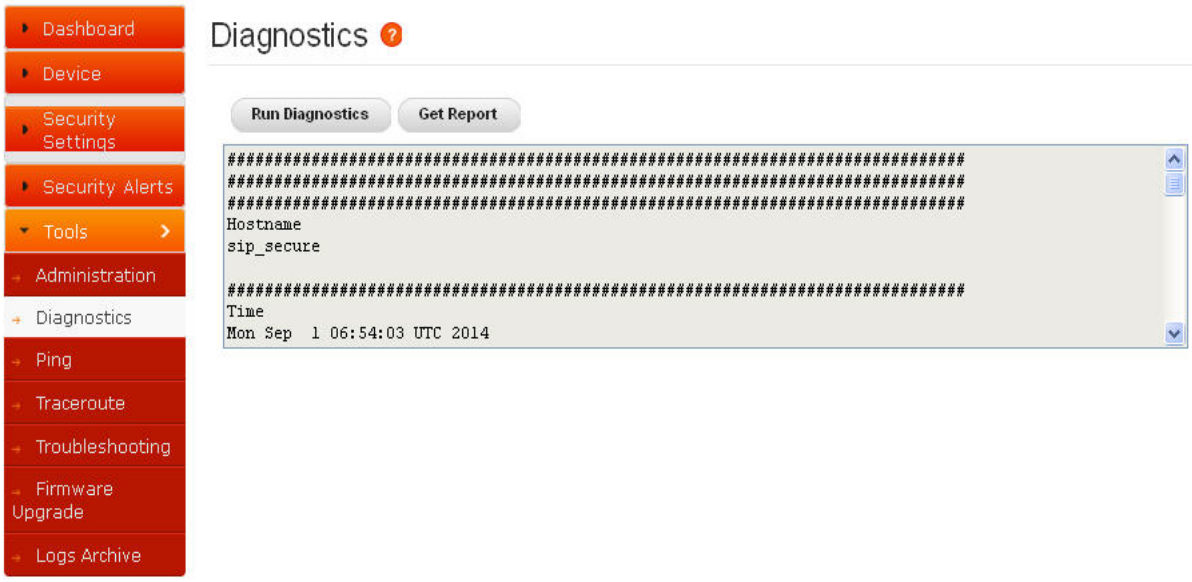

Figure 28: Diagnostics

Cliquer sur le lien ci-dessous pour télécharger les diagnostics

Figure 29: Télécharger le rapport.

6.3. Ping

L'administrateur peut résoudre les problèmes de connectivité réseau en exécutant un ping depuis le boitier Firewall SIP.

L'administrateur doit alors rentrer l'adresse IP à pinguer depuis l'appareil, sélectionner le nombre de pings à effectuer et cliquer sur le bouton « Ping » pour exécuter la tâche. Le résultat du ping sera affiché dans la zone texte une fois l'exécution du ping terminé.

Figure 30: Résultat du ping

6.4. Trace route

L'administrateur peut résoudre les problèmes de connectivités réseau en exécutant un «Trace route » depuis le Firewall SIP.

L'administrateur aura alors besoin d'entrer l'adresse IP qui devra être tracée depuis le Firewall SIP, sélectionner le nombre de sauts et cliquer sur le bouton « Trace route » afin d'exécuter cette tâche.

Le résultat du « Trace route » sera affiché dans la zone texte une fois cette tâche terminée.

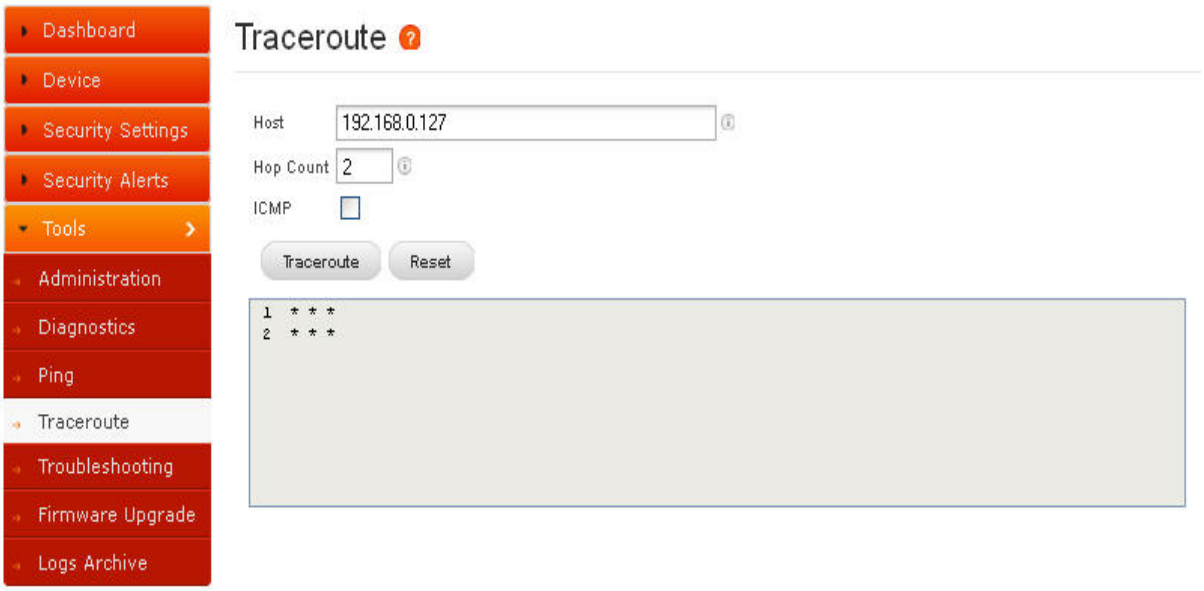

Figure 31: Trace route

6.5. Troubleshooting

Cette page active / désactive le DPI sur le Firewall SIP à des fins de maintenances.

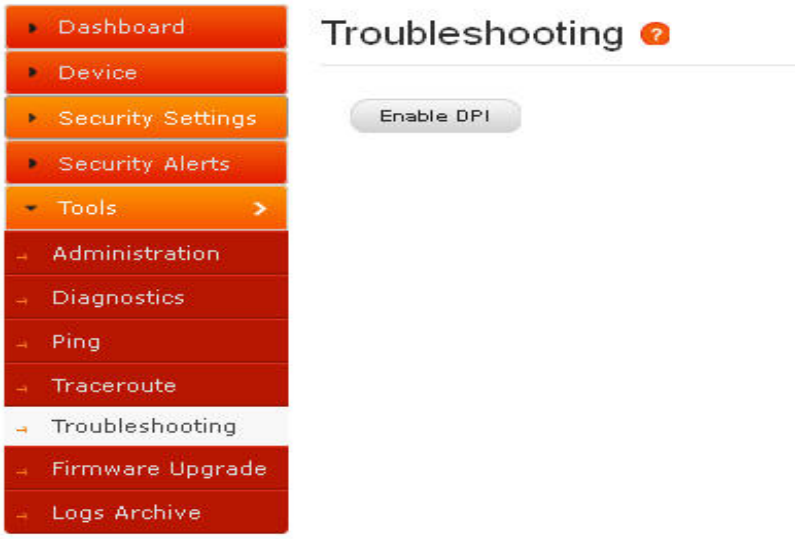

Figure 32: Dépannage

6.6. Mise à jour du Firmware

Le boitier Firewall SIP accepte la mise à jour manuelle du firmware exécuté au sein de cet appareil. La page de mise à jour montre la version actuelle du firmware installée dans le Firewall SIP et permet à l'administrateur de charger le nouveau firmware, puis de l'installer.

Pour installer le firmware :

- Télécharger le package de mise à jour du firmware sur le site Elastix et sauvegardez-le sur votre PC en local.
- Depuis votre navigateur Web de votre station de travail (PC), loguez-vous sur le Firewall et lancez la page de mise à jour du firmware.
- Cliquez sur « Parcourir » et sélectionnez le fichier contenant le package du firmware que vous avez sauvegardé sur votre station de travail en local.
- Après avoir sélectionner le fichier, cliquez sur le bouton « Upgrade »
- L'appareil vérifiera le firmware chargé et l'installera. Après l'installation, le boitier redémarrera et l'administrateur sera redirigé vers la page de login.

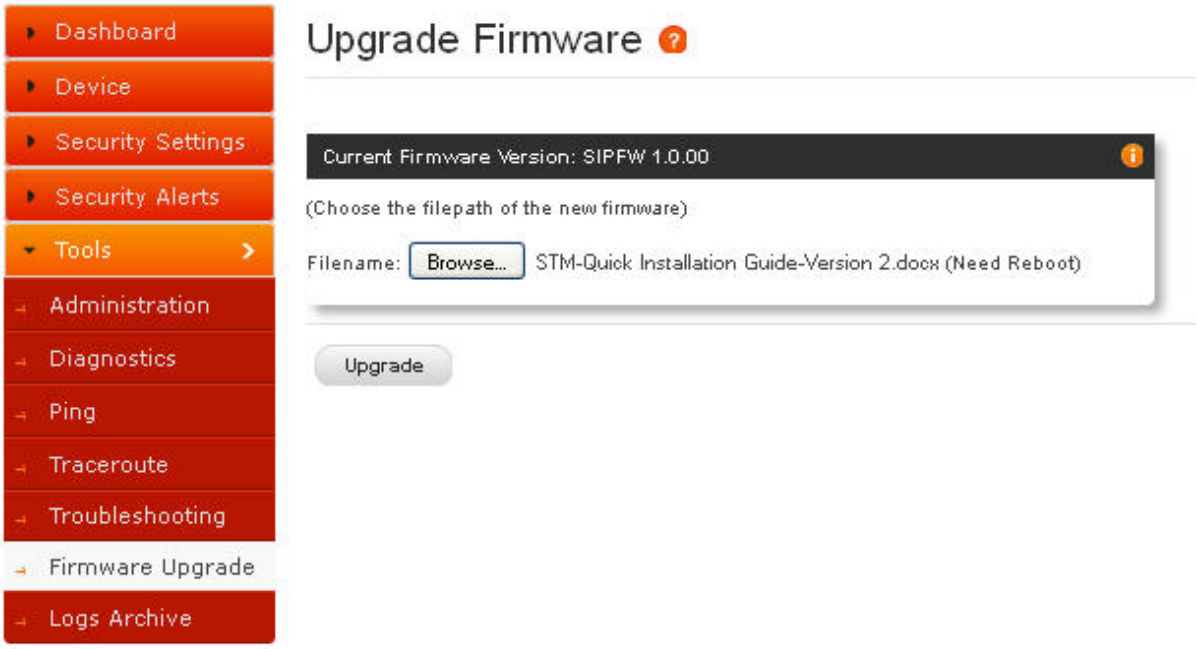

Figure 33: Mise à jour du Firmware

6.7. Archivage du journal d'événements.

Si une clef de stockage USB est branchée sur le Firewall SIP, le boitier tentera d'archiver les plus anciens logs sur cette clef. Une synthèse des informations des logs enregistrés sera affichée dans la page Logs Archive.

Figure 34: Archivage du journal d'événements

ANNEX

7. Annex A – Utilisation de l'accès en mode console.

1. Connecter le cordon série sur le port série du Firewall SIP
2. Utiliser les paramètres suivant pour accéder au CLI
    i. Vitesse : 38400
    ii. Parité : None
    iii. Données : 8
    iv. Bit de stop : 1
    v. Contrôle de flux : No

3. L'utilisateur devrait voir un prompt « Elastix » sur le terminal.
4. Taper « help » pour visualiser la liste des commandes de maintenances valides.

8. Annex B – Configuration de l'Adresse IP du Firewall SIP via la Console

L'utilisateur peut choisir de visualiser ou de paramétrer l'adresse IP du Firewall SIP :

> Show IP

Maintenant vous pouvez vous connecter au boitier depuis le navigateur web en utilisant l'URL https://<device-ip>

Si vous n'avez pas démarré de serveur DHCP lors du déploiement ou si l'appareil a des difficultés à acquérir une adresse IP, alors paramétrez une adresse IP en mode CLI en utilisant le ligne de commande.

Elastix > Set IP <IP address> <mask> <gateway>

Vérifiez l'adresse IP en utilisant la commande « show ip ». Puis utilisez cette adresse IP pour accéder au WebUI ou à la console SSH pour une plus ample configuration.

Pour plus d'assistance technique, veuillez contacter le support au : support@elastix.com