



Implementando Elastix SIP Firewall

Juan Oliva

IMPLEMENTANDO ELASTIX SIP FIREWALL

Manual de instalación y pruebas de
aseguramiento

JUAN OLIVA
@jroliva

[PRIMERA EDICIÓN]

Copyright (c) 2015 Juan Oliva

Esta obra está licenciada bajo la Licencia **Creative Commons**
Atribución-NoComercial-CompartirIgual 3.0 Unported. Para ver una
copia de esta licencia, visite:

<http://creativecommons.org/licenses/by-nc-sa/3.0/>.

Si luego de leerla todavía tiene alguna duda acerca de esta licencia,
envíe una carta a Creative Commons, 171 2nd Street, Suite 300, San
Francisco, California, 94105, USA.

Primera Edición

Dedicado para Angélica y Sebastián

1. Agradecimiento

La telefonía IP, VoIP, Linux y la seguridad informática, siempre ha sido y será mi pasión, sin embargo el desarrollo de estas capacidades no necesariamente hubieran sido posibles, sin el apoyo y confianza de:

Edgar Landívar CEO y creador de Elastix por permitirme ser parte del equipo de colaboradores de Elastix.

Paul Estrella Project Manager de Elastix, el cual siempre me impulsa a desarrollar nuevas ideas y proyectos.

A mi esposa, que gracias a su paciencia y cariño, me brinda la inspiración para seguir adelante.

2. Acerca del autor

Juan Oliva Córdova
@jroliva
<http://jroliva.wordpress.com/>

Es consultor de seguridad informática y Telefonía IP con más de 15 años de experiencia en el campo. Está muy involucrado en proyectos de pruebas de penetración, análisis y explotación de vulnerabilidades, entre otras tareas de la seguridad informática. También desarrolla proyectos de implementación y aseguramiento de plataformas de telefonía IP, basadas en Elastix, proyectos de CallCenter, soluciones Softswitch y hosted PBX.

3. Introducción

Es innegable que el mundo de la VoIP desde sus inicios siempre ha estado rodeado de los ataques informáticos, es así que a lo largo del tiempo las técnicas para comprometer las plataformas han cambiado y suelen ser en la actualidad muy sofisticadas.

Así mismo, también la aparición de herramientas que ayudan a la protección de las plataformas VoIP ha ayudado a minimizar muchos los riesgos de seguridad que involucra el uso este tipo de tecnológica, la cual brinda muchos beneficios.

Sin embargo en la búsqueda de la simplicidad, eficiencia y la herramienta perfecta, los errores de configuración o la carencia de conocimientos para poder validar la seguridad adecuadamente, suelen pasar factura, a la hora de protegerla.

Es así, que el presente libro no solo cubre aspectos que involucran la correcta y adecuada configuración de Elastix SIP FIREWALL, si no también, las pruebas que todo profesional del área de la VoIP, tendría que realizar, para poder validar y comprobar la protección y aseguramiento de su plataforma VoIP es la adecuada.

Teniendo en cuenta que las amenazas en el área de VoIP cambian constantemente, el material cubre los aspectos más importantes de la protección de amenazas usando Elastix SIP FIREWALL.

Juan Oliva
@jroliva

Índice de Contenidos

Agradecimiento	4
Acerca del autor	4
Introducción	5
1. Esquema de funcionamiento	1
2. Configuración e integración con Elastix 2.5	2
2.1 Configuración inicial.....	2
3. Revisión de funcionalidades	4
3.1 Dashboard	4
3.2 Device	5
3.2 Security Settings	7
3.3 Security Alerts.....	10
3.4 Tools.....	11
4 Configuración y detección de prevención de ataques de Fingerprinting	14
4.1 Desarrollando ataque de fingerprint.....	14
4.2 Detección del Ataque.....	14
5 Configuración y detección de ataques de enumeración de usuarios	15
5.1 Desarrollando ataques de enumeración.....	15
5.2 Detección del Ataque.....	15
6 Configuración y bloqueo de Ataques DoS.....	16
6.1 Desarrollando ataques de DOS VoIP	16
6.2 Detección del Ataque.....	16
7 Bloqueo de Intentos de obtención de contraseñas o password cracking.....	17
7.1 Desarrollando ataques de password cracking	17
7.2 Detección del Ataque.....	17
8 Bloqueo de Intentos de ataques de SIP Cross Site Scripting	18
8.1 Desarrollando ataques de SIP Cross Site Scripting	18
8.2 Detección del Ataque.....	19
9 Configuración de listas negra dinámica para amenazas VoIP	20
9.1 Cambiando la dirección IP	20
9.2 Probando el bloqueo pro activo mediante listas negras dinámicas.....	21
9.2.1 Verificando conectividad desde el atacante	21
9.2.2 Realizando un ataque de SIP BRUTE FORCE ATTACK	21
9.2.3 Verificando el bloqueo en SIP FIREWALL	22
10 Configuración de reglas de Blacklist y Whitelist.....	23
10.1 Agregando direcciones IP al Blacklist.....	23
10.2 Agregando direcciones IP al Whitelist.....	26
11 Configuración de bloqueo por ubicación geográfica	27
12 Configuración de acceso a la administración del dispositivo a una IP/red específica.....	28
12.1 Ingresar a Device / Management Access y editar la regla “DefaultAllAccess”.....	28
12.2 Establecer la dirección IP para administración	28
13 Configuración de servidor SYSLOG remoto para registro de eventos.....	30
13.1 Instalación y configuración de SYSLOG Server	30
13.2 Configuración un servidor de SYSLOG externo en Elastix SIP FIREWALL	36
13.3 Probar la integración de Elastix SIP FIREWALL y Servidor SYSLOG externo.	37

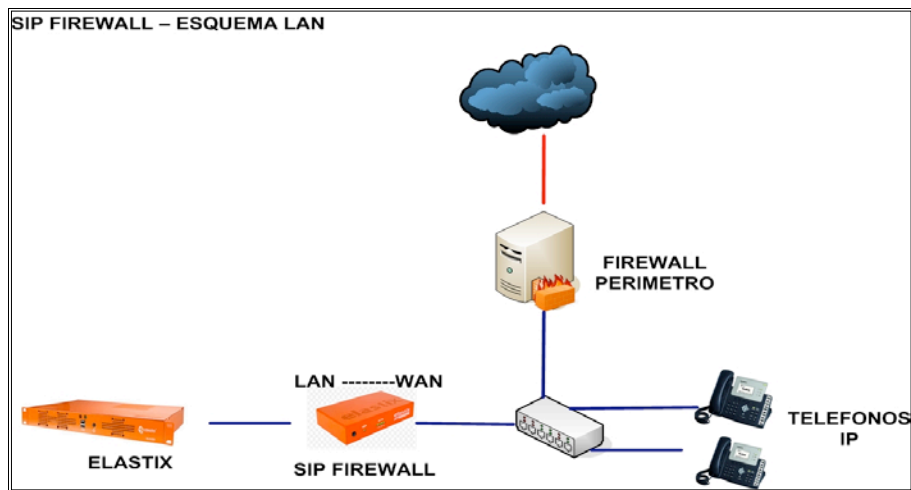
ELASTIX SIP FIREWALL

1. Esquema de funcionamiento

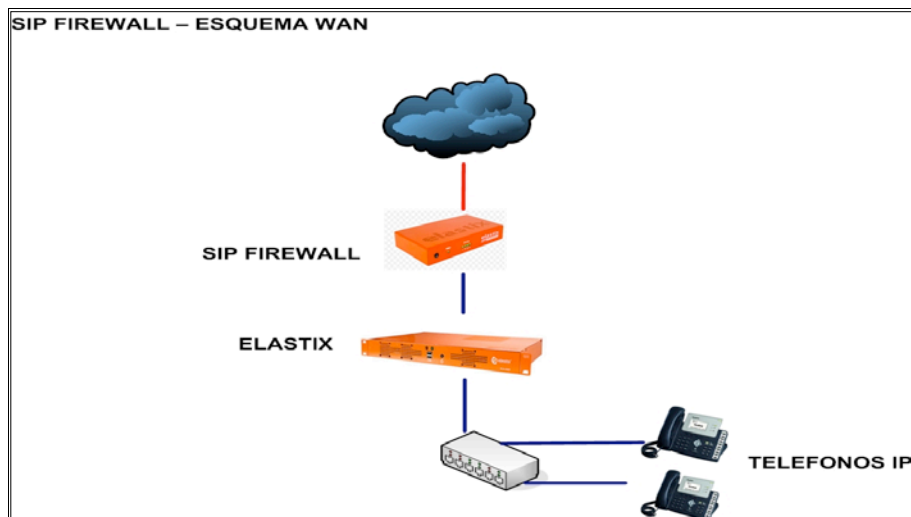
El SIP FIREWALL es dispositivo totalmente agnóstico a la red donde esté posicionado el servidor Elastix PBX, ya que funciona en modalidad mirror.

De tal forma que no es necesario realizar ninguna configuración del lado de la central Elastix.

A.- Configuración de SIP FIREWALL cuando Elastix PBX tiene una sola tarjeta de red (LAN)



B.- Configuración de SIP FIREWALL cuando Elastix PBX tiene dos tarjetas de red (LAN y WAN)

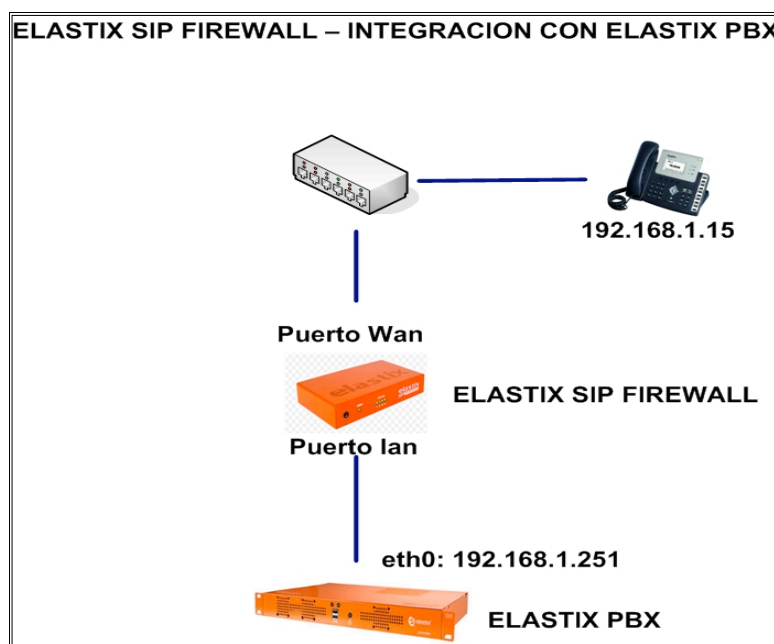


2. Configuración e integración con Elastix 2.5

2.1 Configuración inicial

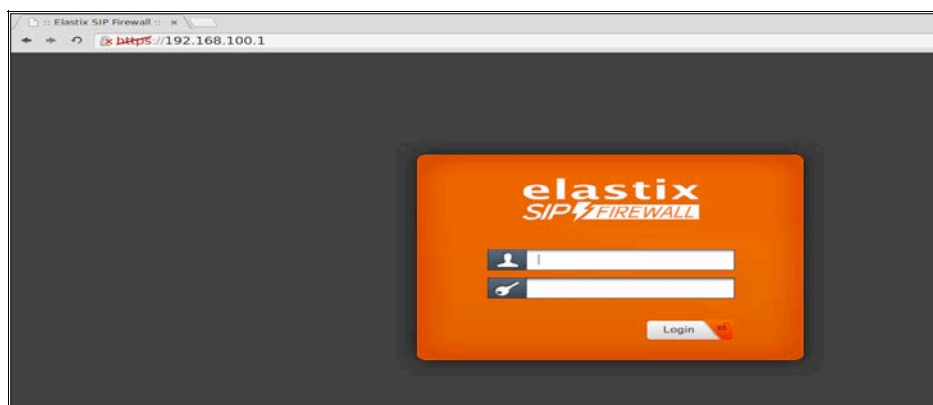
Como se indicó en el punto anterior Elastix SIP FIREWALL se configura de manera transparente con respecto a la PBX, de la siguiente forma:

- Puerto LAN de SIP FIREWALL conectado al puerto LAN de Elastix PBX.
- Puerto WAN de SIP FIREWALL conectado al SWITCH o al FIREWALL de perímetro según sea el caso.



Ingresando a la interface de administración de Elastix SIP FIREWALL

SIP FIREWALL viene configurado con la dirección IP **192.168.100.1/255.255.255.0**, por lo cual será necesario estar en el mismo segmento (192.168.100.0/24), luego ingresar a la interface web en la siguiente URL: <https://192.168.100.1> como se muestra a continuación.



El usuario y contraseña por defecto es admin

Así mismo también deberíamos poder tener conectividad hacia nuestra plataforma Elastix, es decir hacer ping e ingresar a la interface web de manera transparente, pasando por Elastix SIP FIREWALL

3. Revisión de funcionalidades

3.1 Dashboard

System Status

Rendimiento de la memoria RAM, almacenamiento y consumo del CPU

Network Status

Dirección IP de escucha, direcciones MAC

Sig Update Version

Versión de firmas

DPI Status

Estado de DPI

Security Alert Summary,

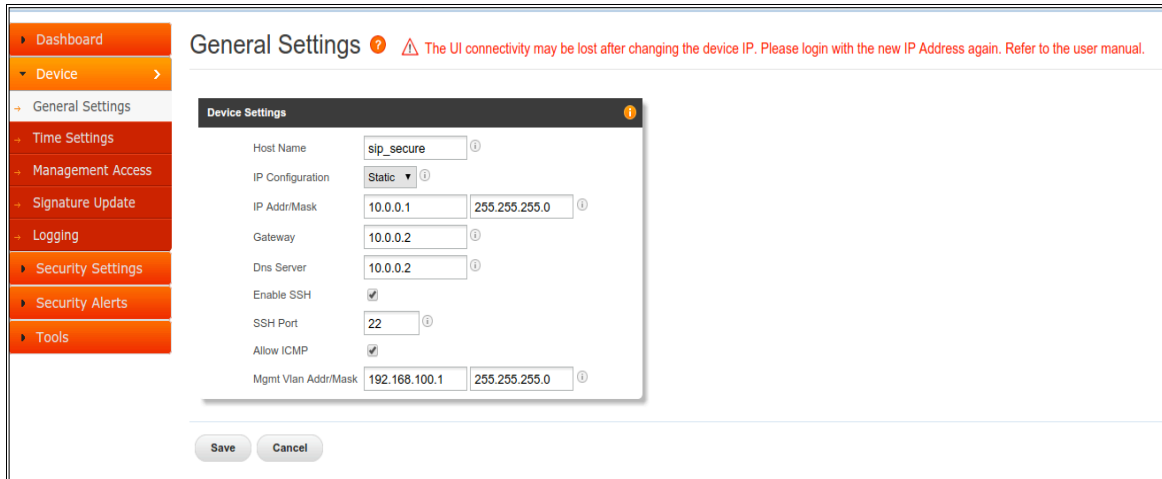
Last 10 Alerts, ultimas 10 alertas detectadas.

The screenshot displays a dashboard with a left-hand navigation menu containing 'Dashboard', 'Device', 'Security Settings', 'Security Alerts', and 'Tools'. The main content area is titled 'Dashboard' and is divided into several sections:

- System Status:** Includes 'Up-Time' (2 min), 'Memory Usage (Total Memory:64MB)' at 74%, 'Flash Usage (Flash Size:16MB)' at 79%, and 'CPU Usage' at 4%.
- Network Status:** Includes 'Network Info' with details: Device IP : 10.0.0.1, LAN MAC : 00:17:F7:00:9C:06, WAN MAC : 00:17:F7:00:9C:07, and Gateway : 10.0.0.2.
- Sig Update Version:** Shows 'Elastix SIP Firewall Signatures 1.0.00'.
- DPI Status:** Shows 'Enabled' and 'Running' with green status indicators.
- Security Alert Summary:** Includes links for 'Top 10 Signatures', 'Top 10 Categories', 'Top Src', and 'Top Dest'.
- Last 10 Alerts:** A table with columns for Time, ID, Category, Message, and Src IP.

3.2 Device

General Settings, Configuración de la dirección IP del dispositivo.

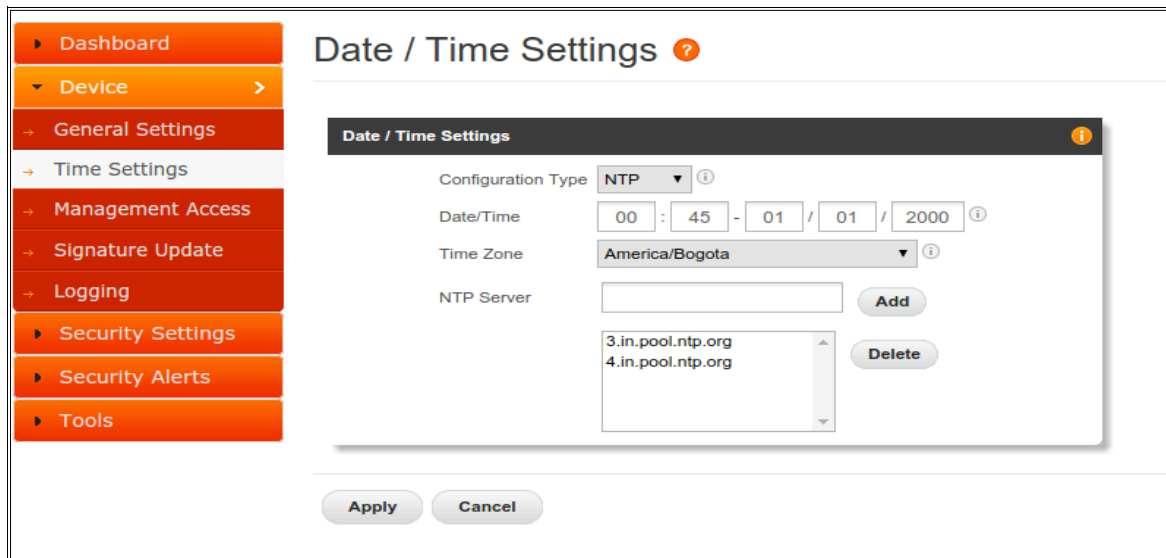


The screenshot shows the 'General Settings' page with a sidebar on the left containing menu items: Dashboard, Device, General Settings, Time Settings, Management Access, Signature Update, Logging, Security Settings, Security Alerts, and Tools. The main content area is titled 'General Settings' and includes a warning message: 'The UI connectivity may be lost after changing the device IP. Please login with the new IP Address again. Refer to the user manual.' A 'Device Settings' dialog box is open, displaying the following configuration:

Host Name	sip_secure	
IP Configuration	Static	
IP Addr/Mask	10.0.0.1	255.255.255.0
Gateway	10.0.0.2	
Dns Server	10.0.0.2	
Enable SSH	<input checked="" type="checkbox"/>	
SSH Port	22	
Allow ICMP	<input checked="" type="checkbox"/>	
Mgmt Vlan Addr/Mask	192.168.100.1	255.255.255.0

Buttons for 'Save' and 'Cancel' are located at the bottom of the dialog box.

Date / Time Settings, configuración de la hora y zona horaria, esta configuración es muy importante, para la correcta correlación de los eventos.



The screenshot shows the 'Date / Time Settings' page with the same sidebar as the previous image. The main content area is titled 'Date / Time Settings' and includes a warning icon. A 'Date / Time Settings' dialog box is open, displaying the following configuration:

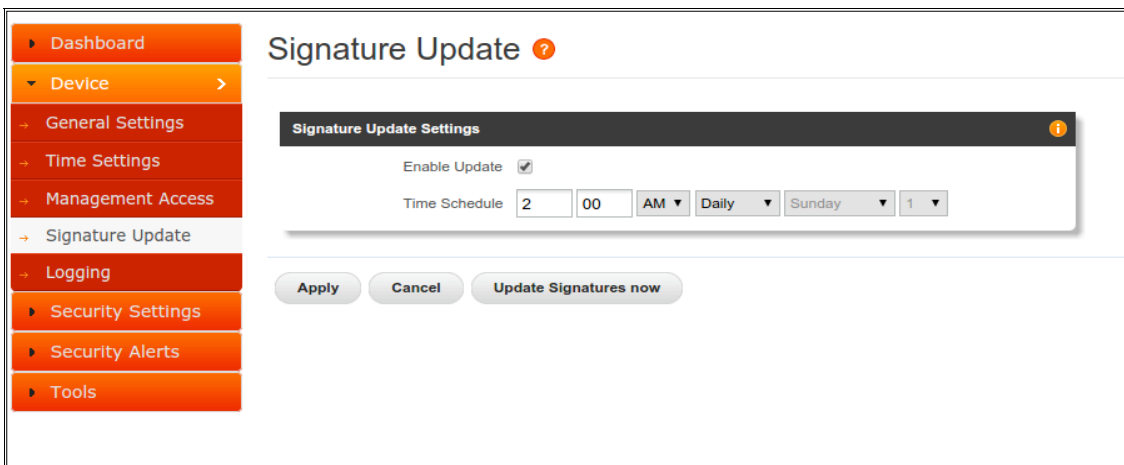
Configuration Type	NTP	
Date/Time	00 : 45 - 01 / 01 / 2000	
Time Zone	America/Bogota	
NTP Server	<input type="text"/> Add	
	3.in.pool.ntp.org 4.in.pool.ntp.org Delete	

Buttons for 'Apply' and 'Cancel' are located at the bottom of the dialog box.

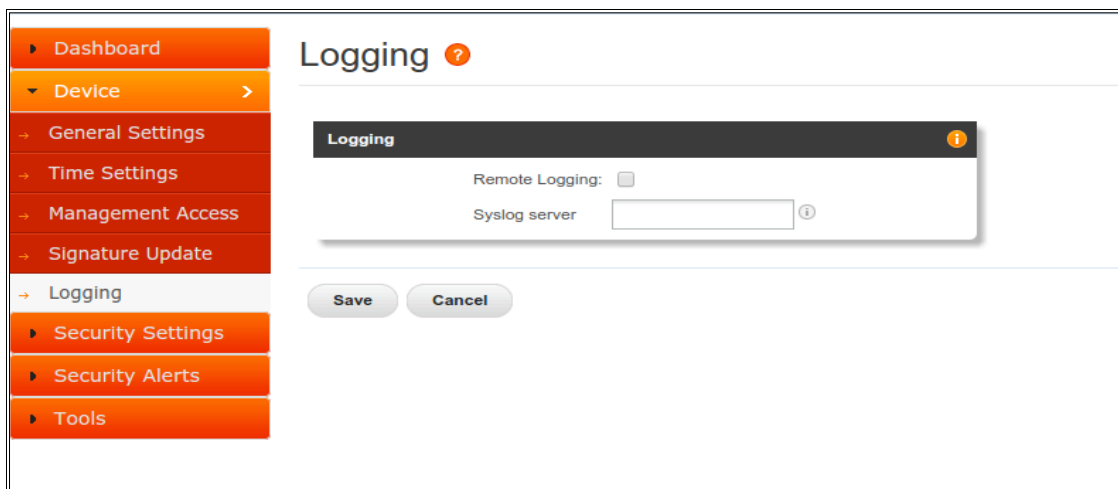
Management Access, Permite crear reglas que restringen el acceso a los servicios WEB y SSH del SIP FIREWALL.



Signature Update, Permite programar la actualización de firmas del sistema.

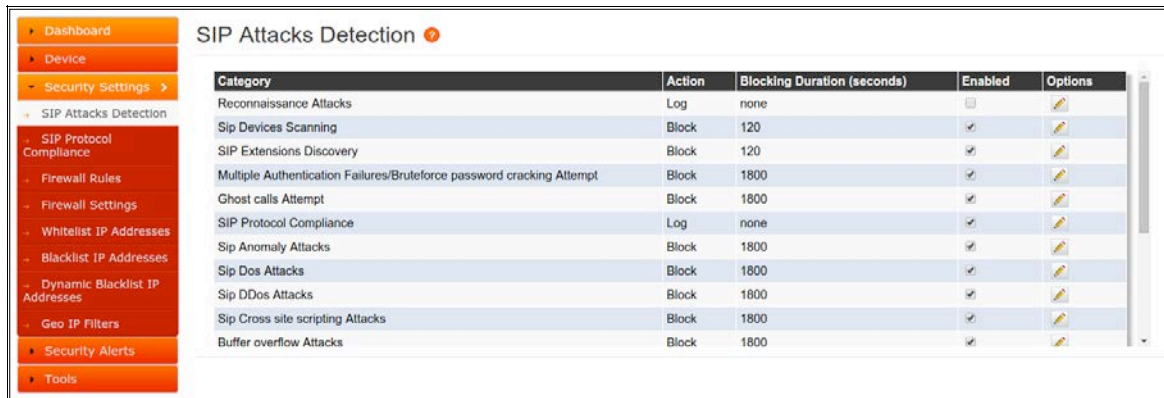


Logging, permite la configuración de un servidor de LOG remoto



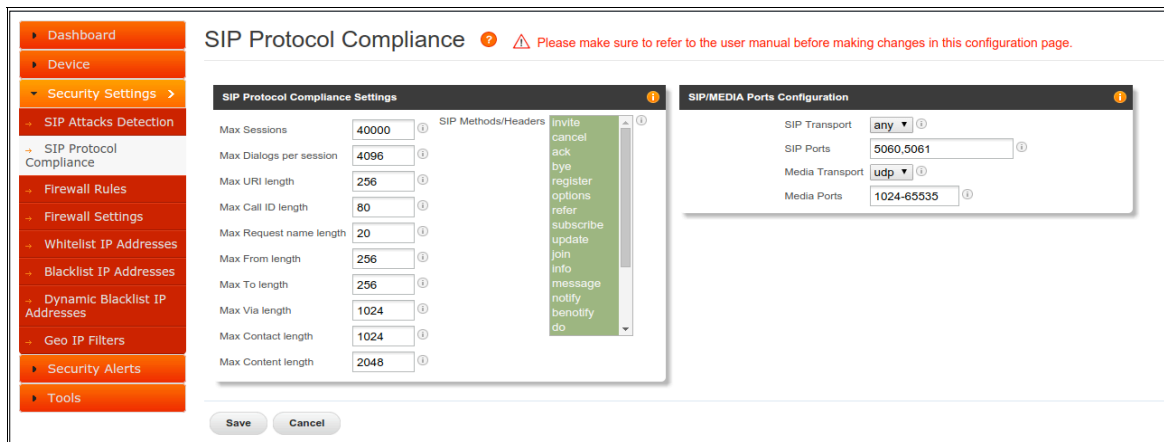
3.2 Security Settings

SIP Attacks Detection, Permite la inspección y análisis de paquetes SIP, es posible habilitar y la inspección para una particular categoría o regla.



Category	Action	Blocking Duration (seconds)	Enabled	Options
Reconnaissance Attacks	Log	none	<input type="checkbox"/>	
Sip Devices Scanning	Block	120	<input checked="" type="checkbox"/>	
SIP Extensions Discovery	Block	120	<input checked="" type="checkbox"/>	
Multiple Authentication Failures/Bruteforce password cracking Attempt	Block	1800	<input checked="" type="checkbox"/>	
Ghost calls Attempt	Block	1800	<input checked="" type="checkbox"/>	
SIP Protocol Compliance	Log	none	<input checked="" type="checkbox"/>	
Sip Anomaly Attacks	Block	1800	<input checked="" type="checkbox"/>	
Sip Dos Attacks	Block	1800	<input checked="" type="checkbox"/>	
Sip DDos Attacks	Block	1800	<input checked="" type="checkbox"/>	
Sip Cross site scripting Attacks	Block	1800	<input checked="" type="checkbox"/>	
Buffer overflow Attacks	Block	1800	<input checked="" type="checkbox"/>	

SIP Protocols Compliance, El motor de inspección de paquetes SIP, permite detectar anomalías en las cabeceras SIP para identificar fallas en el protocolo y tomar una acción según lo configurado.



SIP Protocol Compliance Settings

Max Sessions: 40000
Max Dialogs per session: 4096
Max URI length: 256
Max Call ID length: 80
Max Request name length: 20
Max From length: 256
Max To length: 256
Max Via length: 1024
Max Contact length: 1024
Max Content length: 2048

SIP Methods/Headers

- invite
- cancel
- ack
- bye
- register
- options
- refer
- subscribe
- update
- join
- info
- message
- notify
- benotify
- do

SIP/MEDIA Ports Configuration

SIP Transport: any
SIP Ports: 5060,5061
Media Transport: udp
Media Ports: 1024-65535

Buttons: Save, Cancel

FIREWALL Rules, Permite al administrador configurar el tráfico que permite o deniega desde la red WAN a la cual protege en la PBX IP.

Name	Src Type	Src Addr	Dst Type	Dst Addr	Protocol	Port	Action	Enabled	Options
Dhcp Access	ANY		ANY		udp	67,68	Allow	<input checked="" type="checkbox"/>	
Dns Access	ANY		ANY		any	53	Allow	<input checked="" type="checkbox"/>	
ICMP Access	ANY		ANY		icmp	0	Allow	<input checked="" type="checkbox"/>	
NTP Access	ANY		ANY		udp	123	Allow	<input checked="" type="checkbox"/>	
SSH Access	ANY		ANY		tcp	22	Allow	<input checked="" type="checkbox"/>	
Telnet Access	ANY		ANY		tcp	23	Allow	<input checked="" type="checkbox"/>	
Web Access	ANY		ANY		tcp	80,443,8080,8088	Allow	<input checked="" type="checkbox"/>	

FIREWALL Settings

Global Firewall Settings

TCP Syn Flood Rate:

TCP Syn Flood Burst:

TCP Flood Rate:

TCP Flood Burst:

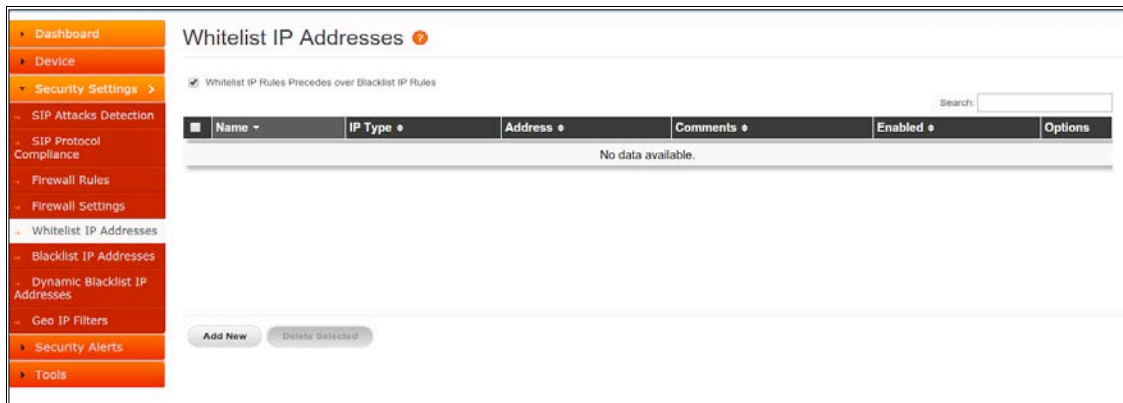
UDP Flood Rate:

UDP Flood Burst:

ICMP Flood Rate:

ICMP Flood Burst:

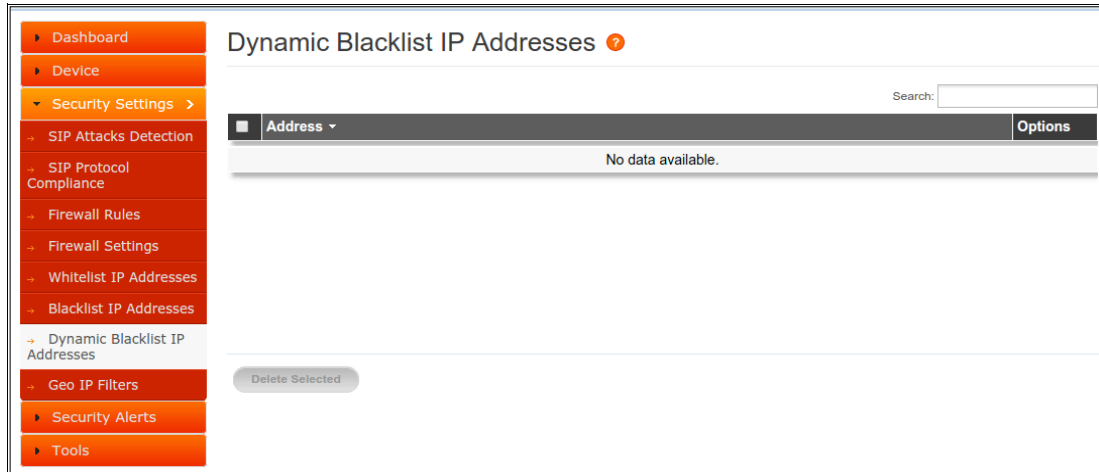
Whitelist IP Addresses, Permite configurar las direcciones IP a la cual se confía desde la red WAN.



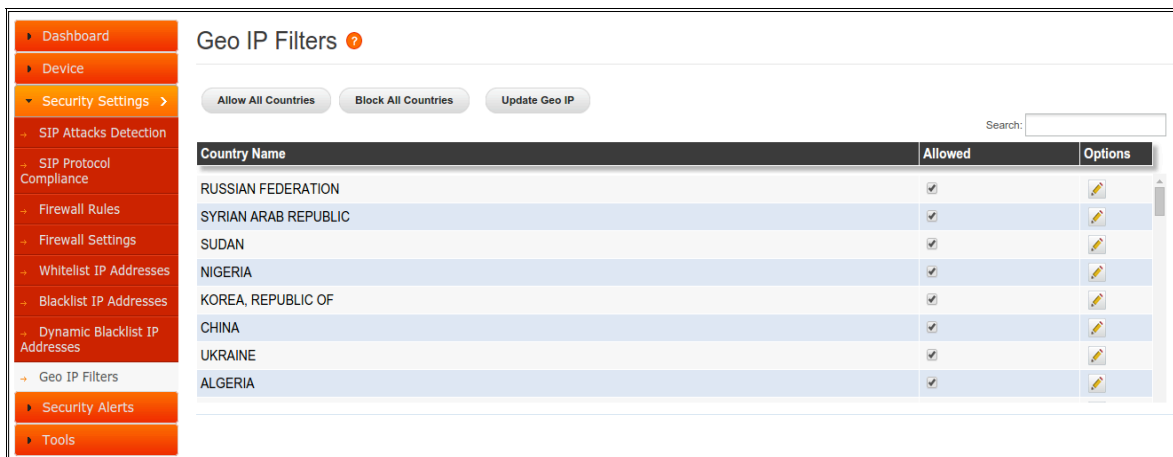
Blacklist IP Addresses, Permite configurar las direcciones IP a la cual no se confía desde la red WAN.



Dynamic Blacklist IP Adresses, Son reglas de bloqueo añadidas por el motor de inspección de paquetes de Elastix SIP FIREWALL.

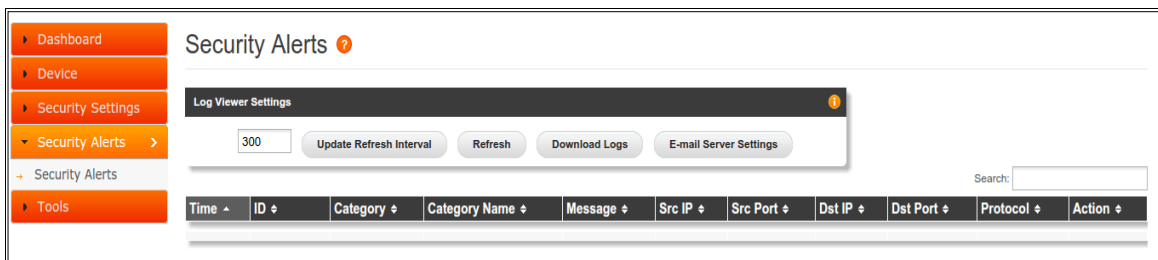


Geo IP Filters, Permite bloquear el tráfico de países en específico, hacia la red SIP protegida.



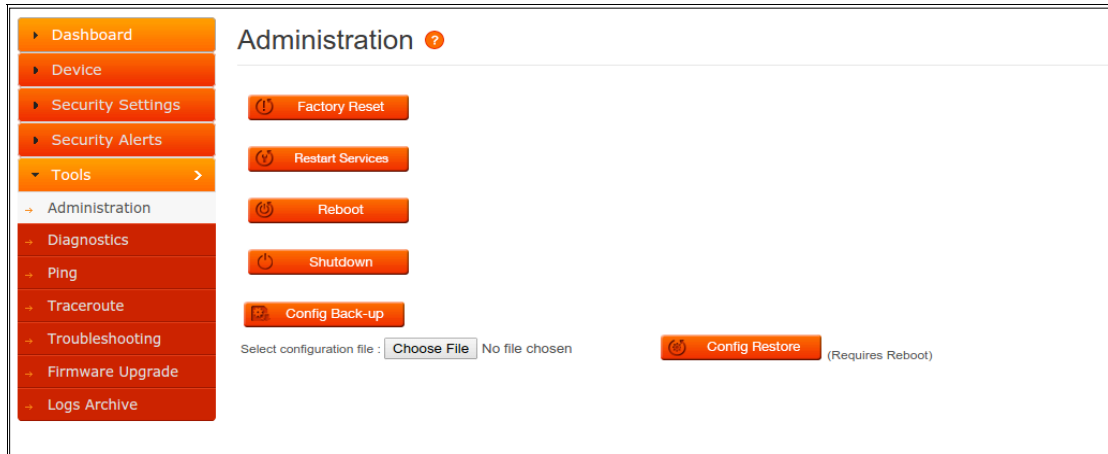
3.3 Security Alerts

Security Alerts, Muestra las alertas detectadas, La tabla muestra Hora, ID, Categoría, Mensaje, IP de origen y el número de puerto, IP destino, puerto y tipo de protocolo.

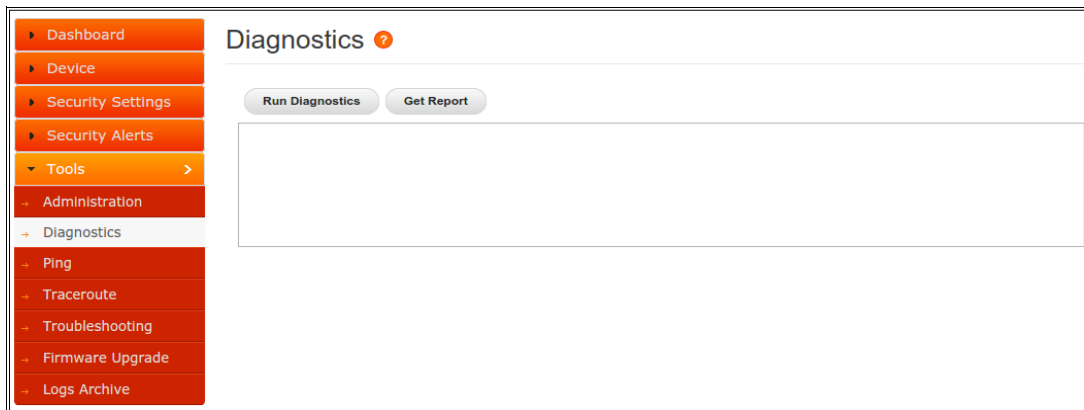


3.4 Tools

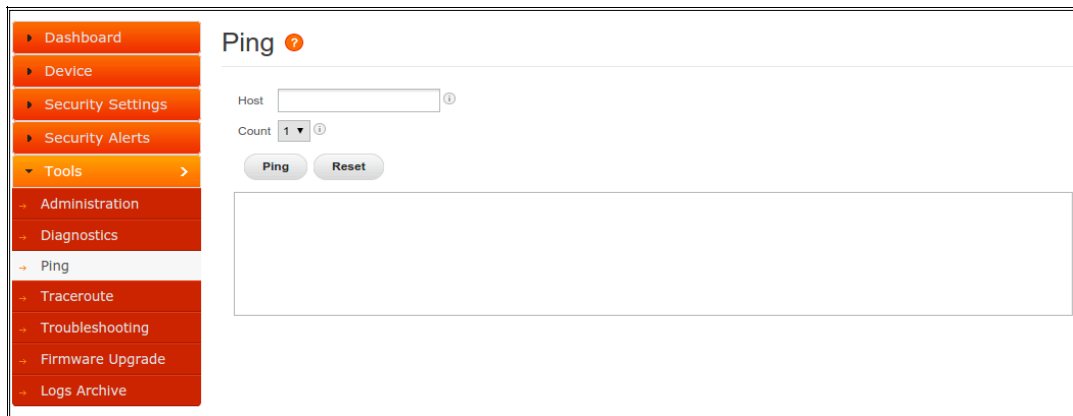
Administration, Permite realizar diversas funciones como, restauración de fábrica, reinicio del sistema, reinicio, apagado, backup y restauración del dispositivo.



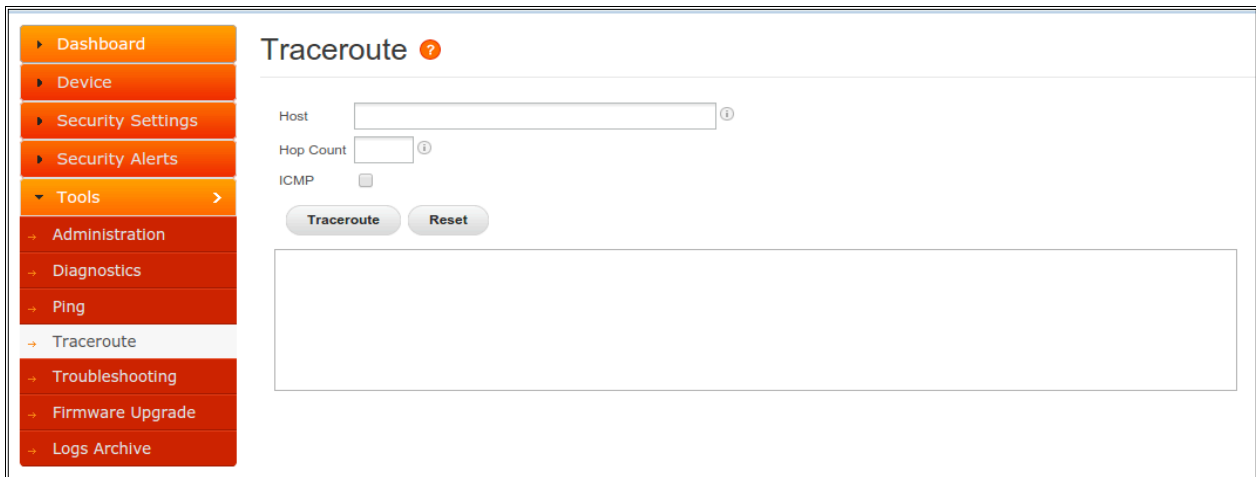
Diagnostics, Permite realizar un test de funcionamiento de Elastix SIP FIREWALL



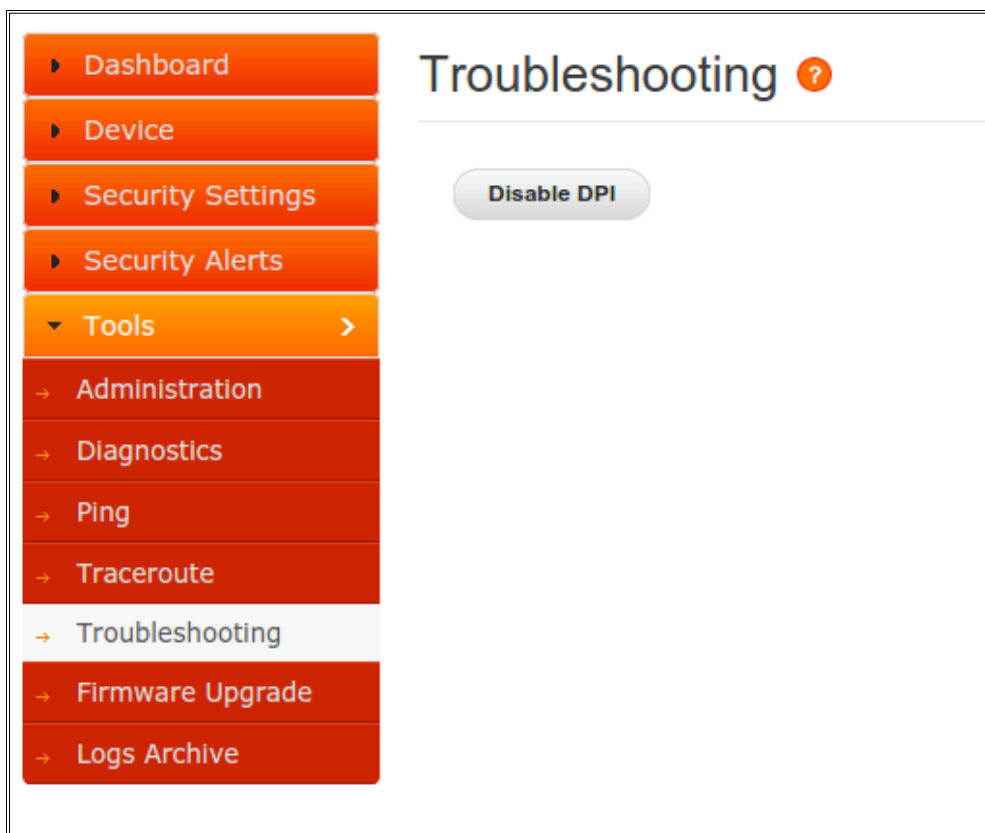
Ping, Permite realizar un ping a un host o domino



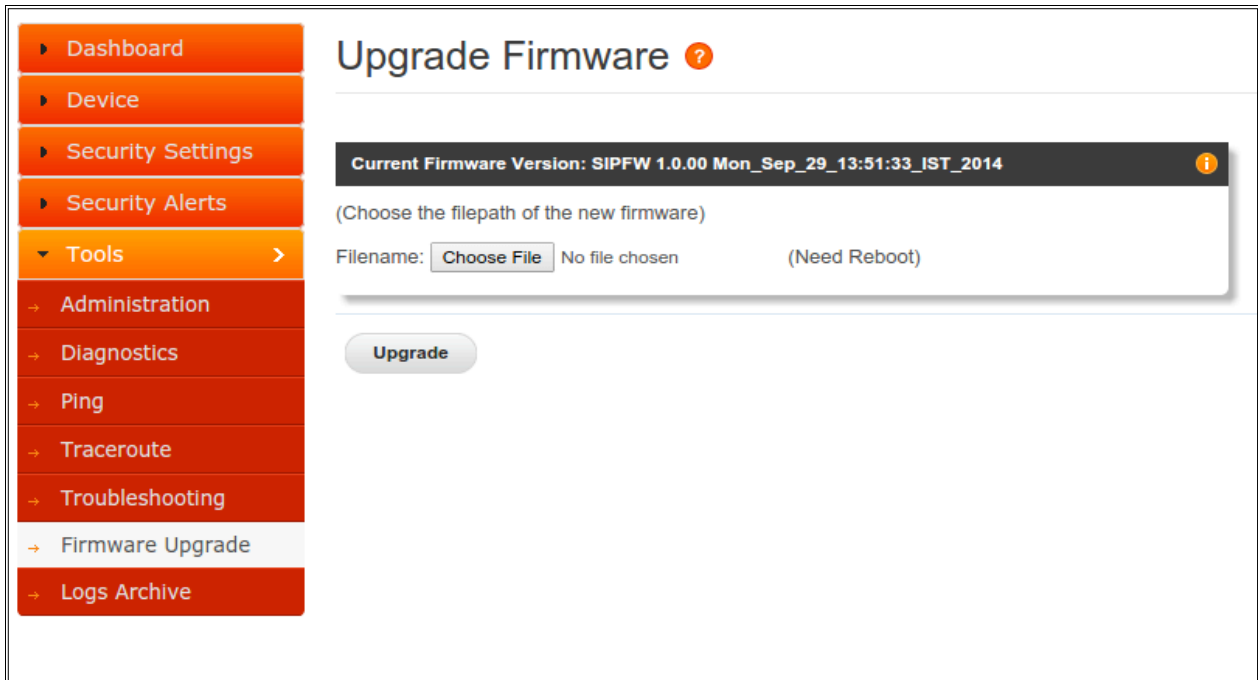
Traceroute, Permite realizar una traza a un host



Troubleshooting, Permite habilitar o deshabilitar DPI



Upgrade Firmware, Permite actualizar el firmware del dispositivo.



Logs Archive, Permite almacenar los registros en un dispositivo USB



4 Configuración y detección de prevención de ataques de Fingerprinting

Para probar si Elastix SIP FIREWALL, detecta ataques de Fingerprinting, se desarrollaran ataques con diferentes herramientas y ver si finalmente el dispositivo bloquea los mismos.

4.1 Desarrollando ataque de fingerprint

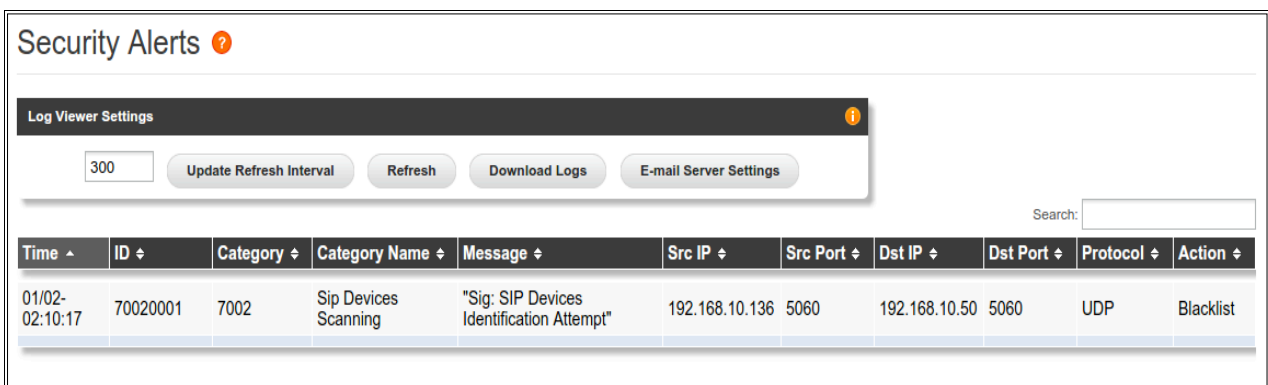
```
#svmap 192.168.10.50
```

Veremos que la respuesta de la herramienta es la siguiente:

```
root@kali:~#  
root@kali:~#  
root@kali:~#  
root@kali:~# svmap 192.168.10.50  
WARNING:root:found nothing  
root@kali:~#  
root@kali:~#  
root@kali:~#
```

4.2 Detección del Ataque.

El dispositivo Elastix SIP FIREWALL detecta el ataque, ingresar a Security Alerts / Security Alerts



The screenshot shows the 'Security Alerts' interface. At the top, there is a 'Log Viewer Settings' section with a '300' value and buttons for 'Update Refresh Interval', 'Refresh', 'Download Logs', and 'E-mail Server Settings'. Below this is a search bar. The main part of the interface is a table with the following columns: Time, ID, Category, Category Name, Message, Src IP, Src Port, Dst IP, Dst Port, Protocol, and Action. A single log entry is visible:

Time	ID	Category	Category Name	Message	Src IP	Src Port	Dst IP	Dst Port	Protocol	Action
01/02-02:10:17	70020001	7002	Sip Devices Scanning	"Sig: SIP Devices Identification Attempt"	192.168.10.136	5060	192.168.10.50	5060	UDP	Blacklist

5 Configuración y detección de ataques de enumeración de usuarios

5.1 Desarrollando ataques de enumeración

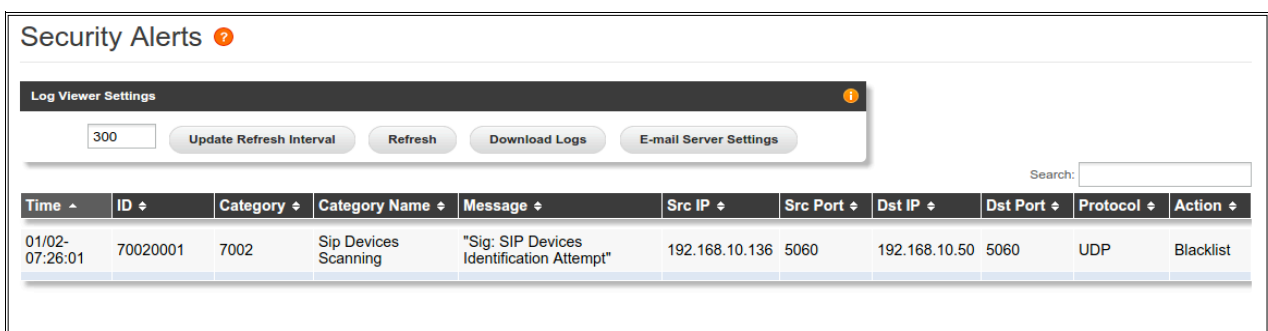
```
#svwar -m INVITE --force 192.168.10.50
```

Veremos que la respuesta de la herramienta es la siguiente:

```
root@kali:~#
root@kali:~#
root@kali:~# svwar -m INVITE --force 192.168.10.50
WARNING:TakeASip:using an INVITE scan on an endpoint (i.e. SIP phone) may cause it to ring and wa
ke up people in the middle of the night
ERROR:TakeASip:socket error: timed out
WARNING:root:found nothing
root@kali:~#
root@kali:~#
root@kali:~#
```

5.2 Detección del Ataque.

El dispositivo Elastix SIP FIREWALL detecta el ataque, ingresar a Security Alerts / Security Alerts



The screenshot shows the 'Security Alerts' interface. At the top, there is a 'Log Viewer Settings' section with a refresh interval set to 300, and buttons for 'Update Refresh Interval', 'Refresh', 'Download Logs', and 'E-mail Server Settings'. Below this is a search bar. The main part of the interface is a table with the following columns: Time, ID, Category, Category Name, Message, Src IP, Src Port, Dst IP, Dst Port, Protocol, and Action. A single log entry is visible:

Time	ID	Category	Category Name	Message	Src IP	Src Port	Dst IP	Dst Port	Protocol	Action
01/02-07:26:01	70020001	7002	Sip Devices Scanning	"Sig: SIP Devices Identification Attempt"	192.168.10.136	5060	192.168.10.50	5060	UDP	Blacklist

6 Configuración y bloqueo de Ataques DoS

6.1 Desarrollando ataques de DOS VoIP

```
#inviteflood eth0 500 192.168.10.136 192.168.10.50 1000000 -a hacker -v
```

6.2 Detección del Ataque.

El dispositivo Elastix SIP FIREWALL detecta el ataque, ingresar a Security Alerts / Security Alerts

Security Alerts ?

Log Viewer Settings i
 Update Refresh Interval Refresh Download Logs E-mail Server Settings

Search:

Time ^	ID ↕	Category ↕	Category Name ↕	Message ↕	Src IP ↕	Src Port ↕	Dst IP ↕	Dst Port ↕	Protocol ↕	Action ↕
01/01-4:-40:-22	70040001	7004	Sip Dos Attacks	"Sig: INVITE flood"	192.168.10.136	9	192.168.10.50	5060	UDP	Blacklist
01/01-4:-40:-22	70040003	7004	Sip Dos Attacks	"Sig: INVITE flood"	192.168.10.136	9	192.168.10.50	5060	UDP	Blacklist

7 Bloqueo de Intentos de obtención de contraseñas o password cracking

7.1 Desarrollando ataques de password cracking

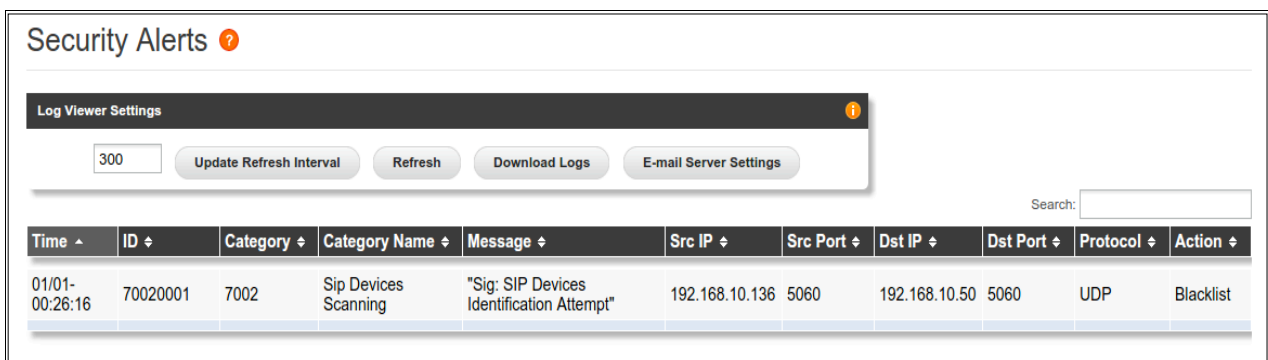
```
#svcrack -u104 192.168.10.50 -d dictionary.txt
```

Veremos que la respuesta de la herramienta es la siguiente:

```
root@kali:~#  
root@kali:~# svcrack -u104 192.168.10.50 -d dictionary.txt  
ERROR:ASipOfRedWine:no server response  
WARNING:root:found nothing  
root@kali:~#
```

7.2 Detección del Ataque.

El dispositivo Elastix SIP FIREWALL detecta el ataque, ingresar a Security Alerts / Security Alerts



Time	ID	Category	Category Name	Message	Src IP	Src Port	Dst IP	Dst Port	Protocol	Action
01/01-00:26:16	70020001	7002	Sip Devices Scanning	"Sig: SIP Devices Identification Attempt"	192.168.10.136	5060	192.168.10.50	5060	UDP	Blacklist

8 Bloqueo de Intentos de ataques de SIP Cross Site Scripting

Elastix SIP FIREWALL, para el caso de detección de ataques Cross Site Scripting o también llamados XSS, hace uso del motor de inspección de paquetes, para detectar códigos maliciosos que viajen vía el servicio/protocolo SIP, es importante referir esto porque los ataques XSS también pueden realizarse hacia servicios como HTTP o HTTPS inclusive.

8.1 Desarrollando ataques de SIP Cross Site Scripting

Para desarrollar esta prueba de concepto, es necesario descargar el archivo “asterisk_cdr_sqlinjection.pl” ubicado en la siguiente dirección url:
http://securityvulns.ru/files/asterisk_cdr_sqlinjection.pl

Una vez descargado en nuestro sistema Kali Linux procedemos a configurar el script de la siguiente forma:

```
#!/asterisk_cdr_sqlinjection.pl 204 192.168.10.251 5060 101 192.168.10.136 5060
```

Donde:

204: Extensión de la central PBX Elastix
192.168.10.251: Dirección IP de la central PBX Elastix
5060: Puerto del protocolo SIP
101: Extensión ficticia del atacante
192.168.10.136: Dirección IP de Kali Linux

Veremos que la respuesta de la herramienta es la siguiente:

```
root@kali:~#  
root@kali:~#  
root@kali:~# ./asterisk_cdr_sqlinjection.pl 204 192.168.10.251 5060 101 192.168.10.136 5060  
root@kali:~#  
root@kali:~#  
root@kali:~#
```

8.2 Detección del Ataque.

El dispositivo Elastix SIP FIREWALL detecta el ataque, ingresar a Security Alerts / Security Alerts

Security Alerts ?

Log Viewer Settings i
 Update Refresh Interval Refresh Download Logs E-mail Server Settings

Search:

Time ^	ID ^	Category ^	Category Name ^	Message ^	Src IP ^	Src Port ^	Dst IP ^	Dst Port ^	Protocol ^	Action ^
12/16-13:08:14	70060011	7006	Sip Cross site scripting Attacks	"Sig:XSS injection attempt"	192.168.10.136	5060	192.168.10.251	5060	UDP	Blacklist

9 Configuración de listas negra dinámica para amenazas VoIP

La funcionalidad “Dynamic Blacklist IP Address” permite el bloqueo pro activo de amenazas a nuestra plataforma Elastix PBX.

Para que está funcionalidad funcione adecuadamente, es necesario configurar SIP FIREWALL, en el mismo segmento de red donde reside Elastix PBX para que pueda realizar el bloqueo adecuadamente.

9.1 Cambiando la dirección IP

Ingresar a Device / General Settings y establecer la dirección IP según el segmento de red que corresponda, hacer clic en el botón “Save” y luego en el botón “Apply Changes”

The screenshot displays the 'Device Settings' configuration window. The settings are as follows:

Field	Value
Host Name	sip_secure
IP Configuration	Static
IP Addr/Mask	192.168.10.252 / 255.255.255.0
Gateway	192.168.10.1
Dns Server	8.8.8.8
Enable SSH	<input checked="" type="checkbox"/>
SSH Port	22
Allow ICMP	<input checked="" type="checkbox"/>
Mgmt Vlan Addr/Mask	192.168.100.1 / 255.255.255.0

Buttons: Save, Cancel

Una vez establecida la dirección IP, ingresar nuevamente desde la nueva dirección.

9.2 Probando el bloqueo pro activo mediante listas negras dinámicas

9.2.1 Verificando conectividad desde el atacante

Realizar pruebas de ping desde el atacante hacia la dirección IP de Elastix PBX

```
root@kali:~#  
root@kali:~#  
root@kali:~# ping 192.168.10.251  
PING 192.168.10.251 (192.168.10.251) 56(84) bytes of data.  
64 bytes from 192.168.10.251: icmp_req=1 ttl=64 time=1.60 ms  
64 bytes from 192.168.10.251: icmp_req=2 ttl=64 time=0.926 ms  
64 bytes from 192.168.10.251: icmp_req=3 ttl=64 time=0.759 ms  
64 bytes from 192.168.10.251: icmp_req=4 ttl=64 time=0.790 ms  
64 bytes from 192.168.10.251: icmp_req=5 ttl=64 time=0.829 ms  
64 bytes from 192.168.10.251: icmp_req=6 ttl=64 time=0.935 ms  
^C  
--- 192.168.10.251 ping statistics ---  
6 packets transmitted, 6 received, 0% packet loss, time 5008ms  
rtt min/avg/max/mdev = 0.759/0.974/1.608/0.292 ms  
root@kali:~# █
```

Como vemos existe conectividad completa

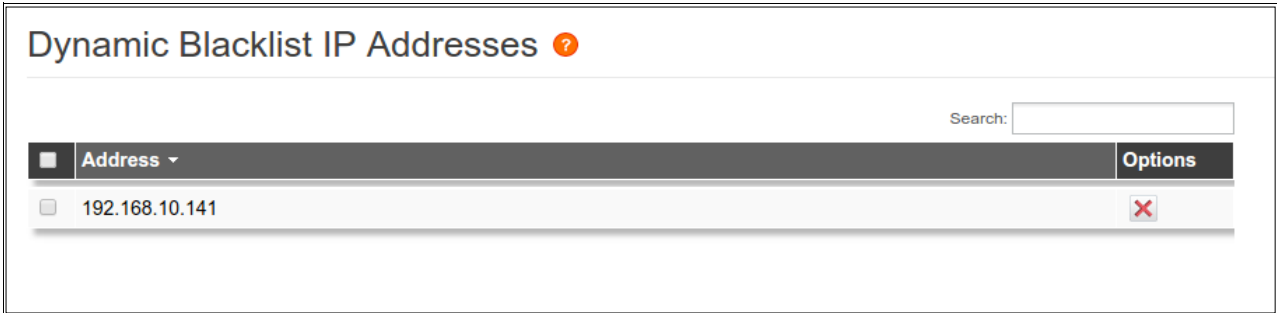
9.2.2 Realizando un ataque de SIP BRUTE FORCE ATTACK

```
root@kali:~#  
root@kali:~#  
root@kali:~# svcrack -u104 192.168.10.251 -d dictionary.txt  
ERROR:ASipOfRedWine:no server response  
WARNING:root:found nothing  
root@kali:~#  
root@kali:~# █
```

Después de unos segundos de realizar el ataque, la herramienta genera un error de conectividad

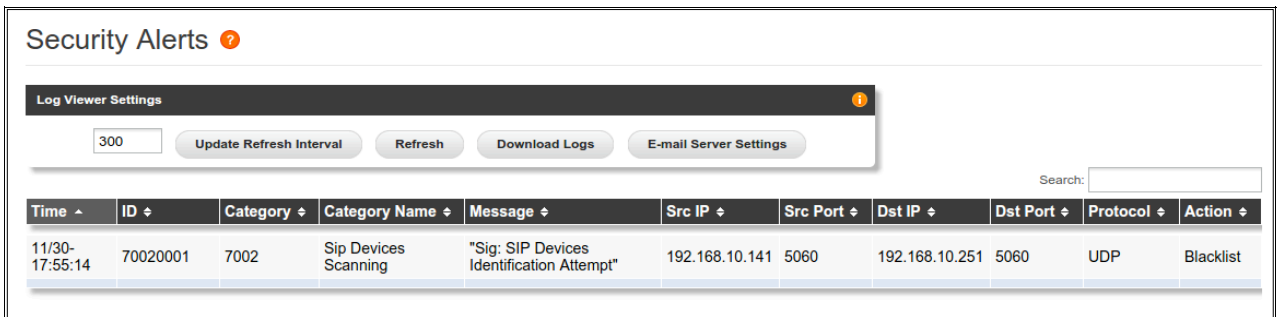
9.2.3 Verificando el bloqueo en SIP FIREWALL

Ingresar a: Security Settings / Dynamic Blacklist IP Address



Veremos que la dirección IP del host atacante en la lista.

En la sección de “Security Alerts” veremos también el evento generado.



Es importante poder identificar el nombre de la categoría con el cual el ataque ha sido identificado.

Adicionalmente no es posible hacer conectividad desde el host atacante hacia la dirección IP de Elastix PBX, como lo vemos a continuación:

```
root@kali:~#
root@kali:~# svcrack -u104 192.168.10.251 -d dictionary.txt
ERROR:ASipOfRedWine:no server response
WARNING:root:found nothing
root@kali:~#
root@kali:~#
root@kali:~#
root@kali:~#
root@kali:~# ping 192.168.10.251
PING 192.168.10.251 (192.168.10.251) 56(84) bytes of data.
^C
--- 192.168.10.251 ping statistics ---
16 packets transmitted, 0 received, 100% packet loss, time 15118ms

root@kali:~#
root@kali:~#
```

10 Configuración de reglas de Blacklist y Whitelist

El objetivo de estas funcionalidades es, poder realizar bloqueo manual de direcciones IP de atacantes (Blacklist) o según sea el caso, agregar direcciones IP que estén siendo detectadas como atacantes en el SIP FIREWALL pero en realidad no lo son, llamados también falsos positivos.


10.1 Agregando direcciones IP al Blacklist.

Ingresar a: Security Settings / Whitelist IP Addresses y hacer clic en el botón “Add New”



The screenshot shows the 'Blacklist IP Addresses' management page. At the top, there is a search bar. Below it is a table with columns: Name, IP Type, Address, Comments, Enabled, and Options. The table is currently empty, displaying 'No data available.' At the bottom left, there are two buttons: 'Add New' and 'Delete Selected'. A red arrow points to the 'Add New' button.

Luego ingresar los parámetros de la siguiente forma:



The screenshot shows the 'Create Blacklist Rule' dialog box. It contains the following fields and options:

- Name: 192-168-10-141
- IP Type: IP_HOST
- Address: 192.168.10.141
- Enable:
- Comments: Dirección IP de atacante

At the bottom right, there are 'SAVE' and 'CANCEL' buttons.

Name: Nombre descriptivo para la regla

IP Type: Es posible realizar bloqueos a nivel de:

Dirección IP (IP_HOST)

Segmento de RED (IP_NETWORK)

Rango de IP (IP_RANGE)

Dirección MAC (MAC_ADDR)

Address: Dirección IP a bloquear

Enable: Establecer si la regla va estar activa o no

Comentario: Comentario descriptivo de la regla.

Una vez creada la regla, hacer clic sobre el botón “APPLY CHANGES” ubicado en la parte superior derecha, como se muestra a continuación.

elastix
SIP FIREWALL

30-November-14 06:45:46 pm SIPFW 1.0.00 Mon_Sep_29_13:51:33_IST_2014 Welcome admin

Dashboard
Device
Security Settings >
SIP Attacks Detection
SIP Protocol Compliance
Firewall Rules
Firewall Settings
Whitelist IP Addresses
Blacklist IP Addresses
Dynamic Blacklist IP Addresses
Geo IP Filters
Security Alerts
Tools

Blacklist IP Addresses

Search:

Name	IP Type	Address	Comments	Enabled	Options
192-168-10-141	IP_HOST	192.168.10.141	Direccion IP del ata	<input checked="" type="checkbox"/>	

Add New Delete Selected

APPLY CHANGES IGNORE CHANGES

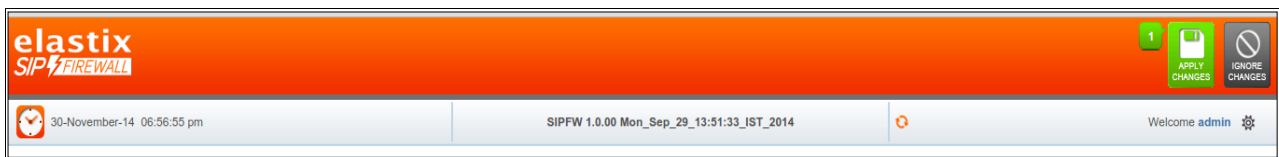
Cuando la regla está grabada correctamente, no será posible establecer conectividad desde la IP bloqueada hacia la dirección IP de ELASTIX PBX, como se muestra a continuación.

```
root@kali:~#  
root@kali:~# ifconfig eth0  
eth0      Link encap:Ethernet  HWaddr 08:00:27:23:60:ec  
          inet addr:192.168.10.141  Bcast:192.168.10.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe23:60ec/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:10325 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:1504 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:1669071 (1.5 MiB)  TX bytes:239951 (234.3 KiB)  
  
root@kali:~# ping 192.168.10.251  
PING 192.168.10.251 (192.168.10.251) 56(84) bytes of data.  
^C  
--- 192.168.10.251 ping statistics ---  
13 packets transmitted, 0 received, 100% packet loss, time 11999ms  
  
root@kali:~#
```

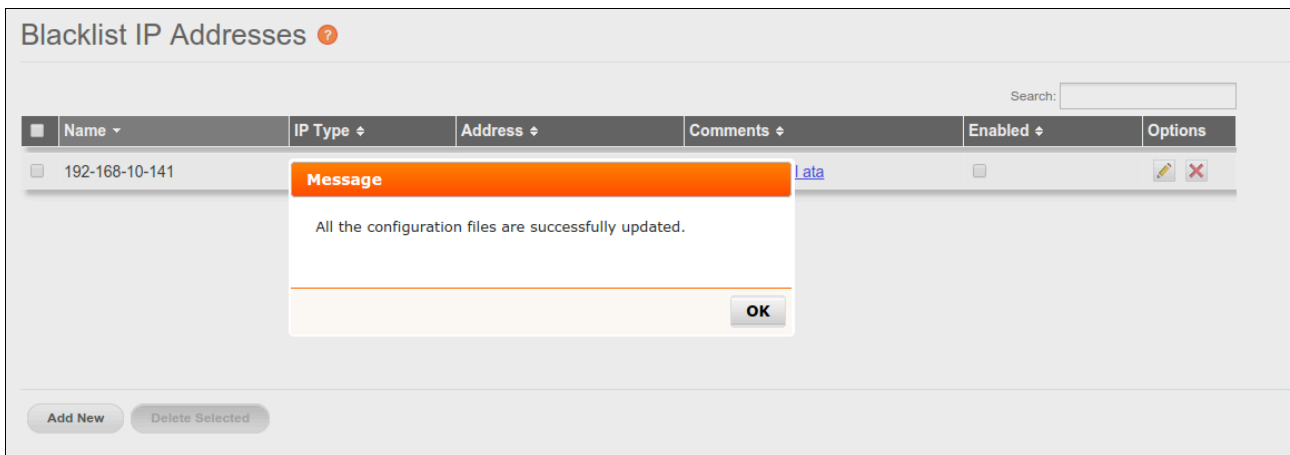

Tener en cuenta que es una regla de bloqueo permanente, hasta que se desactive o elimine la regla según se requiera, de la siguiente forma:



Luego es necesario hacer clic en el botón “APPLY CHANGES”



Finalmente en el botón “OK” como se muestra a continuación:



Finalmente probar si la conectividad se restableció en el host bloqueado.

10.2 Agregando direcciones IP al Whitelist.

Las listas blancas tienen funcionamiento opuesto a las listas negras, y son prioritarias con respecto a las listas dinámicas inclusive.

Ejemplo: crear una regla para evitar el bloqueo de todas las direcciones IP de la red LAN.

Create Whitelist Rule

Name: RED_LAN

Ip Type: IP_NETWORK

Address: 192.168.10.0/24

Enable:

Comments: regla para evitar bloqueo de la red lan

SAVE CANCEL

Whitelist IP Addresses

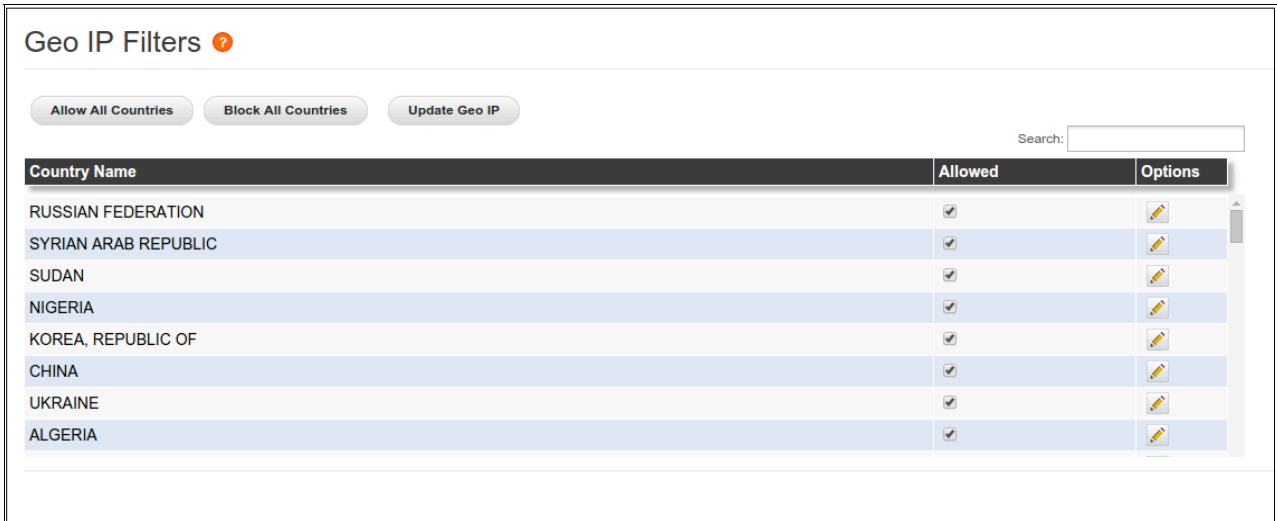
Whitelist IP Rules Precedes over Blacklist IP Rules

Search:

Name	IP Type	Address	Comments	Enabled	Options
<input type="checkbox"/> RED_LAN	IP_NETWORK	192.168.10.0/24	regla para evitar bl	<input checked="" type="checkbox"/>	

11 Configuración de bloqueo por ubicación geográfica

El bloqueo por ubicación geográfica se encuentra en la sección: Security Settings / Geo IP Filters como se muestra a continuación:



Geo IP Filters ?

Allow All Countries Block All Countries Update Geo IP

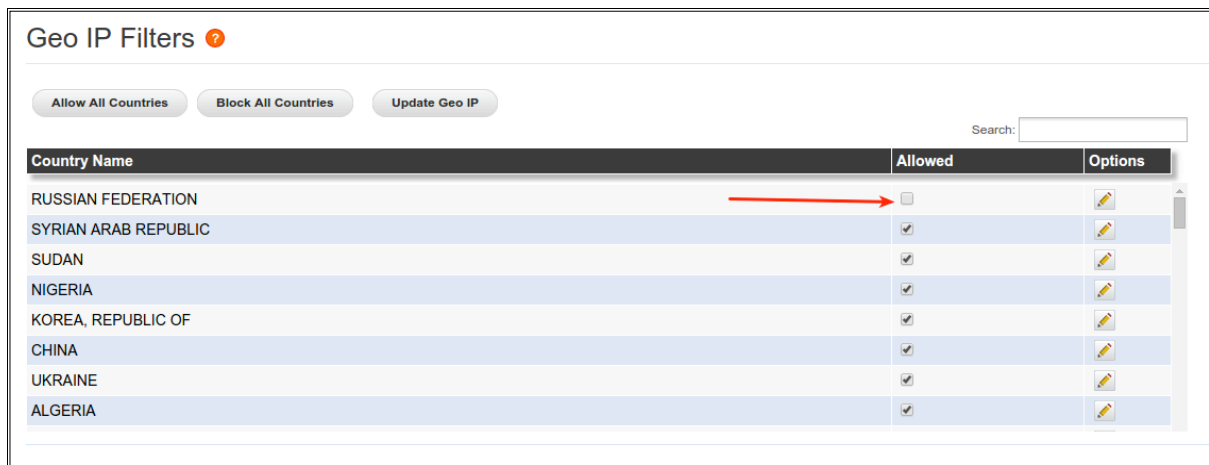
Search:

Country Name	Allowed	Options
RUSSIAN FEDERATION	<input checked="" type="checkbox"/>	
SYRIAN ARAB REPUBLIC	<input checked="" type="checkbox"/>	
SUDAN	<input checked="" type="checkbox"/>	
NIGERIA	<input checked="" type="checkbox"/>	
KOREA, REPUBLIC OF	<input checked="" type="checkbox"/>	
CHINA	<input checked="" type="checkbox"/>	
UKRAINE	<input checked="" type="checkbox"/>	
ALGERIA	<input checked="" type="checkbox"/>	

Por defecto ELASTIX SIP FIREWALL permite todos los países pre configurados en esta sección.

Para bloquear las direcciones IP de todo un país, basta con desactivar la opción “Allowed”

Por ejemplo si deseamos bloquear todas las direcciones IP de RUSIA, como se muestra a continuación:



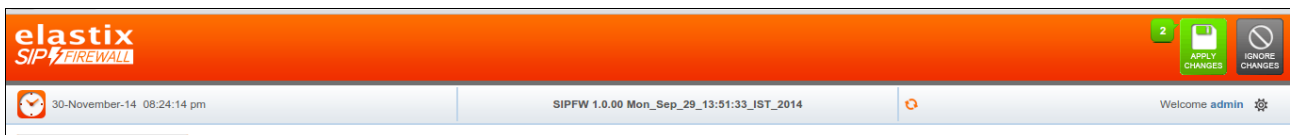
Geo IP Filters ?

Allow All Countries Block All Countries Update Geo IP

Search:

Country Name	Allowed	Options
RUSSIAN FEDERATION	<input type="checkbox"/>	
SYRIAN ARAB REPUBLIC	<input checked="" type="checkbox"/>	
SUDAN	<input checked="" type="checkbox"/>	
NIGERIA	<input checked="" type="checkbox"/>	
KOREA, REPUBLIC OF	<input checked="" type="checkbox"/>	
CHINA	<input checked="" type="checkbox"/>	
UKRAINE	<input checked="" type="checkbox"/>	
ALGERIA	<input checked="" type="checkbox"/>	

Luego hacer clic en “APPLY CHANGES” ubicado en la parte superior derecha.



elastix SIP FIREWALL

30-November-14 08:24:14 pm SIPFW 1.0.00 Mon_Sep_29_13:51:33_IST_2014 Welcome admin

APPLY CHANGES IGNORE CHANGES

12 Configuración de acceso a la administración del dispositivo a una IP/red específica

Es posible configurar que solo sea sea posible ingresar a ELASTIX SIP FIREWALL desde una dirección IP en específico, como lo veremos a continuación.

12.1 Ingresar a Device / Management Access y editar la regla “DefaultAllAccess”




Management Access ?

Search:

Name	IP Type	Address	Comments	Enabled	Options
<input type="checkbox"/> DefaultAllAccess	ANY		Default rule that al	<input checked="" type="checkbox"/>	
<input type="checkbox"/> MgmtVlanAccess	IP_NETWORK	192.168.100.0/24	Access from Mgmt Via	<input checked="" type="checkbox"/>	

12.2 Establecer la dirección IP para administración



Edit Management Access Rule ✕

Name: ⓘ

IP Type: ⓘ

Address: ⓘ

Enable: ⓘ

Comments: ⓘ

Por defecto la regla está establecida para brindar acceso a cualquier dirección IP , en este caso cambiando el valor de IP Type a IP_HOST , es posible establecer la dirección 192.168.10.5 que será la única dirección IP en la RED LAN desde la cual será posible ingresar al dispositivo.

También es posible establecer el acceso según los valores en el parámetro “IP Type”

IP_NETWORK: Segmento de RED

IP_RANGE: Rango de direcciones IP

MAC_ADDR: Dirección MAC

13 Configuración de servidor SYSLOG remoto para registro de eventos.

Elastix SIP FIREWALL permite el envío de los eventos a un servidor de SYSLOG externo, esto es muy importante ya que la correcta monitorización de los eventos es un punto vital en la seguridad.

13.1 Instalación y configuración de SYSLOG Server

Sistema Operativo Centos 6.X
Instalación básica

A.- Configuración de Sistema Operativo

```
#vim /etc/selinux/config
SELINUX=disabled
#chkconfig iptables off
#reboot
```

B.- Instalación de servicios

```
#yum -y install vim wget httpd mysql mysql-server php php-mysql rSYSLOG* --skip-broken
#chkconfig httpd on
#chkconfig mysqld on
#chkconfig rSYSLOG on
#service httpd start
#service mysqld start
#service rSYSLOG start
```

C.- Configuración de base de datos

```
#mysqladmin -u root password '123456'
#mysql -u root -p < /usr/share/doc/rSYSLOG-mysql-5.8.10/createDB.sql
#mysql -u root -p SYSLOG
> GRANT ALL ON SYSLOG.* TO rSYSLOGuser@localhost IDENTIFIED BY 'tucontrasena';
> FLUSH PRIVILEGES;
> exit;
#mysql -u rSYSLOGuser -p SYSLOG
> show tables;
> exit;
```

D.- Configuración de SYSLOG Server

- Des comentar los siguiente parámetros

```
vim /etc/rsyslog.conf

$ModLoad imudp
$UDPServerRun 514
# Provides TCP SYSLOG reception
$ModLoad imtcp
$InputTCPServerRun 514
```

- Agregar los siguientes módulos en el mismo archivo

```
$ModLoad ommysql

*. * :ommysql:127.0.0.1,SYSLOG,rSYSLOGuser, tucontrasena
```

E.- Verificar la integración de SYSLOG server y Mysql

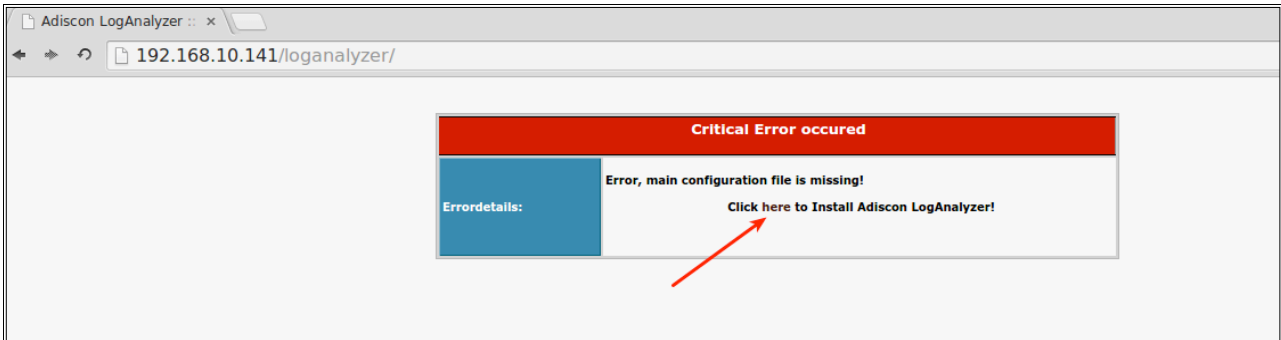
```
#service rsyslog restart
#mysql -u rsysloguser -p SYSLOG
mysql> select count(*) from SystemEvents;
+-----+
| count(*) |
+-----+
|      2 |
+-----+
```

F.- Instalación de LogAnalyzer

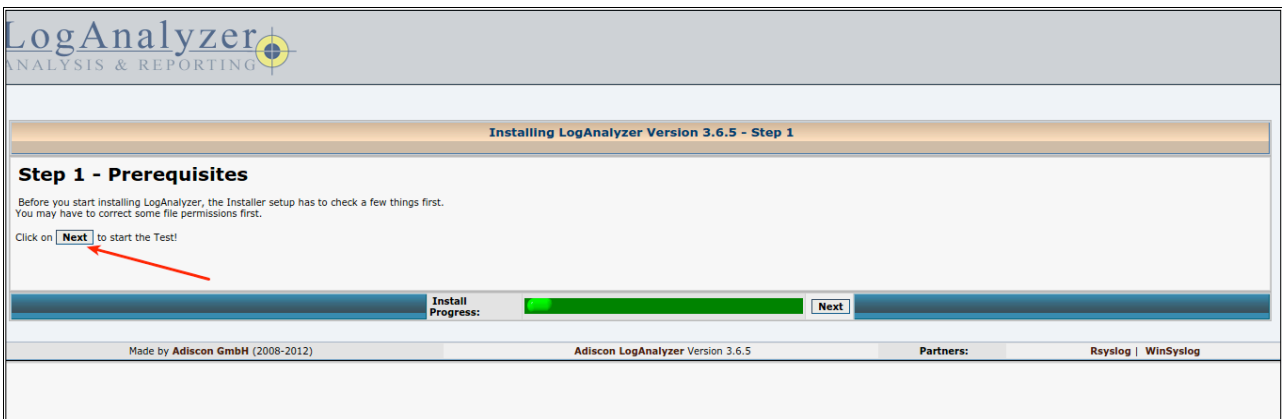
```
#cd /usr/src
#wget http://download.adiscon.com/loganalyzer/loganalyzer-3.6.5.tar.gz
#tar zxvf loganalyzer-3.6.5.tar.gz
#cp -r loganalyzer-3.6.5/src/ /var/www/html/loganalyzer
#cp -r loganalyzer-3.6.5/contrib/* /var/www/html/loganalyzer/
#cd /var/www/html/loganalyzer/
#chmod +x configure.sh secure.sh
#./configure.sh
```

G.- Configuración de LogAnalyzer vía web

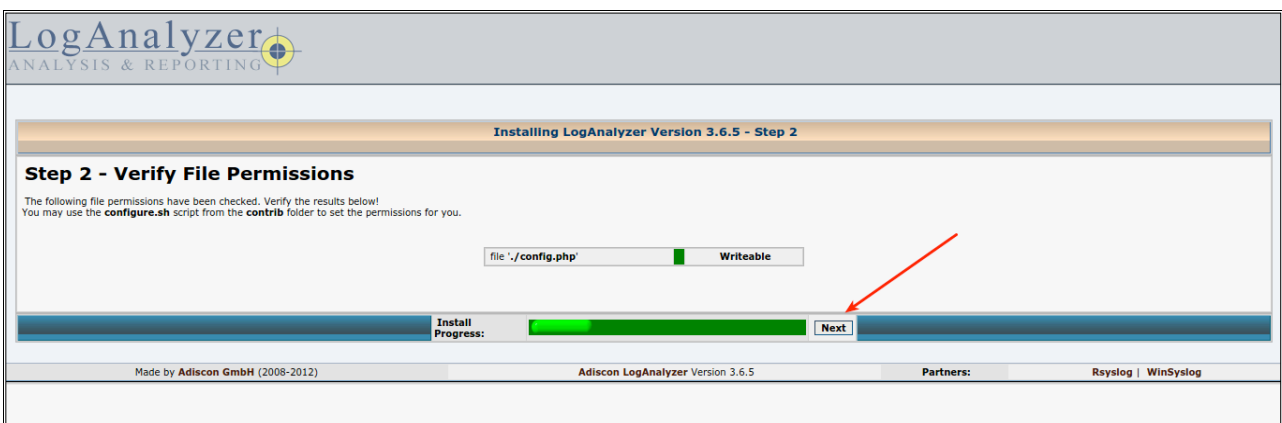
Ingresar desde una navegador web a la dirección: <http://IPCENTOS/loganalyzer> y hacer clic en “here” como se muestra a continuación.



Luego hacer clic en el botón “Next” para iniciar el proceso



Hacer clic en el botón “Next” para continuar el proceso



Configurar el uso de base de datos y luego hacer clic en el botón “Next” de la siguiente forma:

The screenshot shows the configuration interface for LogAnalyzer. It is divided into two main sections: "Frontend Options" and "User Database Options".

Frontend Options:

- Number of syslog messages per page: 50
- Message character limit for the main view: 80
- Character display limit for all string type fields: 30
- Show message details popup: Yes No
- Automatically resolved IP Addresses (inline): Yes No

User Database Options:

- Enable User Database: Yes No (indicated by a red arrow)
- A MySQL database Server is required for this feature. Other database engines are not supported for the User Database System. However for logsources, there is support for other database systems.
- Database Host: localhost
- Database Port: 3306
- Database Name: Syslog (indicated by a red arrow)
- Table prefix: logcon_ (indicated by a red arrow)
- Database User: rsysloguser (indicated by a red arrow)
- Database Password: ***** (indicated by a red arrow)
- Require user to be logged in: Yes No (indicated by a red arrow)
- Authentication method: Internal authentication

At the bottom, there is an "Install Progress" bar and a "Next" button.

Hacer clic en el botón “Next” para la creación de las tablas de la siguiente forma:

The screenshot shows the "Step 4 - Create Tables" screen of the LogAnalyzer installation. The title bar reads "Installing LogAnalyzer Version 3.6.5 - Step 4".

Step 4 - Create Tables

If you reached this step, the database connection has been successfully verified!

The next step will be to create the necessary database tables used by the LogAnalyzer User System. This might take a while!

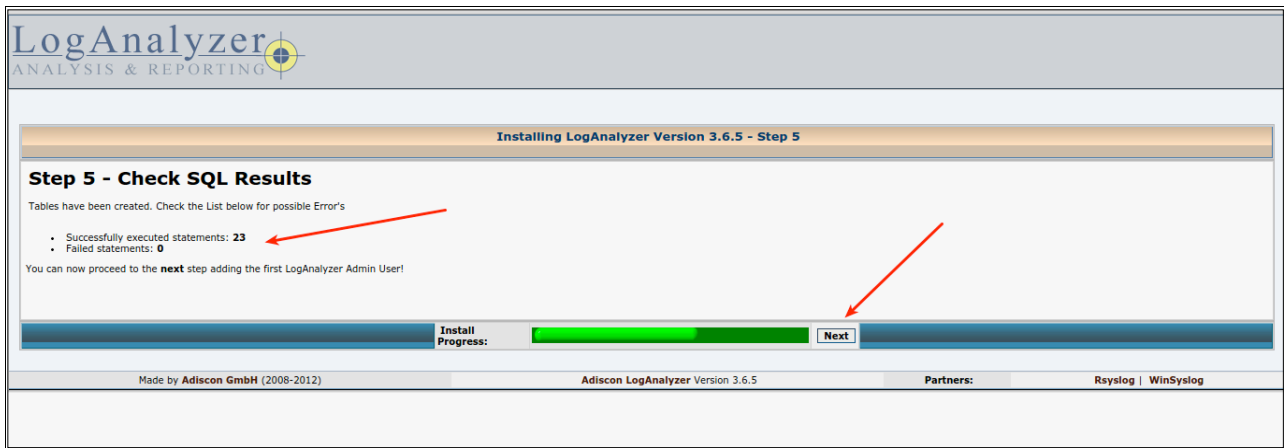
WARNING, if you have an existing LogAnalyzer installation in this database with the same tableprefix, all your data will be **OVERWRITTEN!** Make sure you are using a fresh database, or you want to overwrite your old LogAnalyzer database.

Click on **Next** to start the creation of the tables (indicated by a red arrow).

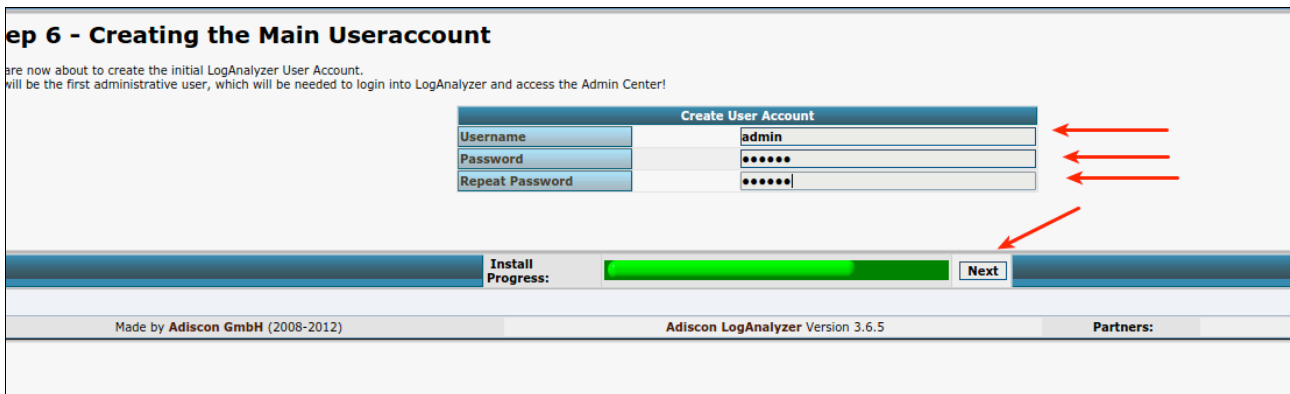
At the bottom, there is an "Install Progress" bar and a "Next" button.

Footer information: Made by Adiscon GmbH (2008-2012), Adiscon LogAnalyzer Version 3.6.5, Partners: Rsyslog | WinSyslog

Una vez creadas las tablas correctamente, hacer clic en el botón “Next” para continuar.



Ahora indicar el usuario con el cual se accederá a la interface web de LogAnalyzer, luego hacer clic para continuar el proceso.




Ahora crear el origen de mensajes para el servidor, configurar los valores de la siguiente forma y hacer clic en “Next”

Successfully created User 'admin'.

Source for syslog messages

First Syslog Source	
Name of the Source	My Syslog Source
Source Type	MYSQL Native
Select View	Syslog Fields

Database Type Options	
Table type	MonitorWare
Database Host	localhost
Database Name	Syslog
Database Tablename	SystemEvents
Database User	rsysloguser
Database Password	*****
Enable Row Counting	<input checked="" type="radio"/> Yes <input type="radio"/> No

Install Progress:  **Next**

©2012) Adiscon LogAnalyzer Version 3.6.5 Partners:

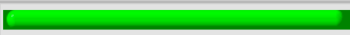
Una vez creado el origen de mensajes, hacer clic en el botón “Next” para finalizar la instalación

Installing LogAnalyzer Version 3.6.5 - Step 8

Step 8 - Done

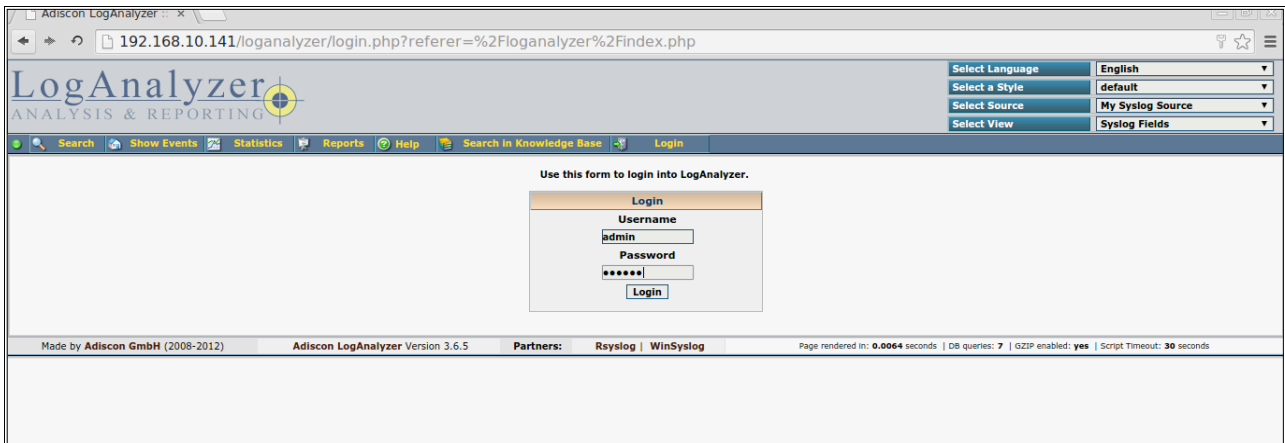
Congratulations! You have successfully installed LogAnalyzer :))

Click [here](#) to go to your installation.

Install Progress:  **Finish!**

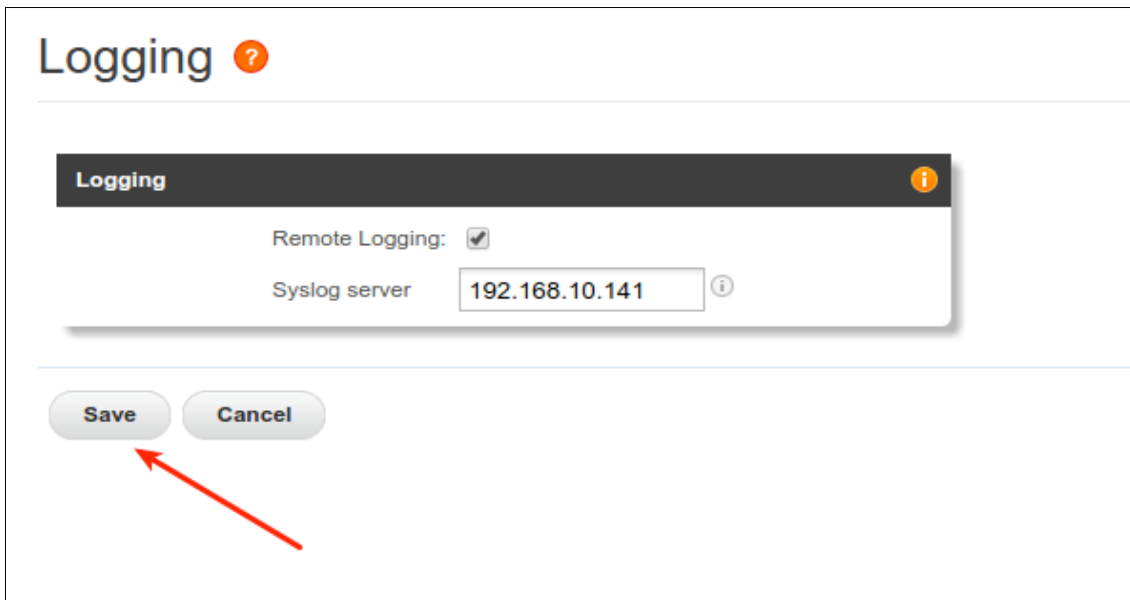
Made by Adiscon GmbH (2008-2012) Adiscon LogAnalyzer Version 3.6.5 Partners: Rsyslog | WinSyslog Page rendered in: 0.0125 seconds | DB queries: 85 | GZIP

Luego ingresar con las credenciales creadas previamente, como se muestra a continuación.

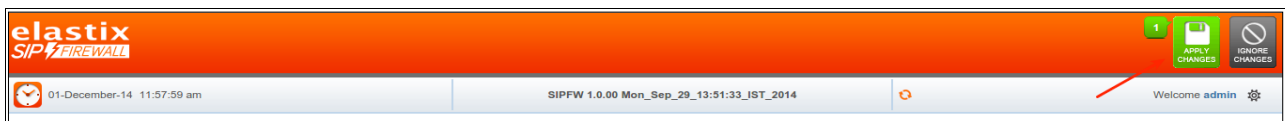


13.2 Configuración un servidor de SYSLOG externo en Elastix SIP FIREWALL

Ingresar a Device / Logging y establecer la dirección IP del servidor externo de la siguiente forma:



Finalmente, aplicar los cambios con el botón “APPLY CHANGES” como se muestra a continuación



13.3 Probar la integración de Elastix SIP FIREWALL y Servidor SYSLOG externo.

Para probar que los eventos del SIP FIREWALL, es enviado al servidor SYSLOG, realizar un ataque contra la dirección IP de Elastix PBX, de la siguiente forma:

```
root@kali:~#  
root@kali:~# svcrack -u104 192.168.10.251 -d dictionary.txt  
ERROR:ASip0fRedWine:no server response  
WARNING:root:found nothing  
root@kali:~#
```

Luego en el Servidor SYSLOG se generará un evento de la siguiente forma:

Date	Facility	Severity	Host	Syslogtag	ProcessID	Message
Today 12:07:23	USER	ALERT	192.168.10.252	snort[901]:	Syslog	[7002:70020001:1] Sig: SIP Devices Identification Attempt [Classification: Sip ...
Today 12:01:01	CRON	NOTICE	monitor	anacron[1556]:		
Today 12:01:01	CRON	NOTICE	monitor	anacron[1556]:		
Today 12:01:01	CRON	NOTICE	monitor	anacron[1556]:		
Today 12:01:01	CRON	NOTICE	monitor	run-parts(/etc/cron.hourly)[15...		
Today 12:01:01	CRON	NOTICE	monitor	anacron[1556]:		
Today 12:01:01	CRON	NOTICE	monitor	anacron[1556]:		
Today 12:01:01	CRON	NOTICE	monitor	run-parts(/etc/cron.hourly)[15...		
Today 11:46:36	USER	INFO	monitor	CROND[1547]:		
Today 11:46:00	SYSLOG	INFO	monitor	yum[1481]:		
Today 11:46:00	KERN	INFO	monitor	rsyslogd:		
Today 11:46:00	KERN	INFO	monitor	kernel:		

Como vemos se generó un evento de tipo ALERT desde la dirección IP de Elastix SIP FIREWALL