



## XVI FORUM DE CIENCIA Y TECNICA 2DA ETAPA

**TITULO:** Una plataforma para la supervisión y el control activo de la Red

**AUTOR:** Alberto Bello Espinosa.

**COAUTORES:** Franklin Manzano Rodríguez

Martín Jodar Velásquez

**CENTRO DE PROCEDENCIA:** Filial de Tecnología y Software, Las Tunas.

**Organismo:** ETECSA

**Sindicato:** Informática y Comunicaciones.

**Municipio:** Las Tunas

**Provincia:** Las Tunas

**Código de la ponencia:** 1050354

**Año de presentación:** 2006

## INDICE

INTRODUCCION .....	4
DESARROLLO .....	5
INSTALACION DEL SERVIDOR PROXY .....	7
INSTALACION DE IPTABLES.....	8
requiera.INSTALACIÓN DEL SISTEMA STILLSECURE® BORDER GUARD .....	10
INSTALACIÓN DEL SISTEMA STILLSECURE® BORDER GUARD .....	11
VALORACION ECONOMICA.....	12
CONCLUSIONES .....	13
RECOMENTACIONES .....	14
BIBLIOGRAFIA .....	15
ANEXO # 1 .....	16
ANEXO # 2 .....	17
ANEXO # 3 .....	18
ANEXO # 4 .....	20
DATOS DEL AUTOR.....	21
CARTA DE PARTICIPACION .....	22

## RESUMEN

**TITULO:** Una plataforma para la supervisión y el control activo de la Red

**AUTOR:** Alberto Bello Espinosa.

Este trabajo consiste en la implementación a partir de herramientas de software libre de un sistema Firewall-Proxy y analizador de tráfico a la vez de manera transparente, que nos permite ponerlo en cualquier intranet para controlar y supervisar todo el tráfico que sale y entra hacia esa intranet, también puede ponerse para controlar y supervisar el tráfico generado hacia servidores importantes en nuestra red, todo esto sin tener que hacer ningún cambio en el direccionamiento, en la infraestructura de la red, en la configuración de los servicios que se brindan a los clientes, ni en las máquinas de los mismos, con este sistema podemos desde cualquier parte de la red obtener informes sobre los sitios hacia los que estén navegando los usuarios, denegar cualquier sitio que se este utilizando indebidamente, denegar el acceso a cualquier servicio dentro y fuera de la red a determinado usuario que haga uso indebido del mismo, se obtienen informes sobre el tráfico hacia cualquier servicio que brindemos, se puede detectar y controlar los virus informáticos por tráfico y por puertos, con este sistema se puede tener un control total de una intranet sin que los usuarios detecten que el mismo esta realizando estas funciones pues no los afecta en nada, se puede cambiar automáticamente el Proxy que se va a usar en la red si tener que cambiar la configuración de las máquinas y sin que los usuarios tengan que cambiar nada.

# INTRODUCCION

La resolución 8 del presidente establece las medidas de control para el uso adecuado de nuestras redes de datos en ella entre otras se expresa:

Proponer e implementar las soluciones técnicas para impedir a trabajadores que brindan servicio a los clientes externos, (Ej. Oficinas Comerciales y Call Center, otros), siempre que no se vea afectado su trabajo, la navegación en sitios que no pertenezcan a la intranet de ETECSA

Presentar el Plan de Implementación de mecanismos de auditorias que permitan el registro de los eventos que se producen en nuestras redes.

Como parte del cumplimiento de estas medidas y de la política de nuestro país de elevar el control y supervisión de las redes de datos, para eliminar algunas manifestaciones de indisciplinas e ilegalidades que empañan el uso adecuado de los recursos que el estado ha puesto en nuestras manos, nos dimos a la tarea de buscar soluciones tecnológicas que permitieran cumplir con estos objetivos , sin afectar la configuración que hasta el momento tienen todas nuestras maquina y mantener la infraestructura de la red y el direccionamiento de la misma, evitando así algún cambio que pudiera afectar los servicios que brindamos a nuestros usuarios, la solución fue la instalación y puesta a punto de un Firewall-Proxy transparente.

# DESARROLLO

Para la implementación del Firewall-Proxy transparente se utilizó el sistema operativo Linux Centos 4.3 con kernel 2.6 el Proxy Squid 2.5, y el firewall Iptables

Primeramente empezaremos por exponer los conceptos básicos.

Un Bridge es un componente de red que une dos segmentos de red de cualquier tipo (Ethernet, Token Ring etc.) de modo transparente para formar una subred. De modo transparente significa que usted no necesita decirle a los componentes de la red (Máquinas, Aplicaciones Etc.) que hay un nuevo dispositivo entre ellos, por lo tanto no se necesita configuración adicional en los mismos. Este es realmente seguro pues no necesita IP para configurarse. Esto puede verse en la siguiente figura1

Los paquetes son reenviados basados en la ethernet address no en la IP como lo hacen los router, este reenvío se hace basado en la capa 2 del modelo de la OSI. Todos los protocolos atraviesan transparentemente el Bridge.

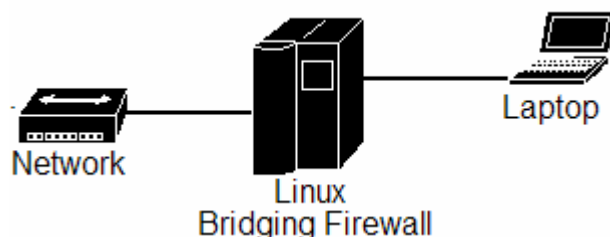


Figura 1 Linux como Bridge

Un firewall es un dispositivo que filtra el tráfico entre redes, como mínimo dos. El firewall puede ser un dispositivo físico o un software sobre un sistema operativo. En general debemos verlo como una caja con DOS o más interfaces de red en la que se establecen una reglas de filtrado con las que se decide si una conexión determinada puede establecerse o no. Incluso puede ir más allá y realizar modificaciones sobre las comunicaciones, como el NAT.

Esa sería la definición genérica, hoy en día un firewall es un hardware específico con un sistema operativo o una IOS que filtra el tráfico TCP/UDP/ICMP/.../IP y decide si un paquete pasa, se modifica, se convierte o se descarta. Para que un firewall entre redes funcione como tal debe tener al menos dos tarjetas de red.

Esta sería la tipología del Firewall Montado:

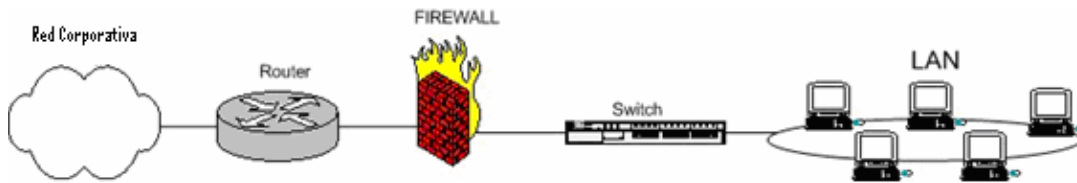


Figura 2: esquema de firewall entre red local y la red corporativa

Este esquema utilizado es un esquema típico de firewall para proteger una red local conectada a Internet a través de un router. El firewall debe colocarse entre el router (con un único cable) y la red local (conectado al switch o al hub de la LAN)

Iptables es un sistema de firewall vinculado al kernel de Linux que se ha extendido enormemente a partir del kernel 2.4 de este sistema operativo. Un firewall de iptables no es como un servidor que lo iniciamos o detenemos, y nunca tendrá tanto peligro como las aplicaciones que escuchan en determinado puerto TCP): iptables está integrado con el kernel, es parte del sistema operativo. ¿Cómo se pone en marcha? Realmente lo que se hace es aplicar reglas. Para ellos se ejecuta el comando iptables, con el que añadimos, borramos, o creamos reglas. Por ello un firewall de iptables no es sino un simple script de shell en el que se van ejecutando las reglas de firewall.

Un Proxy webcache es una computadora que se sitúa entre su red local e Internet usualmente en el gateway, el trabajo de este es capturar todas las páginas que los clientes de su red visitan y guardarla en cache de manera que la segunda vez que un cliente la pida el Proxy la tenga y se la envíe al cliente, esto permite reducir el ancho de banda.

Pasos que se siguieron para la instalación del sistema.

1. Se seleccionó un servidor Pentium 4 A 2.8 GHZ con 256mb de memoria y 17 GB de disco duro y 2 tarjetas de red
2. instalo el sistema operativo Linux Centos 4.3 con kernel 2.6
3. Se iniciaron las dos tarjetas de red eth0 y eth1 sin direcciones IP y se creó y configuró la interface bridge br0 adicionando las 2 tarjetas, en este caso se le puso dirección IP a la Bridge por motivos de administración de la máquina pudiera no ponerse y así no sería alcanzable de la red externa
  - Con esto tenemos un dispositivo que reenvía el tráfico de una tarjeta a otra de modo transparente, por lo que al ponerlo entre la red y el router es totalmente transparente.

# INSTALACION DEL SERVIDOR PROXY

- Se instalo el Proxy Squid 2.5 con autenticación NTLM, esto permite autenticar a los usuarios contra el servidor de dominio, para los usuarios que están dentro del dominio esto es totalmente transparente ya que no necesitan autenticarse, esto nos permite obtener las trazas por usuarios.
- Se aplicaron las reglas de control de acceso siguiente.
- Se permitió todo el dominio etecsa.cu para que el Proxy lo resuelva de manera directa.
- Todo lo demás será enviado al Proxy nacional para que este lo resuelva, siempre y cuando no este denegado en nuestro Proxy, haciendo cache de todas las páginas.
- Se denegó el uso de los vínculos en las páginas que dan servicio de postales y correo electrónico internacional.
- Aquí se pondrá una regla para que las máquinas que atienden directamente al publico solo tengan acceso a la intranet de etecsa.
- Se podrá filtrar cualquier trafico http que se desee en dependencia de la IP o la dirección MAC en el caso que sea necesario.
- Las direcciones de Internet se machean con la Dirección Mac y se dejan pasar a través del firewall directamente al Proxy nacional

## 4. Instalación del sarg.

Este programa nos permites a partir de los Log del squid generar varios reportes en formato html, para esto se configuro el servidor http en el propio Linux y este pone las paginas en este servidor.

Los reportes que nos da el sarg son.

- Sitios accedidos por cada usuario.
- Los sitios mas accedidos por lo usuarios.
- Las páginas bajadas por usuarios.
- Cantidad de byte bajados por cada usuario.
- Relación de usuarios en un fichero que han bajados mas de una determinada cantidad de MB

En el anexo # 1 se pueden observar imágenes de los reportes antes mencionados

# INSTALACION DE IPTABLES

Con el iptables se revisa todo el Tráfico desde la red y hacia la red, permitiendo filtrar cualquier trafico en función de la dirección IP, de la MAC , del puerto de origen o destino.

La política que debe utilizarse es denegar todo primero y después ir permitiendo lo estrictamente necesario. Primeramente se eliminaron el Spoofing de las direcciones de Internet de manera que solo puede salir con la dirección IP de Internet la máquina a la cual le fue asignada y esto se filtra por la Mac de la tarjeta.

Para esto también se instalo y configuro al programa arpwatrch para cuando un usuario cambie de IP o de mac envía un mensaje y un beeper a los administradores.

Se definieron además reglas para que las direcciones de Internet pasaran a través de firewall hacia el Proxy nacional

```
$IPTABLES -t nat -A PREROUTING -p tcp -m tcp -m mac --mac-source 00:11:d8:2c:f0:d7 -s 192.168.22.43 -d 192.168.91.20 --dport 3128 -j DNAT --to-destination 92.168.91.20:3128
```

Todo el trafico http que resta para el Proxy nacional es redirigido al Proxy local de manera que no se necesita cambiar ninguna configuración en las máquinas, esto es lo que hace que el Proxy sea transparente, para esto se usa la siguiente regla.

```
-A PREROUTING -d 192.168.91.20 -i br0 -p tcp -m tcp --dport 3128 -j REDIRECT --to-ports 3128
```

Para la configuración del firewall se instalo el firewallbuilder un programa sobre Windows que permite en un ambiente grafico y amigable escribir las reglas y compilarlas para iptables, este programa tiene objetos predefinidos pero también se pueden agregar nuevos, lo que lo hace muy flexible, después que se compilan el programa detecta si hay reglas repetidas y luego se instalan directamente en el servidor Linux a través de la red con el protocolo SSH.

En el anexo # 2 podemos observar imágenes de este programa y sus reglas.

Como supervisar el Firewall se hace Log solo de los paquetes denegados y se monto el programa **fwlogwath** que nos permite obtener a través de una pagina html los Log del Firewall, obteniendo los paquetes que han sido denegados ordenados por puerto, o por dirección de origen o destino, así como los paquetes denegados hacia un puerto especifico o una dirección especifica, permitiendo detectar cualquier ataque a la red o el ataque de algún virus por el trafico generado, al poner esta pagina automáticamente en el servidor web, permite que desde cualquier parte de la red se puedan obtener estos informes.

En el anexo # 4 se observa una imagen de una página obtenida.



## 5. Se instalo el iptraf que permite auditar todo el tráfico que pasa hacia y desde la red dando los siguientes reportes.

### ➤ Trafico por protocolo por una interface o por todas las interfaces

**\*\*\* Detailed statistics for interface eth0, generated Tue Apr 25 11:13:58 2006**

```
Total:      1361 packets, 578125 bytes
            (incoming: 730 packets, 110768 bytes; outgoing: 631 packets, 467357 bytes)
IP:        1328 packets, 556010 bytes
            (incoming: 704 packets, 97755 bytes; outgoing: 624 packets, 458255 bytes)
TCP:       993 packets, 525969 bytes
            (incoming: 493 packets, 79207 bytes; outgoing: 500 packets, 446762 bytes)
UDP:       308 packets, 28417 bytes
            (incoming: 203 packets, 18056 bytes; outgoing: 105 packets, 10361 bytes)
ICMP:      21 packets, 1264 bytes
            (incoming: 8 packets, 492 bytes; outgoing: 13 packets, 772 bytes)
```

Average rates:

```
Total:      165.18 kbits/s, 48.61 packets/s
Incoming:   31.64 kbits/s, 26.07 packets/s
Outgoing:   133.50 kbits/s, 22.54 packets/s
```

Peak total activity: 262.52 kbits/s, 58.00 packets/s

Peak incoming rate: 48.52 kbits/s, 28.60 packets/s

Peak outgoing rate: 237.37 kbits/s, 29.60 packets/s

### ➤ Trafico total por cada interface

**\*\*\* General interface statistics log generated Tue Apr 25 11:13:24 2006**

lo: 36 total, 36 IP, 0 non-IP, 0 IP checksum errors, average activity 0.71 kbits/s, peak activity 5.00 kbits/s, last 5-second activity 0.00 kbits/s

eth0: 1817 total, 1779 IP, 38 non-IP, 0 IP checksum errors, average activity 154.17 kbits/s, peak activity 488.60 kbits/s, last 5-second activity 47.20 kbits/s

eth1: 1359 total, 1326 IP, 33 non-IP, 0 IP checksum errors, average activity 97.37 kbits/s, peak activity 251.60 kbits/s, last 5-second activity 43.00 kbits/s

### ➤ Trafico IP por una interface o total permitiendo definir filtros para monitorear una conexión específica de una maquina a otra o de un servicio a otro.

```
Tue Apr 25 11:10:16 2006; ***** IP traffic monitor started *****
Tue Apr 25 11:10:16 2006; UDP; eth0; 75 bytes; source MAC address 000bcdcf3776; from
192.168.22.11:1042 to 192.168.91.4:53
Tue Apr 25 11:10:16 2006; UDP; eth0; 78 bytes; source MAC address 00a0c9cde9ce; from
192.168.22.5:137 to 192.168.22.255:137
Tue Apr 25 11:10:16 2006; TCP; eth0; 48 bytes; from 192.168.22.75:2301 to 10.1.0.4:80
(source MAC addr 00018040b5e9); first packet (SYN)
Tue Apr 25 11:10:16 2006; TCP; eth0; 41 bytes; from 192.168.90.52:1433 to
192.168.22.7:3465 (source MAC addr 000f24018870); first packet
Tue Apr 25 11:10:18 2006; TCP; eth0; 46 bytes; from 192.168.22.2:110 to
192.168.235.149:1861 (source MAC addr 000bcd4efa06); FIN sent; 7 packets, 524 bytes, avg
flow rate 0.00 kbits/s
```

## ➤ **Trafico por dirección MAC**

\*\*\* LAN traffic log, generated Tue Apr 25 11:15:10 2006

Ethernet address: 000f24018870

Incoming total 744 packets, 67953 bytes; 744 IP packets

Outgoing total 1185 packets, 1518317 bytes; 1181 IP packets

Average rates: 33.94 kbits/s incoming, 759.12 kbits/s outgoing

Last 5-second rates: 48.20 kbits/s incoming, 762.60 kbits/s outgoing

Ethernet address: 0001804bba4a

Incoming total 933 packets, 1324238 bytes; 933 IP packets

Outgoing total 473 packets, 28446 bytes; 473 IP packets

Average rates: 662.06 kbits/s incoming, 14.19 kbits/s outgoing

Last 5-second rates: 717.60 kbits/s incoming, 15.20 kbits/s outgoing

## ➤ **Trafico TCP y UDP**

UDP/161: 625 packets, 44457 bytes total, 1.40 kbits/s; 313 packets, 21596 bytes incoming, 0.68 kbits/s; 312 packets, 22861 bytes outgoing, 0.72 kbits/s

TCP/80: 13141 packets, 11686374 bytes total, 369.53 kbits/s; 5283 packets, 388578 bytes incoming, 12.28 kbits/s; 7858 packets, 11297796 bytes outgoing, 357.24 kbits/s

UDP/137: 1428 packets, 172452 bytes total, 5.45 kbits/s; 714 packets, 86226 bytes incoming, 2.72 kbits/s; 714 packets, 86226 bytes outgoing, 2.72 kbits/s

UDP/53: 1231 packets, 125533 bytes total, 3.98 kbits/s; 625 packets, 53660 bytes incoming, 1.70 kbits/s; 606 packets, 71873 bytes outgoing, 2.28 kbits/s

Estos informes son de suma importancia para un administrador pues nos permite obtener el trafico que se esta generando por interfase y puertos de manera que podemos obtener el trafico de entrada salida para todos los servicios que prestamos, permitiéndonos reorientar algún servicio, o mejorar algún servidor según se requiera.

# INSTALACIÓN DEL SISTEMA STILLSECURE® BORDER GUARD

Este sistema es una versión libre del Border Guard. Que es un sistema para la detección/prevención de intrusos en la red que permite protegerla de los huecos de seguridad.

El Border Guard identifica y elimina los virus, gusanos, trojans, exploraciones de puerto, ataques, e intrusiones antes de que entren a la red y causen daño, es fácil de usar y ofrece incomparable flexibilidad en responder a los ataques, puede bloquear instantáneamente el paquete que esta haciendo el ataque o bloquear la IP de donde se esta haciendo el mismo, se puede usar como sistema de protección de intrusos o como un sistema de detección de intrusos (IDS).

Este puede se configurado en modo estándar usado con un firewall externo o en modo gateway, donde se utiliza poniendo la máquina en modo bridge y se integra con el iptables.

El Border Guard usa dos políticas de firewall fundamentales para responder a un ataque:

**Pre-emptive firewall policy:** (Esta se usa en modo Gateway y wireless solamente). Esta política bloquea los paquetes de un ataque sin afectar otro tráfico, investigando el contenido del tráfico, se instala automáticamente en el firewall y todo el tráfico siguiente conteniendo este ataque es bloqueada inmediatamente.

**Responsive firewall policy** (Esta se usa en todo los modos) esta política bloquea todo el trafico desde la IP que origina el ataque, dependiendo del tipo de ataque la política elimina el trafico hacia la maquina atacada o hacia toda la red, esta política será insertada de manera automática e el firewall y tiene efecto por un determinado tiempo 30 minutos de modo predeterminado.

Border Guard, puede mantener actualizado desde Internet una serie de reglas de ataques y huecos de seguridad, cuando un ataque de estos es lanzado contra la red, y machea contra una de estas reglas el programa lo detecta como un ataque.

Una regla es la lógica sobre la cual Border Guard detecta y responde a un ataque, los parámetros lógicos pueden se seteados en el editor de reglas, la base de datos de reglas puede ser actualizada constantemente de Internet de los nuevos huecos de seguridad y ataques, esta incluye mas de 1800 reglas, una regla tiene dos componentes Attack Profile y Attack response

**Attack Profile** esta propiedad se usa para detectar un tipo de ataque especifico, el profile contiene el tipo de ataque, la dirección ip o la red fuente, la dirección IP o la red destino, el nivel del ataque, la cantidad de ocurrencia del ataque, y el día y hora cuando un ataque machea con todas estas propiedades el sistema inicia una acción.

**Attack response** es el método que Border Guard usa para bloquear o alertar sobre un posible ataque.

En el anexo # 3 podemos observar imágenes de esta herramienta .

## VALORACION ECONOMICA

1. El costo en la modificación y direccionamiento de la Red es 0 pues no se necesita ninguna inversión en el cambio de la red.
2. Una máquina sin grandes prestaciones puede se usada para esta plataforma.
3. El costo de Software para la implementación del Firewall-Proxy Transparente es 0 pues todas estas herramientas son Libres.

# CONCLUSIONES

Con el uso de un Firewall-transparente con Proxy Webcache obtenemos las siguientes ventajas.

1. Cero configuraciones, este se puede poner entre 2 router o entre un router y un Switch o frente a un simple servidor y no se necesita hacer ninguna variación al direccionamiento ni a la infraestructura de la Red existente, este se puede poner y quitar sin ninguna Implicación para la red
2. Este opera en la capa 2 de modelo de la OSI lo que permite que Se puede poner sin direcciones IP, esto lo hace mas seguro al no ser alcanzable desde la red externa, nadie sabe que esta ahí y esta revisando todo el trafico que circula hacia dentro y hacia fuera de la red.
3. Permite controlar y auditar todo el trafico http y al hacer cache de las paginas visitadas disminuyendo el trafico hacia el Proxy nacional.
4. Permite proteger la red corporativa de posibles ataques de la red externa.
5. Permite establecer las políticas de seguridad de la red.
6. Permite realizar auditorias a todo el tráfico desde la red y hacia la red detectando posibles indisciplinas o ataques
7. Permite observar el tráfico generado por la red y hacia la red por protocolo, por puertos y por interface obteniendo datos sobre el ancho de banda que nos permita ampliar o reorientar la red.
8. Con el sistema IDS/IPS se puede mantener la detección o prevención dependiendo de la configuración de posibles ataques o huecos de seguridad de los software actualizándose automáticamente de Internet de los últimos ataques surgido y así mantener nuestra red libre de estos.

## RECOMENTACIONES

1. Generalizar esta plataforma para el control y supervisión de las redes que lo necesiten.
2. Establecer los procedimientos adecuados para que una vez implementada esta herramienta se mantenga el chequeo de las trazas de auditoria periódicamente.

# BIBLIOGRAFIA

1. Manual de Instalación del Squid
2. Páginas de Internet de Linux como Bridge
3. Manual Practico y Tutorial de iptables
4. Manual de usuario del StillSecure® Border Guard
5. Howto de Linux

# ANEXO # 1



## Squid Analysis Report Generator

### Squid User Access Reports

Período: 2006Apr19-2006Apr19

Top 100 sitios

NUM	SITIO ACCEDIDO	CONEXION	BYTES	HORA
1	<a href="http://www.openwares.org">www.openwares.org</a>	9.45K	13.32M	661
2	<a href="http://www.siemens.com">www.siemens.com</a>	3.84K	12.70M	254.46K
3	<a href="http://office.microsoft.com">office.microsoft.com</a>	3.50K	3.88M	4.52K
4	<a href="http://www.google.com.cu">www.google.com.cu</a>	2.28K	9.36M	1.24M
5	<a href="http://www.almadecuba.cu">www.almadecuba.cu</a>	1.88K	10.24M	779.11K
6	<a href="http://horoscopo.cubasi.cu">horoscopo.cubasi.cu</a>	1.42K	3.73M	165.96K
7	<a href="http://cocina.cuba.cu">cocina.cuba.cu</a>	1.36K	1.90M	0
8	<a href="http://images.google.com.cu">images.google.com.cu</a>	1.32K	4.68M	1.18M
9	<a href="http://www.mitel.com">www.mitel.com</a>	1.28K	5.29M	39.73K
10	<a href="http://www.granma.cubaweb.cu">www.granma.cubaweb.cu</a>	1.25K	4.73M	36.12K
11	<a href="http://officeimages.microsoft.com">officeimages.microsoft.com</a>	1.22K	3.00M	0
12	<a href="http://www.cienfuegos.jovenclub.cu">www.cienfuegos.jovenclub.cu</a>	1.17K	4.82M	0
13	<a href="http://www.atenas.inf.cu">www.atenas.inf.cu</a>	1.12K	2.11M	177.33K
14	<a href="http://www.ericsson.com">www.ericsson.com</a>	1.10K	5.98M	360.61K

Período: 2006Apr19-2006Apr19

### DENEGADO Reporte

USERID	IP/NOMBRE	FECHA/HORA	SITIO ACCEDIDO
192.168.22.126	qventas5.ltu.tel.etcusa.cu	04/19/2006-08:23:17	<a href="http://www.siemens.com/">http://www.siemens.com/</a>
192.168.22.132	istel2.ltu.tel.etcusa.cu	04/19/2006-09:39:42	<a href="http://www.siemens.com/misc/pageMailer/pageMailerPopup.jsp?">http://www.siemens.com/misc/pageMailer/pageMailerPopup.jsp?</a>
		04/19/2006-09:39:51	<a href="http://www.siemens.com/misc/pageMailer/pageMailerPopup.jsp?">http://www.siemens.com/misc/pageMailer/pageMailerPopup.jsp?</a>
		04/19/2006-09:49:40	<a href="http://www.siemens.com/misc/pageMailer/pageMailerPopup.jsp?">http://www.siemens.com/misc/pageMailer/pageMailerPopup.jsp?</a>
192.168.22.135	sgtetpi.ltu.tel.etcusa.cu	04/19/2006-08:42:22	<a href="http://www.siemens.com/index.jsp">http://www.siemens.com/index.jsp</a>
		04/19/2006-08:45:02	<a href="http://www.siemens.com/index.jsp">http://www.siemens.com/index.jsp</a>
192.168.22.139	almacenltu.ltu.tel.etcusa.cu	04/19/2006-08:01:45	<a href="http://www.siemens.com/index.jsp">http://www.siemens.com/index.jsp</a>
		04/19/2006-08:21:00	<a href="http://www.siemens.com/index.jsp">http://www.siemens.com/index.jsp</a>
192.168.22.140	auxiliarvi.ltu.tel.etcusa.cu	04/19/2006-09:04:28	<a href="http://www.siemens.com/misc/pageMailer/pageMailerPopup.jsp?">http://www.siemens.com/misc/pageMailer/pageMailerPopup.jsp?</a>

### Squid User Access Reports

Período: 2006May02-2006May02

### Bajados Reporte

SERID	IP/NOMBRE	FECHA/HORA	SITIO ACCEDIDO
92.168.22.130	pcfinan.ltu.tel.etcusa.cu	05/02/2006-16:31:03	<a href="http://activex.microsoft.com/objects/ocget.dll">http://activex.microsoft.com/objects/ocget.dll</a>
		05/02/2006-16:31:03	<a href="http://activex.microsoft.com/objects/ocget.dll">http://activex.microsoft.com/objects/ocget.dll</a>
92.168.22.153	balancista.ltu.tel.etcusa.cu	05/02/2006-16:20:52	<a href="http://cdm.microsoft.com/UPDATE/Ident.cab">http://cdm.microsoft.com/UPDATE/Ident.cab</a>
		05/02/2006-16:20:52	<a href="http://cdm.microsoft.com/UPDATE/Ident.cab">http://cdm.microsoft.com/UPDATE/Ident.cab</a>
92.168.22.157	jgt	05/02/2006-17:12:03	<a href="http://activex.microsoft.com/objects/ocget.dll">http://activex.microsoft.com/objects/ocget.dll</a>
		05/02/2006-17:12:03	<a href="http://activex.microsoft.com/objects/ocget.dll">http://activex.microsoft.com/objects/ocget.dll</a>
		05/02/2006-17:12:03	<a href="http://activex.microsoft.com/objects/ocget.dll">http://activex.microsoft.com/objects/ocget.dll</a>
		05/02/2006-17:12:25	<a href="http://activex.microsoft.com/objects/ocget.dll">http://activex.microsoft.com/objects/ocget.dll</a>
		05/02/2006-17:12:25	<a href="http://activex.microsoft.com/objects/ocget.dll">http://activex.microsoft.com/objects/ocget.dll</a>
		05/02/2006-17:12:25	<a href="http://activex.microsoft.com/objects/ocget.dll">http://activex.microsoft.com/objects/ocget.dll</a>



ANEXO # 2

Firewall Builder: centosfw.fwb

File Edit Object Rules Help

Firewalls

centos

Objects

Address Ranges

Addresses

Groups

Hosts

Networks

Services

Custom

Groups

ICMP

IP

Object Type: Any  
Object Name: Any  
0.0.0.0/0.0.0.0

Any Network

centos

Firewalls: centos

Policy	inside	outside	loopback	Breadge	NAT	
	Source	Destination	Service	Action	Time	Options
0	Any	siprec	Any	Accept	Any	
1	Any	zap etecsa	Any	Accept	Any	
2	Any	recarga etecsa	Any	Accept	Any	
3	Any	cobros	Any	Accept	Any	
4	Any	gos-sql	Any	Accept	Any	
5	Any	gos	Any	Accept	Any	
6	Any	proxy.etecsa.cu	squid	Accept	Any	
7	Any	proxy.ltu.etecsa.cu	squid	Accept	Any	
8	Any	Telefonialtu	Any	Accept	Any	
9	Any	router tunas	Tiempo	Accept	Any	
10	Telefonialtu	Any	Any	Accept	Any	
11	net_tunas	broadcast	Any	Accept	Any	
12	centos	Any	Any	Accept	Any	
13	antivirus pcduo	Any	Any	Accept	Any	
14	correo.ltu.etecsa.cu	Any	smtp	Accept	Any	

centos							
Firewalls: centos							
Policy	inside	outside	loopback	Breadge	NAT		
	Original Src	Original Dst	Original Srv	Translated Src	Translated Dst	Translated Srv	Comment
0	bello	proxy.etecsa.cu	squid	Original	proxy.etecsa.cu	squid	no se afectan pc
1	ALabrado	proxy.etecsa.cu	squid	Original	proxy.etecsa.cu	squid	no se afectan pc
2	auditor	proxy.etecsa.cu	squid	Original	proxy.etecsa.cu	squid	no se afectan pc
3	Elba	proxy.etecsa.cu	squid	Original	proxy.etecsa.cu	squid	no se afectan pc
4	franklin	proxy.etecsa.cu	squid	Original	proxy.etecsa.cu	squid	no se afectan pc
5	Gerente	proxy.etecsa.cu	squid	Original	proxy.etecsa.cu	squid	no se afectan pc
6	JFerrer	proxy.etecsa.cu	squid	Original	proxy.etecsa.cu	squid	no se afectan pc
7	Jose Rivero	proxy.etecsa.cu	squid	Original	proxy.etecsa.cu	squid	no se afectan pc
8	Martin	proxy.etecsa.cu	squid	Original	proxy.etecsa.cu	squid	no se afectan pc
9	Psicologa	proxy.etecsa.cu	squid	Original	proxy.etecsa.cu	squid	no se afectan pc
10	Rene	proxy.etecsa.cu	squid	Original	proxy.etecsa.cu	squid	no se afectan pc
11	tony	proxy.etecsa.cu	squid	Original	proxy.etecsa.cu	squid	no se afectan pc
12	Pablo Julio	proxy.etecsa.cu	squid	Original	proxy.etecsa.cu	squid	no se afectan pc
13	Nelson Reyes	proxy.etecsa.cu	squid	Original	proxy.etecsa.cu	squid	no se afectan pc
14	net_tunas	proxy.etecsa.cu	squid	Original	centos	Original	se obligan a usar

ANEXO # 3

Actions

Attack profile

Name & description

Research

Select the actions you want to take against the attack profile:


Rule summary:


Prompt before taking action when an attack has the following profile: Attack of type DOS Ascend Route (SID: 281)



Set rule to:

(NOTE: all settings apply to future attacks)

☐ block - always automatically take action

☐ block if vulnerable - automatically take action only if against a vulnerable device (  )

☐ block if accessible - automatically take action only if against an accessible device (  )

☐ block if both - automatically take action only if against a device that is both vulnerable and accessible (   )

☒ prompt - alert me in the Make decisions tab before taking action

☐ log only - only log to the database

☐ disable - always ignore attack and disable actions for this rule

And take these actions:

☒ insert a firewall policy and block:

☐ using the system default (current setting: responsive)

☐ the attack source host (responsive)

☐ based on attack content (pre-emptive)

☐ the attack source host and based on attack content (both)

☐ run a custom script

Also alert me by sending:

(NOTE: enable alerts in System configuration)

☒ email notification

☐ SNMP trap

Set payload logging for this rule to:

☒ use system default (current setting: enabled)

☐ enable payload logging

☐ disable payload logging

StillSecure

Strata Guard™ Free | SMB | Enterprise | GigE

SUBSCRIBE

LOG

Monitor, detect & make decisions:

Security status:

Red

Awaiting 27 decisions  
Critical security events have been detected on your network. You have 27 decisions from high severity attacks.

Activity for the last: 24 hours  
Actions taken: 16  
Total attacks: 48791

Make decisions

Attack activity

Firewall policies

Reports

View by: severity

filter by: all devices

Attack severity: 1 direct attacks

☒ vulnerable device

☒ recon attacks

☒ accessible device

☒ suspicious traffic

☒ both

☒ connection attempt

current actions

in the future

☐ block source host

☐ clear

☒ decide later

prompt

ICMP Large ICMP Packet

Alerts sent: Email

Total attacks: 0

Research this rule

data/time	attack source	flag	attack destination	event details	apply action
5/6/06 2:25:34 PM	192.168.22.19: 8		102.168.22.11: 0	<a href="#">event details</a>	<input checked="" type="checkbox"/>
5/6/06 2:25:35 PM	192.168.22.19: 8		102.168.22.11: 0	<a href="#">event details</a>	<input checked="" type="checkbox"/>
5/6/06 2:25:36 PM	192.168.22.19: 8		102.168.22.11: 0	<a href="#">event details</a>	<input checked="" type="checkbox"/>

ATTACK-RESPONSES-403 Forbidden

Alerts sent: Email

☐ block source host

☐ clear

☒ decide later

prompt

Manage system:

5/6/06 7:54:11 am

System status: running

STOP MONITOR

Currently monitoring: My Network

Mode: Strata Guard Gateway

All processes up

CONFIGURE SYS

Manage rules:

Set rules to do the following:  
1) automatically block attacks  
2) block attacks if vulnerable, if accessible or both  
3) prompt you in Make decisions  
4) take no action and log the attack in reporting  
5) disable and never respond to an attack

Search for:

category	sub category	rule	current action
Best Practices	[521 rules]		prompt
NETBIOS	[430 rules]		prompt
Denial of Service	[87 rules]		prompt
Unk	[2 rules]		block
Web	[972 rules]		block if vulnerable
Database	[360 rules]		block if accessible
Web-Microsoft	[159 rules]		block if both
Email / SMTP	[143 rules]		prompt
Pomography	[21 rules]		log only
TCP / IP (DNS, FTP...)	[270 rules]		disable
Other	[804 rules]		prompt

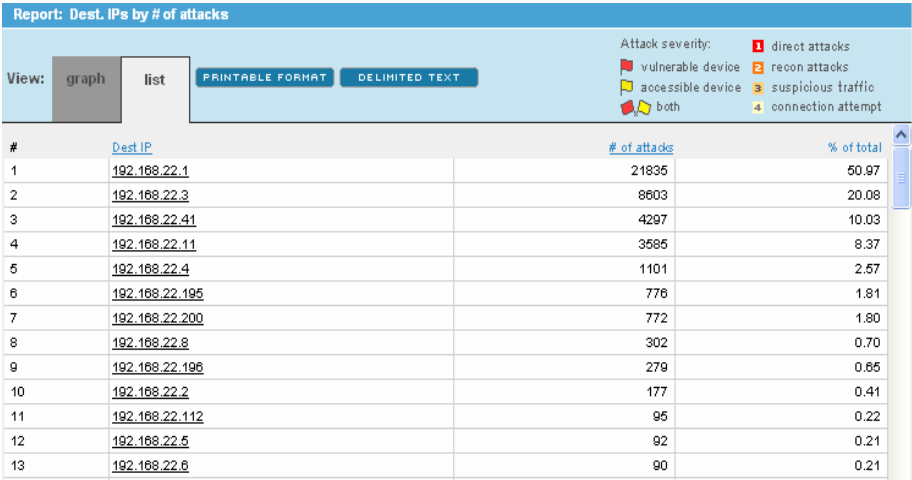
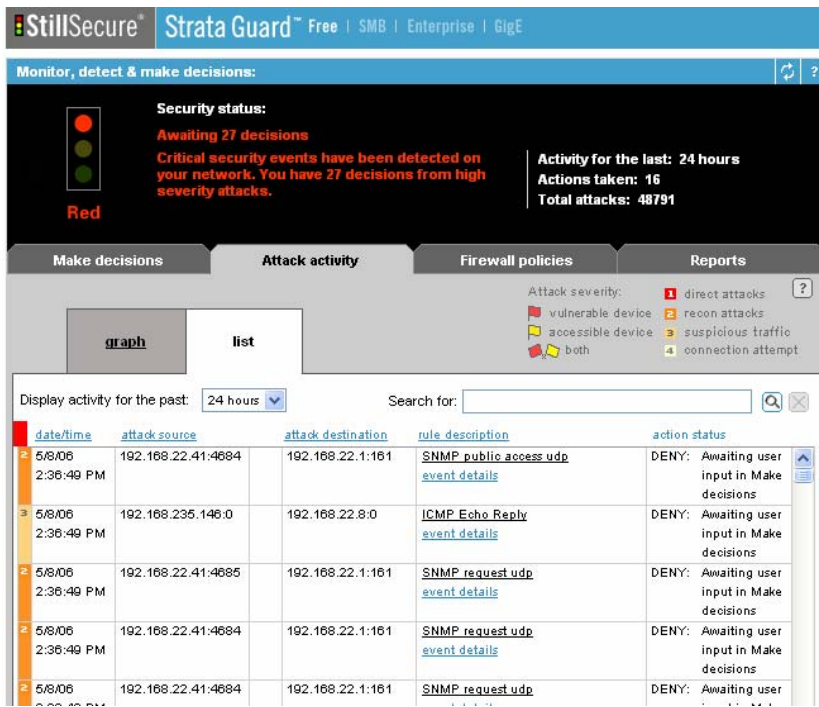
QUICK-TIME

NEW

CANCEL

APPLY

ANEXO # 3



fwlogwatch summary

Generated Thursday June 22 11:12:08 CDT 2006 by root.  
and 54726 older than 86400 seconds) of 93487 entries in the file "/var/log/messages" are packet logs, 394 have unique ch.  
First packet log entry: Jun 22 10:37:21, last: Jun 22 11:12:05.  
All entries were logged by the same host: "proxy".  
All entries are from the same chain: "RULE 46 -- DENY".  
All entries have the same target: "-".  
All entries are from the same interface: "br0".  
Only entries with a count of at least 3 are shown.

#	proto	source	port	service	destination	port	service
3	tcp	192.168.22.69	1424	-	192.168.91.10	3128	squid
3	tcp	192.168.22.69	1426	-	192.168.91.10	3128	squid
3	tcp	192.168.22.69	1431	-	192.168.91.10	3128	squid
3	tcp	192.168.22.69	1435	-	192.168.91.10	3128	squid
3	tcp	192.168.22.69	1437	-	192.168.91.10	3128	squid
3	tcp	192.168.22.69	1446	-	192.168.91.10	3128	squid
3	tcp	192.168.22.69	1450	-	192.168.91.10	3128	squid
32	udp	192.168.24.83	138	netbios-dgm	192.168.24.87	138	netbios-dgm

## DATOS DEL AUTOR

AUTOR: Alberto Bello Espinosa.

EDAD: 32 Años

CALIFICACION: Ingeniero en Telecomunicaciones y Electrónica

CARGO: Administrador de Red

DIRECCION: Calle Menocal Edif. 21 Rpto Medico Las Tunas

INTEGRACION: PCC, UJC, MTT, CDR.

CI: 73122402060

CENTRO DE PROCEDENCIA: Filial de Tecnología y Software, Las Tunas.

% de Participación: 50

EMAIL: [abello@ltu.eteccsa.cu](mailto:abello@ltu.eteccsa.cu)

TELEFONO: 46208.

### COAUTORES

Franklin Manzano Rodríguez

CI: 73062602641

Martín Jodar Velásquez

CI: 73062602641

# Carta de participación

Este trabajo fue realizado con la participación del autor y de los coactares respectivamente, de manera que fue realizado por los administradores de red de nuestra filial con el apoyo intelectual del subgerente de la Filial, a continuación se detalla el por ciento de participación de cada uno.

AUTOR: Alberto Bello Espinosa.	50%
COAUTORES	
Franklin Manzano Rodríguez	30%
Martín Jodar Velásquez	20%

Alberto Bello Espinosa	Franklin Manzano Rodríguez	Martín Jodar Velásquez
------------------------	----------------------------	------------------------