ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"IMPLEMENTACIÓN DE PLATAFORMA DE SEGURIDAD PARA LA APLICACIÓN DE POLÍTICAS UNIFICADAS QUE PERMITAN EL DESPLIEGUE DE LA ESTRATEGIA **"TRAE TU PROPIO DISPOSITIVO**" (BRING YOUR OWN DEVICE, BYOD) EN UNA ORGANIZACIÓN."

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del grado de:

MAGISTER EN SEGURIDAD INFORMATICA APLICADA

MIGUEL ANGEL MAZORRA GRANJA

GUAYAQUIL – ECUADOR

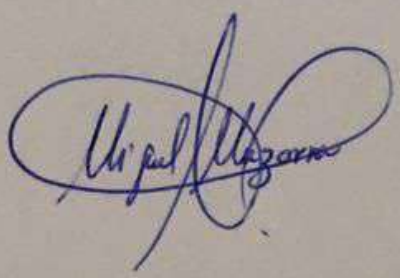
AÑO 2016

AGRADECIMIENTO

Agradezco infinitamente a Dios quien es el Mentor de mi vida a mi madre y a mi familia por el apoyo constante e incondicional. Además a mi hija por agregar ánimo y alegría a cada día de existencia

DEDICATORA

El presente proyecto lo dedico a mis padres por estar siempre a mi lado y a mi esposa e hija como ejemplo de perseverancia y dedicación

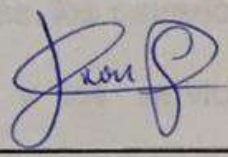


TRIBUNAL DE SUSTENTACIÓN

MSG. Lenín Freire

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA



MSG. Juan García P.

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

RESÚMEN

El propósito de este trabajo es demostrar como las políticas y herramientas de seguridad facilitan implementar la estrategia “Traiga su propio dispositivo” mediante una red más inteligente y segura. La estrategia “Traiga su propio dispositivo” requiere que los departamentos de TI (TECNOLOGÍA DE LA INFORMACIÓN) proporcionen el nivel apropiado de acceso a la red corporativa en base al perfil y al dispositivo del usuario. Además, los usuarios deben tener acceso a las aplicaciones, los datos y los servicios que correspondan.

Las empresas deben responder de manera proactiva ante BYOD con una política móvil mejorada y estrategias de reducción de costos. Esto implica mucho más que una simple reducción de los riesgos. Requiere políticas y capacidad de red para permitir que los empleados aprovechen al máximo sus dispositivos, las aplicaciones y los servicios en la nube a los que acceden, ya que el objetivo principal es una innovación en la forma en que los empleados hacen su trabajo.

ÍNDICE GENERAL

AGRADECIMIENTO……II

DEDICATORIA……III

TRIBUNAL DE SUSTENTACIÓN……IV

RESUMEN……V

INDICE GENERAL ……..VI

INDICE DE FIGURAS……..VIII

INDICE DE TABLAS……X

ABREVIATURAS……..XI

INTRODUCCIÓN……...XII

CAPÍTULO 1: GENERALIDADES

1.1 DESCRIPCIÓN DEL PROBLEMA……..14

1.2 SOLUCIÓN PROPUESTA ……..15

CAPÍTULO 2: ANÁLISIS DE LA SITUACIÓN ACTUAL

2.1 ESTADÍSTICA DEL USO DE DISPOSITIVOS PERSONALES EN LA ORGANIZACIÓN……..17

2.2 TOPOLOGÍA DE RED ACTUAL……18

2.3 ANÁLISIS DE APLICACIONES INTERNAS Y EXTERNAS…...18

2.4 ANÁLISIS DE APLICACIONES EN LA NUBE……19

2.5 REVISIÓN DE POLÍTICAS DE GRUPOS Y PERFILES DE ACCESO……..20
2.6 ANÁLISIS DE RIESGO Y AMENAZAS……21

CAPÍTULO 3: IMPLEMENTACIÓN DE PLATADORMA DE SEGURIDAD
3.1 TOPOLOGÍA DE RED CON PLATAFORMA DE SEGURIDAD PARA IMPLEMENTACIÓN DE BYOD……26
3.2 DEFINICIÓN DE GRUPOS DE USUARIOS Y DISPOSITIVOS..28
3.3 DEFINICIÓN DE PERFILES DE ACCESO PARA GRUPO DE USUARIOS Y DISPOSITIVO……31
3.4 DEFINICIÓN DE PERFILES DE SEGURIDAD PARA GRUPOS DE USUARIO Y DISPOSITIVOS…….35
3.5 CONFIGURACIÓN DE PLATAFORMA DE SEGURIDAD UNIFICADA…….37
3.6 CONFIGURACIÓN DE PLATAFORMA DE ANÁLISIS DE LOGS Y REPORTES ……42
3.7 COMPARACIÓN DE RIESGOS……43
CONCLUSIONES Y RECOMENDACIONES…....……...45
BIBLIOGRAFÍA……...47

ÍNDICE DE FIGURAS

FIGURA 2.1: Topología de red actual organización……..…18

FIGURA 2.2: Uso de ancho de banda de las aplicaciones……19

FIGURA 2.3: Políticas firewall basadas en direccionamiento IP……..….19

FIGURA 2.4: Grupo de redes bloqueadas……20

FIGURA 2.5: Análisis de riesgo 4 a 5……22

FIGURA 2.6: Análisis de riesgo 1 a 3……23

FIGURA 2.7: Intrusiones detectadas……..24

FIGURA 2.8: Amenazas tipo Botnet……..24

FIGURA 2.9: Amenazas malware……..24

FIGURA 2.10: Análisis riesgo tráfico web……..25

FIGURA 3.1: Topología de red con plataforma de seguridad…..……...27

FIGURA 3.2: Integración con servicio de directorio ……29

FIGURA 3.3: Integración firewall – servicio directorio ……29

FIGURA 3.4: Lista de dispositivos de red ……30

FIGURA 3.5: Control de intrusiones tipo cliente……..36

FIGURA 3.6: Control de intrusiones tipo Servidor……..…36

FIGURA 3.7: Control antivirus……..…..37

FIGURA 3.8: Modo de operación ……..38

FIGURA 3.9: Servicios de seguridad Fortinet……38

FIGURA 3.10: Perfil acceso Grupo VIP……...39

FIGURA 3.11: Perfil acceso Grupo Sistemas……..40

FIGURA 3.12: Perfil acceso Grupo Marketing……...40

FIGURA 3.13: Perfil acceso Grupo Estándar……..41

FIGURA 3.14: Perfil acceso Grupo Sin Internet……41

FIGURA 3.15: Perfil acceso a nivel de aplicaciones ……42

FIGURA 3.16: Configuración de eventos de seguridad……...42

FIGURA 3.17: Revisión de eventos de seguridad……43

FIGURA 3.18: Comparación de riesgo nivel 4 al 5……43

FIGURA 3.19: Comparación de riesgo nivel 1 al 3. ……..44

FIGURA 3.20: Comparación de amenazas detectadas.....44

ÍNDICE DE TABLAS

TABLA 1: Riesgo de las aplicaciones……..…21

ABREVIATURAS Y SIMBOLOGÍA

BYOD	BRING YOUR OWN DEVICE
FQDN	FULL QUALIFIED DOMAIN NAME
IP	INTERNET PROTOCOL
TI	TECNOLOGIA INFORMACIÓN

INTRODUCCIÓN

En la actualidad millones de consumidores están comprando dispositivos móviles avanzados. Estos potentes dispositivos tienen interfaces de usuario intuitivas y pueden acceder a cientos de miles de aplicaciones, no solo para usos personales, sino también para fines comerciales.

Cada vez más, las personas están llevando estos dispositivos a su trabajo para integrarlos en su flujo laboral diario. Esta tendencia se conoce como “Traiga su propio dispositivo " o BYOD (Bring your own device). Según datos estadísticos oficiales, en la actualidad el 90% de los empleados en los países desarrollados usan sus propios dispositivos para acceder a la información de la empresa.

BYOD podría tener profundas implicaciones para la forma en que las empresas administran sus redes, sus dispositivos móviles e incluso sus empleados. El 89% de los departamentos de TI permiten el uso de BYOD de una u otra forma. El 69% de los líderes de TI son positivos acerca de BYOD [1]. Y de manera general los empleados creen que BYOD desempeñara un rol crítico en la productividad del negocio.

En promedio, los líderes de TI esperan que la cantidad de dispositivos se eleve de un 2.3 por empleado en 2012 a un 2.8 en una tasa de crecimiento anual compuesta del 10.3%. La cantidad de dispositivos por usuario en aumento es, en gran medida, consecuencia de BYOD. Por ejemplo, el 42% de los teléfonos inteligentes y el 38% de las computadoras portátiles utilizadas en el lugar de trabajo actualmente pertenecen a los empleados. Esto demuestra que BYOD, lejos de ser una tendencia emergente, ya está bien afianzada en las corporaciones de todo el mundo. Y los líderes de TI observan un fuerte crecimiento de BYOD en los próximos dos años; un 63% afirma esperar que aumente el porcentaje de dispositivos pertenecientes a los empleados

CAPÍTULO 1

GENERALIDADES

1.1 Descripción del problema

Junto al crecimiento de los dispositivos móviles pertenecientes a los empleados es lógico que las aplicaciones no autorizadas aumenten, ya que los empleados no solo desean usar el dispositivo de su elección, sino también el software y los servicios de la nube que prefieren.

Existen costos potenciales para las empresas cuando los empleados usan sus propias aplicaciones. Uno de ellos es el mayor ancho de banda que requieren muchas de ellas. Algunas de las aplicaciones más populares que utilizan los empleados incluyen elementos multimedia, entre ellas las redes sociales y la transmisión de servicios multimedia. La combinación de más dispositivos en la red y las aplicaciones multimedia no autorizadas pueden crear cuellos de botella en la red, a menos que los departamentos de TI sean muy meticulosos acerca de su administración de la red y su planificación de recursos.

BYOD plantea nuevos desafíos en cuanto a seguridad y soporte de TI. De no tomarse controles, esta práctica puede ser muy perjudicial para la empresa ya que puede dejar fisuras donde se puede filtrar la información o introducir aplicaciones malignas a la red.

Esto es problemático incluso cuando la amplia mayoría de los dispositivos pertenezcan a la empresa.

1.2 Solución del problema

Las políticas y herramientas de seguridad deben verse como facilitadoras de BYOD mediante una red más inteligente y segura. Algunas de las funcionalidades de seguridad más importantes que se requieren para BYOD son:

Administración unificada de políticas: Protección de datos, aplicaciones y sistemas a través de la aplicación de controles de seguridad de manera unificada a equipos cableados e inalámbricos. Completa visibilidad de los usuarios, dispositivos y aplicaciones para control granular sobre cómo, cuando y donde esos dispositivos y aplicaciones son usados. Una sola plataforma de políticas, en lugar de muchas políticas distribuidas a través de sistemas de TI individuales, puede ayudar a que las empresas

salven de forma rápida y eficiente la falta de políticas móviles, para que la implementación de BYOD sea más segura.

Administración de perfiles de usuarios: BYOD requiere que los departamentos de TI proporcionen el nivel apropiado de acceso a la red corporativa en base al perfil y al dispositivo del usuario. Además, los usuarios deben tener acceso a las aplicaciones, los datos y los servicios que correspondan.

Protección de dispositivos: una capa de seguridad adicional en el nivel del dispositivo, tanto para dispositivos de la empresa como para dispositivos de los usuarios, es esencial para proteger la información confidencial de la empresa. La administración de dispositivos móviles permite a los administradores de la red denegar el acceso a dispositivos contaminados, perdidos o robados.

Transmisión segura de datos: la seguridad y el cifrado directo del dispositivo a la infraestructura de la red permiten que las empresas pongan sus datos más confidenciales a disposición de los usuarios móviles, más allá del dispositivo o su ubicación

CAPÍTULO 2

ANÁLISIS DE LA SITUACIÓN ACTUAL

2.1 Estadística del uso de dispositivos personales en la organización.

Actualmente la empresa Totaltek S.A tiene un total de 230 empleados, de los cuales 215 tienen acceso a los recursos de red internos y 185 tienen acceso a internet. El 80% de los empleados usan sus dispositivos móviles personales para ejecutar alguna actividad laboral.

Basados en esto se tiene un total de 415 dispositivos terminales generando tráfico de red en la organización. El sistema operativo de los dispositivos detectados son los siguientes:

- Windows 7
- Windows XP
- Windows 8
- Windows 2008 R2
- Windows 2012
- iPhone / iOS
- Android
- iPad / iOS
- Fortinet OS

2.2 Topología de red.

La topología de red actual de la organización es la que se muestra en la figura 2.1.

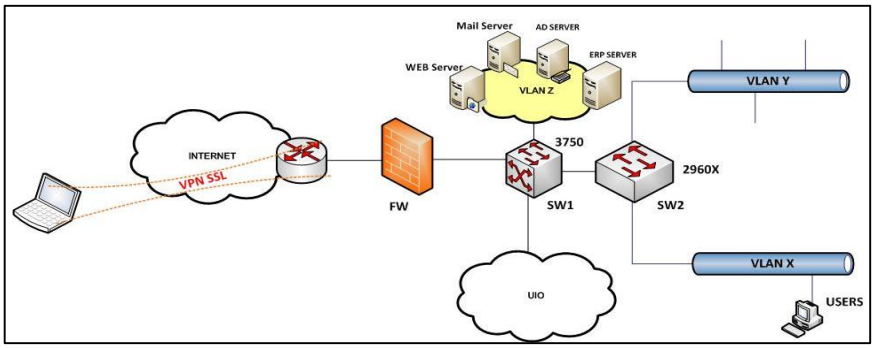


Figura 2.1 Topología de red actual organización.

A nivel interno se verifica capa de acceso y distribución. La organización cuenta con un enlace WAN hacia una sucursal ubicada en la ciudad de QUITO. Para la conexión hacia internet la empresa posee un firewall de seguridad perimetral, además permite el acceso a la información desde internet vía VPN SSL.

2.3 Análisis de aplicaciones internas y externas

Para obtener estadísticas del uso de aplicaciones internas y externas se implementó en el switch principal la configuración de puerto tipo espejo. Se procedió a conectar la herramienta de monitoreo para extraer los respectivos reportes. Los resultados del uso de aplicaciones se muestran en la figura 2.2.

#	Application Category	Number of Applications	Number of Users	Bandwidth	Session
1	Web.Others	7	338	3.75 GB	138,077
2	Network.Service	55	802	1.70 GB	456,386
3	Cloud.IT	5	22	1.18 GB	8,016
4	Video/Audio	18	26	941.63 MB	4,688
5	Email	8	2,500	920.71 MB	20,295
6	Social.Media	20	30	660.91 MB	10,453
7	General.Interest	28	104	321.02 MB	10,601
8	Collaboration	25	174	307.16 MB	38,310
9	Update	13	201	291.40 MB	20,520
10	Storage.Backup	19	23	60.38 MB	2,636
11	Remote.Access	7	32	54.38 MB	556
12	Business	12	10	15.18 MB	1,608
13	Mobile	3	21	8.59 MB	535
14	Proxy	2	7	373.01 KB	67
15	Botnet	2	3	331.07 KB	911
16	Game	2	2	39.62 KB	6
17	VoIP	4	11	18.43 KB	43

Figura 2.2 Uso de ancho de banda de las aplicaciones.

2.4 Revisión de políticas de grupos y perfiles de acceso

Actualmente la organización no tiene definido un documento con políticas de seguridad para el acceso a internet. La organización posee un firewall cisco asa modelo 5512. El acceso a internet está basado en direccionamiento IP ver figura 2.3.

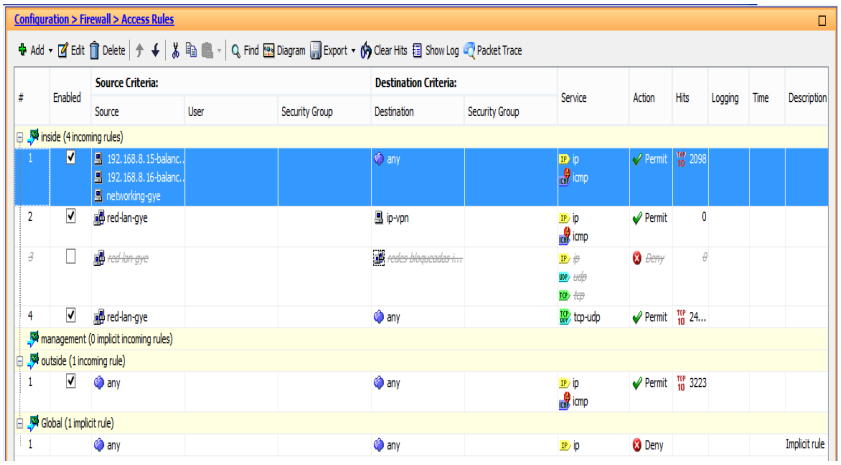


Figura 2.3 Políticas firewall basadas en direccionamiento IP.

Dentro del firewall existen políticas que bloquean el acceso a un grupo de direcciones en internet. Este grupo de direcciones es actualizado por el departamento de redes bajo demanda. Las direcciones pueden ser basadas en IP o FQDN. Ver Figura 2.4.

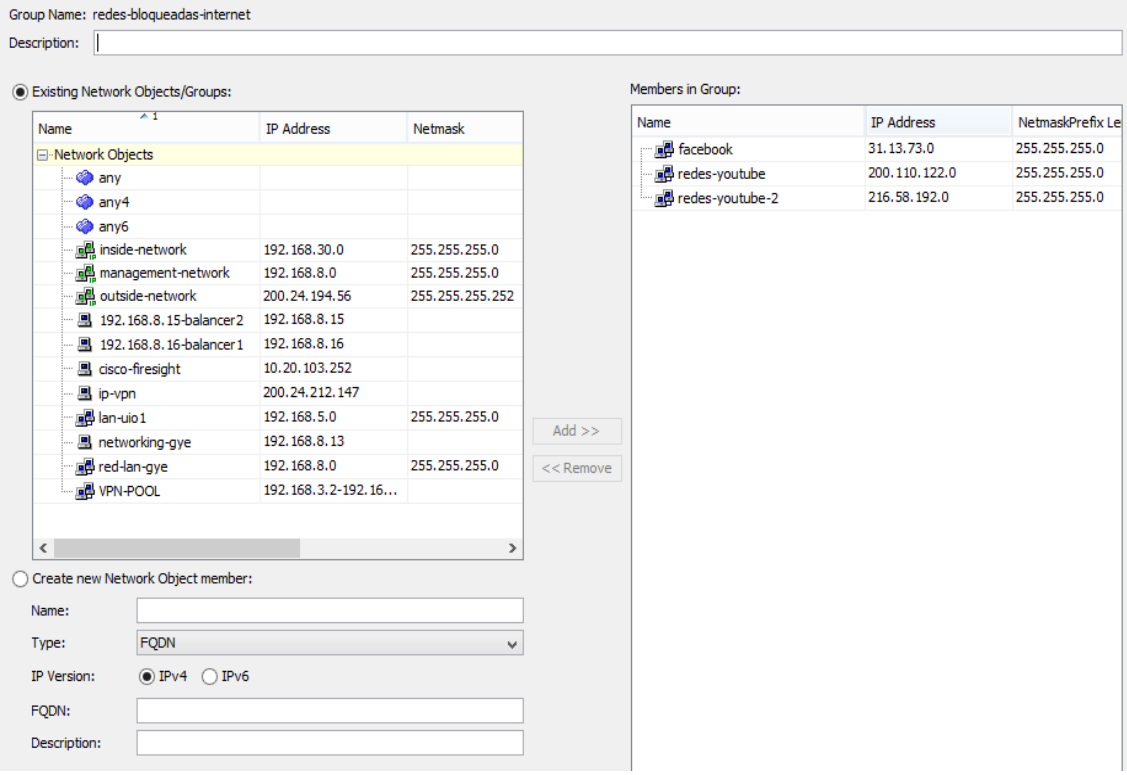


Figura 2.4. Grupo de redes bloqueadas.

2.5 Revisión de configuración de equipamiento de red actual

Se procedió a revisar la configuración de cada uno de los equipos de red para validar el direccionamiento IP y el flujo del paquete para acceso a internet.

2.6 Análisis de riesgo y amenazas

Para obtener un reporte de amenazas y brechas de seguridad de la red de la organización, en lo que respecta al tráfico entrante y saliente de internet, se uso como herramienta de análisis el equipo FORTINET modelo FG-500D. Se aplico el equipo en modo sniffer y se lo conecto a un puerto del switch de acceso configurado en modo promiscuo. El equipo a su vez envía los logs a una plataforma para generar reportes.

Se ha asignado una calificación de 1 a 5 a las aplicaciones basados en las características de su comportamiento. Esta calificación puede ayudar a los administradores a identificar rápidamente las aplicaciones de alto riesgo y tomar mejores decisiones sobre las políticas de control. La clasificación de riesgo se muestra en la tabla 1.

CALIFICACIÓN		CARACTERÍSTICA DE COMPORTAMIENTO
5	Crítica	Aplicaciones maliciosas o aplicaciones que pueden evitar los controles de seguridad
4	Alto	Aplicaciones que pueden causar fuga de información o infección por malware.
3	Medio	Aplicaciones usadas para comunicaciones personales o tienen vulnerabilidades conocidas
2	Elevado	Aplicaciones que consumen ancho de banda o afectan a la productividad
1	Bajo	Aplicaciones de negocio o actualización

Tabla 1. Riesgo de las aplicaciones

El período de análisis se fijo en 7 días. A continuación se muestran los resultados por categorías:

Análisis de riesgo por aplicaciones

#	Risk	Application Name	Category	Technology
1	5	Proxy.Websites	Proxy	Browser-Based
2	5	Ultrasurf_9.6+	Proxy	Client-Server
3	4	Ares	P2P	Peer-to-Peer
4	4	Teamviewer	Remote.Access	Client-Server
5	4	RDP	Remote.Access	Client-Server
6	4	Cisco.VPN.Client	Proxy	Client-Server
7	4	Cisco.VPN	Proxy	Network-Protocol
8	4	Bitcomet.HTTP.Seed	P2P	Peer-to-Peer
9	4	Teamviewer_CallReceive	Remote.Access	Client-Server
10	4	VNC	Remote.Access	Client-Server
11	4	Teamviewer_CallRequest	Remote.Access	Client-Server

Figura 2.5. Análisis de riesgo 4 a 5.

#	Risk	Application Name	Category	Technology	User	Bandwidth	Session
1	2	SIP	VoIP	Network-Protocol	26	1.42 GB	517,060
2	3	HTTPS.BROWSER	Web.Others	Network-Protocol	107	592.62 MB	58,097
3	2	HTTP.BROWSER_Chrome	Web.Others	Browser-Based	88	591.95 MB	52,233
4	1	QUIC	Network.Service	Network-Protocol	82	588.50 MB	17,141
5	3	SSL_TLSv1.0	Network.Service	Network-Protocol	86	574.25 MB	9,829
6	1	Kaspersky.Update	Update	Client-Server	61	453.50 MB	10,423
7	2	MS.Windows.Update	Update	Client-Server	90	329.59 MB	4,380
8	2	Instagram	Social.Media	Client-Server	51	265.33 MB	5,420
9	3	Facebook	Social.Media	Browser-Based	98	230.89 MB	60,404
10	3	HTTP.BROWSER	Web.Others	Browser-Based	112	144.99 MB	28,516
11	2	HTTP.BROWSER_Firefox	Web.Others	Browser-Based	50	104.18 MB	6,204
12	1	Malwarebytes	Update	Client-Server	33	103.98 MB	10,670
13	2	Facebook_Video.Play	Social.Media	Browser-Based	41	97.22 MB	6,647
14	2	Microsoft.Portal	Collaboration	Browser-Based	91	97.21 MB	19,370
15	2	HTTP.Segmented.Download	Network.Service	Browser-Based	55	94.97 MB	3,563
16	3	Spotify	Video/Audio	Client-Server|Peer-to-Peer	4	85.98 MB	106
17	3	SSL_TLSv1.2	Network.Service	Network-Protocol	81	77.16 MB	8,221
18	2	YouTube	Video/Audio	Browser-Based	86	73.22 MB	7,479
19	2	IP.Multicast	Network.Service	Network-Protocol	107	58.52 MB	61,586
20	2	Twitter	Social.Media	Browser-Based	73	48.76 MB	4,402
21	2	HTTP.Audio	Video/Audio	Browser-Based	16	45.84 MB	143
22	2	DNS	Network.Service	Network-Protocol	118	45.19 MB	166,009
23	2	HTTP.Video	Video/Audio	Browser-Based	18	37.70 MB	65
24	1	Avast.Update	Update	Client-Server	25	32.72 MB	655
25	2	Google.Accounts	General.Interest	Browser-Based	95	29.64 MB	4,346
26	2	ICMP	Network.Service	Network-Protocol	110	27.39 MB	146,578
27	3	Dropbox	Storage.Backup	Browser-Based	24	21.15 MB	662
28	3	HTTP.BROWSER_IE	Web.Others	Browser-Based	61	21.11 MB	2,444
29	1	Yandex.bot	Web.Others	Client-Server	1	19.02 MB	220
30	3	Microsoft.Office.Online	Collaboration	Browser-Based|Client-Server	46	17.97 MB	1,507

Figura 2.6. Análisis de riesgo 1 a 3.

Además se detectaron las siguientes amenazas usando la base de firmas de ataques y la base de datos de virus de la nube de FORTINET [2]. En base a esto las amenazas detectadas fueron las siguientes.

#	Attack Name	Severity	Counts
1	Cisco.IOS.HTTP.Command.Execution	Critical	202
2	MS.GDIPlus.JPEG.Buffer.Overflow	Critical	13
3	Bash.Function.Definitions.Remote.Code.Execution	Critical	8
4	POP3.Login.Brute.Force	high	26,416
5	Obfuscated.JavaScript.Access	medium	4
6	Muieblackcat.Scanner	low	216
7	HTTP.Unknown.Tunnelling	info	641
8	HTTP.Overly.Long.URI	info	481
9	HTTP.Chunk.Length.Invalid	info	68

Figura 2.7. Intrusiones detectadas.

#	Botnet Name	Counts
1	Andromeda.Botnet	6,776
2	Conficker.Botnet	6,672
3	Dyre.Botnet	10

Figura 2.8. Amenazas tipo Botnet

.

#	Malware Name	Malware Type	Counts
1	Conficker	Virus	2,912
2	WM/Agent!tr	Virus	139
3	Nivdort	Virus	109
4	Zeus	Virus	57
5	JS/Nemucod.EX!tr	Virus	39
6	W97M/TrojanDownloader.34B7!tr	Virus	10
7	WM/Moat.262C3F76!tr	Virus	2
8	W32/Generic!tr	Virus	1
9	Riskware/ProductKey	Spyware	1
10	PossibleThreat.P0	Virus	1
11	MSIL/Kryptik.ETQ!tr	Virus	1

Figura 2.9. Amenazas malware.

Análisis de riesgo por Navegación web

#	URL Category	User	Count	Bandwidth
1	Information Technology	245	81,288	4.51 GB
2	Advertising	20	21,338	301.95 MB
3	Business	48	20,512	2.78 GB
4	News and Media	11	14,191	2.21 GB
5	Search Engines and Portals	100	13,497	280.16 MB
6	Reference	11	10,410	449.69 MB
7	Content Servers	23	8,726	1.19 GB
8	Unrated	52	8,305	144.74 MB
9	Government and Legal Organizations	6	7,683	154.71 MB
10	Travel	2	4,146	280.95 MB
11	Meaningless Content	21	3,156	15.47 MB
12	Entertainment	7	3,103	375.73 MB
13	Freeware and Software Downloads	11	2,522	279.97 MB
14	Education	9	2,315	81.67 MB
15	Sports	5	2,230	92.09 MB
16	Malicious Websites	14	1,986	91.82 MB
17	Finance and Banking	4	1,982	42.84 MB
18	Shopping and Auction	9	1,897	67.72 MB
19	Information and Computer Security	4	1,710	326.36 KB
20	Personal Websites and Blogs	7	1,695	391.28 MB
21	Job Search	4	1,569	61.38 MB
22	File Sharing and Storage	7	1,277	69.68 MB
23	Social Networking	15	949	5.14 MB
24	Web-based Applications	8	914	1.52 MB
25	Pornography	5	801	104.10 MB

Figura 2.10. Análisis riesgo tráfico web.

CAPÍTULO 3

IMPLEMENTACIÓN DE PLATAFORMA DE SEGURIDAD

3.1 Topología de red con plataforma de seguridad para implementación de BYOD.

Es importante definir la ubicación de la plataforma de seguridad en la red de la organización, para la aplicación de las políticas de control a los usuarios. El equipo de seguridad debe ubicarse donde pueda interceptar todo el tráfico proveniente de la red interna y direccionado a internet. Además donde pueda gestionar el tráfico dirigido hacia los recursos internos de la compañía, es decir, el centro de datos. De acuerdo a la topología de la organización el dispositivo FG-500D debe instalarse entre el switch de acceso y distribución en modo transparente para no alterar el flujo de datos de la organización. Ver figura 3.1.

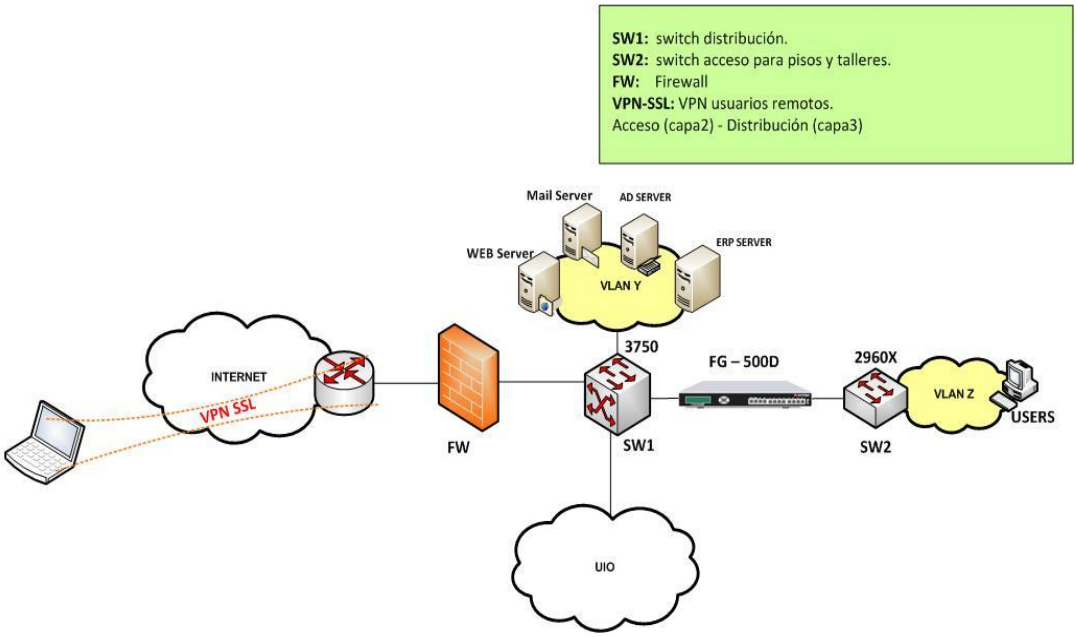


Figura 3.1 Topología de red con plataforma de seguridad.

Con la plataforma de seguridad es posible realizar control por tipo de dispositivos que se conectan a la red.

3.2 Definición de grupos de usuarios y dispositivos.

Una plataforma de seguridad de próxima generación debe ser capaz aplicar controles de seguridad basados en la identidad del usuario y no solo en el direccionamiento IP. Además que tenga visibilidad sobre el tipo de dispositivo que origina el tráfico de red. Para lograr esto se necesita la integración entre la solución de seguridad y el servidor de directorio.

El servicio de directorio de la organización es un Windows active directory. Se solicita la creación de los grupos de usuarios para acceso a internet de acuerdo a las políticas definidas por la empresa. Los grupos definidos son los siguientes:

- Grp Internet VIP
- Grp Internet Sistemas
- Grp Internet Marketing
- Grp Internet Estandar
- Grp Sin Internet

Se procede a instalar el aplicativo de Fortinet para obtener la información de inicio de sesión de los usuarios en los controladores de dominio del servicio de directorio [3]. Ver figura 3.2.

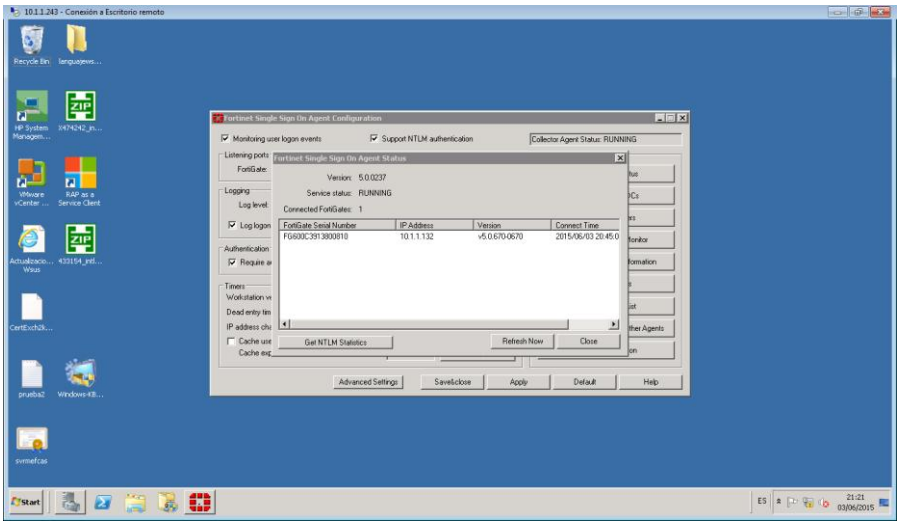


Figura 3.2 Integración con servicio de directorio.

En el equipo de seguridad FG-500D se realiza la configuración para comunicarse con el aplicativo instalado en el controlador de dominio [4]. Se debe especificar la dirección IP del servidor el puerto usado por el servicio y la contraseña para establecer la conexión.

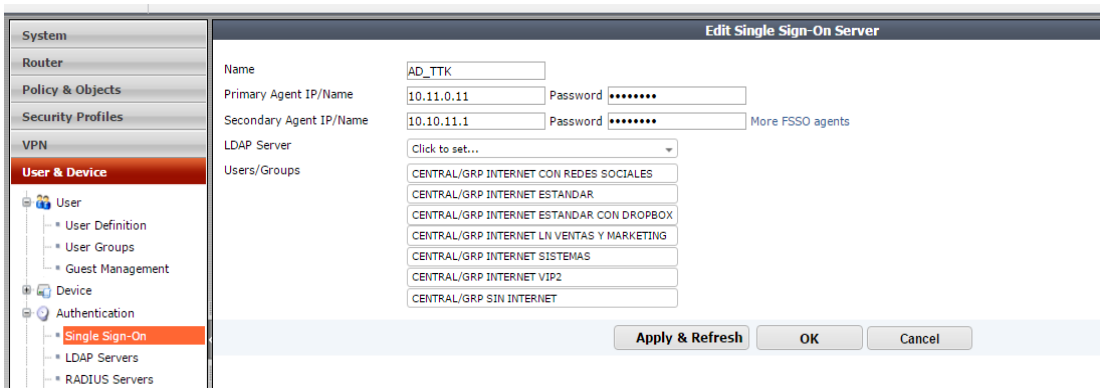


Figura 3.3 Integración firewall – servicio directorio.

En la plataforma FG-500D se activo la opción para detectar los diferentes tipos de dispositivos, los resultados se muestran en la figura 3.4.

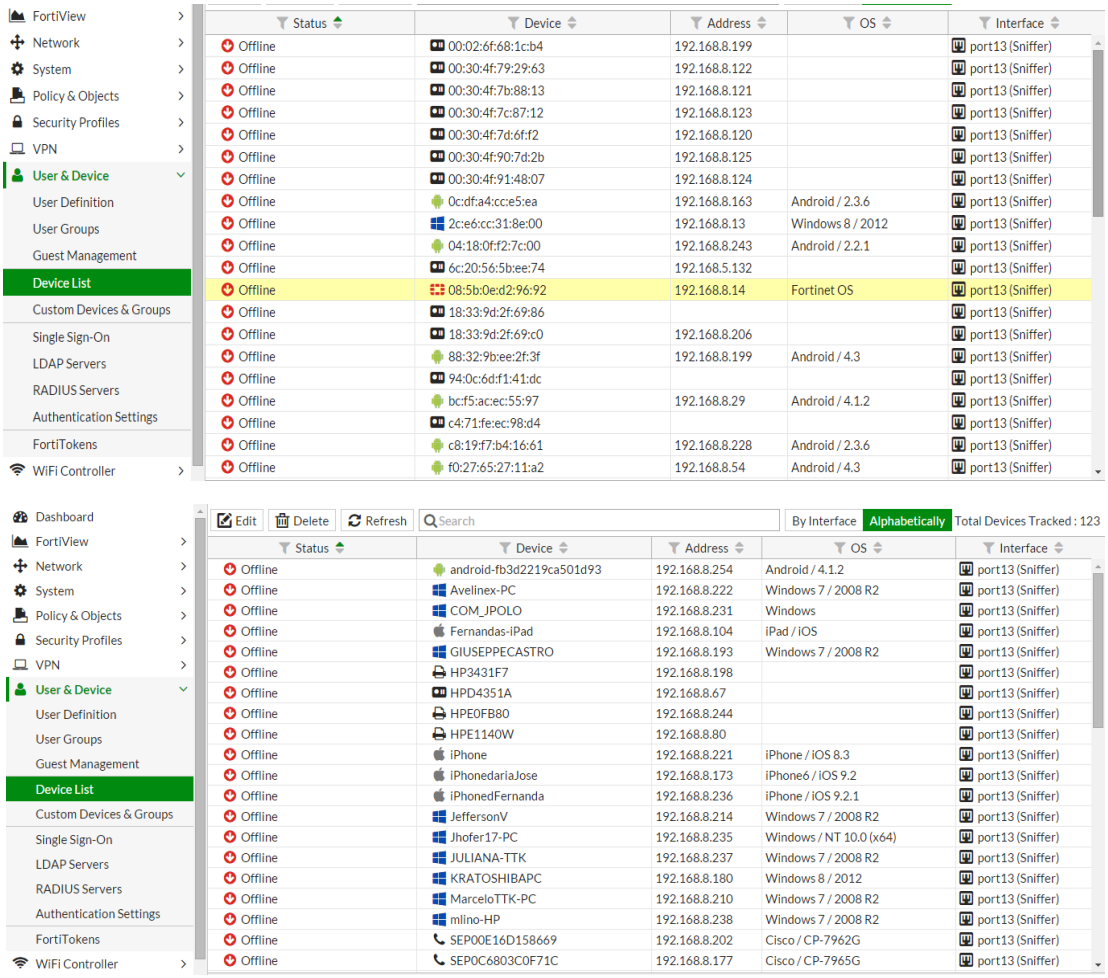


Figura 3.4. Lista de dispositivos de red.

A nivel de dispositivo se permitirá el acceso a internet a los siguientes sistemas operativos

- Windows 7
- Windows XP
- Windows 8

- Windows 2008 R2
- Windows 2012
- iPhone / iOS
- Android
- iPad / iOS
- Fortinet OS

3.3 Definición de perfiles de acceso para grupo de usuarios y dispositivo

Para restringir los accesos a dominios y aplicaciones en internet se debe definir controles de seguridad para permitir o bloquear determinados sitios web. Estos controles de filtrado web y de aplicaciones deben basarse en categorías. La plataforma Fortinet actualmente tiene más de 47 millones de dominios clasificados en 76 categorías [5]. Mientras que la base de las aplicaciones puede detectar alrededor de 2910 firmas.

Se definieron las políticas de seguridad para cada uno de los grupos de usuarios con acceso a internet. Se detalla los permisos o bloqueos por grupo:

- **Grupo Internet VIP**
  Bloquear:
  - **Adult/Mature Content**

  Permitir:
  - Todas las demás categorías y subcategorías.

- **Grupo Internet Sistemas**

Permitir:

- **Security Risk**
- **General Interest - Business**
  - Finance and Banking
  - Search Engines and Portals
  - General Organizations
  - Business
  - Government and Legal Organizations
- **Adult/Mature Content**
  - Sex Education
  - Alcohol
  - Tobacco
- **Bandwidth Consuming**
  - Freeware and Software Downloads
  - File Sharing and Storage
  - Peer-to-peer File Sharing
- **General Interest – Personal**
  - Web-based Email
  - Arts and Culture
  - Education
  - Health and Wellness
  - Job Search
  - Medicine
  - News and Media
  - Political Organizations
  - Global Religion
  - Shopping and Auction
  - Society and Lifestyles
  - Sports
  - Travel
  - Personal Vehicles
  - Folklore
  - Child Education
  - Restaurant and Dining

Bloquear:

- Todas las demás categorías y subcategorías.

- **Grupo Internet Marketing**
  - **General Interest - Business**
    - Finance and Banking
    - Search Engines and Portals
    - General Organizations
    - Business
    - Government and Legal Organizations

  - **Adult/Mature Content**
    - Sex Education
    - Alcohol
    - Tobacco

  - **Bandwidth Consuming**
    - Internet Radio and TV
    - Streaming Media and Download

  - **General Interest - Personal**
    - Web-based Email
    - Arts and Culture
    - Education
    - Health and Wellness
    - Medicine
    - News and Media
    - Social Networking
    - Political Organizations
    - Global Religion
    - Shopping and Auction
    - Society and Lifestyles
    - Sports
    - Travel
    - Personal Vehicles
    - Meaningless Content
    - Folklore
    - Web Chat
    - Instant Messaging
    - Child Education

        - Restaurant and Dining
        - Personal Websites and Blogs

- **Grupo Internet Estandar**
  Permitir:
    - **General Interest - Business**
        - Finance and Banking
        - Search Engines and Portals
        - General Organizations
        - Business
        - Government and Legal Organizations

    - **Potentially Liable**
        - Drug Abuse

    - **Adult/Mature Content**
        - Sex Education
        - Alcohol
        - Tobacco

    - **General Interest – Personal**
        - Web-based Email
        - Arts and Culture
        - Education
        - Health and Wellness
        - Job Search
        - Medicine
        - News and Media
        - Political Organizations
        - Global Religion
        - Shopping and Auction
        - Society and Lifestyles
        - Sports
        - Travel
        - Personal Vehicles
        - Folklore
        - Child Education
        - Restaurant and Dining

  Bloquear:

- Todas las demás categorías y subcategorías.

- **Grupo Sin Internet**
  Bloquear:
  - Todas las categorías y subcategorías.

3.4 Definición de perfiles de seguridad para grupos de usuario y dispositivos.

Para detectar y bloquear los diferentes tipos de amenazas presentes en el tráfico de red entrante y saliente de la organización se usará la base de firmas de ataques y la base de virus FORTINET. Actualmente existen más de 8000 firmas de ataques registradas en la nube FORTINET. A nivel de virus existen millones de registros y estos se actualizan cada semana.

En base al tipo de equipo terminal, sistema operativo, aplicaciones y protocolos se definieron los siguientes controles para la detección y bloqueo de intrusiones:

- Para los equipos tipo clientes se fija como sistema operativo Windows y otros sistemas. Mientras que a nivel de aplicaciones y protocolos se inspecciona todo. Ver figura 3.5

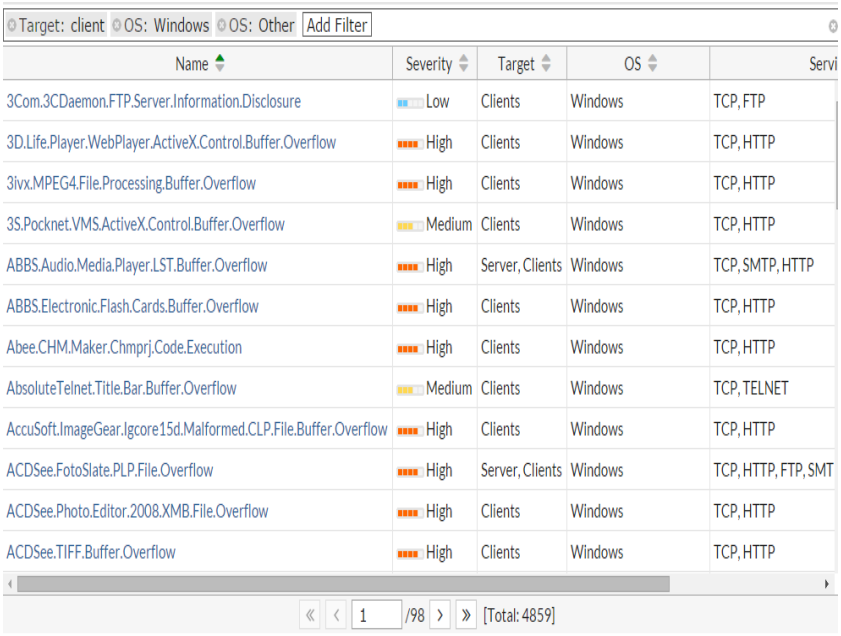


Figura 3.5. Control de intrusiones tipo cliente.

- Para los equipos tipo servidor se fija como sistema operativo Windows. Mientras que a nivel de aplicaciones y protocolos se inspecciona todo. Ver figura 3.6

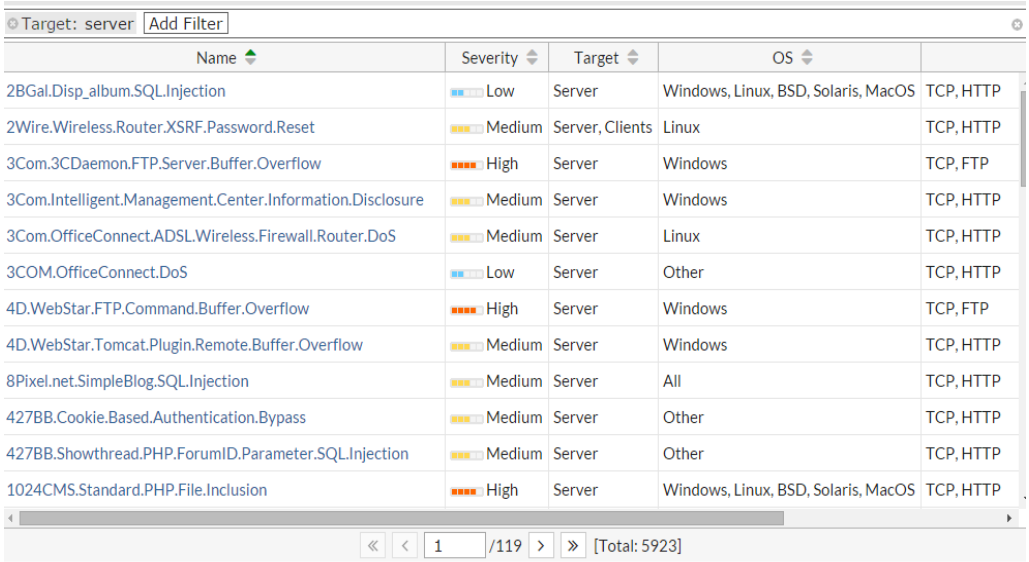


Figura 3.6. Control de intrusiones tipo Servidor.

Para el control antivirus se definió inspeccionar únicamente el protocolo HTTP. Dentro de este control se activa la protección contra malware y conexiones tipo Botnet. Ver figura 3.7.

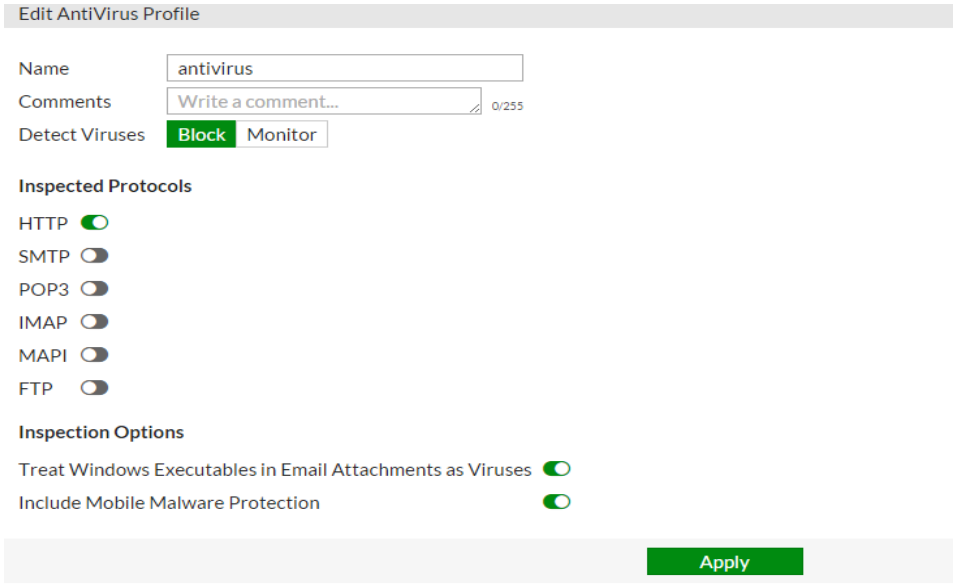


Figura 3.7. Control antivirus.

3.5 Configuración de plataforma de seguridad unificada

Para poder controlar el tráfico que se origina en la red interna hacia internet y tener visibilidad de los dispositivos móviles que se conectan a la red se configuró el equipo en modo transparente entre el switch de acceso y el switch de distribución. Ver figura 3.8.

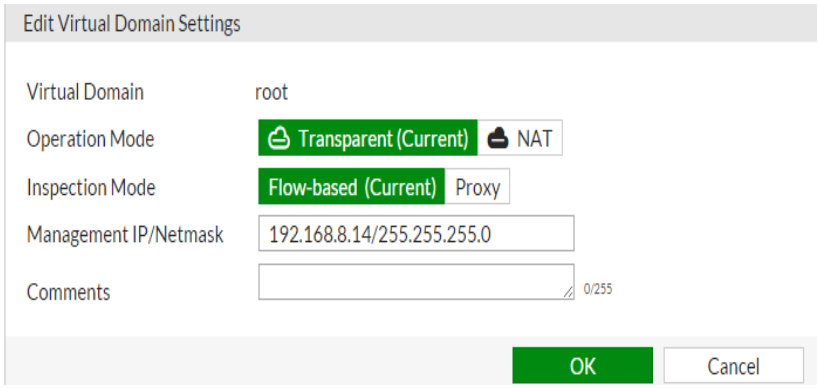


Figura 3.8. Modo de operación.

Se configuraron las respectivas interfaces para detectar los diferentes tipos de dispositivos móviles en la red interna.

Para recibir las actualizaciones de las firmas de ataques y del servicio de filtrado web y de aplicaciones, se configuraron los servidores DNS primario y secundario. Además de registrar el equipo en el portal Fortinet. Ver figura 3.9

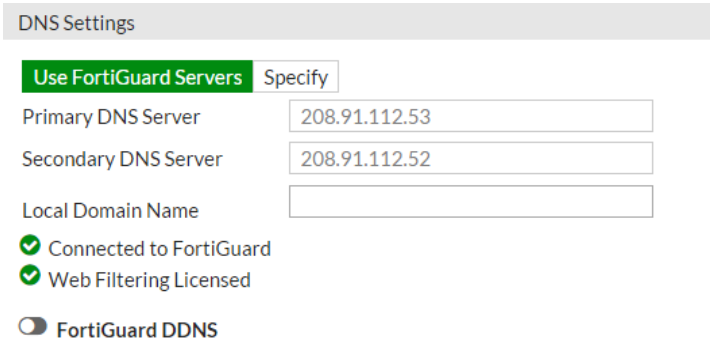


Figura 3.9. Servicios de seguridad Fortinet.

Se configuraron los perfiles de acceso de filtrado web de acuerdo lo definido en las políticas de seguridad de la organización.

- Perfil de acceso Grupo VIP

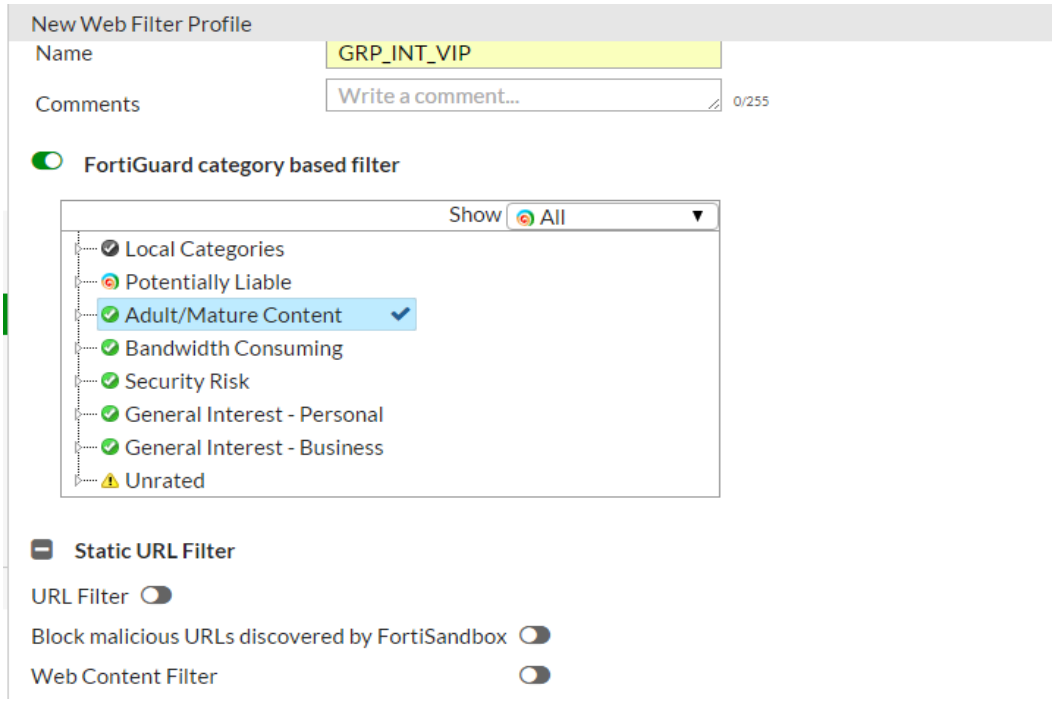


Figura 3.10. Perfil acceso Grupo VIP.

- Perfil de acceso Grupo Sistemas

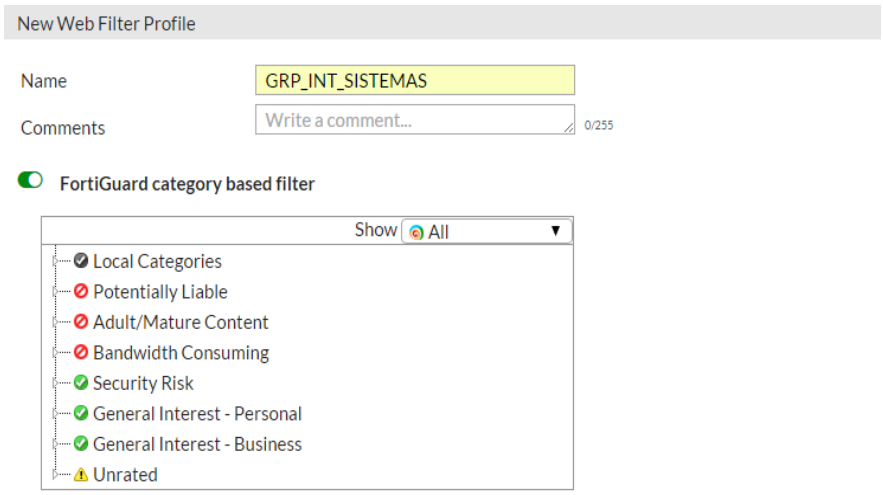


Figura 3.11. Perfil acceso Grupo Sistemas.

- Perfil de acceso Grupo Marketing

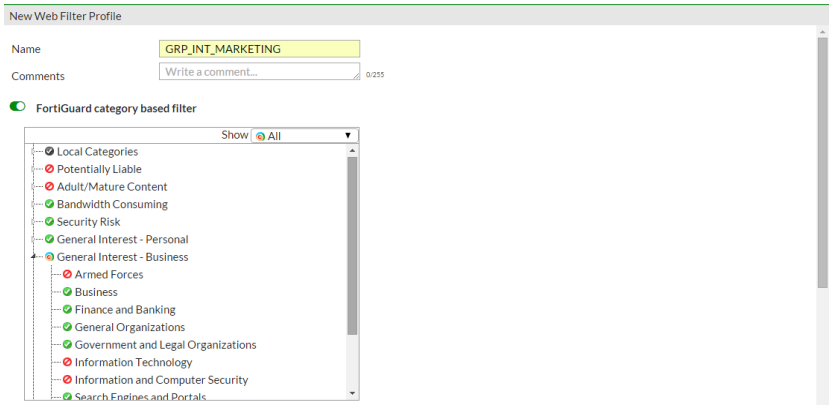


Figura 3.12. Perfil acceso Grupo Marketing.

- Perfil de acceso Grupo Estándar

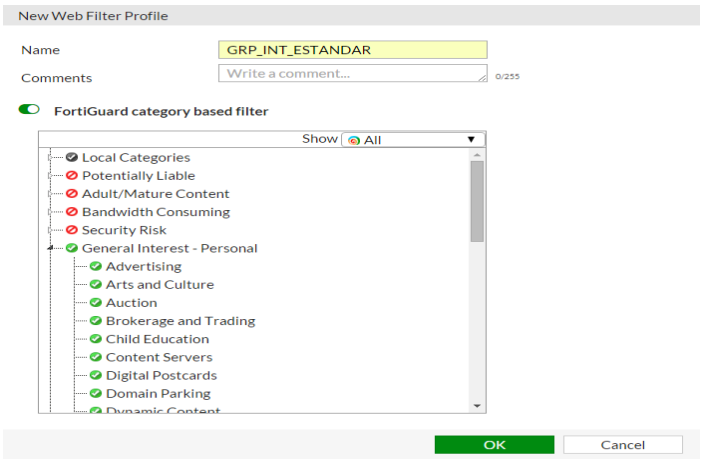


Figura 3.13. Perfil acceso Grupo Estándar.

- Perfil de acceso Grupo Sin Internet

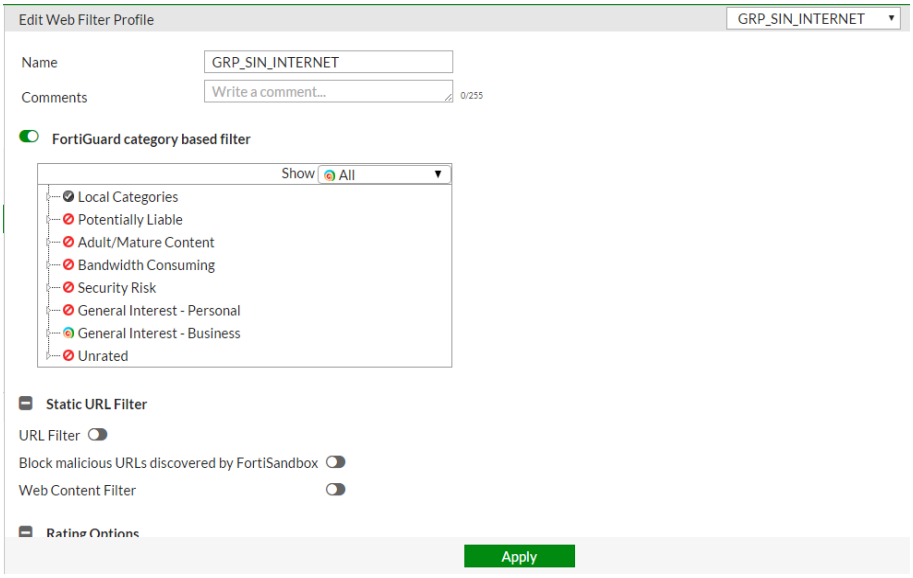


Figura 3.14. Perfil acceso Grupo Sin Internet.

Se configuraron los perfiles de acceso de control de aplicaciones de acuerdo a lo definido en las políticas de seguridad de la organización. Ver figura 3.15.

- Perfil de acceso Grupo VIP
- Perfil de acceso Grupo Marketing

- Perfil de acceso Sistemas
- Perfil de acceso Grupo Estándar
- Perfil de acceso Grupo Sin Internet

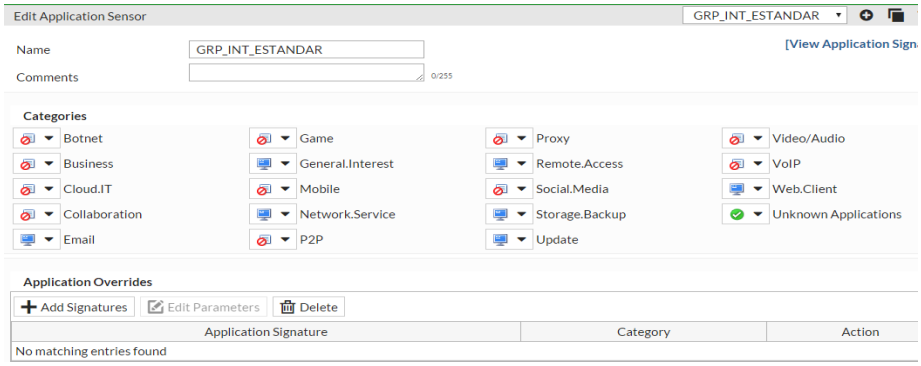


Figura 3.15. Perfil acceso a nivel de aplicaciones.

3.6 Configuración de plataforma de análisis de logs y reportes.

Se aplicó la configuración para que la plataforma de seguridad envié los LOGs al equipo analizador de eventos. Los eventos se envían en tiempo real. Ver figura 3.16.

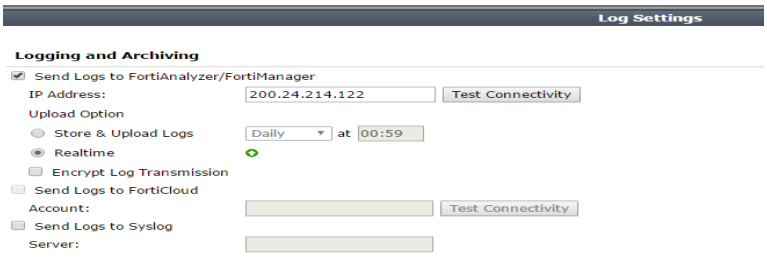


Figura 3.16. Configuración de eventos de seguridad.

Al momento se están recibiendo los eventos de seguridad de la plataforma

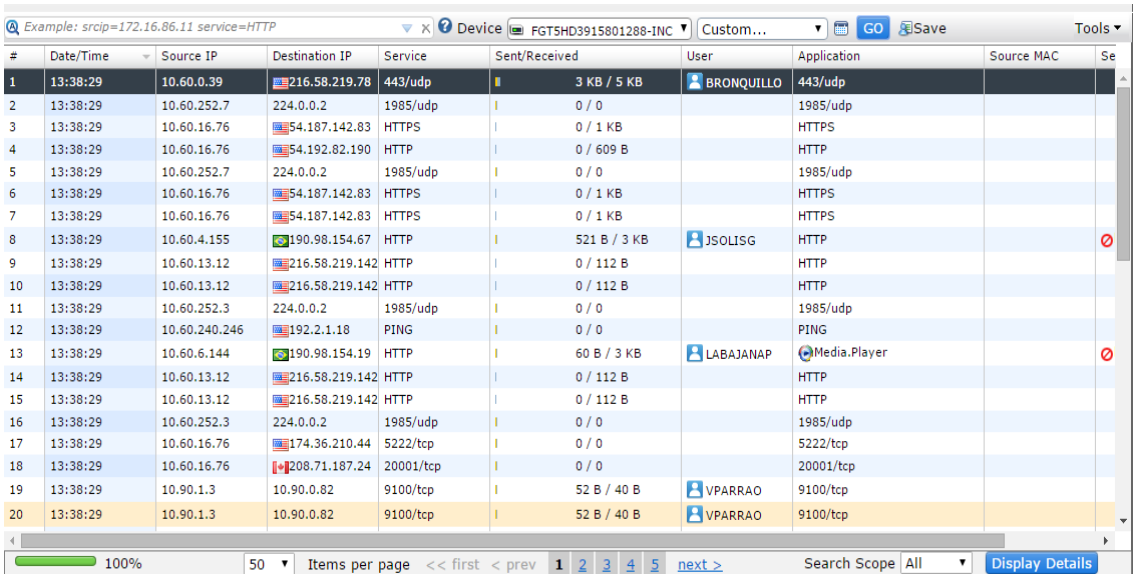


Figura 3.17. Revisión de eventos de seguridad.

3.7 Comparación de riesgos.

Luego de la aplicación de los perfiles de acceso y controles de seguridad a cada uno de los grupos de usuarios, se generó el reporte de análisis de riesgo respectivo los resultados se muestran en las figuras 3.18 y 3.9.

Análisis de riesgo por aplicaciones

#	Risk	Application Name	Category	Technology	User	Bandwidth	Session
1	4	Teamviewer	Remote.Access	Client-Server	8	19.18 MB	15,713
2	4	AnyDesk	Remote.Access	Client-Server	2	8.56 MB	5,398
3	4	IMesh	P2P	Peer-to-Peer	1	25.71 KB	8

Figura 3.18. Comparación de riesgo nivel 4 al 5.

#	Risk	Application Name	Category	Technology	User	Bandwidth	Session
1	2	YouTube	Video/Audio	Browser-Based	47	194.85 MB	1,848
2	2	YouTube_Video.Play	Video/Audio	Browser-Based	2	44.12 MB	152
3	2	MS.Windows.Update	Update	Client-Server	122	27.03 MB	8,853
4	4	Teamviewer	Remote.Access	Client-Server	8	19.18 MB	15,713
5	3	Dropbox	Storage.Backup	Browser-Based	7	15.83 MB	4,656
6	2	Microsoft.Office.Update	Update	Client-Server	1	11.01 MB	3,611
7	4	AnyDesk	Remote.Access	Client-Server	2	8.56 MB	5,398
8	1	Adobe.Update	Update	Client-Server	89	6.36 MB	3,960
9	2	HTTP.Video	Video/Audio	Browser-Based	9	3.20 MB	89
10	2	YouTube_Video.Access	Video/Audio	Browser-Based	2	1.28 MB	28
11	3	Amazon.AWS_S3	Cloud.IT	Browser-Based	6	617.36 KB	166
12	2	YouTube_Channel.Access	Video/Audio	Browser-Based	2	519.23 KB	4
13	3	Dropbox_Client.Sync	Storage.Backup	Client-Server	1	482.49 KB	125
14	2	YouTube_Video.Embedded	Video/Audio	Browser-Based	7	327.83 KB	30
15	3	Google.Drive	Storage.Backup	Browser-Based	4	320.60 KB	60
16	3	iCloud	Storage.Backup	Browser-Based	2	265.86 KB	177
17	1	McAfee.Update	Update	Client-Server	37	242.16 KB	78
18	2	Media.Player	Video/Audio	Client-Server	13	235.21 KB	74
19	3	Facebook	Social.Media	Browser-Based	11	234.14 KB	278
20	2	Amazon.Instant.Video	Video/Audio	Browser-Based	1	219.86 KB	60
21	3	Scribd	Storage.Backup	Browser-Based	3	150.72 KB	30
22	3	iTunes_Store	Video/Audio	Browser-Based	2	140.29 KB	22
23	3	Photobucket_Share	Storage.Backup	Browser-Based	3	106.59 KB	34
24	2	Google.Plus	Social.Media	Browser-Based	9	90.25 KB	654
25	1	Firefox.Update	Update	Client-Server	3	61.47 KB	16
26	3	Acrobat.Cloud	Storage.Backup	Browser-Based	1	36.23 KB	26
27	2	HTTP.Audio	Video/Audio	Browser-Based	1	35.13 KB	2
28	4	IMesh	P2P	Peer-to-Peer	1	25.71 KB	8
29	3	Slideshare	Storage.Backup	Browser-Based	1	24.93 KB	8
30	2	Yahoo.Screen	Video/Audio	Browser-Based	1	22.00 KB	4

Figura 3.19. Comparación de riesgo nivel 1 al 3.

A nivel de intrusiones solo se detecto una amenaza ver figura 3.20. No se encontró ninguna amenaza tipo malware o tipo Botnet.

#	Severity	Threat Name	Type	Victim	Source	Count
1	3	Obfuscated.JavaScript.Access	Anomaly	2	1	6

Figura 3.20. Comparación de amenazas detectadas.

CONCLUSIONES Y RECOMENDACIONES

Al aplicar las políticas de seguridad se redujo el consumo de ancho de banda en las diferentes aplicaciones que usan en la organización.

Los dispositivos no autorizados fueron denegados.

Las aplicaciones no autorizadas fueron denegadas.

El nivel de riesgo relacionado al tráfico de red que se genera desde la red interna de la organización fue reducido.

Obtener un certificado digital para la inspección de tráfico de red sobre puertos seguros.

Socializar las políticas de seguridad al interior de la compañía para lograr colaboración de cada uno de los empleados.

Aplicar técnicas avanzadas para detección de amenazas persistentes que se integren con la plataforma actual.

BIBLIOGRAFÍA

[1] BYOD, Perspectiva Global, http://www.cisco.com/c/dam/en_us/about/ac79/docs/re/byod/BYOD_Horizons-Global_LAS.pdf, fecha de consulta Diciembre 2015.

[2] IPS, base de datos de amenazas, http://fortiguard.com/intrusion, fecha de consulta Enero 2016.

[3] FSSO, aplicativo para servicio de directorio, https://support.fortinet.com/Download/FirmwareImages.aspx, fecha de consulta Enero 2016.

[4] Fortinet, Guía de Administración, FortIOS handbook 2015.

[5] Filtrado Web, Categorías de filtrado Web, http://fortiguard.com/webfilter, fecha de consulta Enero 2016.