Universidad Nacional
SAN LUIS GONZAGA

UNIVERSIDAD NACIONAL "SAN LUIS GONZAGA"

FACULTAD DE INGENIERÍA DE SISTEMAS

DIRECCIÓN DE INVESTIGACIÓN

EVALUACIÓN DE ORIGINALIDAD

CONSTANCIA

El que suscribe, deja constancia que se ha realizado el análisis con el software de verificación de similitud al documento cuyo título es:

MEJORA DE BLOQUEO WEB CON DISPOSITIVO WEB SEGUROS DE CISCO EN CAJA MUNICIPAL DE ICA

Presentado por:

- **SALDAÑA APARCANA LUIS ENRIQUE**

BACHILLER en **PREGRADO** de la facultad de Ingeniería de Sistemas. El resultado obtenido es **(porcentaje de similitud 9%)** por el cual se otorga el calificativo de:

APROBADO, según el Reglamento de Evaluación de la Originalidad.

Se adjunta al presente el reporte de evaluación con el software de verificación de originalidad.

Ica, 15 de abril de 2024

Dr. JAVIER ORLANDO GUTIÉRREZ FERREYRA
Director de la Unidad de Investigación
Facultad de Ingeniería de Sistemas

“AÑO DEL BICENTENARIO, DE LA CONSOLIDACIÓN DE NUESTRA INDEPENDENCIA, Y DE LA CONMEMORACIÓN DE LAS HEROICAS BATALLAS DE JUNÍN Y AYACUCHO”

UNIVERSIDAD NACIONAL “SAN LUIS GONZAGA”
VICERRECTORADO DE INVESTIGACIÓN
Facultad Ingeniería De Sistemas

MEJORA DE BLOQUEO WEB CON DISPOSITIVO WEB SEGUROS DE CISCO EN CAJA MUNICIPAL DE ICA

Línea de investigación: Ciencias naturales, ingeniería y tecnologías sostenibles

TRABAJO DE SUFICIENCIA PROFESIONAL

Autor: SALDAÑA APARCANA, LUIS ENRIQUE

Ica, Perú

2024

DEDICATORIA

Este trabajo va dedicada a Dios y a mis padres por el esfuerzo que han puesto para que yo sea un profesional.
A mis abuelos por sus enseñanzas que cultivaron el amor al estudio y que me ayudaron a conseguir mis metas.

AGRADECIMIENTOS

Agradezco a Dios que guía mi camino que me da la fuerza y voluntad para rendir día a día, a mis padres, familia que me apoyan en cada una de mis metas, que son la fuente de mi motivación, agradezco a los ingenieros de la facultad de sistemas cuya experiencia y sabiduría hicieron que amara más la carrera, agradezco a mis compañeros de la facultad que junto a mi estuvimos días y noches exigiéndonos en mejorar y aprender.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

En el presente trabajo se va a demostrar cómo se ha superado el déficit con el que se contaba ante el libre acceso de páginas Web.

En un principio se encontró que el filtro web lo trabajan bajo políticas generales en el Firewall con el que trabajan, dando así que al momento de que un usuario se movía de agencia se tenía que cambiar la política de acceso web generando horas hombre en hacer el trabajo de cambio y malestar hacia el usuario al no tener los mismos accesos.

Dentro del trabajo se va a demostrar la forma de cómo se fue implementando la aplicación de filtrado web, configuración de políticas según puesto de trabajo y como es el funcionamiento del filtrado web.

Adicional a ello se va a observar de cómo ha mejorado el nivel de seguridad y mejor uso del acceso a Internet, con los cambios ejecutado después de la implementación del filtro web, dando como resultados un mejor aprovechamiento del uso de la red (banda ancha) ya que no se consumen recursos en páginas web que no van al Core del negocio y en seguridad se le da un nivel adicional ya que dentro de las políticas a implementar se está ejecutando el bloqueo de acceso a páginas catalogadas como Ilegales protegiéndonos de una posible descarga de algún malware ya que dichas páginas en su mayoría tienen Phishing y paginas maliciosas vinculadas.

Con el filtro web implementado se puede obtener informes instantáneos, semanal o mensual de páginas más visitas, observar que usuarios tienen más actividad dentro de red tanto como acceso permitido y bloqueado.

Se va a trabajar de la mano con el Área de Seguridad de la Información para la aplicación de políticas de accesos puesto que ellos nos comparten la matriz de accesos por perfiles de trabajo en el cual se tienen más de 150 puestos de trabajo distintos de los cuales se van agrupar por sus tipos de accesos.

ABSTRACT

In the present work it is going to be demonstrated how the deficit that was counted on before the free access of Web pages has been overcome.

At first it was found that the web filter works under general policies in the Firewall with which they work, so that when a user moved from agency to agency, the web access policy had to be changed, generating man hours to do the job. work of change and discomfort towards the user by not having the same accesses.

Within the work, the way in which the web filtering application was implemented, configuration of policies according to job position and how web filtering works will be demonstrated.

In addition to this, it will be observed how the level of security and better use of Internet access have improved, with the changes executed after the implementation of the web filter, resulting in a better use of the network (broadband). since resources are not consumed in web pages that do not go to the Core of the business and in security an additional level is given since within the policies to be implemented, the blocking of access to pages classified as Illegal is being executed, protecting us from a possible download of some malware since these pages mostly have Phishing and linked malicious pages.

With the implemented web filter you can obtain instant, weekly or monthly reports of the most visited pages, observe which users have more activity within the network as well as allowed and blocked access.

It will work hand in hand with the Information Security Area for the application of access policies since they share with us the access matrix by job profiles in which there are more than 150 different jobs of which They will be grouped by their types of access.

INTRODUCCIÓN

El presente trabajo de suficiencia profesional realizado en la empresa CMACICA para la mejora en el control del acceso web dedicado ya que antes el Firewall perimetral cumplía con esta labor. Se va a explicar la forma en la cual está configurado y como se fueron creando los perfiles.

Es importante primero comprender el proceso de análisis que sigue el filtro web. El primer punto de verificación es la lista de Bypass y luego la Identificación.Bypass List, se utiliza para saltar todo el proceso de análisis en relación a una IP o URL, de esta manera se logra que el appliance no dedique tiempo y recursos en una evaluación innecesaria (Lista blanca general).

El siguiente paso es la Identificación, en ella se puede especificar la dirección IP de un usuario, el segmento de red al cual pertenece, un grupo o un usuario de Directorio Activo.

La evaluación continua con el puntaje de reputación web (WBRS CORE) que Cisco establece a cada URL, posterior a ello también revisara la categoría personalizada de páginas web (realizado manualmente por el administrador de red).

De ser necesario, existe un proceso de autenticación y autorización para dar inicio a las evaluaciones de seguridad como: Decryption, Protocols y User Agents, URL Category etc.

En la tesis Propuesta de implementación de políticas de seguridad basado en CISCO ISE (identity services engine) en la red LAN de Caja Huancayo, Huamán, G., Rojas, G. y Rojas, J. (2022), describe como se realizó y ejecuto la implementación de políticas de Cisco ISE dentro de Caja Huancayo donde se dan los permisos de puertos de red Lan con la autenticación de ISE dejando de lado la antigua seguridad de Puertos.

Dentro de la tesis ejecutada en Caja Huancayo se puede rescatar que en nuestro trabajo se puede usar la tecnología ISE para la autenticación de los puertos a nivel LAN que se validara con el directorio activo.[1]

En la tesis Rediseño de red LAN aplicando Cisco para mejorar la seguridad y comunicación de la información en la Subdirección de Circulación Terrestre – DRTC Junín en el cual toma como problemática la jerarquía de red que no existía dentro de la empresa por lo que se implementó la política del uso de Vlans dentro de la organización, lo que da un nivel más de seguridad usando tecnología de Cisco.[2]

Dentro de las investigaciones que se ha ido tomando, nos podemos apoyar de cómo mejorar el nivel de seguridad dentro de una empresa tomamos como referencia de como se ha ido mejorando la seguridad web ya que muchas veces los usuarios pueden sufrir phishing al momento de suplantar a una entidad bancaria dando como finalidad que los ciberdelincuentes nos roben datos muy importantes como numero de tarjeta de crédito, clave secreta entre otros.

A ello se le suma que hay usuarios que no tienen una concientización del uso de Internet ya que muchas veces ingresan a paginas clonadas, pero por no observar bien la URL tienden a caer. [3]

CAPÍTULO I: INFORMACIÓN DE LA INSTITUCIÓN DONDE SE DESARROLLÓ LA EXPERIENCIA

1.1 Descripción de la organización

La Caja Municipal de Ica es una empresa financiera de derecho público que goza de autonomía económica, financiera y administrativa, desarrolla sus actividades basándose en sus principios: Democratización y descentralización del crédito, así como fomentar e incentivar una cultura de ahorro. Igualmente está autorizada a ofrecer el servicio de créditos pignoraticios y desarrollar otros servicios financieros.

Actualmente tiene el nombre de Caja Municipal de Ahorro y Crédito de Ica S.A. (CMAC ICA S.A.).[4]

Orientados por nuestros valores, sabemos lo que debemos hacer por nuestros clientes y el rumbo que seguiremos para seguir creciendo en beneficio de nuestros clientes y de nuestra comunidad

Misión: Impulsar el desarrollo de los emprendedores brindando soluciones financieras integrales con Calidad de Servicio.

Visión: Ser una institución financiera sostenible, reconocida como el principal socio de nuestros clientes por la Excelencia en el Servicio.

Nuestros valores:

Vocación de servicio: Estamos comprometidos en brindar un servicio de calidad (rapidez, transparencia y calidez) a nuestros clientes externos e internos, dando siempre lo mejor de nosotros.

Integridad: trabajamos con honestidad, generamos confianza y actuamos de manera consistente con nuestros principios éticos.

Desarrollo Humano: Nos preocupamos por el bienestar y crecimiento personal y profesional de todos nuestros colaboradores.

Eficiencia: Cumplimos con nuestras metas y objetivos gestionando de manera óptima nuestros recursos

Orientación a resultados: Nos comprometemos y participamos en el cumplimiento de los logros propuestos de la empresa.[5]

La CMAC Ica tiene su Unidad de Infraestructura y comunicaciones supervisada por la gerencia de T.I.C. Dentro de la Unidad de Infraestructura y Comunicaciones se encuentra un apartado que es Seguridad de Informática la cual se observa en el siguiente Organigrama.

Organigrama de la gerencia de tecnología de la información y Comunicaciones

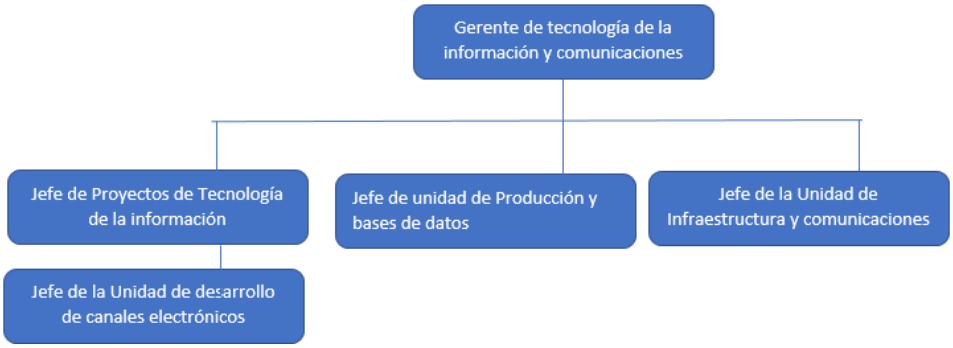


Fig. 1: Organigrama de la gerencia de TI

Fuente: Manual de Organización y funciones de Caja Municipal Ica optenido del MOF 84

En la Figura 1 se puede Observar que la Unidad de Infraestructura y Comunicaciones esta dentro de la Gerencia de TIC tal como se muestra en el organigrama.

Organigrama de la Unidad de Infraestructura y Comunicaciones

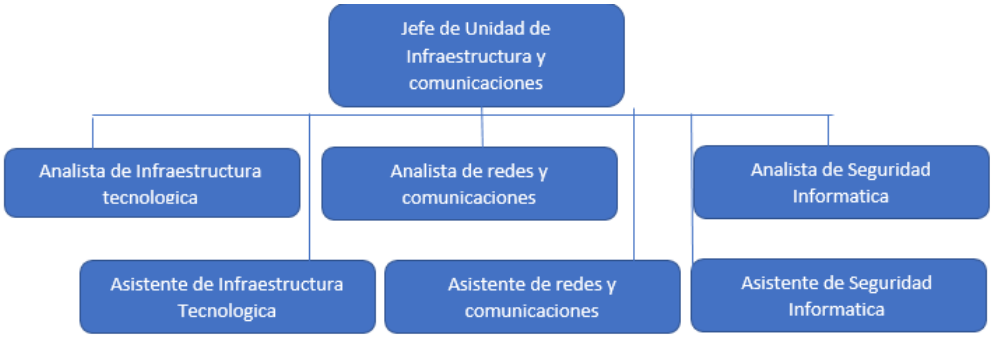


Fig. 2: Organigrama de la Unidad de Infraestructura y comunicaciones

Fuente: Manual de Organización y funciones de Caja Municipal Ica obtenido del MOF 84

En la Figura 2 del Organigrama se observa la Jefatura de Infraestructura y comunicaciones como su equipo de trabajo que lo conforma a la cual yo pertenezco como Asistente de Seguridad Informatica.

CAPÍTULO II: TRAYECTORIA PROFESIONAL

Luis Enrique Saldaña Aparcana ha desempeñado diversos roles según lo encomendado por la Unidad de Infraestructura tecnológica, paso como asistente de Infraestructura Tecnológica (09/12/2020 -31/05/2022) en la cual tenía las siguientes funciones:

- Visita de agencias de CmacIca.
- Mantenimiento preventivo de equipos.
- Mapeo de unidades de red dentro de las agencias (planos físicos como Lógicos)
- Revisión de equipos como file Server de Agencias.

Dentro de las funciones como Asistente de Seguridad Informática (01/06/2022-actualidad) tengo las siguientes funciones:

- Despliegue de antivirus y actualización de versión de Antivirus Kaspersky.
- Despliegue de políticas de Antivirus.
- Monitoreo ante eventos generados dentro de CMACICA.
- Creación de puntos de distribución.
- Mantenimiento lógico de servidores.
- Despliegue, creación de accesos y monitoreo mediante filtro web.
- Despliegue de parches y actualizaciones de seguridad.
- Revisión, liberación y bloqueo mediante AntiSpam
- Monitoreo mediante Firewall perimetral y externo.
- Sacar reportes mediante consola de Antivirus.
- Actualizar la versión del sistema operativo de los equipos.
- Realizar escaneo de vulnerabilidades y parchado de ellos
- Bloqueo de ips catalogadas como maliciosas.
- Monitoreo a políticas que sean aplicadas correctamente.

TABLA I TRAYECTORIA PROFESIONAL

Cargo	Fecha
Asistente de Infraestructura tecnológica	09/12/2020-31/05/2022
Asistente de Seguridad Informática	01/06/2022-actualidad

En la Tabla1, se puede comprobar los más de 02 años de experiencia laboral que he tenido dentro de la Cmacica Luis Enrique Saldaña Aparcana, para que pueda ser considerado en la modalidad para presentar el presente proyecto realizado en la empresa CMACICA.

CAPÍTULO III: APLICACIÓN PROFESIONAL

3.1 Situación Problemática

En un principio el acceso web (HTTP y HTPPS) eran controlados por el firewall perimetral, pero con el crecimiento global de usuarios hacia internet se fue encontrando muchas páginas de Fraudulentas (Phishing) / maliciosas que no se pudieron controlar en su totalidad y ante un crecimiento de personal dentro de Caja Ica en conjunto a los puestos de trabajo que se van implementando se ha convertido en horas hombre al momento de realizar los cambios. Dichos cambios se tenían que hacer al momento de este puesto nuevo se creaba o cuando se mudaba de agencia en agencia como en caso de los coordinadores, jefes regionales, gerencia entre otros lo cual en la unidad de Infraestructura y Comunicaciones se optó por implementar el Filtro Web de Cisco en el cual se evitan aquella problemática.

Para así evitar poder ingresar a páginas que no estén acorde con el negocio y poder tener un control al momento de acceder a paginas peligrosas (adultos, Deep web, Phishing entre otros).

Por otro lado, al tener un Bloqueo constante a páginas que no van acorde al negocio se observó menos quejas por conectividad y se incrementa el nivel de seguridad en los equipos dentro de Caja Ica.

SE EVIDENCIA CUATRO (04) EQUIPOS DE COMPUTO DE LA AGENCIA HUAMANGA CON ACCESO A PAGINAS WEB Y CORREO ELECTRONICO EXTERNO AL NO HABERSE APLICADO LAS POLITICAS DE RESTRICCIÓN POR PARTE DE LA UNIDAD DE INFRAESTRUCTURA Y COMUNICACIONES
Riesgo Medio

CONDICION:
De la revisión efectuada a una muestra de equipos de cómputo de la Agencia Huamanga durante la visita efectuada por la Gerencia de Auditoria Interna se determinó que cuatro (04) equipos de cómputo presentan versión del sistema operativo Windows 10 desactualizado, asimismo, durante la verificación de los equipos se apreció que dos (02) equipos de cómputo ubicados en la sala de comité presentan lentitud. El detalle de los equipos identificados se muestra en el siguiente cuadro:

N°	Hostname	IP	Acceso a correo electrónico externo	Acceso a Paginas Deportivas
1	08DA0410A	172.20.8.89	SI	SI
2	08DA0415A	172.20.8.85	SI	SI
3	08DA0301A	172.20.8.51	SI	SI
4	08DA0305A	172.20.8.55	SI	SI

A continuación, algunos de los equipos verificados en la Agencia Huamanga en las siguientes imágenes:

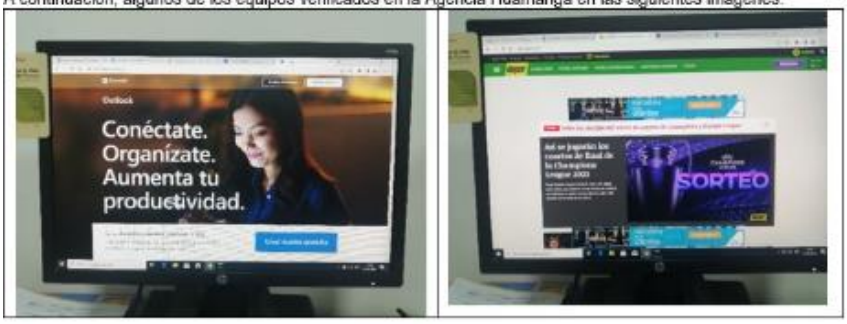


Fig. 3: Observación por parte de Auditoria Interna

Fuente: Obtenida de Observación de Auditoria Interna

Dentro de Caja Municipal Ica se encuentra la gerencia de Auditoria Interna y dentro de ella se encuentra la Unidad de Auditoria de TI la cual hace visitas a las Agencias / oficinas administrativas / oficinas compartidas. De la la cual en la Fig 3 se puede observar que se nos hace la observación por parte de ella a razón de acceso a correos externos, páginas deportivas o páginas que no van a razón del CORE del negocio.

Esto nos generaba una brecha de posible fuga de información hacia el exterior, mal uso del acceso a internet puesto que la línea de internet es limitada y si hay usuarios que lo usan para otros fines (escuchar música, ver películas de páginas catalogadas como streaming) esta se saturaría generando lentitud en la agencia u oficina.

3.2 Proyecto de solución

Después de hacer un análisis por parte de Infraestructura Tecnológica se decidió hacer la adquisición de 2 equipos Aplicación Web Segura (WSA) S395, así garantizando la alta disponibilidad (HA), así que mientras el Filtro Web principal (WSA) este en producción el Filtro Web de contingencia (WSA2) está en espera, pero al momento de que WSA1 falle el WSA2 entra como principal.

Dentro de la solución se va a tener que integrar los directorios Activos que tenemos dentro de Caja Ica, con el fin de que capture a los usuarios y en que Ip ha iniciado sesión, con el fin de que si este usuario ingresa sesión en otra sede de Caja Ica va a tener los accesos hacia páginas web igual a como los tiene en su oficina o sede perteneciente.

El equipo que se complementa es un Agente de Directorio Contextual (CDA) el cual tiene la función de capturar las sesiones de los equipos de red de caja ica luego hace la validación con el Directorio Activo dando asi los accesos que les corresponda.

Con ello se obtiene un mejor uso del acceso a Internet y se evitan horas hombre en estar cambiando los accesos haciéndose de forma automática por la solución de Filtro Web (WSA)

El dispositivo de seguridad Cisco Web Security Appliance (WSA) proporciona la defensa de gateway más completa del sector frente a software espía y malware basado en Web. Esto incluye todo, desde Adware (que causa los problemas de soporte más importantes y consume recursos de red significativos) hasta amenazas más malintencionadas, como troyanos, secuestradores de navegadores, objetos de ayuda de navegador, phishing, pharming, supervisores del sistema, keyloggers, gusanos, etc. [6]

Fig. 4: Equipo Cisco instalado

Fuente: Obtenido desde Data Center de Caja Municipal Ica

Como se observa dentro de la FIG 4 se observa los 2 equipos que se tienen instalados dentro de Caja Municipal Ica los cuales se encuentran raqueados y producción.

Cabe destacar que los equipos se encuentran en alta disponibilidad donde en caso un equipo cae el otro lo suple. Adicional a ello los equipos pueden se pueden hacer un failover para garantizar en caso un equipo se encuentre con problema.

TABLA II CARACTERÍSTICAS DEL EQUIPAMIENTO

Marca	Cisco
Modelo	S395
Factor de Forma	1RU
Flujo de Aire	De delante hacia atrás
Procesador	Intel Xeon 5218
Memoria Ram	32 GB de RAM
RDIMM	DIMM DDR4-2933
Puerto de Gestion	M1
Puerto Proxy	P1 y P2
Puerto de Trafico	T1 y T2
Puerto Usb	USB 3.0 tipo A
Fuente de alimentacion	Dos 770 W CA Intercambiable en caliente y redundante como 1+1
Almacenamiento	Cuatro discos duros SAS de 600 GB RAID 10, intercambiable en caliente

Fuente: Obtenido de documentación interna de Caja Municipal Ica

Dentro de la tabla 2 se puede observar las características de los equipos que se han adquirido dentro del proyecto los cuales ambos son de igual características. Adicional a ello se observa que la fuente de alimentación también se encuentra en alta disponibilidad por si uno de ellos deja de funcionar y el cambio es en caliente.

En cuesto de capacidad se tiene RAID 10 lo cual nos garantiza hacer el cambio en caliente por si ocurriese algún desperfecto dentro de los discos garantizando también la alta disponibilidad de ellos.

Dentro del sistema operativo del dispositivo tiene instalado AsyncOS 14.5, que es un sistema operativo de propiedad de Cisco la cual fue lanzada en marzo del 2022 la cual con la que se va a trabajar, por parte de Cisco recomienda que se use los navegadores de su preferencia como Chrome, Firefox entre otros.[7]

Por otro lado, el equipo tiene soporte de actualización de software para mantenerse actualizado constantemente, como se observa en la tabla 2, dentro del foro de Cisco se observa que es un equipo que tiene soporte tanto de software como Hardware. [8]

3.3 Solución y objetivos

Como solución se tiene:

- Mejora de la seguridad en cuanto a navegación web.
- Aseguramiento de que el uso al acceso de Internet sea con fines del negocio.

- Control en cuanto al acceso por perfiles creados dentro de la Aplicación Web Segura.
- Fuerte protección contra todas las amenazas actuales de Internet.
- Mitigamos el riesgo de fuga de información atreves de páginas de almacenamiento en nube.
- Se ahorran horas hombre al momento de hacer cambios.
- Se mantienen los accesos de los usuarios así cambien de sede.

Cisco Aplicación Web Segura correlaciona las amenazas recopiladas de la red de Cisco para producir un puntaje de comportamiento sobre el cual tomar medidas. Aplica y refuerza las puntuaciones de reputación web en los sitios principales y los sub sitios.

La calificación de las paginas la toma de cisco Talos el cual tiene como función categorizar las páginas que se encuentran en internet por ejemplo en la figura 5 se observa que se busca la página de Cajaica.pe y nos muestra su categoría que es Finanzas, su reputación es Neutral eso quiere decir que no está catalogada como maliciosa también nos muestra el proveedor de red a la cual está conectada la página web.

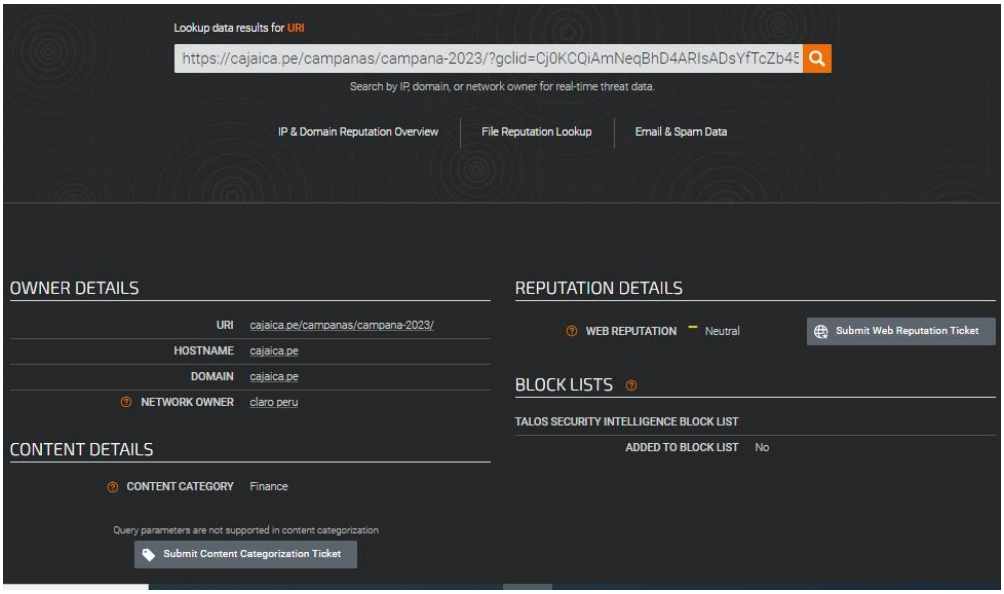


Fig. 5 Talos de Cisco

Fuente: Obtenida de página oficial de Talos Cisco

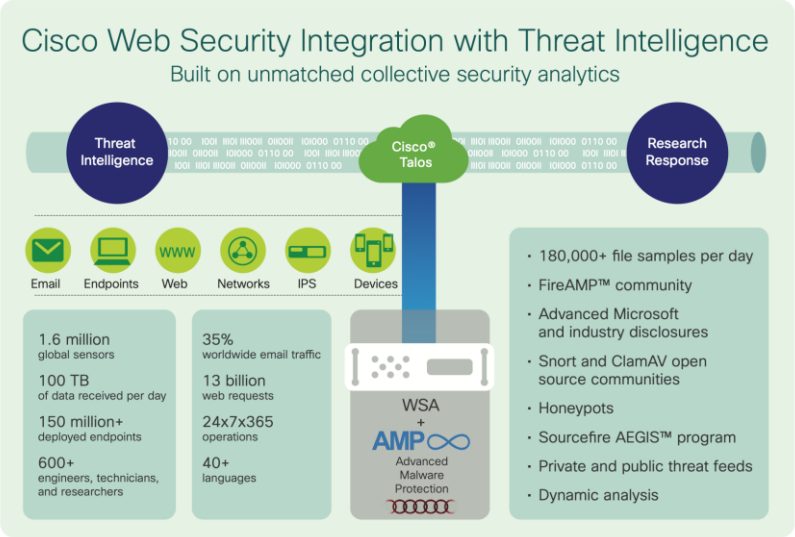


Fig. 6: Inteligencia ante amenazas.
Fuente: Avantec-Cisco Secure Web Appliance. [9]

Dentro de la FIG. 6 se observa la integración que se tiene la Web Segura de Cisco el cual trabaja con Talos.

Se observa que trabaja con un filtrado de trafico web, políticas más granulares por grupos o usuarios dentro de la organización que se aplique. Se aplica para páginas web, correos entre otros.

3.3.1 Planificación

Para realizar la planificación del proyecto de implementación de la Aplicación Web Segura (WSA) se solicitó a la empresa Ganadora del proyecto Adexus Perú para poder implementarlo y nos refirió el siguiente cuadro para la configuración de los equipos.

Dentro de la Fig 7 se observa los Sprint, una metodología usada para hacer los entregables por fechas establecidas. Dentro de la planificación se tienen desde horas hasta días todo de forma cronometrada para poder entregar el proyecto en las fechas establecidas.

Id	Mo de tare	Task Name	Duración	Comienzo	Fin	Predeceso
1		**PLAN DE TRABAJO - CMAC ICA**	**57.01 días**	**16/11**	**5/02**	
2		**PLANIFICACIÓN**	32 días	16/11	30/12	
13		**DESPLIEGUE DE CISCO WSA**	1 día	31/12	31/12	12;2
14		**Pre- Deployment**	**12.51 día**	**7/01**	**25/01**	**13**
15		**Instalación física startUp del servidor**	**0.26 días**	**7/01**	**7/01**	
16		Instalación del Servidor	1 hr	7/01	7/01	
17		Proveer de energía al equipo.	0.1 hrs	7/01	7/01	16
18		Configuraciones básicas de red (IP, máscara, puerta de enlace)	0.5 hrs	7/01	7/01	17
19		Configuraciones básicas para la gestión CIMC (IP, máscara, puerta de enlace)	0.5 hrs	7/01	7/01	18
20		**Actualización y configuración**	**5.25 días**	**7/01**	**14/01**	**15**
21		Actualización del equipo (Versión de filtro web).	6 hrs	7/01	8/01	
22		Configuración de políticas para aplicaciones.	8 hrs	8/01	11/01	21
23		Configuración de políticas HTTP/HTTPS	8 hrs	11/01	12/01	22
24		Activación de analisis HTTPS (desencriptación)	8 hrs	12/01	13/01	23
25		Configuración de WCCP / PBR en equipo capa 3 mas cercano al WSA.	4 hrs	13/01	13/01	24
26		Nateos y verificaciones en el firewall	4 hrs	13/01	14/01	25
27		Verificación de la configuración.	4 hrs	14/01	14/01	26
28		**Pruebas de validación para pase a producción**	**7 días**	**14/01**	**25/01**	**20**
29		Despliegue de certificados intermediarios de manera manual o por GPO	4 hrs	14/01	15/01	
30		Selección de segmento de red y redirección de tráfico hacia WSA	4 hrs	15/01	15/01	29
31		Verificación de filtrado pre ajustes	24 hrs	15/01	20/01	30
32		Ajustes en las politicas	8 hrs	20/01	21/01	31
33		Verificación de filtrado post ajustes	24 hrs	20/01	25/01	32CC
34		**Pase a producción**	**4.5 días**	**25/01**	**1/02**	**14**
35		Instalación física del servidor en centro de datos.	4 hrs	25/01	26/01	
36		Acondicionamiento de infraestructura de red para el servidor.	2 hrs	26/01	26/01	35
37		Redirección de todo el tráfico de red hacia WSA	6 hrs	26/01	27/01	36
38		Verificación de filtrado pre ajustes	24 hrs	27/01	1/02	37
39		Ajustes en las politicas	8 hrs	27/01	28/01	38CC
40		Verificación de filtrado post ajustes	24 hrs	27/01	1/02	39CC

Fig. 7: Plan de trabajo por parte de la empresa que implementa

Fuente: Documentación enviada por la empresa Adexus hacia Caja Ica

Por parte de Cmacica se tiene la tabla creación de Políticas o perfiles de acceso, tomando en cuenta los diferentes tipos de accesos y de referencia un perfil que nos deja creada la empresa.

Fig. 8: Plan de trabajo del proyecto

Fuente: Documentación Interna de Caja Municipal Ica

El plan de trabajo del proyecto de la aplicación, igualmente se realizó la calendarización tentativa de fechas para la recepción, ordenamiento, pruebas y pase a producción de la Aplicación Web Segura a nivel de todas las agencias que corresponden a CMACICA.

TABLA III CALENDARIZACIÓN DE LAS TAREAS DEL DESPLIEGUE

Nombre de la tarea	Duración	Comienzo	Fin
Recepción de matriz de accesos según Mof	1 dia	01/07/2022	01/07/2022
Ordenamiento de Perfiles y comparación por posibles cambios	20 dias	04/07/2022	29/07/2022
Pruebas de políticas en diferentes sedes	11 dias	02/08/2022	16/08/2022
Despliegue general	73 dias	17/08/2022	25/11/2022

Fuente: Documentación Interna de Caja Municipal Ica

Dentro de la TABLA 3 se observa la calendarización para hacer la creación o adición de grupos dentro de las matrices de accesos donde se obtiene el Manual de Organización y Funciones (MOF). Dicho MOF es actualizado por el departamento de Organización y Procesos la cual es compartido al Área de Seguridad de la Información y Ciberseguridad donde este asigna los accesos por puesto de trabajo finalizando él envió a la Unidad de infraestructura Tecnológica para su ejecución.

Para poder agrupar por perfiles de trabajo se hizo el trabajo de validar perfil por perfil de trabajo de forma minuciosa con el fin de que no halla errores.

Al momento de la implementación se llegaron a crear 23 perfiles los cuales se encuentran en los anexos del presente trabajo los cuales no contiene por tipo de empleo, sino que tiene los mismos accesos, por ejemplo, en el perfil 1 se encuentran en su mayoría los jefes de y funcionarios de caja ica.

3.3.2 Implementación del proyecto

La Implementación del Proyecto de bloqueo de páginas web mediante Aplicación Web Segura salió como iniciativa de la Unidad de Infraestructura Tecnológica a razón de tener un mejor control del acceso a internet dando un bloqueo y monitoreo del acceso a páginas web (HTTP y HTTPS) como aplicaciones.

Por ello se elevó hacia nuestra gerencia de TI para presentarlo como iniciativa en comité de gerencia. Donde se aprobó para la implementación.

En el punto anterior se muestran los planes de trabajo que se van a realizar como la implementación y el despliegue.

Para la implementación se hizo un análisis de espacio dentro de los gabinetes auto contenidos que tenemos en Caja Ica la carga térmica y la carga energética ya que los equipos generan calor y consumen energía.

El consumo energético de igual forma se tuvo que analizar a que por ser una entidad que no puede parar sus funciones cuenta con baterías de respaldo (UPS) y grupo electrógeno para que puedan trabajar sin interrupciones.

3.3.3 Descripción del proyecto

Dentro del proyecto se tiene como indicador la protección de todos los dispositivos a través de una sofisticada infraestructura global de inteligencia de amenazas, que incluye Cisco Talos Security Inteligencie and Research Group (Talos) que nos garantizara una protección web.

Además de ello se va a implementar el acceso web /aplicaciones por perfiles de trabajo el cual es capturado por el CDA que se está integrando con los active Directory que tenemos en Cmacica

Integre todo en su entorno para unificar la visibilidad, habilitar la automatización y fortalecer la protección.

Habilite el control avanzado de todo el tráfico web, incluido el contenido web dinámico, como las aplicaciones de redes sociales, y bloquee los comportamientos de riesgo sin obstaculizar la productividad del usuario.

Proteja todos los dispositivos a través de una infraestructura global sofisticada de inteligencia contra amenazas, con tecnología de Cisco Talos, y manténgase a la vanguardia de las amenazas con una visibilidad e inteligencia procesable líderes en la industria.

El segmento de IPs que se van a toma es de mascara 8 que nos da 16777214 host o ips el cual son las agencias de CMACICA y tenemos Holgura de ips libres para poder expandirnos sin problemas.

3.3.4 Alcance del proyecto

Para la implementación WSA fue necesario establecer su alcance segmentos a donde se va aplicar (IPs) , Perfiles de políticas tanto en política de descifrado y política de acceso.

TABLA IV ALCANCE DEL PROYECTO EXPRESADO EN REQUERIMIENTOS

Alcance	Requerimiento
Ac001	Alcance de segmento (172.0.0.0/8)
Ac002	Creacion de Decryption Policies
Ac003	Creación de Access Policies
Ac004	Indicador de cantidad de equipos activos

Dentro de la TABLA 4 se observa que el rango de red que va a tomar seria nuestra lan interna que empieza con 172.x.x.x con mascara 8 lo cual nos da un numero de 16777214 host o ips donde se van a conectar.

Dicho rango de IPs, afecta directamente a nuestras agencias /oficinas donde se tiene un gran número de equipos y donde se tiene el mayor tráfico de red ya que se encuentran los administradores, analistas de créditos, oficinas administrativas, entre otros

3.4 Implementación de la solución

Dentro de la CMAC contamos con los firewalls externos como internos los cuales suplían la función de bloqueo de acceso de acceso a Internet mediante IPs.
Lo cual generaba un poco de malestar puesto que al momento que un usuario cambiaba de agencia se debía liberar la nueva ip generando la pérdida de tiempo hora/Hombre por lo que se opto por adquirir el filtro web seguro que tenemos, el cual lee el usuario que esta logueado dentro del equipo y dicho usuario pertenece a un grupo de seguridad. Dicho grupo de seguridad es leído por la Aplicación Web Segura y hace la búsqueda dentro de las configuraciones y otorga o restringe el acceso a internet.
Por ejemplo, si el usuario con el perfil de Gerente tiene acceso a páginas de categoría Videoconferencia en la agencia o lugar donde se autentique este va a tener los mismos accesos evitando estar liberando ips donde valla a estar laborando o visitando.

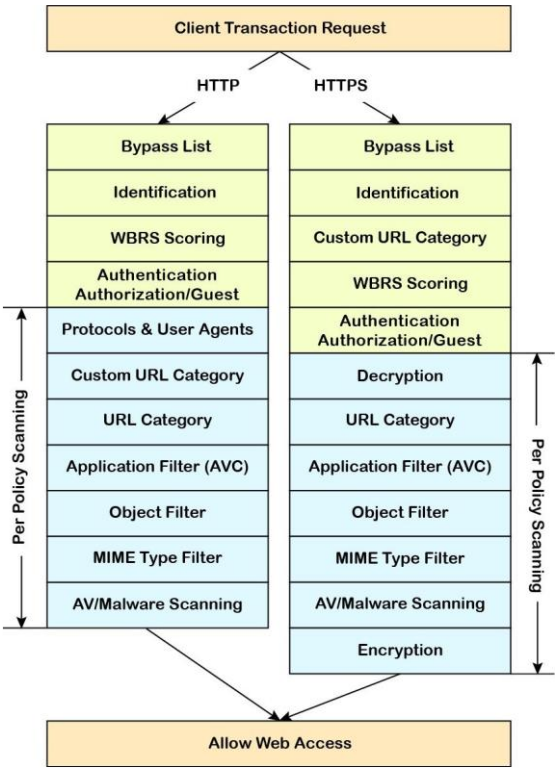


Fig. 9: Flujo de análisis realizado por Aplicación Web Segura.

Fuente: Documentación enviada por la empresa Adexus hacia Caja Ica

Dentro de la FIG 9 se puede observar cómo pasa el trafico HTTP (puerto 80) y HTTPS (puerto 443). Todo el tráfico es recibido por la Aplicación Web Segura (WSA) se analiza y hace el pase por capas como se muestra en la imagen, por ejemplo, si entramos a la paginas asociadas a Caja Municipal Ica como la SBS a la cual se hace la identificación cae en la categoría Gubernamental la cual está habilitada en todos los perfiles dentro de Caja Municipal Ica hace también un escáner de antimalware y brinda finalmente el acceso todo en cuestión de milisegundos sin afectar la productividad.

Antes de iniciar las configuraciones vamos a ingresar sesión, en esta ocacion iniciamos con mi usuario LESA para realizar las configuraciones

Fig. 10 Ingreso a consola de administración

Fuente: Imagen obtenida de la consola de administración de web segura de Caja Municipal de Ica

Dentro de los usuarios que se encuentran dentro de la consola de administración de web segura de Cisco se tienen usuarios con privilegios de administrador y usuarios con permisos de lectura, por ejemplo, mi usuario LESA tiene privilegios de administrador para poder realizar los cambios/ configuraciones que se van a demostrar en las siguientes figuras.

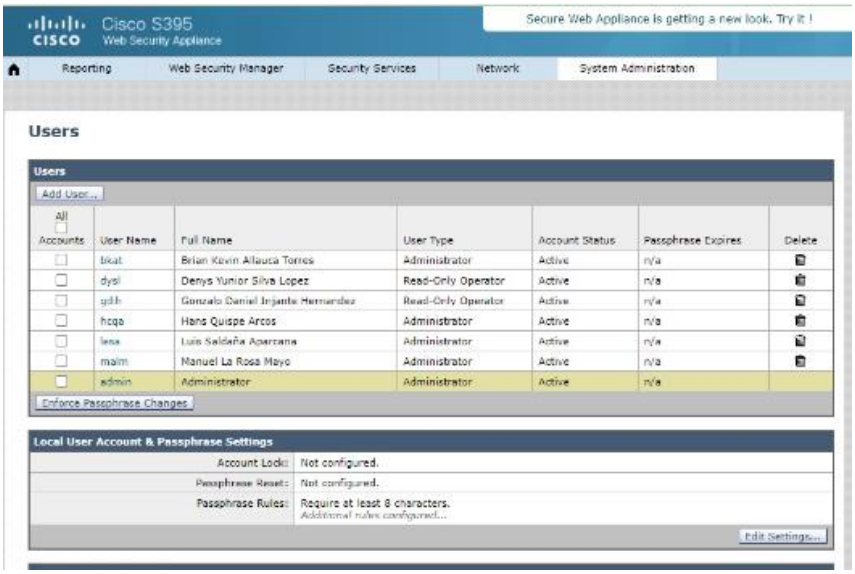


Fig. 11 Usuarios Creados dentro de la consola

Los servidores de Aplicación Web Segura tienen acceso a internet ya que finalmente son estos los que acceden a las múltiples páginas web y no los usuarios. Para se establecen los parámetros de DNS.

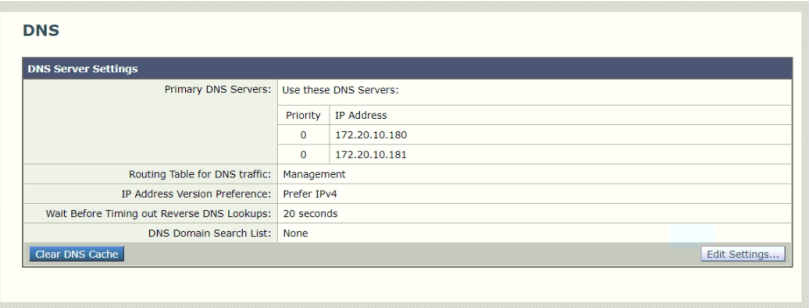


Fig. 12: Parámetros DNS.

Fuente: Imagen obtenida de la consola de administración de web segura de Caja Municipal de Ica

Dentro de Caja Municipal Ica se tienen Controladores de Dominio (AD) de lo cual se pueden identificar en la FIG 12

Dentro de los controladores de dominio (AD) se encuentran usuarios de dominio, grupos de seguridad y grupos de distribución. Adicional a ello dentro del AD hace la autenticación y validación de los usuarios, clave de inicio de sesión actualizada.

Dentro de las licencias tenemos lo siguientes:

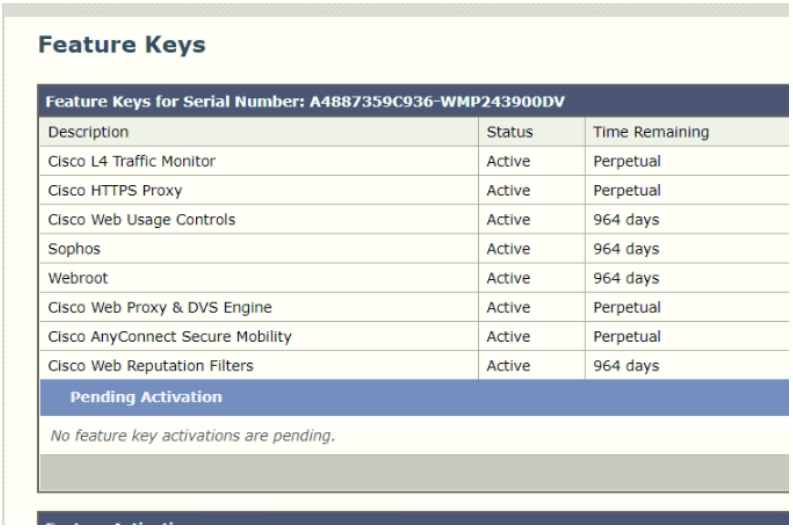


Fig. 13: Características habilitadas – Licencias.

Fuente: Imagen obtenida de la consola de administración de web segura

Dentro de la FIG 13 se observa las licencias que se tienen asignadas dentro de la web segura de Cisco (WSA).

Los perfiles de identificación permiten seleccionar dirección de host, segmentos de red, usuario o grupos de Active Directory. También características avanzadas como protocolos y puertos de proxy.

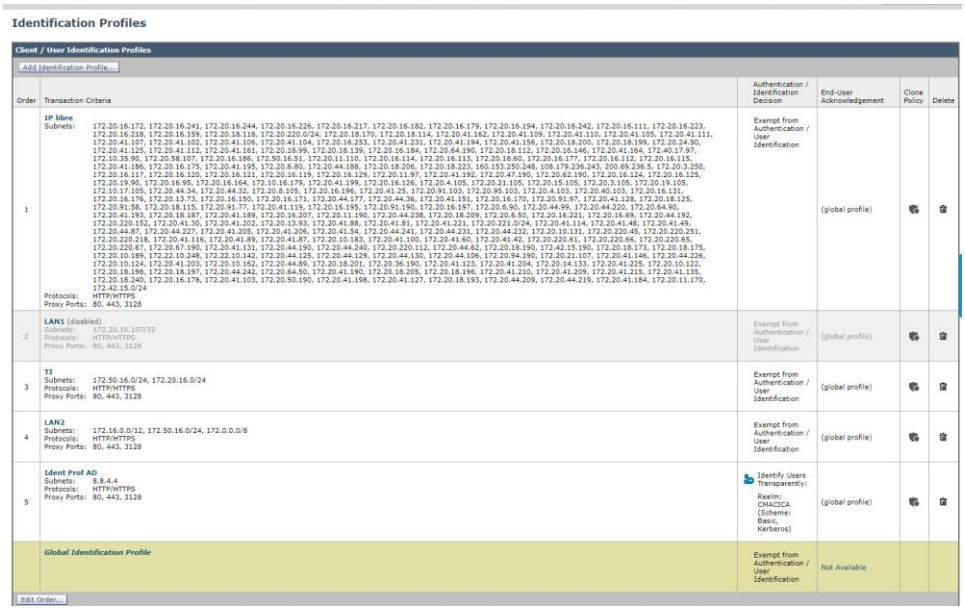


Fig. 14: Perfiles de autenticación

Fuente: Imagen obtenida de la consola de administración de web segura

En nuestro caso contamos con 4 perfiles de autenticación, la primera que es IP libre, dentro de esta política tiene el paso total y sin restricciones claro dando un nivel de seguridad que nos brinda WSA, allí donde se encuentra los equipos de Gerencia Central, Jefaturas y usuarios especiales.

Otro perfil se encuentra el grupo de TI el cual se tiene acceso a páginas referentes a desarrollo como Wordpress, AWS, github entre otras.

En tercer lugar, se el perfil que cae a los equipos de agencia siguiendo el lineamiento del core de negocio.

Por último, se tiene la política de autenticación de usuarios el cual brinda el acceso a cada usuario por su puesto de trabajo. Los perfiles de autenticación se pueden modificar la prioridad por ejemplo si queremos que primero se autentiquen los perfiles de los usuarios el perfil Ident Prof Ad se posiciona en primera escala y los otros perfiles se ejecutan siempre y cuando no pasen por Ident Prof Ad.

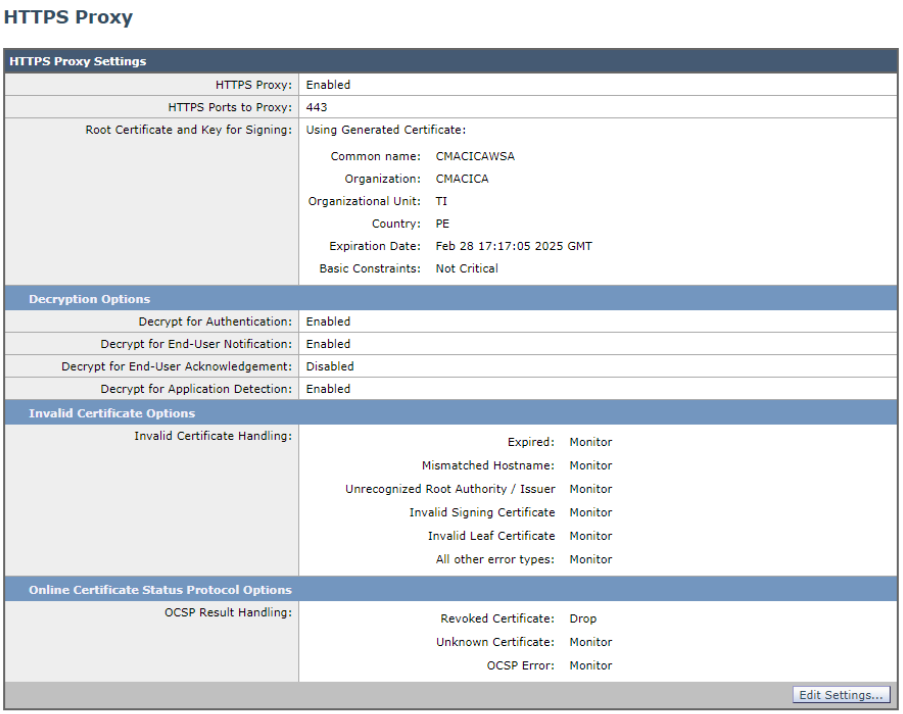


Fig. 15: Proxy https habilitado y certificado generado.

Fuente: Imagen obtenida de la consola de administración de web segura

Para que las políticas de acceso puedan funcionar se requiere tener instalado el Certificado digital para que halla la comunicación entre equipo final con WSA, dicho certificado finaliza el 28 de febrero del 2025 el cual se tendría que renovar en esa fecha. Los despliegues de los certificados se hacen por tareas ejecutados en el AD con el fin de su instalación sea automática y no de forma manual.

También se habilitó el proxy http en los puertos 80 y 3128. El modo de trabajo es transparente. Esto quiere decir que no hay necesidad de que el usuario configure su explorador web para que la data sea analizada por la Aplicación Web Segura. La labor de reenvió de tráfico web la realiza el firewall interno por medio de enrutamiento basado en políticas – PBR

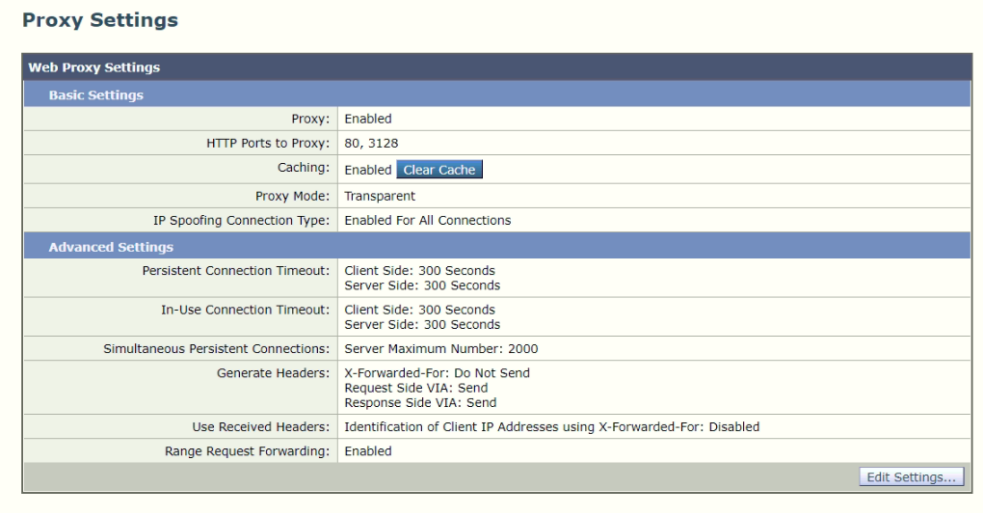


Fig. 16: Proxy http habilitado.

Fuente: Imagen obtenida de la consola de administración de web segura

Otra característica habilitada es el uso de puntajes de reputación para el análisis.

Esta información es proporcionada por Cisco TALOS y utilizada por Aplicación Web Segura para tomar tomar una acción, por ejemplo: Si la IP o URL tiene un puntaje de 0, entonces el tráfico será des encriptado y analizado con las políticas locales, si

por el contrario, el valor es -9.5, el usuario no podrá acceder al sitio web, pero si el puntaje es 7, la página web cargará sin problema.

Los primeros filtros de reputación web del sector proporcionan una potente capa externa de defensa. Aprovechando SenderBase , los filtros de reputación web de Cisco analizan más de 50 tráfico web diferentes y parámetros relacionados con la red para evaluar con precisión la fiabilidad de una URL. Se utilizan sofisticadas técnicas de modelado de seguridad para ponderar individualmente cada parámetro y generar una única puntuación en una escala de -10 a +10. Las políticas configuradas por el administrador se aplican de forma dinámica, en función de las puntuaciones de reputación. [6]

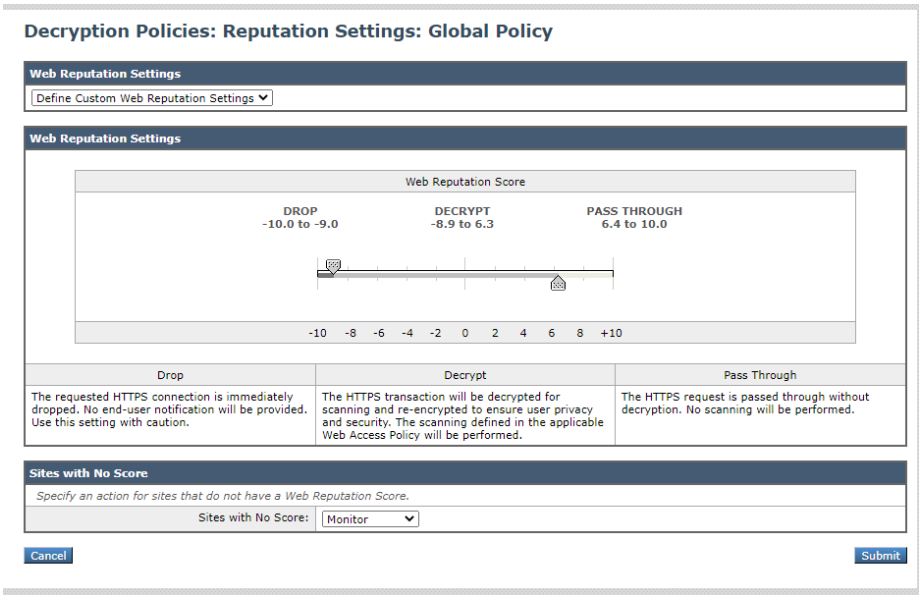


Fig. 17: Parámetros de reputación

Fuente: Imagen obtenida de la consola de administración de web segura

Adicional a ello se pueden crear categorías de URL externas y personalizadas ya que, al bloquear una categoría de forma parcial, con las categorías personalizables se puede liberar o bloquear páginas que quizás no estén categorizadas dentro de cisco.

Las aplicaciones de confianza de videoconferencia son: Microsoft Teams, Meet de google, Zoom, y cisco Webex.

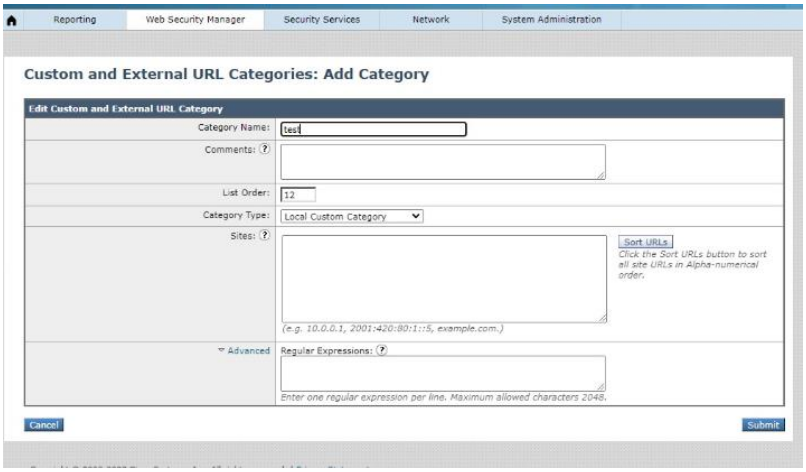


Fig. 18 Creación de Categorías personalizadas

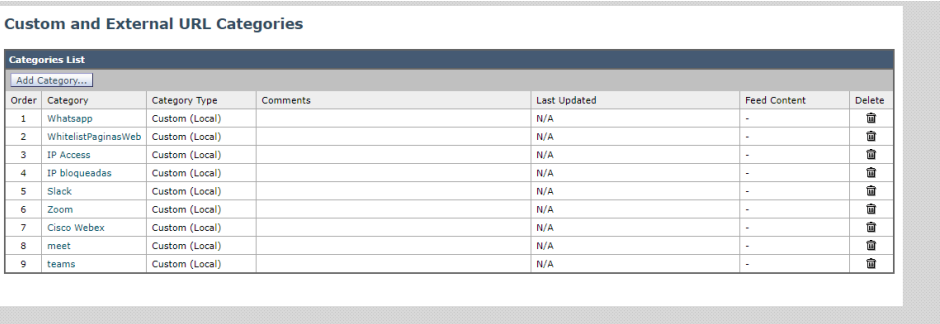


Fig. 19: Categorías externas Personalizadas

Fuente: Imagen obtenida de la consola de administración de web segura

El acceso a internet lo podemos hacer por 2 métodos, por autenticación de usuarios con conexión al active directory o por acceso de ips (imagen 8) por el cual se muestra de las siguientes formas

La categoría en la que cae una URL está determinada por una base de datos de categorías de filtrado. El dispositivo Web Security recopila información y mantiene una base de datos separada para cada motor de filtrado de URL. Las bases de datos de categorías de filtrado reciben periódicamente actualizaciones del servidor de actualización de Cisco y son mantenidas por Cisco TALOS. Talos, el grupo de investigación e inteligencia de seguridad de Cisco, realiza un seguimiento constante de un amplio conjunto de atributos para evaluar las conclusiones sobre un host determinado.

Puede haber situaciones en las que desee clasificar una URL/dominio/dirección IP de manera diferente y tener una clasificación local personalizada para su caja. Puede lograr esto con Categorías de URL personalizadas.

Cuando el motor de filtrado de URL hace coincidir una categoría de URL con la URL de una solicitud de cliente, primero evalúa la URL con las categorías de URL personalizadas incluidas en el grupo de políticas. Si la URL de la solicitud no coincide con una categoría personalizada incluida, el motor de filtrado de URL la compara con las categorías de URL predefinidas.[10]

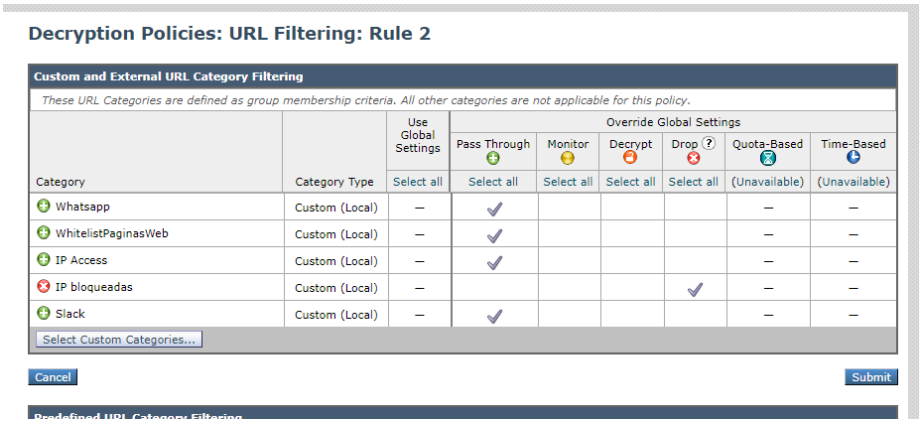


Fig. 20: Politica de decifrado

Fuente: Imagen obtenida de la consola de administración de web segura

3.5 Creación de reglas.

Creamos como primera instancia la política de descifrado y le nombramos Rule2 en el cual no va a tener autenticación, se trabajarán con los puertos 8080,443 y 3128.
Las políticas de descifrado definen el manejo del tráfico HTTPS dentro del proxy web:

- Cuándo descifrar el tráfico HTTPS.
- Cómo manejar las solicitudes que utilizan certificados de seguridad revocados o no válidos.

Puede crear políticas de descifrado para manejar el tráfico HTTPS de las siguientes maneras:

- Pasar a través del tráfico encriptado.
- Descifre el tráfico y aplique las políticas de acceso basadas en contenido definidas para el tráfico HTTP. Esto también hace posible el escaneo de malware. [11]

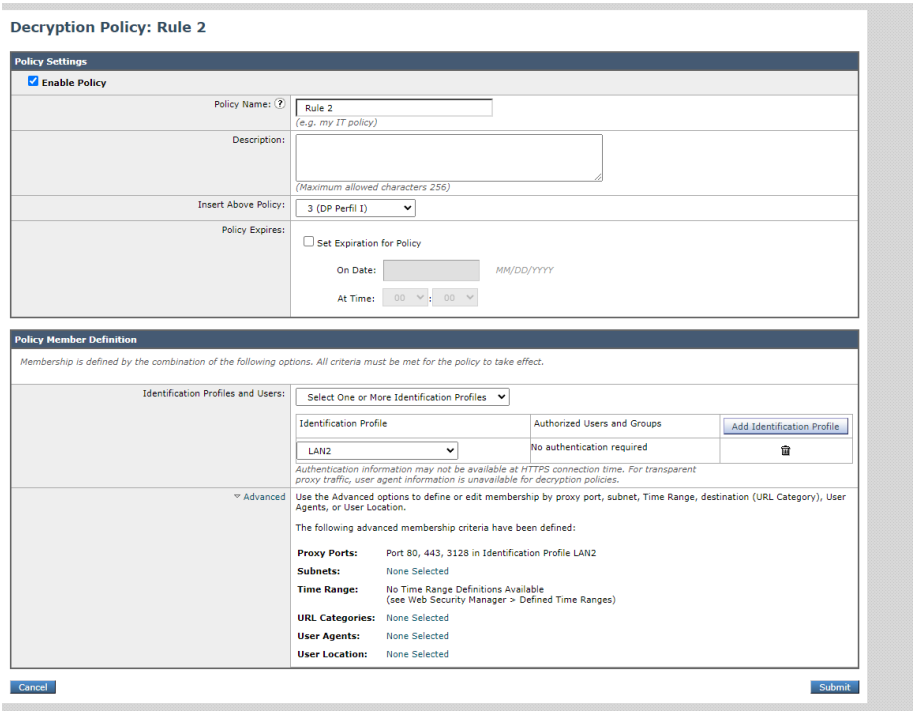


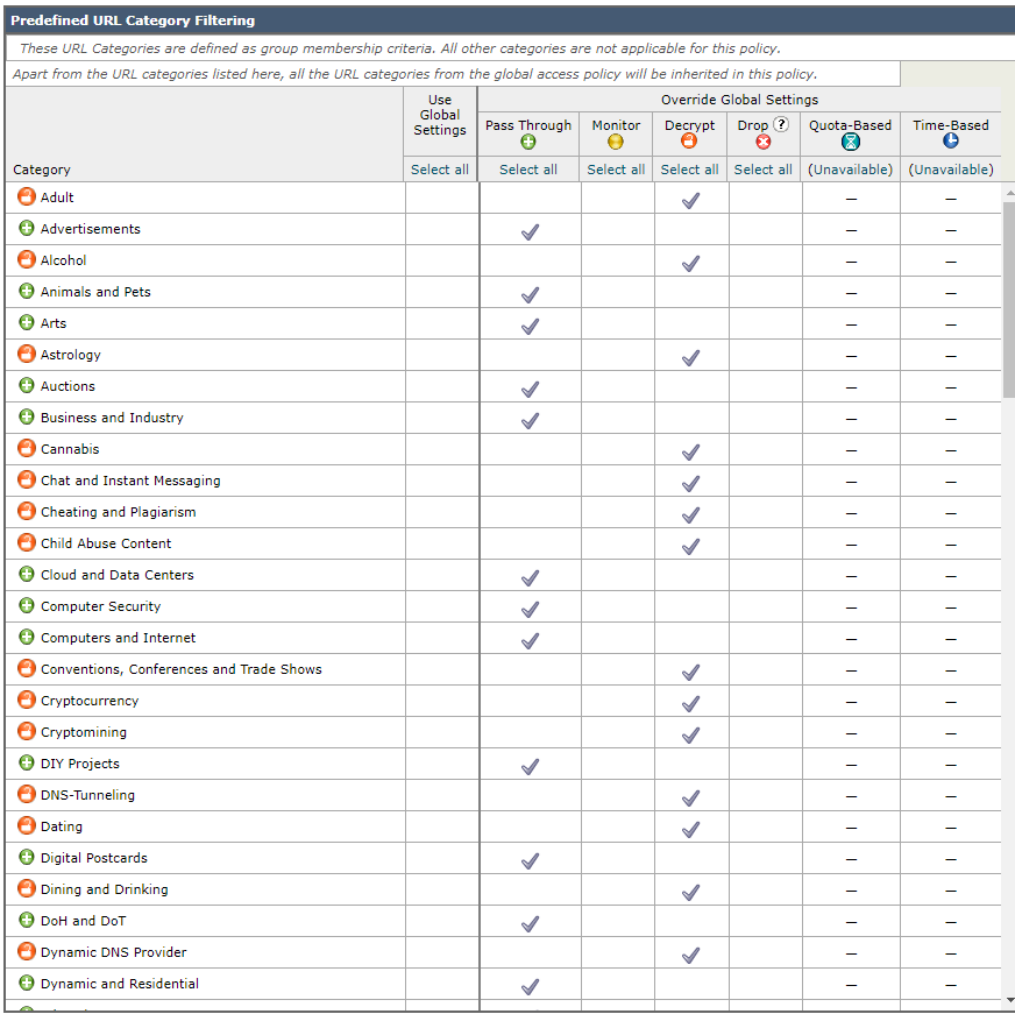
Fig. 21: Creación de nueva regla

Fuente: Imagen obtenida de la consola de administración de web segura

Seleccionamos los accesos y bloqueo al cual va a tener el grupo lo que se observa en la figura 21,22,23 y 24 lo que hace que la Aplicación Web Segura pueda des encriptar la información que pasa y pueda mejor catalogarlo dando así una mejor seguridad.

Se aplicarán políticas de enrutamiento, políticas accesos y política de descifrado. [12]

La norma (ISO/IEC 27032) facilita la colaboración segura y fiable para proteger la privacidad de las personas en todo el mundo. De esta manera, puede ayudar a prepararse, detectar, monitorizar y responder a los ataques", han explicado desde ISO. La organización espera que ISO/IEC 27032 permita luchar contra ataques de ingeniería social, hackers, malware, spyware y otros tipos de software no deseado. [13]



Predefined URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Apart from the URL categories listed here, all the URL categories from the global access policy will be inherited in this policy.

Category	Use Global Settings	Override Global Settings					
		Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Adult				✓		–	–
Advertisements		✓				–	–
Alcohol				✓		–	–
Animals and Pets		✓				–	–
Arts		✓				–	–
Astrology				✓		–	–
Auctions		✓				–	–
Business and Industry		✓				–	–
Cannabis				✓		–	–
Chat and Instant Messaging				✓		–	–
Cheating and Plagiarism				✓		–	–
Child Abuse Content				✓		–	–
Cloud and Data Centers		✓				–	–
Computer Security		✓				–	–
Computers and Internet		✓				–	–
Conventions, Conferences and Trade Shows				✓		–	–
Cryptocurrency				✓		–	–
Cryptomining				✓		–	–
DIY Projects		✓				–	–
DNS-Tunneling				✓		–	–
Dating				✓		–	–
Digital Postcards		✓				–	–
Dining and Drinking				✓		–	–
DoH and DoT		✓				–	–
Dynamic DNS Provider				✓		–	–
Dynamic and Residential		✓				–	–

Fig. 22: Política de descifrado: Filtrado de URL en la regla 2

Fuente: Imagen obtenida de la consola de administración de web segura

Dentro de esta política se va a configurar que es lo que a va pasar y si va a pasar se tiene que descifrar para que nuestro WSA pueda leer y analizar la página web solicitante. Con esto se gana que nuestro WSA pueda descifrar lo que contiene la página web.

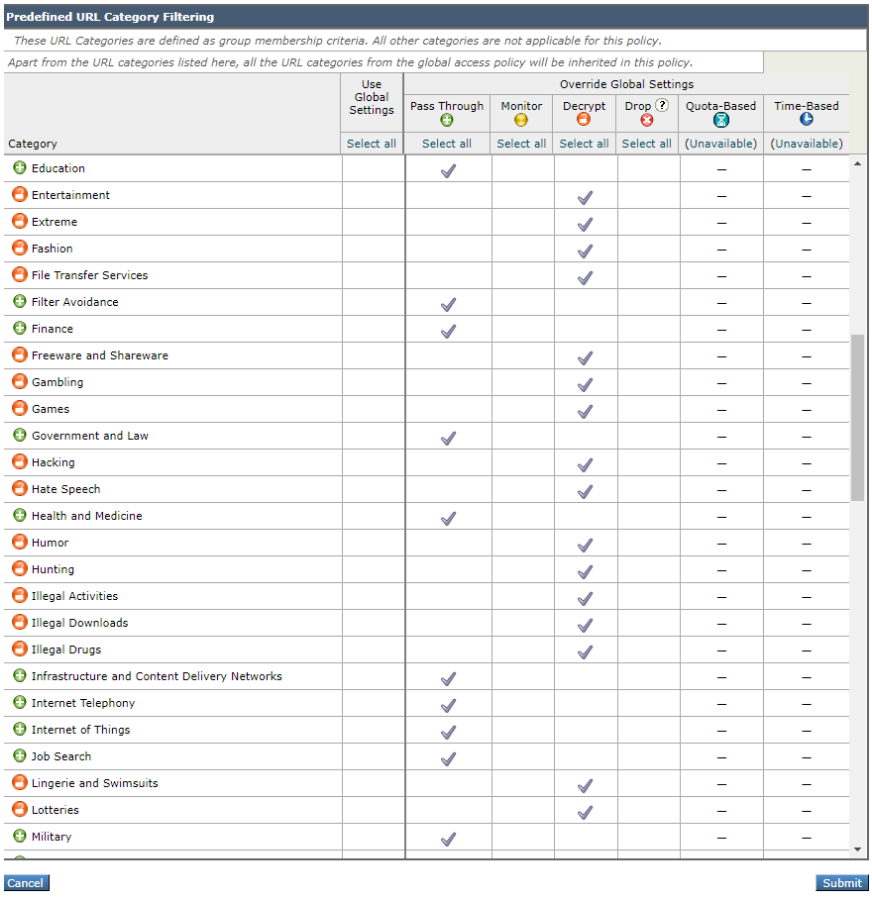


Fig. 23: Política de descifrado: Filtrado de URL en la regla 2
Fuente: Imagen obtenida de la consola de administración de web segura

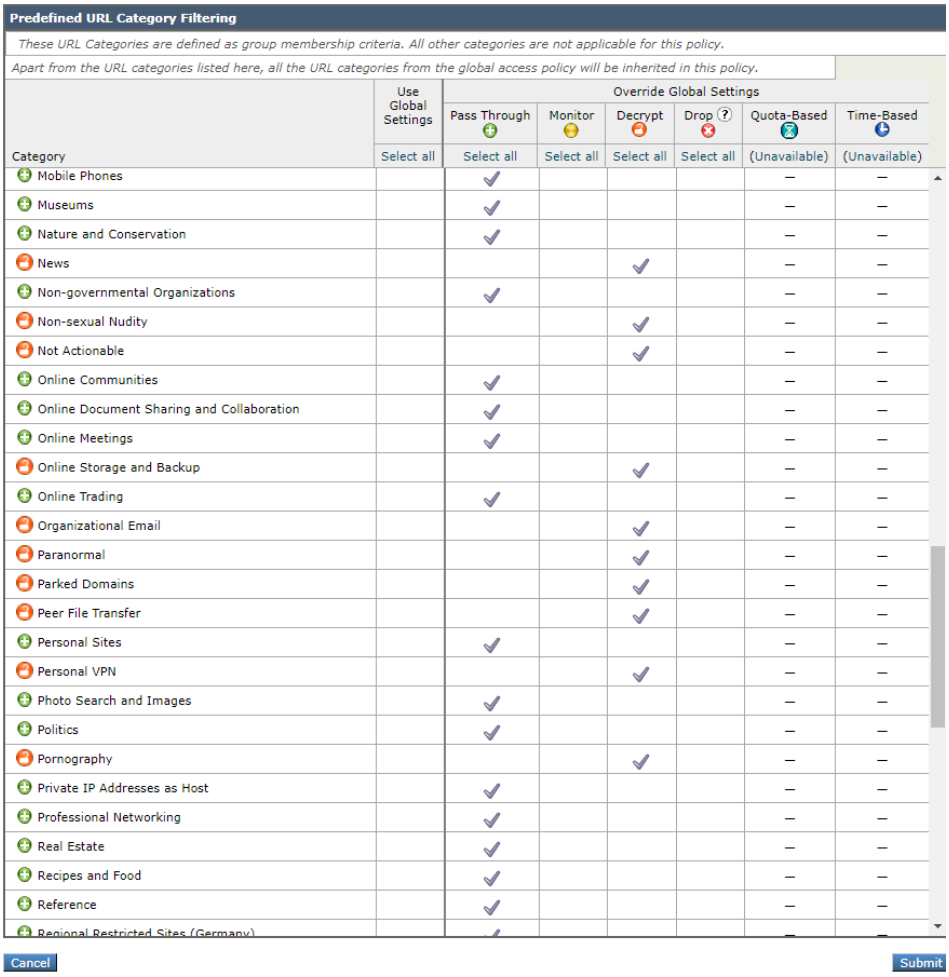


Fig. 24: Política de descifrado: Filtrado de URL en la regla 2

Fuente: Imagen obtenida de la consola de administración de web segura

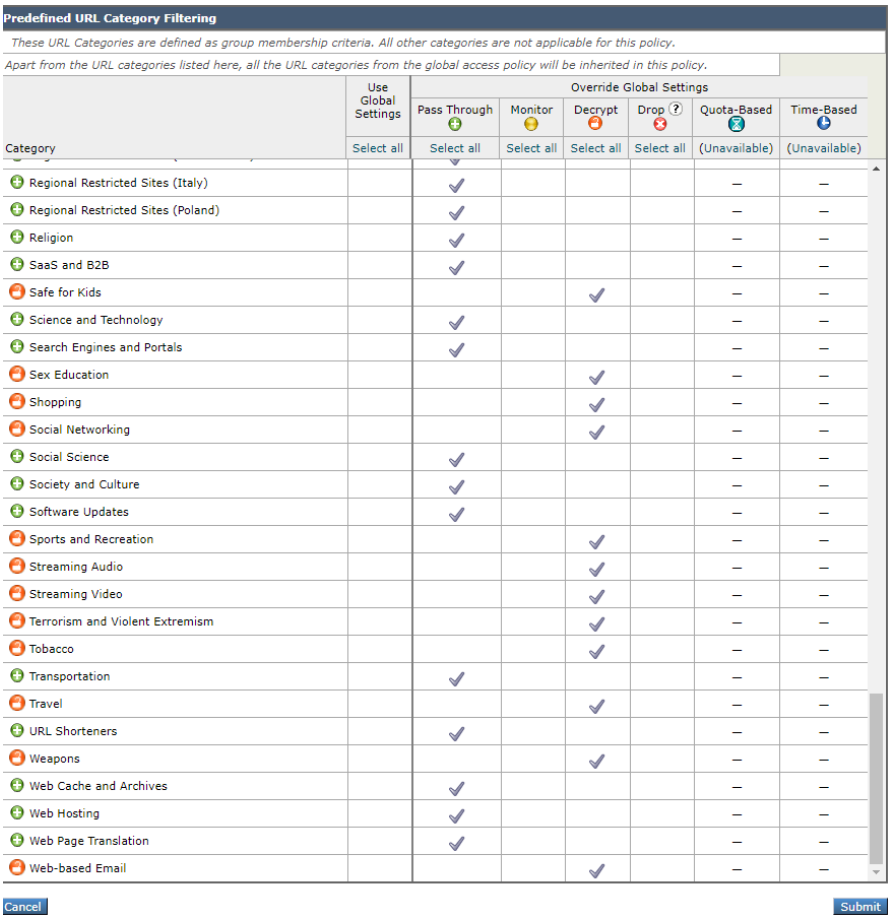
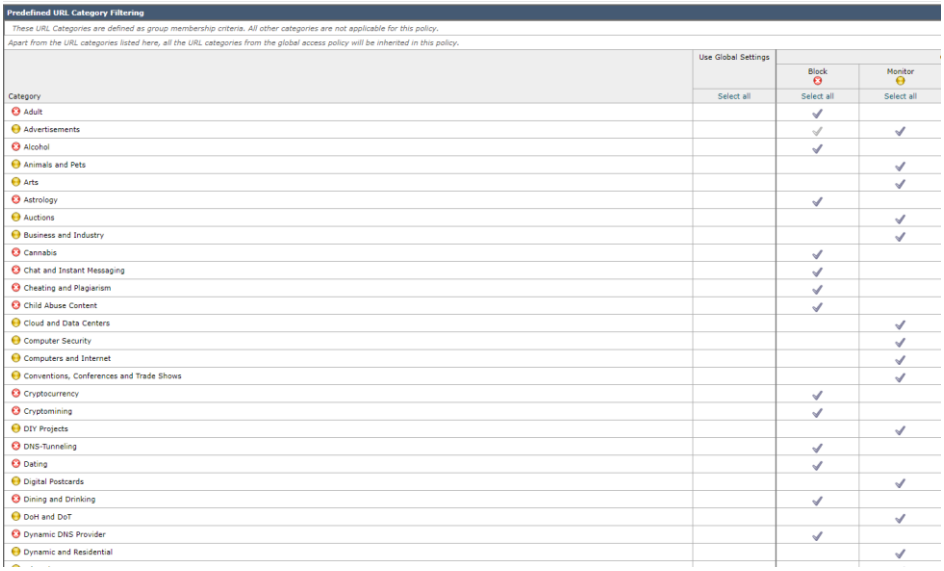


Fig. 25: Política de descifrado: Filtrado de URL en la regla 2

Fuente: Imagen obtenida de la consola de administración de web segura

Una vez que acabamos en la sección de políticas de descifrado le damos en guardar y pasamos al acceso de política el cual va de igual forma se crea y damos los accesos o bloqueo.

Se pueden observar dentro la figura 25,26,27 y 28.



Predefined URL Category Filtering

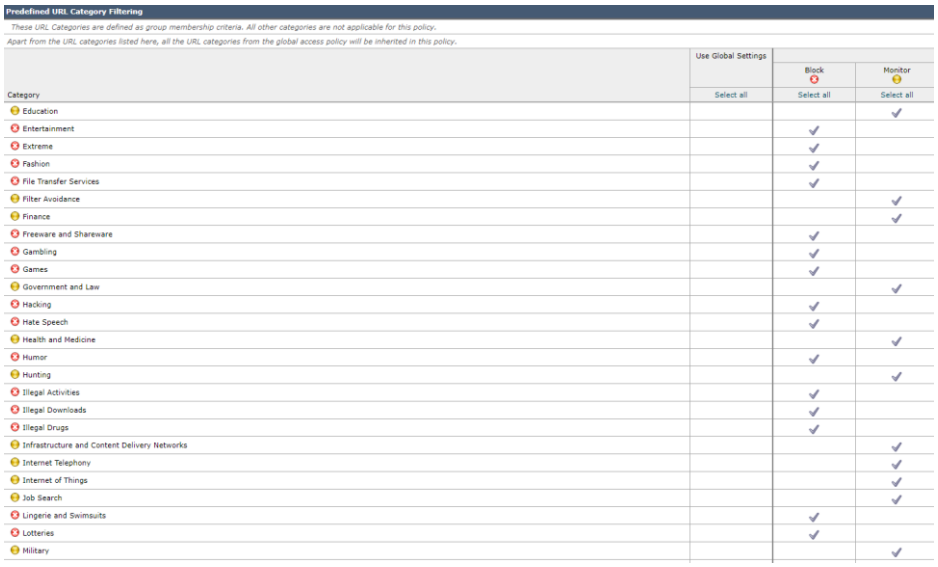
These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Apart from the URL categories listed here, all the URL categories from the global access policy will be inherited in this policy.

Category	Use Global Settings	Block	Monitor
	Select all	Select all	Select all
Adult		✓	
Advertisements		✓	✓
Alcohol		✓	
Animals and Pets			✓
Arts			✓
Astrology		✓	
Auctions			✓
Business and Industry			✓
Cannabis		✓	
Chat and Instant Messaging		✓	
Cheating and Plagiarism		✓	
Child Abuse Content		✓	
Cloud and Data Centers			✓
Computer Security			✓
Computers and Internet			✓
Conventions, Conferences and Trade Shows			✓
Cryptocurrency		✓	
Cryptomining		✓	
DIY Projects			✓
DNS-Tunneling		✓	
Dating		✓	
Digital Postcards			✓
Dining and Drinking		✓	
DoH and DoT			✓
Dynamic DNS Provider		✓	
Dynamic and Residential			✓

Fig. 26: Política de acceso: Filtrado de URL en la regla 2

Fuente: Imagen obtenida de la consola de administración de web segura



Predefined URL Category Filtering

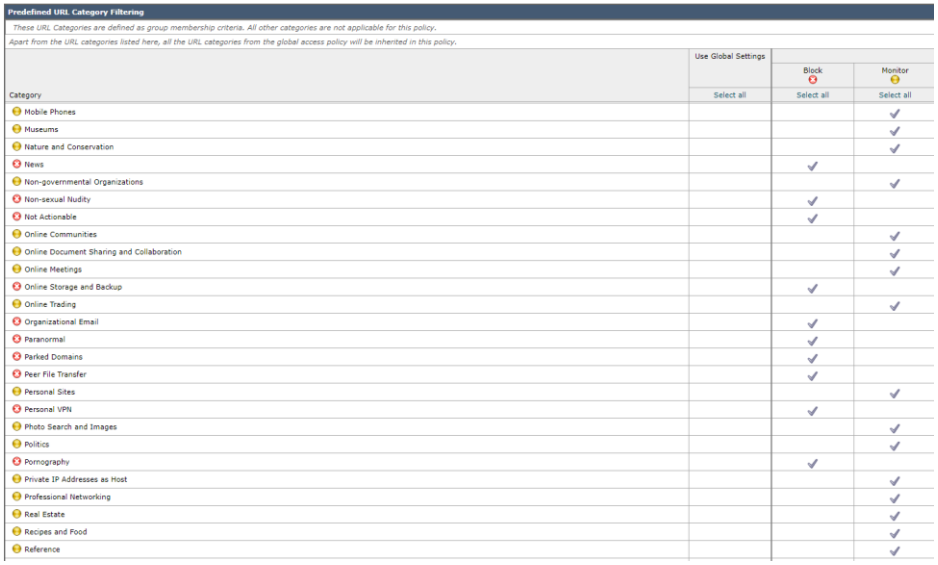
These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Apart from the URL categories listed here, all the URL categories from the global access policy will be inherited in this policy.

Category	Use Global Settings	Block	Monitor
	Select all	Select all	Select all
Education			✓
Entertainment		✓	
Extreme		✓	
Fashion		✓	
File Transfer Services		✓	
Filter Avoidance			✓
Finance			✓
Freeware and Shareware		✓	
Gambling		✓	
Games		✓	
Government and Law			✓
Hacking		✓	
Hate Speech		✓	
Health and Medicine			✓
Humor		✓	
Hunting			✓
Illegal Activities		✓	
Illegal Downloads		✓	
Illegal Drugs		✓	
Infrastructure and Content Delivery Networks			✓
Internet Telephony			✓
Internet of Things			✓
Job Search			✓
Lingerie and Swimsuits		✓	
Lotteries		✓	
Military			✓

Fig. 27: Política de acceso: Filtrado de URL en la regla 2

Fuente: Imagen obtenida de la consola de administración de web segura



Predefined URL Category Filtering

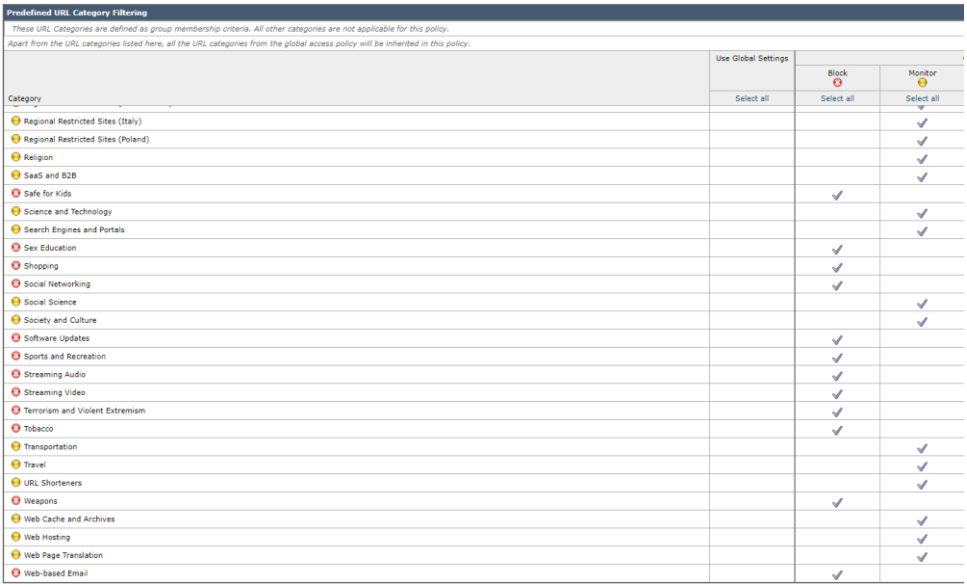
These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Apart from the URL categories listed here, all the URL categories from the global access policy will be inherited in this policy.

Category	Use Global Settings	Block	Monitor
	Select all	Select all	Select all
Mobile Phones			✓
Museums			✓
Nature and Conservation			✓
News		✓	
Non-governmental Organizations			✓
Non-sexual Nudity		✓	
Not Actionable		✓	
Online Communities			✓
Online Document Sharing and Collaboration			✓
Online Meetings			✓
Online Storage and Backup		✓	
Online Trading			✓
Organizational Email		✓	
Paranormal		✓	
Parked Domains		✓	
Peer File Transfer		✓	
Personal Sites			✓
Personal VPN		✓	
Photo Search and Images			✓
Politics			✓
Pornography		✓	
Private IP Addresses as Host			✓
Professional Networking			✓
Real Estate			✓
Recipes and Food			✓
Reference			✓

Fig. 28: Política de acceso: Filtrado de URL en la regla 2

Fuente: Imagen obtenida de la consola de administración de web segura



Predefined URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Apart from the URL categories listed here, all the URL categories from the global access policy will be inherited in this policy.

Category	Use Global Settings	Block	Monitor
	Select all	Select all	Select all
Regional Restricted Sites (Italy)			✓
Regional Restricted Sites (Poland)			✓
Religion			✓
SaaS and B2B			✓
Safe for Kids		✓	
Science and Technology			✓
Search Engines and Portals			✓
Sex Education		✓	
Shopping		✓	
Social Networking		✓	
Social Science			✓
Society and Culture			✓
Software Updates		✓	
Sports and Recreation		✓	
Streaming Audio		✓	
Streaming Video		✓	
Terrorism and Violent Extremism		✓	
Tobacco		✓	
Transportation			✓
Travel			✓
URL Shorteners			✓
Weapons		✓	
Web Cache and Archives			✓
Web Hosting			✓
Web Page Translation			✓
Web-based Email		✓	

Fig. 29: Política de acceso: Filtrado de URL en la regla 2

Fuente: Imagen obtenida de la consola de administración de web segura

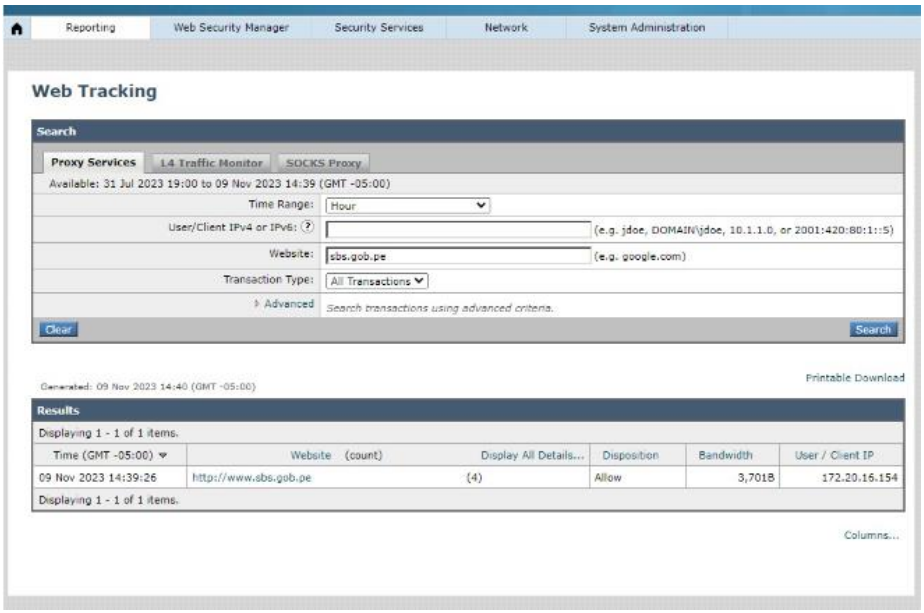


Fig. 30 Validación de página Web

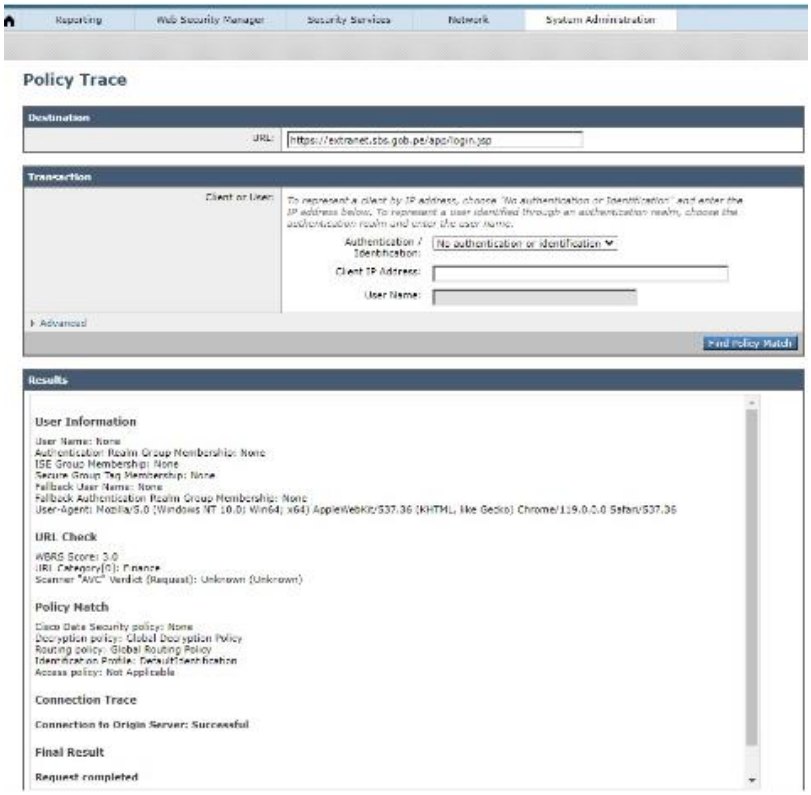


Fig. 31 Validación de trafico de una página Web

Para validar que las configuraciones se encuentran bien ejecutadas podemos hacer un test, nos dirigimos en la sección de Reporting - Web Tracking para ver si hay tráfico, como se observa en la Fig. 27.

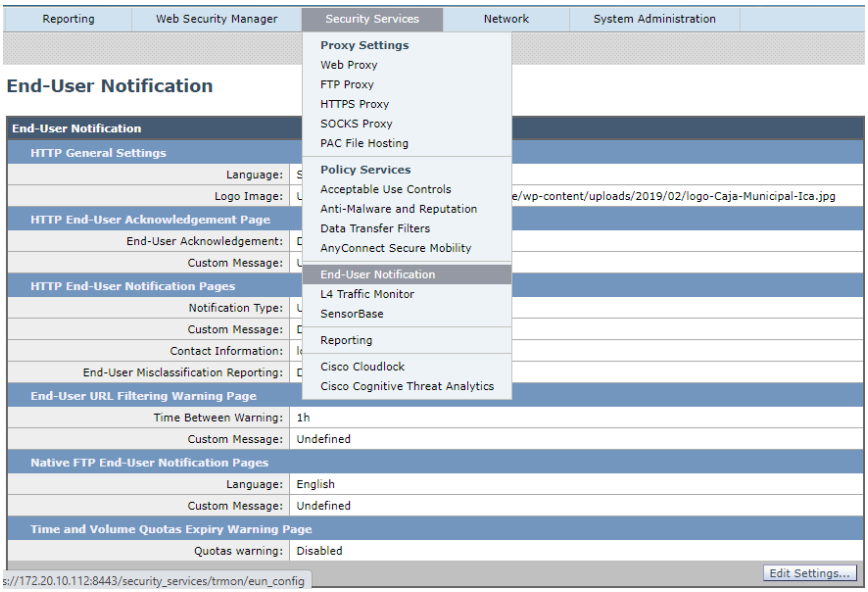


Fig. 32: Configuración de Mensaje a usuarios finales

Fuente: Imagen obtenida de la consola de administración de web segura

En la FIG 26 vamos a configurar el mensaje de bloqueo que va a visualizar al momento de ingresar una página prohibida. Para ello nos dirigimos la sección Security Services ---- End User Notification y seleccionamos en editar

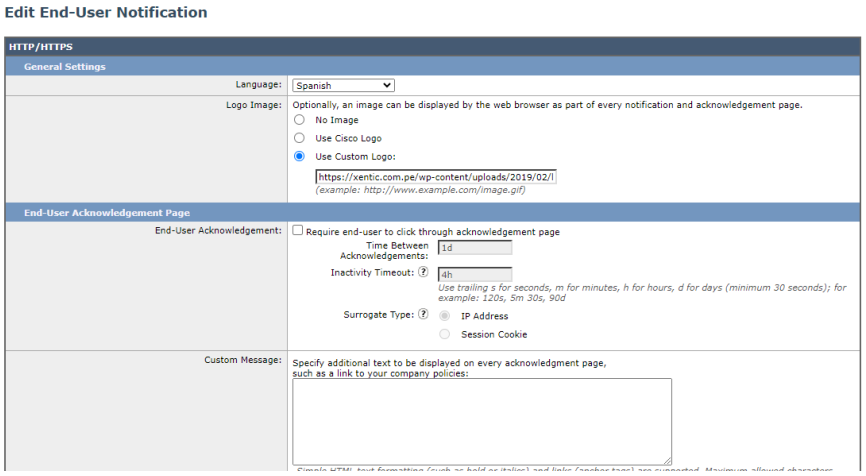


Fig. 33:Configuración de mensaje a usuarios finales

Fuente: Imagen obtenida de la consola de administración de web segura

En la FIG 27 agregamos el logotipo de Caja Municipal Ica donde se va a observar en la FIG 29. El Logo puede ser cualquiera, pero para fines de mejor presentación y acorde a la empresa seleccionamos que sería el logo de Caja Ica

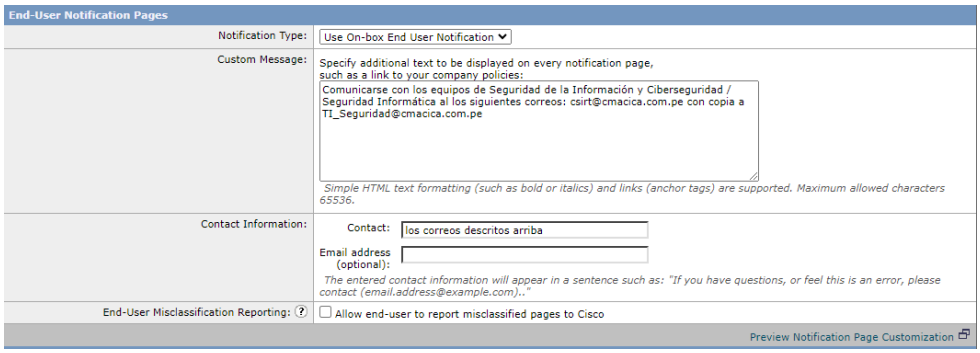


Fig. 34:Configuración de mensaje a usuarios

Fuente: Imagen obtenida de la consola de administración de web segura

Dentro del mensaje se va a incluir lo siguiente: “Comunicarse con los equipos de Seguridad de la Información y Ciberseguridad / Seguridad Informática a los siguientes correos: csirt@cmacica.com.pe con copia a TI_Seguridad@cmacica.com.pe”

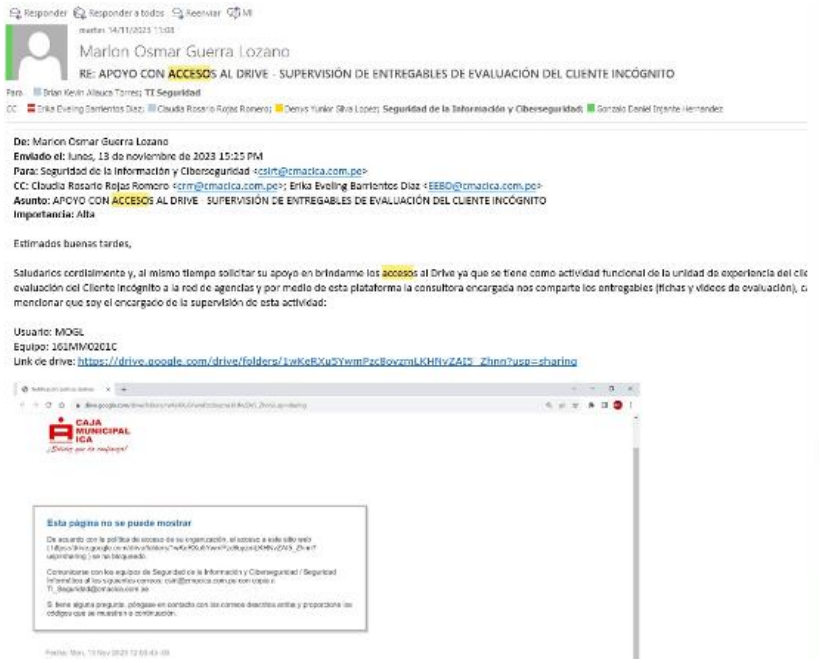


Fig. 35 Solicitud de accesos

Fig. 36:Mensaje final ante una página bloqueada

Fuente: Imagen obtenida de la consola de administración de web segura

En la FIG 36 se observa el mensaje que le aparece al usuario que desea acceder a páginas que no van acorde al Core o páginas que no son categorizadas.

Para realizar los permisos especiales a usuarios o perfiles se hace el siguiente flujo:

El usuario envía un correo al área de Seguridad de la Información con Copia al área de Infraestructura y Comunicaciones, una vez que el área de Seguridad de la Información da el visto bueno, nuestra área de Infraestructura y Comunicaciones ejecuta lo solicitando creando un perfil nuevo o una variación de perfiles en el perfil seleccionados.

Desde esta etapa se va a demostrar la efectividad de la solución en imágenes obtenidas por la web segura de cisco, como los reportes y ello.

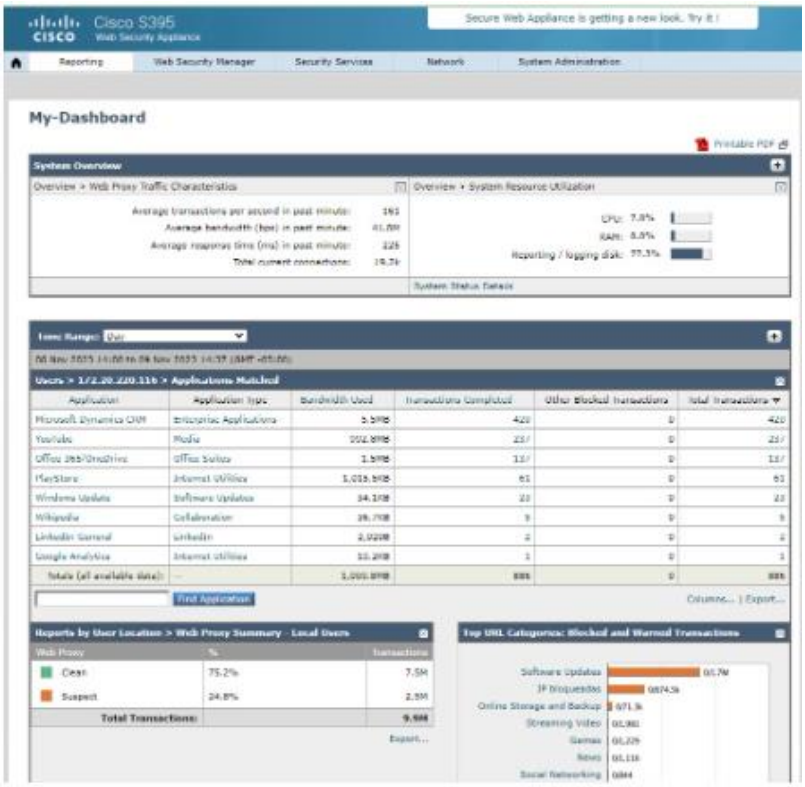


Fig. 37 Dashboard principal al iniciar sesión

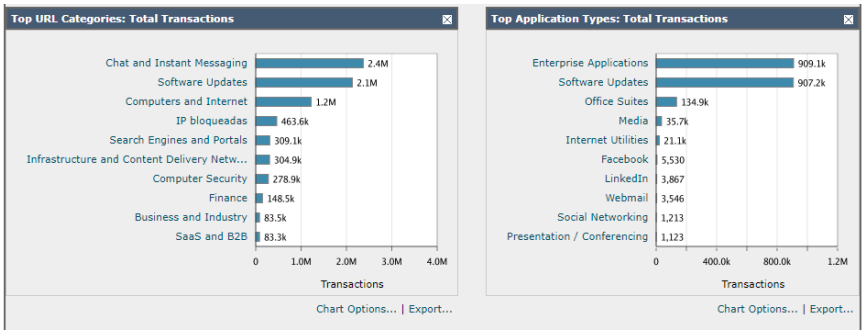


Fig. 38: Reporte generado

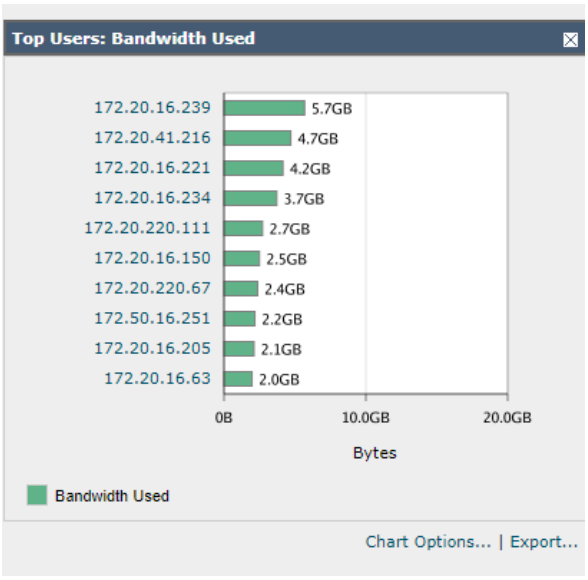


Fig. 39: Reporte de usuarios que más se conectan

Fuente: Imagen obtenida de la consola de administración de web segura

Dentro del equipo Web Segura de Aplicaciones se pueden sacar múltiples reportes como el que se puede observar en la FIG 39 y 40.

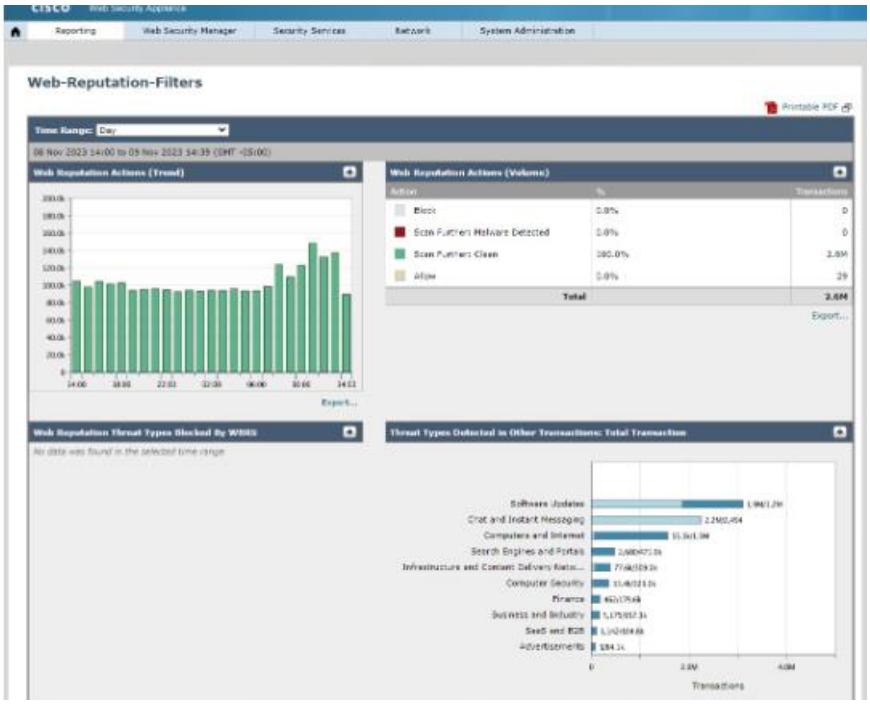


Fig. 40 Reputación Web Filtrada

También podemos sacar un reporte de reputación web filtrada como se observa en la figura que se encuentra arriba.

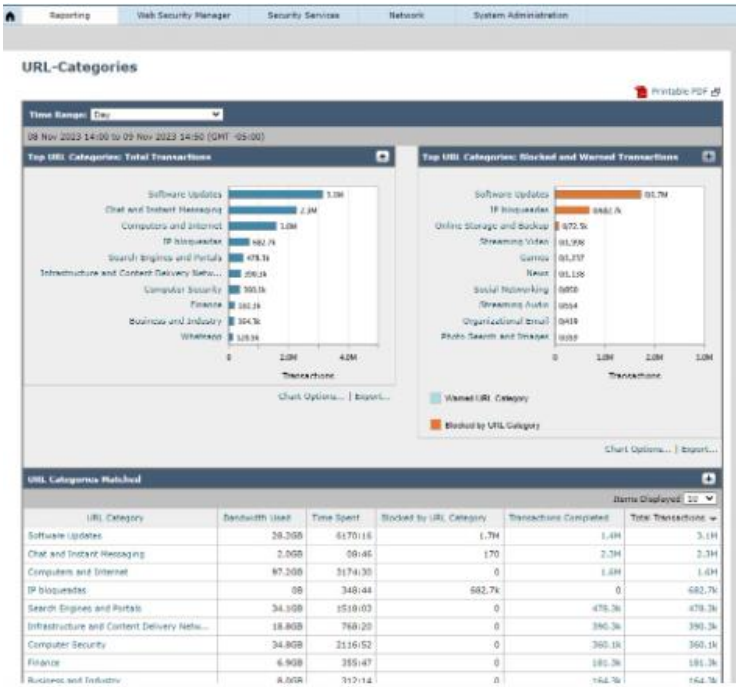


Fig. 41 Categorías de URL

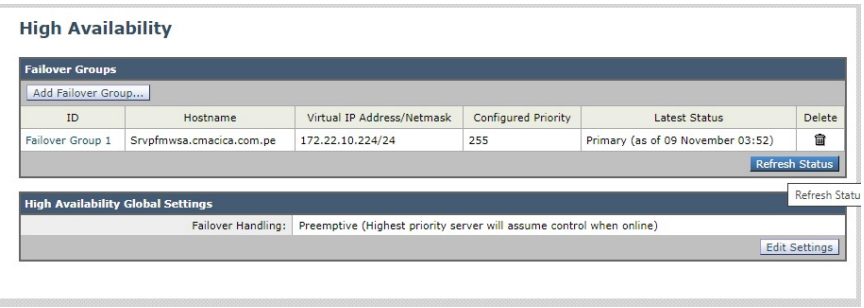


Fig. 42 Alta Disponibilidad

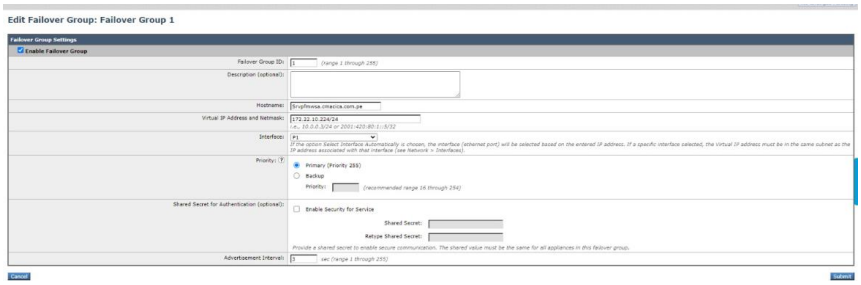


Fig. 43 Editar la Alta Disponibilidad

Para poder validar que tenemos alta disponibilidad se va a tener que hacer un Failover por lo que se tiene que agregar la ip Virtual dando prioridad 255 para el primario y 254 u otro número para el secundario, para hacer el failover se tendría que pasar el principal como backup y el backup como principal.

Con esto garantizamos que exista la Alta Disponibilidad (HA) de los servicios en caso pase un evento como que el equipo principal falle.

Mantenimiento de consola de administración de Web segura con cisco

Dentro del mantenimiento pactado entre Caja Municipal Ica con la empresa Adexus son los mantenimiento físicos y lógicos en el cual tiene como objetivo actualizar con los últimos parches de Cisco como versiones de sistema operativo, mantenimiento a discos físicos y limpieza física de dichos equipos.

Por ello ingresamos por consola (SSH) al cual ingresamos por líneas de comandos, en este caso usaremos el programa putty.[14]

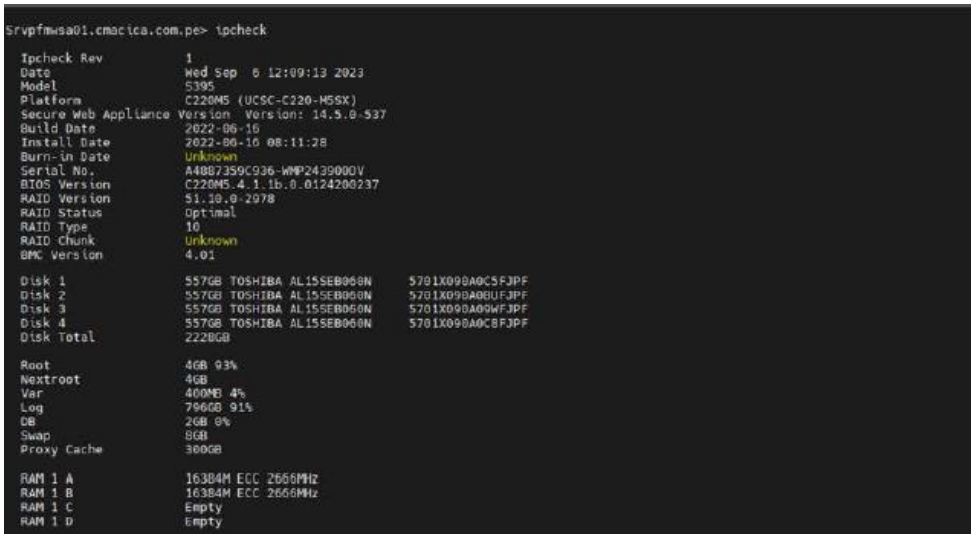


Fig. 44 Versión de Firmware de Web Segura de Cisco 1

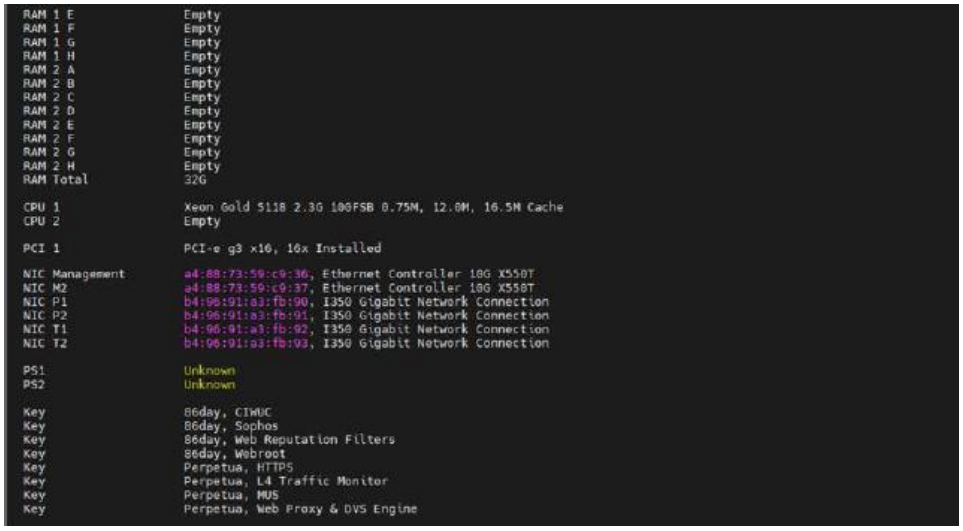


Fig. 45 Versión de Firmware de Web Segura de Cisco 1

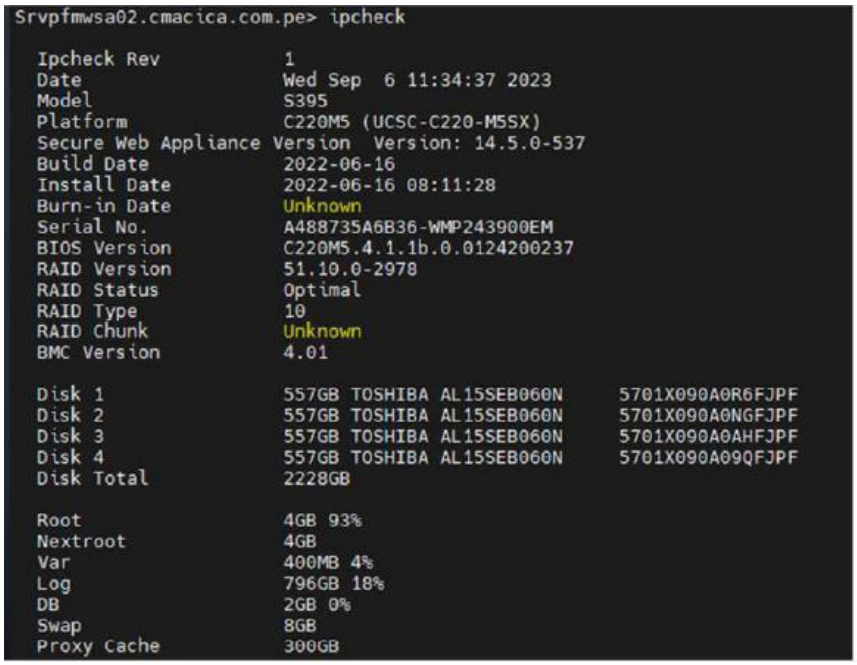


Fig. 46 Versión de Firmware de Web Segura de Cisco 2

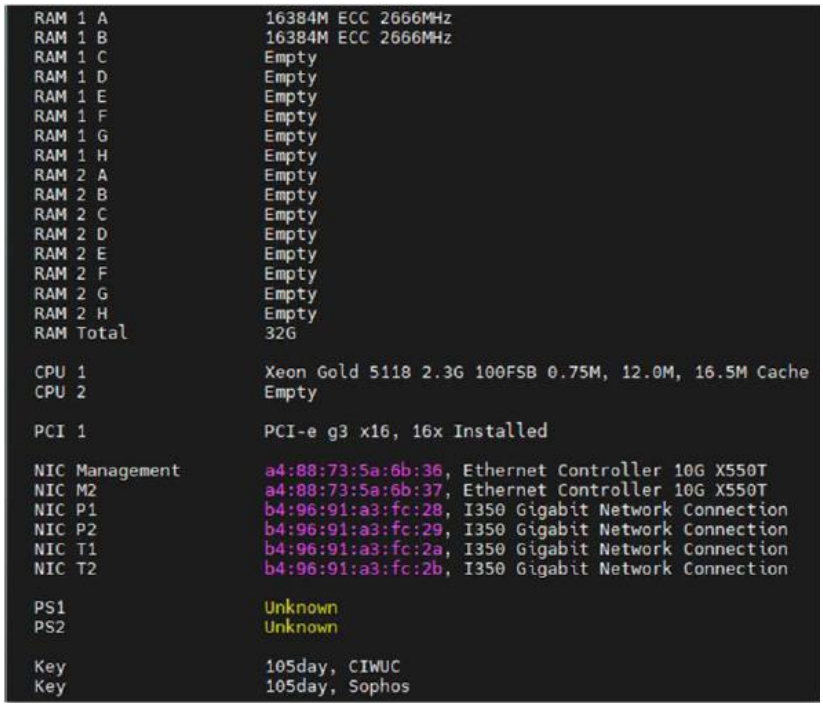


Fig. 47 Versión de Firmware de Web Segura de Cisco 2

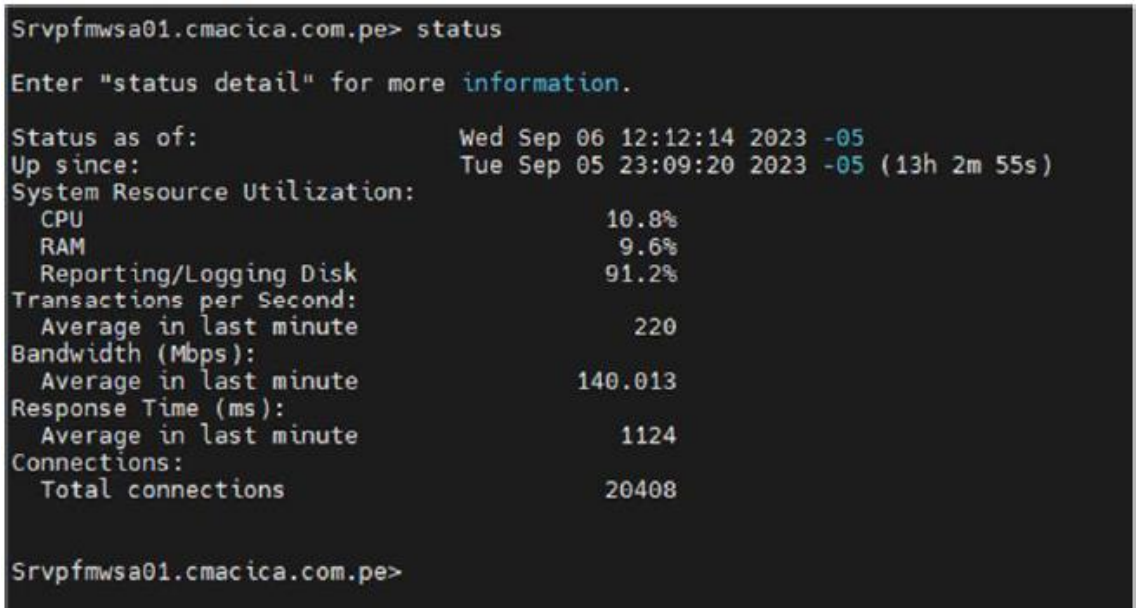


Fig. 48 Memoria Ram y CPU de Web Segura de Cisco 1

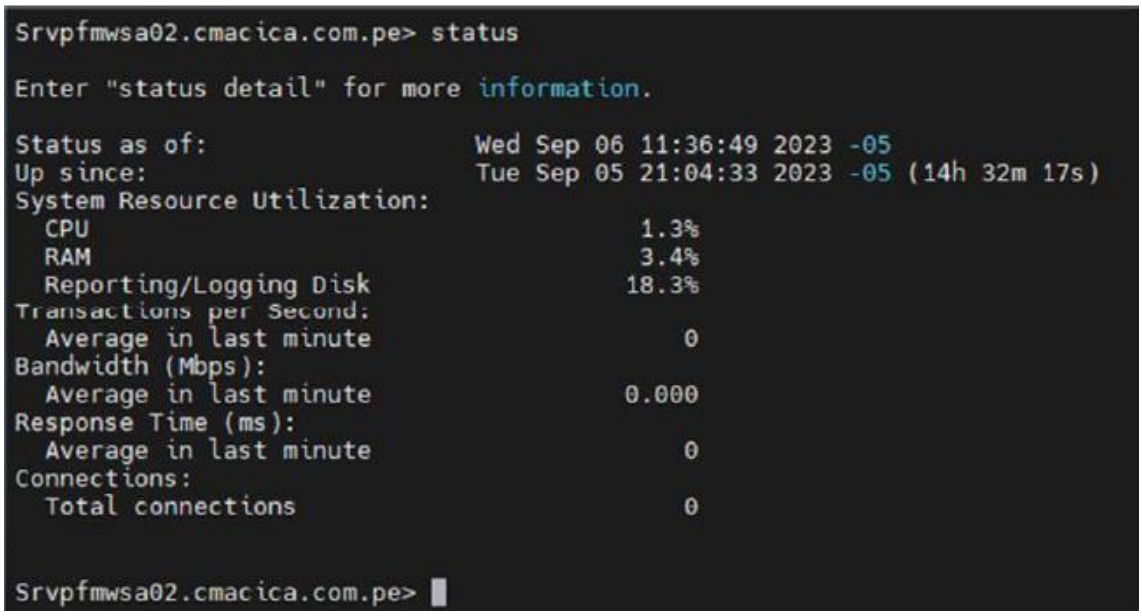


Fig. 49 Memoria Ram y CPU de Web Segura de Cisco 2

Para realizar el mantenimiento profundo del disco de la Web Segura de Cisco se genera ticket con misma Marca de Cisco

Fig. 50 Ticket Generado con el TAC de Cisco

En esta seccion podemos obsercar la version del software, modelo entre otra informacion del equipo.

Web Appliance Version Information	
Model:	S395
Version:	14.5.0-537 for Web
Build Date:	2022-06-16
Install Date/Time:	2022-06-16 08:11:28
Serial Number:	A4887359C936-WMP243900DV
Hardware	
RAID Status:	Optimal

Fig. 51 Informacion del Appliance

Para poder garantizar la alta disponibilidad se hacen las pruebas de cambio de prioridad, a ello se le llama hacer un Failover es un modo operativo de respaldo en el que un componente secundario asume las funciones de un componente del sistema cuando el componente principal deja de estar disponible. El propósito del failover es hacer que un sistema sea más tolerante a errores. La conmutación por error puede aplicarse a cualquier aspecto de un sistema: dentro de una computadora personal, por ejemplo, la conmutación por error puede ser un mecanismo para proteger contra un procesador fallido; dentro de una red, la conmutación por error se puede aplicar a cualquier componente de red o sistema de componentes, como una ruta de conexión, un dispositivo de almacenamiento o un servidor web. Por ejemplo, un servidor de conmutación por error resulta cuando un servidor de respaldo está configurado y preparado para asumir el control cuando falla el servidor primario.

La configuración de failover requiere dos dispositivos de seguridad idénticos conectados el uno al otro a través de un link de failover dedicado y, opcionalmente, de un link de stateful failover. El estado de las unidades y las interfaces activas se monitorea para determinar si se cumplen las condiciones específicas de failover. Si se cumplen esas condiciones, el failover ocurre.

En cuestion de equipo fisico las dos unidades en una configuración de failover deben tener la misma configuración de hardware. Deben tener el mismo modelo, el mismo número y los mismos tipos de interfaces, y la misma cantidad de RAM

En cuestion de equipo logico deben tener la misma versión de software principal (primer número) y de menor importancia (segundo número), pero usted puede utilizar diversas versiones del software dentro de un proceso de actualización.

Fig. 52 Failover de Equipos

CAPÍTULO IV: APORTES A LA INSTITUCIÓN

Los aportes que se ha podido hacer en esta etapa de trabajo serían los siguientes en tanto a mi cargo se Seguridad Informática.

- Mejoro en un 95% de mejora en el acceso a Internet acorde a su perfil de trabajo.
- Se tenía acceso a páginas de almacenamiento en nube lo cual era una brecha de fuga de información la cual se mitigo con la aplicación de Web Segura.
- Optimizamos el uso adecuado de la red orientada al Core de negocio.
- Se están actualizando y parchando vulnerabilidades de Windows de agencias como servidores.
- La herramienta de Aplicación Web Segura nos permite alcanza un estándar de seguridad de muchas entidades no solo financieras ya que se conecta con la red de cisco la cual cataloga el acceso a las páginas.
- Mediante la herramienta se puede monitorear y sacar el acceso a páginas top como también que usuario ha hecho más interacciones visitando paginas libres o bloqueadas.
- Se aumentó el nivel de acceso hacia Internet para los usuarios en un 99%.
- Se aplicaron políticas de seguridad acorde al core de negocio.
- Dentro del área se agregó el EDR dentro de Caja Ica
- Se expandió la protección a nuestras oficinas informativas alejadas usando la nube como solución.
- Se está migrando la consola de administración de Antivirus a Cloud.
- De igual forma la Email Security se tiene ya en Cloud,
- Se mantiene actualizado en conjunto con el SOC el Firewall a razón de evitar posibles ataques

CONCLUSIONES

Después de la experiencia dentro del área de Infraestructura tecnológica en la sección de Seguridad Informática puedo decir que no es fácil pero tampoco difícil ya que fue un reto cambiar la forma de trabajar a los usuarios por lo que puedo llegar a las siguientes conclusiones:

1. Después de las implementaciones realizadas se notó al principio una disconformidad de 80% por parte de los usuarios, pero como fue pasando el tiempo los usuarios empezaron a concientizar que el uso del Internet ya que a las páginas que querían ingresar no estaban acorde del negocio.
2. Se implementaron políticas de acceso a razón de una matriz de acceso el cual se encuentra dentro del anexo, dicha matriz de acceso fue otorgada por el área de Seguridad de la Información y Ciberseguridad de Caja Ica y se mejoró el uso de la red.
3. Después del despliegue de políticas se obtuvo una mejora de un 85% de la red de agencias las cuales al no poder ingresar a páginas que no están asociadas al negocio la banda ancha asignada se emplea solo para aplicaciones/paginas asociadas al negocio.
4. Se redujeron hasta en un 100% las observaciones de auditoria sobre el mal uso de internet por los usuarios.
5. En cuanto a uso de gigas se redujo considerablemente en las agencias de un promedio de 250gb por mes a solo 50 gb.
6. Después de la implementación se redujeron las horas hombre que se usaba para el cambio de políticas por el constante cambio del personal por las agencias

RECOMENDACIONES

Luego de la experiencia vivida en la implementación del Aplicación Web Segura en el área de Seguridad Informática se puede decir lo siguiente:

1. Mantener el equipo actualizado en sus políticas y estándares de seguridad para brindar un mejor servicio con el que se mitigan posibles fugas de información, ataques de ciberseguridad entre otros.
2. Brindar capacitaciones constantes al personal que se encarga de la gestión de los equipos de seguridad informática debido a que ellos son el eslabón más débil dentro las capas de seguridad.
3. Siempre hay que tener la iniciativa de proveer nuevas soluciones informáticas que se puedan encontrar en el mercado o mejorar las que ya tenemos.
4. Recordar que la seguridad dentro de la empresa está en tus manos y de los que laboran en conjunto dentro del área ya que somos responsables de rea.
5. Estar preparados para afrontar alguna adversidad y saber aplicar los conocimientos adquiridos tanto en los estudios universitarios como complementarios.
6. Realizar pruebas de concepto y concientización a los usuarios de la empresa para que se adecuen a las nuevas soluciones y estándares de seguridad. De esta manera se reduce las posibles fallas al momento del despliegue de la solución.
7. Guiarse mucho de los estándares o normas ISO como por ejemplo la Norma ISO/IEC 27032 que trata de los nuevos estándares seguridad.

REFERENCIAS BIBLIOGRÁFICAS

[1] G. G. Huaman Mauricio, G. R. Rojas Marcelo, y J. K. Rojas Marcelo, «Propuesta de implementación de políticas de seguridad basado en CISCO ISE (identity services engine) en la red LAN de Caja Huancayo», Universidad Continental, 2022. [En línea]. Disponible en: https://repositorio.continental.edu.pe/handle/20.500.12394/13127

[2] K. Munive Canchumani, «Rediseño de red LAN aplicando Cisco para mejorar la seguridad y comunicación de la información en la Subdirección de Circulación Terrestre – DRTC Junín», Universidad Nacional del Centro del Perú, 2023. [En línea]. Disponible en: http://repositorio.uncp.edu.pe/handle/20.500.12894/9388

[3] D. Scott y R. Sharp, «Abstracting application-level web security», en *Proceedings of the 11th international conference on World Wide Web*, en WWW '02. New York, NY, USA: Association for Computing Machinery, may 2002, pp. 396-407. doi: 10.1145/511446.511498.

[4] «Quiénes Somos - Caja Ica». [En línea]. Disponible en: https://cajaica.pe/institucional/quienes-somos/

[5] «Propósito, Misión, Visión y Valores - Caja Ica». [En línea]. Disponible en: https://cajaica.pe/institucional/mision-vision-y-valores/

[6] «¿Proporciona el dispositivo de seguridad Cisco Web Security Appliance (WSA) protección frente a malware/spyware?», Cisco. [En línea]. Disponible en: https://www.cisco.com/c/es_mx/support/docs/security/web-security-appliance/117952-qanda-wsa-00.html

[7] «Release Notes for AsyncOS 14.5 for Cisco Secure Web Appliance», Cisco. Accedido: 11 de noviembre de 2023. [En línea]. Disponible en: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa-14-5/release-notes/release-notes-for-wsa-14-5.html

[8] «Proceso de actualización local de WSA/ESA», Cisco. Accedido: 14 de noviembre de 2023. [En línea]. Disponible en: https://www.cisco.com/c/es_mx/support/docs/security/email-security-appliance/117804-technote-wsa-00.html

[9] «Cisco Secure Web Appliance», AVANTEC. [En línea]. Disponible en: https://www.avantec.ch/loesungen/cisco-security/cisco-web-security/

[10] «Define Custom URL Categories in WSA», Cisco. [En línea]. Disponible en: https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/216032-define-custom-url-categories-in-wsa.html

[11] «User Guide for AsyncOS 12.0 for Cisco Web Security Appliances - GD (General Deployment) - Create Decryption Policies to Control HTTPS Traffic [Cisco Secure Web Appliance]», Cisco. [En línea]. Disponible en: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa_12-0/user_guide/b_WSA_UserGuide_12_0/b_WSA_UserGuide_11_7_chapter_01011.html

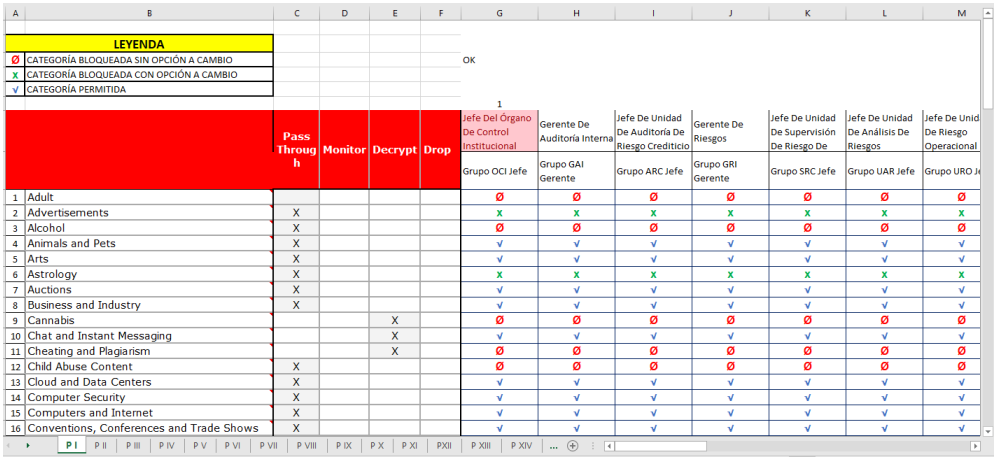
[12] «Introduction to WSA Policies». [En línea]. Disponible en: https://www.kareemccie.com/2019/11/introduction-to-wsa-policies.html

[13] admincpwmx, «Nuevo estándar para seguridad cibernética: ISO/IEC 27032», *Computerworld México*, 10 de septiembre de 2013. [En línea]. Disponible en: https://computerworldmexico.com.mx/Nuevo-estandar-para-seguridad-cibernetica-ISOIEC-27032/

[14] «SSH: qué es y cómo funciona este protocolo». [En línea]. Disponible en: https://www.arsys.es/blog/ssh#:~:text=SSH%20son%20las%20siglas%20de,como%20v%C3%ADa%20para%20las%20comunicaciones.

ANEXOS

Anexo 1: Puestos de trabajo según su afinidad de acceso a internet, en la parte inferior se puede observar los perfiles los cuales tenemos agregados por P de perfil.

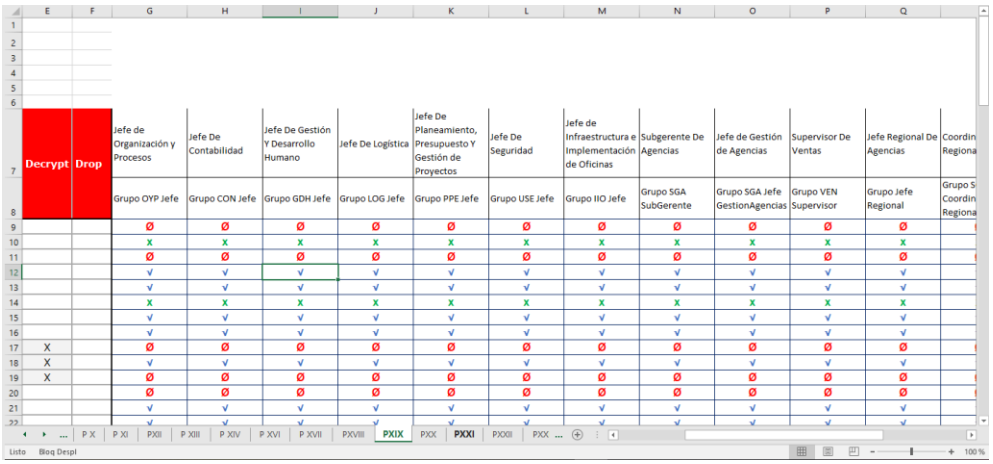


	LEYENDA
Ø	CATEGORÍA BLOQUEADA SIN OPCIÓN A CAMBIO
X	CATEGORÍA BLOQUEADA CON OPCIÓN A CAMBIO
√	CATEGORÍA PERMITIDA

OK

1

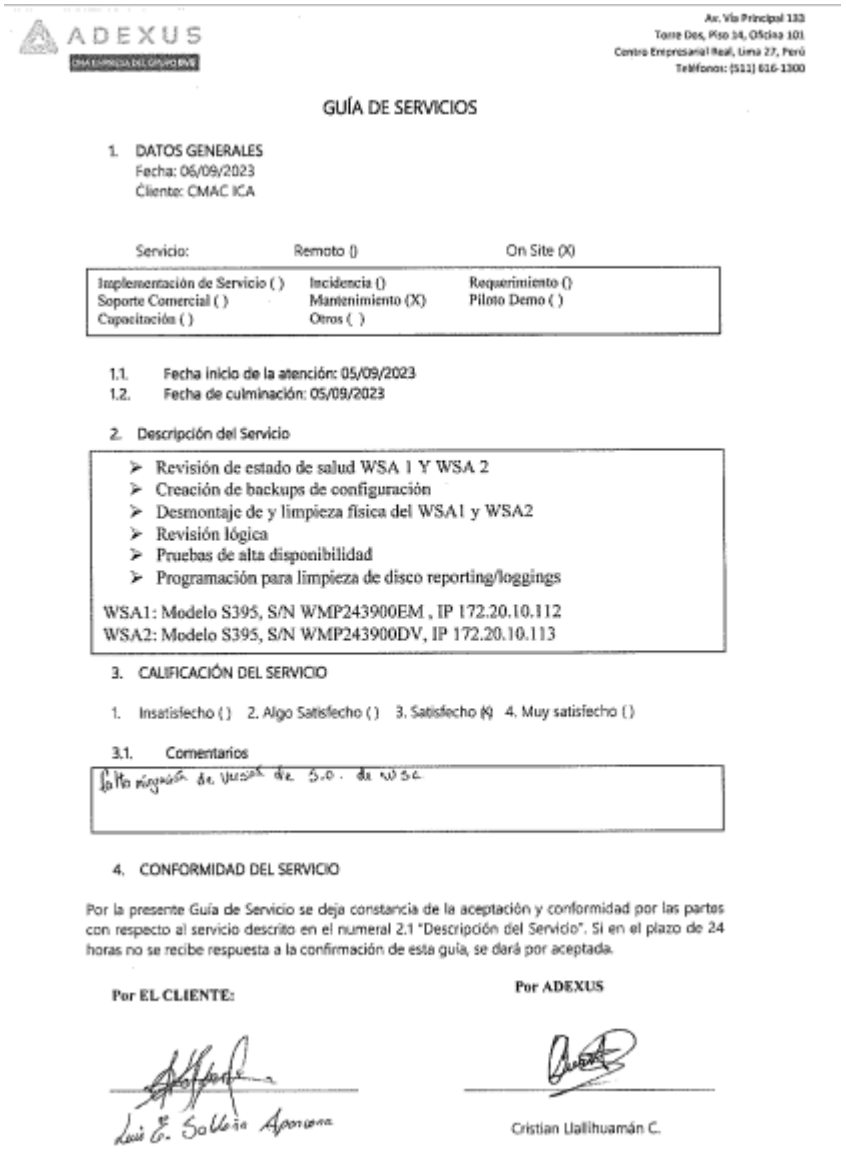
		Pass Through	Monitor	Decrypt	Drop	Jefe Del Órgano De Control Institucional	Gerente De Auditoría Interna	Jefe De Unidad De Auditoría De Riesgo Crediticio	Gerente De Riesgos	Jefe De Unidad De Supervisión De Riesgo De	Jefe De Unidad De Análisis De Riesgos	Jefe De Unid De Riesgo Operacional
						Grupo OCI Jefe	Grupo GAI Gerente	Grupo ARC Jefe	Grupo GRI Gerente	Grupo SRC Jefe	Grupo UAR Jefe	Grupo URO J
1	Adult					Ø	Ø	Ø	Ø	Ø	Ø	Ø
2	Advertisements	X				X	X	X	X	X	X	X
3	Alcohol	X				Ø	Ø	Ø	Ø	Ø	Ø	Ø
4	Animals and Pets	X				√	√	√	√	√	√	√
5	Arts	X				√	√	√	√	√	√	√
6	Astrology	X				X	X	X	X	X	X	X
7	Auctions	X				√	√	√	√	√	√	√
8	Business and Industry	X				√	√	√	√	√	√	√
9	Cannabis			X		Ø	Ø	Ø	Ø	Ø	Ø	Ø
10	Chat and Instant Messaging			X		√	√	√	√	√	√	√
11	Cheating and Plagiarism			X		Ø	Ø	Ø	Ø	Ø	Ø	Ø
12	Child Abuse Content	X				Ø	Ø	Ø	Ø	Ø	Ø	Ø
13	Cloud and Data Centers	X				√	√	√	√	√	√	√
14	Computer Security	X				√	√	√	√	√	√	√
15	Computers and Internet	X				√	√	√	√	√	√	√
16	Conventions, Conferences and Trade Shows	X				√	√	√	√	√	√	√



	Decrypt	Drop	Jefe de Organización y Procesos	Jefe De Contabilidad	Jefe De Gestión Y Desarrollo Humano	Jefe De Logística	Jefe De Planeamiento, Presupuesto Y Gestión de Proyectos	Jefe De Seguridad	Jefe de Infraestructura e Implementación de Oficinas	Subgerente De Agencias	Jefe de Gestión de Agencias	Supervisor De Ventas	Jefe Regional De Agencias	Coordin Regiona
			Grupo OYP Jefe	Grupo CON Jefe	Grupo GDH Jefe	Grupo LOG Jefe	Grupo PPE Jefe	Grupo USE Jefe	Grupo IIO Jefe	Grupo SGA SubGerente	Grupo SGA Jefe GestionAgencias	Grupo VEN Supervisor	Grupo Jefe Regional	Grupo S Coordin Regiona
9			Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	
10			X	X	X	X	X	X	X	X	X	X	X	
11			Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	
12			√	√	√	√	√	√	√	√	√	√	√	
13			√	√	√	√	√	√	√	√	√	√	√	
14			X	X	X	X	X	X	X	X	X	X	X	
15			√	√	√	√	√	√	√	√	√	√	√	
16			√	√	√	√	√	√	√	√	√	√	√	
17	X		Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	
18	X		√	√	√	√	√	√	√	√	√	√	√	
19	X		Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	
20			Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	
21			√	√	√	√	√	√	√	√	√	√	√	

Fuente: Archivos Caja Municipal Ica

Anexo 2: Se observa la guia de servicio donde participo de los mantenimiento de los equipos que tenemos actualmente instalados.



ADEXUS
UNA EMPRESA DEL GRUPO BVL

Av. Vía Principal 133
Torre Dos, Piso 14, Oficina 101
Centro Empresarial Real, Lima 27, Perú
Teléfonos: (511) 616-1300

GUÍA DE SERVICIOS

1. DATOS GENERALES
Fecha: 06/09/2023
Cliente: CMAC ICA

Servicio:	Remoto ()	On Site (X)
Implementación de Servicio ( )	Incidencia ()	Requerimiento ()
Soporte Comercial ( )	Mantenimiento (X)	Piloto Demo ( )
Capacitación ( )	Otros ( )	

1.1. Fecha inicio de la atención: 05/09/2023
1.2. Fecha de culminación: 05/09/2023

2. Descripción del Servicio

- Revisión de estado de salud WSA 1 Y WSA 2
- Creación de backups de configuración
- Desmontaje de y limpieza física del WSA1 y WSA2
- Revisión lógica
- Pruebas de alta disponibilidad
- Programación para limpieza de disco reporting/loggings

WSA1: Modelo S395, S/N WMP243900EM , IP 172.20.10.112
WSA2: Modelo S395, S/N WMP243900DV, IP 172.20.10.113

3. CALIFICACIÓN DEL SERVICIO

1. Insatisfecho ( ) 2. Algo Satisfecho ( ) 3. Satisfecho (X) 4. Muy satisfecho ( )

3.1. Comentarios

Se hizo migración de versión de S.O. de WSA

4. CONFORMIDAD DEL SERVICIO

Por la presente Guía de Servicio se deja constancia de la aceptación y conformidad por las partes con respecto al servicio descrito en el numeral 2.1 "Descripción del Servicio". Si en el plazo de 24 horas no se recibe respuesta a la confirmación de esta guía, se dará por aceptada.

Por EL CLIENTE:

Luis E. Salcedo Aparicio

Por ADEXUS

Cristian Llallihuamán C.

Fuente: Archivos Caja Municipal Ica

Anexo 3, reporte fotografico optenido por los mantenimiento e implementacion de Web Segura de Cisco, dentro del reporte fotografico observamos el equipamento que tenemos, adicional a ello se observa que este tiene aun la capacidad de crecer en Hardware.

Montaje frontal de los equipos WEB segura de Cisco

Montaje frontal de los equipos WEB segura de Cisco

Montaje Posterior de los equipos WEB segura de Cisco