



“Responsabilidad con pensamiento positivo”

UNIVERSIDAD TECNOLÓGICA ISRAEL

**TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE:
INGENIERO EN ELECTRÓNICA DIGITAL Y
TELECOMUNICACIONES**

TEMA:

IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD
PERIMETRAL PARA SEGURIDAD DE LA INFORMACIÓN DEL
SERVICIO NACIONAL DE CONTRATACIÓN PÚBLICA.

AUTOR:

SERGIO EUCLIDES TOAPANTA VIRACOCCHA

TUTOR:

MG. FLAVIO DAVID MORALES ARÉVALO

QUITO, ECUADOR

2019

DECLARACIÓN

Yo, Sergio Euclides Toapanta Viracocha, declaro que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento. La Universidad Tecnológica Israel, puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido en su reglamento y por la normatividad institucional vigente.

.....

Sergio Euclides Toapanta Viracocha

UNIVERSIDAD TECNOLÓGICA ISRAEL

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de titulación certifico:

Que el trabajo de titulación “**IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD PERIMETRAL PARA SEGURIDAD DE LA INFORMACIÓN DEL SERVICIO NACIONAL DE CONTRATACIÓN PÚBLICA.**”, presentado por el Sr. Sergio Euclides Toapanta Viracocha, estudiante de la carrera de Electrónica Digital y Telecomunicaciones, reúne los requisitos y méritos suficientes para ser sometido a la evaluación del Tribunal de Grado, que se designe, para su correspondiente estudio y calificación.

Quito D.M. Febrero del 2019

TUTOR

.....

Mg. Flavio David Morales Arévalo

AGRADECIMIENTO

Quiero dar gracias a Dios por ayudarme a llegar a cumplir este objetivo tan anhelado, por bendecirme y darme las fuerzas para seguir cada día.

Quiero agradecer a mis padres por ser mi ejemplo de lucha, perseverancia y humildad. Por enseñarme, guiarme, apoyarme y estar siempre conmigo en todo momento con sus palabras de aliento y amor.

Quiero agradecer a mi familia mi esposa, mis hijos Aron y James, por su comprensión y apoyo, por su amor y cariño, por ser la fortaleza y entusiasmo para cumplir mi meta, por tantos días y noches que no puede compartir con ellos y dedicarme a conseguir esta carrera profesional.

Agradecer también a mis profesores por compartir conmigo sus conocimientos, experiencias y anécdotas, sé que me servirán de mucho para enfrentarme al mundo en mi vida profesional.

Quiero agradecer a todos y cada una de las personas que estuvieron conmigo con su apoyo incondicional, a mis compañeros con quienes compartí gratos momentos que los llevare en mis recuerdos como la más bonita experiencia de mi vida estudiantil.

DEDICATORIA

Quiero dedicar este triunfo a mis padres Abel y Carmen por su apoyo incondicional, por toda la lucha que realizaron día a día, por las gotas de sudor que dejaron en sus largas jornadas de trabajo para darme las bases académicas, morales y de valores que han sido muy importantes para alcanzar esta meta tan anhelada.

A mi esposa, a mis hijos James y Aron, por su amor, comprensión y cariño en todo momento, por ser la inspiración para no desistir y salir adelante en la vida.

A mis hermanos y hermanas, y a todas las personas que aportaron con todo su apoyo para que llegue a cumplir mi meta.

TABLA DE CONTENIDO

DECLARACIÓN	ii
APROBACIÓN DEL TUTOR.....	iii
AGRADECIMIENTO	iv
DEDICATORIA	v
LISTA DE TABLAS	xiii
LISTA DE FIGURAS	xiv
RESUMEN.....	xvii
ABSTRACT	xviii
INTRODUCCIÓN	1
Antecedentes	1
Planteamiento y justificación del problema	3
Objetivos del trabajo de titulación.....	4
Objetivo general	4
Objetivos específicos.....	5
Alcance.....	5
Descripción de los capítulos.....	5
CAPÍTULO 1	7
FUNDAMENTACIÓN TEÓRICA.....	7
1.1 Seguridad Perimetral	7
1.1.1 Ejemplo de arquitectura sin seguridad perimetral	7
1.1.2 Ejemplo de arquitectura sin seguridad perimetral	8
1.2 WAF	9
1.4 Firewall (Cortafuegos).....	11
1.4.1 Funcionamiento del cortafuegos.....	11
1.4.2 <i>Firewall</i> de próxima generación (NGFW)	12

1.5 ISO/IEC (Organización Internacional de Normalización)/(Comisión Electrotécnica Internacional) 27000	13
1.5.1 ISO 27001.....	14
1.5.2 EGSI (Esquema Gubernamental de Seguridad de la Información).....	14
1.5.2. Introducción.....	15
1.5.2. Política de Seguridad de la Información	15
1.5.2. Organización de la Seguridad de la Información	16
1.6 Caracterización de la institución	17
1.6.1 Información del Servicio Nacional de Contratación Pública	17
1.6.2 Información general de la institución.....	18
1.6.3. Misión institucional.....	18
1.6.4. Visión institucional.....	18
1.6.5. Política institucional	18
1.6.6. Ubicación.....	19
1.6.7 Coordinación Técnica de Innovación Tecnológica.....	19
1.6.7. Direcciones que conforman la Coordinación Técnica de Innovación Tecnológica.....	20
1.6.7. Dirección de seguridad informática.....	20
1.6.7. Misión:.....	20
1.6.7. Atribuciones y responsabilidades:.....	20
CAPÍTULO 2	22
MARCO METODOLÓGICO	22
CAPÍTULO 3	24
PROPUESTA.....	24
3.1 Análisis de riesgos, amenazas y vulnerabilidades.....	24
3.1.1 Riesgo identificado.....	24
3.1.2 Controles	24
3.1.3 Control de Activos:	24

3.1.4 Control de amenazas:	25
3.2.1 Topología de seguridad propuesto	25
3.2.2 Selección de equipos físicos para los servidores	27
3.2.3 Selección de <i>software firewall</i>	27
3.2.4 Selección del equipo físico para <i>management/reporter</i>	28
3.2.5 Licenciamiento de <i>clúster</i> de borde.....	28
3.2.6 Licenciamiento para administración y reporte	29
3.3 Análisis de costo y selección de <i>software y hardware</i>	30
CAPÍTULO 4	32
IMPLEMENTACIÓN.....	32
4.1 Levantamiento de información.....	32
4.1.1 Servidores, computadores PC y portátiles.....	34
4.1.2 Levantamiento de redes existentes en la institución	34
4.1.3 Pool de IP públicas de los servicios	35
4.1.4 Configuración actual del firewall perimetral.....	35
4.1.6 Topología lógica de la red de datos SERCOP.....	36
4.1.7 Direccionamiento IP equipos <i>firewall Check Point</i>	37
4.1.8 Reglas configuradas en equipos Check Point edificio El Telégrafo	38
4.1.9 Reglas configuradas en equipos Check Point data Center CNT	38
4.2 Implementación	38
4.2.1 Configuración de equipos.....	40
4.2.1 Instalación Hypervisor.....	40
4.2.2. Creación RAID (Redundant Array of Independent Disks) 1	40
4.2.2 Instalación EXSi (Plataforma Virtual de VMware)	41
4.2.3 Despliegue de VM-300 PAN	43
4.2.4 FW_Activo	45
4.2.5 FW_Pasivo	45

4.3 Configuración de networking virtual.....	46
4.3.1 Direccionamiento IP utilizado.....	48
4.4 Configuración de firewall edificio El Telégrafo	49
4.4.1 Creación objetos	49
4.4.2 Objetos de IP catalogadas como Spam.....	49
4.4.3 Objetos de equipos de usuarios internos	50
4.5 Agrupación de objetos, redes y servicios	50
4.5.1 Grupos de la red de servidores	50
4.5.2 Grupos de redes	50
4.5.3 Servicios TCP/IP	51
4.6 Creación de perfiles de navegación.....	51
4.6.1 Navegación gerencial	51
4.6.2 Navegación básica.....	52
4.6.2 Navegación básica más cursos	52
4.6.3 Navegación básica más redes sociales	52
4.7 Creación grupo de aplicaciones.....	53
4.8 Configuración de reglas NAT	54
4.9 Configuración de políticas de seguridad	55
4.9.1 Permisos de navegación gerencial.....	55
4.9.2 Permisos de navegación básica	56
4.9.13 Permisos de navegación de la red de invitados	56
4.10 Permisos de acceso entre redes LAN	57
4.11 Permisos de comunicación red VPN	57
4.12 Permisos de conexión remota.....	58
4.13 Permiso para actualizaciones antivirus.....	59
4.14 Bloqueos de actualizaciones UPDATE.....	60
4.15 Permiso de acceso red invitados.....	61

Fuente: Elaborado por el autor.....	62
4.16 Permiso de acceso sin restricción	62
4.17 Bloqueo por defecto	63
4.18 Configuración VPN.....	63
4.18.1 Configuración rutas de acceso VPN.....	66
Fuente: Elaborado por el autor	66
4.18.2 Configuración de usuarios VPN.....	66
4.18.2 Configuración de Acceso VPN para Linux	67
4.19 Instalación física de los equipos	67
4.20 Configuración del firewall del Data Center CNT.....	70
4.20.1 Configuración de interfaces de red.....	70
4.20.2. Anillo interministerial	70
4.20.2 TELCONET	70
4.20.3 CNT	71
4.20.4 Datos.....	72
4.20.5 Red LAN CNT	73
4.20.6 Zonas de seguridad.....	73
4.20.7 Creación de Rutas.....	74
4.20.8 Configuración protocolo ECMP para ISP redundantes.....	74
4.20.9 Creación de objetos	75
4.20.10 Servidores alojados en el Data Center CNT.....	75
4.20.11 Agrupación de servidores	75
4.20.12 Agrupación de redes	76
4.20.13 Servicios TCP/IP	76
4.20.14 Navegación para servidores.....	77
4.20.15 Configuración de reglas NAT	78
4.20.16 Reglas NAT de publicación de servicios.....	79

4.20.17 Regla de publicación SOCE TELCONET	79
4.20.17 Regla de publicación SOCE CNT	79
4.20.17 Regla publicación SOCE Anillo Interministerial	80
4.20.18 Publicación del Portal de Compras Públicas por CNT	80
4.20.19 Publicación del portal de compras públicas por el anillo interministerial.	81
4.20.20 Publicación DNS CNT	81
4.20.21 Publicación DNS TELCONET	82
4.20.22 Configuración de políticas de seguridad	82
4.20.23 SOCE TELCONET y CNT	82
4.20.24 Portal	82
4.20.25 Regla de seguridad acceso DNS TELCONET y CNT	83
4.20.26 Permisos de acceso entre redes LAN	83
4.20.27 Permisos de navegación <i>Atmailing</i>	83
4.20.28 Permisos de Navegación Antispam.....	84
4.20.29 Permiso para navegación CITRIX (Balanceador de Carga).....	84
4.20.30 Configuración de reglas para protección.....	85
4.20.31 Bloqueo de <i>blacklist</i>	85
4.20.32 Bloqueo de <i>boot</i> para SOCE	85
4.21 Ubicación de los equipos en los Rack DC CNT.....	86
4.22 Topología de red final	87
4.3 Pruebas de funcionamiento	89
4.3.1 Pruebas de navegación	90
4.3.2 Pruebas de bloqueos	90
4.3.3 Pruebas de comunicación entre equipos de SERCOP y CNT.....	91
4.3.4 Pruebas de acceso VPN	91
4.4 Análisis de resultados	92
4.4.1 Análisis resultados de comunicación entre redes	92

4.4.3 Análisis de resultados acceso VPN	92
4.4.4 Análisis resultados de control de <i>malware</i>	92
Conclusiones	96
Recomendaciones	97
BIBLIOGRAFÍA	98
Anexos	100
Anexo 1 Matriz de riesgos de la Dirección de Seguridad Informática.....	101
Anexo 2 Proformas equipos	105
Anexo 3 Tabla comparativa de herramientas Check Point y paloalto Networks .	108
Anexo 4 Manual de usuario.....	110
Anexo 5 Cronograma de actividades.....	116

LISTA DE TABLAS

Tabla 1. Información general de la institución pública	18
Tabla 2. Costos propuesto	30
Tabla 3. Presupuesto total del proyecto.....	31
Tabla 4. Plan de levantamiento de información	32
Tabla 5. Enlaces de Internet SERCOP	36
Tabla 6. Enlace de datos SERCOP.....	37
Tabla 7. Red LAN SERCOP	37
Tabla 8. Direccionamiento ip equipos firewall	37
Tabla 9. Actividades realizadas de implementación	39
Tabla 10. IP red de administración.....	43
Tabla 11. Direccionamiento IP utilizado.....	48
Tabla 12. IP interfaces.....	48
Tabla 13. Pruebas de Funcionamiento	89
Tabla 14. Mejora de seguridad de la red y la información.	94
Tabla 15. Uso CPU Check Point y paloalto	95

LISTA DE FIGURAS

Figura 1. Arquitectura sin seguridad perimetral.....	8
Figura 2. Arquitectura con seguridad perimetral.....	8
Figura 3. Protección WAF	9
Figura 4. Esquema funcionamiento DMZ.....	10
Figura 5. Ubicación actual de la institución	19
Figura 6. Esquema de seguridad propuesto	26
Figura 7. Captura de Appliance Check Point 4600	35
Figura 8. Interfaz BIOS	41
Figura 9. Interfaz para creación de virtual disk	41
Figura 10. Interfaz de instalación de imagen de disco	42
Figura 11. Selección de RAID 1	42
Figura 12. Interfaz de ingreso	42
Figura 13. Interfaz de selección management	43
Figura 14. Descarga de OVA (<i>Open Virtual Appliance</i>).....	44
Figura 15. Despliegue imagen ISO	44
Figura 16. Seleccionar OVA	44
Figura 17. Firewall activo	45
Figura 18. Firewall pasivo.....	46
Figura 19. Configuración networking virtual.....	47
Figura 20. Objetos de IP Spam.....	49
Figura 21. Agrupación de redes de servidores	50
Figura 22. Agrupación de objetos de redes	50
Figura 23. Agrupación de servicios.....	51
Figura 24. Perfil de navegación gerencial	51
Figura 25. Perfil de navegación básica.....	52
Figura 26. Perfil de navegación básica más cursos	52
Figura 27. Perfil de navegación básica más redes sociales	53
Figura 28. Agrupación de aplicaciones para perfil navegación básica	53
Figura 29. Aplicaciones de perfil de navegación básica	53
Figura 30. Aplicaciones de perfil de navegación básica	54
Figura 31. Configuración de regla NAT	54
Figura 32. Configuración de regla NAT para publicación de servicios	55
Figura 33. Regla de seguridad navegación gerencial	55
Figura 34. Aplicación de Perfil en Regla de Seguridad Navegación Básica	56
Figura 35. Regla de seguridad de navegación de la red de invitados	56
Figura 36. Aplicación del perfil en la regla de seguridad de navegación de invitados.....	57
Figura 37. Regla de seguridad para navegación básica	57
Figura 38. Comunicación de red VPN	58

Figura 39. Regla de acceso remoto	58
Figura 40. Regla de seguridad para navegación básica	58
Figura 41. Aplicación del perfil aplicaciones acceso remoto	59
Figura 42. Regla de actualizaciones antivirus	59
Figura 43. Regla de sincronización antivirus con red local.....	60
Figura 44. Bloqueo grupo de aplicaciones UPDATE.....	60
Figura 45. Grupo de aplicaciones UPDATE	60
Figura 46. Regla de acceso red invitados	61
Figura 47. Regla de acceso aplicaciones específicas.....	61
Figura 48. Regla de bloqueo red invitados a el DC CNT	62
Figura 49. Regla de bloqueo total aplicaciones.....	62
Figura 50. Regla de navegación sin restricción	62
Figura 51. Regla de permisos aplicaciones libres	63
Figura 52. Regla implícita de bloqueo	63
Figura 53. Configuración de certificado VPN.....	64
Figura 54. Configuración del perfil de autenticación	64
Figura 55. Configuración del gateway VPN	65
Figura 56. Configuración autenticación gateway VPN	65
Figura 57. Configuración de la interfaz VPN.....	65
Figura 58. Configuración rutas de acceso VPN	66
Figura 59. Configuración del portal VPN	66
Figura 60. Grupos de usuarios VPN.....	67
Figura 61. Configuración VPN linux	67
Figura 62. Colocación equipo <i>gateway</i> 1 y equipo <i>gateway</i> 2 en el DC El Telégrafo	68
Figura 63. Cableado de equipo <i>gateway</i> 1, equipo <i>gateway</i> 2 y reporteador en el DC El Telégrafo ...	68
Figura 64. Topología de conexiones equipos firewall y administración en DC El Telégrafo	69
Figura 65. Configuración de la interfaz anillo interministerial	70
Figura 66. Configuración de la interfaz ISP TELCONET	71
Figura 67. Configuración de la interfaz Pool 1 CNT	71
Figura 68. Configuración de la interfaz Pool 1 CNT	72
Figura 69. Configuración de la interfaz de datos	72
Figura 70. Configuración de la red LAN CNT.....	73
Figura 71. Configuración de zonas de seguridad	73
Figura 72. Configuración de rutas	74
Figura 73. Configuración de zonas de seguridad	74
Figura 74. Objetos servidores del Data Center CNT.....	75
Figura 75. Objetos IP atacantes	75
Figura 76. Agrupación de servidores	76
Figura 77. Agrupación de redes	76
Figura 78. Configuración servicios	76

Figura 79. Bloqueo de tráfico de servidores.....	77
Figura 80. Bloqueo navegación servidores	77
Figura 81. Configuración del perfil de navegación de servidores	78
Figura 82. Regla NAT.....	78
Figura 83. Configuración regla NAT navegación	79
Figura 84. Regla publicación SOCE TELCONET	79
Figura 85. Regla publicación SOCE CNT	80
Figura 86. Regla de publicación SOCE Anillo Interministerial	80
Figura 87. Regla de publicación del portal compras públicas por CNT.....	80
Figura 88. Regla de publicación del Portal Compras Públicas por Anillo Interministerial	81
Figura 89. Regla de publicación DNS CNT.....	81
Figura 90. Regla de publicación DNS CNT.....	82
Figura 91. Regla seguridad acceso SOCE por CNT y TELCONET	82
Figura 92. Regla de seguridad de acceso al portal	82
Figura 93. Regla de seguridad DNS TELCONET y CNT	83
Figura 94. Regla de seguridad acceso entre Redes.....	83
Figura 95. Regla de seguridad para navegación <i>Atmailing</i>	84
Figura 96. Regla de seguridad para navegación <i>ANTISPAM</i>	84
Figura 97. Regla de seguridad para navegación <i>ANTISPAM</i>	85
Figura 98. Regla de seguridad para bloqueo blacklist.....	85
Figura 99. Regla de seguridad bloqueo <i>BOOTS</i>	85
Figura 100. Ubicación RACK DC CNT	86
Figura 101. Topología de red final del Data Center CNT	87
Figura 102. Topología final del edificio El Telégrafo.....	88
Figura 103. Prueba navegación Internet.....	90
Figura 104. Bloqueos de sitios por <i>malware</i>	90
Figura 105. Ping servidor ubicado DC CNT	91
Figura 106. Acceso VPN Windows y Android	91
Figura 107. Ejecución o compilación de cambios PAN	93
Figura 108. Rendimiento firewall paloalto Networks	95

RESUMEN

Este proyecto trata de la implementación de un sistema de seguridad perimetral para el Servicio Nacional de Contratación Pública que ayuda a mantener la integridad, confidencialidad y disponibilidad de la información que maneja la institución, protegiendo los sistemas de amenazas internas y externas a los cuales se encuentran expuestas todas las empresas e instituciones públicas y privadas.

Se empieza con una descripción general de la institución para conocerla y tener una idea clara de los servicios que ofrece la misma, a continuación se realiza un levantamiento de información para saber el estado actual de su red de datos y de sus componentes de seguridad perimetral.

Se identifica un riesgo tecnológico tras realizar un breve análisis de riesgos ya que los equipos de seguridad perimetral actuales han concluido su vida útil y presentan lentitud en la aplicación de políticas y control de amenazas.

Por lo que se propone renovar los equipos de seguridad perimetral con equipos virtualizados que permitan ampliar su capacidad cuando sea necesario para así mantener su efectividad en el control de amenazas. Adicional se propone que los equipos trabajen en HA (High Availability) en los dos centros de datos por lo que se presenta una topología con cuatro equipos.

Se implementan los equipos de seguridad con software paloalto *NETWORKS* los cuales aplican políticas en tiempo real. Trabajan con módulos de filtrado URL, IPS, antimalware, antivirus, sandboxing y control de aplicaciones brindando una protección efectiva a toda la plataforma tecnológica de la institución.

Palabras clave: seguridad, sistema, implementación, perimetral, network, información, virtual.

ABSTRACT

This project deals with the implementation of a perimeter security system for the National Public Procurement Service that helps maintain the integrity, confidentiality and availability of the information managed by the institution, protecting the systems of internal and external threats to which they are exposed. exposed all companies and public and private institutions.

You start with a general description of the institution to get to know it and have a clear idea of the services offered by it, then a survey is made to know the current status of your data network and its perimeter security components.

A technological risk is identified after conducting a brief risk analysis, since the current perimeter security teams have completed their useful life and are slow to apply policies and control threats.

Therefore, it is proposed to renew the perimeter security equipment with virtualized equipment that allows to expand its capacity when necessary to maintain its effectiveness in the control of threats. Additionally, it is proposed that the teams work in HA (High Availability) in the two data centers, so a topology with four teams is presented.

The security teams with paloalto software NETWORKS are implemented, which apply policies in real time. They work with URL, IPS, antimalware, antivirus, sandboxing and application control modules providing effective protection to the entire technological platform of the institution.

Keywords: security, system, implementation, perimeter, network, information, virtual.

INTRODUCCIÓN

Antecedentes

A nivel mundial se ha empezado a dar mucha importancia a la seguridad de la información debido al aumento de amenazas en los últimos años. La seguridad ya no se trata solo de proteger los equipos con un buen antivirus. Con el pasar del tiempo y el avance de la tecnología han ido apareciendo nuevas técnicas y nuevos ataques usados para vulnerar sistemas.

En octubre del año 2010 un estudiante de la Escuela Politécnica Nacional, realizó el proyecto de “ Diseño de un esquema de seguridad para la red de datos de una institución educativa”, para lo cual usan el modelo de seguridad SAFE de CISCO y el *Penetration testing methodology* para el análisis de riesgos de vulnerabilidades y el esquema físico. La metodología antes mencionada consta de 5 fases: preparación, reconocimiento, análisis de información y riesgos, intentos activos de intrusión y análisis final. Ellos recomiendan que se haga un análisis de la situación actual para tener una idea clara del problema y buscar su solución. Encontraron varios problemas en la institución como el uso de software no licenciado, carencia de antivirus en los equipos de computo y el desconocimiento de políticas de seguridad informática de los empleados. Los resultados obtenidos fueron satisfactorios al licenciar los computadores y actualizar los parches de seguridad en los mismos y añadir software antivirus con lo cual reducen el riesgo en la institución. (Martinez, 2010)

La Escuela Politécnica del Ejército (ESPE) en el año 2015 apoyó un proyecto realizado para las empresas privadas Teamsourcing sobre la Implementación de un sistema de seguridad perimetral usando software libre ClearOS y el desarrollo de las políticas de seguridad basadas en el estándar ISO-27001. Este proyecto tiene un resultado satisfactorio en el control de tráfico y malware, con esta solución ClearOS se obtuvo una mejora en su interfaz y administración a nivel de gestionar permisos. La reportería es otro factor importante de mencionar ya que se obtuvo un mejor reporte necesario para el análisis de

tráfico diario. Las políticas de la ISO 27001 se cran de acuerdo al estado y necesidad de la empresa para que su nivel de cumplimiento sea efectivo (Pilacuán, 2015)

En el libro Mundo Hacker sobre Seguridad perimetral, monitorización y ataques en redes, explica cómo asegurar e interceptar las comunicaciones, desde el punto de vista del atacante y de la víctima. Uno de los puntos importantes en la seguridad es analizar el espionaje de redes y la intrusión en las mismas, para prevenir estas amenazas se debe usar métodos y técnicas con herramientas de monitorización de tráfico de red, técnicas de interceptación de información, interpretación de la información obtenida y métodos de protección contra intrusos. Existen varias herramientas de seguridad perimetral que ayudan a mantener más seguras las redes, como *firewalls*, *honey pots*, *iptables* y muchos más. Asegurar la red es muy importante ya que se trata de configurar una barrera que no permita el acceso de redes desconocidas a la infraestructura. De este modo se asegura la confidencialidad e integridad de los datos, analizando sistemas criptográficos, tratando aspectos de los certificados digitales y analizando los distintos usos del cifrado de datos, como *SSH*, *IPSec*, *VPN-SSL* y otros. Con estos métodos y técnicas se previene que la seguridad de la información se pueda ver comprometida desde distintos puntos: Correos electrónicos, archivos en discos e información enviada a través de entornos web, entre otros (Ramos, Gonzáles, & Picouto, 2014)

Como parte de los antecedentes de la institución donde se implementará el sistema de seguridad perimetral, en el tercer inciso del Art. 97 de la LOSNCP señala: “El Servicio Nacional de Contratación Pública, implementará los mecanismos tecnológicos para asegurar integridad de la información, independientemente de la plataforma o sistema empleado para crearlo, transmitirlo o almacenarlo”.

El numeral 410-12 del referido Acuerdo establece que: "Administración de soporte de tecnología de información" establece que "La unidad de tecnología definirá, aprobará y difundirá procedimientos de operación que faciliten la adecuada administración y soporte tecnológico y garanticen la seguridad (...)".

En el artículo Seguridad Perimetral publicado por la Universidad Regional Concepción del Uruguay manifiesta que la seguridad informática se encarga de proteger la información, pero para que cumpla esta labor debe preservar la integridad, confidencialidad y disponibilidad de la misma (Arellano, 2005).

El Servicio Nacional de Contratación Pública – SERCOP, es el ente rector responsable de mantener disponible el Sistema Oficial de Contratación del Estado -SOCE, mediante el cual las entidades contratantes realizan los procesos de compra, por esta razón, se debe asegurar la confiabilidad, integridad y disponibilidad de la información así como también de los aplicativos que acceden los usuarios internos y externos a la institución.

Planteamiento y justificación del problema

La plataforma de seguridad perimetral, constituye un sistema crítico para la actividad del SERCOP ya que permite mantener segura a la red y a las conexiones internas y externas a la Institución, lo que contribuye al normal funcionamiento y al correcto desenvolvimiento de las actividades diarias. Adicionalmente, el acceso a los servidores, aplicaciones y servicios con los que cuenta la institución son controlados por el firewall para establecer conexiones seguras.

Es sumamente importante asegurar el correcto funcionamiento de estos equipos, con todos los servicios necesarios activos, soporte tanto técnico local como del fabricante, que brinde al equipo de la Dirección de Seguridad Informática las herramientas necesarias para resolver problemas o inconvenientes con los mismos, ya que los servicios que el SERCOP brinda a la comunidad dependen de esta solución.

El Servicio Nacional de Contratación Pública –SERCOP-, cuenta con dos equipos firewalls perimetrales (Gateway Check Point 4800) en alta disponibilidad (High Availability – HA) en el Data Center, un firewall perimetral (Gateway CheckPoint 4600) en las instalaciones del SERCOP, un equipo de administración de toda la solución (Appliance 4600), así como un equipo reporteador (Appliance Check Point 4600). Esta solución actualmente permite proteger de ataques de accesos no autorizados, varios tipos de malware, ataques de día cero, denegación de servicio, ataques selectivos lanzados en tiempo real a las aplicaciones web de la institución, como el SOCE, Catálogo Electrónico, SICM, SICAE, y herramientas de consulta.

El SERCOP ha utilizado esta solución durante cinco (5) años. Los especialistas encargados han implementado políticas que aseguran la disponibilidad del servicio, así como la seguridad, integridad y confidencialidad de la información con la que cuenta el SERCOP. Es por este motivo que la solución de seguridad implementada es de suma

importancia para garantizar niveles adecuados de seguridad en las plataformas tecnológicas del SERCOP.

Debido a que las plataformas de seguridad en los actuales momentos ya han cumplido su tiempo de vida y presentan algunos inconvenientes, como los que se mencionan:

- Implementación de políticas de 10 a 20 minutos desde Management hacia los Gateway de seguridad.
- Saturación de equipo CheckPoint 4600 repentinamente especialmente en horas pico, quedando sin conexión a nivel de tarjetas de red, por saturación del equipo.
- Revisión y análisis de Logs a través de SmartView Tracker demasiado lento.

El riesgo tecnológico detectado mediante el análisis de riesgos levantado en la Dirección de Seguridad Informática nos lleva a la necesidad de renovar el sistema de seguridad perimetral.

Es necesario renovar la plataforma de seguridad perimetral con un sistema virtualizado que soporte el tráfico que cada vez va en aumento a nivel nacional, y que permitan ampliar y modificar almacenamiento y memoria según se necesite.

Esta Implementación se basará en el EGSI (Esquema Gubernamental de Seguridad de la Información) que está contemplada en la ISO 27000 que menciona: “Disponer a las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información” (SNAP, 2013)

Objetivos del trabajo de titulación

Objetivo general

Implementar un sistema de seguridad perimetral virtualizado que permita mitigar riesgos de seguridad de la información del Servicio Nacional de Contratación Pública.

Objetivos específicos

- Realizar el análisis de riesgos, amenazas y vulnerabilidades.
- Diseñar una propuesta para mitigar el riesgo.
- Implementar el sistema de seguridad perimetral.
- Verificar que toda la configuración cumpla con el Esquema Gubernamental de Seguridad de la Información –EGSI contemplada en la norma ISO 27002.
- Realizar pruebas y validación del funcionamiento.

Alcance

Las especificaciones técnicas han sido desarrolladas para mejorar el sistema de seguridad perimetral que hoy en día tiene la Institución. La implementación a realizar busca mejorar y mitigar el riesgo de seguridad de la información y tecnológico del Servicio Nacional de Contratación Pública.

Descripción de los capítulos

El Capítulo 1 contiene la fundamentación teórica dónde se realiza una descripción general de la institución, se describe el EGSI (Esquema Gubernamental de Seguridad de la Información) y se realiza un levantamiento de información de la situación actual de la plataforma tecnológica.

A continuación en el capítulo 2 se detalla la metodología empleada en la investigación, se describe todas las técnicas usadas en el desarrollo del proyecto tales como el método investigativo, empírico o teórico aplicado según el caso.

En el capítulo 3 se trata de la propuesta del proyecto en el cual se presenta un análisis de riesgos y una solución virtual que permite mejorar la administración, la capacidad de los equipos y el bloqueo de amenazas en tiempo real. Se describe cada uno de los equipos que conforman este proyecto su funcionamiento y capacidad. Se analiza los costos y características de cada uno. En general también se habla del presupuesto requerido para la ejecución del proyecto.

Finalmente el capítulo 4 indica la implementación del proyecto, topologías, instalación, configuración puesta en marcha de la solución; así como también las pruebas realizadas y resultados obtenidos.

CAPÍTULO 1

FUNDAMENTACIÓN TEÓRICA

En la actualidad la necesidad de contar con información íntegra, disponible y auténtica, que brinde un grado de confiabilidad y confidencialidad satisfactorio, se ha convertido en el objetivo principal para el funcionamiento de una empresa ya que se considera el activo más importante (Díaz, Perez, & Proenza, 2014).

La pérdida de información y ataques informáticos constituye un problema para las organizaciones, por lo que la *seguridad informática*, ayuda a desarrollar normas, procesos o técnicas que permiten asegurar las redes de datos para resguardar o proteger la información principalmente ante ataques malintencionados o no, que cualquier individuo o grupo realice (Aguilera, 2010).

1.1 Seguridad Perimetral

La seguridad perimetral es la primera línea de protección, presenta varias soluciones contra las amenazas de seguridad y los códigos dañinos, lo constituyen varios dispositivos que integran servicios como antivirus, filtrado de contenido, IPS, IDS, cortafuegos para seguridad perimetral y un servidor VPN para crear túneles de acceso a la infraestructura tecnológica (Gómez Vieites, 2014).

1.1.1 Ejemplo de arquitectura sin seguridad perimetral

En la figura 1 se muestra una arquitectura en la cual no tiene ningún tipo de seguridad perimetral con sus características.

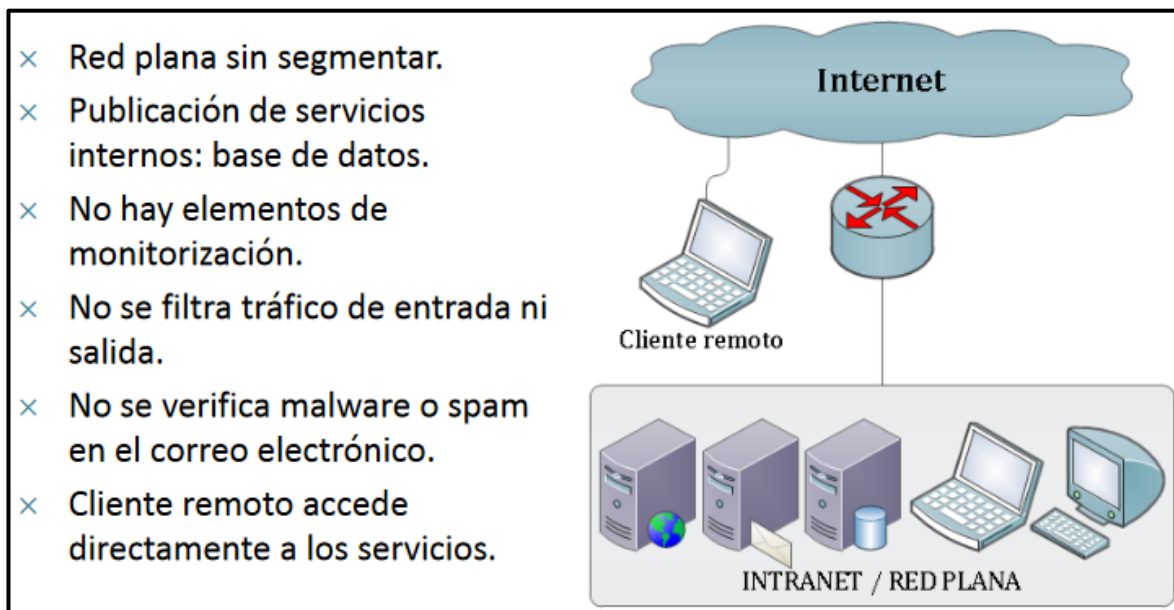


Figura 1. Arquitectura sin seguridad perimetral

Fuente: Elaborado por el autor tomado de *Tiger Team Manager*. 2011.

1.1.2 Ejemplo de arquitectura sin seguridad perimetral

En la figura 2 se muestra una arquitectura con seguridad perimetral con sus características.

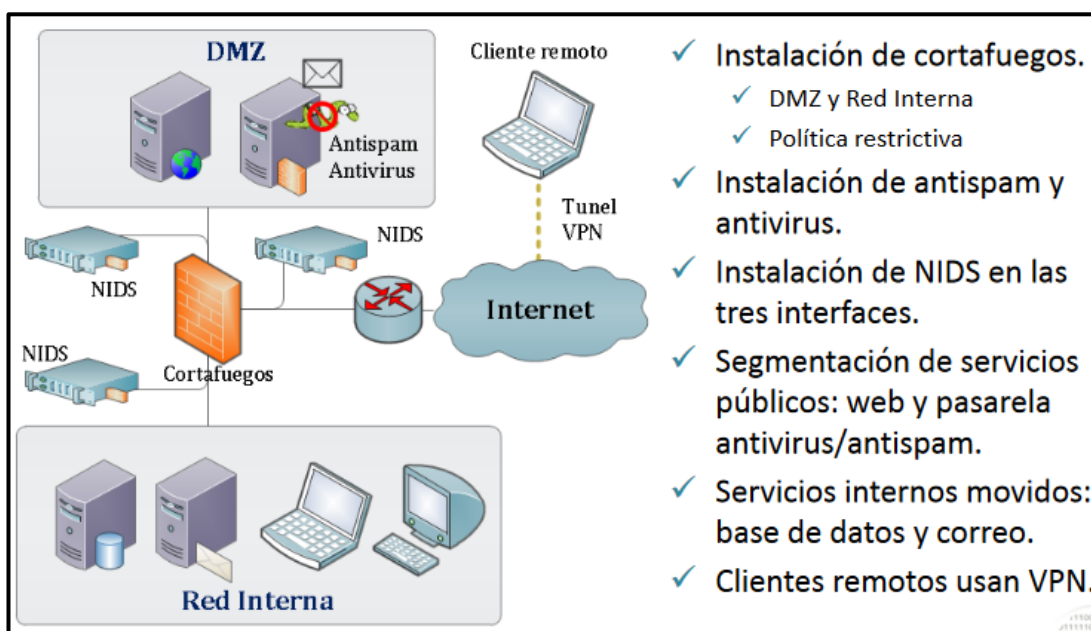


Figura 2. Arquitectura con seguridad perimetral

Fuente: *Tiger Team Manager*. 2011. *Information security encyclopedia*

El sistema de seguridad perimetral puede constar de los siguientes elementos:

- WAF (*Web Application Firewall*)
- DMZ (Zona Desmilitarizada)
- Firewall (Cortafuegos)

1.2 WAF

El *Web Application Firewall* es un firewall de aplicaciones web (WAF) que protege los sitios y las aplicaciones web tanto de ataques conocidos como desconocidos, incluidas las amenazas en la capa de aplicación y de día cero. (citrix.com, 2019)

El análisis de aplicación a nivel de capa 7 perteneciente al modelo OSI, ayuda a mantener un control eficaz, con este sistema más un cortafuegos aseguran el perímetro de la red. En la figura 3 se muestra la protección hacia donde va dirigido el WAF, y la profundidad que esto significa según las capas del modelo OSI (Interconexión de sistemas abiertos).

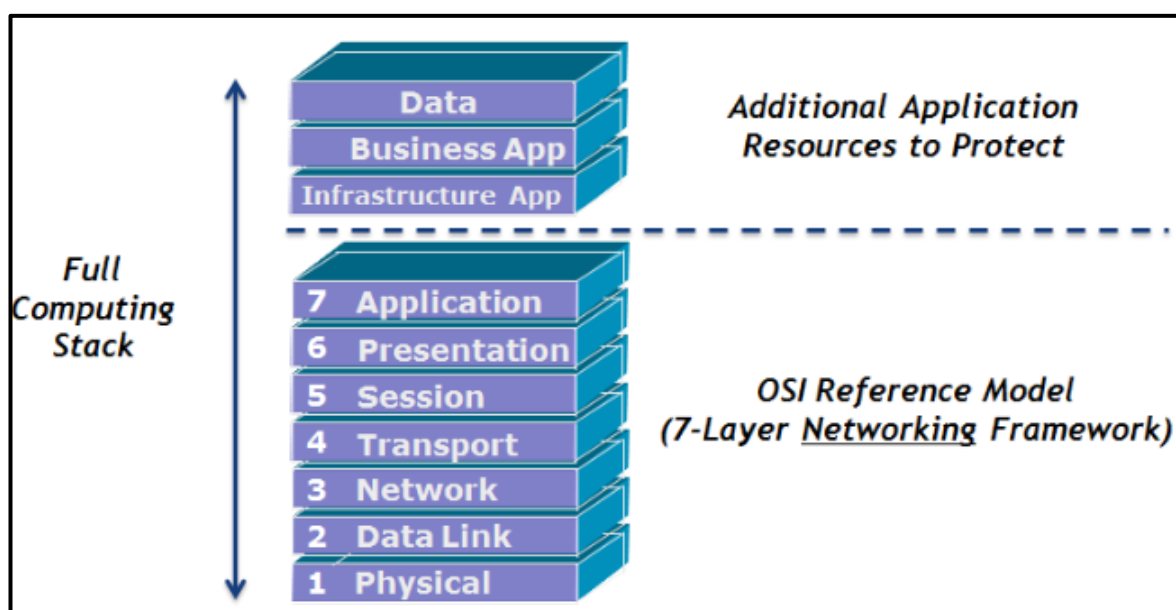


Figura 3. Protección WAF

Fuente: White paper. 2015. <https://www.citrix.com>

1.3 DMZ (Zona desmilitarizada)

Se conoce como zona desmilitarizada (demilitarized zone) que se sitúa entre la red interna y la red externa (Internet). La función de una DMZ es permitir las conexiones tanto desde la red interna como de la externa, mientras que las conexiones que parten de la DMZ solo puedan salir a la red interna; así, los equipos locales (hosts) jamás podrían conectarse a la red interna. En la figura 4 se muestra el esquema de funcionamiento de un DMZ (muycomputer.com, 2014)

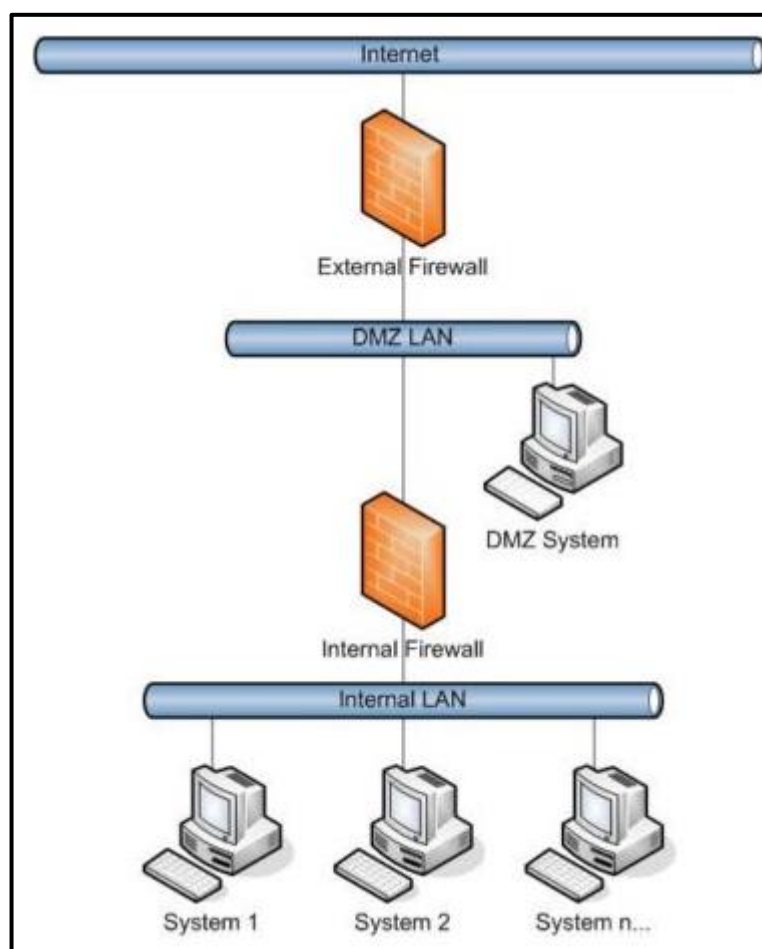


Figura 4. Esquema funcionamiento DMZ

Fuente: DMZ. 2014. <https://www.muycomputer.com/>

1.4 Firewall (Cortafuegos)

Según la multinacional CISCO especializada en redes y fabricante de varios de los equipos usados actualmente, define un *firewall* como “ Un dispositivo de seguridad de la red que monitorea el tráfico de red -entrante y saliente- y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad. Los firewalls han constituido una primera línea de defensa en seguridad de la red durante más de 25 años. Establecen una barrera entre las redes internas protegidas y controladas en las que se puede confiar y redes externas que no son de confianza, como Internet. Un firewall puede ser hardware, software o ambos” (CISCO.com)

Firewall o corta fuegos es un sistema capaz de permitir, bloquear, cifrar o decodificar el tráfico de comunicaciones entre un área local y la Internet, impidiendo que sistemas o usuarios no autorizados tengan acceso. Este puede ser físico o digital, que combinado con otros equipos o software protegen al seguridad perimetral de un entorno de trabajo, empresa pública o privada. Los precursores o los primeros firewall surgieron en la época de 1980, desde entonces estos se han ido perfeccionando así como también el tipo de amenazas y malware existente (Raffino, 2018)

1.4.1 Funcionamiento del cortafuegos

Los cortafuegos distinguen entre las conexiones permitidas y las peligrosas o sospechosas, en base a diferentes procedimientos, tales como:

Políticas de firewall. Empleando los números de IP y otros sistemas de identificación, el cortafuegos suspende cualquier petición de comunicación que no provenga de la red interna o del propio sistema, disfrazando detrás de un IP propio el conjunto de los recursos internos, de modo que nadie pueda monitorearlos desde afuera.

Filtrado de contenido. A través de un sistema de reglas de exclusión en el que el usuario puede tener la última palabra, el firewall distingue entre los contenidos problemáticos, sospechosos o inseguros, y aquellos que quedan a discrecionalidad del usuario. Así, se puede bloquear el acceso a páginas Web o servidores enteros como precaución.

Servicios de antimalware. Muchos firewall tienen incorporadas definiciones de virus y malware provistas por diversos programas defensivos, de modo de también ayudar a tener la expansión de estos programas perniciosos.

Servicios de DPI. Se llama así a los procedimientos de Inspección Profunda de Paquetes (IPP o DPI por sus siglas en inglés: Deep Package Inspection), que añade una segunda capa de seguridad al sistema, revisando el contenido profundo de los paquetes de información recibidos (Raffino, 2018)

1.4.2 *Firewall* de próxima generación (NGFW)

Los firewalls han evolucionado más allá de la inspección activa y el filtrado simple de paquetes. La mayoría de las empresas están implementando firewalls de próxima generación para bloquear las amenazas modernas, como los ataques de la capa de aplicación y el malware avanzado.

Según la definición de Gartner, Inc., un firewall de próxima generación debe incluir lo siguiente:

- Funcionalidades de firewall estándares, como la inspección con estado.
- Prevención integrada de intrusiones.
- Reconocimiento y control de aplicaciones para ver y bloquear las aplicaciones peligrosas.
- Rutas de actualización para incluir fuentes de información futuras.
- Técnicas para abordar las amenazas de seguridad en evolución.

Los NGFW se han convertido en la solución importante para las empresas en la actualidad, además de las funciones anteriores el NGFW centrado en amenazas incluyen todas las funcionalidades de un NGFW tradicional y también brindan funciones de detección y corrección de amenazas avanzadas. Con un NGFW centrado en amenazas, puede hacer lo siguiente:

- Estar al tanto de cuáles son los activos que corren mayor riesgo con reconocimiento del contexto completo.

- Reaccionar rápidamente ante los ataques con automatización de seguridad inteligente que establece políticas y fortalece las defensas en forma dinámica.
- Detectar mejor la actividad sospechosa o evasiva con correlación de eventos de terminales y la red.
- Reducir significativamente el tiempo necesario desde la detección hasta la eliminación de la amenaza con seguridad retrospectiva que monitorea continuamente la presencia de actividad y comportamiento sospechosos, incluso después de la inspección inicial.
- Facilitar la administración y reducir la complejidad con políticas unificadas que brindan protección en toda la secuencia del ataque (cisco.com)

1.5 ISO/IEC (Organización Internacional de Normalización)/(Comisión Electrotécnica Internacional) 27000

“Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI”. (PriteshGupta.com, 2016)

Es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical Commission*), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña (PriteshGupta.com, 2016)

1.5.1 ISO 27001

Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información.

Según la ISO 27001 la seguridad de la información, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así, estos tres términos constituyen la base sobre la que se cimienta todo el contexto de la seguridad de la información:

- **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad:** Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

El SGSI (Sistema de gestión de seguridad de la información) es el concepto central en el que se enfatiza la ISO 27001 (PriteshGupta.com, 2016)

1.5.2 EGSI¹ (Esquema Gubernamental de Seguridad de la Información)

Mediante Acuerdos Ministeriales Nos. 804 y 837 de 29 de julio y 19 de agosto de 2011, respectivamente, la Secretaría Nacional de la Administración Pública creó la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación conformada por delegados del Ministerio de Telecomunicaciones y de la Sociedad de la Información, la Secretaría Nacional de Inteligencia y la Secretaría Nacional de la Administración Pública y dentro de sus atribuciones tiene la de establecer lineamientos de seguridad informática, protección de infraestructura computacional y todo lo relacionado con ésta, incluyendo la información contenida para las entidades de la Administración Pública Central e Institucional.

¹ Fuente: Esquema Gubernamental de Seguridad de la Información EGSI, Acuerdo Ministerial 166.

La Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación en referencia ha desarrollado el Esquema Gubernamental de Seguridad de la Información (EGSI), elaborado en base a la norma NTE INEN-ISO/IEC 27002 "Código de Práctica para la Gestión de la Seguridad de la Información".

1.5.2. Introducción²

El presente documento, denominado Esquema Gubernamental de Seguridad de la Información (EGSI), está basado en la norma técnica ecuatoriana INEN ISO/IEC 27002 para Gestión de la Seguridad de la Información y está dirigido a las Instituciones de la Administración Pública Central, Dependiente e Institucional.

El EGSI establece un conjunto de directrices prioritarias para Gestión de la Seguridad de la Información e inicia un proceso de mejora continua en las instituciones de la Administración Pública.

El EGSI no reemplaza a la norma INEN ISO/IEC 27002 sino que marca como prioridad la implementación de algunas directrices.

1.5.2. Política de Seguridad de la Información³

"Las entidades de la Administración Pública Central, Dependiente e Institucional que generan, utilizan, procesan, comparten y almacenan información en medio electrónico o escrito, clasificada como pública, confidencial, reservada y no reservada, deberán aplicar el Esquema Gubernamental de Seguridad de la Información para definir los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad, integridad y disponibilidad de esa información, en los medios y el tiempo que su legitimidad lo requiera".

² Fuente: Esquema Gubernamental de Seguridad de la Información EGSI, Acuerdo Ministerial 166.

³ 1. POLÍTICA SEGURIDAD DE LA INFORMACIÓN, LITERAL b), EGSI.

1.5.2. Organización de la Seguridad de la Información⁴

El responsable de Seguridad del Area de Tecnologías de la Información tendrá las siguientes responsabilidades:

- a) Controlar la existencia de documentación física o electrónica actualizada relacionada con los procedimientos de comunicaciones, operaciones y sistemas.
- b) Evaluar el posible impacto operativo a nivel de seguridad de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando responsabilidades.
- c) Administrar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento.
- d) Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad para soportar potenciales amenazas a la seguridad de la información que procesan.
- e) Controlar la obtención de copias de resguardo de información, así como la prueba periódica de su restauración.
- f) Asegurar el registro de las actividades realizadas por el personal operativo de seguridad de la información, para su posterior revisión.
- g) Desarrollar y verificar el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.
- h) Implementar los controles de seguridad definidos (ej., evitar software malicioso, accesos no autorizados, etc.).
- i) Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento (ej., cintas, discos, etc.) e informes impresos, y verificar la eliminación o destrucción segura de los mismos, cuando proceda.

⁴ 2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, LITERAL 2.3, EGSÍ.

- j) Gestionar los incidentes de seguridad de la información de acuerdo a los procedimientos establecidos.
- k) Otras que por naturaleza de las actividades de gestión de la seguridad de la información deban ser realizadas.

El Esquema Gubernamental de Seguridad de la Información (EGSI), dispone que se cumpla un sin número de normativas propuestas las cuales aseguran el funcionamiento de los equipos tecnológicos y resguardan la información que es el activo más importante de una organización.

1.6 Caracterización de la institución

1.6.1 Información del Servicio Nacional de Contratación Pública

El Servicio Nacional de Contratación Pública, se crea como un organismo de “derecho público, técnico regulatorio, con personalidad jurídica propia y autonomía administrativa, técnica, operativa, financiera y presupuestaria. Su máximo personero y representante legal será el Director General o la Directora, quien será designado por el Presidente de la República...”.

“El Servicio Nacional de Contratación Pública, SERCOP, es la entidad rectora del Sistema Nacional de Contratación Pública (SNCP), responsable de desarrollar y administrar el Sistema Oficial de Contratación Pública del Ecuador y de establecer las políticas y condiciones en la materia, a nivel nacional; en este contexto en concordancia con la Ley Orgánica del Sistema Nacional de Contratación Pública, los principales objetivos institucionales son: articular y armonizar a todas las “instancias, organismos e instituciones en los ámbitos de planificación, programación, presupuesto, control, administración y ejecución de las adquisiciones de bienes y servicios así como en la ejecución de obras públicas que se realicen con recursos públicos...”, a fin de generar espacios de planificación y establecimiento de políticas institucionales que conlleven a una optimización en el uso de los recursos públicos, hacer uso de la tecnología e innovación que permita el monitoreo de entidades contratantes y de proveedores del Estado, dinamizar la economía y la socialización adecuada de requerimientos institucionales para captar


mayor participación de personas naturales o jurídicas en los procedimientos de compras públicas (SERCOP, 2008).

El Servicio Nacional de Contratación Pública, actualmente tiene 500 computadores distribuidos a nivel nacional en las diferentes dependencias.

1.6.2 Información general de la institución

A continuación en la tabla 1 se describe la información de la institución en la cual se implementará el proyecto:

Tabla 1. Información general de la institución pública

 SERVICIO NACIONAL DE CONTRATACIÓN PÚBLICA	
Nombre Institución:	Servicio Nacional de Contratación Pública
Tipo:	Institución Pública
Directora General:	Econ. Silvana Vallejo
Dirección:	Avenida de Los Shyris 38 – 28 y el Telégrafo.
Teléfono:	(593-2) 2440050
Página Web:	https://portal.compraspublicas.gob.ec/SERCOP/

Fuente: Elaborado por el autor.

1.6.3. Misión institucional

Es el ente rector, técnico, regulador y autónomo de la contratación pública de Ecuador, que brinda a instituciones públicas y proveedores un modelo de gestión que asesora, controla y supervisa, sobre la base de los principios de eficacia eficiencia, transparencia, calidad y concurrencia, en los procedimientos de contratación.

1.6.4. Visión institucional

Ser al 2021, la institución pública reconocida a nivel regional por su alto grado de transparencia y calidad en sus servicios, facilitando e innovando la contratación pública.

1.6.5. Política institucional

“Comprometidos con la calidad, eficiencia, eficacia transparencia, confianza y satisfacción de nuestros usuarios mejoramos continuamente Sistema Nacional de

contratación pública a través del uso eficiente del gasto Público de regulación normalización de productos y servicios de la compra pública, Innovación de nuestros procesos y servicios y capacitación a nuestros actores, cumpliendo los requisitos técnicos y legales apoyados y un equipo humano responsable”.

1.6.6. Ubicación

El Servicio Nacional de Contratación Pública funciona en dos edificios principales ubicados en la Avenida de los Shyris 38-28 y El Telégrafo con su edificio matriz, y Edificio Alban al frente. Esta distribuido a nivel nacional con 7 zonales que cubren todas las provincias del país. Para este proyecto se ha tomado al edificio principal como Matriz Telégrafo, al secundario como Alban y a las sucursales como zonales respectivamente. A continuación en la figura 5 se muestra la ubicación actual del edificio donde funciona la institución.

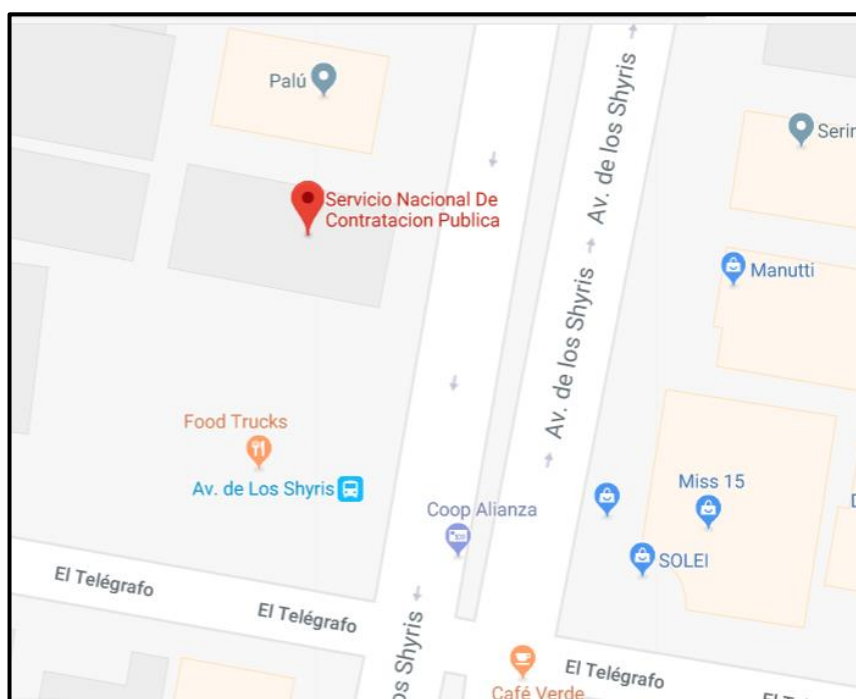


Figura 5. Ubicación actual de la institución

Fuente: Elaborado por el autor.

1.6.7 Coordinación Técnica de Innovación Tecnológica

En el Estatuto Orgánico de Gestión Organizacional por Procesos del SERCOP, artículo 1.3.2.4 se menciona que: “La Coordinación Técnica de Innovación Tecnológica

del Servicio Nacional de Contratación Pública es el corazón de la institución, el motor que da vida a los servicios que ofrece la institución al público”. Por esta razón todos sus recursos están actualizados y en correcto funcionamiento. Las compras públicas mueven millones de dólares a nivel nacional.

1.6.7. Direcciones que conforman la Coordinación Técnica de Innovación Tecnológica

Dirección de Desarrollo de Soluciones

Dirección de Gestión de Servicios Informáticos

Dirección de Operaciones de Innovación Tecnológica

Dirección de Seguridad Informática

1.6.7. Dirección de seguridad informática

Según el Estatuto Orgánico de Gestión Organizacional por Procesos del SERCOP, en el artículo 1.3.2.4.4 describe lo siguiente:

1.6.7. Misión:

Planificar, desarrollar y controlar la seguridad informática a través de la aplicación de políticas, normas, procedimientos y controles que garanticen la confidencialidad, integridad y disponibilidad de la información de la Institución.

1.6.7. Atribuciones y responsabilidades:

1. Definir lineamientos técnicos para garantizar la confidencialidad, integridad y disponibilidad de la información;
2. Elaborar instructivos para el otorgamiento de acceso a los servicios de tecnologías de información de la Institución;
3. Establecer los roles y perfiles para otorgar el acceso a los servicios de tecnologías de información de la Institución;
4. Elaborar instructivos para la implementación de controles de seguridad informática;

5. Implementar acciones correctivas y preventivas en el ámbito de la seguridad informática para las aplicaciones informáticas de la Institución;
6. Gestionar el monitoreo del funcionamiento del ambiente de producción en lo referente a seguridad informática;
7. Gestionar el monitoreo de la plataforma tecnológica en lo relacionado a la de seguridad informática de la Institución;
8. Articular el análisis y respuesta a incidentes de seguridad informática;
9. Elaborar informes de cumplimiento de políticas y normas de seguridad de la información en el ámbito de tecnologías de información; y,
10. Cumplir las demás atribuciones y responsabilidades que le fueran asignadas por la Coordinación Técnica de Innovación Tecnológica (SERCOP E. O., 2015)

CAPÍTULO 2

MARCO METODOLÓGICO

Para este proyecto se usaron varios métodos de investigación así como varias técnicas como la revisión bibliográfica y búsqueda de información por Internet, esta técnica nos ayuda a conocer más sobre el sistema a implementar tomando ejemplos anteriores para mejorar el proyecto. Para definir el uso de uno u otro equipo en el proyecto se buscó en varias fuentes y marcas para escoger la más conveniente en eficacia de funcionamiento y eficiencia en el presupuesto, ya que el costo también es muy importante para ejecutar el proyecto planteado.

Para la fundamentación teórica se utilizará el método teórico analítico sintético el mismo que nos ayudara a determinar en resumen los conceptos necesarios para comprender la importancia del sistema de seguridad, así como también la técnica de revisión bibliográfica y por Internet agrupando información necesaria para la realización de este proyecto.

En el marco metodológico se usará el método empírico de recolección de información y revisión documental ya que se necesita tener una visión clara de la situación actual para desarrollar una topología de seguridad apta para la institución que ayude a mejorar el nivel de seguridad en el proyecto a implementar.

Para realizar la propuesta se usará el método de análisis y recopilación de información que ayudará a tener una perspectiva clara de la necesidad y con la ayuda del método inductivo y de modelación permitirá el diseño de la topología propuesta para el proyecto. El método deductivo consiste en desarrollar una teoría empezando por formular sus puntos de partida o hipótesis básicas y deduciendo luego sus consecuencias con la ayuda de las subyacentes teorías formales. Sus partidarios señalan que toda explicación verdaderamente científica tendrá la misma estructura lógica, estará basada en una ley universal, junto a esta, aparecen una serie de condicionantes iniciales o premisas, de las cuales se deducen las afirmaciones sobre el fenómeno que se quiere explicar. El método inductivo se trata de un método que consiste en establecer enunciados universales ciertos a

partir de la experiencia, esto es, ascender lógicamente a través del conocimiento científico, desde la observación de los fenómenos o hechos de la realidad a la ley universal que los contiene.

Para la realización de la investigación se utilizó como técnica e instrumento para recolectar datos, la observación y lectura de manuales técnicos, herramientas electrónicas, software, entre otras. En esta investigación se utilizó la técnica de la observación documental, de presentación resumida, “una lectura general de los textos que contienen las fuentes de información que son de mucho interés, extrayendo los datos identificados de utilidad para la investigación” (Ballestrine, 2006). La misma fue ejecutada en esta investigación a partir de las búsquedas especializadas de documentos, patentes, informes o publicaciones relativas a tendencias tecnológicas asociadas con la implementación de un sistema de seguridad perimetral para seguridad de la información del Servicio nacional de contratación pública. En cuanto al instrumento aplicado, Arias lo define como “cualquier recurso, dispositivo o formato (en papel o digital) que se utiliza para obtener, registrar o almacenar información” (Arias, 2012).

Para la implementación y configuración del sistema de seguridad perimetral se utilizará el método práctico, así como también en la fase de pruebas y paso a producción, ya que se realizó una renovación total de los equipos firewall. En esta fase donde se realiza pruebas nos ayudó el método experimental ya que es susceptible a errores y se puede realizar comprobaciones previas para el buen funcionamiento del sistema implementado. En esta fase se hace un reconocimiento de los equipos físicos y lógicos existentes, un levantamiento de software y se acuerdan los mecanismo para la comunicación entre ambos. A continuación se realiza la conexión de todos los equipos, configuración y depuración de reglas. Se presenta un diseño de topología de seguridad de red perimetral y se finaliza con las pruebas de funcionamiento y validación de accesos hacia las diferentes zonas de la infraestructura tecnológica.

Todos y cada uno de los métodos seguidos para el desarrollo del proyecto se centran en buscar la solución y mejoramiento del sistema a implementar en el Servicio nacional de contratación pública.

CAPÍTULO 3

PROPUESTA

3.1 Análisis de riesgos, amenazas y vulnerabilidades

Se procedió a realizar un análisis de riesgos a nivel de coordinación tecnológica que se encuentra en el Anexo 1, identificando lo siguiente:

3.1.1 Riesgo identificado: Riesgo Tecnológico/Amenazas y Vulnerabilidades.

El riesgo tecnológico es alto debido a que si no reemplazamos los equipos a su debido tiempo, toda la plataforma tecnológica estará en peligro debido a los diferentes tipos de amenazas y vulnerabilidades existentes. Pudiendo la institución ser víctima de ataques realizados por cyberdelincuentes. El firewall perimetral es la herramienta primordial de protección en el sistema de seguridad perimetral.

3.1.2 Controles: Medios para contrarrestar los riesgos incluyendo políticas, lineamientos, procedimientos practicas o estructuras organizacionales. Lo controles se pueden aplicar en los diferentes módulos del sistema de seguridad perimetral como: cortafuegos perimetral, VPN IPSEC, VPN SSL, IPS, control de aplicaciones, conectividad de directorio activo, antimalware, sandboxing, antivirus, filtrado URL.

3.1.3 Control de Activos: Se consideran como activos a aquellos elementos que son considerados como esenciales para el correcto funcionamiento de la red y que tenga que ver con el alcance propuesto por la institución.

El activo más importante dentro de la institución es la información, con el riesgo tecnológico identificado pone en peligro la información contenida en los servidores de bases de datos, así como también en los computadores de los todos los funcionarios de la empresa, los cuales son vulnerables por virus u intromisiones fraudulentas.

La afectación en caso de intromisión a la información será a los servicios ofrecidos a la ciudadanía a nivel nacional y al estado en general.

3.1.4 Control de amenazas: Las amenazas se pueden definir como eventos, cosas o sucesos que pueden causar daño a los activos de la empresa. Los cuales pueden ser naturales (Terremotos, inundaciones, etc) o intencionales u causados por usuarios por errores o un ataque con fines malintencionados.

3.2 Propuesta de implementación

La seguridad comprende la parte más importante y crítica de la institución, por ello se propone implementar un sistema de seguridad perimetral basado en servidores virtuales que reemplace a los equipos físicos cerrados que actualmente tiene la institución.

La idea es que el software para firewall seleccionado sea instalado en los servidores virtuales para así tener abierta la posibilidad de aumentar o disminuir recursos cuando sea necesario para que el sistema siempre esté funcionando al 100%. Esto se requiere ya que constantemente está creciendo la población y la inserción a la participación de nuevas empresas como proveedores del estado y el tráfico crece significativamente cada año.

Los equipos estarán instalados en High Availability (HA), dos servidores en el Data Center de la Matriz El Telégrafo, dos servidores en el Data Center de CNT. En el DC del Telégrafo estará instalado también un servidor que servirá como management para administrar los cuatro equipos, además este mismo servirá de reporteador con un espacio suficiente como para almacenar *logs* que se sincronizan de todos los equipo.

3.2.1 Topología de seguridad propuesto

En la figura 6 se muestra la topología propuesta para el proyecto de implementación de un sistema de seguridad perimetral para seguridad de la información del Servicio Nacional de Contratación Pública.

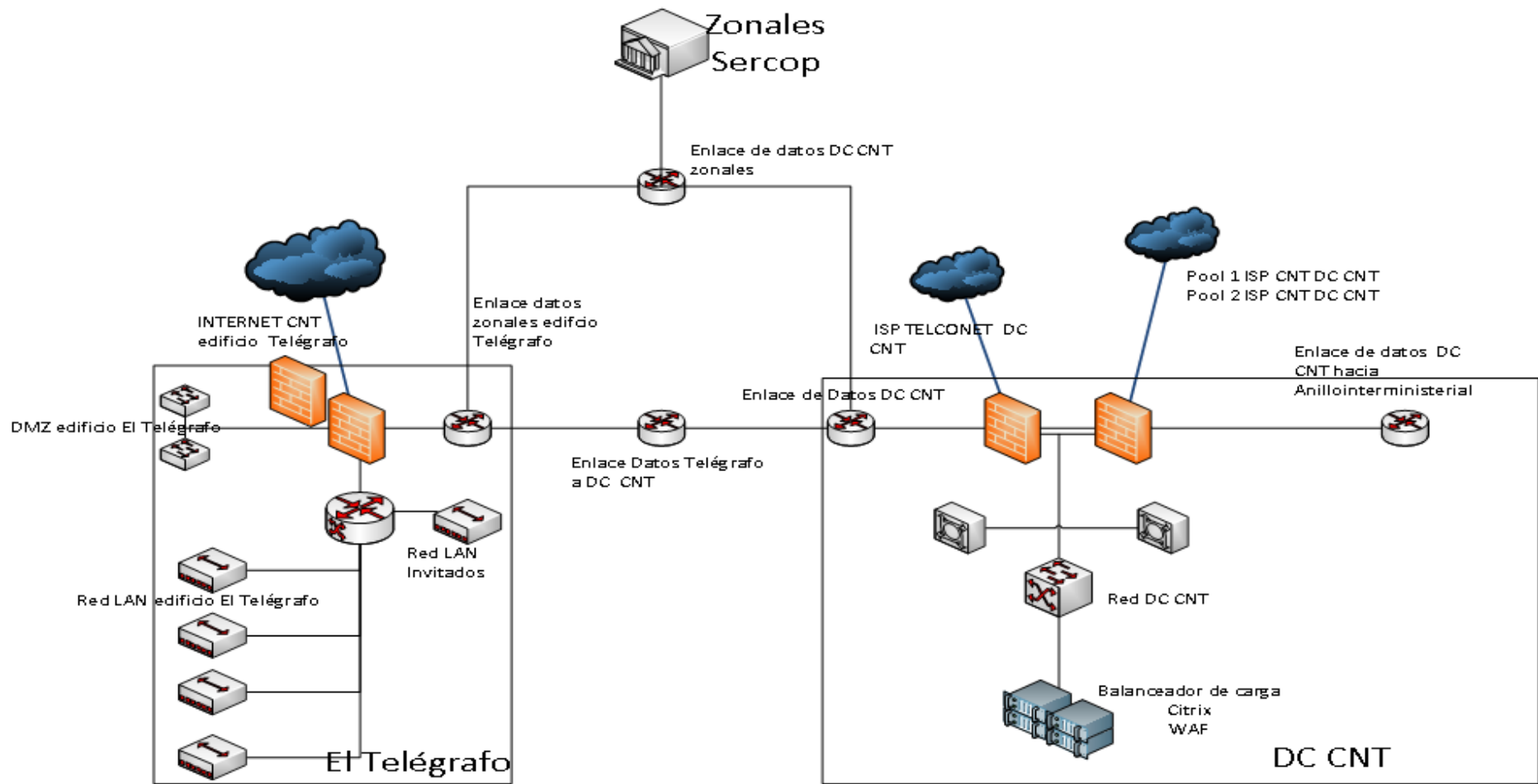


Figura 6. Esquema de seguridad propuesto

Fuente: Elaborado por el autor.

Como se puede observar en la figura 6 la propuesta se basa en usar 4 equipos físicos para implementar el firewall perimetral que reemplazará al anterior, ampliando la alta disponibilidad para los dos data center. En los equipos físicos se instalarán licencias de VMware para virtualizarlos e instalar en ellos un *software firewall*. En un quinto servidor físico será instalado de igual forma VMware para virtualizarlo y en el será instalado el *software management* para los cuatro equipos que además se encargará de correlacionar *logs* y generar reportes.

3.2.2 Selección de equipos físicos para los servidores

Para seleccionar los equipos físicos que se usarán como servidores para la herramienta de seguridad perimetral se tomó en cuenta que cumplan los siguientes requisitos:

- Cada servidor con al menos 3 *cores*.
- Los servidores deben ser tipo *RACK* los cuales serán instalados en el DC del edificio El Telégrafo y en el Data Center de CNT
- Dos discos SSD 480 GB o mejor.
- Tarjeta *smart array* para generación de RAID-1.
- 16 GB en RAM por equipo.
- 8 *interfaces* de red 10/100/1000 Mbps

3.2.3 Selección de *software firewall*

Para seleccionar el *software* que se usará como *firewall* se tomó en cuenta las siguientes características que debe cumplir:

- Rendimiento como firewall: mínimo 450 Mbps.
- Rendimiento como IPS: mínimo 250 Mbps.
- Sesiones concurrentes: mínimo 100.000.
- Nuevas conexiones por segundo: mínimo 7.000.
- Rendimiento de IPSec VPN: mínimo 175 Mbps.
- Pares VPN: Mínimo 100.
- Soporte para aplicaciones y sitios WEB: mínimo 4.000.
- Número de categorías para filtrado URL: mínimo 80.
- Número de URL categorizadas para filtrado URL: mínimo 280'000.000.

- La inspección de tráfico deberá realizarse totalmente a nivel de aplicaciones (app control).
- La solución no deberá inspeccionar con la tecnología *statefull inspection*.
- El equipo deberá correlacionar los *logs* sin agregar un equipo adicional. Es decir, deberá generar reportes personalizados y gráficas de las aplicaciones más utilizadas así como de los usuarios con mayor número de sesiones concurrentes sobre el mismo equipo.
- El equipo deberá tener la opción para descifrar el tráfico SSL.
- Alta disponibilidad: activo/*standby*
- VLAN: mínimo 1.024.

3.2.4 Selección del equipo físico para *management/reporter*

El equipo físico donde se instalará el software de administración para la gestión centralizada y reporteador debe cumplir con las siguientes características:

- Número de equipos a gestionar: hasta 25 equipos.
- Eventos de IPS: mínimo 30'000.000
- Espacio de almacenamiento para eventos: mínimo 900 GB.
- Tamaño de mapa de red (*hosts/usuarios*): 50.000/50.000.
- Flujos por segundo: mínimo 5.000.
- Control de políticas de acceso integrado
- Gestión multiusuario y herencia de directivas
- Visibilidad completa de amenazas
- El equipo deberá correlacionar los *logs* de los 4 equipos

La solución de perímetro se implementará sobre servidores de marcas como HP, CISCO, DELL, etc.

3.2.5 Licenciamiento de *clúster* de borde

Licenciamiento para el *clúster* de borde para los servicios que ofrece el SERCOP a la ciudadanía, el cual deberá ser instalado en el Data Center de CNT, que permita tener las siguientes funcionalidades:

- Firewall perimetral.
- VPN IPSec, con cualquier plataforma.

- Soporte de alta disponibilidad (activo-pasivo).
- VPN SSL.
- IPS.
- Control de aplicaciones.
- Conectividad al directorio activo.
- *Antimalware*.
- Soporte de *sandboxing*.

Licenciamiento para un *clúster* de perímetro para aplicativos y salida a Internet de usuarios de la institución, que deberá ser instalado en el edificio matriz El Telégrafo del SERCOP, que permita las siguientes funcionalidades:

- Firewall perimetral.
- VPN IPsec, con cualquier plataforma.
- Soporte de alta disponibilidad (activo-pasivo).
- VPN SSL.
- IPS.
- Control de aplicaciones.
- Filtrado de URL.
- Conectividad al directorio activo.
- *Antivirus*.
- *Antimalware*.
- *Sandboxing*

3.2.6 Licenciamiento para administración y reporte

La solución de administración será implementada sobre plataforma virtualizada entregada por la institución.

- Licencia para administración de los equipos gateways de seguridad perimetral.
- Licencia para reporteador.
- Licencia para correlacionar *logs* de alerta de todos los equipos *gateway*.
- La solución deberá ser parte del cuadrante Leader en el cuadrante Gartner mínimo 2016 de Next Generation Firewall.

3.3 Análisis de costo y selección de *software* y *hardware*

En base a los requisitos planteados y teniendo en cuenta que el proyecto tiene una duración de 3 años por lo que el licenciamiento del *software* de seguridad debe tener esta vigencia, tanto de actualizaciones y soporte, se solicitaron proformas de costos tanto de los equipos físicos como del *software* necesario para el sistema. A continuación en la tabla 2 se detalla los costos de las propuestas recibidas de varias empresas del sector de la seguridad:

Tabla 2. Costos propuestos

Empresa	Marca	Costo
Grupo Radical	Palo Alto Networks	121.000 + IVA
Ebtel	Check Point	174.000 + IVA
Digiware	Check Point	185.000 + IVA
CNT	Palo Alto Networks	246.408 incluido IVA
Point Technical Solutions	Palo Alto Networks	121.000 + IVA

Fuente: Elaborado por el autor

Los costos detallados en la tabla 2 se refieren al total del costo que incluye equipamiento físico y lógico, actualizaciones y soporte, para los tres años planteados.

De acuerdo a lo descrito se observa que el presupuesto referencial necesario para la adquisición de los equipos tanto *hardware* y *software*, así como también el respectivo licenciamiento de firewall y soporte es de aproximadamente 136.000 dólares.

Una vez revisadas las propuestas presentadas se eligieron a 2 empresas, las cuales cumplieron con los requisitos para participar en la subasta inversa que se realiza para adquirir un bien en todas las instituciones públicas.

Luego del procedimiento correspondiente, se declaró como ganador y se adjudicó el contrato al oferente empresa Point Technical Soluciones CIA LTDA, por el valor de USD \$ 118,577.00 (Ciento dieciocho mil quinientos setenta y siete dólares de los Estados Unidos de América con 00/100) sin incluir IVA.

En la tabla 3 se detalla la propuesta ganadora con la descripción de productos, hardware, software licenciado para firewall, software licenciado para virtualización y soporte por 3 años.

Tabla 3. Presupuesto total del proyecto

Presupuesto total del proyecto:		\$ 135,520.00		
DESGLOSE DE COMPONENTES (BIENES TANGIBLES E INTANGIBLES)				
Tipo de recurso	Descripción producto / servicio	Cantidad	Costo unitario	Total
Software	Palo Alto Networks Perpetual Bundle (BND2) for VM-Series that includes VM-100, Threat Prevention, PANDB URL filtering, Global Protect and WildFire subscriptions, and Premium Support, 3 year 7x24 con la fabrica.	4	\$ 10,000.00	\$ 40,000.00
Software	Panorama central management software, 25 devices	1	\$ 12,000.00	\$ 12,000.00
Software	Premium support 3 year prepaid , Panorama 25 devices, 3 year 7x24 con la fabrica.	1	\$ 5,000.00	\$ 5,000.00
Hardware	Servidores recomendados por la fabrica con 8 INTERFACES COBRE	4	\$ 6,000.00	\$ 24,000.00
Software	VMware vSphere Enterprise Plus	5	\$ 6,800.00	\$ 34,000.00
Subtotal				\$ 115,000.00
IVA (12 %)				\$ 13,800.00
Total				\$ 128,800.00
DESGLOSE DE COMPONENTES (SERVICIOS)				
Tipo de servicio	Cantidad	Costo unitario	Total	
Instalación, Soporte 7x24x365, Soporte N1 vía SOC, 2 Mantenimientos	1	\$ 2,000.00	\$ 2,000.00	
Preventivos en el primer año				
Soporte de la Solucion de Firewall 2do año	1	\$ 2,000.00	\$ 2,000.00	
Soporte de la Solucion de Firewall 3er año	1	\$ 2,000.00	\$ 2,000.00	
Subtotal:				\$6,000.00
IVA (12%):				\$720.00
Total				\$6,720.00

Fuente: Elaborado por el autor

CAPÍTULO 4

IMPLEMENTACIÓN

En el Servicio Nacional de Contratación Pública se realizan miles de transacciones moviendo millones de dólares diarios, la institución es el ente rector de la contratación a nivel nacional. La información que se maneja dentro de la empresa es de carácter crítico y confidencial.

Para proteger una red se deben tomar todas las medidas necesarias, por esta razón se necesita un firewall perimetral para realizar un filtrado, permitir y negar el paso a los paquetes que no cumplan las políticas que se configuran en el equipo.

4.1 Levantamiento de información

Para empezar el proceso y desarrollo de la implementación se realizaron varias actividades previas de levantamiento de información que fueron necesarias para tener una visión clara antes de la instalación y configuración. En la tabla 4 se detalla las actividades realizadas.

Tabla 4. Plan de levantamiento de información

Plan de levantamiento de información				
Actividad	Actores	Responsabilidad	Actores	Acción
Recopilación de información	Sergio Toapanta	Solicitar información como redes, topología, direccionamiento IP, dispositivos	SERCOP	Entregar información solicitada
Levantamiento de información <i>firewall</i>	Sergio Toapanta	Solicitud de información de políticas de seguridad	SERCOP	Entregar información solicitada
	Sergio Toapanta	Solicitud de información de políticas de NAT	SERCOP	Entregar información solicitada
	Sergio Toapanta	Solicitud de información de políticas de filtrado WEB	SERCOP	Entregar información solicitada
	Sergio Toapanta	Solicitud de información de políticas IPS	SERCOP	Entregar información solicitada

	Sergio Toapanta	Solicitud de información de políticas de VPN	SERCOP	Entregar información solicitada
	Sergio Toapanta	Solicitud de información de objetos de red	SERCOP	Entregar información solicitada
	Sergio Toapanta	Solicitud de información de grupos de objetos de red	SERCOP	Entregar información solicitada
	Sergio Toapanta	Solicitud de información de servicios de red	SERCOP	Entregar información solicitada
	Sergio Toapanta	Solicitud de información de grupos de servicios de red	SERCOP	Entregar información solicitada
	Sergio Toapanta	Solicitud de información de usuarios de accesos	SERCOP	Entregar información solicitada
	Sergio Toapanta	Solicitud de información de grupos de usuarios accesos	SERCOP	Entregar información solicitada
Conexiones de Red	Sergio Toapanta	Solicitud de direccionamiento IP, interfaces físicas.	SERCOP	Entregar información solicitada
	Sergio Toapanta	Solicitud de rutas.	SERCOP	Entregar información solicitada
	Sergio Toapanta	Solicitud de zonas de red.	SERCOP	Entregar información solicitada
	Sergio Toapanta	Solicitud de direccionamiento de red LAN.	SERCOP	Entregar información solicitada
Revisión de información firewall	Sergio Toapanta	Revisión de políticas de seguridad	SERCOP	Detalle de políticas
	Sergio Toapanta	Revisión de políticas de NAT	SERCOP	Detalle de políticas
	Sergio Toapanta	Revisión de políticas de filtrado WEB	SERCOP	Detalle de políticas
	Sergio Toapanta	Revisión de políticas IPS	SERCOP	Detalle de políticas
	Sergio Toapanta	Revisión de políticas de VPN	SERCOP	Detalle de políticas
Objetos de red	Sergio Toapanta	Revisión de objetos de red	SERCOP	Detalle de políticas
	Sergio Toapanta	Revisión de grupos de objetos de red	SERCOP	Detalle de políticas
	Sergio Toapanta	Revisión de servicios de red	SERCOP	Detalle de políticas
	Sergio Toapanta	Revisión de grupos de servicios de red	SERCOP	Detalle de políticas
	Sergio Toapanta	Revisión de usuarios de acceso	SERCOP	Detalle de políticas

	Sergio Toapanta	Revisión de grupos de usuarios de acceso	SERCOP	Detalle de políticas
Conexiones de Red	Sergio Toapanta	Revisión de direccionamiento IP interfaces físicas.	SERCOP	Detalle de políticas
	Sergio Toapanta	Revisión de ruteo.	SERCOP	Detalle de políticas
	Sergio Toapanta	Revisión de zonas de red.	SERCOP	Detalle de políticas
	Sergio Toapanta	Revisión de direccionamiento de red LAN.	SERCOP	Detalle de políticas
Entrega de equipamiento	Point Technical	Desempaque de equipos	SERCOP	Comprobación y validación
	Sergio Toapanta	Revisión componentes ofertados	SERCOP	Comprobación y validación
	Sergio Toapanta	Entrega recepción de los equipos	SERCOP	Comprobación y validación

Fuente: Elaborado por el actor

La implementación se lo realiza en una institución pública y debido a políticas de confidencialidad firmados previo a la realización del proyecto solo se mostrará extractos del levantamiento de información realizado.

4.1.1 Servidores, computadores PC y portátiles

La institución cuenta con un total de 486 equipos con sistema operativo windows, linux y MAC. Todos estos se encuentran protegidos por un antivirus licenciado. A nivel de servidores cuenta con 264 en el data center de CNT y 40 servidores en el edificio El Telégrafo.

4.1.2 Levantamiento de redes existentes en la institución

La institución tiene un edificio matriz El Telégrafo y siete zonales distribuidas en las diferentes provincias del país, cada equipo tiene asignada una ip dentro de las redes que se despliegan a nivel nacional. En el Anexo 3 se detalla un extracto de todas las redes existentes en la institución a nivel de usuario final, por políticas de confidencialidad.

A continuación en el anexo 4 se detalla un extracto del direccionamiento IP usado para los servidores de producción internos que al salir por una política de NAT son

publicados los servicios que ofrece la institución a la ciudadanía, desde el *data center* de CNT.

4.1.3 Pool de IP públicas de los servicios

Para realizar la publicación de los servicios que ofrece la institución se usan dos pools de IP públicas contratadas a CNT con rango 1 190.152.X.32/28 con máscara 255.255.255.240 obteniendo 14 host, rango 2 190.152.X.64/26 con máscara 255.255.255.192 obteniendo 62 host.

4.1.4 Configuración actual del firewall perimetral

Los equipos de seguridad perimetral actuales han cumplido con su vigencia tecnológica al estar en funcionamiento 5 años, los equipos son appliance marca *Check Point* modelo 4600 con sistema operativo GAIA Versión R77.30 para navegación web y para la publicación de servicios que ofrece la institución el *appliance Check Point* 4800 con GAIA Versión R77.30. En la figura 4.9 se muestra captura del *appliance 4600*.

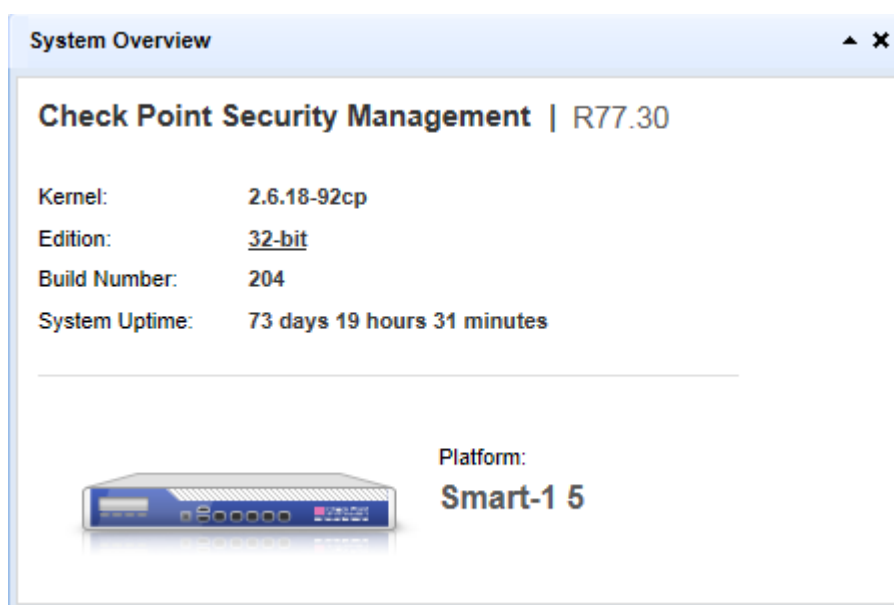


Figura 7. Captura de *Appliance Check Point* 4600

Fuente: Elaborado por el autor

El SERCOP, posee un equipamiento de seguridad perimetral basado en una plataforma CHECKPOINT el cual se encuentra distribuido en dos ambientes de producción.

Dado que el SERCOP posee un edificio como planta central ubicada en las calles Av. Shyris y el Telégrafo en el cual se establecen las coordinaciones y direcciones administrativas y de giro de negocio, se establece un equipo de seguridad perimetral que cumple la función de *gateway* y *firewall* para dotar de seguridad en la navegación de los usuarios internos de la ciudad de Quito y de las coordinaciones zonales a nivel nacional.

Para la publicación de servicios el SERCOP mantiene el servicio de *housing* en el centro de datos de CNT ubicado en la Av. Gaspar de Villarroel, en donde poseen toda la granja de servidores y la comunicación con el anillo de datos interministerial.

Una vez realizado la recopilación de información se puede evidenciar la topología lógica y física aplicada en los dos sitios.

4.1.6 Topología lógica de la red de datos SERCOP

En la tabla 5, 6 y 7 se muestra los enlaces de Internet, datos, LAN que están distribuidos de la siguiente manera:

Tabla 5. Enlaces de Internet SERCOP

Enlaces de Internet	
Pool ISP CNT Edificio Telégrafo	181.113.X.187/29
Pool 1 ISP CNT DC CNT	190.152.X.32/28
Pool 2 ISP CNT DC CNT	190.152.X.64/26
Pool 1 ISP TELCONET DC CNT	190.X.X.1/29

Fuente: Elaborada por el autor

Tabla 6. Enlace de datos SERCOP

Enlace de datos	
Enlace Datos Provincias ISP CNT Edif. Telégrafo	10.X.3.0/24
Enlace Datos Telégrafo a DC CNT	192.X.4.0/24
Enlace de Datos DC CNT a Provincias	10.X.15/24
Enlace de Datos DC CNT a Anillo Interministerial	10.X.X.0/24

Fuente: Elaborada por el autor

Tabla 7. Red LAN SERCOP

Red LAN	
DMZ 1 Edificio El Telégrafo	192.X.0./24
DMZ 2 Edificio el Telégrafo	172.X.254.0/24
Red lan Edificio el Telégrafo	172.X.6.0/24
Red Lan Invitados	10.X.10./24
Red DC CNT Y Red de Provincias	192.X.0.0/16

Fuente: Elaborada por el autor

4.1.7 Direccionamiento IP equipos *firewall Check Point*

A continuación en la tabla 8 se presenta el direccionamiento ip utilizado para el acceso y administración de los equipos Chek Point tanto del Data Center Matriz como de Data Center CNT.

Tabla 8. Direccionamiento ip equipos firewall

Ubicación	Descripción	IP	URL
Data Center CNT	Gateway01 (sg1dc)	10.x.15.2	https://10.X.15.2
	Gateway02 (sg2dc)	10.x.15.3	https://10.X.15.3

Edificio El Telégrafo	Gateway03 (sghq)	172.x.254.25	https://172.X.254.25
	Manager (smhq)	172.x.254.25	https://172.X.254.25
	Reporter (erhq)	172.x.254.25	https://172.X.254.25

Fuente: Elaborada por el autor

4.1.8 Reglas configuradas en equipos Check Point edificio El Telégrafo

En los equipos Check Point se evidencian políticas configuradas para permisos de navegación, acceso VPN, acceso a páginas restringidas, acceso a streaming media, correos externos, etc. Todos estos permisos a nivel de usuario y equipos que se encuentran en el edificio Matriz Telégrafo. En el Anexo # se lista las políticas que actualmente tiene el equipo.

4.1.9 Reglas configuradas en equipos Check Point data Center CNT

Dentro del Data Center de CNT tenemos equipos 4800 Check Point en HA, en los cuales se encuentran configuradas todas las reglas de seguridad y reglas de NAT para publicar todos los servicios que ofrece la institución a la ciudadanía como Sistema Oficial de Contratación del Estado (SOCE), Catalogo Electrónico, Subasta Inversa de Medicamentos (SICM), etc.

Una vez concluido con la revisión de la información recopilada se procede a la implementación de los equipos adquiridos así como también a la configuración de políticas y reglas de seguridad.

4.2 Implementación

A continuación se muestra en la tabla 9, las actividades realizadas de implementación:

Tabla 9. Actividades realizadas de implementación

IMPLEMENTACIÓN				
Actividad	Actor	Responsabilidad	Actor	Responsabilidad
Puesta física de equipamiento	Sergio Toapanta	Ubicación en los RACK	SERCOP	Verificación de disponibilidad y asignación
	Sergio Toapanta	Mapeo interfaces físicas de red vs switch virtuales	SERCOP	Verificación de disponibilidad y asignación
	Sergio Toapanta	Conexión de cableado y etiquetado	SERCOP	Verificación de disponibilidad y asignación
	Sergio Toapanta	Encendido de equipos	SERCOP	Verificación de disponibilidad y asignación
Instalación y configuración de VM 300	Sergio Toapanta	Instalación ESXI 6.0 u3	SERCOP	Verificación de disponibilidad y asignación
	Sergio Toapanta	Configuración <i>networking</i> ESXI 6.0 u3	SERCOP	Verificación de disponibilidad y asignación
	Sergio Toapanta	Instalación VM-300	SERCOP	Verificación de disponibilidad y asignación
Configuración de los equipos	Sergio Toapanta	Creación de tablas de rutas estáticas	SERCOP	Verificación de disponibilidad y asignación
	Sergio Toapanta	Creación alta disponibilidad entre equipos	SERCOP	Verificación de disponibilidad y asignación
	Sergio Toapanta	Configuración red de administración	SERCOP	Verificación de disponibilidad y asignación
	Sergio Toapanta	Configuración de interfaces de red	SERCOP	Verificación de disponibilidad y asignación
	Sergio Toapanta	Configuración de zonas de red	SERCOP	Verificación de disponibilidad y asignación
	Sergio Toapanta	Creación de objetos de red	SERCOP	Verificación de disponibilidad y asignación
	Sergio Toapanta	Creación de grupos de objetos	SERCOP	Verificación de disponibilidad y asignación
	Sergio Toapanta	Creación de servicios	SERCOP	Verificación de disponibilidad y asignación

	Sergio Toapanta	Creación de grupos de servicios	SERCOP	Verificación de disponibilidad y asignación
Configuración de políticas	Sergio Toapanta	Configuración de políticas de Seguridad	SERCOP	Verificación de disponibilidad y asignación
	Sergio Toapanta	Configuración de políticas de NAT	SERCOP	Verificación de disponibilidad y asignación
	Sergio Toapanta	Configuración de políticas VPN	SERCOP	Verificación de disponibilidad y asignación
Licenciamiento	Sergio Toapanta	Instalación de licenciamiento.	SERCOP	Verificación de disponibilidad y asignación
	Sergio Toapanta	Actualización de software	SERCOP	Verificación de disponibilidad y asignación
	Sergio Toapanta	Presentación de equipo con perfil básico instalado	SERCOP	Verificación de disponibilidad y asignación
Pruebas y verificación de funcionamiento	Sergio Toapanta	Ping hacia interfaces	SERCOP	Verificación de disponibilidad y asignación
	Sergio Toapanta	Navegación por INTERNET	SERCOP	Verificación de disponibilidad y asignación
	Sergio Toapanta	Publicación de servicios	SERCOP	Verificación de disponibilidad y asignación

Fuente: Elaborada por el autor

4.2.1 Configuración de equipos

Los trabajos de implementación empiezan con la instalación del HYPERVISOR dónde van estar alojados los servidores virtuales, como se muestra a continuación:

4.2.1 Instalación Hypervisor

4.2.2. Creación RAID (Redundant Array of Independent Disks) 1

Se procede a realizar la configuración de RAID 1 en la que se instalará el *hypervisor* ESXi 6.0, se procede a realizar el siguiente procedimiento:

Se ingresa a la utilidad de BIOS. Se muestra en la figura 8.



Figura 8. Interfaz BIOS

Fuente: Elaborado por el autor

Se ingresa a los dispositivos del equipo, se procede a crear el *virtual disk* con las unidades físicas disponibles. Se muestra en la figura 9.



Figura 9. Interfaz para creación de virtual disk

Fuente: Elaborado por el autor

Y se procede a reiniciar el equipo.

4.2.2 Instalación EXSi (Plataforma Virtual de VMware)

Se procedió a iniciar desde la unidad USB en donde se tiene cargado la imagen personalizada para equipos Dell y/o HPE. Se muestra en la figura 10.

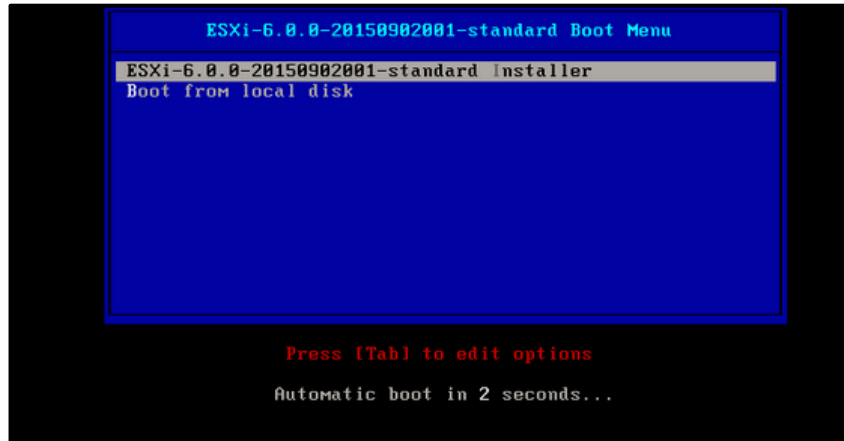


Figura 10. Interfaz de instalación de imagen de disco

Fuente: Elaborado por el autor

Se procedió a escoger el RAID 1 configurado anteriormente. Se muestra en la figura 11.

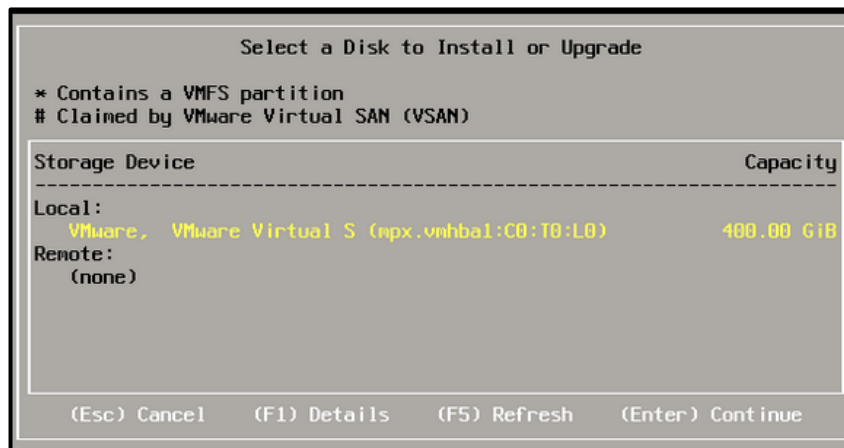


Figura 11. Selección de RAID 1

Fuente: Elaborado por el autor

Se ingresa las credenciales necesarias por ejemplo, **usuario: root, contraseña: password.**

Se muestra en la figura 12.



Figura 12. Interfaz de ingreso

Fuente: Elaborado por el autor

Una vez finalizada la instalación el servidor se reinicia y se configura la red de administración. Se muestra en la figura 13.

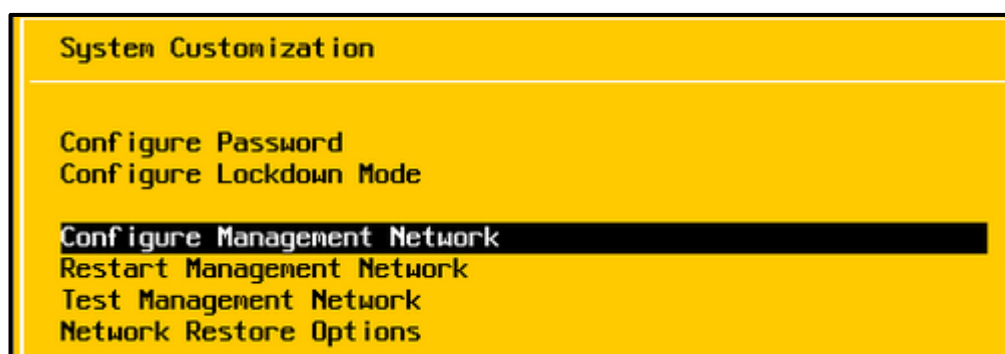


Figura 13. Interfaz de selección management

Fuente: Elaborado por el autor

Las IP usadas para la red de administración configuradas son las siguientes. Se muestra en la tabla 10:

Tabla 10. IP red de administración

IP red de administración	
Dirección IP ESXi 1:	172.X.X.241 /24
Gateway:	172.X.X.254
Dirección IP ESXi 2:	172.X.X.242 /24
Gateway:	172.X.X.254
Dirección IP ESXi 3:	172.X.X.245 /24
Gateway:	172.X.X.254

Fuente: Elaborada por el autor

4.2.3 Despliegue de VM-300 PAN

Una vez se cuenta con el acceso al hypervisor se realiza la instalación de la VM-300 de paloalto NETWORKS, para esto se realiza el siguiente procedimiento.

Se descarga la vm desde el portal de soporte de paloalto Networks, como se muestra en la figura 14.

PAN-OS for VM-Series Base Images					
8.1.2	10/11/2018	Release Notes	PA-VM-ESX-8.1.2.ova	2.6 GB	<input type="button" value="Checksum"/>
8.1.0	03/03/2018	Release Notes	PA-VM-ESX-8.1.0.ova	2.1 GB	<input type="button" value="Checksum"/>

Figura 14. Descarga de OVA (*Open Virtual Appliance*)

Fuente: Elaborado por el autor

Se ingresa el servidor ESXi, se realiza el despliegue de la imagen descargada. Se muestra en la figura 15.

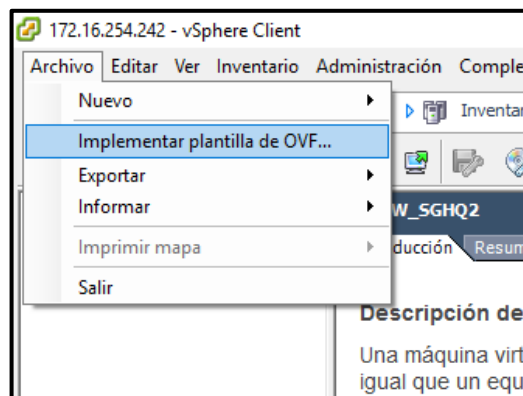


Figura 15. Despliegue imagen ISO

Fuente: Elaborado por el autor

Se carga la imagen OVA en el servidor ESXi. Con la imagen cargada al sistema se procede a actualizar a la capacidad de los recursos como se muestra en la figura 16.

Hardware	Resumen
Memoria	8772 MB
CPU	8
Video card	Video card
VMCI device	Obsoleto
SCSI controller 0	LSI Logic Parallel
CD/DVD drive 1	Dispositivo cliente
Hard disk 1	Disco virtual
Network adapter 1	MNGMT-PA
Network adapter 2	DATOS_SERCOP
Network adapter 3	DATOS_SERCOP
Network adapter 4	DATOS_SERCOP
Network adapter 5	DATOS_SERCOP
Network adapter 6	DATOS_SERCOP
Network adapter 7	DATOS_SERCOP
Network adapter 8	DATOS_SERCOP
Network adapter 9	DATOS_SERCOP

Figura 16. Seleccionar OVA

Fuente: Elaborado por el autor

El sistema detectará el servicio DHCP disponible y asignará una IP a la interfaz física de administración, con la que se puede acceder al GUI web para seguir con la configuración.

Se asignan las siguientes interfaces para la administración de las VM-300, por las que el aplicativo procede a realizar las actualizaciones y descarga de firmas, así como de licenciamiento.

4.2.4 FW_Activo

Esta configuración de los equipos firewall es porque están en alta disponibilidad, uno permanece en activo y el otro en pasivo para cuando exista algún problema con el principal activo se levanta el pasivo. Se muestra en la figura 17.

Configuración de interfaz de gestión	
Tipo de IP	<input checked="" type="radio"/> Estático <input type="radio"/> Cliente DHCP
Dirección IP	172.16.254.243
Máscara de red	255.255.255.0
Puerta de enlace predeterminada	172.16.254.254
Dirección IPv6/Longitud de prefijo	
Puerta de enlace IPv6 predeterminada	
Velocidad	auto-negotiate
MTU	1500

Figura 17. Firewall activo

Fuente: Elaborado por el autor

4.2.5 FW_Pasivo

A continuación en la figura 18 se muestra la configuración de la interfaz del firewall pasivo.

Configuración de interfaz de gestión	
Tipo de IP	<input checked="" type="radio"/> Estático <input type="radio"/> Cliente DHCP
Dirección IP	172.16.254.244
Máscara de red	255.255.255.0
Puerta de enlace predeterminada	172.16.254.254
Dirección IPv6/Longitud de prefijo	
Puerta de enlace IPv6 predeterminada	
Velocidad	auto-negotiate
MTU	1500

Figura 18. Firewall pasivo

Fuente: Elaborado por el autor

4.3 Configuración de networking virtual.

En la figura 19 se muestra la configuración de mapeo de la red virtual versus las interfaces físicas del servidor.

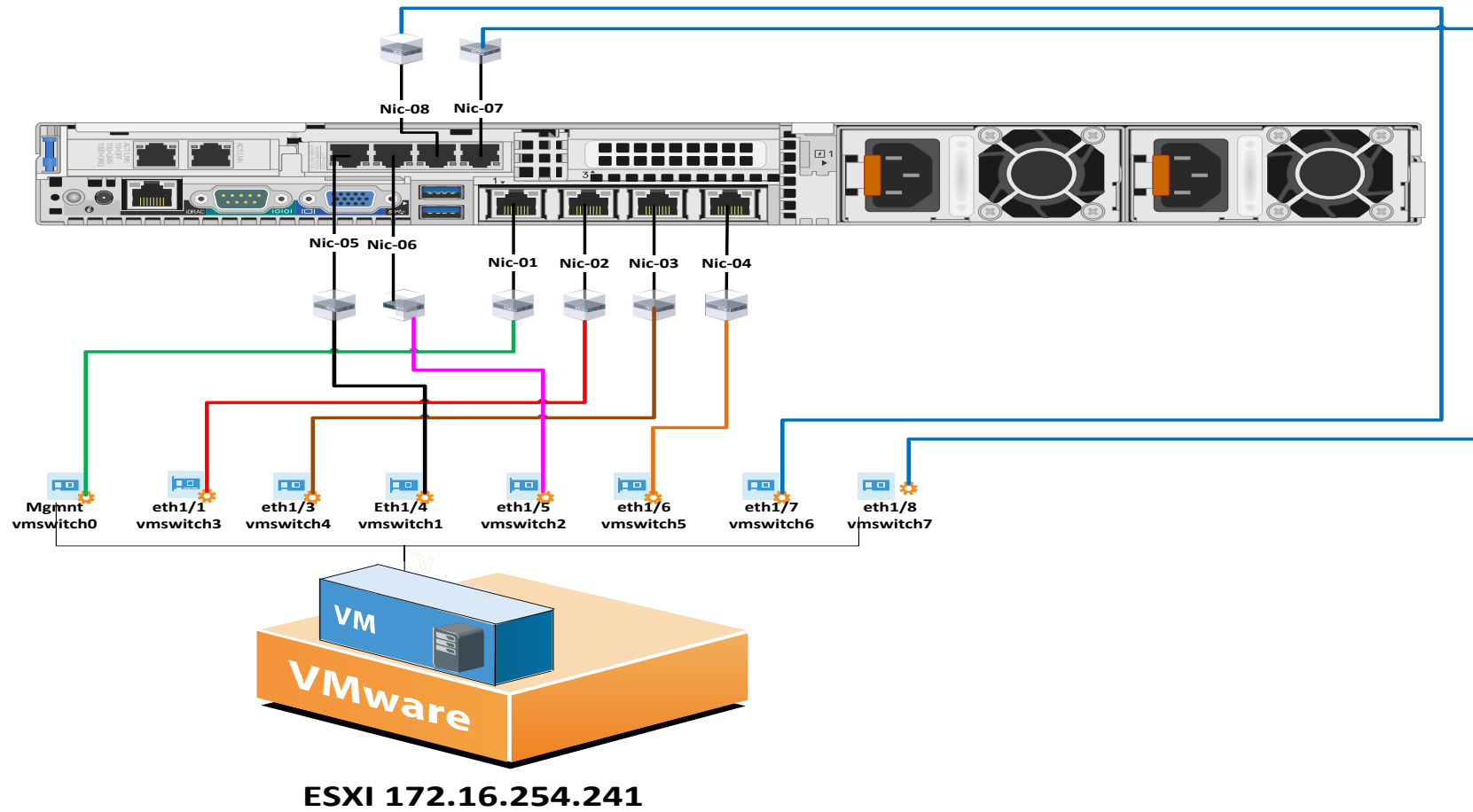


Figura 19. Configuración networking virtual

Fuente: Elaborado por el autor

4.3.1 Direccionamiento IP utilizado

En la tabla 11 y 12 se muestra el direccionamiento IP utilizado para los servidores virtuales de VM-300 y firewall palo alto.

Tabla 11. Direccionamiento IP utilizado

EQUIPO		DIRECCIÓN IP
Vmware		
ESXi 1		172.16.X.X
ESXi 2		172.16.X.X
ESXi 3		172.16.X.X
Panorama		172.16.X.X

Fuente: Elaborada por el autor

Tabla 12. IP interfaces

INTERFAZ	MAC-ADDRESS	DIRECCIÓN IP
Palo Alto 01		
Ethernet1/1	00:0c:29:a9:0a:c4	181.113.X.187/29
		181.113.X.186/32
		181.113.X.189/32
Ethernet1/3	00:0c:29:a9:0a:d8	172.X.0.X/24
Ethernet1/4	00:0c:29:a9:0a:e2	10.X.5.231/24
Ethernet1/5	00:0c:29:a9:0a:ec	10.X.10.X/24
Ethernet1/6	00:0c:29:a9:0a:f6	172.X.6.253/24
Ethernet1/7	00:0c:29:a9:0a:00	1.1.X.2/30
Ethernet1/8	00:0c:29:a9:0a:0a	1.1.X.2/30
Palo Alto 02		
Ethernet1/1	00:0c:29:58:cd:e3	181.113.X.187/29
		181.113.X.186/32
		181.113.X.189/32
Ethernet1/3	00:0c:29:58:cd:f7	172.X.0.X/24
Ethernet1/4	00:0c:29:58:cd:01	10.X.5.231/24
Ethernet1/5	00:0c:29:58:cd:0b	10.X.10.X/24
Ethernet1/6	00:0c:29:58:cd:15	172.X.6.253/24
Ethernet1/7	00:0c:29:58:cd:1f	1.1.X.2/30
Ethernet1/8	00:0c:29:58:cd:29	1.1.X.2/30

Fuente: Elaborada por el autor

4.4 Configuración de firewall edificio El Telégrafo

Una vez realizada las configuraciones de la red en el equipo Palo Alto se procede a realizar la creación de objetos, reglas, perfiles de seguridad, VPN, usuarios, etc.

4.4.1 Creación objetos

Con la referencia del equipo *Check Point* se procede a crear los objetos para ser utilizados en las políticas de seguridad.

4.4.2 Objetos de IP catalogadas como Spam

En la figura 20 se muestra los objetos de IP catalogados como Spam para ser bloqueados en las políticas de seguridad.

<input type="checkbox"/>	BLOCK_IP_SPAM_132.148.147.9	Máscara de red IP	132.148.147.9
<input type="checkbox"/>	BLOCK_IP_SPAM_146.0.77.190	Máscara de red IP	146.0.77.190
<input type="checkbox"/>	BLOCK_IP_SPAM_18.188.74.66	Máscara de red IP	18.188.74.66
<input type="checkbox"/>	BLOCK_IP_SPAM_185.114.234.58	Máscara de red IP	185.114.234.58
<input type="checkbox"/>	BLOCK_IP_SPAM_46.105.51.28	Máscara de red IP	46.105.51.28
<input type="checkbox"/>	BLOCK_IP_SPAM_62.210.139.65	Máscara de red IP	62.210.139.65
<input type="checkbox"/>	BLOCK_IP_SPAM_88.99.246.136	Máscara de red IP	88.99.246.136
<input type="checkbox"/>	BLOCK_USA_75.0.0.0	Máscara de red IP	75.0.0.0/10
<input type="checkbox"/>	BLOCK_WANADOO_193.253.178.0	Máscara de red IP	193.253.178.0/24

Figura 20. Objetos de IP Spam

Fuente: Elaborado por el autor

4.4.3 Objetos de equipos de usuarios internos

Se procede a crear los objetos con las IP pertenecientes a los usuarios internos de la institución, estos objetos nos servirán para identificar a quien pertenece la IP y conceder permisos o bloqueos solicitados.

4.5 Agrupación de objetos, redes y servicios

4.5.1 Grupos de la red de servidores

A continuación en la figura 21 se muestra un extracto de a forma de agrupar redes necesarias. No se puede mostrar las redes por políticas de confidencialidad.

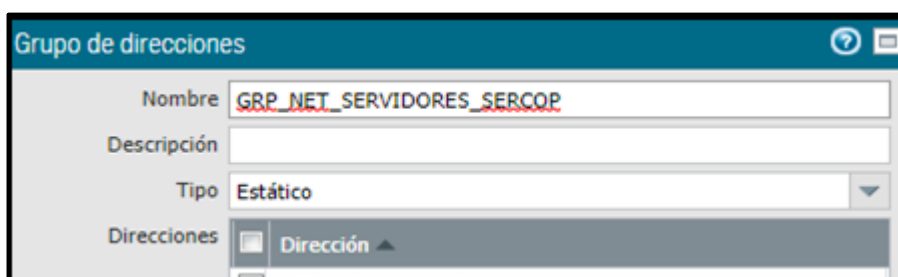


Figura 21. Agrupación de redes de servidores

Fuente: Elaborado por el autor

4.5.2 Grupos de redes

Para conceder permisos y simplificar reglas se necesita la agrupación de redes para una mejor administración. A continuación en la figura 22 se muestra un ejemplo de agrupación de redes.

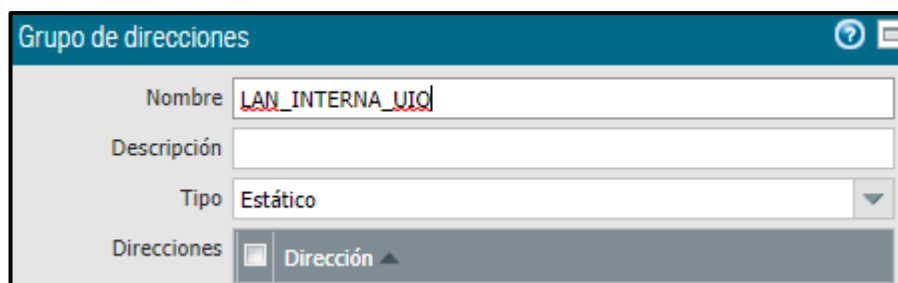


Figura 22. Agrupación de objetos de redes

Fuente: Elaborado por el autor

4.5.3 Servicios TCP/IP

De igual forma se necesita agrupar servicios y puertos usados para la comunicación eficaz de usuarios y equipos servidores, navegación para servidores por lo que se procede a agrupar servicios. Se muestra en la figura 23.

<input type="checkbox"/>	Rngo_Puertos_Rastreo_Satelital		TCP	8100-8300
<input type="checkbox"/>	service-http	Predefinido	TCP	80,8080
<input type="checkbox"/>	service-https	Predefinido	TCP	443

Figura 23. Agrupación de servicios

Fuente: Elaborado por el autor

4.6 Creación de perfiles de navegación

Se procede a crear los perfiles de navegación, *antivirus*, IPS (Sistema de prevención de intrusos), para el control de la navegación del edificio El Telégrafo y coordinaciones zonales. Este perfilamiento se lo realiza según la necesidad de cada dirección y coordinación, y siguiendo las recomendaciones descritas en el EGSi para protección y buen uso del INTERNET.

4.6.1 Navegación gerencial

En este perfil tiene un nivel de privilegio como *streaming*, *youtube*, redes sociales, correos externos, etc. De acuerdo a solicitud y autorización del oficial de seguridad de a institución se aplica este tipo de privilegios. A continuación en la figura 24 se muestra la regla por la de permisos gerenciales.

<input type="checkbox"/>	NAV_GERENCIAL_COMUNICACION	*.unbouncepages.c...	block	*.freepik.com *.freepik.es www.freepik.com/ freepik.cdnpk.net/ img.freepik.com/ trk.freepik.com/ stats.g.doubleclick.net/ más...	Allow Categories (0) Alert Categories (36) Continue Categories (0) Block Categories (31) Override Categories (0)	Allow Categories (21) Alert Categories (13)
--------------------------	----------------------------	----------------------	-------	---	--	--

Figura 24. Perfil de navegación gerencial

Fuente: Elaborado por el autor

4.6.2 Navegación básica

Este perfil es restringido, contiene accesos solo a páginas gubernamentales e investigación para el desempeño normal de los funcionarios internos. En la figura 25 se muestra la regla de perfil básico.

<input type="checkbox"/> NAVEGACION BASICA		block	*.google.com www.flickr.com/ *.carsync.com/ *.github.com/ 181.211.103.214/registroSanitario... wsdl www.youtube.com/watch?v=aapEFOOcABQ&feature=youtu.be *. GoogleVideo.com/videoplayback más...	Allow Categories (0) Alert Categories (29) Continue Categories (0) Block Categories (38) Override Categories (0)	Allow Categories (0) Alert Categories (29) Continue Categories (0) Block Categories (38)
--	--	-------	--	--	---

Figura 25. Perfil de navegación básica

Fuente: Elaborado por el autor

4.6.2 Navegación básica más cursos

Este perfil contiene la navegación básica más un adicional de accesos a ciertos links de cursos recomendados por la institución. Se muestra en la figura 26.

<input type="checkbox"/> NAVEGACION_BASICA MAS CURSOS		block	www.github.com www.flickr.com/ *.carsync.com/ *.googlevideo.com/ *.courses.edx.org www.youtube.com/watch?v=aapEFOOcABQ&feature=youtu.be *. GoogleVideo.com/videoplayback más...	Allow Categories (0) Alert Categories (29) Continue Categories (0) Block Categories (38) Override Categories (0)	Allow Categories (21) Alert Categories (8)
---	--	-------	--	--	---

Figura 26. Perfil de navegación básica más cursos

Fuente: Elaborado por el autor

4.6.3 Navegación básica más redes sociales

Este perfil contiene los permisos básicos más un adicional de navegación y acceso a redes sociales específicamente. Se muestra en la figura 27.

<input type="checkbox"/> NAVEGACION_BASICA_MAS_FACE_TWIT		block	www.github.com www.flickr.com/ *.facebook.com *.twitter.com	Allow Categories (0) Alert Categories (30) Continue Categories (0) Block Categories (37) Override Categories (0)	Allow Categories (21) Alert Categories (9)
--	--	-------	--	--	---

Figura 27. Perfil de navegación básica más redes sociales

Fuente: Elaborado por el autor

4.7 Creación grupo de aplicaciones

Se procede a crear un grupo de aplicaciones por cada perfil de navegación. Se muestra en la figura 28.

<input type="checkbox"/> NAV_BASICA		11	google-analytics google-base google-maps google-translate flickr web-browsing ssl más...
-------------------------------------	--	----	---

Figura 28. Agrupación de aplicaciones para perfil navegación básica

Fuente: Elaborado por el autor

Se agregan las aplicaciones más comunes usadas dentro del tiempo de monitoreo y bajo el perfil de navegación obtenido del *Check Point*. Se muestra en la figura 29.

<input type="checkbox"/> Aplicaciones
<input type="checkbox"/> google-analytics
<input type="checkbox"/> google-base
<input type="checkbox"/> google-maps
<input type="checkbox"/> google-translate
<input type="checkbox"/> flickr
<input type="checkbox"/> web-browsing
<input type="checkbox"/> ssl
<input type="checkbox"/> trello
<input type="checkbox"/> google-docs-base

Figura 29. Aplicaciones de perfil de navegación básica

Fuente: Elaborado por el autor

Estos pasos se siguen con los demás perfiles de navegación agrupando las aplicaciones y asignando a cada uno de los anteriormente creados, como se muestra en la figura 30.

<input type="checkbox"/> NAV_BASICA_FACEBOOK		12	<ul style="list-style-type: none"> google-analytics google-base google-maps google-translate flickr web-browsing ssl más...
<input type="checkbox"/> NAV_TECNOLOGIA		27	<ul style="list-style-type: none"> google-analytics google-base google-maps google-translate flickr web-browsing ssl más...
<input type="checkbox"/> NAV_BASICA_CURSOS		12	<ul style="list-style-type: none"> google-analytics google-base google-maps google-translate flickr web-browsing

Figura 30. Aplicaciones de perfil de navegación básica

Fuente: Elaborado por el autor

4.8 Configuración de reglas NAT

Toda la red interna necesita navegación hacia Internet por lo que para protección de la red interna, se procede a configurar las reglas de NAT para navegación de la red SERCOP. Todos navegan por las IP pública 181.113.X.187. En la figura 31 se muestra la regla de NAT configurada.


Nombre	Paquete original			Paquete traducido		
	Zona de origen	Zona de destino	Dirección de destino	Traducción de origen	Traducción de destino	
SALIDA_INTERNET	<ul style="list-style-type: none">  DATOS_SERCOP_TELEGRAFO  DMZ_2_TELEGRAFO  INVITADOS_TELEGRAFO  RED_TELEGRAFO 	 INTERNET_TELEGRAFO	any	any	<ul style="list-style-type: none"> dynamic-ip-and-port ethernet1/1 181.113.19.187/29 	ninguno

Figura 31. Configuración de regla NAT

Fuente: Elaborado por el autor

Se procede a configurar la publicación de servicios web por https y http como se muestra en la figura 32.

Nombre	Paquete original				Paquete traducido	
	Zona de origen	Zona de destino	Dirección de destino	Servicio	Traducción de origen	Traducción de destino
5 Publicacion_WebChat	INTERNET_TELEGRAFO	INTERNET_TELEGRAFO	EXT_181.113.19.186	service-https	none	destination-translation dirección: 172.16.4.43 puerto: 443

Figura 32. Configuración de regla NAT para publicación de servicios

Fuente: Elaborado por el autor

4.9 Configuración de políticas de seguridad

Se procede a crear las políticas de seguridad de acceso a navegación de la red SERCOP. Los perfiles de navegación se manejan por jerarquías y se debe posicionar en orden los grupos con las respectivas excepciones de navegación.

4.9.1 Permisos de navegación gerencial

Se concede a las personas que están dentro del Nivel Jerárquico Superior, en esta categoría tienen navegación libre. Ya sea a streaming, correos externos, redes sociales, etc. Se añade como origen las IP de los equipos que requieren de estos permisos, como se muestra en la figura 33.

Nombre	IP Origen		IP Destino		Aplicación	Servicio
	Zona	Dirección	Zona	Dirección		
35 NAV_GERENCIAL	DATOS_SERCOP_TELEGRAFO RED_TELEGRAFO	172.16.10.135 INFR_F.PIEDRA_172.16.20.21 INFR_V.PONCE_172.16.20.206 INFR_V.PONCE_172.16.99.207 IP_Comunicaciones_172.16.105.122 Net_Alban_Comunicacion_Social_172.16.107.0 NET_UIO_ASESORES_172.16.22.0 más...	INTERNET_TELEGRAFO	any	any	application-default

Figura 33. Regla de seguridad navegación gerencial

Fuente: Elaborado por el autor

4.9.2 Permisos de navegación básica

Se concede a las personas que están dentro de las áreas administrativas, jurídicas, bienes, catálogo es decir todos los servidores. En esta categoría solo tienen acceso a páginas de carácter básico por ejemplo no tienen acceso a youtube, redes sociales correos externos, etc.

En cada política de seguridad según los permisos, se aplica el perfil de navegación correspondiente. Como se muestra en la figura 34.

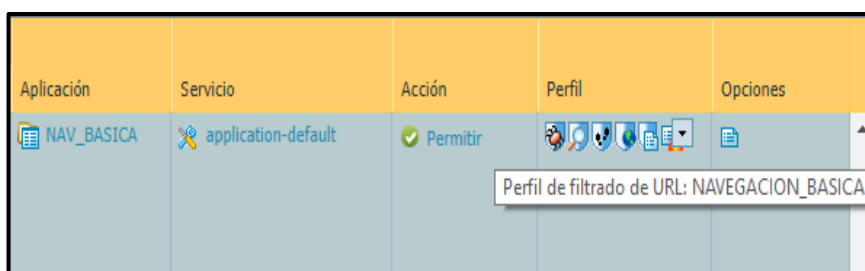


Figura 34. Aplicación de Perfil en Regla de Seguridad Navegación Básica

Fuente: Elaborado por el autor

4.9.13 Permisos de navegación de la red de invitados

Esta regla es creada por seguridad y protección de infecciones que puedan ingresar usuarios que necesitan conectarse a la red cuando están de visita en la institución pueden ser proveedores o ciudadanía, se les asigna una ip dentro de la red aislada con permisos con nivel básico solo a páginas del SERCOP exclusivamente. Como se muestra en la figura 35.

Nombre	IP Origen		IP Destino		Aplicación	Servicio
	Zona	Dirección	Zona	Dirección		
32 NAV_INVITADOS	INVITADOS_TELEGRAFO	NET_10.249.10.0	INTERNET_TELEGRAFO	any	google-base ocsp ssl web-browsing	application-default
	RED_TELEGRAFO	NET_UIO_GUEST_172.16.3.0				

Figura 35. Regla de seguridad de navegación de la red de invitados

Fuente: Elaborado por el autor

Se aplica el perfil de navegación correspondiente. Como se muestra en la figura 36.

Aplicación	Servicio	Acción	Perfil	Opciones
<ul style="list-style-type: none"> google-base ocsp ssl web-browsing 	application-default	Permitir	<div style="border: 1px solid gray; padding: 2px;"> Grupo de perfiles: NAV_INVITADOS </div>	

Figura 36. Aplicación del perfil en la regla de seguridad de navegación de invitados

Fuente: Elaborado por el autor

4.10 Permisos de acceso entre redes LAN

Se procede a crear la política de comunicación entre las redes LAN, datos, DC_CNT, anillo interministerial. Como se muestra en la figura 37.

	Nombre	IP Origen		IP Destino		Aplicación	Servicio
		Zona	Dirección	Zona	Dirección		
40	REDES_INTERNAS	<ul style="list-style-type: none"> DATOS_SERCOP_TELEGRAFO DMZ_2_TELEGRAFO RED_TELEGRAFO VPN 	any	<ul style="list-style-type: none"> DATOS_SERCOP_TELEGRAFO DMZ_2_TELEGRAFO INVITADOS_TELEGRAFO RED_TELEGRAFO VPN 	any	any	any

Figura 37. Regla de seguridad para navegación básica

Fuente: Elaborado por el autor

No se aplica ningún perfil de navegación debido a que no se cuenta con un listado de aplicaciones, puertos y protocolos a denegar o permitir, entre redes internas.

4.11 Permisos de comunicación red VPN

Se procede a crear la política de acceso de la red VPN hacia las redes de SERCOP. Como se muestra en la figura 38.

	Nombre	IP Origen		IP Destino		Aplicación	Servicio
		Zona	Dirección	Zona	Dirección		
20	Acceso_VPN_Cliente	INTERNET_TELEGRAFO	any	INTERNET_TELEGRAFO	any	any	any
21	Vpn_to_INTERNET	VPN	any	INTERNET_TELEGRAFO	any	any	any
22	Vpn_to_RED_SERCOP	VPN	any	DATOS_SERCOP_TELEGRAFO DMZ_2_TELEGRAFO RED_TELEGRAFO	any	any	any

Figura 38. Comunicación de red VPN

Fuente: Elaborado por el autor

4.12 Permisos de conexión remota

Se procede a crear una política de acceso para aplicaciones de acceso remoto, Anydesk, Logmein, etc. Como se muestra en la figura 39.

	Nombre	IP Origen		IP Destino		Aplicación	Servicio	Acción
		Zona	Dirección	Zona	Dirección			
27	Permitido AnyDesk	RED_TELEGRAFO	PC_PRUEBAS_172.16.254.130	INTERNET_TELEGRAFO	any	any	application-default	Permitir

Figura 39. Regla de acceso remoto

Fuente: Elaborado por el autor

Se procede a crear una política de bloqueo para todas las App de acceso remoto que se excluirán del permiso, dentro de un filtro de aplicaciones definido. Como se muestra en la figura 40.

	Nombre	IP Origen		IP Destino		Aplicación	Servicio	Acción
		Zona	Dirección	Zona	Dirección			
28	Bloqueo Escritorio_remoto	any	any	INTERNET_TELEGRAFO	any	GRUPO_REMO...	any	Denegar

Figura 40. Regla de seguridad para navegación básica

Fuente: Elaborado por el autor

En la figura 41 se muestra como crear el perfil de aplicaciones para acceso remoto.

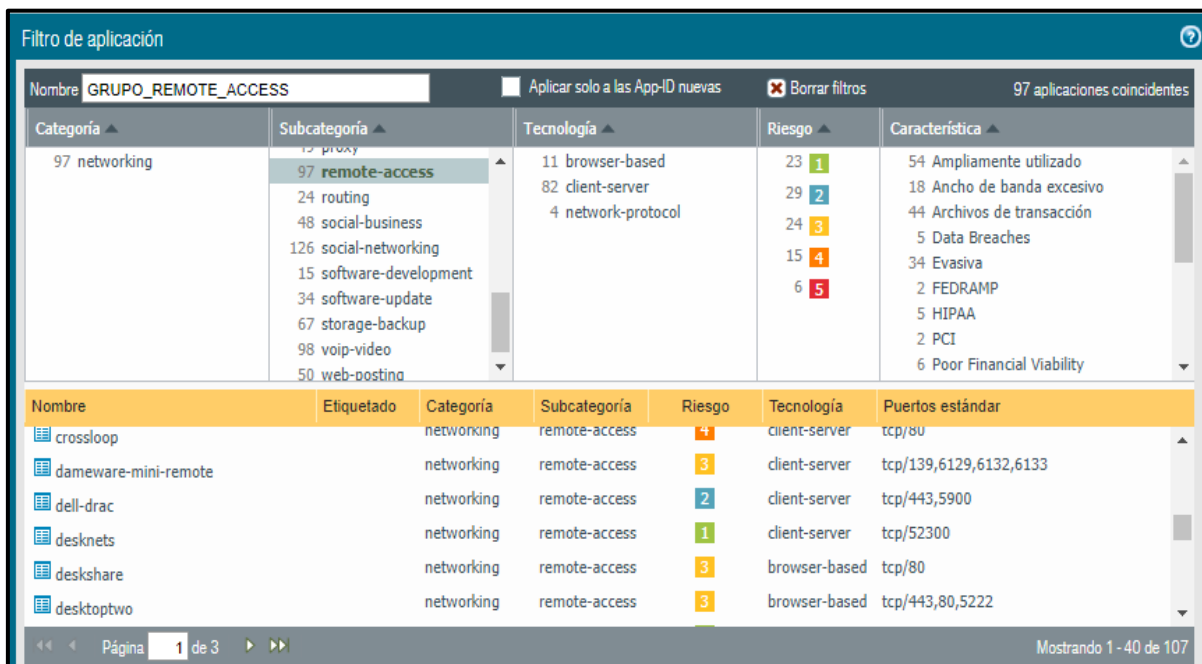


Figura 41. Aplicación del perfil aplicaciones acceso remoto

Fuente: Elaborado por el autor

4.13 Permiso para actualizaciones antivirus

Se crea la política para que el servidor de antivirus sea el único quien se actualice al Internet, para así garantizar el ancho de banda. Como se muestra en la figura 42.

Nombre	IP Origen		IP Destino		Aplicación
	Zona	Dirección	Zona	Dirección	
15 Update_ServerEset	any	UTO_SRV_ESET_172.16.0.220	INTERNET_TELEGRAFO	GRP_ESET_UPDATES	any

Figura 42. Regla de actualizaciones antivirus

Fuente: Elaborado por el autor

La salida hacia actualizaciones son configuradas al grupo de IP de ESET publicadas por el fabricante. Se crea la política permitiendo la sincronización con el servidor de actualizaciones antivirus ESET en la red local. Se muestra en la figura 43.

Nombre	IP Origen		IP Destino	
	Zona	Dirección	Zona	Dirección
16 Update_LAN_to_Eset	DATOS_SERCOP... RED_TELEGRAFO	any	DMZ_2_TELEGRAFO	UIO_SRV_ESET_172.16.0.220

Figura 43. Regla de sincronización antivirus con red local

Fuente: Elaborado por el autor

4.14 Bloqueos de actualizaciones UPDATE

Se procede a bloquear todas las actualizaciones hacia el Internet para optimizar ancho de banda consumida por actualizaciones como Windows Update. Se muestra en la figura 44.

Aplicación	Servicio	Acción	Perfil
GRUPO_UPDATES	any	Denegar	none

Figura 44. Bloqueo grupo de aplicaciones UPDATE

Fuente: Elaborado por el autor

El perfil de aplicaciones UPDATES creado anteriormente es aplicado a la política de seguridad creada para no permitir actualizaciones. Se muestra en la figura 45.

Filtro de aplicación

Nombre: GRUPO_UPDATES Aplicar solo a las App-ID nuevas Borrar filtros 34 aplicaciones coincidentes

Categoría	Subcategoría	Tecnología	Riesgo	Característica
34 business-systems	38 database 45 erp-crm 179 general-business 366 management 11 marketing 69 office-programs 15 software-development 34 software-update 67 storage-backup	3 browser-based 31 client-server	18 1 7 2 8 3 1 4	19 Ampliamente utilizado 4 Ancho de banda excesivo 8 Archivos de transacción 9 Evasiva 2 Tuneliza otras aplicaciones 21 Vulnerabilidades

Nombre	Etiquetado	Categoría	Subcategoría	Riesgo	Tecnología	Puertos estándar
360-safeguard-update		business-systems	software-update	2	client-server	80,8090,dynamic,tcp,udp
adobe-update		business-systems	software-update	2	client-server	443,80,tcp
apple-update		business-systems	software-update	3	client-server	443,80,tcp
avast-av-update		business-systems	software-update	1	client-server	443,80,tcp
avg-update		business-systems	software-update	1	client-server	80,tcp
avira-antivir-update		business-systems	software-update	2	client-server	443,80,tcp

Mostrando 1 - 34 de 34

Figura 45. Grupo de aplicaciones UPDATE

Fuente: Elaborado por el autor

4.15 Permiso de acceso red invitados

La red de invitados es completamente restrictiva y aislada, por lo cual cuando un proveedor necesita acceder a los servidores o red interna, se permite bajo un estricto control y mediante formulario que tiene las firmas de autorización con el proceso respectivo. Se procede a crear la política de seguridad que da acceso a un proveedor desde la red de invitados hacia los servidores de DC_CNT. Se muestra en la figura 46.

	Nombre	IP Origen		IP Destino	
		Zona	Dirección	Zona	Dirección
10	Acceso BalticContron_SOCE_Desa	RED_TELEGRAFO	172.16.3.100 172.16.3.102	DATOS_SERCOP_TELEGRAFO	DC_PS_SOCE2_192.168.9.196 DC_PS_SOCE3_192.168.9.197

Figura 46. Regla de acceso red invitados

Fuente: Elaborado por el autor captura de configuración en equipo PAN

Se concede el acceso solo por las aplicaciones necesarias y específicas. Se muestra en la figura 47.

Aplicación	Servicio	Acción	Perfil	Opciones
soap ssl web-browsing	application-default	Permitir	none	

Figura 47. Regla de acceso aplicaciones específicas

Fuente: Elaborado por el autor

Se procede a crear una política que bloquee el acceso de toda la red invitados hacia el Data Center CNT. Se muestra en la figura 48.

	Nombre	IP Origen		IP Destino	
		Zona	Dirección	Zona	Dirección
13	Bloqueo Red 172.16.3.0 Invitados	RED_TELEGRAFO	NET_UIO_GUEST_172.16.3.0	DATOS_SERCOP_TELEGRAFO	any
14	Bloqueo Red Invitados	any	NET_10.249.10.0	DATOS_SERCOP_TELEGRAFO DMZ_2_TELEGRAFO RED_TELEGRAFO	NAT_CLOUD_TECLCONET NET_DC_192.168.9.0 NET_DC_192.168.100.0 NET_DC_PREPRODUCCION_192.168.140.0 NET_DC_PRODUCION_192.168.120.0 NET_DC_PRUEBAS_192.168.150.0 NET_DC_PRUEBAS_SEGURIDAD_192.168.130.0 más...

Figura 48. Regla de bloqueo red invitados a el DC CNT

Fuente: Elaborado por el autor

Se bloquea el acceso de todas las aplicaciones por defecto. Se muestra en la figura 49.

Aplicación	Servicio	Acción	Perfil	Opciones
any	any	Denegar	none	
any	any	Descartar	none	

Figura 49. Regla de bloqueo total aplicaciones

Fuente: Elaborado por el autor

4.16 Permiso de acceso sin restricción

Se procede a configurar la política para los host con permiso libre hacia el Internet, Este tipo de permisos se concede con el control respectivo mediante formulario. Usado principalmente por el administrador de la herramienta PAN. Se muestra en la figura 50.

	Nombre	IP Origen		IP Destino	
		Zona	Dirección	Zona	Dirección
20	NAV_SIN_RESTRICCION	RED_TELEGRAFO	172.16.20.227 172.16.254.130 INFR_O.ANDRADE_172.16.20.19 INFRA_I.BELALCAZAR_172.16.20.209 INFRA_I.BELALCAZAR_172.16.99.216 INFRA_O.ANDRADE_172.16.99.102 Oper_V.Aumala_172.16.99.103	any	any

Figura 50. Regla de navegación sin restricción

Fuente: Elaborado por el autor

Por motivos de implementación, pruebas y ejecución de reglas se permite la navegación hacia el Internet permitiendo todas las aplicaciones, bajo las autorizaciones con el formulario respectivo. Se muestra en la figura 51.

Aplicación	Servicio	Acción	Perfil	Opciones
any	 application-default	 Permitir	 Grupo de perfiles: NAV_SIN_RESTRICCIONES	

Figura 51. Regla de permisos aplicaciones libres

Fuente: Elaborado por el autor

4.17 Bloqueo por defecto

Se procede a crear una política implícita para bloquear cualquier acceso no permitido, a partir de esta se irá dando permisos según la necesidad y solicitudes respectivas. Se muestra en la figura 52.



	Nombre	IP Origen		IP Destino		Aplicación	Servicio	Acción	Perfil	Opciones
		Zona	Dirección	Zona	Dirección					
82	IMPLICITA	any	any	any	any	any	any	 Denegar	none	

Figura 52. Regla implícita de bloqueo

Fuente: Elaborado por el autor

4.18 Configuración VPN

Se procede a configurar el acceso remoto mediante VPN hacia la Red LAN del SERCOP, para esto se crea el certificado que utilizará la conexión VPN. La conexión creada es a través de un túnel cifrado seguro. A continuación se muestra en la figura 53 el certificado que se usará para las conexiones remotas.

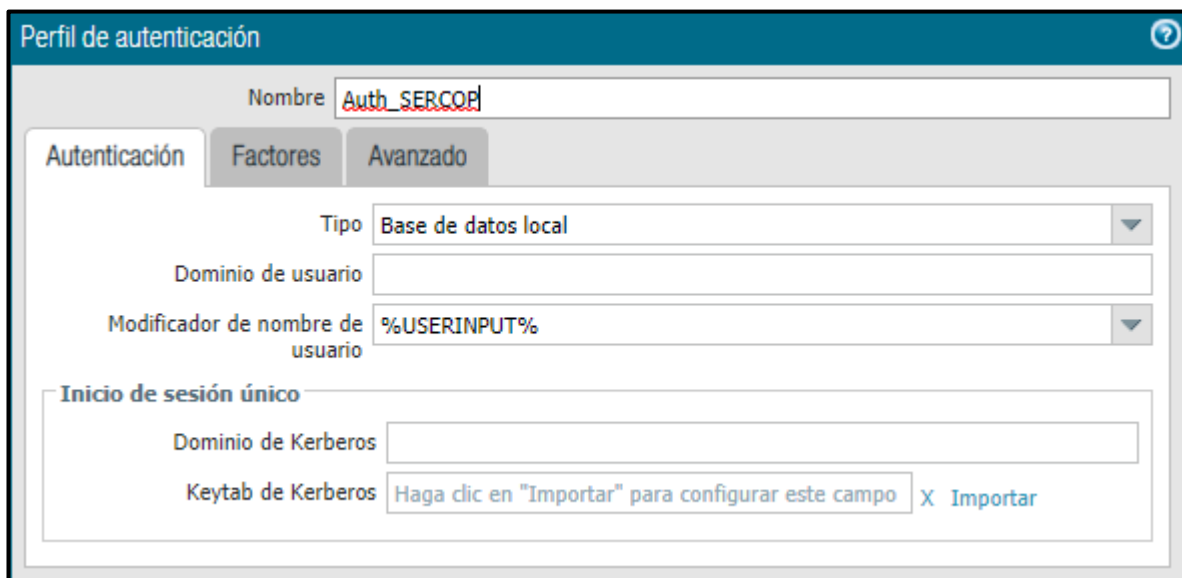


Nombre	vpn_sercop
Asunto	/CN=181.113.19.187
Emisor	/CN=181.113.19.187
No es válido antes de	Nov 7 16:33:05 2018 GMT
No es válido después de	Aug 3 16:33:05 2021 GMT
Algoritmo	RSA
<input checked="" type="checkbox"/>	Autoridad del certificado
<input type="checkbox"/>	Reenviar certificado fiable
<input type="checkbox"/>	Reenviar certificado no fiable
<input type="checkbox"/>	CA raíz de confianza

Figura 53. Configuración de certificado VPN

Fuente: Elaborado por el autor

Se procede a crear el perfil de autenticación para el servicio de VPN, se configura con una base de datos local. Se muestra en la figura 54.

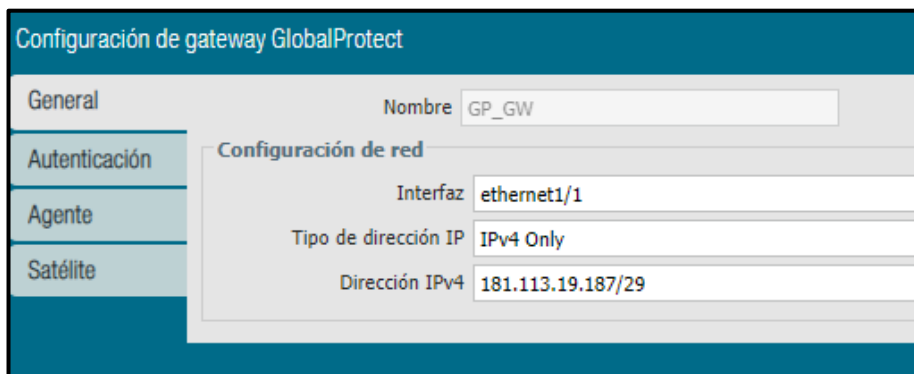


Nombre	Auth_SERCOP
Tipo	Base de datos local
Dominio de usuario	
Modificador de nombre de usuario	%USERINPUT%
Inicio de sesión único	
Dominio de Kerberos	
Keytab de Kerberos	Haga clic en "Importar" para configurar este campo X Importar

Figura 54. Configuración del perfil de autenticación

Fuente: Elaborado por el autor

Se configura el Gateway para la VPN, y se asigna la dirección IP pública como se muestra en la Figura 55.



The screenshot shows the 'Configuración de gateway GlobalProtect' interface. On the left, there is a sidebar with tabs: 'General', 'Autenticación', 'Agente', and 'Satélite'. The 'General' tab is selected. The main area is titled 'Configuración de red' and contains the following fields:

Nombre	GP_GW
Interfaz	ethernet1/1
Tipo de dirección IP	IPv4 Only
Dirección IPv4	181.113.19.187/29

Figura 55. Configuración del gateway VPN

Fuente: Elaborado por el autor

A continuación se configura la autenticación para el Gateway VPN. Se muestra en la figura 56.



The screenshot shows the 'Autenticación de cliente' interface. It contains the following fields:

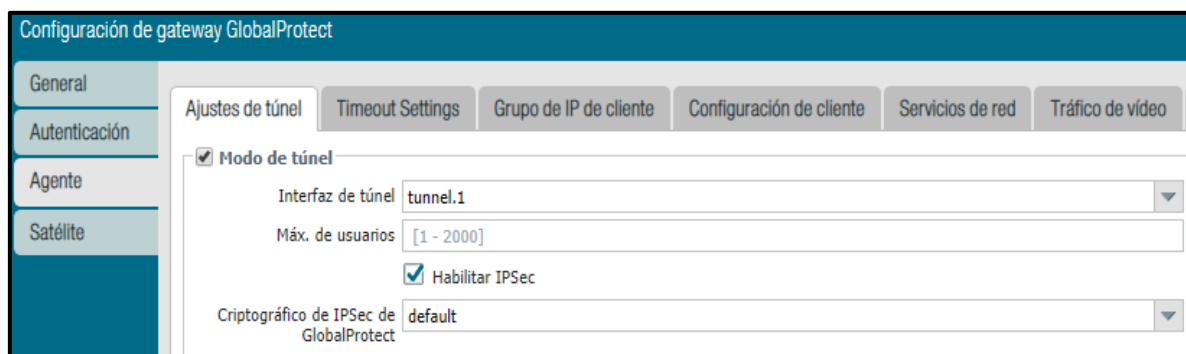
Nombre	GP_GW
SO	Any
Perfil de autenticación	Auth_SERCOP
Pantalla de inicio de sesión de la aplicación GlobalProtect	
Etiqueta de nombre de usuario	Username
Etiqueta de contraseña	Password
Mensaje de autenticación	Enter login credentials

El mensaje de autenticación puede tener un máximo de 256

Figura 56. Configuración autenticación gateway VPN

Fuente: Elaborado por el autor

Se configura la interfaz de escucha para las conexiones VPN. La red que utilizará el servicio de VPN es 10.X.X.0/24. Se muestra en la figura 57.



The screenshot shows the 'Configuración de gateway GlobalProtect' interface with the 'Ajustes de túnel' tab selected. The sidebar on the left has tabs: 'General', 'Autenticación', 'Agente', and 'Satélite'. The main area contains the following fields:

<input checked="" type="checkbox"/> Modo de túnel	
Interfaz de túnel	tunnel.1
Máx. de usuarios	[1 - 2000]
<input checked="" type="checkbox"/> Habilitar IPSec	
Criptográfico de IPSec de GlobalProtect	default

Figura 57. Configuración de la interfaz VPN

Fuente: Elaborado por el autor

4.18.1 Configuración rutas de acceso VPN

A continuación se crea las rutas de acceso VPN hacia la red El Telégrafo, DC_CNT y las redes de Coordinaciones Zonales. Se muestra en la figura 58.



Configuraciones	Usuario/grupo de usuarios	SO	Grupo de IP	Incluir ruta de acceso
<input checked="" type="checkbox"/>	GP	any		0.0.0.0/0 10.0.0.0/8 172.0.0.0/8 192.0.0.0/8

Figura 58. Configuración rutas de acceso VPN

Fuente: Elaborado por el autor

Por último se configura el portal de VPN con la IP pública 181.113.19.187. Se muestra en la figura 59.



Configuración de portal de GlobalProtect

General

Nombre: Portal_GP_VPN

Autenticación

Agente

VPN sin cliente

Configuración de red

Interfaz: ethernet1/1

Tipo de dirección IP: IPv4 Only

Dirección IPv4: 181.113.19.187/29

Figura 59. Configuración del portal VPN

Fuente: Elaborado por el autor

4.18.2 Configuración de usuarios VPN

Una vez creados los recursos necesarios se proceden a crear los usuarios locales para el servicio VPN, una vez presentados las solicitudes mediante formulario y autorizaciones respectivas. Por confidencialidad no se presenta los usuarios creados.

Se procede a crear grupos de usuarios por direcciones para una mejor administración. Se muestra en la figura 60.

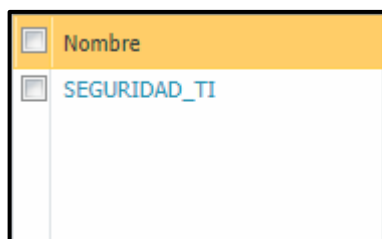


Figura 60. Grupos de usuarios VPN

Fuente: Elaborado por el autor

4.18.2 Configuración de Acceso VPN para Linux

Dentro de los equipos que se usan para el desarrollo de soluciones existe un 10 % de que tienen sistema operativo Linux por lo que se configura el Acceso VPN para equipos Linux, para este propósito se crea un grupo en cual se encerraran los equipos para su protocolo de conexión. Se muestra en la figura 61.

Group name: **linuxVpn**
Group password: **XXXXXXXX**

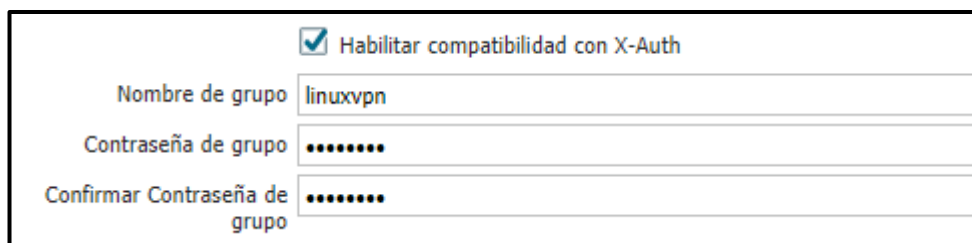
A screenshot of a VPN configuration form. At the top, there is a checked checkbox labeled 'Habilitar compatibilidad con X-Auth'. Below this, there are three input fields: 'Nombre de grupo' containing the text 'linuxvpn', 'Contraseña de grupo' with masked characters (dots), and 'Confirmar Contraseña de grupo' also with masked characters.

Figura 61. Configuración VPN linux

Fuente: Elaborado por el autor

4.19 Instalación física de los equipos

Una vez que los equipos cuentan con las configuraciones base se procede a instalar físicamente los equipos en los espacios designados por el personal que administra el centro de datos del Edificio El Telégrafo.

Los equipos se colocarán dentro del rack de servidores conectando al Switch de Core por medio de *patchcords* certificados CAT 6 como se muestra en la topología de la figura 62.



Figura 62. Colocación equipo *gateway* 1 y equipo *gateway* 2 en el DC El Telégrafo

Fuente: Elaborado por el autor

A continuación se muestra en la figura 63, la colocación de los equipos dentro del Data Center El Telégrafo, dos equipos servidores para *security gateway* y un equipo panorama de administración y reporte.

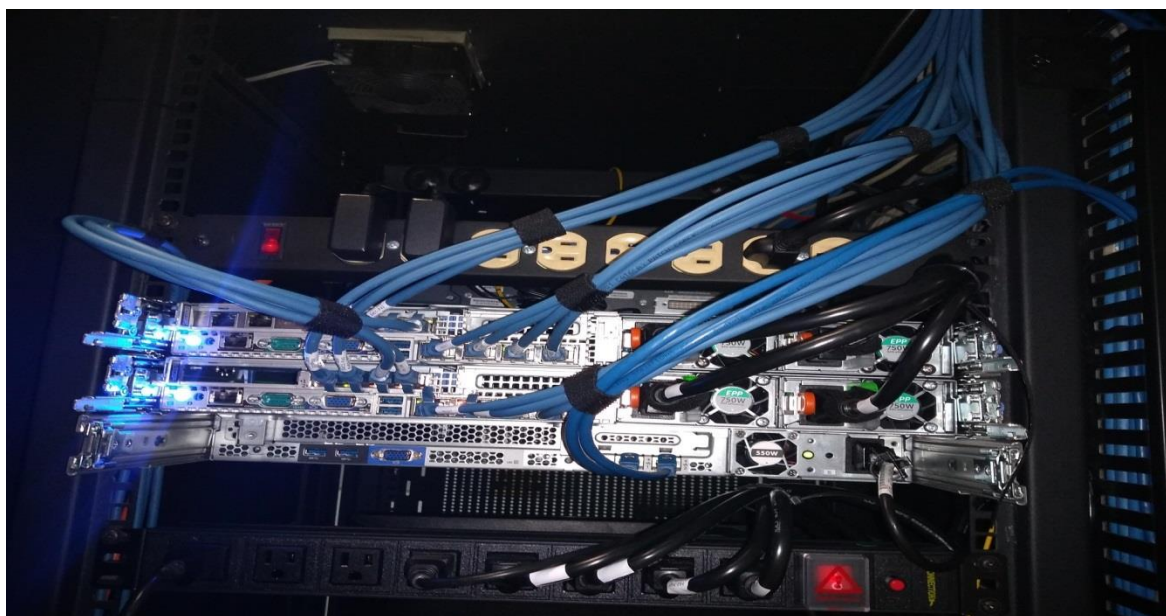


Figura 63. Cableado de equipo *gateway* 1, equipo *gateway* 2 y reporteador en el DC El Telégrafo

Fuente: Elaborado por el autor

A continuación en la figura 64 se presenta una descripción de la topología de conexiones realizada en el data center del edificio El Telégrafo.

TOPOLOGIA DE CONEXIONES FIREWALL EL TELÉGRAFO

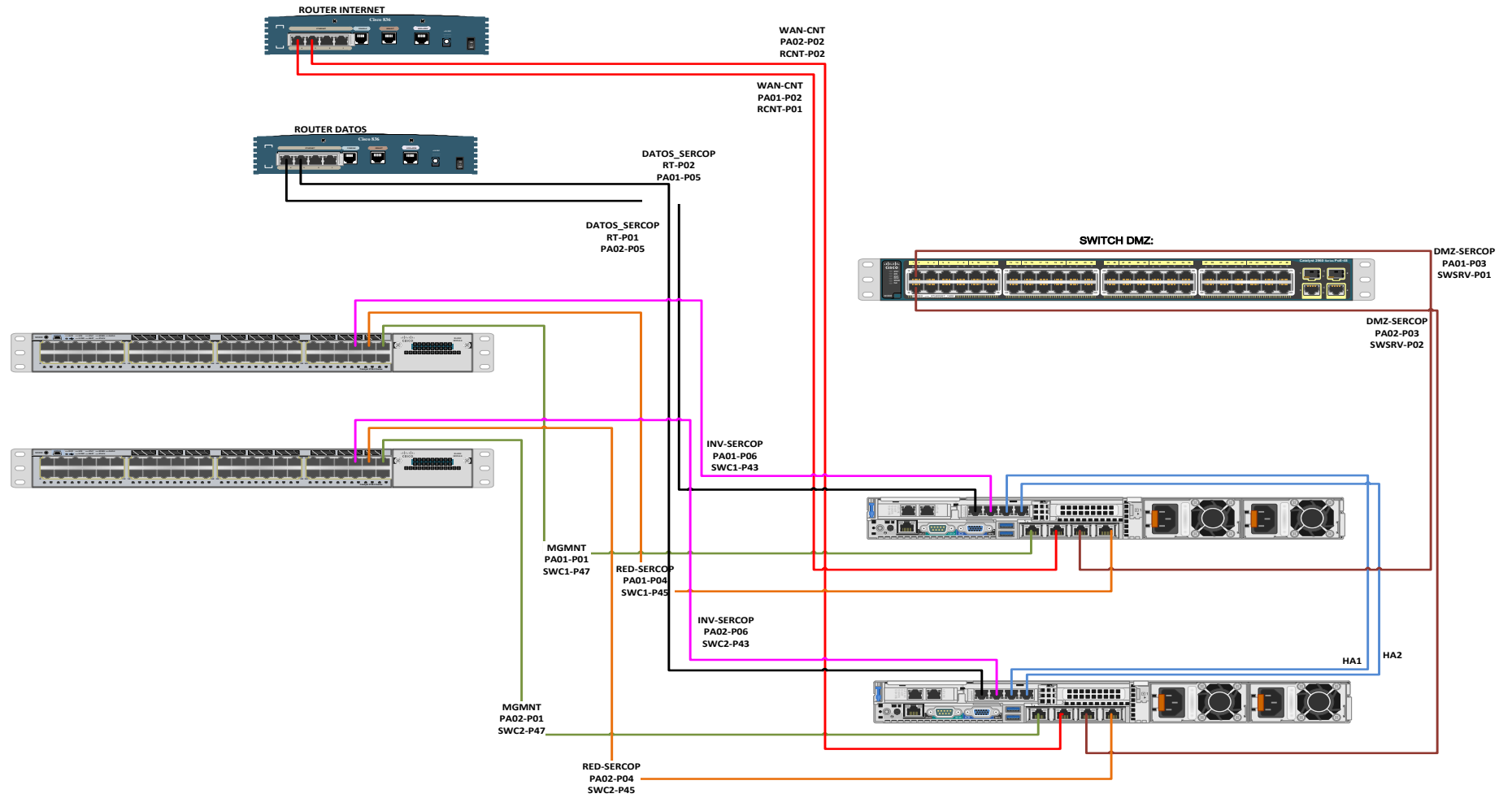


Figura 64. Topología de conexiones equipos firewall y administración en DC El Telégrafo

Fuente: Elaborado por el autor

4.20 Configuración del firewall del Data Center CNT

Una vez realizada las configuraciones de la red en el equipo Palo Alto se procede a realizar la creación de objetos, reglas, perfiles de seguridad, VPN, usuarios, etc.

En estos equipos se encuentra toda la configuración de protección, pruebas, producción y publicación de los servicios que brinda la institución a la ciudadanía.

4.20.1 Configuración de interfaces de red

4.20.2. Anillo interministerial

La configuración del anillo interministerial es fundamental ya que es un cumplimiento del esquema gubernamental de seguridad de la información, por medio del anillo se realiza el consumo de WEB *services* entre instituciones del estado como SRI, Registro Civil, Aduana, etc. Se muestra en la figura 65.

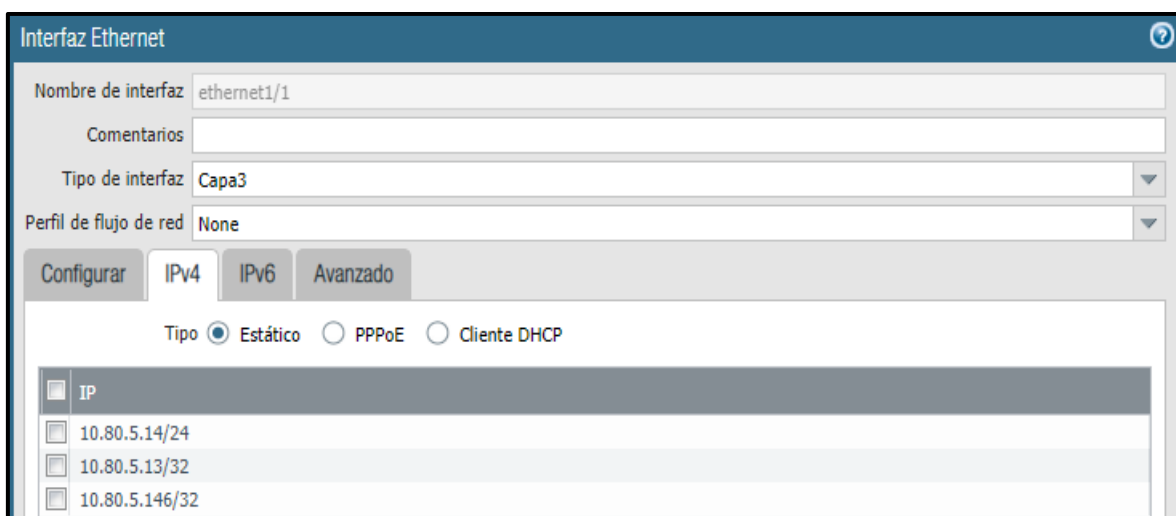


Figura 65. Configuración de la interfaz anillo interministerial

Fuente: Elaborado por el autor

4.20.2 TELCONET

Como habíamos mencionado anteriormente la institución funciona con dos ISP (Proveedor de servicio de internet) para tener alta disponibilidad en caso de que se presenten problemas, en este sentido son CNT como principal y TELCONET como secundaria o backup para siempre garantizar la disponibilidad de los servicios. Se muestra en la figura 66.

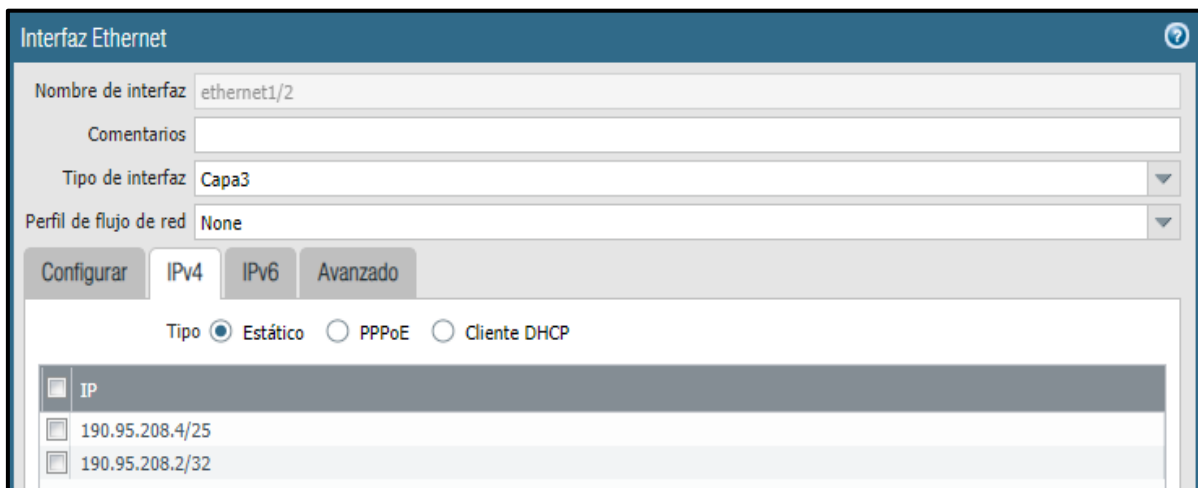


Figura 66. Configuración de la interfaz ISP TELCONET

Fuente: Elaborado por el autor

4.20.3 CNT

CNT trabaja como ISP principal para Internet y datos, brindando servicio y soporte 24/7 ante cualquier eventualidad. Como habíamos mencionado antes tenemos contratado dos pools de IP públicas para todos los servicios. En la Figura 67 y 68 se muestra la configuración de las interfaces de red.

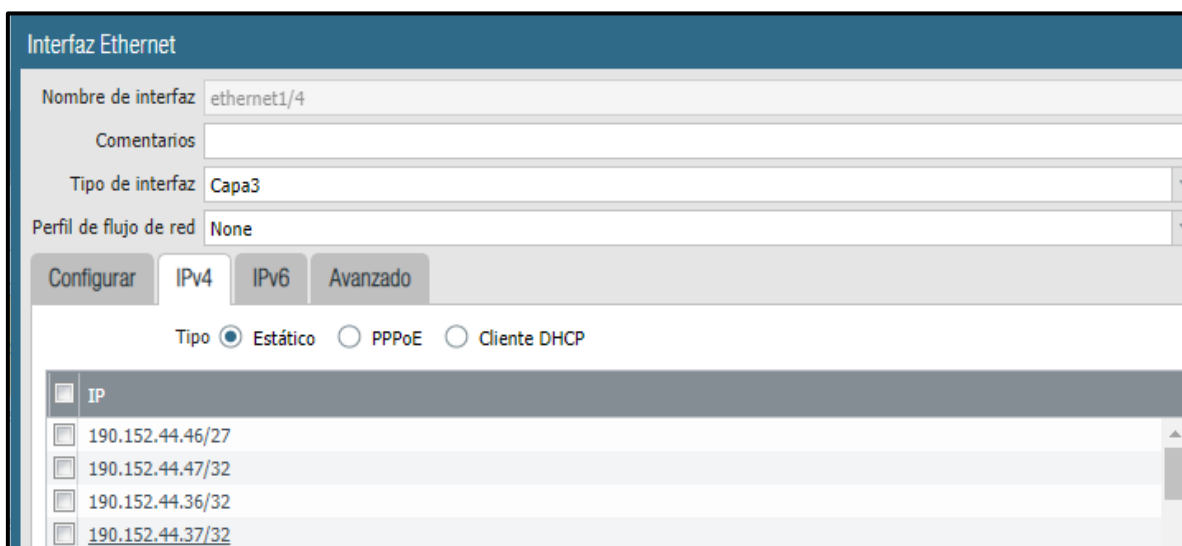


Figura 67. Configuración de la interfaz Pool 1 CNT

Fuente: Elaborado por el autor



Figura 68. Configuración de la interfaz Pool 1 CNT

Fuente: Elaborado por el autor

4.20.4 Datos

A continuación se muestra la configuración de la interfaz de datos. Se muestra en la figura 69.

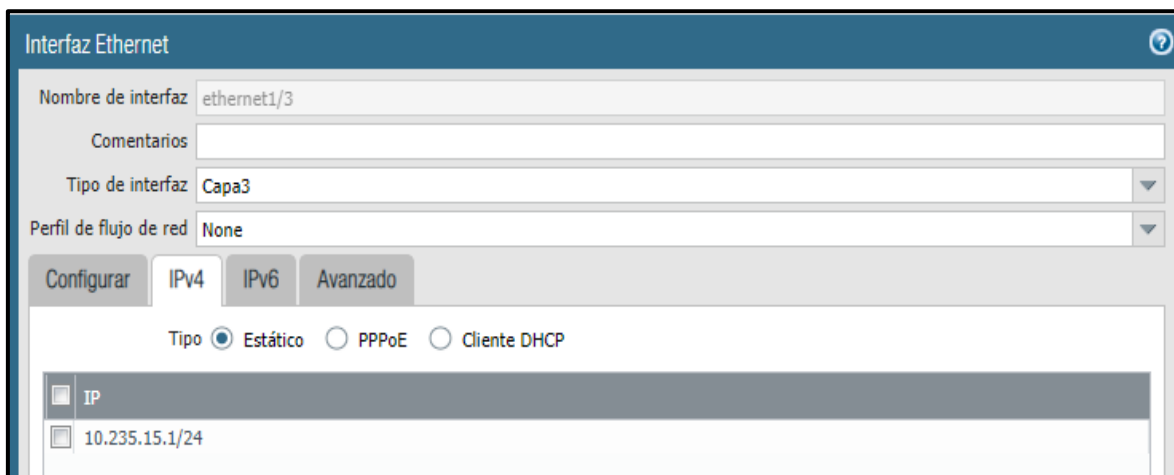


Figura 69. Configuración de la interfaz de datos

Fuente: Elaborado por el autor

4.20.5 Red LAN CNT

Continuando con la configuración de las interfaces en la figura 70 se muestra la configuración de la interfaz de Red LAN CNT.

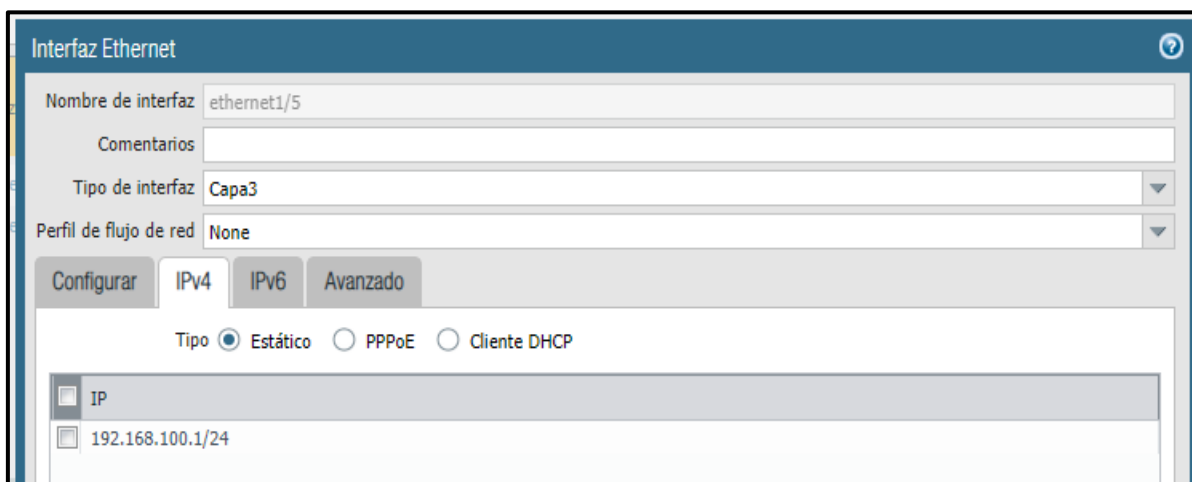


Figura 70. Configuración de la red LAN CNT

Fuente: Elaborado por el autor

4.20.6 Zonas de seguridad

Palo Alto Network trabaja con zonas de seguridad para protección de las redes y servidores, por lo que se crea y configura las zonas de seguridad, solo estas zonas tendrán comunicación según las necesidades y solicitudes respectivas. Se muestra en la figura 71.

<input type="checkbox"/>	Nombre	Tipo	Interfaces / sistemas virtuales	Perfil de protección de zona	Protección de búfer de paquetes	Ajuste de log	Habilitado
<input type="checkbox"/>	ANILLO_INTERMINI...	layer3	ethernet1/1		<input type="checkbox"/>		<input type="checkbox"/>
<input type="checkbox"/>	DATOS_SERCOP	layer3	ethernet1/3		<input type="checkbox"/>		<input type="checkbox"/>
<input type="checkbox"/>	ISP_CNT	layer3	ethernet1/4		<input checked="" type="checkbox"/>		<input type="checkbox"/>
<input type="checkbox"/>	ISP_CNT_POOL2	layer3	ethernet1/6		<input type="checkbox"/>		<input type="checkbox"/>
<input type="checkbox"/>	ISP_TELCONET	layer3	ethernet1/2		<input checked="" type="checkbox"/>		<input type="checkbox"/>
<input type="checkbox"/>	LAN_DC_CNT	layer3	ethernet1/5		<input type="checkbox"/>		<input type="checkbox"/>
<input type="checkbox"/>	RED_TELEGRAFO	layer3			<input type="checkbox"/>		<input type="checkbox"/>
<input type="checkbox"/>	VPN	layer3	tunnel.1		<input type="checkbox"/>		<input checked="" type="checkbox"/>
<input type="checkbox"/>	VPN_DINARDAP	layer3	tunnel.2		<input type="checkbox"/>		<input checked="" type="checkbox"/>

Figura 71. Configuración de zonas de seguridad

Fuente: Elaborado por el autor

4.20.7 Creación de Rutas

La comunicación de la red interna hacia el Data Center donde se encuentran alojados todos los servidores de pruebas y producción es muy importante por esta razón en la siguiente figura 72 se muestra dicha configuración, solo un extracto debido a políticas de confidencialidad.

Nombre	IP Destino	Interfaz	Siguiete salto		Distancia administrativa	Métrica	BFD	Tabla de enrutamiento
			Tipo	Valor				
RED_10.0.0.32	10.0.0.32/29	ethernet1/3	ip-address	10.235.15.10	default	10	None	unicast
RED_10.16.5.0	10.16.5.0/24	ethernet1/3	ip-address	10.235.15.10	default	10	None	unicast
RED_10.212.134.0	10.212.134.0/24	ethernet1/3	ip-address	10.235.15.10	default	10	None	unicast
RED_172.16.2.0	172.16.2.0/24	ethernet1/3	ip-address	10.235.15.10	default	10	None	unicast
RED_172.16.3.0	172.16.3.0/24	ethernet1/3	ip-address	10.235.15.10	default	10	None	unicast
RED_172.16.4.0	172.16.4.0/24	ethernet1/3	ip-address	10.235.15.10	default	10	None	unicast
RED_172.16.10.0	172.16.10.0/24	ethernet1/3	ip-address	10.235.15.10	default	10	None	unicast
RED_172.16.11.0	172.16.11.0/24	ethernet1/3	ip-address	10.235.15.10	default	10	None	unicast
RED_172.16.12.0	172.16.12.0/24	ethernet1/3	ip-address	10.235.15.10	default	10	None	unicast
RED_172.16.13.0	172.16.13.0/24	ethernet1/3	ip-address	10.235.15.10	default	10	None	unicast
RED_172.16.14.0	172.16.14.0/24	ethernet1/3	ip-address	10.235.15.10	default	10	None	unicast
RED_172.16.15.0	172.16.15.0/24	ethernet1/3	ip-address	10.235.15.10	default	10	None	unicast
RED_172.16.16.0	172.16.16.0/24	ethernet1/3	ip-address	10.235.15.10	default	10	None	unicast
RED_172.16.17.0	172.16.17.0/24	ethernet1/3	ip-address	10.235.15.10	default	10	None	unicast
RED_172.16.18.0	172.16.18.0/24	ethernet1/3	ip-address	10.235.15.10	default	10	None	unicast
RED_172.16.19.0	172.16.19.0/24	ethernet1/3	ip-address	10.235.15.10	default	10	None	unicast
RED_172.16.20.0	172.16.20.0/24	ethernet1/3	ip-address	10.235.15.10	default	10	None	unicast

Figura 72. Configuración de rutas

Fuente: Elaborado por el autor

4.20.8 Configuración protocolo ECMP para ISP redundantes

A continuación se muestra la configuración ECMP para proveedores de Internet redundantes. Se muestra en la figura 73.

Interfaz	Peso
ethernet1/4	50
ethernet1/2	15

Figura 73. Configuración de zonas de seguridad

Fuente: Elaborado por el autor

4.20.9 Creación de objetos

Con la referencia del equipo checkpoint se procede a crear los objetos para ser utilizados en las políticas de seguridad.

4.20.10 Servidores alojados en el Data Center CNT

A continuación se crean los objetos pertenecientes a los servidores que se encuentran alojados en el Data Center de CNT, por acuerdos de confidencialidad se muestra en la figura 74 solo un extracto de los objetos creados.

<input type="checkbox"/>	DC_NS_ULTIMUS_192.168.100.230	Máscara de red IP	192.168.100.230
<input type="checkbox"/>	DC_NS_USHAY_192.168.100.200	Máscara de red IP	192.168.100.200
<input type="checkbox"/>	DC_NS_WEBMAIL_CNT_192.168.100.220	Máscara de red IP	192.168.100.220

Figura 74. Objetos servidores del Data Center CNT

Fuente: Elaborado por el autor

A continuación se crean los objetos de IP catalogadas como atacantes durante el monitoreo diario, los mismos estaban reconocidos en el *firewall Check Point*. Se muestra en la figura 75.

Nombre	Ubicación	Tipo	Dirección
<input type="checkbox"/>	BLACK_LIST_IP_192.221.134.11	Máscara de red IP	192.221.134.11
<input type="checkbox"/>	BLOCK_IP_109.100.166.147	Máscara de red IP	109.100.166.147
<input type="checkbox"/>	BLOCK_IP_168.181.196.36	Máscara de red IP	168.181.196.36
<input type="checkbox"/>	BLOCK_IP_185.222.209.84	Máscara de red IP	185.222.209.84

Figura 75. Objetos IP atacantes

Fuente: Elaborado por el autor

4.20.11 Agrupación de servidores

Para una mejor administración y disminución de reglas de permisos se procede a agrupar los servidores como se muestra en la figura 76.

<input type="checkbox"/> GRP_ATMAILING		20	SCP_192.168.120.181 SCP_192.168.120.182 SCP_192.168.120.183 SCP_192.168.120.184 SCP_192.168.120.185 SCP_192.168.120.186 SCP_192.168.120.187
--	--	----	---

Figura 76. Agrupación de servidores

Fuente: Elaborado por el autor

4.20.12 Agrupación de redes

Se realiza una agrupación de redes para una mejor administración y seguridad. Se muestra en la figura 77.

<input type="checkbox"/> LAN_Interna_AMB		4	NET_AMB_D_172.16.130.0 Net_AMB_Guest_172.16.133.0 Net_AMB_Video_172.16.132.0 Net_AMB_Voip_172.16.131.0
--	--	---	---

Figura 77. Agrupación de redes

Fuente: Elaborado por el autor

4.20.13 Servicios TCP/IP

Los servicios se habilitan de acuerdo a la necesidad de los servidores para ofrecer un servicio efectivo. Se muestra en la figura 78.

<input type="checkbox"/> TCP_2087		TCP	2087
<input type="checkbox"/> TCP_21		TCP	21
<input type="checkbox"/> TCP_22146		TCP	22146
<input type="checkbox"/> TCP_2222		TCP	2222

Figura 78. Configuración servicios

Fuente: Elaborado por el autor

4.20.14 Navegación para servidores

La salida a Internet para servidores está bloqueada solo se habilita de forma temporal cuando lo solicitan de manera justificada y con el formulario correspondiente.

Se bloquea todo el tráfico no permitido desde la red de servidores como se muestra en la figura 79 y 80.

	Nombre	If Origin		If Destino		Opciones	Aplicación	Servicio	Acción
		Zona	Dirección	Zona	Dirección				
72	NAVEGACION_SERVIDORES	LAN_DC_CNT	any	ISP_CNT ISP_TELCONET	any		any	application-default	Denegar

Figura 79. Bloqueo de tráfico de servidores

Fuente: Elaborado por el autor

<input checked="" type="checkbox"/>	NAVEGACION_SERVIDORES			block		Allow Categories (0)	Allow Categories (0)
						Alert Categories (66)	Alert Categories (13)
						Continue Categories (0)	Continue Categories (0)
						Block Categories (0)	Block Categories (53)
						Override Categories (0)	

Figura 80. Bloqueo navegación servidores

Fuente: Elaborado por el autor

En caso de necesitar navegación para algún servidor se configura un perfil que contenga acceso a repositorios de actualizaciones o páginas específicamente necesarias, como se muestra en la figura 81. Los permisos temporales se conceden con temporizadores apropiados que desactivan el permiso automáticamente en el tiempo estipulado.

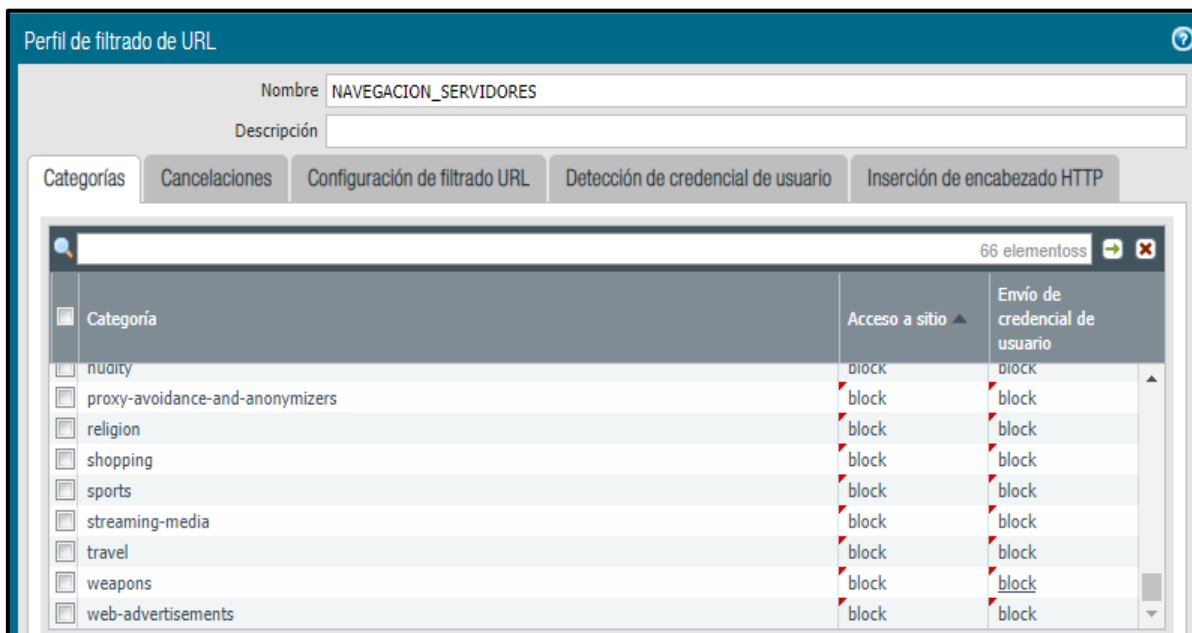


Figura 81. Configuración del perfil de navegación de servidores

Fuente: Elaborado por el autor

4.20.15 Configuración de reglas NAT

A continuación se procede a configurar la política de NAT para navegación servidores de la red SERCOP, para que el tráfico salga con la IP 190.152.X.46. Se muestra en la figura 82 y 83.

Nombre	Etiquetas	Paquete original			Traducción de origen
		Zona de origen	Zona de destino	Servicio	
108 prueba_LAN_to_internet	none	DATOS_SERCOP LAN_DC_CNT	ISP_CNT	any	dynamic-ip-and-port ethernet1/4 190.152.44.46/27

Figura 82. Regla NAT

Fuente: Elaborado por el autor

Figura 83. Configuración regla NAT navegación

Fuente: Elaborado por el autor

4.20.16 Reglas NAT de publicación de servicios

Como se había mencionado anteriormente en el Data Center de CNT se encuentran alojados todos los servidores de los servicios que ofrece la institución a la ciudadanía por lo que a continuación se procede a configurar la publicación de servicios web de SERCOP.

4.20.17 Regla de publicación SOCE TELCONET

En la figura 84 se muestra la regla de publicación del Sistema Oficial de Contracción Pública del Ecuador, por los servicios de http y https por TELCONET.

	Nombre	Zona de origen	Zona de destino	Dirección de destino	Servicio	Traducción de destino
1	Publicacion HTTPS_SOCE_TELCO	ISP_TELCONET	ISP_TELCONET	EXT_190.95.208.2	service-https	destination-translation dirección: DC-NS-SOCE_TELCONET_192.168.100.252 puerto: 443

Figura 84. Regla publicación SOCE TELCONET

Fuente: Elaborado por el autor

4.20.17 Regla de publicación SOCE CNT

De la misma manera en la Figura 85 se muestra la regla de publicación del Sistema Oficial de Contracción Pública del Ecuador, por los servicios de http y https por CNT como ISP principal.

	Nombre	Zona de origen	Zona de destino	Dirección de destino	Servicio	Traducción de destino
92	Publicacion HTTPS_SOCE_CNT	ISP_CNT	ISP_CNT_POOL2	CNT_190.152.44.100	service-https	destination-translation dirección: DC-NS-SOCE_CNT_192.168.100.254 puerto: 443
93	Publicacion HTTP_SOCE_CNT	ISP_CNT	ISP_CNT_POOL2	CNT_190.152.44.100	service-http	destination-translation dirección: DC-NS-SOCE_CNT_192.168.100.254 puerto: 80

Figura 85. Regla publicación SOCE CNT

Fuente: Elaborado por el autor

4.20.17 Regla publicación SOCE Anillo Interministerial

A continuación en la Figura 86 se muestra la regla de publicación del Sistema Oficial de Contración Pública del Ecuador, por los servicios de http y https por el Anillo Interministerial.

191	Publicacion HTTPS Soce Anillo	ANILLO_INTE...	ANILLO_INTERMINISTE...	EXT_10.80.5.14	service-https	destination-translation dirección: DC-NS-SOCE_CNT_192.168.100.254 puerto: 443
192	Publicacion HTTP Anillo	ANILLO_INTE...	ANILLO_INTERMINISTE...	EXT_10.80.5.14	service-http	destination-translation dirección: DC-NS-SOCE_CNT_192.168.100.254 puerto: 80

Figura 86. Regla de publicación SOCE Anillo Interministerial

Fuente: Elaborado por el autor

4.20.18 Publicación del Portal de Compras Públicas por CNT

De igual forma se continúa con la publicación de los demás servicios en esta ocasión en la figura 87 se muestra la publicación del Portal de Compras Públicas del Servicio Nacional de Contratación Pública por http y https.

	Nombre	Zona de origen	Zona de destino	Dirección de destino	Servicio	Traducción de destino
94	342_ISP_CNT TO LAN	ISP_CNT	ISP_CNT_POOL2	CNT_190.152.44.109	service-http	destination-translation dirección: SCP_192.168.100.240 puerto: 80
95	343_ISP_CNT TO LAN	ISP_CNT	ISP_CNT_POOL2	CNT_190.152.44.109	service-https	destination-translation dirección: SCP_192.168.100.240 puerto: 443

Figura 87. Regla de publicación del portal compras públicas por CNT

Fuente: Elaborado por el autor

4.20.19 Publicación del portal de compras públicas por el anillo interministerial

Publicación del Portal de Compras Públicas por el Anillo Interministerial, las demás reglas de publicación con su respectiva IP pública no se puede evidenciar por razones de confidencialiad. Se muestra en la figura 88.

183	Publicacion HTTP Portal Anillo	ANILLO_INTE...	ANILLO_INTERMINISTE...	Ext_10.80.5.145	service-http	destination-translation dirección: SCP_192.168.100.240 puerto: 80
184	Publicacion HTTPS Portal Anillo	ANILLO_INTE...	ANILLO_INTERMINISTERIAL	Ext_10.80.5.145	service-https	destination-translation dirección: SCP_192.168.100.240 puerto: 443

Figura 88. Regla de publicación del Portal Compras Públicas por Anillo Interministerial

Fuente: Elaborado por el autor

4.20 20 Publicación DNS CNT

Se realiza la publicación del DNS de CNT para los pool de IP públicas de todos los servicios. Se muestra en la figura 89.

	Nombre	Zona de origen	Zona de destino	Dirección de destino	Servicio	Traducción de destino
98	Publicacion_DNS_UDP_SOCE_CNT	ISP_CNT	ISP_CNT_POOL2	CNT_190.152.44.118	service_UDP_...	destination-translation dirección: SCP_192.168.100.249 puerto: 53
99	Publicacion_DNS_TCP_SOCE_CNT	ISP_CNT	ISP_CNT_POOL2	CNT_190.152.44.118	service_TCP_...	destination-translation dirección: SCP_192.168.100.249 puerto: 53

Figura 89. Regla de publicación DNS CNT

Fuente: Elaborado por el autor

4.20.21 Publicación DNS TELCONET

En la Figura 90 se muestra la publicación del DNS de TELCONET por tcp y udp.

	Nombre	Zona de origen	Zona de destino	Dirección de destino	Servicio	Traducción de destino
101	Publicacion_DNS_UDP_SOCE_TELCO	ISP_TELCONET	ISP_TELCONET	EXT_190.95.208.2	service_UDP_...	destination-translation dirección: SCP_192.168.100.250 puerto: 53
102	Publicacion_DNS_TCP_SOCE_TELCO	ISP_TELCONET	ISP_TELCONET	EXT_190.95.208.2	service_TCP_...	destination-translation dirección: SCP_192.168.100.250

Figura 90. Regla de publicación DNS CNT

Fuente: Elaborado por el autor

4.20.22 Configuración de políticas de seguridad

A continuación realizamos la configuración de las reglas de seguridad para dar permisos de acceso a los servicios.

4.20.23 SOCE TELCONET y CNT

En la figura 91 se muestra la configuración por CNT y TELCONET.

	Nombre	Zona	Dirección	Zona	Dirección	Opciones	Aplicación	Servicio	Acción
57	web_soce	ISP_CNT	any	LAN_DC_CNT	190.152.44.100		ssl web-browsing	application-default	Permitir

Figura 91. Regla seguridad acceso SOCE por CNT y TELCONET

Fuente: Elaborado por el autor

4.20.24 Portal

En la figura 92 se representa la regla de publicación y acceso al SOCE.

	Nombre	Zona	Dirección	Zona	Dirección	Opciones	Aplicación	Servicio	Acción
62	Web Portal	ISP_CNT	any	LAN_DC_CNT	190.152.44.109		ssl web-browsing	application-default	Permitir

Figura 92. Regla de seguridad de acceso al portal

Fuente: Elaborado por el autor

4.20.25 Regla de seguridad acceso DNS TELCONET y CNT

A continuación se muestra en la Figura 93 la regla de seguridad para el acceso de los DNS de TELCONET y CNT.

	Nombre	Zona	Dirección	Zona	Dirección	Opciones	Aplicación	Servicio	Acción
64	DNS-208.2	ISP_TELCONET	any	any	190.95.208.2		dns	application-default	Permitir
65	DNS-118	ISP_CNT	any	LAN_DC_CNT	190.152.44.118		dns	application-default	Permitir

Figura 93. Regla de seguridad DNS TELCONET y CNT

Fuente: Elaborado por el autor

4.20.26 Permisos de acceso entre redes LAN

Se procede a crear la política de comunicación entre las redes LAN, DATOS, DC_CNT, ANILLO INTERMINISTERIAL. Se muestra en la figura 94.

	Nombre	Zona	Dirección	Zona	Dirección	Opciones	Aplicación	Servicio	Acción
74	DATOS_to_DATOS	DATOS_SERC...	any	DATOS_SERCOP	any		any	application-default	Permitir
75	DATOS_SERCOP TO LAN_DC_CNT	DATOS_SERC...	any	LAN_DC_CNT	any		any	any	Permitir
76	LAN_DC_CNT to DATOS_SERCOP	LAN_DC_CNT	any	DATOS_SERCOP	any		any	any	Permitir
77	ANILLO_to_ANILLO	ANILLO_INT...	any	ANILLO_INTERMINI...	any		any	application-default	Permitir

Figura 94. Regla de seguridad acceso entre Redes

Fuente: Elaborado por el autor

4.20.27 Permisos de navegación *Atmailing*

Se procede a crear la política de navegación de *Atmailing* como se muestra en la Figura 95.

	Nombre	Zona	Dirección	Zona	Dirección	Opciones	Aplicación	Servicio	Acción
15	Atmailing-192.168.120.181	LAN_DC_CNT	192.168.120.181	ISP_CNT	any		ssl web-browsing	application-default	Permitir
20	Grupo Atmailing	LAN_DC_CNT	192.168.120.0/24 Rango_Atmailing_120.1...	ISP_CNT	any		atmailing smtp	application-default	Permitir
81	Accesos al ATMAILING	any	any	any	CNT_ATMAILING_190.152...		any	application-default	Permitir
82	Navegacion ATMAILING	any	UIO_SRV_ATMAILING_...	any	any		any	service-http service-https TCP_20 TCP_21	Permitir
83	Permisos ATMAILING	any	any	any	UIO_SRV_ATMAILING_192.1...		any	service-http service-https service_ssh service_TCP_7316	Permitir
104	Atmailing to AD	any	UIO_VS_AD_172.16.0.12	any	UIO_SRV_ATMAILING_192.1... Srv_SRVSQL_ULTIMUS_192... Srv_192.168.9.206		any	any	Permitir
105	Atmailing to AD int	LAN_DC_CNT	any	any	UIO_VS_AD_172.16.0.12		any	any	Permitir

Figura 95. Regla de seguridad para navegación *Atmailing*

Fuente: Elaborado por el autor

4.20.28 Permisos de Navegación Antispam

En *ANTISPAM* debe tener configurado navegación para realizar su trabajo de protección por lo que se procede a crear una política de acceso para aplicaciones de *ANTISPAM* como se muestra en la figura 96.

	Nombre	Zona	Dirección	Zona	Dirección	Opciones	Aplicación	Servicio	Acción
21	Antispam	any	192.168.9.39	ISP_CNT...	any		app_antispa... APP_UDP_113 APP_UDP_62... dns smtp web-browsing	application-default	Permitir
22	Nav_Antispam	LAN_DC_CNT	192.168.1.88 192.168.9.39 192.168.9.40 192.168.9.41	ISP_CNT...	any		any	any	Permitir
41	SRV Antispam	ISP_CNT	any	LAN_DC...	CNT_190.152.44.105		any	application-default	Permitir

Figura 96. Regla de seguridad para navegación *ANTISPAM*

Fuente: Elaborado por el autor

4.20.29 Permiso para navegación CITRIX (Balanceador de Carga)

Se crea la política para que el servidor CITRIX pueda navegar hacia el Internet y así poder acceder a la administración vía web, como se muestra en la figura 97.

	Nombre	Zona	Dirección	Zona	Dirección	Opciones	Aplicación	Servicio	Acción
30	CITRIX_TO_ANY	LAN_DC_CNT	DC-APL-CITRIX2_192.168.1.56 DC-APL-CITRIX_192.168.1.57 DC_AP_CITRIX1_192.168.1.55	ISP_CNT ISP_TELCONET	any		any	application-default	Permitir

Figura 97. Regla de seguridad para navegación *ANTISPAM*

Fuente: Elaborado por el autor

4.20.30 Configuración de reglas para protección

Como parte de la protección se ha visto la necesidad de crear reglas para bloquear IP atacantes, IP *black list*, *boots*, IP que son reportadas por el administrador de correos, etc.

4.20.31 Bloqueo de *blacklist*

En la figura 98 se muestra la regla de bloqueo configurada para IP categorizadas en listas negras.

7	Bloqueo Google boot	any	any	ISP_CNT ISP_TELCONET	GRP_IPS_BLACKLIST NL		any	any	Denegar
---	---------------------	-----	-----	-------------------------	-------------------------	--	-----	-----	---------

Figura 98. Regla de seguridad para bloqueo blacklist

Fuente: Elaborado por el autor

4.20.32 Bloqueo de *boot* para SOCE

A continuación en la Figura 99 se muestra la regla de bloqueo para IP categorizadas como boots que intentan atacar al SOCE.

	Nombre	Zona	Dirección	Zona	Dirección	Opciones	Aplicación	Servicio	Acción
6	Bloqueo Google boot Soce	any	40.101.128.221 GRP_IPS_BLACKLIST IE NL SPAM	ISP_CNT ISP_CNT_POOL2 LAN_DC_CNT	190.95.208.2 190.152.44.100		any	any	Denegar

Figura 99. Regla de seguridad bloqueo *BOOTS*

Fuente: Elaborado por el autor

4.21 Ubicación de los equipos en los Rack DC CNT

Una vez concluida con la configuración base en los equipos, procedemos a colocar en los Rack ubicados en el Data Center de CNT, de igual forma para la conexión usamos cable UTP categoría 6 certificado. Las conexiones se realizan según el diagrama propuesto en la figura 3.1.

A continuación se muestra en la figura 100 la ubicación de los equipos en el rack del SERCOP en CNT:

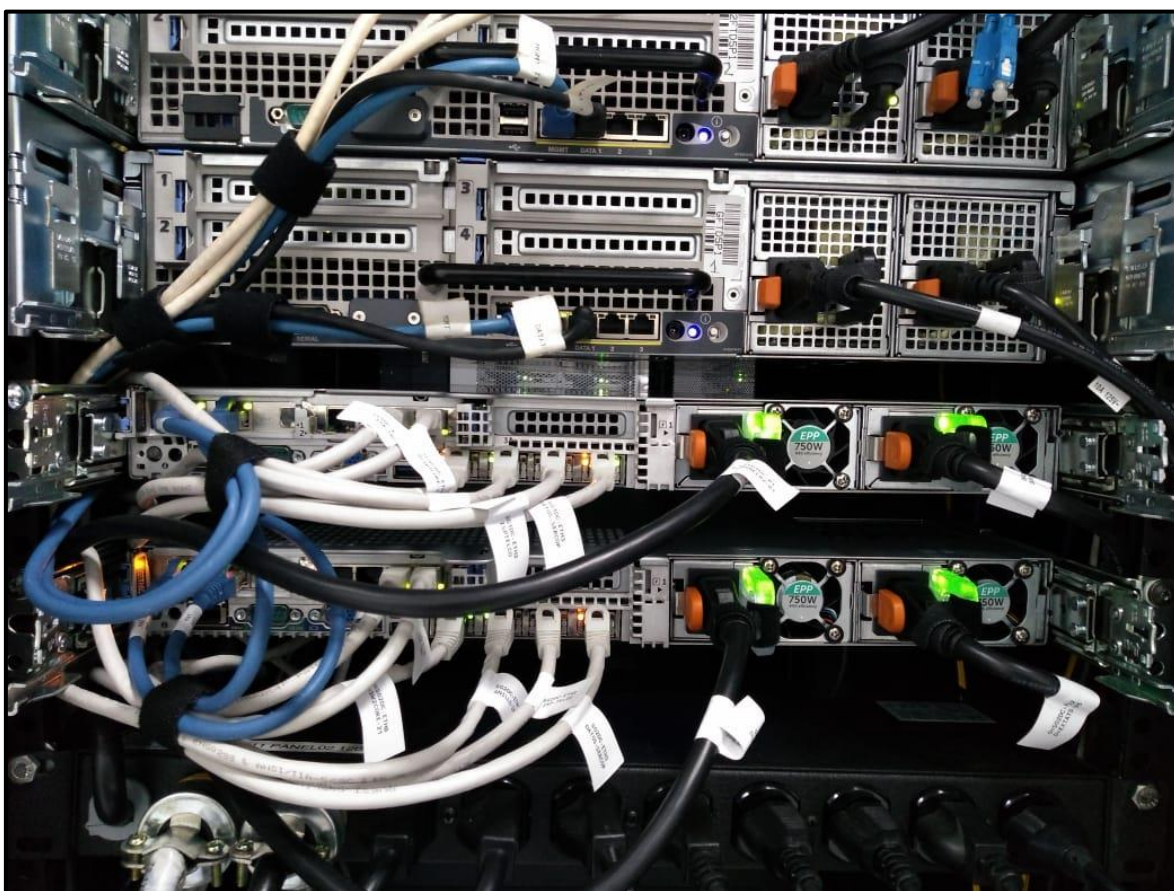


Figura 100. Ubicación RACK DC CNT

Fuente: Elaborado por el autor

En la figura 101 y 102 se muestran las topologías finales de implementación en cada uno de los data center.

4.22 Topología de red final

Topología del Data Center CNT

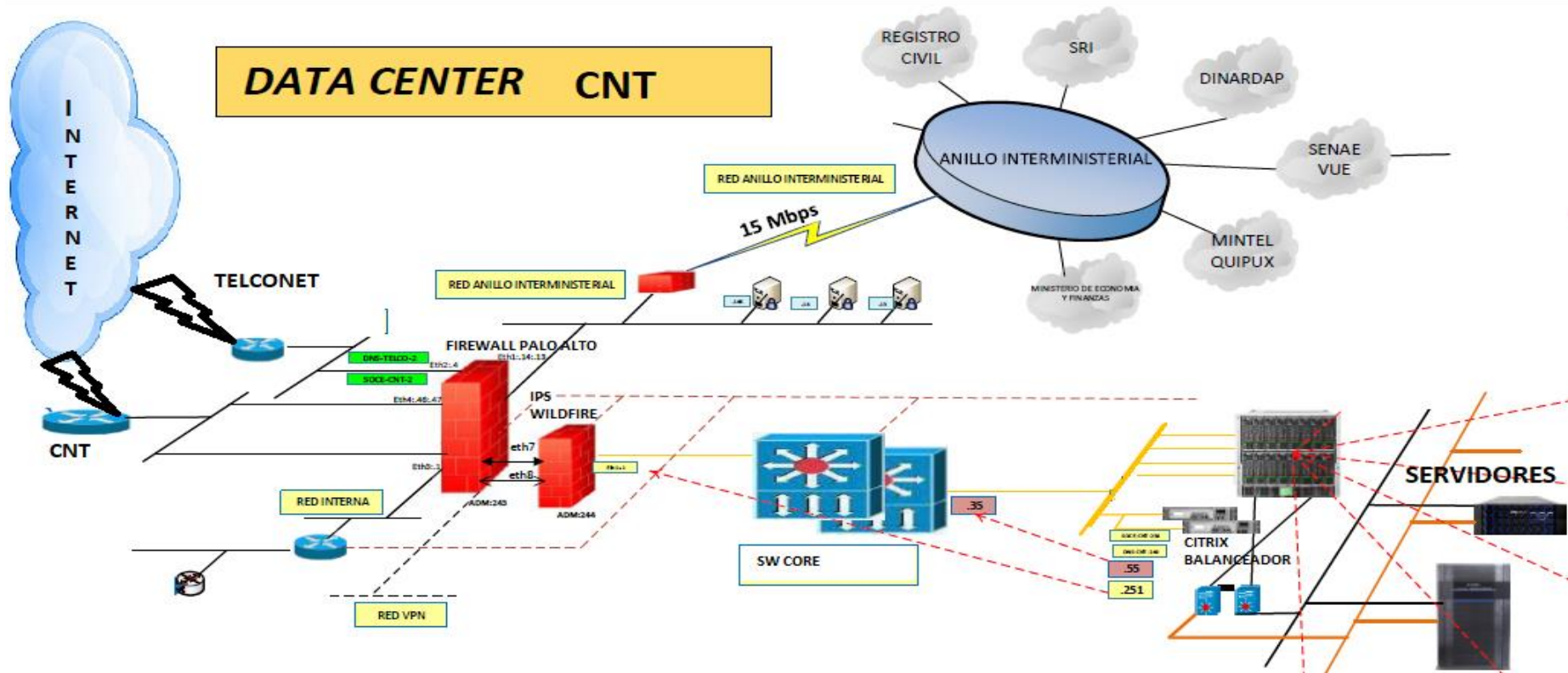


Figura 101. Topología de red final del Data Center CNT

Fuente: Elaborado por el autor

Topología del edificio El Telégrafo

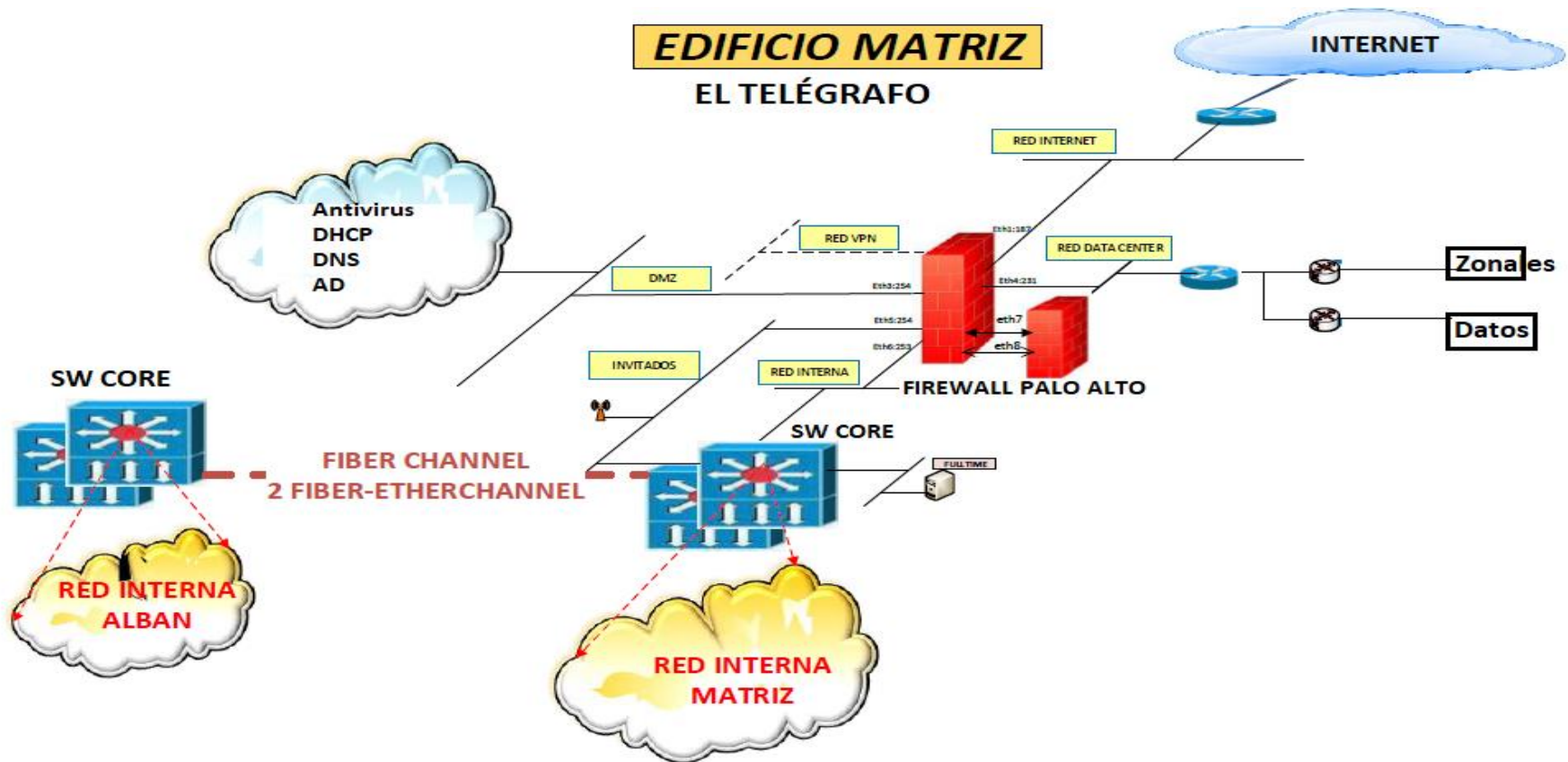


Figura 102. Topología final del edificio El Telégrafo

Fuente: Elaborado por el autor

4.3 Pruebas de funcionamiento

Una vez culminada la configuración y ubicación de los equipos se procede a hacer validaciones y pruebas según el siguiente cuadro, como se muestra en la tabla 13.

Tabla 13. Pruebas de Funcionamiento

PRUEBAS Y FUNCIONAMIENTO				
Actividad General	Actor	Actividad Específica	Cumple	No Cumple
Revisión	Sergio Toapanta	Revisión de zonas de red	X	
Revisión	Sergio Toapanta	Revisión de objetos de red	X	
Revisión	Sergio Toapanta	Revisión de grupos de objetos	X	
Revisión	Sergio Toapanta	Revisión de servicios	X	
Revisión	Sergio Toapanta	Revisan de grupos de servicios	X	
Revisión	Sergio Toapanta	Revisión de políticas de seguridad	X	
Revisión	Sergio Toapanta	Revisión de políticas de NAT	X	
Revisión	Sergio Toapanta	Revisión de políticas VPN	X	
Revisión	Sergio Toapanta	Revisión de tablas de ruteo estáticas	X	
Revisión	Sergio Toapanta	Revisión de mapeo interfaces físicas de red vs <i>switch virtuales</i>	X	
Revisión	Sergio Toapanta	Revisión de HA entre equipos	X	
Revisión	Sergio Toapanta	Revisión de instalación de licenciamiento.	X	
Pruebas	Sergio Toapanta	Pruebas de conectividad	X	
Pruebas	Sergio Toapanta	Validación de políticas de NAT	X	
Pruebas	Sergio Toapanta	Validación de políticas de seguridad	X	
Pruebas	Sergio Toapanta	Validación de servicios internos	X	
Pruebas	Sergio Toapanta	Reporte de cambios y/o depuración de políticas	X	
Pruebas	Sergio Toapanta	Revisión de cambios.	X	
Check List de Configuración	SERCOP	Aprobación de configuraciones realizadas.	X	
	SERCOP	Revisión general	X	

Fuente: Elaborado por el autor

4.3.1 Pruebas de navegación

De acuerdo a los permisos concedidos se realiza una prueba de navegación hacia Internet en particular se toma el *streaming* como *youtube*, como se muestra en la figura 103 a continuación:

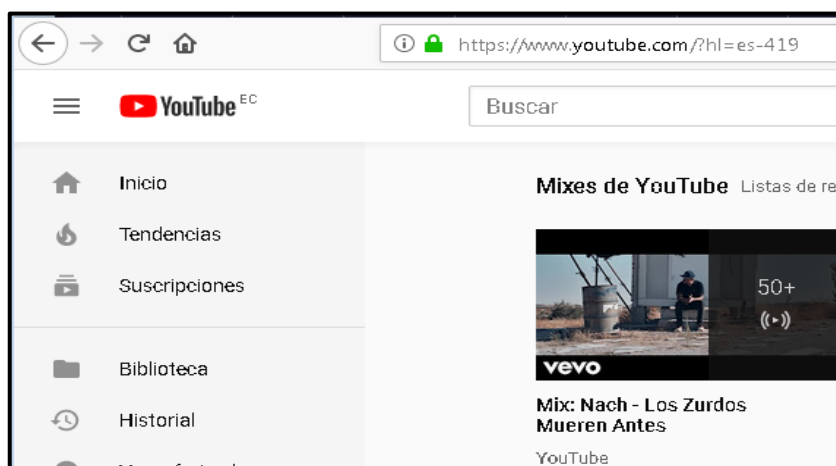


Figura 103. Prueba navegación Internet

Fuente: Elaborado por el autor

4.3.2 Pruebas de bloqueos

Según los permisos asignados y solicitudes recibidas de bloqueos para mantener un buen ancho de banda para todos los usuarios, se muestra el bloqueo en equipos que no tienen permisos de *streaming*, bloqueos por *malware*, bloqueos de páginas no permitidas, etc. como se muestra en la figura 104.

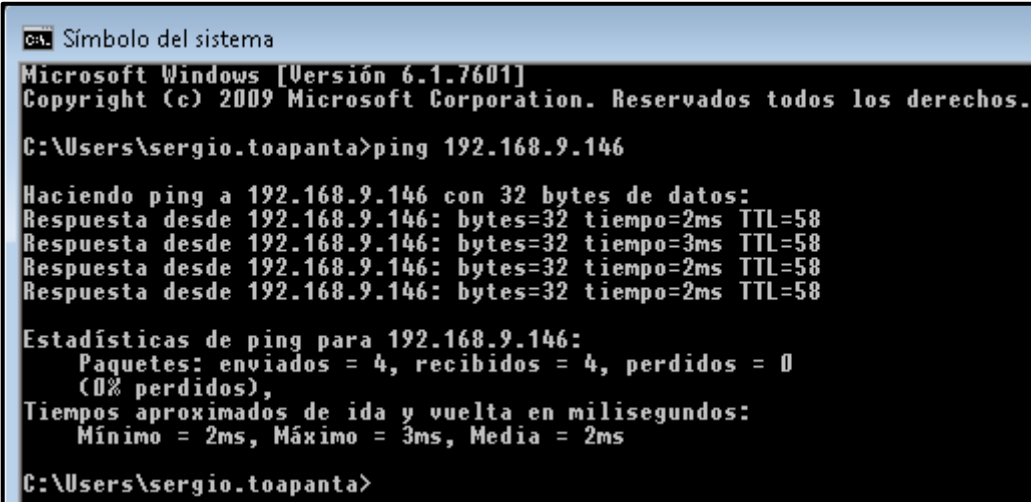


Figura 104. Bloqueos de sitios por *malware*

Fuente: Elaborado por el autor

4.3.3 Pruebas de comunicación entre equipos de SERCOP y CNT

Se realiza un test usando el ping hacia un servidor ubicado en la red de producción del Data Center de CNT, como se muestra en la figura 105:



```
CA: Símbolo del sistema
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\sergio.toapanta>ping 192.168.9.146

Haciendo ping a 192.168.9.146 con 32 bytes de datos:
Respuesta desde 192.168.9.146: bytes=32 tiempo=2ms TTL=58
Respuesta desde 192.168.9.146: bytes=32 tiempo=3ms TTL=58
Respuesta desde 192.168.9.146: bytes=32 tiempo=2ms TTL=58
Respuesta desde 192.168.9.146: bytes=32 tiempo=2ms TTL=58

Estadísticas de ping para 192.168.9.146:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 2ms, Máximo = 3ms, Media = 2ms

C:\Users\sergio.toapanta>
```

Figura 105. Ping servidor ubicado DC CNT

Fuente: Elaborado por el autor

4.3.4 Pruebas de acceso VPN

Luego de haber configurado el portal VPN y crear los usuarios de acceso VPN, procedemos a validar el acceso usando el cliente *Global Protect* tanto a nivel de Windows como de Android, como se muestra en las siguientes figuras 106:

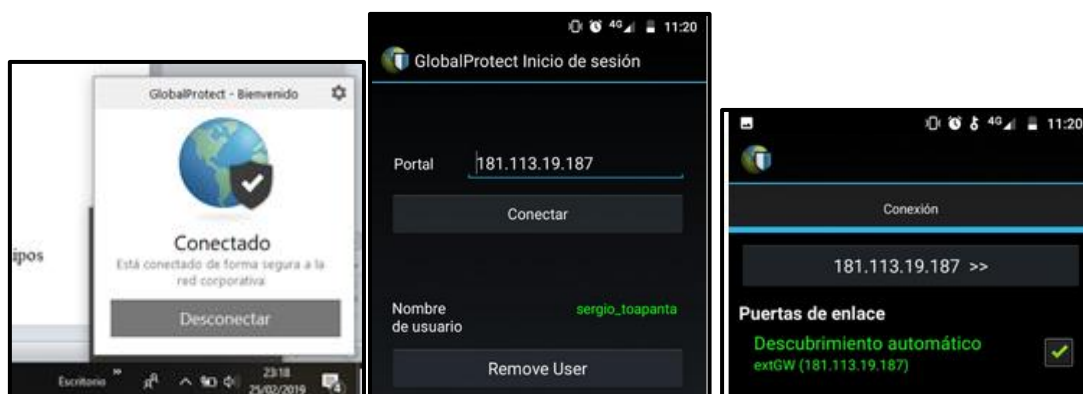


Figura 106. Acceso VPN Windows y Android

Fuente: Elaborado por el autor

4.4 Análisis de resultados

Terminadas las fases respectivas, vemos el funcionamiento de los equipos observando lo siguiente:

4.4.1 Análisis resultados de comunicación entre redes

Después de ver el resultado de las pruebas que se describen en la tabla 4.18, realizando un ping hacia el servidor de la red 9 ubicada en el DC CNT se puede afirmar que la comunicación entre equipos es exitosa.

4.4.2 Análisis de resultados de navegación

Como se evidencia en la figura 103 Pruebas de navegación Internet se puede distinguir que los equipos con permisos de navegación están accediendo normalmente hacia el Internet y a todas la páginas validas de la institución.

4.4.3 Análisis de resultados acceso VPN

Como se muestra en la figura 106 se puede ver las conexiones realizadas de VPN hacia la infraestructura del SERCOP. Estas conexiones son tanto del sistema operativo *Windows* y *Android*.

4.4.4 Análisis resultados de control de *malware*

Como se puede observar en la figura 4.104, el bloqueo y control de *malware* se mantiene eficaz ya sea a sitios visitados como de configuración.

- Se analizó también lo siguiente que se lista a continuación:
- Comunicación entre redes Data Center El Telégrafo y Data Center CNT.
- Resolución DNS por CNT y TELCONET.
- Publicación de servicios para la ciudadanía como SOCE, CATÁLOGO, PORTALSICM, etc.
- Acceso a Internet desde todas las redes e IP de la institución.
- Acceso VPN desde PC y dispositivos móviles, de acuerdo a solicitudes y autorizaciones presentadas.

- Acceso a servidores restringido, solo se otorga a equipos que presenten la solicitud mediante formulario y firmas de autorización.
- Navegación con permisos según el perfil y solicitudes presentadas.

En el anexo 3, se presenta una comparación de las características de la herramienta de seguridad *firewall* anterior con la nueva implementación, para así encontrar la mejora en la seguridad de la red y la información.

El tiempo de aplicación de cambios o compilar permisos es la característica más significativa de la nueva herramienta, ya que permite realizarlo en tiempo real de 1-10 max como tiempo máximo, esto nos permite combatir con efectividad ataques en tiempo real ya sea de DOS (Denegación de servicio). La herramienta anterior no nos permitía esto pues lo realizaba en un tiempo aproximado de 10 a 15 min. En figura 107 se muestra una ejecución de cambios en la nueva plataforma de paloalto Networks.

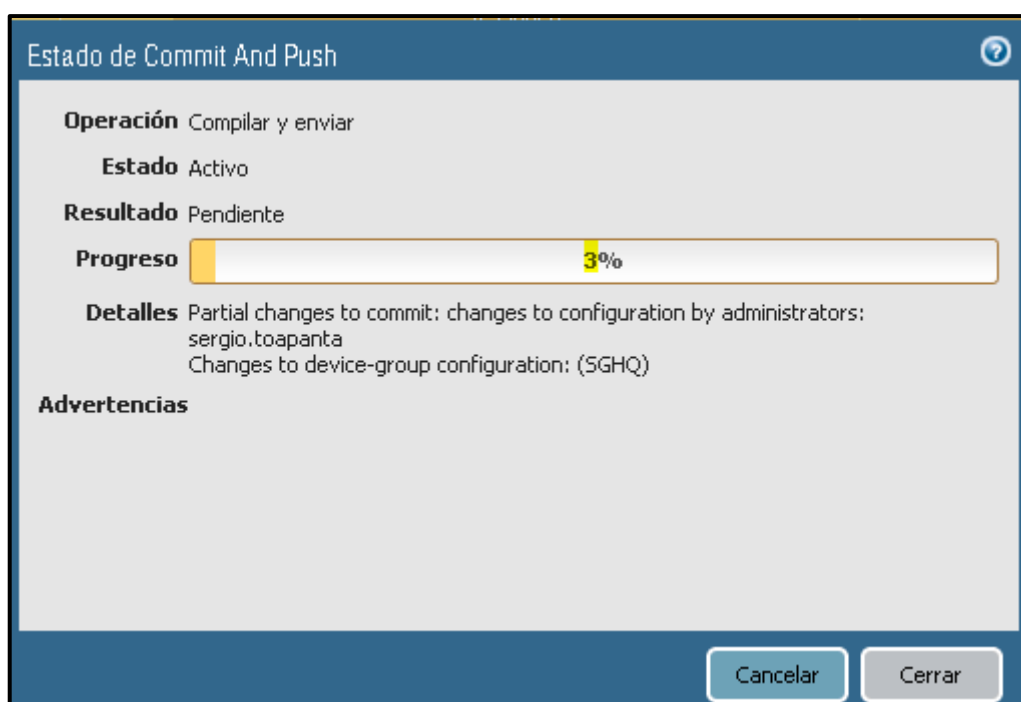


Figura 107. Ejecución o compilación de cambios PAN

Fuente: Elaborado por el autor

A continuación en la tabla 14 se detalla las mejoras encontradas de la comparación entre las dos herramientas descritas en el anexo 3. De esta manera se demuestra que la red

y la información están más seguras con la implementación de los nuevos equipos de seguridad perimetral.

Tabla 14. Mejora de seguridad de la red y la información.

	Características	Check Point	paloalto Networks
Mejora	Mejora de seguridad de la red y la información		
	Identifica la aplicación, independientemente del puerto, la encriptación (SSL/SSH) o las técnicas evasivas empleadas	NO	SI
	Usa la aplicación, no el puerto, como base para todas sus decisiones de políticas de habilitación segura como permitir, denegar, programar, inspeccionar y aplicar el control de tráfico	NO	SI
	Categoriza aplicaciones no identificadas para el control de políticas, la investigación forense de amenazas o el desarrollo de tecnología App-ID™.	NO	SI
	Habilita la integración sin agentes con Microsoft Active Directory® y Terminal Services, LDAP, Novell eDirectory™ y Citrix	NO	SI
	Aplicación de políticas en tiempo real de 1-10 segundos.	NO	SI
	NEXT GENERATION FIREWALL	NO	SI
	Divide una aplicación en capas para un mejor control de seguridad de fuga de información.	NO	SI
	Administración por consola WEB	NO	SI

Fuente: Elaborada por el autor

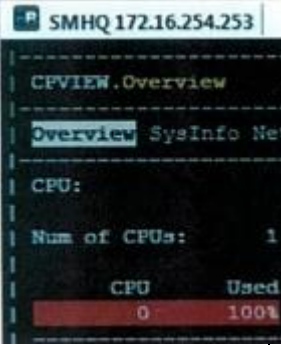
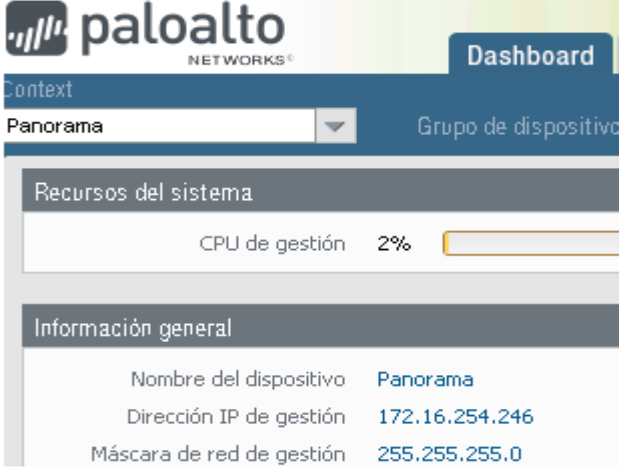
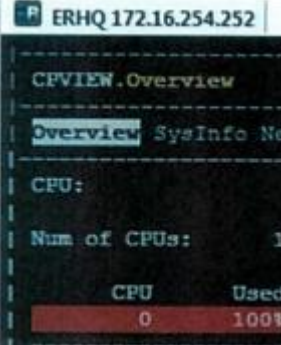
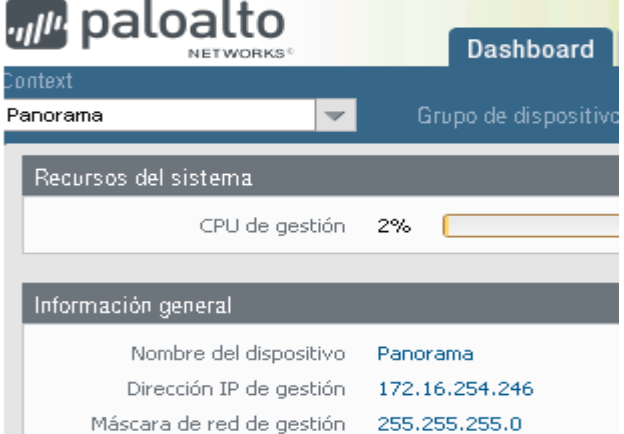
En cuanto al rendimiento en la figura 108 y tabla 15 se muestra la capacidad del firewall paloalto networks. La capacidad actual nos da una estabilidad ya que con la anterior herramienta en consumo de CPU estábamos al 100 % y la administración así como la protección era demasiado lenta.

Rendimiento y Capacidad	PA-3050
Tasa de rendimiento de firewall ¹	4 Gbps
Tasa de rendimiento de Threat Prevention ²	2 Gbps
Tasa de rendimiento de VPN IPsec ³	500 Mbps
Nuevas sesiones por segundo ⁴	50 000
Sesiones máximas	500 000
Sistemas virtuales (base/máx.) ⁵	1/6

Figura 108. Rendimiento firewall paloalto Networks

Fuente: Elaborado por el autor

Tabla 15. Uso CPU Check Point y paloalto

	Check Point	paloalto NETWORKS
Administración		
Reporteador		

Fuente: Elaborado por el autor

Conclusiones

- La implementación de un firewall perimetral en la institución permite incrementar la eficacia en el control de accesos y protección de los equipos y sistemas tecnológicos existentes en la institución.
- Las reglas y políticas de permisos implementados en el sistema firewall perimetral mejoran la seguridad de la información existente en cuanto a integridad, confidencialidad y disponibilidad de la misma.
- Con la implementación de este sistema se concluye que se ha dado solución al problema encontrado al inicio del proyecto y que la empresa SERCOP logró encontrar muchos beneficios con el uso del firewall perimetral.
- Con la configuración que permite la comunicación y consumo de servicios a través del anillo interministerial en el sistema de seguridad informática del SERCOP, se da cumplimiento al Esquema Gubernamental de Seguridad de la Información (EGSI) y sus políticas.
- Al implementar el firewall en servidores virtuales, da la facilidad de aumentar la capacidad del CPU en cualquier momento que sea necesario y así asegurar el buen funcionamiento de los equipos de protección de la infraestructura tecnológica y la información de la institución.
- La implementación del firewall en servidores virtuales facilita el incremento de la capacidad del CPU, acorde a las variaciones de tráfico y uso del sistema de compras públicas, asegurando de esta manera el buen funcionamiento de los equipos de protección de la infraestructura tecnológica y la información de la institución.

Recomendaciones

- Se recomienda seguir un estricto control de accesos hacia servidores y equipos críticos de la institución, el control llevado mediante formulario es válido como prueba de lo solicitado, pero podría ser automatizado para un mejor administración.
- Se recomienda monitorear el tráfico constantemente para evidenciar el aumento y preveer el incremento de CPU en los equipos de seguridad perimetral, en caso de ser necesario.
- Se recomienda llevar un perfil bien definido de permisos para cada área, así la administración será mejor y se podrá tener un control con bitácora de cambios y políticas, para asegurar el acceso.
- Se recomienda para una segunda fase de implementación de seguridad perimetral, añadir en el Data Center de CNT una DMZ para realizar un control interno de comunicación entre redes de los servidores de producción que se encuentran alojados en el mismo.

BIBLIOGRAFÍA

- PriteshGupta.com.* (2016). Obtenido de <http://www.iso27000.es/iso27000.html>
- citrix.com.* (2019). Obtenido de <https://lac.citrix.com/products/citrix-web-app-firewall/>
- Aguilera, P. (2010). *SEGURIDAD INFORMÁTICA*. Editex S.A.
- Arellano, G. (04 de Marzo de 2005). *Seguridad Perimetral*. Recuperado el 05 de Marzo de 2005, de [www.academia.edu:https://www.academia.edu/4690646/Seguridad_Perimetral](http://www.academia.edu/4690646/Seguridad_Perimetral)
- Arias, F. (2012). *El proyecto de investigación*. Caracas: Episteme.
- Ballestrine, M. (2006). *Como se realiza una investigación*. Caracas: Consultores & Asociados.
- CISCO.com.*(s.f.).Obtenidodehttps://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html
- Díaz, Y., Perez, Y., & Proenza, D. (2014). *Sistema para la Gestión de la Información de Seguridad Informática en la Universidad de Ciencias Médicas de Holguín*. Holguín.
- Gómez Vieites, Á. (2014). *Enciclopedia de la Seguridad Informática*. Madrid: RA-MA ISBN.
- Martinez, V. (octubre de 2010). *bibdigital.epn.edu.ec*. Obtenido de <https://bibdigital.epn.edu.ec/>
- Pilacuán, E. (2015). *Repositorio ESPE*. Obtenido de <http://repositorio.espe.edu.ec/handle/21000/9890>
- Raffino, M. E. (23 de Noviembre de 2018). *concepto.de*. Obtenido de <https://concepto.de/firewall/#ixzz5rzY6oZQt>

Ramos, A., Gonzáles, J., & Picouto, F. (2014). *Seguridad perimetral, monitorización y ataques en redes*. Madrid: RA-MA Editorial.

SERCOP. (agosto de 2008). *Portal de compras públicas*. Obtenido de <https://portal.compraspublicas.gob.ec/sercop/>

SERCOP, E. O. (2015). *Portal compras públicas*. Obtenido de <https://portal.compraspublicas.gob.ec/sercop/>

SNAP, S. n. (septiembre de 2013). Esquema gubernamental de seguridad de la información. *EGSI*. Quito, Pichincha, ECUADOR: Acuerdo Ministerial 166.

Soriano, M. (2014). Seguridad en Redes y Seguridad de la Información. *IMPROVET*, 80.

Anexos

Anexo 1 Matriz de riesgos de la Dirección de Seguridad Informática

Anexo 2 Proformas de equipos

Anexo 3 Tabla comparativa de herramientas Check Point y paloalto Networks

Anexo 4 Manual de usuario

Anexo 5 Cronograma de Actividades

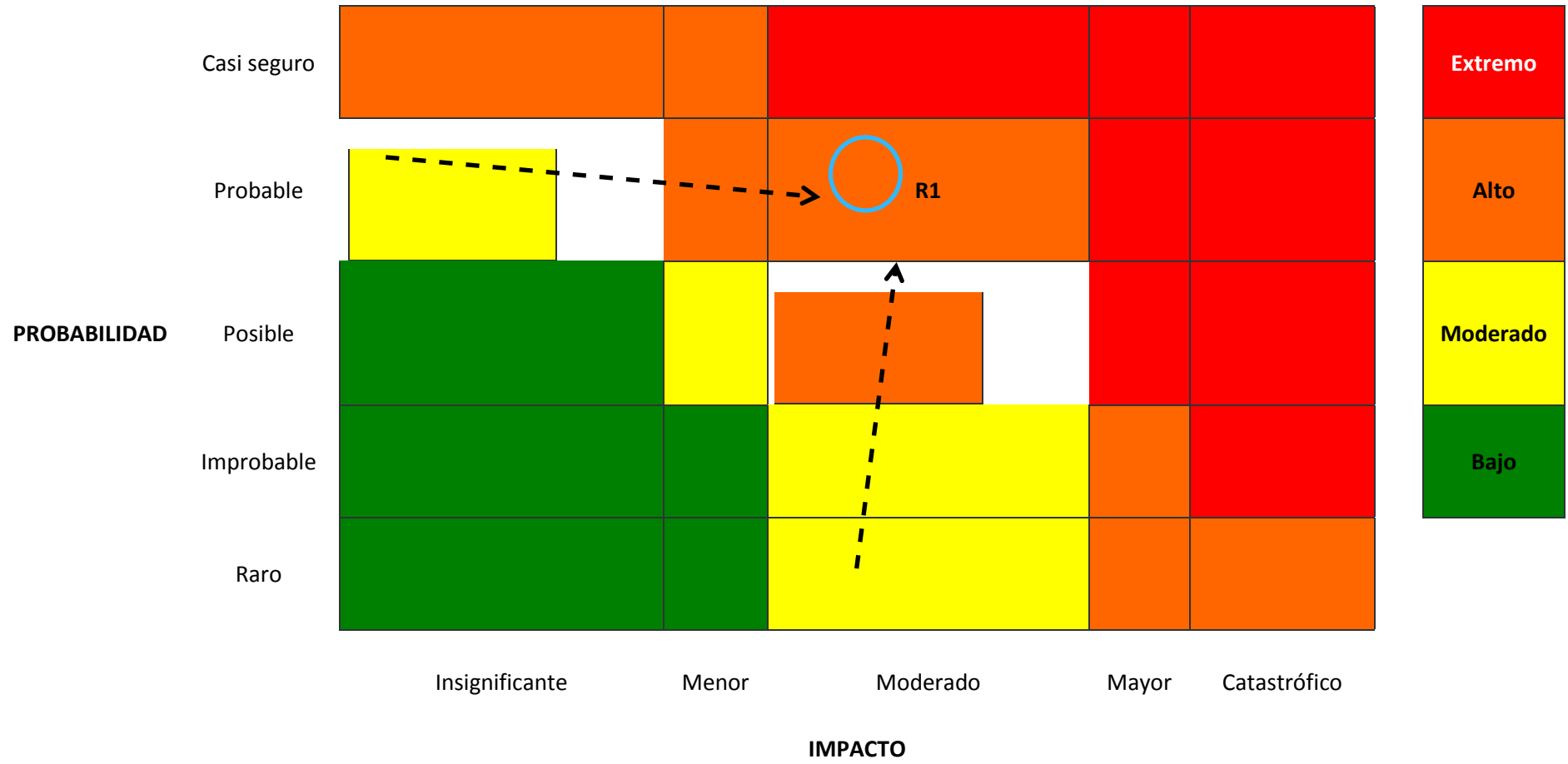
Anexo 1 Matriz de riesgos de la Dirección de Seguridad Informática

Matriz de riesgos y controles							
No.	Macroproceso / Servicio	Proceso / Producto	ACTIVO	Descripción del riesgo	Tipo de Riesgo	Causas	Factor del Riesgo Externo
R1	Coordinación Técnica de Innovación Tecnológica	Dirección de Seguridad Informática	APLICATIVOS DE COMPRAS PÚBLICAS (SOCE, CATALOGO ELECTRÓNICO, SICM,SICAE)	Probabilidad de perder el servicio por fallo tecnológico.	Tecnológico	Presencia de posibles conexiones entre la red corporativa e internet, que se encuentren fuera de las políticas de Seguridad del SERCOP.	Social
						Falta de oportunidad de poder compartir en forma segura y ágil las aplicaciones, archivos y equipos entre todas las ubicaciones del SERCOP.	Tecnológico
						Indisponibilidad de información necesaria y permitida a usuarios, dispositivos y entidades autorizadas.	Cultural
						Falta de comunicación segura en interconexiones entre empresas y falta de alcance entre redes para usuarios finales.	Político
R2			APLICATIVOS Y SALIDA A INTERNET DE USUARIOS DE LA INSTITUCIÓN	Probabilidad de que se filtre información sensible o privada a personas y entidades que no deberían tener acceso a ella.	Tecnológico	Falta de control de acceso en una red informática para proteger a los sistemas de posibles ataques y abusos	N/A
						La falta de visibilidad y control sobre usuarios y sus aplicaciones	
						La falta de administración de usuarios, grupos de usuarios, permisos y asignaciones de recursos y políticas de acceso a equipos de red, el no saber gestionar su inicio de sesión en equipos conectados, así como también sus políticas.	N/A
						No poder detectar o remediar software malicioso en los dispositivos informáticos y sistemas del SERCOP.	
ASESORÓ: DSI		ELABORÓ: SERGIO TOAPANTA					

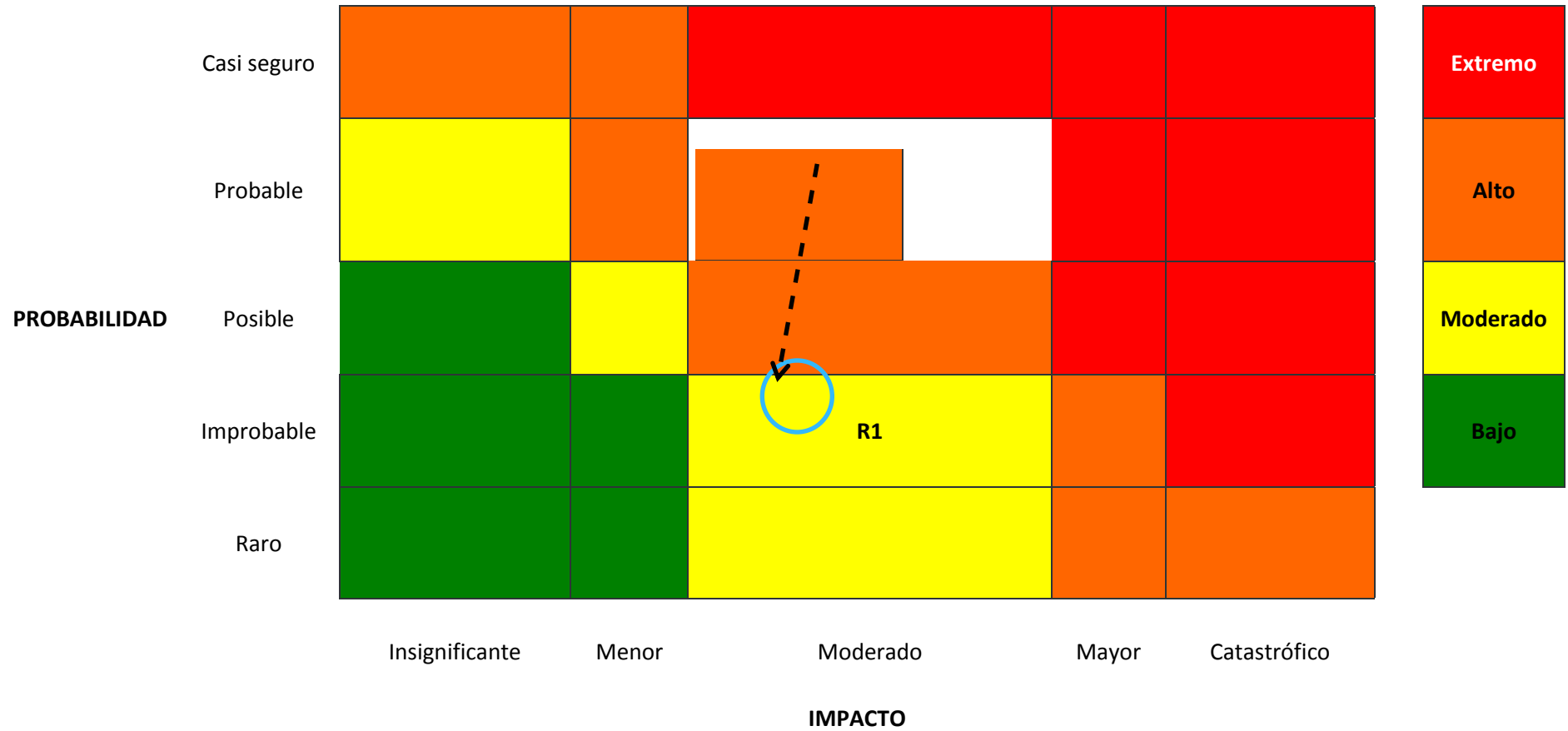
Módulo SIG Planes de Mejoramiento

Factor del Riesgo Interno	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Frecuencia	Plan de Mejoramiento (CONTROL QUE VAN A IMPLEMENTAR O RENOVAR)		
N/A	Probable	Mayor	Alto	Firewall Perimetral;	Permanente	Firewall Perimetral;		
N/A				VPN IPSec, con cualquier plataforma.	Cuando se requiera	VPN IPSec, con cualquier plataforma.		
N/A				Soporte de alta disponibilidad (activo-pasivo).	Permanente	Soporte de alta disponibilidad (activo-pasivo).		
N/A				VPN SSL.	Cuando se requiera	VPN SSL.		
Procesos y procedimientos		Moderado		IPS.	Permanente	IPS.		
				Control de aplicaciones.	Permanente	Control de aplicaciones.		
Recursos humanos				Conectividad del Directorio Activo.	Permanente	Conectividad del Directorio Activo.		
Sistemas de información				Antimalware.	Permanente	Antimalware.		
ASESORÓ: DSI ELABORÓ: SERGIO TOAPANTA								

Mapa de Riesgo Inherente



Mapa de Riesgo Residual



Anexo 2 Proformas equipos

RADICAL: Oferta Descriptiva: SOLUCIÓN NEXT GENERATION FIREWALL PALO ALTO NETWORKS

6. PROPUESTA ECONÓMICA:

ITEM	DESCRIPCIÓN	CANT.	PRECIO UNITARIO	PRECIO TOTAL
PALO ALTO NETWORKS				
1	Palo Alto Networks Perpetual Bundle (BND2) for VM-Series that includes VM-100, Threat Prevention, PANDB URL filtering, Global Protect and WildFire subscriptions, and Premium Support, 3 year 7x24 con la fabrica.	4	\$ 10.000,00	\$ 40.000,00
2	Panorama central management software, 25 devices	1	\$ 12.000,00	\$ 12.000,00
3	Premium support 3 year prepaid , Panorama 25 devices, 3 year 7x24 con la fabrica.	1	\$ 5.000,00	\$ 5.000,00
4	Servidores recomendados por la fabrica con 8 INTERFACES COBRE	4	\$ 6.000,00	\$ 24.000,00
5	VMware vSphere Enterprise Plus	4	\$ 8.500,00	\$ 34.000,00
6	Instalación, Soporte 7x24x365, Soporte N1 via SOC primer Año, 2 Mantenimientos preventivos	1	\$ 2.000,00	\$ 2.000,00
TOTAL AÑO 1				\$ 117.000,00
ARRENDAMIENTO AÑO 2				
7	Soporte de la Solucion de Firewall	1	\$ 2.000,00	\$ 2.000,00
ARRENDAMIENTO AÑO 3				
8	Soporte de la Solucion de Firewall	1	\$ 2.000,00	\$ 2.000,00
TOTAL GENERAL (Antes de IVA)				\$ 121.000,00

EBTEL: Solución Check Point

Inversión a 1 año de solución Check Point

#	Descripción	Cant	Precio Unit	Precio Tot
1	Appliances Check Point 5600 en Clúster con suscripción Next Generation Threat Prevention por 1 año	2	\$ 33.000,00	\$ 66.000,00
2	Appliances Check Point 5600 en Clúster con suscripción Next Generation Firewall por 1 año	2	\$ 33.000,00	\$ 66.000,00
3	Appliance de Check Point Smart-1 410, con funcionalidades de gestión, logs y reportes por 1 año	1	\$ 17.000,00	\$ 17.000,00
4	Soporte Colaborativo con Check Point, con vigencia de 1 año	1	\$ 13.000,00	\$ 13.000,00
5	Servicio técnico eBTel: <ul style="list-style-type: none"> • Instalación, configuración, migración y puesta en producción. • Soporte 24x7x365 UIO durante 12 meses • Mantenimiento preventivo semestral • Paquete de 10 hrs totales para nueva configuración durante los 12 meses • Transferencia de conocimientos no oficial para 3 personas, duración 48 horas 	1	\$ 12.000,00	\$ 12.000,00
Subtotal General sin IVA			\$ 174.000,00	

DIGIWARE: Next Generation Firewall



DIGIWARE SEGURIDAD DE ECUADOR
IGNACIO SAN MARIA ES 30 Y NUNEZ DE VELA
Tel: + 593 6044110
www.digiware.net

COTIZACION No.	1.1
Fecha de Cotización	20/06/2018

EMPRESA	SERCOP		
ATENCIÓN	Nombre: Francisco Barros Cargo: Director de Seguridad	Teléfono: 022440050 Ext.1475 E-mail: francisco.barros@sercop.gob.ec	

Cambio de plataforma 5600, cambio de managment, por 1 año				
Referencia	Productos	Cantidad	Precio Unitario	Precio Total
CPAP-SC5600-NCTP	5600 Next Generation Threat Prevention Appliance	2	\$ 31.402,02	\$ 62.804,04
CPAP-SC5600-NCTP-HA	5600 Next Generation Threat Prevention Appliance for High Availability	2	\$ 25.121,62	\$ 50.243,23
CPAC-PSU-5600/5800	Additional/Replacement AC Power Supply for 5600 and 5800 appliances	4	\$ 2.165,66	\$ 8.662,63
CPSB-MOB-50	Mobile Access Blade for 50 concurrent connections	1	\$ 1.459,11	\$ 1.459,11
CPSB-MOB-50-HA	Mobile Access Blade for 50 concurrent connections - HA	1	\$ 1.165,39	\$ 1.165,39
CPSM-NGSM5	Next Generation Security Management Software for 5 gateways (SmartEvent & Compliance 1 year)	1	\$ 5.590,10	\$ 5.590,10
CPSM-NGSM5-EVNT	Next Generation Security Management SmartEvent dedicated Server for 5 gateways (perpetual)	1	\$ 5.590,10	\$ 5.590,10
CPCE-SO-STANDARD-ADD	Standard Collaborative Enterprise Support For 1 Year	1	\$ 16.957,18	\$ 16.957,18
server HP	Servidor DL360 o DL380, Cen 9 o Gen 10 de minimo 1 procesador con 10 cores, 64 GB en RAM , almacenamiento de 2 TB, tarjeta de 4 puertos 1GB cobre, fuente redundante AC 100-250 V, tarjeta 811546-	2	\$ 6.666,67	\$ 13.333,33
			Subtotal	\$ 165.805,12
			Iva (12%)	\$ 19.896,61
			TOTAL PRODUCTOS	\$ 185.701,73

CNT: Next Generations Firewall Palo Alto Networks

PROPUESTA ECONOMICA Y CONSIDERACIONES

3.1 VALOR DE LA INVERSIÓN

En base al alcance detallado en el ítem 2 por el cliente SERCOP para contratación de servicios de seguridad, se presenta la propuesta económica como datos referenciales.

Pago Mensual

DESCRIPCION DE LA OFERTA	DOS AÑOS
	PAGO MENSUAL
NEXT GENERATION FIREWALL SERCOP - V AMBIENTE VIRTUAL	\$ 10.267,36

Valores sin impuestos

Pago Bajo Demanda

SERVICIO	HORAS	VALOR UNITARIO	OBSERVACIÓN
HORAS DE SOPORTE TÉCNICO ESPECIALIZADO	20	\$ 85,00	Bajo demanda requerido inicial mínimo 20 horas

Valores sin impuestos

Anexo 3 Tabla comparativa de herramientas Check Point y paloalto Networks

Tabla Comparativa de características entre Check Point y paloalto Networks			
	Características	Check Point	paloalto Networks
<i>Gateway security</i>	Administración Centralizada	SI	SI
<i>Gateway security</i>	Previsión de Intrusos (IPS)	SI	SI
<i>Gateway security</i>	Identificación por usuarios	SI	SI
<i>Gateway security</i>	Control de aplicaciones por capas	NO	SI
<i>Gateway security</i>	Control de URL	SI	SI
<i>Gateway security</i>	Antivirus / Antimalware WILDFIRE	NO	SI
<i>Gateway security</i>	NATs dinámicos y estáticos	SI	SI
<i>Gateway security</i>	Portal Cautivo	SI	SI
<i>Gateway security</i>	Integración Nativa con Active Directory, LDAP, RADIUS, TACAC, KERBEROS.	NO	SI
<i>Gateway security</i>	Clústering	SI	SI
<i>Gateway security</i>	QoS	SI	SI
<i>Gateway security</i>	Escaneo de virus y bloquearlos en al menos los siguientes protocolos: POP3, FTP, SMTP y HTTP	SI	SI
<i>Gateway security</i>	Inspección de tráfico encriptado HTTPS tanto Inbound como Outbound sin agente	NO	SI
<i>Gateway security</i>	Habilidad de analizar y detectar código malicioso (malware) en documentos como Adobe PDFs y archivos de Microsoft Office, así como también archivos EXE y Zip	SI	SI
<i>Gateway security</i>	Base de datos de inteligencia al menos 100 millones de direcciones para descubrimiento de bots, que incluyan al menos, de: direcciones IP de Command and Control, URL y DNS	NO	SI
<i>Gateway security</i>	Sandboxing para Protección contra ataques de día cero	NO	SI
<i>Gateway security</i>	Funcionalidades de VPN por IPSec	SI	SI
<i>Gateway security</i>	VPN SSL	SI	SI
<i>Gateway security</i>	VPN SSL sin necesidad de instalar cliente	NO	SI
<i>Gateway security</i>	Compatible con VMWare	SI	SI
Gestión centralizada	Administración Centralizada	SI	SI
Gestión centralizada	Al menos 5 dominios de gestión	SI	SI
Gestión centralizada	Debe poderse configurar límites que tomen acciones cuando sean superados. Las acciones deben incluir: Log, alert, send an SNMP trap, send an email y execute a user defined alert.	SI	SI

Gestión centralizada	Monitoreo de forma automática y en tiempo real la infraestructura de gateways de seguridad de red buscando el cumplimiento de estándares regulatorios internacionales y mejores prácticas de seguridad.	NO	SI
Gestión logs	Almacenamiento de logs de todos los gateways.	NO	SI
Gestión logs	Los logs se pueden exportar en formato de base de datos	SI	SI
Gestión logs	Captura de paquetes automáticamente de paquetes IPS, para análisis forense	SI	SI
Correlacionador de eventos y de reportes avanzados	Correlación de eventos de seguridad centralizada de todos los gateways de seguridad.	NO	SI
	Reportes avanzados de seguridad.	SI	SI
	Reportes centralizados de toda la solución.	SI	SI
	Visualización de eventos de seguridad en tiempo real.	SI	SI
	Geolocalización de eventos en mapa	SI	SI
	Acciones automáticas para detener o mitigar actividad maliciosa	NO	SI
	Capacidad de generar reportes de eventos de seguridad en formato HTML, PDF, CSV	NO	SI



Manual de usuario:
Administración de herramienta paloalto NETWORKS

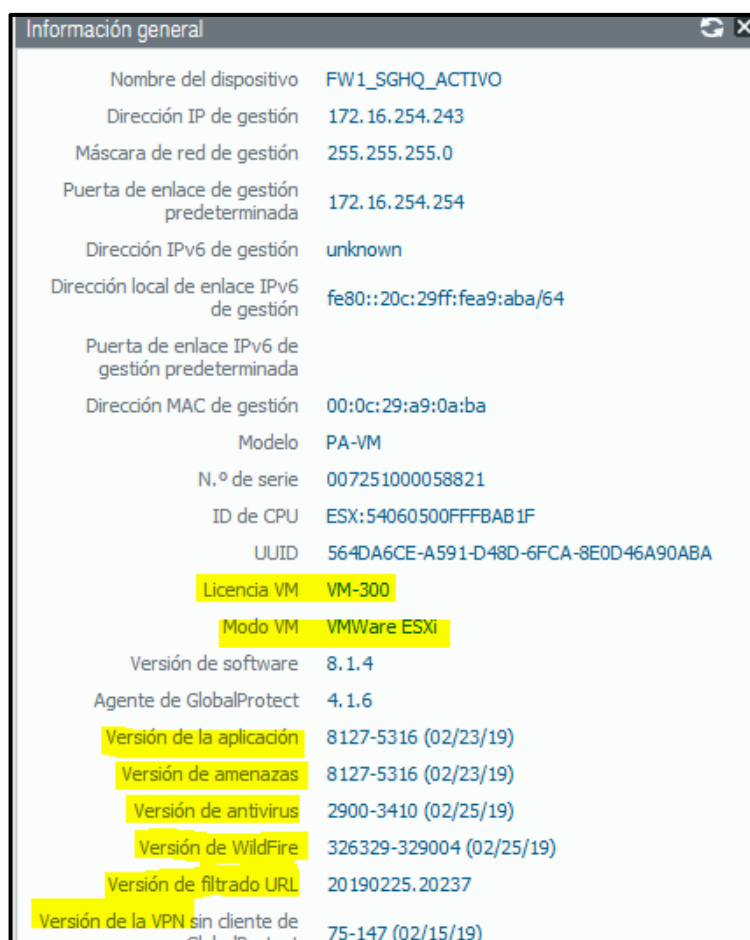
Autor: Sergio Toapanta

Quito - Ecuador
2019

Manual de Usuario

1. Descripción General

El sistema está diseñado para mejorar la protección de la información general de la institución. Al implementar un firewall perimetral sobre servidores virtuales tenemos la facilidad de aumentar su capacidad cuando lo necesitemos debido al aumento de tráfico generado por los usuarios. En la figura 1 se puede observar las características generales de la solución:



Información general	
Nombre del dispositivo	FW1_SGHQ_ACTIVO
Dirección IP de gestión	172.16.254.243
Máscara de red de gestión	255.255.255.0
Puerta de enlace de gestión predeterminada	172.16.254.254
Dirección IPv6 de gestión	unknown
Dirección local de enlace IPv6 de gestión	fe80::20c:29ff:fea9:aba/64
Puerta de enlace IPv6 de gestión predeterminada	
Dirección MAC de gestión	00:0c:29:a9:0a:ba
Modelo	PA-VM
N.º de serie	007251000058821
ID de CPU	ESX:54060500FFFBAB 1F
UUID	564DA6CE-A591-D48D-6FCA-8E0D46A90ABA
Licencia VM	VM-300
Modo VM	VMWare ESXi
Versión de software	8.1.4
Agente de GlobalProtect	4.1.6
Versión de la aplicación	8127-5316 (02/23/19)
Versión de amenazas	8127-5316 (02/23/19)
Versión de antivirus	2900-3410 (02/25/19)
Versión de WildFire	326329-329004 (02/25/19)
Versión de filtrado URL	20190225.20237
Versión de la VPN sin cliente de GlobalProtect	75-147 (02/15/19)

Figura 1. Información general

Fuente: Elaborado por el autor

Este sistema cuenta con una interfaz web desde donde se puede configurar, crear políticas, crear permisos, bloqueos y aplicar perfiles de protección según las necesidades. En la Figura 2 se muestra la interfaz del firewall paloalto Network.

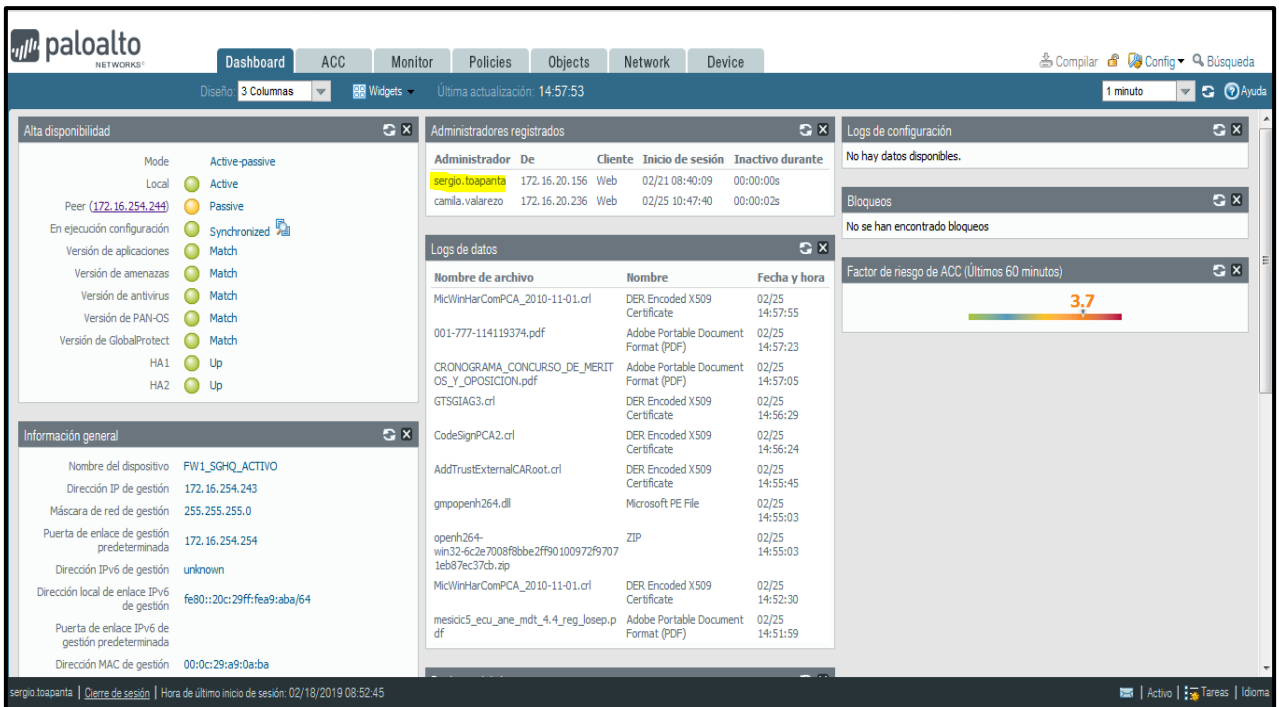


Figura 2. Interfaz web dashboard PAN

Fuente: Elaborado por el autor

Para acceder a la administración de la herramienta se debe acceder con un usuario y contraseña como se muestra en la figura 3 la interfaz de inicio de sesión.



Figura 3. Interfaz de inicio de sesión PAN

Fuente: Elaborado por el autor.

2. Especificaciones técnicas

La solución tiene las siguientes especificaciones técnicas que se muestran a continuación en la tabla 1:

Tabla 1. Especificaciones Técnicas

Tipo:	Descripción:
Software	Palo Alto Networks Perpetual Bundle (BND2) for VM-Series that includes VM-300, Threat Prevention, PANDB URL filtering, Global Protect and WildFire subscriptions.
Hardware	Servidores Dell Gen10, 8 interfaces, 16 GB RAM, SSD 480, 8 CORE.

Fuente: Elaborado por el autor

3. Indicaciones generales para su administración

Las consideraciones generales para su administración son las siguientes:

- Para acceder a la interfaz de administración se debe considerar los permisos concedidos y autorizados por el inmediato superior.
- En la interfaz de administración existe un módulo de monitoreo (Monitor) donde se puede observar en tiempo real si existe algún bloqueo de servicios, urls, o servidores, por lo que se puede adelantar a revisar ese modulo, como se muestra en la figura 4.
- Todas las configuraciones y reglas creadas están replicadas en el firewall pasivo.
- La posición de la regla tienen mucho que ver para la efectividad de su funcionamiento tanto en bloqueo y permiso.

Fecha de registro	Categoría	Acción	URL	Zona Origen	Zona Destino	IP Origen	Usuario de origen	IP Destino	Aplicación	Regla	Encabezado
02/25 12:39:21	computer-and-internet-info	alert	push.services.mozilla.c...	RED_TELEGRAFO	INTERNET_TELEGRAFO	172.18.8.5		34.208.211.12	ssl	NAV_BASICA	
02/25 12:39:19	computer-and-internet-info	alert	detectportal.firefox.co...	RED_TELEGRAFO	INTERNET_TELEGRAFO	172.18.8.5		186.47.206.185	web-browsing	NAV_BASICA	
02/25 12:39:16	computer-and-internet-info	alert	detectportal.firefox.co...	RED_TELEGRAFO	INTERNET_TELEGRAFO	172.18.8.5		186.47.206.185	web-browsing	NAV_BASICA	
02/25 12:39:15	computer-and-internet-info	alert	detectportal.firefox.co...	RED_TELEGRAFO	INTERNET_TELEGRAFO	172.18.8.5		186.47.206.185	web-browsing	NAV_BASICA	
02/25 12:39:15	computer-and-internet-info	alert	www.msftconnecttest...	RED_TELEGRAFO	INTERNET_TELEGRAFO	172.18.8.5		13.107.4.52	web-browsing	NAV_BASICA	
02/25 12:36:39	computer-and-internet-info	alert	ssl.gstatic.com/	RED_TELEGRAFO	INTERNET_TELEGRAFO	172.18.8.5		172.217.1.99	google-base	NAV_BASICA	

Figura 4. Interfaz de monitoreo

Fuente: Elaborado por el autor

4. Creación y configuración de reglas de seguridad

En la interfaz en la parte superior derecha se puede observar el módulo de políticas (*Políticas*) como se muestra en la figura 5. En este módulo se procede a crear bloqueos, permisos, accesos tanto de navegación así como también de accesos a la infraestructura tecnológica. En la misma interfaz tenemos la opción de NAT ahí es donde configuramos o creamos reglas que nos ayuden a proteger nuestras IP internas que estarán expuestas al público con algún servicio. Otra de las opciones que se puede emplear es la de QoS (Calidad de Servicio) con estas reglas se ayuda a priorizar el consumo de ancho de banda en aplicaciones o lugares que requieren más atención o criticidad.

Nombre	Etiquetas	Tipo	Zona	Dirección	Usuario	Perfil HIP	Zona
1 Bloqueo_Streaming	none	universal	any	any	any	any	any
2 test team viewer	none	universal	[[[DATOS_SERCOP_...	172.16.110.0/24	any	any	any
3 Bloqueo_SPAM	none	universal	any	any	any	any	[[[INTERNET_TELEGRAFO
4 Rastreo Satelital	none	universal	any	any	any	any	[[[INTERNET_TELEGRAFO
5 Entrada_Webchat	none	universal	[[[INTERNET_TELEG...	any	any	any	[[[RED_TELEGRAFO

Figura 5. Interfaz de políticas, NAT, QoS

Fuente: Elaborado por el autor

5. Accesos VPN

La herramienta también permite la creación de usuarios para acceso VPN, para ellos se dirige a la interfaz de Device donde se puede crear usuarios con el formato establecido ejemplo (sergio.toapanta) a continuación deben ingresar un usuario y contraseña. En la Figura 6 se muestra la interfaz y ejemplo de usuarios.

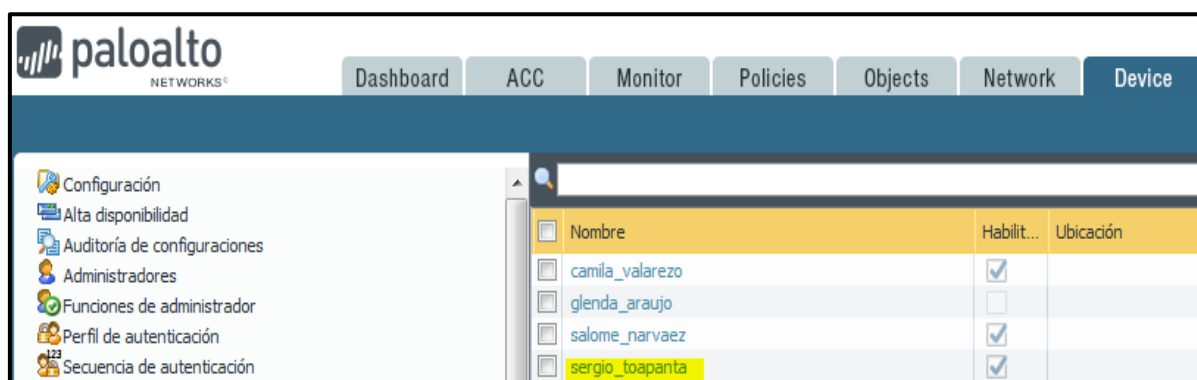


Figura 6. Interfaz de creación de usuario VPN

Fuente: Elaborado por el autor

6. Detección y solución de problemas

En la tabla 2 se detallan los posibles errores o problemas más comunes que pueden surgir, junto con la forma de solucionarlos.

Tabla 2 Detección y solución de problemas

Problema	Solución
Acceso remoto a los equipos	Revisar puerto 3389 habilitado en el firewall.
No accede a redes sociales	Revisar permisos en perfiles de navegación
No accede a Youtube	Revisar accesos streaming.
No accede por VPN	Revisar usuario y contraseña de acceso habilitado.
No conexión de directorio activo	Revisar comunicaciones entre zonas y servidores.
No accede pese a tener permisos	Revisar alertas de malware y añadir a excepciones de ser una página válida.
No hay ping hacia lo equipos	Revisar enlaces y comunicación de infraestructura.

Fuente: Elaborado por el autor

Anexo 5 Cronograma de actividades

