



FACULTAD DE INGENIERÍA

Carrera de Ingeniería de Sistemas Computacionales

“IMPLEMENTACIÓN DE OPNSENSE COMO PLATAFORMA DE ACCESO REMOTO SEGURO EN EL CONGRESO DE LA REPÚBLICA, LIMA 2020”

Trabajo de suficiencia profesional para optar el título profesional de:

Ingeniero de Sistemas Computacionales

Autor:

Emilio Alberto Cobos Benavides

Asesor:

Ing. Eduardo Martín Reyes Rodríguez

Lima - Perú

2021

TABLA DE CONTENIDOS

DEDICATORIA	2
AGRADECIMIENTO	3
ÍNDICE DE TABLAS	5
ÍNDICE DE FIGURAS	6
RESUMEN EJECUTIVO	12
CAPÍTULO I. INTRODUCCIÓN	13
CAPÍTULO II. MARCO TEÓRICO.....	22
CAPÍTULO III. DESCRIPCIÓN DE LA EXPERIENCIA.....	56
CAPÍTULO IV. RESULTADOS.....	168
CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES.....	197
REFERENCIAS	202
ANEXOS	207

ÍNDICE DE TABLAS

Tabla 1 Comparación de protocolos VPN	30
Tabla 2 Lista de plataformas de seguridad a evaluar	69
Tabla 3 Evaluación de plataformas de seguridad	70
Tabla 4 Evaluación de alternativas de conectividad de OPNsense.....	84
Tabla 5 Configuración de red de la plataforma OPNsense.....	88
Tabla 6 Rutas estáticas en OPNsense	88
Tabla 7 Gateways en OPNsense.....	89
Tabla 8 Rutas estáticas en Firewall Perimetral.....	89
Tabla 9 Características técnicas de servidor.....	93
Tabla 10 Parámetros y valores para creación de Autoridad de Certificación	116
Tabla 11 Parámetros y valores para creación de Certificado de Servidor	118
Tabla 12 Parámetros y valores para creación de Certificado de Servidor	122
Tabla 13 Parámetros y valores para creación de Certificado de Servidor	125
Tabla 14 Valores para configurar Servidor VPN para clientes de escritorio.....	135
Tabla 15 Valores para configurar un nuevo CSO.....	142
Tabla 16 Valores para configurar Servidor VPN para clientes móviles Android.....	145
Tabla 17 Parámetros para exportar cliente	159
Tabla 18 Clientes VPN de escritorio conectados a las 17:20 del día 2/9/2021.....	180
Tabla 19 Clientes VPN de teléfonos móviles conectados a las 17:20 del día 2/9/2021.....	183
Tabla 20 Muestreo de conexiones de usuarios de escritorio VPN concurrentes	192
Tabla 21 Muestreo de conexiones de usuarios VPN Android concurrentes.....	195

ÍNDICE DE FIGURAS

Figura 1 Palacio Legislativo	14
Figura 2 Hemiciclo de Sesiones	17
Figura 3 Organigrama del Congreso - Estructura Principal.....	20
Figura 4 Organigrama del Congreso - Dirección General Parlamentaria	21
Figura 5 Organigrama del Congreso - Dirección General Administrativa	21
Figura 6 Esquema básico de Acceso Remoto Seguro mediante VPN	22
Figura 7 Niveles de amenazas detenidas por soluciones Antivirus / EDR	27
Figura 8 Diagrama típico de una conexión VPN	29
Figura 9 Esquema típico de una VPN de Acceso Remoto Clientes hacia un sitio remoto	33
Figura 10 Esquema típico de VPN Site to Site - Conexión de un sitio a otro sitio remoto	34
Figura 11 Ejemplo de proceso de Autenticación y Autorización con LDAP	35
Figura 12 Autenticación Multifactor: algo que sabes + algo que tienes/eres	37
Figura 13 Logo de OPNsense.....	40
Figura 14 Reglas de firewall para interface OpenVPN	41
Figura 15 Servidores de autenticación LDAP y local.....	41
Figura 16 Ejemplo de lista de usuarios.....	42
Figura 17 Autoridad de Certificación (CA).....	43
Figura 18 Ejemplo de certificados generados.....	43
Figura 19 Servidores VPN OpenVPN en servicio.....	44
Figura 20 Consola del sistema (Dashboard).....	45
Figura 21 Sesión de Comisión de Fiscalización en Microsoft Teams	58
Figura 22 Vista frontal de servidor IBM x3850	61
Figura 23 Conexiones LAN del servidor IBM x3850	62
Figura 24 Rack de servidores y comunicaciones del Centro de Datos Edificio LAS	62
Figura 25 Consola de administración de Antivirus TrendMicro	64
Figura 26 Cliente antivirus TrendMicro OfficeScan	64

Figura 27 Pantalla de administración de MDM Samsung KnoxManage.....	65
Figura 28 Pantalla de cliente MDM en teléfono Android.....	66
Figura 29 Esquema de la prueba de concepto.....	73
Figura 30 Pantallas de las 3 máquinas virtuales	74
Figura 31 Configuración vía web de OPNsense	75
Figura 32 Prueba de conexión VPN en PC externa	76
Figura 33 Acceso remoto a la PC interna desde la PC externa vía VPN	76
Figura 34 Coordinaciones con el Jefe de Infraestructura Tecnológica	78
Figura 35 Esquema de red del Congreso	79
Figura 36 Alternativa 1 OPNsense detrás de firewall perimetral	81
Figura 37 Alternativa 2 OPNsense delante de firewall perimetral	82
Figura 38 Alternativa 3 conexión OPNsense directa a la LAN	83
Figura 39 Esquema de red final	86
Figura 40 Grupo de Active Directory OpenVPN	92
Figura 41 Configuración de vSwitch WAN	94
Figura 42 Configuración de vSwitch DMZ_VPN	94
Figura 43 Configuración de vSwitch ADM.....	94
Figura 44 Balanceador de líneas de internet Peplink Balance 13500.....	95
Figura 45 Configuración de NAT para IP público.....	96
Figura 46 Asociación de IP NAT a público.....	96
Figura 47 Reglas de Firewall Fortigate	97
Figura 48 Rutas estáticas en firewall Fortigate.....	97
Figura 49 Firewall Checkpoint (antes de retirarlo de servicio)	98
Figura 50 Firewall Fortinet Fortigate (nuevo equipamiento).....	98
Figura 51 Configuración de máquina virtual en VMware ESXi	101
Figura 52 Pantalla inicial de OPNsense CLI	101
Figura 53 Ventana de bienvenida	102
Figura 54 Configuración de teclado y fuente de texto.....	103
Figura 55 Selección de tipo de instalación	103

Figura 56 Selección de disco duro.....	104
Figura 57 Selección de tipo de sector de arranque	104
Figura 58 Selección de tamaño de partición Swap	105
Figura 59 Pantalla de ingreso de contraseña para usuario root.....	105
Figura 60 Pantalla de mensaje de reinicio	106
Figura 61 Pantalla de arranque inicial	106
Figura 62 Menú principal de interface de línea de comando (CLI).....	107
Figura 63 Pantalla de ingreso de interface web	108
Figura 64 Asistente de configuración inicial	108
Figura 65 Asistente de configuración: Información general.....	109
Figura 66 Asistente de configuración: servidor de tiempo	110
Figura 67 Selección de tipo de configuración de IP WAN.....	110
Figura 68 Ingreso de IP WAN.....	110
Figura 69 Selección de bloqueo de redes.....	111
Figura 70 Ingreso de IP LAN	111
Figura 71 Cambio de contraseña inicial	112
Figura 72 Recarga de configuración.....	112
Figura 73 Pantalla después de recargar configuración por primera vez	113
Figura 74 Consola principal de OPNsense	113
Figura 75 Gateways.....	114
Figura 76 Rutas a redes y servidores	115
Figura 77 Creación de Autoridad de Certificación	116
Figura 78 Pantalla de parámetros de nueva Autoridad de Certificación.....	117
Figura 79 Lista de Autoridades de Certificación	118
Figura 80 Ventana de listas de certificados con el certificado web por omisión.....	118
Figura 81 Pantalla 1 de parámetros de nuevo certificado de servidor	119
Figura 82 Pantalla 2 de parámetros de nuevo certificado de servidor	120
Figura 83 Lista de certificados con nuevo certificado de servidor	120
Figura 84 Configuración de servidor de autenticación (parte 1)	123

Figura 85 Configuración de servidor de autenticación (parte 2)	123
Figura 86 Configuración de servidor de autenticación (parte 3)	124
Figura 87 Lista de servidores de autenticación.....	124
Figura 88 Configuración de servidor de autenticación (parte 1)	126
Figura 89 Configuración de servidor de autenticación (parte 2)	127
Figura 90 Lista de servidores de autenticación con tres servidores.....	127
Figura 91 Importación de usuarios	128
Figura 92 Selección de usuarios LDAP a importar	129
Figura 93 Usuarios importados.....	130
Figura 94 Creación de certificado de usuario	131
Figura 95 Pantalla de creación de certificado de usuario (parte 1).....	131
Figura 96 Pantalla de creación de certificado de usuario (parte 2).....	132
Figura 97 Retorno a pantalla de lista de usuarios	132
Figura 98 Creación de código QR para TOTP	133
Figura 99 Mostrar código QR.....	133
Figura 100 Código QR para TOTP.....	134
Figura 101 Prueba de autenticación de usuario	135
Figura 102 Configuración de servidor VPN para clientes de escritorio (parte 1).....	137
Figura 103 Configuración de servidor VPN para clientes de escritorio (parte 2).....	138
Figura 104 Configuración de servidor VPN para clientes de escritorio (parte 3).....	138
Figura 105 Configuración de servidor VPN para clientes de escritorio (parte 4).....	139
Figura 106 Configuración de servidor VPN para clientes de escritorio (parte 5).....	140
Figura 107 Configuración de servidor VPN para clientes de escritorio (parte 6).....	140
Figura 108 Servidor VPN para clientes de escritorio creado.....	141
Figura 109 Agregar un CSO	142
Figura 110 Cálculo de subred para los clientes VPN de escritorio.....	143
Figura 111 Rango de subred para CSO del primer usuario VPN de escritorio.....	143
Figura 112 Configuración de CSO para primer usuario VPN de escritorio.....	144
Figura 113 Rango de subred para CSO del segundo usuario VPN de escritorio	144

Figura 114 Configuración de CSO para segundo usuario VPN de escritorio.....	145
Figura 115 Servidor SSL VPN para dispositivos Android.....	147
Figura 116 Creación de Alias para puertos VPN externos.....	148
Figura 117 Creación de regla de acceso WAN.....	149
Figura 118 Aplicar cambios en Firewall.....	150
Figura 119 Regla permisiva en interface OPT1.....	150
Figura 120 Creación de alias RANGO_VPN_DESKTOP.....	152
Figura 121 Creación de alias SERVIDORES_CONGRESO.....	152
Figura 122 Creación de alias PUERTOS_WEB_SERVERS_CONGRESO.....	153
Figura 123 Creación de regla de firewall para acceso a servidores (parte 1).....	154
Figura 124 Creación de regla de firewall para acceso a servidores (parte 2).....	154
Figura 125 Creación de alias ecobos_vpn.....	156
Figura 126 Creación de alias ecobos_pc.....	156
Figura 127 Creación de regla de firewall para acceso a escritorio remoto (parte 1).....	157
Figura 128 Creación de regla de firewall para acceso a escritorio remoto (parte 2).....	158
Figura 129 Reglas de acceso a consola web por omisión.....	159
Figura 130 Pantalla de exportación de archivo de configuración de usuario.....	160
Figura 131 Descarga de cliente OpenVPN.....	161
Figura 132 Instalación de cliente OpenVPN (paso 1).....	162
Figura 133 Instalación de cliente OpenVPN (paso 2).....	162
Figura 134 Instalación de cliente OpenVPN (paso 3).....	163
Figura 135 Instalación de cliente OpenVPN (paso 4).....	163
Figura 136 Instalación de cliente OpenVPN (paso 5).....	164
Figura 137 Instalación de cliente OpenVPN (paso 6).....	164
Figura 138 Acceso directo de OpenVPN.....	165
Figura 139 Instalación de archivo de configuración de usuario.....	165
Figura 140 Conectar a VPN (paso 1).....	166
Figura 141 Conectar a VPN (paso 2).....	166
Figura 142 Evidencia de número de usuarios en grupo OpenVPN del Active Directory.....	169

Figura 143 Caso típico de acceso a recursos de la institución desde un domicilio.....	170
Figura 144 Conexión exitosa de cliente OpenVPN.....	171
Figura 145 Mensaje de conexión a VPN en Windows 10	171
Figura 146 Acceso a escritorio remoto (PC en el Congreso) desde domicilio vía VPN.....	172
Figura 147 Acceso a recurso web interno del Congreso desde domicilio vía VPN.....	173
Figura 148 Cliente OpenVPN en Android.....	174
Figura 149 Conexión OpenVPN en Android.....	174
Figura 150 Sistema de Asistencia y Votación Remota.....	175
Figura 151 Marcado de asistencia	175
Figura 152 Marcado de votación	176
Figura 153 Ejemplo de marcado de votación	176
Figura 154 Pruebas del sistema de Asistencia y Votación remota y presencial	177
Figura 155 Acceso a servidor de Base de Datos de Desarrollo vía VPN	178
Figura 156 Gráfico de conexiones concurrentes para usuarios VPN de escritorio.....	179
Figura 157 Sesiones concurrentes de congresistas con dispositivos móviles junio-julio 2021	182
Figura 158 Tráfico total de datos VPN.....	185
Figura 159 Tráfico de datos VPN de equipos de escritorio	186
Figura 160 Tráfico de datos VPN de equipos móviles	186
Figura 161 Tráfico total de internet en la institución.....	187
Figura 162 Uso de recursos computacionales.....	188
Figura 163 Detalle parcial de clientes VPN de escritorio activos en consola web OPNsense.....	189
Figura 164 Detalle parcial de clientes VPN Android activos en consola web OPNsense	190
Figura 165 Usuarios del Congreso con Acceso VPN configurado.....	191
Figura 166 Usuarios concurrentes de los últimos dos meses.....	192
Figura 167 Gráfico de dispersión de usuarios concurrentes para VPN de escritorio.....	194
Figura 168 Máximo de usuarios concurrentes de VPN Android	196

RESUMEN EJECUTIVO

A inicios del año 2020 se detectaron a nivel mundial múltiples casos del Síndrome Respiratorio Severo Agudo Coronavirus 2 (SARS-CoV-2), el que fue catalogado como pandemia denominada COVID-19 por la OMS, generando la declaración de Estado de Emergencia Sanitaria por parte del Estado Peruano.

En este escenario, con el propósito de minimizar la exposición del recurso humano al virus SARS-CoV-2, el Congreso de la República dispuso la implementación del trabajo remoto como una de las medidas para permitir el desarrollo de las labores institucionales. Uno de los retos tecnológicos que se debieron enfrentar fue habilitar el acceso remoto seguro, cuya implementación y optimización se detalla en este trabajo.

La solución de acceso remoto seguro implementada en el Congreso se basó en la plataforma de código abierto OPNsense, la que se integró a la arquitectura de conectividad y seguridad existentes en la institución. Desde su despliegue, esta solución permitió mejorar la continuidad de funciones del Congreso, al brindar acceso remoto seguro a PCs y recursos web por parte del personal del Servicio Parlamentario, así como brindar el acceso de comunicaciones para la nueva aplicación de Asistencia y Votación Remota basada en dispositivos móviles, utilizada por los Congresistas para confirmar asistencia y emitir su voto durante las sesiones remotas del Pleno del Congreso.

PALABRAS CLAVE: OPNsense, OpenVPN, acceso remoto seguro, firewall, VPN, 2FA, doble factor de autenticación, múltiple factor de autenticación, RDP.

NOTA DE ACCESO

No se puede acceder al texto completo pues contiene datos confidenciales

REFERENCIAS

Abdelmajid Lakbabi, G. O. (s.f.). *Network Access Control Technology*. Obtenido de <https://arxiv.org/ftp/arxiv/papers/1304/1304.0807.pdf>

Cisco. (s.f.). *What Is a Next-Generation Firewall?* Obtenido de <https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html>

Comodo. (2 de agosto de 2021). *Endpoint Detection and Response (EDR)*. Obtenido de <https://enterprise.comodo.com/blog/what-is-endpoint-detection-response/>

ComputerScience. (s.f.). *ComputerScience Wiki*. Obtenido de <https://computersciencewiki.org/index.php/VPN>

Congreso. (junio de 2011). *Parlamento Escolar*. Obtenido de https://www.congreso.gob.pe/Docs/participacion/parlamento-escolar/files/separata_uso_video.pdf

Congreso. (26 de mayo de 2020). *Portal del Congreso de la República*. Obtenido de https://www.congreso.gob.pe/Docs/medidas-covid19/files/acuerdo_n_028-2020-2021mesa-cr.pdf

Congreso. (s.f.). *Funciones del Congreso de la República*. Obtenido de <https://www.congreso.gob.pe/funciones/>

Congreso. (s.f.). *Misión y Visión del Congreso*. Obtenido de <https://www.congreso.gob.pe/VisionMision/>

Congreso. (s.f.). *Organización del Congreso*. Obtenido de <https://www.congreso.gob.pe/home?K=17>

DoubleOctopus. (s.f.). *The Secret Security Wiki*. Obtenido de <https://doubleoctopus.com/security-wiki/authentication/time-based-one-time-password/>

Forcepoint. (s.f.). *What is a Firewall?* Obtenido de <https://www.forcepoint.com/es/cyber-edu/firewall>

Forcepoint. (s.f.). *What is Malware?* Obtenido de <https://www.forcepoint.com/cyber-edu/malware>

Forcepoint. (s.f.). *What is Sandbox Security?* Obtenido de <https://www.forcepoint.com/es/cyber-edu/sandbox-security>

GeeksforGeeks. (26 de junio de 2018). *GeeksforGeeks*. Obtenido de <https://www.geeksforgeeks.org/computer-network-aaa-authentication-authorization-and-accounting/>

HelpSystems. (29 de diciembre de 2020). *What's the Difference Between Two-Factor Authentication and Multi-Factor Authentication?* Obtenido de <https://www.helpsystems.com/resources/articles/whats-difference-between-two-factor-authentication-and-multi-factor>

HelpSystems. (29 de diciembre de 2020). *What's the Difference Between Two-Factor Authentication and Multi-Factor Authentication?* Obtenido de <https://www.helpsystems.com/resources/articles/whats-difference-between-two-factor-authentication-and-multi-factor>

Hope, C. (6 de julio de 2021). *Virus signature*. Obtenido de <https://www.computerhope.com/jargon/v/virus-signature.htm>

IVPN. (s.f.). *Comparison of VPN protocols*. Obtenido de <https://www.ivpn.net/pptp-vs-ipsec-ikev2-vs-openvpn-vs-wireguard/>

Lord, N. (10 de setiembre de 2018). *Digital Guardian*. Obtenido de <https://digitalguardian.com/blog/what-endpoint-protection-data-protection-101>

ManageEngine. (s.f.). *Manage Engine Desktop Central*. Obtenido de <https://www.manageengine.com/products/desktop-central/endpoint-management.html>

Miradore. (8 de setiembre de 2020). *A Complete Guide to Mobile Device Management (MDM)*. Obtenido de <https://www.miradore.com/blog/mdm-mobile-device-management/>

Okta. (s.f.). *Authentication vs. Authorization*. Obtenido de <https://www.okta.com/identity-101/authentication-vs-authorization>

OPNsense. (s.f.). *OPNsense*. Obtenido de <https://opnsense.org/about/about-opnsense/>

Oracle. (s.f.). *What is IoT?* Obtenido de <https://www.oracle.com/internet-of-things/what-is-iot/>

Paessler. (s.f.). *IT Explained: Active Directory*. Obtenido de <https://www.paessler.com/es/it-explained/active-directory>

PaloAlto. (s.f.). *Endpoint detection and response*. Obtenido de <https://www.paloaltonetworks.com/cyberpedia/what-is-endpoint-detection-and-response-edr>

PaloAlto. (s.f.). *What Is a Site-to-Site VPN?* Obtenido de <https://www.paloaltonetworks.com/cyberpedia/what-is-a-site-to-site-vpn>

PaloAlto. (s.f.). *What is an Endpoint?* Obtenido de <https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint>

PCI. (s.f.). *PCI Security Standards Council.* Obtenido de <https://es.pcisecuritystandards.org/minisite/env2/>

PCMagazine. (s.f.). *PC Magazine.* Obtenido de <https://www.pcmag.com/encyclopedia/term/accountability>

Presidencia. (11 de marzo de 2020). *Diario Oficial El Peruano.* Obtenido de <https://busquedas.elperuano.pe/normaslegales/decreto-supremo-que-declara-en-emergencia-sanitaria-a-nivel-decreto-supremo-n-008-2020-sa-1863981-2/>

ProofPoint. (s.f.). *What is a Sandbox?* Obtenido de <https://www.proofpoint.com/us/threat-reference/sandbox>

Rehan, S. A. (6 de diciembre de 2020). *Remote Access VPN To Work From Home Using OpenVPN Access Server.* Obtenido de <https://nprog.medium.com/remote-access-vpn-to-work-from-home-283402bbc83>

Samsung. (s.f.). *Knox Manage.* Obtenido de <https://www.samsungknox.com/es-419/solutions/it-solutions/knox-manage>

Short, T. (13 de febrero de 2020). *Software Advice.* Obtenido de <https://www.softwareadvice.com/resources/saas-10-faqs-software-service/>

Technopedia. (29 de noviembre de 2017). *Access Control.* Obtenido de <https://www.techopedia.com/definition/5831/access-control>

Techslang. (s.f.). *What is On Premises?* Obtenido de <https://www.techslang.com/definition/what-is-on-premises/>

TechTarget. (s.f.). *TechTarget*. Obtenido de <https://searchsecurity.techtarget.com/definition/two-factor-authentication>

TechTerms. (s.f.). *Encryption*. Obtenido de <https://techterms.com/definition/encryption>

TechTerms. (s.f.). *QR Code*. Obtenido de https://techterms.com/definition/qr_code

TechTerms. (s.f.). *Remote Desktop*. Obtenido de <https://techterms.com/definition/remotedesktop>

TrendMicro. (s.f.). *Endpoint Security con Apex One*. Obtenido de https://www.trendmicro.com/es_es/business/products/user-protection/sps/endpoint.html

Varonis. (s.f.). *The Difference Between Active Directory and LDA*. Obtenido de <https://www.varonis.com/blog/the-difference-between-active-directory-and-ldap/>

VMware. (s.f.). Obtenido de <https://www.vmware.com/topics/glossary/content/secure-remote-access>

Webroot. (s.f.). *What is Antivirus Software?* Obtenido de <https://www.webroot.com/us/en/resources/tips-articles/what-is-anti-virus-software>

welivesecurity. (4 de mayo de 2017). *A short history of the computer password*. Obtenido de <https://www.welivesecurity.com/2017/05/04/short-history-computer-password/>

Wiki, C. S. (s.f.). *Computer Science Wiki*. Obtenido de <https://computersciencewiki.org/index.php/VPN>