



FIREWALL PARA CENTRO DE CONTROL NACIONAL

1. GENERALIDADES.

1.1. Objetivos

Establecer los requerimientos técnicos que deberán cumplirse para el suministro de los Firewall para su uso en Datacenter en adelante Firewall.

Detallar los factores que se deberán tener en cuenta para que el sistema soporte futuras expansiones.

2. ALCANCE DEL SUMINISTRO

EL SUMINISTRO DEBERÁ INCLUIR, MÁS NO LIMITARSE, A LOS SIGUIENTES EQUIPOS, MATERIALES Y SERVICIOS:

2.1. Cantidad de Firewalls: **2 (dos)**

2.2. Firewall conforme a lo descrito en la presente Especificación Técnica.

2.3. Servicio de Montaje y configuración (ruteo y seguridad) que garanticen la conexión de los equipos del Datacenter con la red de ANDE.

2.4. Pruebas según lo descrito en la EETT.

2.5. Documentación técnica completa para el montaje, instalación, puesta en servicio, operación y mantenimiento del sistema.

2.6. El fabricante propietario de la solución deberá contar en su portfolio global de soluciones con productos posicionados entre los líderes del cuadrante de Gartner en las categorías de Firewalls de Red o SD-WAN.

2.8. El proveedor deberá contar en su plantel técnicos certificados en el producto ofertado, los cuales deberán formar parte de la nómina con al menos 1 año. Esta antigüedad deberá ser comprobada con la documentación o constancia emitida por el IPS (Instituto de Previsión Social) o su equivalente en el país de origen del oferente, para la fase de implementación o brindar soporte local en caso de que sea requerido.

2.9. Garantía escrita de 3 años emitida por el fabricante o su representante oficial en el Paraguay por la solución ofertada. Debe incluir 36 meses de soporte local que deberá ser ejecutado por los técnicos locales certificados del oferente, incluirá acceso a actualizaciones y escalamientos posteriores, para la resolución de problemas relacionados a la solución a implementar.

2.10. El proveedor deberá presentar una carta del fabricante o su representante oficial en Paraguay, en la cual avale que el mismo se encuentra en condiciones y autorizado para la venta, instalación, configuración y soporte de la solución ofertada,

Preparado	Revisado	Aprobado	Fecha	Revisión	Observación
			24/02/2025	REV01	



- 2.11. Cursos de capacitación en los siguientes temas: montaje, configuración, ajustes, parametrización, pruebas, actualizaciones y puesta en servicio de los Firewall. El curso deberá ser con la modalidad teórico-practico, y el contenido deberá ser presentado a la ANDE para su aprobación pudiendo ANDE agregar/o sacar módulos del contenido si considera necesario. El profesional especialista que impartirá el curso deberá tener experiencia y deberá contar con certificaciones técnica del producto, equipo y sistema ofertado.

3. CARACTERÍSTICAS TÉCNICAS

3.1. Modo de Funcionamiento.

3.1.1 Los Firewalls deberán permitir el envío de paquetes entre redes (WAN/LAN) mediante Protocolos TCP/IP, a los efectos de interconectar puntos remotos transmitiendo datos. Deberán ser controlados por microprocesador, basándose en programas almacenados.

3.1.2 Los Firewalls ofertados deberán ser de la misma marca y esta condición deberá constar en los documentos técnicos entregados por el Oferente.

3.1.3 El Firewall debe soportar el Protocolo de Parallel Redundancy Protocol (PRP).

3.1.4 El Firewall debe permitir el ruteo estático, y el ruteo dinámico a través de protocolos estándares, OSPF.

3.1.5 El Firewall debe tener los siguientes servicios:

3.1.5.1 Application Control, incluyendo firmas especializadas para entornos de Tecnología Operacional (OT)

3.1.5.2 IPS (incluyendo firmas especializadas para entornos de Tecnología Operacional - OT)

3.1.5.3 Anti-Malware con capacidad de detección basada en comportamientos.

3.1.5.4 Filtrado Web, utilizando un mínimo de 90 (noventa) categorías de URLs, así como una base de datos de al menos 300 millones de URLs categorizadas.

3.1.5.5 Protección contra botnets

3.1.5.6 Filtrado y seguridad DNS.

3.1.5.7 Autenticación de usuarios a través de LDAP

3.1.5.8 Ranking de seguridad

3.1.5.9 Servicio de Seguridad Industrial

3.1.5.10 inspección profunda de paquetes (Deep Packet Inspection -DPI)

3.1.5.11 Reputación de direccion IP/dominios

3.1.6 El detalle de Configuración, arquitectura e integración deberá ser presentada a la ANDE para su evaluación antes del SOW - Statement of Work y será revisado durante el SOW para la aprobación respectiva.

Preparado	Revisado	Aprobado	Fecha	Revisión	Observación
			24/02/2025	REV01	



3.1.7 Cada firewall deberá poder integrarse al sistema centralizado de actualizaciones de firma, con las licencias necesarias para el efecto. A su vez, deben permitir el monitoreo continuo y puntuación de la configuración de este, como mínimo en las siguientes áreas:

3.1.7.1 Postura de seguridad del firewall (endurecimiento o hardening, almacenamiento de logs o logging, gestión de amenazas y vulnerabilidades, políticas y diseño de la red).

3.1.7.2 Cobertura (estado de actualización de firmware y servicios, políticas y diseño de la red).

3.2. Compatibilidad con el Sistema de Comunicación de Datos de la ANDE(Existente)

3.2.1 El equipamiento ofertado deberá ser completamente compatible a nivel de físico (interfaces físicas) y lógico (protocolos de comunicaciones, seguridad, gerenciamiento y demás softwares) con el equipamiento existente actualmente en la ANDE, compuesto básicamente por los siguientes dispositivos que operan utilizando el Protocolo de Primer Camino Más Corto (**OSPF: Open Shortest Path First**)

- Firewall marca Fortinet modelo Fortigate-300E
- Firewall marca Fortinet modelo Fortigate-400E
- Firewall marca Fortinet modelo Fortigate-VM64-KVM
- Firewall marca Fortinet modelo Fortigate-100D
- Router marca Cisco Systems modelo 3600
- Router marca Cisco Systems modelo 3845
- Router marca Cisco Systems modelo 2821
- Router marca Cisco Systems modelo 2600
- Router marca Cisco Systems modelo 1600
- Router marca Huawei modelo AR550

3.3 Condiciones Ambientales

Los Routers deberán funcionar normalmente en las condiciones ambientales detalladas a continuación:

- 3.3.1 Temperatura Operación: 0°C a 40°C
- 3.3.2 Temperatura de almacenamiento: -35°C a 70°C
- 3.3.3 Humedad 5% a 90% sin condensar

3.4 Características eléctricas y de funcionamiento.

- 3.4.1 Tensión de alimentación (AC): 100-240, 50/60Hz

Preparado	Revisado	Aprobado	Fecha	Revisión	Observación
			24/02/2025	REV01	

3.4.2 Doble entrada de alimentación.

3.5 Protocolos requeridos funciones ruteo

Los protocolos de enrutamiento que se indican a continuación son las mínimas necesarias para atender los requerimientos deseados.

3.5.1 Protocolo Internet (IP: *Internet Protocol*)

3.5.3 Protocolo Standart 802.1d Spanning Tree.

3.5.4 Protocolo de configuración dinámica de host (*DHCP: Dynamic Host Configuration Protocol*) server, cliente, relay

3.5.5 Protocolos DNS, DNS Proxy

3.5.6 Protocolos IPv4 e IPv6

3.5.7 Protocolo Open Shortest Path First (*OSPF*)

3.5.8 Protocolo de Gateway Fronterizo (*BGP: Border Gateway Protocol*)

3.5.9 Multicast Internet Group Management Protocol (*IGMPv3*)

3.5.10 Protocolo IPSec

3.5.11 Protocolo de Detección de Reenvío Bidireccional (*BFD: Bi-Directional Forwarding Detection*)

3.5.12 Protocolo de enrutamiento Primero el Camino Abierto más Corto (*OSPF: Open Shortest Path First*)

3.5.13 Protocolo de Operación de Sistema Intermedio a Sistema Intermedio (*IS-IS Protocol*)

3.5.15 Funcionalidades de SD-WAN nativas.

3.5.16 Protocolo de encapsulación Ethernet 802.1q VLAN.

3.6 Prestaciones mínimas requeridas del Firewall

Las prestaciones que se indican a continuación son las mínimas necesarias para atender los requerimientos.

3.6.1 Sistema de prevención de intrusos (IPS)

3.6.2 Interfase de túneles virtuales dinámica (VPN Dynamic Virtual Tunnel Interfaces)

3.6.3 Traducción de direcciones de red (NAT)

3.6.4 Soporte de protocolo de inicio de sesión según la prioridad (SIP)

3.6.6 Filtrado MAC

3.6.8 Encriptación estándar avanzada y Algoritmos de encriptación triple (*Triple-Data Encryption Standard Algorithm Encryption*)

3.6.9 Direccionamiento IPv4 e IPv6.

Preparado	Revisado	Aprobado	Fecha	Revisión	Observación
			24/02/2025	REV01	

- 3.6.10 Autenticación de contraseñas (*Multicast Source Discovery Protocol MD5*)
- 3.6.11 Enrutamiento Basado en Política (*Policy Based Routing*)
- 3.6.13 ICMP de limitación de rango de usuarios para retroalimentación (*Internet Control Message Protocol Unreachable Rate Limiting User Feedback*)
- 3.6.14 Protocolos de Seguridad IP: (*IPSec*) *DES* (*DES*, *3DES*), y *AES* (*AES 128*, *192*, y *256*)
- 3.6.15 Control de Aplicaciones e IPS signatures: Protocolo IEC 60870-5-104
- 3.6.16 Control de Aplicaciones e IPS signatures: Protocolo DNP3 Serial/TCP
- 3.6.17 Control de Aplicaciones e IPS signatures: IEC 60870-6 (TASE.2/ICCP)
- 3.6.18 Control de Aplicaciones e IPS signatures: ELCOM 90
- 3.6.19 Control de Aplicaciones e IPS signatures: IEC 61850 (MMS)
- 3.6.20 Control de Aplicaciones e IPS signatures: Modbus TCP
- 3.6.21 Control de Aplicaciones e IPS signatures: IEEE C37.118 Synchrophasor
- 3.6.22 Soporte de Conmutación Etiquetada de Multiprotocolos VPN (*MPLS VPN support*).
- 3.6.26 Control e Inspección de Aplicaciones Avanzadas (*Advanced Application Inspection and Control*)
- 3.6.29 Capacidad de Memoria y CPU para operación en condiciones de alta carga de procesamiento (*CPU/Memory Thresholding*)
- 3.6.30 Protocolo Simple de Administración de Redes versión 3 (*Simple Network Management Protocol Version 3 “SNMPv3”*)
- 3.6.31 Control de Admisión a la Red (*Network Admission Control “NAC”*)
- 3.6.34 Lista de control de acceso (*ACLs: Access Control List*)
- 3.6.35 Servicio Diferenciado (DiffServ)
- 3.6.36 Traffic Shaping Policies.
- 3.6.37 Enrutamiento basado en políticas (PBR)
- 3.6.38 Clase de servicio (CoS)
- 3.6.39 Acceso Remoto Seguro SSL VPN
- 3.6.40 Encriptación por Hardware (DES, 3DES, AES 128, AES 192 y AES 256)
- 3.6.41 Soporte para Infraestructura de Clave Pública (PKI)
- 3.6.42 Firewall con estado de inspección
- 3.6.43 Seguridad de HTTP (HTTPS), FTP(SFTP)
- 3.6.44 Autenticación Proxy Telnet.
- 3.6.45 Seguridad Estática y Dinámica de puerto
- 3.6.47 Funcionalidades IPv6: Mecanismos de transición a IPv6, Resolución de nombres IPv6, Arquitectura de direccionamiento IPv6, Estadísticas IPv6, ICMPv6

Preparado	Revisado	Aprobado	Fecha	Revisión	Observación
			24/02/2025	REV01	

- 3.6.48 Servicio de Autenticación, Autorización y Auditoria para seguridad de redes (*Authentication, Authorization, and Accounting "AAA"*)
- 3.6.49 Soporte de 802.1x (*IEEE 802.1x*)
- 3.6.50 Soporte de 802.3ah (*IEEE 802.3*)
- 3.6.51 Servicio de Seguridad en Redes LAN inalámbricas (*Secure Wireless LAN Services*)
- 3.6.52 Soporte de Enrutamiento entre Dominios sin Clase (*CIDR: Classless Interdomain Routing*)
- 3.6.53 Soporte de uso de Mascara de Subred de Longitud Variable (*VLSM: Variable Length Subnet Mask*)
- 3.6.54 Utilización de Ruteo Estático y Dinámico
- 3.6.55 Control de colisión (*Storm Control*)
- 3.6.56 Control de Aplicaciones
- 3.6.57 Soporte configuración en alta disponibilidad (HA- high availability) sin pérdida de datos, hot-hot y hot-standby.
- 3.6.58 MTBF - Mean Time Between Failures ≥ 180.000 Horas
- 3.6.59 Envío de logs de eventos de ciberseguridad en el portal nube(cloud) del fabricante, en una cuenta exclusiva para ANDE, donde se pueda ver y filtrar los registros anomalías como del Antivirus, de los Sistemas de Detección de Intrusos, las principales amenazas, entre otros eventos del sistema. A traves del software de administración centralizada según ítem 3.7.4
- 3.6.60 Todas las funcionalidades requeridas deberán estar activadas a nombre de ANDE, en caso que requieran algún tipo de licencia deberá estar vigente al menos tres años contados a partir de la puesta en servicio del firewall.
- 3.6.61 Deberá dar soporte del fabricante del equipo de al menos tres años contados a partir de la puesta en servicio del firewall.

3.7 Administración/Gestión/Configuración

- 3.7.1 El Firewall deberá tener la opción de poder realizar la configuración a través de los protocolos HTTPS, SSH y serial, a estos protocolos se podrá crear reglas de seguridad con usuarios y contraseñas.
- 3.7.2 La configuración, pruebas, puesta en servicio y capacitación deberán ser realizado por especialistas certificados a modo de asegurar la correcta implementación de las reglas de seguridad restrictiva, donde se permite solo el tráfico esencial y se deniega todo lo demás, esto aplica a las siete capas del modelo OSI- *Open Systems Interconnection*. En la última capa de aplicación, las funciones no utilizadas de los protocolos deberán ser bloqueadas.
- 3.7.3 La Especificación de Diseño de Ciberseguridad - EDC deberá ser presentada a la ANDE para su evaluación antes del SOW - Statement of Work, acompañado del documento de reglas a ser aplicadas, las modificaciones podrán ser realizadas a solicitud de ANDE.

Preparado	Revisado	Aprobado	Fecha	Revisión	Observación
			24/02/2025	REV01	



Una vez aprobada la EDC cualquier otra modificación que surja en el proceso deberán ser evaluados en conjunto el impacto y sus implicancias.

- 3.7.4 Para las actualizaciones de la base de datos de firmas (*signature*) de los módulos Antimalware, IPS/IDS, Control de Aplicaciones y otros, podrán realizarse a través de la aplicación *FortiManager* existente en ANDE o deberán incluir licencia de la aplicación similar de la marca a ser proveída para la Centralización de las actualizaciones de las diversas firmas que la componen. No se permite la conexión directa a internet.
- 3.7.5 WAN.: La integración a la red OT de ANDE se realizará a través de los protocolos de enrutamiento dinámico OSPF, se utilizarán los puertos SFP ópticos (OPGW o ADSS según disponibilidad)
- 3.7.6 LAN.: La integración a la red de área local se realizará en configuración Alta Disponibilidad con los switches.

3.8 Equipamiento mínimo del Firewall

3.8.1	Puertos RJ45 >=	16
3.8.2	Puertos 1GE SFP >=	8
3.8.3	Puertos 10GE SFP+ >=	4
3.8.4	Puertos 25GE/10GE SFP >=	4
3.8.5	Puerto GE RJ45 MGMT	1
3.8.6	Puerto GE RJ45 HA	1
3.8.7	Puertos USB	2
3.8.8	Cantidad de Puertos de consola RJ45	1
3.8.9	Almacenamiento interno >=	480 GB SSD

4 CIBER SEGURIDAD.

4.1 Control de Acceso

- 4.1.1 Autenticación mutua y autorización de todos los nodos conectados a la red.
- 4.1.2 Autenticación basada IEEE 802.1x, control de acceso basado en roles (RBAC)
- 4.1.3 Identificación basada en certificados, nombre de usuario y contraseñas.
- 4.1.4 Soporte para inclusión de autoridades certificadoras

4.2 Integridad de Datos, confidencialidad y privacidad.

- 4.2.1 Cifrado de datos en la capa de enlace local.
- 4.2.2 Cifrado de datos en la capa de red WAN mediante (Ipssec)
- 4.2.3 Administración de claves escalables, generación, intercambio y renovación de claves de cifrado.

Preparado	Revisado	Aprobado	Fecha	Revisión	Observación
			24/02/2025	REV01	

4.3 Detección y Mitigación de Amenazas

5 NORMAS Y CERTIFICACIONES

SE REQUIERE EL CUMPLIMIENTO DE LAS NORMAS Y CERTIFICACIONES O SU EQUIVALENTE.

5.1 Inmunidad Electromagnética y seguridad

- EN 55032
- IEC 62368
- EN 62311
- EN 50665
- EN 62479

5.2 Compatibilidad electromagnética

- EN 55035
- EN 61000-3-2
- EN 61000-3-3
- EN 301 489-1
- EN 301 489-17

5.3 RoHs

5.4 Certificaciones

- Antivirus
- Firewall Throughput $\geq 70\text{Gbps}$ (64 byte)
- IPS $\geq 14\text{ Gbps}$
- IPsec $\geq 55\text{Gbps}$ (512 byte)
- SSL-VPN Throughput $\geq 4\text{ Gbps}$

6 ACCESORIOS

El conjunto de accesorios forma parte de la Oferta Básica y deberá incluir mas no limitarse a lo siguiente:

6.1 Todos los accesorios como ser: cables, conectores, adaptadores, dispositivos, software (con sus correspondientes licencias), etc., para el montaje, la alimentación (VDC), operación, ajuste, programación, configuración, calibración y mantenimiento del equipamiento ofertado.

6.2 Accesorios para cableado de interconexión de equipos, **misma cantidad por cada Firewall.**

6.2.1 Transceiver SFP Giga Ethernet, Fibra óptica Single mode LC ($\geq 10\text{km.}$), cantidad 8 (ocho) por equipo.

6.2.5 Transceiver SFP 10 Giga Ethernet, Fibra óptica Multimode LC, cantidad: 4 (cuatro) por equipo.

Preparado	Revisado	Aprobado	Fecha	Revisión	Observación
			24/02/2025	REV01	



6.2.6 Transceiver SFP 25 Giga Ethernet, Fibra óptica Multimode LC, cantidad: 4 (cuatro) por equipo.

6.3 Patch-Cord RJ45: 16 por cada Firewall

6.4 Patch-Cord de Fibra Óptica según la siguiente tabla de cantidades:

TIPO DE CONECTOR	LONGITUD	CANTIDAD
1 Gb single mode LC-SC	5 metros	8
	15 metros	8
10 Gb multimode LC-SC	5 metros	4
	15 metros	4
10/25 Gb multimode LC-SC	5 metros	4
	15 metros	4

Tabla 3. Tabla de cantidades de patch cord.

6.5 El proveedor deberá contar en su plantel técnicos certificados en el producto ofertado, los cuales deberán formar parte de la nómina con al menos 1 año. Esta antigüedad deberá ser comprobada con la documentación o constancia emitida por el IPS (Instituto de Previsión Social) o su equivalente en el país de origen del oferente, para la fase de implementación o brindar soporte local en caso de que sea requerido.

7 DOCUMENTOS A SER PRESENTADOS

- 7.1. Planilla de Datos Garantizados: Debidamente completada en todos sus ítems.
- 7.2. Catálogos / Folletos Técnicos: De manera a corroborar la información consignada en la planilla de datos garantizados.
- 7.3. Manuales y Procedimientos: Manuales y procedimientos para la administración, gestión, configuración y mantenimiento de los equipos (mensual, trimestral, semestral y anual)

OBSERVACIÓN: Todas las hojas presentadas (oferta de precios, especificaciones técnicas, planilla de datos garantizados, catálogos, documentos, etc.) deberán estar debidamente firmadas y selladas por el oferente.

Preparado	Revisado	Aprobado	Fecha	Revisión	Observación
			24/02/2025	REV01	