



IT-OPE-001
Memoria Técnica
Firewall PAN PA-5250
Palo Alto Networks PA-5250

Responsables

Elaboró:	Líder SOC
Revisó:	Control de Documentos
Aprobó:	Gerente de Operaciones

Control de versiones

Versión	Fecha	Descripción del cambio
1	28/02/2019	Emisión inicial
2	04/04/2022	Actualización memoria técnica
3	12/10/2022	Actualización de formato y revisión general del documento.

Clave del formato de instructivo: F-SGI-003 v3
Comentarios o dudas: sgi@silent4business.com

Contenido

1	Objetivo.....	4
2	Alcance	4
3	Definiciones.....	4
4	Descripción del instructivo.....	4
4.1	Características de Software y Hardware de los equipos.....	4
4.2	Firewall 1	4
4.3	Firewall 2	6
4.4	Usuarios de administración.....	8
4.5	Licencia.....	8
4.6	PA-5050_B.....	8
4.7	PA-5050_A.....	9
4.8	Alta Disponibilidad	10
4.9	PA-5050_B / Modo Activo.....	10
4.10	PA-5050_A / Modo Pasivo	11
4.11	Rutas Estáticas	12
4.12	Interfaces	15
4.13	Zonas de Seguridad	16
4.14	Funcionalidades	16
4.15	Políticas de Seguridad	16
4.16	Políticas implícitas.....	18
4.17	Políticas Basadas en NAT	18
4.18	Perfiles de seguridad.....	19
4.19	Perfil Antivirus.....	19
4.20	Perfil Anti-Spyware	19
4.21	Perfil Protección de Vulnerabilidades.....	20
4.22	Perfil Filtrado de URL	20
4.23	Perfil Bloqueo de archivos	21
4.24	Perfil WildFire Analysis.....	21
4.25	Perfiles de autenticación.....	21
4.26	Servidores LDAP	24

4.27	Grupos de Direcciones	26
4.28	Objetos y grupos de servicios	28
4.29	Grupos de Servicios.....	29
4.30	Diagrama de red.....	29
4.31	Control de versiones	29
5	Anexos.....	29

1 Objetivo

El objetivo de este documento es describir la configuración base con la que se encuentra implementado y operando la solución tecnológica de Seguridad Perimetral “Palo Alto Networks” PA-5050_A que forma parte de la infraestructura de S4B (Silent4Business) con domicilio en Torre Murano, Insurgentes Sur No. 2453, piso 4, Col. Tizapán San Ángel, Del. Álvaro Obregón, C.P. 01090, Ciudad de México. Todo ello para la ejecución de la renovación tecnológica la cual estará basada sobre la presente configuración.

2 Alcance

Este documento está enfocado a la descripción y configuración con la que cuenta la solución tecnológica de Seguridad Perimetral PA-5050, cuyas configuraciones se enumeran de la siguiente manera.

Configuraciones del clúster Firewall Palo Alto.

Diagramas de la solución de seguridad perimetral clúster Firewall Palo Alto.

3 Definiciones

Firmware: Es un programa que es grabado en una memoria ROM y establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo.

Unidad de rack: Es una unidad de medida usada para describir la altura del equipamiento preparado para ser montado en un rack de 19 o 23 pulgadas de ancho. Una unidad rack equivale a 1,75 pulgadas (4,445 cm) de alto.

4 Descripción del instructivo

4.1 Características de Software y Hardware de los equipos

4.2 Firewall 1



Tipo: Palo Alto PA-5050 / Software Versión 8.1.4

Dispositivo: Firewall

Hostname: PA-5050_B

Sistema Operativo: PAN-OS 8.1.4

Ubicación y dirección Física

Torre Murano, Insurgentes Sur No. 2453, piso 4, Col. Tizapán San Ángel, Del. Álvaro Obregón, C.P. 01090, Ciudad de México

Contacto: Luis Alberto Valle Rueda / Abraham Carrillo Ortiz.

HARDWARE	CARACTERISTICAS
Firmware	PAN-OS 8.1.4
Número de Serie	002201003975
Fabricante	Palo Alto Networks
Memoria RAM	No Disponible
Memoria Flash	No Disponible
Espacio en Disco Duro	SSD de 240 GB, RAID 1
Rack Mount	2U, rack estándar de 19" (22,86 cm) (8,89 x 41,91 x 44,45 cm – 3,5 x 21 x 17,5 pulgadas)
Fuente de Poder	450 W AC (270 W/340 W) redundante
Modelo del Equipo	PA-5050
Cantidad de "U" para Rack	2U, bastidor estándar de 19"
Velocidad de Interfaz	(8) puertos SFP Gigabit, (4) puertos SFP+ Gigabit
Troughput del dispositivo	10 Gbps
Procesador	No Disponible
SOFTWARE	CARÁCTERISTICAS
Sistema Operativo	PAN-OS 8.1.4
Firewall	Enable
VPN	Enable
WildFire	Enable
AV	Enable
IPS	Enable
Filtrado de URLs	Enable
AutoFocus	Enable
Tipo de Clúster	HA Activo/Pasivo
Configuración Clúster	Enable
CONFIGURACIÓN ADMINISTRATIVA	

sgi@silent4business.com



Insurgentes Sur #2453, Piso 4, Col. Tizapán San Ángel, Álvaro Obregón, 01090 Ciudad de México, CDMX

"La información contenida en este documento es propiedad intelectual de SILENT4BUSINESS SA DE CV, por lo que queda estrictamente prohibida su reproducción, modificación, divulgación, uso o aprovechamiento por cualquier medio impreso, mecánico o electrónico sin la autorización previa por escrito de Silent4Business."



GENERAL	CARACTERISTICA
Hostname	PA-5050_B
Consola Principal	Web
Versión y updates	8.1.4
Tipo de Acceso para Monitoreo y Administración	SSH HTTPS
Servicios de Red	Ping SNMP
Modo HA	Activo
Certificados	GP-Cert GP_Cert_Alterno Inspeccion SSL CA_Silent4Business.com
RED	CARACTERISTICA
Dirección IP MGT/Máscara Red	192.168.110.12
Gateway MGT	192.168.110.254
Servidores DNS	192.168.9.30, 192.168.9.31
Servidor NTP	192.168.9.30
SNMP	N/A
Servidor syslog	192.168.9.1 192.168.3.61

4.3 Firewall 2



Tipo: Palo Alto PA-5250/ Software Versión 8.1.7

Dispositivo: Firewall

Hostname: CDMX02Ins-NavPA5250-2

Sistema Operativo: PAN-OS 8.1.7

Ubicación y dirección Física

Av. de los Insurgentes Sur 1089, Noche Buena, 03720 Ciudad de México, CDMX.

Contacto: Luis Alberto Valle Rueda / Abraham Carrillo Ortiz.

HARDWARE	CARACTERISTICAS
Firmware	PAN-OS 8.1.4
Número de Serie	002201003944
Fabricante	Palo Alto Networks
Memoria RAM	No Disponible
Memoria Flash	No Disponible
Espacio en Disco Duro	SSD de 240 GB, RAID 1
Rack Mount	2U, rack estándar de 19" (22,86 cm) (8,89 x 41,91 x 44,45 cm – 3,5 x 21 x 17,5 pulgadas)
Fuente de Poder	450 W AC (270 W/340 W) redundante
Modelo del Equipo	PA-5050
Cantidad de "U" para Rack	2U, bastidor estándar de 19"
Velocidad de Interfaz	(8) puertos SFP Gigabit, (4) puertos SFP+ Gigabit
Troughput del dispositivo	10 Gbps
Procesador	No Disponible
SOFTWARE	CARÁCTERISTICAS
Sistema Operativo	PAN-OS 8.1.4
Firewall	Enable
VPN	Enable
WildFire	Enable
AV	Enable
IPS	Enable
Filtrado de URLs	Enable
AutoFocus	Enable
Tipo de Clúster	HA Activo/Pasivo
Configuración Clúster	Enable
CONFIGURACIÓN ADMINISTRATIVA	
GENERAL	CARACTERISTICA
Hostname	PA-5050_A
Consola Principal	Web
Versión y updates	8.1.4
Tipo de Acceso para Monitoreo y Administración	SSH HTTPS
Servicios de Red	Ping SNMP
Modo HA	Activo
Certificados	GP-Cert GP_Cert_Alterno Inspeccion SSL CA_Silent4Business.com

RED	CARACTERISTICA
Dirección IP MGT/Máscara Red	192.168.110.11
Gateway MGT	192.168.110.254
Servidores DNS	192.168.9.30, 192.168.9.31
Servidor NTP	192.168.9.30
SNMP	N/A
Servidor syslog	192.168.9.1 192.168.3.61

4.4 Usuarios de administración

<input type="checkbox"/>	Name	Role	Administer/(View)	
			Profile	Virtual Systems
<input type="checkbox"/>	admin	Superuser		All
<input type="checkbox"/>	analistasoc	Superuser (read-only)		(All)
<input type="checkbox"/>	david.montes	Custom role-based administrator	Operaciones	
<input type="checkbox"/>	elvira.rivera	Custom role-based administrator	Operaciones	
<input type="checkbox"/>	abraham.carrillo	Superuser		All
<input type="checkbox"/>	miguel.rios	Custom role-based administrator	Operaciones	
<input type="checkbox"/>	carlos.hernandez	Superuser (read-only)		(All)
<input type="checkbox"/>	luis.valle	Superuser		All
<input type="checkbox"/>	pablo.rojas	Custom role-based administrator	Operaciones	
<input type="checkbox"/>	juan.jaimes	Superuser		All

4.5 Licencia

En este apartado se muestra el tipo de licencia en cada uno de los dispositivos Firewall que componen el clúster.

4.6 PA-5050_B

PAN-DB URL Filtering	
Fecha de emisión	May 01, 2017
Fecha de caducidad	May 01, 2020
Descripción	Palo Alto Networks URL Filtering License
Activo	Sí
Descargar estado	DownloadNow

WildFire License	
Fecha de emisión	May 01, 2017
Fecha de caducidad	May 01, 2020
Descripción	WildFire signature feed, integrated WildFire logs, WildFire API

Prevención de amenazas	
Fecha de emisión	May 01, 2017
Fecha de caducidad	May 01, 2020
Descripción	Threat Prevention

4.7 PA-5050_A

PAN-DB URL Filtering	
Fecha de emisión	May 01, 2017
Fecha de caducidad	May 01, 2020
Descripción	Palo Alto Networks URL Filtering License
Activo	Sí
Descargar estado	DownloadNow

WildFire License	
Fecha de emisión	May 01, 2017
Fecha de caducidad	May 01, 2020
Descripción	WildFire signature feed, integrated WildFire logs, WildFire API

Prevención de amenazas	
Fecha de emisión	May 01, 2017
Fecha de caducidad	May 01, 2020
Descripción	Threat Prevention

4.8 Alta Disponibilidad

4.9 PA-5050_B / Modo Activo

Alta disponibilidad

Mode

Active-passive

Local

Active

Peer (192.168.110.11)

Passive

En ejecución configuración

Synchronized

Versión de aplicaciones

Match

Versión de amenazas

Match

Versión de antivirus

Match

Versión de PAN-OS

Match

Versión de GlobalProtect

Match

HA1

Up

Copia de seguridad HA1

Up

HA2

Up

Configuración

Habilitar HA

☒

ID de grupo

1

Descripción

Modo

active-passive

Habilitar sincronización de configuración

☒

Dirección IP de HA de peer

1.1.1.10

Crear copia de seguridad de la dirección IP de HA1 del mismo nivel

192.168.110.11

Enlace de control (HA1)

Puerto

dedicated-ha1

Dirección IPv4/IPv6

1.1.1.11

Máscara de red

255.255.255.0

Puerta de enlace

Velocidad de enlace

Dúplex de enlace

Cifrado habilitado

☐

Supervisar tiempo de espera (ms)

3000

Enlace de datos (HA2)

Habilitar sincronización de sesión

☒

Puerto

dedicated-ha2

Dirección IPv4/IPv6

2.2.2.11

Máscara de red

255.255.255.0

Puerta de enlace

Velocidad de enlace

Dúplex de enlace

Transporte

ethernet

Acción

log-only

Umbral (ms)

10000



Configuración Activa/Pasiva

Estado de los enlaces en el pasivo auto
Supervisar fallo de tiempo de espera descendente (minuto) 1

Configuración de elección

Prioridad de dispositivo 100

Preferente ☐

Copia de seguridad de heartbeat ☒

Configuración de temporizador de HA Avanzado

Tiempo de espera de promoción (ms) 2000

Intervalo de saludo (ms) 8000

Intervalo de heartbeat (ms) 1000

Máximo de flaps 5

Tiempo de espera para ser preferente (minuto) 1

Supervisar fallo de tiempo de espera ascendente (ms) 0

Tiempo de espera principal adicional (ms) 500

4.10 PA-5050_A / Modo Pasivo

Alta disponibilidad

Mode Active-passive

Local  Passive

Peer (192.168.110.12)  Active

En ejecución configuración  Synchronized

Versión de aplicaciones  Match

Versión de amenazas  Match

Versión de antivirus  Match

Versión de PAN-OS  Match

Versión de GlobalProtect  Match

HA1  Up

Copia de seguridad HA1  Up

HA2  Up

Configuración

Habilitar HA ☒

ID de grupo 1

Descripción

Modo active-passive

Habilitar sincronización de configuración ☒

Dirección IP de HA de peer 1.1.1.11

Crear copia de seguridad de la dirección IP de HA1 del mismo nivel 192.168.110.12

Enlace de control (HA1)	
Puerto	dedicated-ha1
Dirección IPv4/IPv6	1.1.1.10
Máscara de red	255.255.255.0
Puerta de enlace	
Velocidad de enlace	
Dúplex de enlace	
Cifrado habilitado	<input type="checkbox"/>
Supervisar tiempo de espera (ms)	3000

Enlace de datos (HA2)	
Habilitar sincronización de sesión	<input checked="" type="checkbox"/>
Puerto	dedicated-ha2
Dirección IPv4/IPv6	2.2.2.10
Máscara de red	255.255.255.0
Puerta de enlace	
Velocidad de enlace	
Dúplex de enlace	
Transporte	ethernet
Acción	log-only
Umbral (ms)	10000

Configuración Activa/Pasiva	
Estado de los enlaces en el pasivo	auto
Supervisar fallo de tiempo de espera descendente (minuto)	1

Configuración de elección	
Prioridad de dispositivo	66
Preferente	<input type="checkbox"/>
Copia de seguridad de heartbeat	<input checked="" type="checkbox"/>
Configuración de temporizador de HA	Avanzado
Tiempo de espera de promoción (ms)	2000
Intervalo de saludo (ms)	8000
Intervalo de heartbeat (ms)	1000
Máximo de flaps	5
Tiempo de espera para ser preferente (minuto)	1
Supervisar fallo de tiempo de espera ascendente (ms)	0
Tiempo de espera principal adicional (ms)	500

4.11 Rutas Estáticas

A continuación, se muestran las rutas estáticas contenidas en la solución de seguridad Firewall.

115 elementos								
	Nombre	IP Destino	Interfaz	Siguiente salto		Distancia administrativa	Métrica	Tabla de enrutamiento
				Tipo	Valor			
<input type="checkbox"/>	Alestra	0.0.0.0/0	ethernet1/4	ip-address	189.210.45.89	default	5	unicast
<input type="checkbox"/>	Axtel	0.0.0.0/0	ethernet1/1	ip-address	148.240.123.1	default	10	unicast
<input type="checkbox"/>	NEDXO_IT	10.106.32.0/24	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
<input type="checkbox"/>	dev	192.168.50.0/24	tunnel.5			default	10	unicast
<input type="checkbox"/>	VPN_S4B-SCT	10.36.248.0/28	tunnel.10			default	10	unicast
<input type="checkbox"/>	VPN_S4B-SCT_ASA1	10.33.248.2/32	tunnel.10			default	10	unicast
<input type="checkbox"/>	VPN_S4B-SCT_ASA2	10.33.247.11/32	tunnel.10			default	10	unicast
<input type="checkbox"/>	VPN_S4B-SCT_ASA3	10.33.247.18/32	tunnel.10			default	10	unicast
<input type="checkbox"/>	VPN_S4B-SCT_F5_1	10.33.247.54/32	tunnel.10			default	10	unicast
<input type="checkbox"/>	VPN_SCT_ASA_DC	10.33.251.249/32	tunnel.10			default	10	unicast
<input type="checkbox"/>	ASA_SCT_Otro	10.40.101.2/32	tunnel.10			default	10	unicast
<input type="checkbox"/>	ASA_Nuevo_SCT	10.36.248.18/32	tunnel.10			default	10	unicast
<input type="checkbox"/>	ASA_NUEVO_Management	10.33.247.40/32	tunnel.10			default	10	unicast
<input type="checkbox"/>	ASA_Firepower	10.36.248.19/32	tunnel.10			default	10	unicast
<input type="checkbox"/>	F5_SCT	10.33.158.101/32	tunnel.10			default	10	unicast
<input type="checkbox"/>	F5_Hypervisor_SCT	10.33.247.50/32	tunnel.10			default	10	unicast
<input type="checkbox"/>	ISSSTE_NexoIT	10.222.0.0/16	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
<input type="checkbox"/>	ISSSTE_NexoIT_2	10.1.215.0/24	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
<input type="checkbox"/>	ISSSTE_NexoIT_3	10.150.0.0/15	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
<input type="checkbox"/>	ISSSTE_NexoIT_4	10.152.0.0/14	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
<input type="checkbox"/>	ISSSTE_NexoIT_5	10.200.0.0/16	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
<input type="checkbox"/>	ISSSTE_NexoIT_6	10.223.7.0/24	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
<input type="checkbox"/>	ISSSTE_NexoIT_7	192.160.0.0/13	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
<input type="checkbox"/>	ISSSTE_NexoIT_8	192.168.64.0/19	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
<input type="checkbox"/>	ISSSTE_NexoIT_9	192.168.128.0/17	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
<input type="checkbox"/>	ISSSTE_NexoIT_10	192.168.1.3/32	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
<input type="checkbox"/>	ISSSTE_NexoIT_11	192.168.105.0/24	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
<input type="checkbox"/>	ISSSTE_NexoIT_12	192.168.118.0/24	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
<input type="checkbox"/>	ISSSTE_NexoIT_13	192.168.120.0/24	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
<input type="checkbox"/>	ISSSTE_NexoIT_14	192.168.3.64/30	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
<input type="checkbox"/>	ISSSTE_NexoIT_15_REMEDY	192.168.61.0/24	tunnel.3			default	10	unicast
<input type="checkbox"/>	SENER_RED	172.16.0.0/16	tunnel.20			default	10	unicast
<input type="checkbox"/>	BCONNECT	172.21.1.52/32	tunnel.22			default	10	unicast

BCONNECT_1	172.21.1.137/32	tunnel.22			default	10	unicast
BCONNECT_2	172.21.1.139/32	tunnel.22			default	10	unicast
ASA_20	10.36.248.20/32	tunnel.10			default	10	unicast
PA-Publicaciones	10.33.248.147/32	tunnel.10			default	10	unicast
ISSSTE_NexoIT_18	10.250.53.37/32	tunnel.3			default	10	unicast
VPN_S4B_SCT_FWVPN	10.33.247.130/32	tunnel.10			default	10	unicast
SCT_fwnav	10.33.247.34/32	tunnel.10			default	10	unicast
L2LTest	192.168.179.210/32	tunnel.3			default	10	unicast
VPN_S4B-SCT_ASA4	10.33.247.131/32	tunnel.10			default	10	unicast
VPN_S4B_SCT_FW_NAV2	10.33.247.35/32	tunnel.10			default	10	unicast
SCT_QRO	10.38.0.0/16	tunnel.9			default	10	unicast
ISSSTE_NexoIT_16	192.168.123.0/24	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
ISSSTE_NexoIT_17	10.223.2.0/24	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
ISSSTE_NexoIT_19	192.168.15.0/24	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
VPN_S4B_SCT_F5_100	10.33.248.100/32	tunnel.9			default	10	unicast
VPN_S4B_SCT_F5_101	10.33.248.101/32	tunnel.9			default	10	unicast
VPN_S4B_SCT_F5_102	10.33.248.102/32	tunnel.9			default	10	unicast
ISSSTE_NexoIT_20	192.168.19.0/24	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
VPN_S4B-Consola_Forcepoint	10.33.247.36/32	tunnel.10			default	10	unicast
VPN_SCT_EDOMEX	10.14.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_AGS	10.1.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_BCN	10.2.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_BCS	10.3.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_CHIH	10.6.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_CHS	10.5.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_HGO	10.12.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_JAL	10.13.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_MOR	10.16.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_NL	10.18.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_PUE	10.20.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_QRO	10.21.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_SLP	10.23.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_TAM	10.27.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_TLAX	10.28.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_VER	10.29.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_YUC	10.30.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_COL	10.8.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_SON	10.25.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_SIN	10.24.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_ZAC	10.31.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_OAX	10.19.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_CAM	10.4.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_COA	10.7.251.235/32	tunnel.10			default	10	unicast
PN_SCT_DGO	10.9.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_GTO	10.10.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_GRO	10.11.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_MCH	10.15.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_NAY	10.17.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_QOO	10.22.251.235/32	tunnel.10			default	10	unicast
VPN_SCT_TAB	10.26.251.235/32	tunnel.10			default	10	unicast
VPN_SCT-LAS_FLORES	10.33.248.50/32	tunnel.10			default	10	unicast
VPN_REMEDY_SCT	10.33.149.251/32	tunnel.10			default	10	unicast
VPN_SCT-LAS_BOMBAS	10.33.248.66/32	tunnel.10			default	10	unicast
VPN_SCT-TOREO	10.33.246.253/32	tunnel.10			default	10	unicast
VPN_FW_SCT_PRINCIPAL	10.33.247.38/32	tunnel.10			default	10	unicast
ISSSTE_NexoIT_21	10.223.3.0/24	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
S4B-ServidorFP	10.33.247.37/32	tunnel.10			default	10	unicast
ISSSTE_NexoIT_1_2	10.1.25.18/32	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
ISSSTE_NexoIT_22	192.168.111.12/32	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
ISSTEMPLS	10.250.53.37/32	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
ISSTEMPLS1	192.168.55.148/32	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
ISSTEMPLS2	10.1.18.62/32	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
SCT_PICUS	10.33.142.254/32	tunnel.10			default	10	unicast
ISSTEMPLS3	10.223.100.0/22	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
ISSTEMPLS4	10.223.104.0/21	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
ISSTEMPLS5	10.223.112.0/24	ethernet1/8	ip-address	10.90.11.1	default	10	unicast

test	8.8.8.8/32	ethernet1/4	ip-address	189.210.45.89	default	10	unicast
ISSSTEMPLS6	10.1.236.12/32	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
ISSSTEMPLS7	10.1.236.13/32	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
ISSSTEMPLS8	10.2.193.10/32	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
ISSSTEMPLS9	10.2.193.11/32	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
ISSSTE_NexoIT_23	10.1.8.67/32	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
VPN_S4B_GPO-MODELO-LOG_DECODER	10.88.3.154/32	tunnel.23			default	10	unicast
VPN_S4B_GPO-MODELO-LOG_CONCENT	10.88.3.153/32	tunnel.23			default	10	unicast
VPN_S4B_GPO-MODELO-SAS	10.88.3.152/32	tunnel.23			default	10	unicast
VPN_S4B_GPO-MODELO-ESA	10.89.144.53/32	tunnel.23			default	10	unicast
VPN_S4B_GPO-MODELO-ARCHIVER	10.89.144.54/32	tunnel.23			default	10	unicast
ISSSTE_NexoIT_24	10.250.54.38/32	ethernet1/8	ip-address	10.90.11.1	default	10	unicast
F5_Hypervisor_guest	10.33.247.51/32	tunnel.10			default	10	unicast
F5_Hypervisor_guest2	10.33.247.52/32	tunnel.10			default	10	unicast
F5_Hypervisor_guest3	10.33.247.53/32	tunnel.10			default	10	unicast
SCT_10_33_247	10.33.247.0/26	tunnel.10			default	10	unicast

4.12 Interfaces

Se muestra la configuración actual que se tiene sobre las interfaces Ethernet administradas en la solución de seguridad Firewall.

Interfaz	Tipo de interfaz	Perfil de gestión	Estado de enlace	Dirección IP	Enrutador virtual	Etiqueta	VLAN / Virtual-Wire	Sistema virtual	Zona de seguridad	Características	Comentarios
ethernet1/1	Layer3			148.240.123.2/24	default	Untagged	none	vsys1	Internet		Enlace Internet 1 (Axtel)
ethernet1/2	Layer3	Only ping		172.18.10.254/24	default	Untagged	none	vsys1	DMZ Sinkhole		DMZ-Sinkhole
ethernet1/3	Layer3	Only ping		172.17.10.253/24	default	Untagged	none	vsys1	DMZ DNS		DMZ-DNS
ethernet1/4	Layer3			189.210.45.91/29	default	Untagged	none	vsys1	Internet		Enlace Internet 2 (Alestra)
ethernet1/5	Layer3	Only ping		172.19.10.254/24	default	Untagged	none	vsys1	DMZ NAS		DMZ Respaldos
ethernet1/6	Layer3			172.16.10.254/24	default	Untagged	none	vsys1	DMZ Laboratorio		DMZ-Laboratorio
ethernet1/7				none	none	Untagged	none	none	none		
ethernet1/8	Layer3	Only ping		10.90.11.6/28	default	Untagged	none	vsys1	MPSL_ISSSTE		
ethernet1/9				none	none	Untagged	none	none	none		
ethernet1/10	Layer3	Only ping		2.2.2.2/29	default	Untagged	none	vsys1	L2L_ISSSTE		Enlace L2L hacia NexoIT
ethernet1/11	Aggregate (ae1)			none	none	Untagged	none	none	none		
ethernet1/12	Aggregate (ae1)			none	none	Untagged	none	none	none		
ethernet1/13				none	none	Untagged	none	none	none		
ethernet1/14				none	none	Untagged	none	none	none		
ethernet1/15				none	none	Untagged	none	none	none		
ethernet1/16				none	none	Untagged	none	none	none		
ethernet1/17				none	none	Untagged	none	none	none		
ethernet1/18				none	none	Untagged	none	none	none		
ethernet1/19				none	none	Untagged	none	none	none		
ethernet1/20				none	none	Untagged	none	none	none		
ethernet1/21				none	none	Untagged	none	none	none		
ethernet1/22				none	none	Untagged	none	none	none		
ethernet1/23				none	none	Untagged	none	none	none		
ethernet1/24				none	none	Untagged	none	none	none		
ae1	Layer3	Userid		none	none	Untagged	none	vsys1	none		
ae1.2	Layer3	Userid		192.168.2.253/24	default	2	none	vsys1	Trust-L3		Videoconferencias
ae1.3	Layer3	Userid		192.168.3.62/26	default	3	none	vsys1	SOC		Operadores
ae1.4	Layer3	Userid		192.168.4.254/24	default	4	none	vsys1	WIFI		Wireless
ae1.5	Layer3	Userid		192.168.5.254/24	default	5	none	vsys1	LAN		Oficinas
ae1.6	Layer3	Userid		192.168.6.253/24	default	6	none	vsys1	Trust-L3		Control de Acceso
ae1.7	Layer3	Only ping		192.168.7.254/24	default	7	none	vsys1	Ciberinteligencia		Laboratorio
ae1.8	Layer3	Userid		192.168.8.253/24	default	8	none	vsys1	Trust-L3		Voz
ae1.9	Layer3	Userid		192.168.9.253/24	default	9	none	vsys1	Trust-L3		Administración
ae1.10	Layer3	Userid		192.168.10.253/24	default	10	none	vsys1	Trust-L3		CCTV
ae1.11	Layer3	Only ping		192.168.22.14/28	default	22	none	vsys1	FINANZAS		
ae1.100	Layer3	Userid		192.168.100.253/24	default	100	none	vsys1	Trust-L3		LAN
ae1.110	Layer3	Userid		192.168.110.253/24	default	110	none	vsys1	Trust-L3		Admin VMWare
ae1.600	Layer3	Userid		172.29.1.253/23	default	600	none	vsys1	Trust-L3		Externos

4.13 Zonas de Seguridad

En esta sección se muestran las Zonas de Seguridad configuradas en la solución de seguridad Firewall.

Nombre	Ubicación	Tipo	Interfaces / sistemas virtuales	Perfil de protección de zona	Protección de búfer de paquetes	Ajuste de log	Habilitado	ID de usuario	
								Redes incluidas	Redes excluidas
Clasificación	vsys1	layer3	ae1.7				<input checked="" type="checkbox"/>	cualquiera	ninguno
DMZ DNS	vsys1	layer3	ethernet1/7			Loghythm	<input checked="" type="checkbox"/>	cualquiera	ninguno
DMZ Laboratorio	vsys1	layer3	ethernet1/6			Loghythm	<input checked="" type="checkbox"/>	cualquiera	ninguno
DMZ NAS	vsys1	layer3	ethernet1/5			Loghythm	<input checked="" type="checkbox"/>	cualquiera	ninguno
DMZ Sinkhole	vsys1	layer3	ethernet1/2			Loghythm	<input checked="" type="checkbox"/>	cualquiera	ninguno
FINANZAS	vsys1	layer3	ae1.11			Loghythm	<input checked="" type="checkbox"/>	cualquiera	ninguno
GP-VPN-Dev	vsys1	layer3	tunnel.4			Loghythm	<input checked="" type="checkbox"/>	cualquiera	ninguno
Internet	vsys1	layer3	ethernet1/1			Loghythm	<input checked="" type="checkbox"/>	cualquiera	ninguno
			ethernet1/4						
			tunnel.11						
L2L_SISSTE	vsys1	layer3	ethernet1/10				<input checked="" type="checkbox"/>	cualquiera	ninguno
LAN	vsys1	layer3	ae1.5				<input checked="" type="checkbox"/>	cualquiera	ninguno
HPDL_SISSTE	vsys1	layer3	ethernet1/8				<input checked="" type="checkbox"/>	cualquiera	ninguno
SOC	vsys1	layer3	ae1.3			Loghythm	<input checked="" type="checkbox"/>	cualquiera	ninguno
Trust-L3	vsys1	layer3	ae1.2			Loghythm	<input checked="" type="checkbox"/>	cualquiera	ninguno
			ae1.6						
			ae1.8						
			ae1.9						
			ae1.10						
			ae1.110						
			mid...						
VPN-Dev	vsys1	layer3	tunnel.5			Loghythm	<input checked="" type="checkbox"/>	cualquiera	ninguno
VPN-NEOIT	vsys1	layer3	tunnel.3				<input checked="" type="checkbox"/>	cualquiera	ninguno
VPN_Alerno	vsys1	layer3	tunnel.2				<input checked="" type="checkbox"/>	cualquiera	ninguno
VPN_BCONNECT	vsys1	layer3	tunnel.22				<input checked="" type="checkbox"/>	cualquiera	ninguno
VPN_SF	vsys1	layer3	tunnel				<input checked="" type="checkbox"/>	cualquiera	ninguno
VPN_MODEL0	vsys1	layer3	tunnel.23				<input checked="" type="checkbox"/>	cualquiera	ninguno
VPN_SCT	vsys1	layer3	tunnel.10			Loghythm	<input checked="" type="checkbox"/>	cualquiera	ninguno
VPN_SCT_APODACA	vsys1	layer3	tunnel.8			Loghythm	<input checked="" type="checkbox"/>	cualquiera	ninguno
VPN_SCT_QRO	vsys1	layer3	tunnel.9			Loghythm	<input checked="" type="checkbox"/>	cualquiera	ninguno
VPN_SCHER	vsys1	layer3	tunnel.20				<input checked="" type="checkbox"/>	cualquiera	ninguno
WIFI	vsys1	layer3	ae1.4				<input checked="" type="checkbox"/>	cualquiera	ninguno

4.14 Funcionalidades

El dispositivo de seguridad de la red nos permite monitorear el tráfico de red entrante y saliente, así mismo, decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.

4.15 Políticas de Seguridad

Actualmente se tiene varias políticas configuradas sobre las diferentes interfaces de la solución de seguridad firewall, esto con la finalidad de tener un correcto control sobre los servicios y aplicaciones que fluyen a través de la infraestructura de la Secretaria de Comunicaciones y Transportes, así mismo poder proporcionar los permisos acceso o denegación adecuados en cada una de sus diferentes zonas.

Nombre	Etiquetas	Tipo	IP Origen			IP Destino			Uso de reglas			Aplicación	Servicio	Acción	Perfil	Opciones
			Zona	Dirección	Usuario	Perfil	Zona	Dirección	Recuento de acciones	Último acierto	Primer acierto					
1 AS_Entrada	ACTIVIDAD SOSPEC.	universal	Internet	Gpu_Actividad_Scope	any	any	any	any	19061	2019-04-08 16:28:12	2019-03-21 17:34:42	any	any	Descartar	none	
2 Bloqueo Proxy	Bloqueo	universal	any	any	any	any	Internet	any	889	2019-04-08 16:12:57	2019-03-21 20:21:38	any	application-default	Permitir	none	
3 Publicacion_DMZ_SISSTE	Publicaciones	universal	Internet	any	any	any	DMZ DNS	NAT_DMZ	49225	2019-04-08 16:30:22	2019-03-21 18:52:08	any	any	Permitir		
4 Publicacion_PTGT_SISSTE	Publicaciones	universal	Internet	any	any	any	Trust-L3	NAT_PTGT	2135795	2019-04-08 16:30:30	2019-11-01 18:56:53	any	any	Permitir		
								NAT_PTGT2								
5 Publicacion_SFTP	Publicaciones	universal	Internet	any	any	any	DMZ DNS	NAT_SFTP_123.4	27834	2019-03-27 15:02:52	2019-03-21 18:53:00	any	any	Permitir		
6 VPN_SMB-SCT	VPN	universal	SOC	any	any	any	VPN_SCT	any	20148038	2019-04-08 16:30:30	2019-11-01 18:57:06	any	any	Permitir		
	SCT		Trust-L3				VPN_SCT									
7 VPN_SMB-SCT_1	VPN	universal	VPN_SCT	any	any	any	Trust-L3	any	34011	2019-04-08 16:30:21	2019-11-01 19:46:15	any	any	Permitir		
	SCT		VPN_SCT_QRO				SOC									
8 VPN_SMB-SCT_SHTP	VPN	universal	VPN_SCT	any	any	any	DMZ DNS	SFTP-RELAY_10.1	65	2019-04-05 15:02:32	2019-03-22 11:32:15	any	SFTP	Permitir		
	SCT		VPN_SCT_QRO													
9 VPN_SCHER	VPN	interzone	Trust-L3	Host_192.168.9.10	any	any	VPN_SCHER	Red_SCHER	9837363	2019-04-08 16:30:30	2019-11-01 18:57:07	any	any	Permitir	none	
	SCHER		SOC	VLAN SOC												
10 VPN_SCHER_REMEDY	VPN	universal	VPN_SCHER	172.16.60.156	any	any	SOC	Host_192.168.9.10	10595	2019-04-08 16:19:51	2019-03-21 17:01:18	any	any	Permitir		
	SCHER			Host_172.16.60.160			Trust-L3	Nuevo_Remedio_9								
				NOP_172.16.85.31				Panorama_9.18								
				PAI_Scherm_85.35				RemedyWeb								
				PAI_Scherm_85.36				Scherm_192.168.9.161								
11 VPN_BCONNECT	VPN	interzone	VPN_BCONNECT	any	any	any	Trust-L3	192.168.9.165	3111	2019-04-08 16:10:19	2019-03-21 19:09:17	any	any	Permitir		
	BCONNECT_1		BCONNECT_1				SOC	Host_192.168.9.150								
	SISSTE		BCONNECT_3					VLAN SOC								
12 VPN_BCONNECT_2	VPN	interzone	Trust-L3	Host_192.168.9.150	any	any	VPN_BCO...	BCONNECT_1	5426	2019-04-07 13:54:32	2019-03-22 10:48:42	any	any	Permitir		
	VPN_BCONNECT_2		SOC	Host_192.168.9.165				BCONNECT_2								
	SISSTE			VLAN SOC				BCONNECT_3								

13	Monitoring to L2L-VPN-N...	VPN ASISTE	interzone	Trust-L2 SOC	Server Augusto X Servers Loghythm Servers Pasador PRTG VLAN SOC	any	any	VPN-NEX...	10.80.20.8 10.80.20.6 10.80.20.7 10.80.20.8 10.80.20.9 10.80.20.10	0	-	-	any	any	Permitir		
14	VPN_NEXO	VPN ASISTE	universal	VPN-NEXOT	192.168.61.23 192.168.61.30	any	any	Trust-L3	192.168.9.155	39475	2019-04-08 16:30:25	2019-03-21 18:43:41	any	any	Permitir		
15	VPN_S4B_NEXOT	VPN ASISTE	universal	Trust-L3 SOC	VLAN Servidores VLAN SOC	any	any	VPN-NEX...	Nueva_Remedy_5...	112010	2019-04-08 16:30:11	2019-03-21 18:29:14	any	any	Permitir		
16	L2L-VPN-NEXO to Hw...	VPN ASISTE	interzone	VPN-NEXOT	10.80.20.5 10.80.20.6 10.80.20.7 10.80.20.8 10.80.20.9 10.80.20.10	any	any	Trust-L3	Server Augusto X Servers Loghythm Servers Pasador P...	0	-	-	any	any	Permitir		
17	VPN_S4B_MODELO	VPN VPN-MODELO ASISTE	universal	SOC Trust-L3	Host_192.168.9.10 VLAN SOC	any	any	VPN-MO	GPO-MODELO	1222504	2019-04-08 16:30:29	2019-03-21 17:00:05	any	any	Permitir		
18	Conexion ISSSTE L2L-1	ASISTE	universal	Trust-L3 L2L_ISSSTE	192.168.61.23 192.168.61.30	any	any	Trust-L3	192.168.9.155	38	2018-11-01 19:40:16	2018-11-01 19:45:16	any	any	Permitir		
19	Conexion ISSSTE L2L	ASISTE	universal	Trust-L3 SOC	VLAN Servidores VLAN SOC	any	any	Trust-L3 L2L_ISSSTE	Nueva_Remedy_5...	631892	2019-04-08 16:30:28	2018-11-01 18:57:07	any	any	Permitir	none	
20	Conexion MPLS ISSSTE	ASISTE	universal	Trust-L3 SOC	VLAN Servidores VLAN SOC	any	any	MPLS_ISS...		446912214	2019-04-08 16:30:38	2018-11-01 18:57:07	any	any	Permitir	none	
21	Public DNS-NTP	DNS DNS Internet	interzone	DMZ DNS SOC Trust-L3	Externals DNS Group_PRTG_ISSSTE Internals DNS Navigation Servidores SFTP-RELAY_10.1 VLAN SOC	any	any	Internet		4453317	2019-04-08 16:30:29	2019-03-21 17:00:01	dns ntp ntp	application-default	Permitir		
22	AccessPoints	Navigation Navigation_Bro	universal	WIFI	APs_548	any	any	Internet		1492462	2019-04-08 16:30:30	2019-03-21 17:01:07	any	any	Permitir		
23	Bloques	Navigation Internet	interzone	any	any	any	any	Internet		28604	2019-04-08 16:30:03	2018-11-01 18:53:16	Bloques D...	application-default	Descartar	none	
24	Navigation Basica	Navigation Internet	universal	LAN WIFI	Navigation_Basica	any	any	Internet		113129	2019-04-08 16:30:20	2018-11-01 18:56:58	Navigation...	Navigation	Permitir		
25	PermisosEspeciales	Navigation Navigation_Bro	universal	Ciberinteligencia SOC	Usuarios Permis Es...	any	any	Internet		1290251	2019-04-08 16:30:00	2018-11-01 18:57:06	any	any	Permitir	none	
26	Navigation RH	Navigation Internet	universal	Trust-L3 WIFI	APs_548	any	any	Internet		63199	2019-04-08 16:30:27	2019-03-21 17:01:18	Navigation...	Navigation	Permitir		
27	Navigation NOC	Navigation Internet	universal	LAN SOC	NOC	any	any	Internet		2120308	2019-04-08 16:30:29	2018-11-01 19:46:04	Navigation...	Navigation	Permitir		
28	Block	Bloqueo	universal	Trust-L3	Host_192.168.8.158	any	any	L2L_ISSSTE		8	-	-	any	TCP_1688	Descartar	none	
29	Block Perfiles IP	Bloqueo	universal	LAN SOC WIFI	Navigation_Basica NOC	any	any	Internet		832294	2019-04-08 16:30:16	2019-03-21 18:07:46	any	any	Descartar	none	
30	Bloqueo Perfiles	Bloqueo	universal	LAN WIFI	APs_548	any	any	Internet		57229	2019-04-08 16:25:57	2019-03-22 10:33:54	any	any	Descartar	none	
31	Red Oficinas	Navigation Internet	interzone	Ciberinteligencia LAN WIFI	VLAN Ciberinteligencia VLAN Oficinas VLAN Wireless	any	any	Internet		3313242	2019-04-08 16:30:25	2018-11-01 18:57:01	any	Navigation	Permitir		
32	Red Oficinas-CorreoExter...	Navigation Internet	interzone	LAN WIFI	VLAN Oficinas VLAN Wireless	any	any	Internet	Correo_Externo	1026	2019-04-08 16:09:41	2019-03-21 17:01:18	any	Correo_Externo	Permitir		
33	Red SOC	Navigation Internet	interzone	SOC	VLAN SOC	any	any	Internet		1636090	2019-04-08 16:30:29	2019-03-21 17:01:08	any	any	Permitir		
34	Updates	Update Internet	interzone	Trust-L3	192.168.2.100/32 Hgt PalabritasNetworks Server Augusto X FINANZAS_22.8-38	any	any	Internet		274422	2019-04-08 16:30:16	2018-11-01 18:56:54	Cisco Spark Updates P... Updates A...		Permitir		
35	Navigation_Server	Navigation Internet	universal	DMZ DNS FINANZAS Trust-L3	Group_PRTG_ISSSTE Navigation Servidores Remedy_VS Servers Pasador PRTG	any	any	Internet		8593375	2019-04-08 16:30:29	2018-11-01 18:57:06	any	any	Permitir		
36	Updates1	LOGSHTTHRM Internet	interzone	DMZ DNS DMZ Laboratorios Trust-L3	Servers Loghythm VLANs to CrowdStrike	any	any	Internet	CrowdStrike Conne... Updates Loghythm	10368	2019-04-08 16:19:02	2018-11-01 18:53:31	tel web-br...	service-http service-https	Permitir		
37	Notificaciones Remedy H...	REMEDY Internet	universal	Trust-L3	Remedy Servers	any	any	Internet		6	2018-11-01 19:44:50	2018-11-01 19:44:50	Notificacio...	application-default	Permitir		
38	Impresora_Hector	LAN	universal	LAN	Indroque_5.204	any	any	WIFI	mpepar_4.12	22	2019-03-25 13:19:48	2019-03-22 13:50:36	any	application-default	Permitir	none	
39	Eps	LOCAL	universal	Trust-L3 SOC	Eps_5.17 Kaspersky_5.19 VLAN SOC	any	any	SOC Trust-L3		424227	2019-04-08 16:30:29	2019-03-21 16:59:57	any	any	Permitir	none	
40	Kaspersky	LOCAL	universal	Trust-L3	Kaspersky_5.19	any	any	Ciberinte		94579	2019-04-08 16:04:40	2019-03-21 17:00:01	any	any	Permitir		
41	Administracion	LOCAL	universal	LAN SOC WIFI	Administradores VLAN SOC	any	any	any		20523510	2019-04-08 16:30:30	2018-11-01 18:57:07	any	any	Permitir		
42	AdmonRemedy	LAN LOCAL	universal	LAN	alecadio_5.161	any	any	Trust-L3	Remedy_VS RemedyFgo RemedyDB RemedyWeb	4820	2019-04-08 16:23:34	2019-03-22 01:19:51	Port_3389 service-https		Permitir		
43	Servidor_Calidad	none	universal	LAN WIFI	Calidad host_192.168.4.39 host_192.168.4.41 host_192.168.4.48	any	any	Trust-L3	HOST_192.168.9.3	413	2019-04-03 14:09:02	2019-03-22 11:57:50	any	any	Permitir	none	
44	Calidad-PRTG	LAN	universal	LAN	Calidad	any	any	Trust-L3	PRTG1_5.10	18314	2019-04-04 18:20:07	2019-03-22 12:43:57	tel	application-default	Permitir	none	

45	Finanzas	LOCAL	universal	LAN	Finanzas	any	any	FINANZ	Finanzas_22.1	7946	2019-04-08 16:28:18	2019-03-21 17:01:45	any	any	Permitir		
46	HIGHT PRO	LOCAL	universal	LAN	any	any	any	FINANZ	Finanzas_22.1	17640	2019-04-08 16:30:23	2019-03-21 16:58:34	any	any	Permitir		
47	WIFI_CBER	TEMPORAL	universal	WIFI	apac_4.10	any	any	Ciberseg	VLAN Ciberseg	0	-	-	any	any	Permitir		
48	DNS interno Drop	DNS Interno	interzone	Trust-L3	any	any	any	Trust-L3	Internals DNS	151851	2019-04-08 16:30:28	2019-04-04 20:06:05	any	any	Denegar		
49	Impresoras-AD	LOCAL	interzone	Trust-L3	any	any	any	Trust-L3	Herramientas_Cor	6086422	2019-04-08 16:30:30	2018-11-01 18:57:05	any	any	Permitir		
50	Backups_Cellmanager	LOCAL	universal	Trust-L3	Host_192.168.8.2	any	any	SOC	192.168.3.2	0	-	-	any	any	SSH		
51	Impresoras	LOCAL	universal	Trust-L3	192.168.5.200	any	any	SOC	VLAN SOC	2	2019-03-25 22:10:06	2019-03-22 12:45:42	any	any	any		
52	Splunk Test	LOCAL	universal	Trust-L3	Mgt-PA-5050_1	any	any	SOC	Splunk_192.168.3.61	268	2019-04-07 14:00:05	2019-03-22 01:57:03	any	any	Syslog		
53	Internet VLAN-1	LOCAL	universal	Trust-L3	VLAN Servidores	any	any	DMZ NA	DMZ Server Pasap	2730	2019-04-08 16:01:18	2018-11-01 18:56:30	any	any	Permitir		
54	Idadi	LOCAL	universal	WIFI	IpsaBt_Group	any	any	Trust-L3	videconferencia...	80	2019-04-08 11:54:30	2019-03-22 12:02:46	any	any	Permitir		
55	SIBI	LOCAL	universal	WIFI	API_548	any	any	Trust-L3	192.168.8.1	87054	2019-04-08 16:29:44	2018-11-01 18:56:35	any	any	Permitir		
56	FileServer	FILESERVER	universal	LAN	VLAN Ciberseg	any	any	Trust-L3	FileServer_9_70	7369	2019-04-08 16:28:51	2018-11-01 18:55:00	any	any	FileServer		
57	Internet DNS to external	DNS Interno	interzone	Trust-L3	VLAN Oficinas	any	any	DMZ ON	Externals DNS	6328238	2019-04-08 16:30:29	2018-11-01 18:57:05	any	any	application-default		
58	Monitoreo	ADMINISTRACION	universal	Trust-L3	IPADICION_9_9	any	any	Ciberseg	any	3123293	2019-04-08 16:30:29	2018-11-01 18:57:06	any	any	Permitir		
59	Relay Interno	LOCAL	interzone	Trust-L3	Relay_SFTP	any	any	DMZ ON	SFTP-RELAY_10.1	360	2019-04-08 15:14:37	2019-03-22 01:57:03	any	any	smtp		
60	SFTP_Audit	LOCAL	interzone	DMZ DNS	SFTP-RELAY_10.1	any	any	SOC	Splunk_192.168.3.61	48180	2019-04-08 16:30:23	2019-03-21 16:58:31	any	any	syslog		
61	Administradores-VPN	VPN-GP	universal	VPN-GP	VPN_Rest	any	any	SOC	Abraham_Centur...	80	2019-04-07 14:07:18	2019-03-26 14:39:37	any	any	Permitir		
62	VPN TEMPORAL	TEMPORAL	universal	VPN-GP	VPN_Rest	any	any	Ciberseg	VLAN Ciberseg	0	-	-	any	any	Permitir		
63	VPN Client cybernetic	VPN-Alterna	universal	VPN-Alterna	VPN_Rest_Alterna	any	any	Trust-L3	Net_172.29.8.23	0	-	-	any	any	Permitir		
64	VPN-Ringreso-ciber	VPN-Alterna	universal	Trust-L3	Net_172.29.8.23	any	any	VPN-GP	VPN_Rest_Alterna	0	-	-	any	any	Permitir		
65	VPN_Remedy	VPN-GP	universal	VPN-GP	VPN_Rest	any	any	Trust-L3	Remedy_V5	0	-	-	any	any	Port_1433		
66	NOC PRGT_VPN	VPN-GP	universal	VPN-GP	VPN_Rest	any	any	Trust-L3	Host_192.168.9.150	111355	2019-04-05 14:47:39	2019-03-30 03:14:55	any	any	tel web-br...		
67	Directorio Activo	VPN-GP	universal	VPN-GP	VPN_Rest	any	any	Trust-L3	IP_192.168.9.153	292062	2019-04-07 14:26:36	2019-03-21 21:04:51	any	any	Directorio...		
68	VPN_FileServer	VPN-GP	universal	VPN-GP	VPN_Rest	any	any	Trust-L3	192.168.9.31	637	2019-04-06 09:18:17	2019-03-21 21:01:16	any	any	FileServer		
69	Finanzas-VPN	VPN-GP	universal	VPN-GP	VPN_Rest	any	any	FINANZ	Nuevo_Remedy_9...	5782	2019-04-04 21:29:24	2019-03-24 21:11:57	any	any	tel web-br...		
70	Updator-Cymmetria	Administracion	interzone	DMZ-SidHub	any	any	any	Internet	any	0	-	-	any	any	Permitir		
71	Respaldos Trust-L3 to DMZ	DNS-STRONG	interzone	Trust-L3	Respaldos Internet	any	any	DMZ NA	DMZ Server Pasap	0	-	-	any	any	application-default		

4.16 Políticas implícitas

A continuación, se muestran las políticas implícitas la cual bloquea todo lo no esté explícitamente permitido.

72	Intrazone-default	none	intrazone	any	any	any	any	Intrazone	any	933876	2019-04-08 16:30:27	2018-11-01 18:57:05	any	any	Permitir		
73	Interzone-default	none	interzone	any	any	any	any	any	any	10418557	2019-04-08 16:30:30	2018-11-01 18:57:07	any	any	Denegar		

4.17 Políticas Basadas en NAT

En la siguiente tabla se muestra las direcciones NAT existentes en la solución de seguridad firewall.

Nombre	Etiquetas	Zona de origen	Zona de destino	Paquete original			Paquete traducido			Uso de reglas			
				Interfaz de destino	Dirección de origen	Dirección de destino	Servicio	Traducción de origen	Traducción de destino	Recuento de aciertos	Último acierto	Primer acierto	
1 Publicacion_PRTG-F5	Publicaciones	Internet	Internet	ethernet1/2	any	NAT_PRTG_V5	any	none	destination-translation dirección: V5_PRTG	21153	2019-04-08 15:20:07	2019-04-02 14:14:40	
2 Publicacion_PRTG	Publicaciones	Internet	Internet	ethernet1/1	any	NAT_PRTG1	any	none	destination-translation dirección: PRTG_ISSSTE	1154573	2019-04-08 15:20:38	2018-11-01 18:56:57	
3 Publicacion_PRTG-2	Publicaciones	Internet	Internet	ethernet1/1	any	NAT_PRTG2	any	none	destination-translation dirección: PRTG2_ISSSTE	64626	2019-04-08 15:20:28	2019-04-02 15:13:50	
4 Publicacion_DNS_ISSTE	Publicaciones	Internet	Internet	ethernet1/1	any	NAT_DNS	any	none	destination-translation dirección: DNS_COM-1SSTE-COM	106953	2019-04-08 15:20:23	2018-11-01 18:18:58	
5 Publicacion_SFTP	Publicaciones	Internet	Internet	ethernet1/1	any	NAT_SFTP_12...	any	none	destination-translation dirección: SFTP-RELAY_10.1	50425	2019-03-27 15:03:20	2019-03-21 18:40:52	
6 Publicacion_SFTP-1	Publicaciones	DMZ DNS	Internet	ethernet1/1	SFTP-RELAY_10.1	any	any	static-ip NAT_SFTP_123.4	Indirección: no	ninguno	671345	2019-04-08 15:19:46	2018-11-13 18:18:20
7 MPLS_ISSSTE-6	ISSSTE	SOC Trust-L3	MPLS_ISSSTE	ethernet1/8	Host_192.168.9.1 Host_192.168.9.1 Host_192.168.9.1 Host_192.168.9.1 Host_192.168.9.1 Host_192.168.9.1 Host_192.168.9.1 mis...	any	any	dynamic-ip-and-port 10.90.11.6/28	Indirección: no	ninguno	1090480038	2019-04-08 15:20:39	2018-11-01 18:20:08
8 MPLS_ISSSTE-7	ISSSTE	SOC Trust-L3	MPLS_ISSSTE	ethernet1/8	Abraham_Centos...	any	any	dynamic-ip-and-port 10.90.11.7	Indirección: no	ninguno	277	2018-11-12 19:04:24	2018-11-12 19:00:53
9 MPLS_ISSSTE-8	ISSSTE	SOC Trust-L3	MPLS_ISSSTE	ethernet1/8	VLAN SOC	any	any	dynamic-ip-and-port 10.90.11.8	Indirección: no	ninguno	42479127	2019-04-08 15:20:39	2018-11-01 18:57:07
10 NAT_L2L_ISSSTE	ISSSTE	Trust-L3	L2L_ISSSTE	ethernet1/10	Host_192.168.9.1 Host_192.168.9.1 Host_192.168.9.1 Host_192.168.9.1	L2L_Nexo	any	dynamic-ip-and-port ethernet1/10	Indirección: no	ninguno	378039	2019-04-08 15:20:24	2018-11-01 18:20:07
11 Externos	Navigation Internet	Trust-L3	Internet	ethernet1/4	Net_172.29.0.0_20	any	any	dynamic-ip-and-port tunnel.11	Indirección: no	ninguno	6092501	2019-03-21 16:58:00	2018-11-01 18:20:08
12 Ciber_Astel	Navigation Internet	CiberAstel	Internet	ethernet1/4	VLAN CiberAstel...	any	any	dynamic-ip-and-port 189.210.45.92	Indirección: no	ninguno	2208708	2019-04-08 15:20:39	2019-02-05 19:10:07
13 Source Astel	Navigation Internet	DMZ DNS DMZ Labor DMZ NAS DMZ Sinh FINANZAS LAN SOC	Internet	ethernet1/1	any	any	any	dynamic-ip-and-port ethernet1/1	Indirección: no	ninguno	18115431	2019-04-08 15:20:36	2018-11-01 18:20:08
14 Source Alestra	Navigation Internet	DMZ DNS DMZ Labor DMZ NAS DMZ Sinh FINANZAS LAN SOC	Internet	ethernet1/4	any	any	any	dynamic-ip-and-port ethernet1/4	Indirección: no	ninguno	64341908	2019-04-08 15:20:39	2018-11-01 18:20:08

4.18 Perfiles de seguridad

A continuación, se muestran los perfiles de seguridad.

4.19 Perfil Antivirus

A continuación, se muestra el perfil de seguridad de antivirus.

		Desconfiadores				Excepciones de aplicación		
Nombre	Ubicación	Paquete Captu.	Nombre	Acción	Acción de WildFire	Nombre	Acción	Amenaza Excepciones
default	Predefinido	<input type="checkbox"/>	http	default (reset-both)	default (reset-both)			0
			smtp	default (alert)	default (alert)			
			imap	default (alert)	default (alert)			
			pop3	default (alert)	default (alert)			
			ftp	default (reset-both)	default (reset-both)			
			smb	default (reset-both)	default (reset-both)			
Strict protection	vsys1	<input checked="" type="checkbox"/>	http	default (reset-both)	default (reset-both)			0
			smtp	reset-both	reset-both			
			imap	default (alert)	default (alert)			
			pop3	default (alert)	default (alert)			
			ftp	default (reset-both)	default (reset-both)			
			smb	default (reset-both)	default (reset-both)			
Antivirus Alert Profile	vsys1	<input type="checkbox"/>	http	alert	reset-both			0
			smtp	alert	alert			
			imap	alert	alert			
			pop3	alert	alert			
			ftp	alert	reset-both			
			smb	alert	reset-both			
VA_Silent	vsys1	<input type="checkbox"/>	http	drop	default (reset-both)			0
			smtp	drop	reset-both			
			imap	drop	reset-both			
			pop3	drop	reset-both			
			ftp	drop	default (reset-both)			
			smb	drop	default (reset-both)			

4.20 Perfil Anti-Spyware

A continuación, se muestra el perfil de seguridad Anti-Spyware.

Nombre	Ubicación	Recuento	Nombre de regla	Nombre de amenaza	Gravedad	Acción	Captura de paquetes	Captura de paquetes DNS
default	Predefinido	Reglas: 4	simple-critical	any	critical	default	disable	disable
			simple-high	any	high	default	disable	
			simple-medium	any	medium	default	disable	
			simple-low	any	low	default	disable	
strict	Predefinido	Reglas: 5	simple-critical	any	critical	reset-both	disable	disable
			simple-high	any	high	reset-both	disable	
			simple-medium	any	medium	reset-both	disable	
			simple-informational	any	informational	default	disable	
			simple-low	any	low	default	disable	
Strict-PCAP-and-sinkhole	vsys1	Reglas: 5	simple-critical	any	critical	default	single-packet	extended-capture
			simple-high	any	high	default	single-packet	
			simple-medium	any	medium	default	single-packet	
			simple-low	any	low	default	single-packet	
			simple-informational	any	informational	default	disable	
AntiSpyware Alert Profile	vsys1	Reglas: 2	Critical	any	critical,high	alert	extended-capture	disable
			No-critical	any	low,medium	alert	disable	
SP_Silent	vsys1	Reglas: 2	Alto-Critico-Block	any	high,critical	drop	disable	disable
			Bajo-Medio.Alert	any	medium,low	alert	disable	

4.21 Perfil Protección de Vulnerabilidades

A continuación, se muestra el perfil de seguridad de protección de vulnerabilidades.

Nombre	Ubicación	Recuento	Nombre de regla	Nombre de amenaza	Tipo de host	Gravedad	Acción	Captura de paquetes
strict	Predefinido	Reglas: 10	simple-client-critical	any	client	critical	reset-both	disable
			simple-client-high	any	client	high	reset-both	disable
			simple-client-medium	any	client	medium	reset-both	disable
			simple-client-informational	any	client	informational	default	disable
			simple-client-low	any	client	low	default	disable
			simple-server-critical	any	server	critical	reset-both	disable
			simple-server-high	any	server	high	reset-both	disable
			más...					
			simple-client-critical	any	client	critical	default	disable
			simple-client-high	any	client	high	default	disable
default	Predefinido	Reglas: 6	simple-client-medium	any	client	medium	default	disable
			simple-server-critical	any	server	critical	default	disable
			simple-server-high	any	server	high	default	disable
			simple-server-medium	any	server	medium	default	disable
			Reconn	any	client	any	drop	disable
Vulnerability Alert Profile	vsys1	Reglas: 1	Servidores_Windows	any	server	any	default	disable
Servicios_Web	vsys1	Reglas: 1	Alto-Critico-Block	any	any	high,critical	block-ip (source-and-destination,3600)	disable
Publicaciones	vsys1	Reglas: 2	Low-Medio-Alert	any	any	medium,low	default	disable
Navegacion	vsys1	Reglas: 2	Alto-Critico-Block	any	client	critical,high	drop	disable
			Bajo-Medio-Alert	any	client	medium,low	default	disable
FileServer	vsys1	Reglas: 5	Exploit	any	any	critical,high,medium	default	disable
			EjecucionCodigo	any	any	critical,high,medium	default	disable
			EjecucionComandos	any	any	critical,high,medium	default	disable
			Overflow	any	any	critical,high,medium	default	disable
			Escaneo	any	any	critical,high,medium	default	disable
Clientes	vsys1	Reglas: 5	Exploit	any	any	critical,high	default	disable
			EjecucionCodigo	any	any	critical,high	default	disable
			EjecucionComandos	any	any	critical,high	default	disable
			Overflow	any	any	critical,high	default	disable
			Escaneo	any	any	critical,high	default	disable
Red Interna	vsys1	Reglas: 3	Critical	any	any	critical	drop	disable
			Alta	any	any	high	drop	disable
			Media	any	any	medium	default	disable
Monitoreo	vsys1	Reglas: 3	Critical	any	any	critical	alert	disable
			Alta	any	any	high	alert	disable
			Media	any	any	medium	alert	disable

4.22 Perfil Filtrado de URL

A continuación, se muestra el perfil de seguridad de filtrado URL.

sgi@silent4business.com



Insurgentes Sur #2453, Piso 4, Col, Tizapán San Ángel, Álvaro Obregón, 01090 Ciudad de México, CDMX

"La información contenida en este documento es propiedad intelectual de SILENT4BUSINESS SA DE CV, por lo que queda estrictamente prohibida su reproducción, modificación, divulgación, uso o aprovechamiento por cualquier medio impreso, mecánico o electrónico sin la autorización previa por escrito de Silent4Business."



Nombre	Ubicación	Lista de bloqueadas	Acción para lista de bloques	Lista de permitidas	Acceso a sitio	Envío de credencial de usuario	Inserción de encabezado HTTP
default	Predefinido		block		Allow Categories (37) Alert Categories (0) Continue Categories (0) Block Categories (9) Override Categories (0)	Allow Categories (66) Alert Categories (0) Continue Categories (0) Block Categories (0)	
URL Alerting Profile	vsys1		block		Allow Categories (2) Alert Categories (98) Continue Categories (0) Block Categories (1) Override Categories (0)	Allow Categories (2) Alert Categories (98) Continue Categories (0) Block Categories (1)	
Navegación Básica	vsys1		block		Allow Categories (12) Alert Categories (39) Continue Categories (0) Block Categories (29) Override Categories (0)	Allow Categories (50) Alert Categories (1) Continue Categories (0) Block Categories (29)	
General	vsys1		block		Allow Categories (0) Alert Categories (63) Continue Categories (0) Block Categories (16) Override Categories (0)	Allow Categories (63) Alert Categories (0) Continue Categories (0) Block Categories (16)	
Navegación RH	vsys1		block		Allow Categories (0) Alert Categories (55) Continue Categories (0) Block Categories (24) Override Categories (0)	Allow Categories (54) Alert Categories (1) Continue Categories (0) Block Categories (24)	
Navegación Avanzada	vsys1		block		Allow Categories (0) Alert Categories (32) Continue Categories (0) Block Categories (27) Override Categories (0)	Allow Categories (31) Alert Categories (1) Continue Categories (0) Block Categories (27)	
CSOC	vsys1		block		Override Categories (0) Allow Categories (50) Alert Categories (50) Continue Categories (0) Block Categories (11) Override Categories (0)	Allow Categories (68) Alert Categories (0) Continue Categories (0) Block Categories (11)	
Monitoreo	vsys1		block		Override Categories (0) Allow Categories (0) Alert Categories (78) Continue Categories (0) Block Categories (1) Override Categories (0)	Allow Categories (78) Alert Categories (0) Continue Categories (0) Block Categories (1)	
Navegación CSOC	vsys1		block		Allow Categories (0) Alert Categories (64) Continue Categories (0) Block Categories (15) Override Categories (0)	Allow Categories (83) Alert Categories (1) Continue Categories (0) Block Categories (15)	
Bloqueo UltraSurf	vsys1		block		Allow Categories (79) Alert Categories (0) Continue Categories (0) Block Categories (1) Override Categories (0)	Allow Categories (79) Alert Categories (0) Continue Categories (0) Block Categories (1)	

4.23 Perfil Bloqueo de archivos

A continuación, se muestra el perfil de seguridad de bloqueo de archivos.

Nombre	Ubicación	Nombre de regla	Aplicaciones	Tipos de archivos	Dirección	Acción
basic file blocking	Predefinido	Block high risk file types Continue prompt encrypted files Log all other file types	any any any	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, ocs, PE, pdf, rar, sct, torrent, vbs, wsf encrypted-rar, encrypted-zip any	both both both	block continue alert
strict file blocking	Predefinido	Block all risky file types Block encrypted files Log all other file types	any any any	7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, jar, msi, Multi-Level-Encoding, ocs, PE, pdf, rar, sct, tar, torrent, vbs, wsf encrypted-rar, encrypted-zip any	both both both	block block alert
Strict	vsys1	Files to block Files req continue Files to Alert	any any any	bat, chm, class, dll, hlp, jar, link, Multi-Level-Encoding, PE, torrent, vbs encrypted-rar, encrypted-zip, exe, gzip, rar, zip any	both both both	block continue alert
File Alerting Profile	vsys1	All	any	any	both	alert
Block_Silent	vsys1	Torrents	any	torrent	both	block
FileServer	vsys1	Ejecutables	any	bat, cab, cmd, dll, exe, iso, msi, msi, vbs	both	alert
		Multimedia	any	avi, avi-divx, avi-xvid, cab, flash, flv, mp3, mpeg, mpeg-ts	both	block
		Ejecutables	any	cab, class, dll, exe, exe, jar, msi, pkg, reg, sh, vbs	both	block
		Archivos	any	acc, dmg, iso, torrent	both	block

4.24 Perfil WildFire Analysis

A continuación, se muestra el perfil de seguridad wildfire analysis.

Nombre	Ubicación	Nombre de regla	Aplicaciones	Tipos de archivos	Dirección	Análisis
default	Predefinido	default	any	any	both	public-cloud
Strict	vsys1	Semi-all	any	any	both	public-cloud
WildFire Analysis Profile	vsys1	All	any	any	both	public-cloud
WildFire_Silent	vsys1	Moviles	any	apk	download	public-cloud
		Documentos	any	ms-office, pdf, pe	both	public-cloud
		Adjuntos	any	email-link, flash, jar	download	public-cloud
		SO	any	linux, MacOSX	download	public-cloud

4.25 Perfiles de autenticación

En esta sección se muestran los perfiles de autenticación configurados en el Firewall.

Nombre	Ubicación	Intentos fallidos (n.º)	Tiempo de bloqueo (minutos)	Lista de permitidas	Autenticación	Perfil de servidor	Factores de autenticación	Otros	Usuarios bloqueados
Interno	vsys1	10	1	all	Local				none
SAS-LDAP	vsys1	0	0	all	LDAP	User-ID AD		Mensaje de vencimiento de contraseña: 7 días	none
Remedy	vsys1	0	0	all	Local				none
localusers	vsys1	0	0	all	Local				none
Usuarios_Externos	vsys1	0	0	cybernetic	Local				none

Perfil de autenticación

Nombre

Interno

Ubicación

vsys1

Autenticación

Factores

Avanzado

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

ACEPTAR

Cancelar

Perfil de autenticación

Nombre

S4B-LDAP

Ubicación

vsys1

Autenticación

Factores

Avanzado

Tipo

LDAP

Perfil de servidor

User-ID AD

Atributo de inicio de sesión

Aviso de caducidad de contraseña

7

Número de días antes de advertir a un usuario acerca de la caducidad de la clave.

Dominio de usuario

s4b.com

Modificador de nombre de usuario

%USERINPUT%

Inicio de sesión único

Dominio de Kerberos

s4b.com

Keytab de Kerberos

Haga clic en "Importar" para configurar este campo

X

Importar

ACEPTAR

Cancelar

Perfil de autenticación

Nombre

Remedy

Ubicación

vsys1

Autenticación

Factores

Avanzado

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

ACEPTAR

Cancelar

Perfil de autenticación

Nombre

localusers

Ubicación

vsys1

Autenticación

Factores

Avanzado

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

ACEPTAR

Cancelar

Perfil de autenticación

Nombre:

Ubicación:

Autenticación Factores Avanzado

Tipo:

Dominio de usuario:

Modificador de nombre de usuario:

Inicio de sesión único

Dominio de Kerberos:

Keytab de Kerberos: X Importar

ACEPTAR Cancelar

4.26 Servidores LDAP

Perfil de servidor LDAP

Nombre de perfil:

Ubicación:

Lista de servidor

Nombre	Servidor LDAP	Puerto
AD Principal	192.168.9.30	389
AD Secundario	192.168.9.31	389

+ Añadir - Eliminar

Introduzca la dirección IP o FQDN del servidor LDAP

Configuración de servidor

Tipo:

DN base:

Enlazar DN:

Contraseña:

Confirmar Contraseña:

Tiempo de espera de enlace:

Tiempo de espera de búsqueda:

Intervalo de reintento:

☐ Solicitar conexión SSL/TLS protegida

☐ Verificar certificado de servidor para sesiones SSL

ACEPTAR Cancelar

DIRECCIONES Y GRUPOS DE RED

Direcciones

Dado que son 743 direcciones definidas en el Firewall. Se acompaña el presente documento con el archivo:

sgi@silent4business.com



Insurgentes Sur #2453, Piso 4, Col, Tizapán San Ángel, Álvaro Obregón, 01090 Ciudad de México, CDMX

"La información contenida en este documento es propiedad intelectual de SILENT4BUSINESS SA DE CV, por lo que queda estrictamente prohibida su reproducción, modificación, divulgación, uso o aprovechamiento por cualquier medio impreso, mecánico o electrónico sin la autorización previa por escrito de Silent4Business."



Memoria Técnica FW S4B Anexo 1 Objetos.csv

4.27 Grupos de Direcciones

A continuación, se muestran los grupo de direcciones definidos en el Firewall.

Nombre	Ubicación	Recuento de miembros	Direcciones	Etiquetas
Administradores	vsys1	4	acarillo_4.28 chernandez_4.25 chernandez_5.152 lvallie_4.8	
API_548	vsys1	5	AP_192.168.4.1 AP_192.168.4.2 AP_192.168.4.3 AP_192.168.4.4 AP_192.168.4.5	
Calidad	vsys1	3	egomez_5.149 flabares_5.147 rpalomero_5.144	
CDR_ISSSTE	vsys1	2	Host_192.168.9.165 Host_192.168.9.166	
Correo_Externo	vsys1	2	Netxar_inmap Netxar_outmap	
CrowdStrike Connections	vsys1	4	Public Updates CrowdStrike1 Public Updates CrowdStrike2 Public Updates CrowdStrike3 Public Updates CrowdStrike4	
Externals DNS	vsys1	3	DNS Server DNS 1 DNS Server DNS 2 DNS_Externo	
Finanzas	vsys1	5	asentiller_5.132 hrodriguez_5.204 jflores_5.155 labadia_5.145 Timp_MPMO_5.1	
GPO-MODELO	vsys1	5	Modelo_10.88.3.152 Modelo_10.88.3.153 Modelo_10.88.3.154 Modelo_10.89.144.53 Modelo_10.89.144.54	
Gpo_Actividad_Suspechosa	vsys1	2	S48_A5 S48_A5_1	
Group_PRTG_ISSSTE	vsys1	10	Host_192.168.9.144 Host_192.168.9.145 Host_192.168.9.146 Host_192.168.9.147 Host_192.168.9.148 Host_192.168.9.149 Host_192.168.9.150 mike...	
Herramientas_Corporativas	vsys1	7	Impresora_5.209 Impresora_5.203 Impresora_5.201 Internals DNS Kaspersky_5.19 Remedy_VS WSUS_5.33	
Internals DNS	vsys1	2	Server DNS Interno 1 Server DNS Interno 2	
Ipad_Grupo	vsys1	2	Ipad_192.168.4.15 Ipad_192.168.4.18	
Listafianza	vsys1	1	messenger.provideresupport.com	
Mgt PaloAltoNetworks	vsys1	4	Mgt PA-5050_1 Mgt PA-5050_2 Mgt Panorama Panorama_110.10	
Monitoreo Externo PRTG	vsys1	5	Public Enlace Alireza Public Enlace Ariel Public Enlace Ariel bgo Public Horaki Dashboard Public Horaki snmp	
Navegacion Servidores	vsys1	16	cuckoo.4b.com_9.26 DMZ Server DNS 1 DMZ Server DNS 2 DNS_Externo Epo_9.17 FS_9.4 SPADHON_9.9 mike...	
Navegacion_Basica	vsys1	4	flabares_5.147 flabares_4.11 vysp_4.13 vysp_5.146	
NOC	vsys1	10	Analista05 Analista06 Analista07 Analista08 Analista11 Analista12 Analista13 mike...	
NTPs-Publics	vsys1	5	Public NTP 1 Public NTP 2 Public NTP 3 Public NTP 4 Public NTP 5	
Publics OpenDNS	vsys1	2	Public OpenDNS 1 Public OpenDNS 2	

Redes_Royal	vsys1	7	Red_Royal_1 Red_Royal_2 Red_Royal_3 Red_Royal_4 Red_Royal_5 Red_Royal_6 Red_Royal_7
Relay_SHTP	vsys1	6	Epo_9.17 Impresora_5.200 Impresora_5.203 Kaspersky_9.19 PA1_110.11 PA2_110.12
Remedy Servers	vsys1	3	RemedyApp RemedyDB RemedyWeb
Remedy_VS	vsys1	6	Remedy_9.6 Remedy_9.7 Remedy_9.12 Remedy_9.13 Remedy_9.13-16 Remedy_VS_9.29
Respaldo Interiores	vsys1	5	VLAN Admin VLAN Oficinas VLAN Servidores VLAN SOC VLAN Wireless
S4B_AS	vsys1	302	185.94.111.1 AS_107.170.198.108 AS_1119.10.199 AS_1119.14.83 AS_1234.201.109 AS_5140.30.11 AS_23140.82.66 mic...
S4B_AS_1	vsys1	87	AS_1179.146.156 AS_250.55.162 AS_37.221.178.184 AS_45.227.255.82 AS_46.209.216.233 AS_49.363.34.79 AS_58.59.2.26 mic...
Servers LogRhythm	vsys1	4	Server LogRhythm DI Server LogRhythm DP Server LogRhythm PH Server LogRhythm VC
Servers Passler PRIG	vsys1	2	PRIG1_9.10 PRIG2_9.11
SOC	vsys1	4	Analista01 Analista02 Analista03 Analista04
Updates AugurioX	vsys1	6	Public Updates AugurioX1 Public Updates AugurioX2 Public Updates AugurioX3 Public Updates AugurioX4 Public Updates AugurioX5 Public Updates AugurioX6
Updates LogRhythm	vsys1	59	Public Updates 9 Public Updates LR1 Public Updates LR2 Public Updates LR3 Public Updates LR4 Public Updates LR5 Public Updates LR6 mic...
Updates PRIG	vsys1	8	Public Updates PRIG1 Public Updates PRIG2 Public Updates PRIG3 Public Updates PRIG4 Public Updates PRIG5 Public Updates PRIG6 Public Updates PRIG7 mic...
Usuarios Permisos Especiales	vsys1	5	Abraham_Centos_3.10 acwills_4.28 Analista11 hualle_4.8 Net_172.29.0.0_23
VLANs to CrowdStrike	vsys1	8	DMZ Server DNS 1 DMZ Server DNS 2 VLAN Admin VLAN Oficinas VLAN SegFisica VLAN Servidores VLAN SOC mic...
VPR Nube-augurio	vsys1	7	PRIG1_9.10 PRIG2_9.11 Server DNS Interno 1 Server DNS Interno 2 Server LogRhythm DI Server LogRhythm DP Server LogRhythm PH

4.28 Objetos y grupos de servicios

En esta sección se muestran los objetos y grupos de servicios definidos en el Firewall.

Objetos

Nombre	Ubicación	Protocolo	Puerto de destino	Etiquetas
<input type="checkbox"/> DNS	vsys1	UDP	53	
<input type="checkbox"/> FTP	vsys1	TCP	21	
<input type="checkbox"/> Port_1433	vsys1	TCP	1433	
<input type="checkbox"/> Port_23560	vsys1	TCP	23560	
<input type="checkbox"/> Port_3389	vsys1	TCP	3389	
<input type="checkbox"/> Port_5020	vsys1	TCP	5020	
<input type="checkbox"/> Port_6870	vsys1	TCP	6870	
<input type="checkbox"/> Port_8118	vsys1	TCP	8118	
<input type="checkbox"/> PRGTG to Meraki TCP ida	vsys1	TCP	16100	
<input type="checkbox"/> SCCP	vsys1	TCP	2000	
<input type="checkbox"/> service-http	Predefinido	TCP	80,8080	
<input type="checkbox"/> service-https	Predefinido	TCP	443	
<input type="checkbox"/> SIP	vsys1	TCP	5060	
<input type="checkbox"/> SIP_UDP	vsys1	UDP	5060	
<input type="checkbox"/> SMTP	vsys1	TCP	25	
<input type="checkbox"/> SMTPS over TLS	vsys1	TCP	587	
<input type="checkbox"/> SSH	vsys1	TCP	22	
<input type="checkbox"/> ssh-zero	vsys1	TCP	1194	
<input type="checkbox"/> Syslog	vsys1	UDP	514	
<input type="checkbox"/> TCP_1024-65535	vsys1	TCP	1024-65535	
<input type="checkbox"/> TCP_1099	vsys1	TCP	1099	
<input type="checkbox"/> TCP_1138	vsys1	TCP	1138	
<input type="checkbox"/> TCP_1139	vsys1	TCP	1139	
<input type="checkbox"/> TCP_135	vsys1	TCP	135	
<input type="checkbox"/> TCP_137	vsys1	TCP	137	
<input type="checkbox"/> TCP_139	vsys1	TCP	139	
<input type="checkbox"/> TCP_1434	vsys1	TCP	1434	
<input type="checkbox"/> TCP_1775	vsys1	TCP	1775	
<input type="checkbox"/> TCP_1880	vsys1	TCP	1880	
<input type="checkbox"/> TCP_2000	vsys1	TCP	2000	
<input type="checkbox"/> TCP_2003	vsys1	TCP	2003	
<input type="checkbox"/> TCP_2083	vsys1	TCP	2083	
<input type="checkbox"/> TCP_2121	vsys1	TCP	2121	
<input type="checkbox"/> TCP_3268	vsys1	TCP	3268	
<input type="checkbox"/> TCP_3269	vsys1	TCP	3269	
<input type="checkbox"/> TCP_389	vsys1	TCP	389	
<input type="checkbox"/> TCP_4100	vsys1	TCP	4100	
<input type="checkbox"/> TCP_42	vsys1	TCP	42	
<input type="checkbox"/> TCP_445	vsys1	TCP	445	
<input type="checkbox"/> TCP_464	vsys1	TCP	464	
<input type="checkbox"/> TCP_465	vsys1	TCP	465	
<input type="checkbox"/> TCP_49156	vsys1	TCP	49156-49159	
<input type="checkbox"/> TCP_49158	vsys1	TCP	49158	
<input type="checkbox"/> TCP_52600	vsys1	TCP	52600	
<input type="checkbox"/> TCP_53	vsys1	TCP	53	
<input type="checkbox"/> TCP_543	vsys1	TCP	543	
<input type="checkbox"/> TCP_587	vsys1	TCP	587	
<input type="checkbox"/> TCP_636	vsys1	TCP	636	
<input type="checkbox"/> TCP_7653	vsys1	TCP	7653	
<input type="checkbox"/> TCP_8080	vsys1	TCP	8080	
<input type="checkbox"/> TCP_8081	vsys1	TCP	8081	
<input type="checkbox"/> TCP_82	vsys1	TCP	82	
<input type="checkbox"/> TCP_8443	vsys1	TCP	8443	
<input type="checkbox"/> TCP_8473	vsys1	TCP	8473	
<input type="checkbox"/> TCP_88	vsys1	TCP	88	
<input type="checkbox"/> TCP_9047	vsys1	TCP	9047	
<input type="checkbox"/> TCP_9049-9082	vsys1	TCP	9047-9082	
<input type="checkbox"/> TCP_9080	vsys1	TCP	9080	
<input type="checkbox"/> TCP_993	vsys1	TCP	993	
<input type="checkbox"/> FTP_TCP	vsys1	TCP	69	
<input type="checkbox"/> FTP_UDP	vsys1	UDP	69	
<input type="checkbox"/> UDP_137	vsys1	UDP	137	
<input type="checkbox"/> UDP_137-139	vsys1	UDP	137-139	
<input type="checkbox"/> UDP_123	vsys1	UDP	123	
<input type="checkbox"/> UDP_135	vsys1	UDP	135	
<input type="checkbox"/> UDP_137	vsys1	UDP	137	
<input type="checkbox"/> UDP_138	vsys1	UDP	138	
<input type="checkbox"/> UDP_1434	vsys1	UDP	1434	
<input type="checkbox"/> UDP_2121	vsys1	UDP	2121	
<input type="checkbox"/> UDP_389	vsys1	UDP	389	
<input type="checkbox"/> UDP_445	vsys1	UDP	445	
<input type="checkbox"/> UDP_464	vsys1	UDP	464	
<input type="checkbox"/> UDP_52600	vsys1	UDP	52600	
<input type="checkbox"/> UDP_53	vsys1	UDP	53	
<input type="checkbox"/> UDP_88	vsys1	UDP	88	
<input type="checkbox"/> UDP_9047	vsys1	UDP	9047	
<input type="checkbox"/> UDP_9080	vsys1	TCP	9080	

4.29 Grupos de Servicios

Nombre	Ubicación	Miembros	Servicios	Etiquetas
Contpaqi	vsys1	7	TCP_1024-65535 TCP_1099 TCP_1138 TCP_1139 TCP_1775 TCP_2003 TCP_9049-9082	
Correo_Externo	vsys1	2	TCP_465 TCP_993	
Directorio_Activo	vsys1	18	TCP_42 TCP_53 TCP_88 TCP_125 TCP_139 TCP_209 TCP_445 más...	
GpsClient_Softphone	vsys1	5	Port_6970 TCP_3000 TFIP_TCP TFIP_UDP UDP_137	
Mpro	vsys1	22	Port_1433 service-http service-https TCP_135 TCP_137 TCP_139 TCP_445 más...	
Navegacion	vsys1	9	service-http service-https TCP_82 TCP_943 TCP_2083 TCP_4100 TCP_7653 más...	

4.30 Diagrama de red

Anexos de Configuración de la solución tecnológica Seguridad Perimetral “Palo Alto Networks”

NOMBRE DOCUMENTO	DEL	DESCRIPCIÓN, PROPÓSITO	NOMBRE DEL ARCHIVO ANEXO
Anexo 1		Direcciones definidas en el Firewall	Memoria Técnica FW S4B Anexo 1 Objetos.csv

4.31 Control de versiones

FECHA		No. REVISIÓN	CAMBIO REALIZADO
Abril 2019		1	Creación

5 Anexos

No aplica.