

CREACIÓN DE REGLAS DE NAT

ROL	NOMBRE	CARGO / ROL
Elaborado nor:	Arturo David Ochoa Surco	Especialista en Arquitectura de Soluciones TI
	Daniel Fernando Vicente Vilca Romero	Asistente de Infraestructura de Redes y Comunicaciones
Revisado por:	Gustavo Adolfo Bernal Soto	Jefe (t) de la Unidad de Modernización
Aprobado por:	José Antonio Callirgos Paz	Jefe de la Oficina de Tecnología de la Información



Código: GTI-OTI-IN007

CONTROL DE CAMBIOS

N°	Ítems (Sección del documento)	Descripción del cambio
-	-	Versión inicial del documento



ÍNDICE

1.	OBJETIVO	4
2.	ALCANCE	4
3.	SIGLAS / ACRONIMOS	4
4.	DEFINICIONES	4
5.	DESARROLLO DEL INSTRUCTIVO	4
	5.1 INGRESO A CONSOLA SOPHOS FIREWALL. 5.2 CONFIGURACIÓN REGLAS DE FIREWALL 5.3 CONFIGURACIÓN REGLAS NAT	.4 .5 .7



Página 4 de 10

1. OBJETIVO

Establecer las instrucciones para la creación de reglas de NAT para que un dispositivo de red, como un firewall, pueda traducir las direcciones IP y puertos para la correcta gestión del tráfico entre redes internas (privadas) y externas (públicas, como Internet).

2. ALCANCE

El presente documento es de aplicación obligatoria para el equipo de infraestructura y soporte técnico de la Oficina de Tecnologías de Información.

3. SIGLAS / ACRONIMOS

- OTI : Oficina de Tecnologías de Información
- NAT : Network Address Translation (Traducción de Direcciones de Red).

INSTRUCTIVO

Código: GTI-OTI-IN007

IP : Protocolo de Internet

4. DEFINICIONES

- **4.1 Plataforma de Firewall Sophos:** Es una solución de seguridad de red diseñada para proteger sistemas informáticos y redes contra amenazas y ataques cibernéticos. Sophos es una empresa reconocida en el ámbito de la ciberseguridad y ofrece diversas soluciones de seguridad, entre las que destacan sus firewalls.
- **4.2 Regla:** Es una directiva o configuración específica que se aplica en una red para controlar y gestionar el tráfico de datos, mejorar la seguridad, y asegurar el rendimiento adecuado de la red. Estas reglas son esenciales para el funcionamiento eficaz y seguro de una red y se implementan en dispositivos de red como firewalls, routers, switches y sistemas de prevención de intrusiones (IPS).
- 4.3 Reglas de NAT: Son configuraciones específicas que determinan cómo un dispositivo de red, como un router o firewall, debe traducir las direcciones IP y los números de puerto en los paquetes de datos mientras se mueven entre una red interna (privada) y una red externa (pública, como Internet). Estas reglas son fundamentales para el funcionamiento del NAT, permitiendo a múltiples dispositivos en una red local compartir una única dirección IP pública y gestionar el tráfico entrante y saliente de manera segura y eficiente.
- 4.4 Zona de origen: Es la red desde la cual se inicia el tráfico de datos.
- **4.5 Zona de destino:** Es la red desde la cual se dirige el tráfico de datos.

5. DESARROLLO DEL INSTRUCTIVO

5.1 INGRESO A LA CONSOLA SOPHOS FIREWALL.

- a) Acceder a la plataforma mediante el siguiente enlace https://10.10.1.1:4443/webconsole/webpages/login.jsp.
- b) Ingresar el usuario y contraseña de dominio asignada en la pantalla de inicio de sesión:



INSTRUCTIVO Código: GTI-OTI-IN007



5.2 CONFIGURACIÓN REGLAS DE FIREWALL

a) En el menú izquierdo, seleccionar "Reglas y políticas" y luego "Reglas de Firewall":

SOPHOS C	Re	egla	is y p	olítica	S					Comentarios 👘 Guia	s explicativas Vi	tor de registros Ayuda adminiĝiso SUPERINTENDENCIANACIONAL DE SEI	iphoský sunassigobipa • RVICIOS DE SANEAMIENTO
Informes					Reglas de firewall			Regias NAT				Reglas de inspección SSL/TLS	
Protección de día cero Diagnósticos	e		PV6	Desactivar	filtro						Añadir r	egla de firewall 🐱 Desectiv	ar Eliminar
PROTEGER	T	ipo de re	egia		Zona de origen	Zona de destino	Estado	▼ ID de regli Add Filter ▼					Restablecer filtro
Reglas y políticas					Nombre		Origen	Destino	Qué	D	Acción	Función y servício	
Prevención de Intrusiones			1	1	ACCESO VPN TEMP entrada 0 B, salida 0 B		VPN, Cualquier host, vpn_pms	LAN, 1010.3.9-ad	Cualquier servicio	#92	Aceptar	(195) AF WEELARD (195) HS) Driverskit (199) (199)	Θ
Web Aplicaciones			s	1	ACCESO VPN entrada 1.66 TB, salida 1.70 TB		VPN, Cualquier host, GRUPO_VPN[LAN, Cualquier host	Cualquier servicio	\$66	Aceptar	(PSTAC INCLUSE (PSTAC) Construction (PSTAC)	Θ
Inalámbrico Correo electrónico	1		3	<	dialacole entrada 21.12 MB, salida 24.21 MB		LAN, 10.10.3.223	WAN, 185 32 76 134, 185 32 76 176	SIP, RTP, RTP-2, 2211	#65	Aceptar	(1951) AV DACELAPPICATE HET	Θ

b) Hacer clic en "Añadir regla de Firewall" y seleccionar "Nueva regla de Firewall":

R	egla	s y p	olítica	IS				Comentarios 🖬 Gu	las explicativas Vi	sor de registros Ayu SUPERINTENDENCIA	ida admini NACIONAL DE	() sophosxy sunass gob.pe SERVICIOS DE SANEAMIENT
				Reglas de firewall		Regias NAT				Reglas de inspección SS	L/TLS	
æ	-	Pv6	Desactivar	filtro					Añadir r	egla de firewall 🛛 🗸	Dese	ctivar Eliminar
1	îpo de r	igla		Zona de origen	stino Estado	ID de regi Add Filter 👻		1	Nueva regla de J	mpwall		Restablecer filtr
				Nombre	Origen	Destino	Qué	ID	Asistente de aco	ceso al servidor		
:		1	1	ACCESO VPN TEMP entrada 0 B, salida 0 B	VPN, Cualquier host, vpn_pms	LAN, 10.10.3.9-ad	Cualquier servicio	#92	(DNAT)			
		2		ACCESO VPN entrade 1.66 TB, salide 1.70 TB	VPN, Cualquier host, GRUP0_VPN[LAN, Cualquier host	Cualquier servicio	#66	Aceptar		10000 Herei	Θ
		з	<	dialappie entrada 21.12 MB, salida 24.21 MB	LAN, 10.10.3.223	WAN, 185 32 76 134, 185 32 76 176.	SIP, RTP, RTP-2, 2211	#65	Aceptar	DPS126/TWORLAN	100	Θ
		•		LAN->WAN entrade 87.38 GB, salida 1.02.55 GB								/
				Network_Policy_Administrator								/

adir regla de firewall		Comentarios IN Guias explicativas Visor de registros Ayuda admin@sophosag suna SUPERINTENDENCIA NACIONAL DE SERVICIOS DE SA
Estado de la regla		
lombre de regla *	Descripción	Posición de regla
Introducir Nombae de regla	Introducir Descripción	Abajo 🔽
cción		Grupo de reglas
Aceptar		Automático
Registrar tráfico de firewall Registra el tráfico que coincide con esta regia de firewall en el dispositivo (por servidor syslog configurado.	v defecta) o en el	De forma automática se añade una regla a un grupo existente en función de la primera coincidencia con el tipo de regla y las zonas de origen-destino.
Esca regia se anacira automaticamente a grupo de r	Tugas Der 2004	
)rigen eleccione las zonas, redes y dispositivos de origen. a regla se aplica al tráfico de estos origenes durante el periodo de tier	impo programado.	
brigen eleccione las zonas, redes y dispositivos de origen. engla es aplica al tráficos de estos origenes durante el periodo de tre nega de origen *	impo programado. Dispositivos y redex de origen *	Duranta la hora programada
trigen eleccione las zonas, nelles y dispositivos de origen. e reção es aplicas al tráficio de estos origenes durante el penodo de tele unas de origen *	Inge programads. Dispositives y relate de origen * CUALQUIERA	Duranta la fora programada Sempre
htigen executive la zonea, nodes y dispositives de angen. Les availes a attalistes de estos origines durante el periodo de tele anea de origin *	mise programado. Dispositivos y velos de organ * CUALQUIERA	Currente la livera programada Sempre Sonocere para aplicar la regia a un periodo de formanyo de los la semanas específicos.
Driggen unecome tes somen, reder y dispositives de erigen: a reçõe e activa el tráfico de estos origenes durante el pendos de tes anas de origen * Mador nuevo elemento	repo programado. Dispositivos y rede de organ * CUALQUIERA Madr nuevo elemento	Curants la hora programada Serrora Soloccione para aplicar la regia e un periodo de Tierray y de de la semana expecíficas.
Srigen Ander nuevo elemento	rrge programado: Dispublica y rede de orgen * CUALQUERA Alador nuevo elemento Bates de detos *	Curants is hore programmatic Services Software per subject is regis a un person de transcer y de la te services expectitions.
Drigen executors et al zones, review y dispositivos de enfers. executors et al zones, review y dispositivos de enfers. executors et al zones, review y dispositivos y enforces de streates et al particido de tree anales et al particido de tree anales et al particido de tree anales et al particidos de tree anales et al particidos et al trainfers anales et al particidos et al trainfers hacine estas destinos. Destino y serviciolos executors et al trainfers hacine estas destinos. a regis se activa al trainfers hacine estas destinos. anales de stactino *	Innee programado. Dispositivos y redes de origen * CUALQUIERA Afadar nuevo elemento Redes de destroe * CUALQUIERA	Durante la hora programada Serregne Sociocomo para najbara la suj portudo de tierray y de de la somarea específicas. Servicios *
Higgen werden bis zuman, nutes y dispositives de origen. werdes ex aplica al traffica de exitos origenes durante el periodo de tem exe de origen * Aflador nuevo elemento Destino y servicios executos e las banas, ruites dispositivos y servicios de destino. rengia se aducta al traffico hacies estas destinos. mas de destino *	rege programado: Dispublica y rede de organ * CLALQUIERA Madr nuevo elemento Refes de destro * CLALQUIERA CLALQUIERA	Curates is hole programmals Services - Services - Services - CULAQUERA

ESTE DOCUMENTO IMPRESO ES UNA COPIA NO CONTROLADA Para ver el documento controlado ingrese al portal del SIG de la Sunass Uso Interno



c) Asignar un nombre a la regla y habilitar la opción "Registrar tráfico de firewall":

0	K Estado de la regla
No	ombre de regla *
F	Permitir_Morea
Ac	ción
	Acep
~	Registrar tráfico de firewall
	Registra el tráfico que coincide con esta regla de firewall en el dispositivo (por defecto) o servidor evelos configurado

d) Seleccionar el grupo de reglas correspondientes:

WAN->LAN				

e) Agregar la zona de origen:

Oriaen		
Seleccione las zonas, redes y	y dispositivos de origen.	
La regla se aplica al tráfico de	e estos orígenes durante el periodo de tiempo pro	ogramad
lonas de origen *		
WAN	0	
	-	
	alamanta	

f) Agregar la zona de destino:

Seleccione las zonas, redes, dispositivos y	servicios de destino.
La regla se aplica al tráfico hacia estos des	stinos.
Zonas de destino *	
LAN (m	Nombre LAN
	Miembros Port1 Tipo LAN

g) Especificar las redes de destino:

edes de destino *	
161.132.207.233	10
Añadir nuevo ele	mento

h) Colocar los servicios asociados:



HTTP	10
HTTPS	<i>a</i> 0
TCP_8080	
Añadir nuevo e	lemento

i) Configurar la política Web como "Allow All" y habilitar las opciones, dar clic en la muesca de "Bloquear el protocolo QUIC" y "Escanear HTTP y descifrar HTTPS".

Funciones de seguridad		
✓ Filtrado web		
Politica web Allow All Allow All Allow All Allow All Additionado de tráfico basado en categoría web Bloquear el protocolo QUIC	Enceneado de malvare y contantão Casamer en TITP y desofrare HTTPs URitzar anotección de sila cero Escanear FTP en busca de malvare	Filtrands puertos web comunes Usar prozy web en lugar de motor DPI

j) Hacer clic en "Guardar" para terminar:

ditar regla de fire	ewall		Comentarios
💽 Estado de la regla			
Nombre de regla *		Descripción	Grupo de reglas
Permitir_Morea		Intraducir Descripción	WAN->LAN
Acción			
Acept	-		
Penistrar tráfico de firewa			
Registra el tráfico que coincide servidor systog configurado.	i con esta regla de firewail en el dispositivo (por d	tefecta) o en el	
UTIGEN Seleccione las zonas, redes y La regla se aplica al tráfico de Zonas de origen * WAN	Sispositivos de origen. estos origenes durante el periodo de tiem	po propremado. Disposiblices y redea de origen * CUALQUIERA	Duranta la hora programada Sempre
Añadir nuevo e	lemento	Añadir nuevo elemento	Seleccione para aplicar la regla a un periodo de tiempo y día de la semana específicos.
Destino y servicios	ispositivos y servicios de destino. Lia estos destinos.	Data de Antico 4	Tanàn 1
Seleccione las zonas, redes, d La regla se aplica al tráfico har Zenne de destino *		161 132 207 233	HTTP A @
Seleccione las zonas, redes, d La regla se aplica al tráfico hai Zonas de destino *			
Seleccione las zonas, redes, d La regla se aplica al tráfico hai Zonas de destino *	0	10	HTTPS
Seleccione las zonas, redes, d La regla se aplica al tráfico ha Zonas de destino * LAN Añardir pueson e	•	Añadir nuevo elemento	
Seleccione las zonas, redes, d La regla se aplica al tráfico har Zones de destino * LAN Añadir nuevo e	emento	Añadir nuevo elemento	HTTPS / O TCP_8080 / O
Seleccione las zonas, redes, d La regla se aplica al tráfico har Zonas de destino * LAN Añadir nuevo e	emento	Afladir nuevo elemento	HTTPS PO TCP_8080 PO Altedir nutvo tilemento
Seleccione las zonas, redes, d La regla se aplica al tráfico ha Zonas de destino * LAN Añadir nuevo e	emento	Añadr nuevo elemento	HTTPS TCP_8080 TCP_8080 Ander nuevo elemento Los envices on typo se talfor beauto en una contanación de protocolar y puntos.

5.3 CONFIGURACIÓN REGLAS NAT

a) En el menú izquierdo, seleccionar "Reglas y políticas" y luego "Reglas NAT":



	Regias de firewall		Region NUT		reglas de inspección SSL/TLS	
	Desactiver filtro	Video: Cómo usar NAT	Regiss tour	Añod	ár regla NAT 🖌 🗸	Desactivar
0 Se han WAN y	creado muchas regias NAT (SNAT) vinculadas enm activar la regia MASQ predeterminada en la parte in	escaradas durante la migración. No las hernos eliminado aut fanior de la tablia de reglas NAT. Para obtener más detalles, co	tométicamente para asegurarnos de que no haya cambios de ansulte la ayuda online.	comportamiento después de la migración. Puede eliminar las Eliminar restas NAT vinculadas (solo MASO: de	regias MASQ con el destino estino: WANI De acu	establecido :
Tipo NAT	Estado	 ID de regi Ocultar regle NAT vinculada 				
	# Norrbre	Original	Trabusida	Interfag	D	Uso
• 0	1 OS. Web. Wo O IO de regla de Trewait 9 1	Origen: Dualquier heat, Servicio: Cualquier servicio Destino, Cualquier heat	Drigen: MASO Services Original Destino Original	Entrante: Cualquier interfaz Saliente: Cualquier interfaz Útimo uso: 2024-06-14 11:08	#86	🛧 852К
•	2 <u>65 Web Susarvice</u> 9 ID de regla de firewal. 9 0	Origen: Cualquier host Servicio: Cualquier kervicio Destino: Cualquier host	Orgen: MASD Servicio: Orginal Destino: Orginal	Entrante: Cualquier interfez Saliente: Cualquier interfez Último uso: 8024 06-14 11.07	#85	Ф 80К
• •	3 GS. Web. Standard G IC) de regla de finexal: 8 9	Origan: Qualquier host Servicio: Cualquier servicio Destino: Cualquier hast	Organ NASD Saniclo Orginal Destino Orginal	Entrante Cuelquier interfaz Saliente: Cuelquier interfaz Útorno uso: 2024-06-14 11.07	854	? 218K
• 0	4 OS Web Basico D de regla de finewalt 8 8	Origan: Cualquier host Servicio: Cualquier servicio Destino: Cualquier host	Drigen: MASD Servicito Original Destino: Original	Entrante: Cuelquier interfez Saliente: Cuelquier interfez Últorno uso: 2024-06-14.11.08	#83	^ 46K
• •	s <u>Talefonia</u>	Origen Diel 10 10 3 223 Servicio, Cualquier servicio Destino: Cualquier hist	Organ: 341.132.2072201611. Servicio: Orginal Destino: Orginal	Entrante: Cuelquier interfaz Saliente: Cuelquier interfaz Último uso: 2024-06-14 11.08	871	* 77K
• •	6 EXCHANGE DUT 9 10 de regla de frewait 6	Origen: 10 10 3 342-10 10 3 342 Servicio: Cualquier servicio	Origen: 161.132.207207.161.1 Servicio: Original	Entrante: Cualquier interfaz Saliente: Cualquier interfaz	#65	118 K

b) Hacer clic en "Añadir regla NAT" y seleccionar "Nueva regla NAT":

		Reglas de firewall		Reglas NAT	Reglas de i	nspección SSL/	ILS	
Pv4)	IPv6	Desactivar filtro	Vídeo: Cómo usar NAT		Añadir regla NAT	Desa	ctivar	Eliminar
	ie han crei eglas MAS	ado muchas reglas NAT (SNAT) vinculad Q con el destino establecido solo en WA	ias enmascaradas durante la migración. No las hemos N y activar la regla MASQ predeterminada en la parte in	eliminado automáticamente para asegurarnos de que n nferior de la tabla de reglas NAT. Para obtener más detall Eliminar reglas I	^{o h} Nueva regla NAT es. NA Asistente de acceso al servidor [DNAT]	a migración. De acuer	Puede eliminar do. No eliminar	las X
ipo N	AT	Estado	D de regiz 🔲 Ocultar regla NAT vincul	ada			Re	stablecer
	=	Nombre	Original	Traducida	Interfaz	ID	Uso	
C] 1	GS Web Vip	Drigen: Cualquier host Servicio: Cualquier servicio Destino: Cualquier host	Origen: MASQ Servicio: Original Destino: Original	Entrante: Cualquier interfaz Selliente: Cualquier interfaz Último uso: 2024-06-2011.56	#86	🛧 508К	Θ
C) 2	GS_Web_SuperVia TD de regla de firewall: 9 0	Origen: Cualquier host Servicio: Cualquier servicio Destino: Cualquier host	Origen: MASQ Servicio: Original Destino: Original	Entrante: Cualquier interfaz Saliente: Cualquier interfaz Último uso: 2024-06-20 11:56	#85	🛧 व9К	Θ
C] 3	GS_Web_Standard SID de regla de firewall: 8	Origen: Cualquier host Servicio: Cualquier servicio Destino: Cualquier host	Drigen: MASQ Servicio: Driginal Destino: Original	Entrante: Cualquier interfaz Seliente: Cualquier interfaz Último uso: Unused	#84	小 0	Θ
C] व	OS_Web_Basico ID de regla de firewall: 8 8	Origen: Cualquier host Servicio: Cualquier servicio Destino: Cualquier host	Origen: MASQ Stervicio: Original Destino: Original	Entrante: Cualquier interfaz Seliente: Cualquier interfaz Último uso: 2024-06-18 09:50	#83	🛧 ЭЗК	Θ
		Relation in	0-1 Pi-110 10 0 000	Origona 161 199 907 990 161 1	Febreate, Contraint Interfax	II71	d 32K	0

ñadir regla NAT			Comentarios	Gulas explicativas	Visor de registros Ayuda a SUPERINTENDENCIA NACION	idmin@sophosxg sunass gob pe IAL DE SERVICIOS DE SANEAMIENT
Estado de la regla						
Nombre de regla *		Descripción		Posición de regla		
Introducir Nombre de regla				Abajo	•	
Configuración de traducción						
Seleccione los criterios de coincidencia y	y la configuración d	le traducción para el origen, el destino y los servicios.				
Origen original *		Destino original *		Servicio original *		
CUALQUIERA	0	CUALQUIERA	0	CUALQUIERA	0	
Añadir nuevo elemento		Añadir nuevo elemento		Añad	fir nuevo elemento	
Origen traducido (SNAT)		Destino traducido [DNAT]		Servicio traducido ((PAT)	
Original	-	Original	-	Original	· · · · · · · · · · · · · · · · · · ·	
Criterios de coincidencia de Interfaz de entrada *	interfaz O	Interfaz de salida * CUALQUIERA	0			
Añadir nuevo elemento		Afladir nuevo elemento				
		Sobreescribir traducción de direcciones de para interfaces de salida especificas	red de origen (SNAT)			
		~		Contraction of the second	Barlana A	

ESTE DOCUMENTO IMPRESO ES UNA COPIA NO CONTROLADA Para ver el documento controlado ingrese al portal del SIG de la Sunass Uso Interno



Código: GTI-OTI-IN007

INSTRUCTIVO

c) Asignar un nombre a la regla NAT:

Editar regla NAI	
Estada de la regla	
Estado de la regia	
Nombre de regla *	

d) Agregar "Origen original":

Configuración de tra	ducción
eleccione los criterios de co	bincidencia y la con
rigen original *	
CUALQUIERA	0
A Bodir puovo o	Iomonto
Añadir nuevo e	lemento

e) Colocar la IP del "Destino original":

Añadir nuevo elemento	Nombre Tipo Dirección IP Subred	161.132.207.233 Host IP 161.132.207.233 255.255.255.255
Destino traducido (DNAT)		
Destino traducido (DNAT)		

f) Agregar el tipo de servicio en "Servicio original":

TCP_8080 Añadir nuevo elemento	Nombre TCP_8080 Tipo TCP/UDP Detalles TCP (1.65535) / (8080)
Servicio traducido (PAT)	
Original	-

g) Agregar la IP de "Destino traducido".

10.10.3.227	Nombre	10.10.3.227
0	Tipo	Host IP
	Dirección IP	10.10.3.227
	Subred	255,255,255,255



Página 10 de 10

h) Hacer clic en "Guardar" para terminar:

ditar regla NAT		Comentarios B4 Gulas explicativas Visor de registros Áyuda admingeophosis sunass gob p SUPERINTENDENCIA NACIONAL DE SERVICIOS DE SANEAMEM
Configuración de traducción		
Seleccione los criterios de coincidencia y la configuración de trad	lucción para el origen, el destino y los servicios.	
Origen original *	Destino original *	Servicio original *
CUALQUIERA	161132207233	TCP_8080
Añadir nuevo elemento	Añadir nuevo elemento	Añadir nuevo elemento
Irigen traducido (SNAT)	Destino traducido (DNAT)	Servicio traducido (PAT)
Original	10103227	Original
Añodir pupus elemento	CUALQUIERA	
Andul huero elemento	Sobrescribri traducción de direcciones de red de origen (SNAT) ; salida específicas	para interfaces de
Opciones avanzadas	Þ	
étodo de equilibrio de carga	n,	
Select v		