

**SIEMENS**  
Ingenuity for life



## SINEC NMS Firewall Management

SINEC NMS V1.0 SP1

<https://support.industry.siemens.com/cs/ww/en/view/109762792>

Siemens  
Industry  
Online  
Support



---

## Información legal

### **Uso de ejemplos de aplicación.**

Los ejemplos de aplicación ilustran la solución de tareas de automatización a través de una interacción de varios componentes en forma de módulos de texto, gráficos y/o software. Los ejemplos de aplicación son un servicio gratuito de Siemens AG y/o una filial de Siemens AG ("Siemens"). No son vinculantes y no pretenden ser completos o funcionales con respecto a la configuración y el equipamiento. Los ejemplos de aplicación simplemente ofrecen ayuda con tareas típicas; no constituyen soluciones específicas para el cliente. Usted mismo es responsable del funcionamiento correcto y seguro de los productos de acuerdo con las normas vigentes y también debe verificar la función del ejemplo de aplicación respectivo y personalizarlo para su sistema.

Siemens le otorga el derecho no exclusivo, no sublicenciable e intransferible de que los ejemplos de aplicación sean utilizados por personal técnicamente capacitado. Cualquier cambio en los ejemplos de aplicación es su responsabilidad. Solo se permite compartir los ejemplos de aplicación con terceros o copiar los ejemplos de aplicación o extractos de los mismos en combinación con sus propios productos.

Los ejemplos de aplicación no están obligados a someterse a las pruebas e inspecciones de calidad habituales de un producto facturable; pueden tener defectos funcionales y de rendimiento, así como errores. Es su responsabilidad usarlos de tal manera que cualquier mal funcionamiento que pueda ocurrir no resulte en daños a la propiedad o lesiones a las personas.

### **Descargo de responsabilidad**

Siemens no asumirá ninguna responsabilidad, por ningún motivo legal, incluida, entre otras, la responsabilidad por la usabilidad, disponibilidad, integridad y ausencia de defectos de los ejemplos de aplicación, así como por la información relacionada, los datos de configuración y rendimiento y cualquier daño causado por ello. . Esto no se aplicará en casos de responsabilidad obligatoria, por ejemplo, en virtud de la Ley alemana de responsabilidad por productos defectuosos, o en casos de dolo, negligencia grave o muerte culposa, lesiones corporales o daños a la salud, incumplimiento de una garantía, incumplimiento fraudulento. -revelación de un defecto o incumplimiento culposo de obligaciones contractuales materiales. No obstante, las reclamaciones por daños derivados del incumplimiento de obligaciones contractuales materiales se limitarán a los daños previsibles típicos del tipo de acuerdo, a menos que la responsabilidad surja de dolo o negligencia grave o se base en la pérdida de la vida, lesiones corporales o daños a la salud. Las disposiciones anteriores no implican ningún cambio en la carga de la prueba en su perjuicio. Deberá indemnizar a Siemens frente a reclamaciones existentes o futuras de terceros a este respecto, excepto cuando Siemens sea responsable obligatorio.

Al utilizar los ejemplos de aplicación, reconoce que Siemens no se hace responsable de ningún daño más allá de las disposiciones de responsabilidad descritas.

### **Otra información**

Siemens se reserva el derecho de realizar cambios en los ejemplos de aplicación en cualquier momento sin previo aviso. En caso de discrepancias entre las sugerencias de los ejemplos de aplicación y otras publicaciones de Siemens, como catálogos, prevalecerá el contenido de la otra documentación.

Los términos de uso de Siemens (<https://support.industry.siemens.com>) también se aplicará.

### **Información de seguridad**

Siemens ofrece productos y soluciones con funciones de Seguridad Industrial que respaldan el funcionamiento seguro de plantas, sistemas, máquinas y redes.

Para proteger plantas, sistemas, máquinas y redes contra amenazas ciberneticas, es necesario implementar, y mantener continuamente, un concepto de seguridad industrial holístico y de última generación.

Los productos y soluciones de Siemens constituyen un elemento de dicho concepto.

Los clientes son responsables de evitar el acceso no autorizado a sus plantas, sistemas, máquinas y redes. Dichos sistemas, máquinas y componentes solo deben conectarse a una red empresarial oa Internet si y en la medida en que dicha conexión sea necesaria y solo cuando estén implementadas las medidas de seguridad adecuadas (por ejemplo, cortafuegos y/o segmentación de la red).

Para obtener información adicional sobre las medidas de seguridad industrial que pueden implementarse, visite <https://www.siemens.com/industrialsecurity>.

Los productos y soluciones de Siemens se someten a un desarrollo continuo para hacerlos más seguros.

Siemens recomienda enfáticamente que las actualizaciones del producto se apliquen tan pronto como estén disponibles y que se utilicen las últimas versiones del producto. El uso de versiones de productos que ya no son compatibles y la falta de aplicación de las últimas actualizaciones puede aumentar la exposición del cliente a las ciberamenazas.

Para mantenerse informado sobre las actualizaciones de productos, suscríbase a la fuente RSS de Siemens Industrial Security en: <https://www.siemens.com/industrialsecurity>.

Tabla de contenido

---

# Tabla de contenido

<b>Información legal.....</b>	<b>2</b>
<b>1      Introducción.....</b>	<b>4</b>
1.1     Descripción general.....	4
1.2     Principio de funcionamiento.....	5
1.3     Componentes utilizados.....	6
<b>2      Configuración de hardware .....</b>	<b>7</b>
<b>3      Ingeniería .....</b>	<b>9</b>
3.1     Requerimientos básicos .....	9
3.2     Definición de las relaciones de comunicación .....	17
3.3     Configuración del acceso al cortafuegos .....	19
3.4     Configuración del acceso de una sola vez a la celda .....	32
3.5     Acceder a los datos del PLC .....	45
3.6     Resultado .....	59
3.7     Manejo de errores .....	60
3.8     Pista de auditoría .....	62
<b>4 Información útil .....</b>	<b>63</b>
4.1     Estructura de una Relación de Comunicación en SINEC NMS .....	63
4.1.1     Estado de las Relaciones de Comunicación en SINEC NMS .....	67
4.2     .....	68
4.2.1     Fuente NAT .....	69
4.2.2     NAT de destino .....	70
<b>5      Apéndice .....</b>	<b>71</b>
5.1     Servicio y soporte .....	71
5.2     Enlaces y literatura .....	72
5.3     Modificar la documentación .....	72

## 1. Introducción

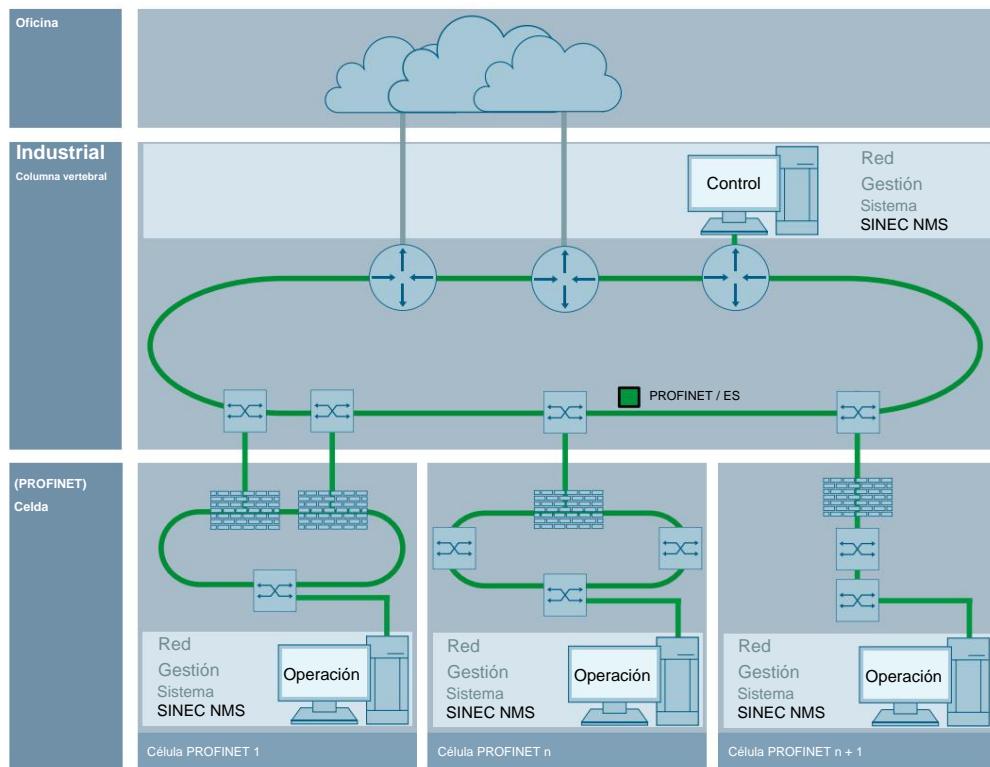
# 1 Introducción

## 1.1

### Descripción general

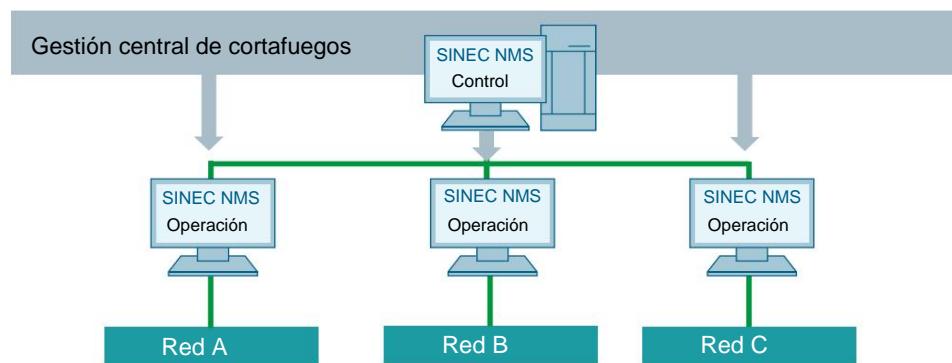
Los cortafuegos se utilizan para asegurar la comunicación entre diferentes subredes. Para llevar a cabo esta tarea, analizan y restringen el tráfico de comunicaciones.

Figura 1-1



Desde una ubicación central, SINEC NMS se puede usar para crear reglas de firewall para todos los firewalls conectados y monitorear cualquier cambio manual realizado en la configuración del firewall.

Figura 1-2



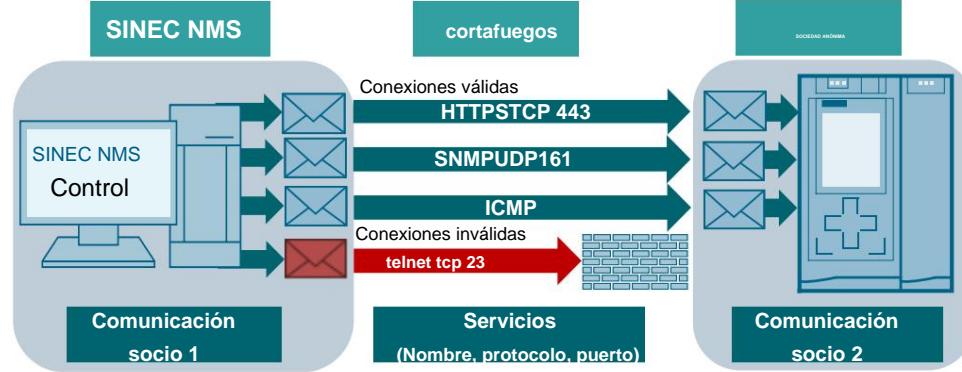
## 1. Introducción

**1.2 Principio de funcionamiento**

La funcionalidad de cortafuegos de SCALANCE S y RUGGEDCOM tiene la función de proteger la red interna de interferencias de la red externa. Esto significa que solo se permiten ciertas relaciones de comunicación predefinidas entre la red interna y la red externa. Los cortafuegos, o filtros de paquetes, pueden bloquear las comunicaciones no deseadas filtrando los paquetes IP de acuerdo con las reglas definidas previamente por el usuario. Cada regla determina si un paquete IP se reenvía o no según una determinada condición. Cuando se procesa un paquete IP, se compara con las reglas de filtrado existentes. Si el paquete cumple la condición, se ejecuta la acción definida en la regla (reenviar o bloquear). Si el paquete no coincide con ninguna regla de filtro, el paquete se bloquea de forma predeterminada en aras de la seguridad.

Tanto la comunicación entrante como la saliente se pueden filtrar.

Figura 1-3



En este ejemplo, se habilitará el acceso a través de SNMP, ICMP y HTTPS a un servidor web de la CPU S7-1500. Para ello se crea una relación de comunicación en el Control. Una relación de comunicación describe qué socios de comunicación pueden comunicarse a través de qué servicios, así como qué dispositivos de seguridad se utilizan para asegurar esta comunicación. Luego, el sistema genera automáticamente las reglas específicas del dispositivo.

---

 1. Introducción

### 1.3 Componentes utilizados

Este ejemplo de aplicación se creó con los siguientes componentes de hardware y software:

Tabla 1-1

Componentes	Número de artículo	Dirección IP	enrutador	Nota
XB208	6GK5 208-0BA00-2AB2	172.16.0.2	172.16.0.1	
CPU 317-2 PN/PD	6ES7 317-2EK14-0AB0	172.16.0.5	172.16.0.1	
CPU 1513-1 NP	6ES7 516-3FN01-0AB0	172.16.0.3	172.16.0.1	
ESCALANCE S615	6GK5 615-0AA00-2AA2	Vlan 1 (Int): 172.16.0.1  Vlan 2 (Ext): 10.0.1.1		enrutador
XB208	6GK5 208-0BA00-2AB2	192.168.0.2	192.168.0.1	
W761-1 RJ45 6GK5 761-1FC00-0AA0		192.168.0.14	192.168.0.1	
W722-1 RJ45 6GK5 722-1FC00-0AA0		192.168.0.13	192.168.0.1	
CPU 1212C		192.168.0.10	192.168.0.1	
ET 200SP	6ES7 155-6AU00-0BN0	192.168.0.11	192.168.0.1	
ESCALANCE S615	6GK5 615-0AA00-2AA2	Vlan1 (int): 192.168.0.1  Vlan2 (Ext): 10.0.1.2		enrutador
XB208	6GK5 208-0BA00-2AB2	10.0.1.3		
Control & Operación 1		10.0.1.4	10.0.1.1	Se admite cualquier SIMATIC IPC que cumpla los requisitos de software.
Operación 2		10.0.1.5	10.0.1.2	

Este ejemplo de aplicación consta de los siguientes componentes:

Tabla 1-2

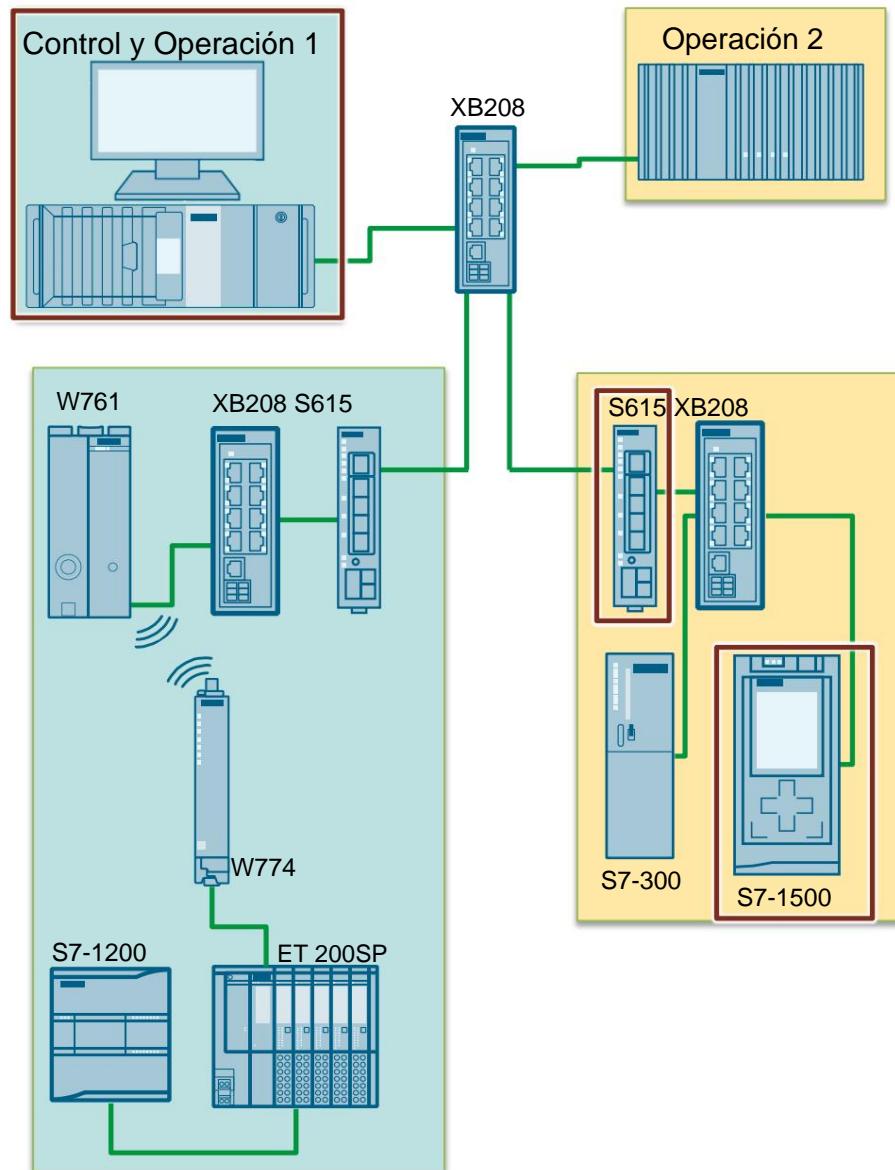
Componentes	Nombre del archivo	Nota
Este documento	109762792_SINEC_NMS_Firewall_V1_0.es	

2 Configuración de hardware

## 2 configuración de hardware

En el siguiente documento se establecerá una relación de comunicación entre SINEC NMS Control y el S7-1500 a través de los servicios HTTPS, ICMP y SNMP. El objetivo es habilitar el diagnóstico del S7-1500, así como el acceso del servidor web al S7-1500. La relación de comunicación se crea en el Control.

Figura 2-1

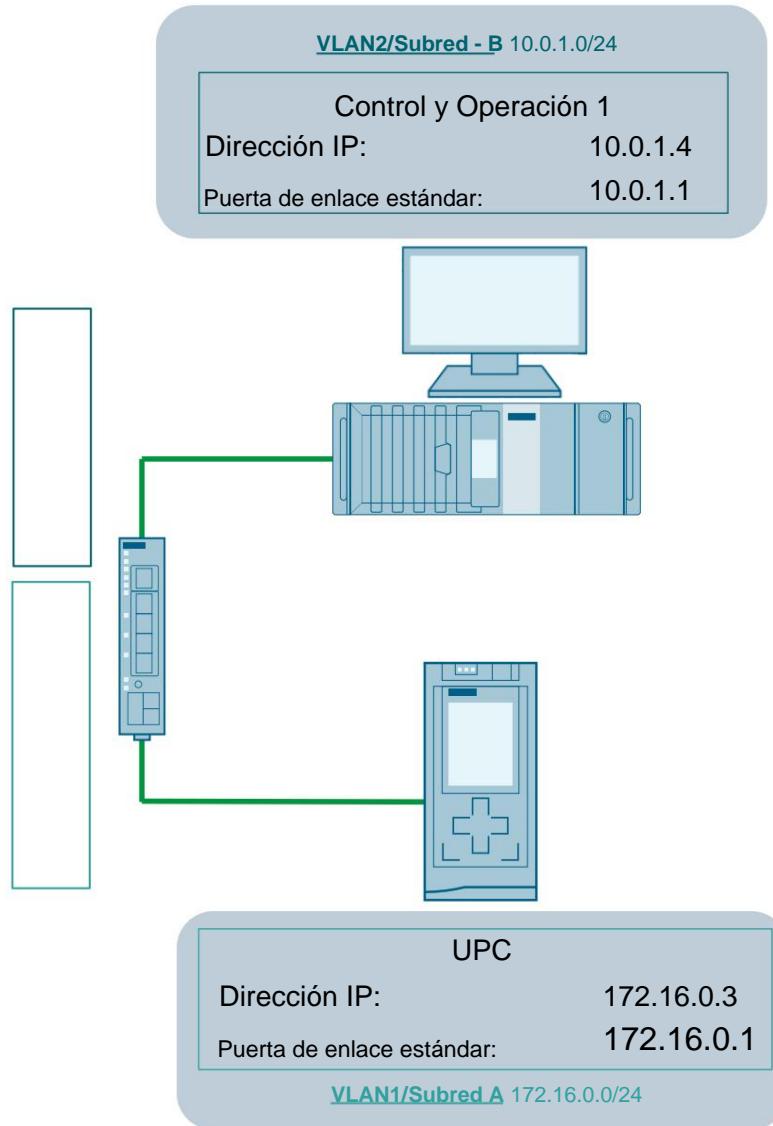


---

[2 Configuración de hardware](#)**Comunicación a través de enrutador**

Para el acceso al servidor web se crea una relación de comunicación entre PC y CPU.

Figura 2-2



## 3 Ingeniería

### 3.1 Requerimientos básicos

Para utilizar las funciones en SINEC NMS, se deben cumplir los siguientes requisitos básicos:

1. La función "Gestión de cortafuegos" es compatible con los siguientes dispositivos.

Tabla 3-1

familia de dispositivos	Versión SINEC NMS > Versión de firmware Dispositivos
ESCALANCE S615	SINEC NMS 1.0 SP1 (>=6.2.x)
ESCALANCE SC600	SINEC NMS 1.0 SP1 (>=2.0.x)
RUGGEDCOM ROX2	SINEC NMS 1.0 SP1 (>= 2.13.2)

**Nota**

La cantidad de reglas de firewall generadas para un dispositivo no se verifica antes de la implementación.

El usuario debe asegurarse de que no se supere el número máximo de reglas:

- SC600: 1000 reglas de cortafuegos (>= v2.0.0)
- S615: 128 reglas de cortafuegos (>= v5.0.0)
- RUGGEDCOM ROX2: 1000 reglas de cortafuegos

Sin embargo, si se excede el número, se mostrará un resultado incorrecto en la ejecución de la política.

## 3 Ingeniería

2. SNMP está disponible en diferentes versiones (SNMPv1, SNMPv2c y SNMPv3).

Sin embargo, SNMPv1 y SNMPv2c no deben usarse, ya que estas versiones solo tienen mecanismos de seguridad limitados o no están implementados. A partir de la versión 3, especificada en 2002, SNMP ofrece además administración de usuarios con autenticación, así como cifrado opcional de paquetes de datos. Esto aumentó considerablemente la seguridad de SNMP.

Si utiliza SNMP en la versión v1/v2c para la configuración, la propiedad "Read-Only" debe estar desactivada en SCALANCE S Web Based Management.

Figura 3-1



172.16.0.1/SCALANCE S615

The screenshot shows the 'System Configuration' page of the SCALANCE S615 web interface. The left sidebar has a 'Configuration' section selected. The main area shows various server configuration options. In the 'SNMP' section, there is a checkbox labeled 'SNMPv1/v2 Read-Only' which is checked and highlighted with a red box. Other options in this section include 'SNMPv1 Traps' (unchecked), 'SINEMA Configuration Interface' (checked), and 'DHCP DUID Configuration'. Below the configuration section, there are fields for 'Link-layer Address Plus Time', 'Vendor Enterprise Number', and 'Link-layer address'. At the bottom, there are buttons for 'Set Values', 'Refresh', 'Automatic Save' (selected), and 'Write Startup Config'.

de uso gratuito

3 Ingeniería

Si solo desea utilizar "SNMPv3" para la configuración y la supervisión, selecciónelo en el menú "Sistema > SNMP" en la pestaña "General".

Figura 3-2

**SIEMENS**  
172.16.0.1/SCALANCE S615

Welcome admin

[Logout](#)

- ▶ Wizards
- ▶ Information
- ▼ System
  - ▶ Configuration
  - ▶ General
  - ▶ Restart
  - ▶ Load&Save
  - ▶ Events
  - ▶ SMTP Client
  - ▶ SNMP**
  - ▶ System Time

**Simple Network Management Protocol (SNMP) General**

**General** **Traps** **v3 Groups** **v3 Users**

SNMP: **SNMPv3**

SNMPv1/v2c Read Community String: -  
SNMPv1/v2c Read/Write Community String: **private**

SNMPv1/v2c Trap Community String: public

SNMPv1 Traps  
 SNMPv3 User Migration

SNMP Engine ID: 80.00.10.e9.03.00.1b.1b.ca.0f.48  
SNMP Agent Listen Port: 161

**Set Values** **Refresh**

Asigne un nombre de grupo y seleccione un nivel de seguridad. Haga clic en el botón "Crear". Los permisos de lectura y escritura se crean automáticamente.

Figura 3-3

**SIEMENS**  
172.16.0.1/SCALANCE S615

Welcome admin

[Logout](#)

- ▶ Wizards
- ▶ Information
- ▼ System
  - ▶ Configuration
  - ▶ General
  - ▶ Restart
  - ▶ Load&Save
  - ▶ Events
  - ▶ SMTP Client
  - ▶ SNMP**

**Simple Network Management Protocol (SNMP) v3 Groups**

**General** **Traps** **v3 Groups** **v3 Users**

Group Name:	Network Administrator				
Security Level:	no Auth/no Priv				
Select	Group Name	Security Level	Read	Write	Persistence
<input type="checkbox"/>	Network Administrat	no Auth/no Priv	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	no

1 entry.

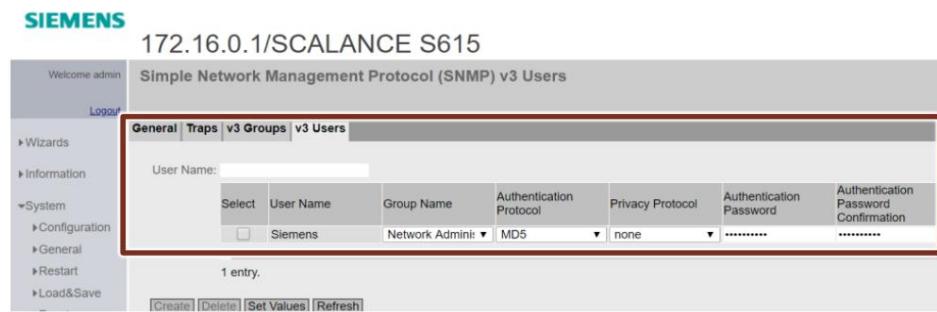
**Create** **Delete** **Set Values** **Refresh**

de uso gratuito

3 Ingeniería

Asigne un nombre de usuario. Haga clic en el botón "Crear". Asigne un nombre de grupo, un protocolo de autenticación y un protocolo de cifrado. Introduzca la contraseña de autenticación que utilizó en SINEC NMS. Haga clic en el botón "Aceptar configuración".

Figura 3-4

**Nota**

Como alternativa a la ingeniería de proyectos en WBM, también puede configurar el sistema en SINEC NMS mediante una política. Para ello, configure la tarea "Establecer usuario SNMP V3" en la política. La configuración de SNMPv3 se copia automáticamente en el directorio de datos de inicio de sesión del dispositivo.

Irrestricto

## 3 Ingeniería

3. Las propiedades de la interfaz en SCALANCE S615 se configuraron de la siguiente manera. Elas propiedades de la interfaz se pueden encontrar en Administración basada en web en "Capa 3 > Subredes".

Tabla 3-2

Interfaz	Puerto	dirección IP	Máscara de subred
vlan2 (EXT)	5	10.0.1.1	255.255.255.0
vlan1 (INT)	1 a 4	172.16.0.1	255.255.255.0

Figura 3-5

Select	Interface	TIA Interface	Interface Name	MAC Address	IP Address	Subnet Mask
<input checked="" type="checkbox"/>	vlan1	yes	INT	00-1b-1b-ca-0f-48	172.16.0.1	255.255.255.0
<input type="checkbox"/>	vlan2	-	EXT	00-1b-1b-ca-0f-4c	10.0.1.1	255.255.255.0

Ahora abra las propiedades del cortafuegos en "Seguridad > Cortafuegos". Aquí deben restringirse, entre otras cosas, las "reglas IPv4 predefinidas", que permiten el acceso al SCALANCE S con los correspondientes protocolos de gestión o diagnóstico. Active SNMP y SSH para vlan2 para permitir que SINEC NMS se conecte a SCALANCE S.

Figura 3-6

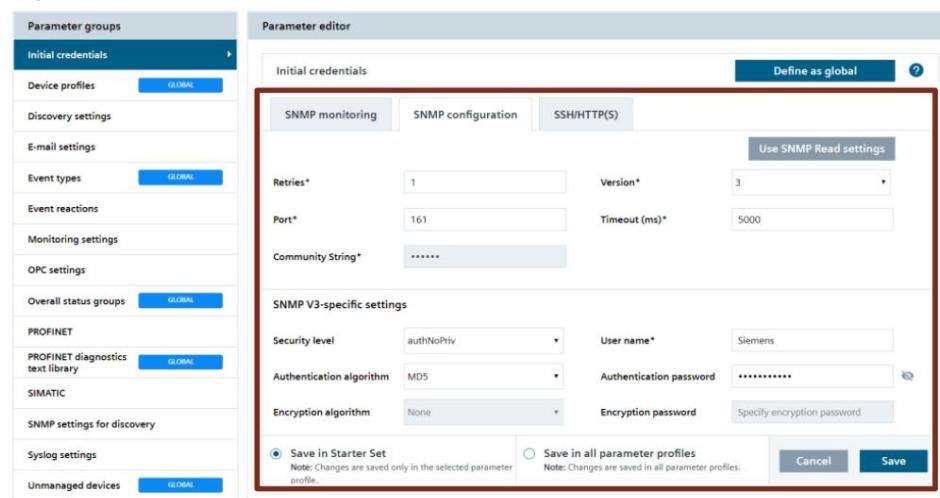
Interface	All	HTTP	HTTPS	DNS	SNMP	Telnet	IPsec VPN	SSH	DHCP	Ping
vlan1 (INT)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
vlan2 (EXT)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ppp2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

de uso gratuito

## 3 Ingeniería

4. SINEC NMS requiere datos de inicio de sesión del dispositivo para establecer una conexión con los dispositivos a través de SSH y SNMP. Los datos de inicio de sesión se definen en el Control en el menú "Perfil de parámetros de operación", en el grupo de parámetros "Datos iniciales de inicio de sesión". En las pestañas SSH/HTTP(S) y SNMP, puede ingresar los valores deseados y guardarlos en el perfil de parámetros.

Figura 3-7

**Nota**

Además, los datos de inicio de sesión se pueden almacenar y editar en el directorio de datos de inicio de sesión del dispositivo de Operation para cada dispositivo individual. Si no se almacenan datos de inicio de sesión específicos en el directorio de datos de inicio de sesión del dispositivo, los datos de inicio de sesión iniciales se transfieren al directorio de datos de inicio de sesión del dispositivo y se utilizan para el inicio de sesión.

En "Administración del sistema > Perfiles de parámetros de operación > Configuración de monitoreo > Cambio de perfil de dispositivo", se puede activar la función Cambio automático de tipo de dispositivo. Al activar esta opción, se buscan automáticamente los perfiles de dispositivos adecuados y los tipos de dispositivos que contiene para los dispositivos a los que se les ha asignado un perfil predeterminado.

de uso gratuito

3 Ingeniería

También debe crear un nuevo perfil para SNMP V3 en "Configuración de SNMP para detección". SINEC NMS lo utiliza para la detección de dispositivos.

Figura 3-8

Edit SNMP settings for discovery			
Name*	SNMP Settings V3	Version*	3
Retries*	3	Timeout (ms)*	2000
Community String	* Specify community string for reac...	Use for discovery <input checked="" type="checkbox"/>	
Port*	161		
SNMP V3-specific settings			
Security level	authNoPriv	User name	Siemens
Auth. algorithm	MD5	Auth. password	.....
Encrypt. algorithm	None	Confirmation of auth. password	.....
Context Name	Specify name	Encrypt. password	Enter password
Cont. Machine ID	Machine ID	Confirmation of encrypt. password	Enter password again

**Cancel** **OK**

3 Ingeniería

5. Después de la exploración de la red, se puede acceder a los siguientes dispositivos a través de SINEC NMS:
- Control y operación de SINEC NMS
  - ESCALANCE XB208
  - SCALANCE S615

Figura 3-9



de uso gratuito

## 3.2 Definición de relaciones de comunicación

La siguiente tabla ofrece una descripción general de las relaciones de comunicación que se configurarán:

### Relación de comunicación 1: SINEC NMS a SCALANCE S

Tabla 3-3

Escenario	Variante de cortafuegos	Servicio	Fuente	Dispositivo de destino
1	Cortafuegos basado en IP	<ul style="list-style-type: none"> <li>• Permitir protocolos seguros:           <ul style="list-style-type: none"> <li>– Permitir el acceso al servidor web HTTPS (Puerto TCP 443)</li> <li>– SSH (Puerto TCP 22)</li> <li>– SNMP (UDP 161)</li> <li>– ICMP</li> </ul> </li> </ul>	10.0.1.4 (Control y Operación)	10.0.1.1 (ESCALANCÍA S615)
2	Cortafuegos basado en IP	<ul style="list-style-type: none"> <li>• Impedir todos los demás protocolos</li> </ul>		

### Relación de comunicación 2: SINEC NMS a PLC 1500

Tabla 3-4

Guion	variante de cortafuegos	Servicio	Fuente	Dispositivo de destino
1	Cortafuegos basado en IP	<ul style="list-style-type: none"> <li>• Permitir protocolos seguros:           <ul style="list-style-type: none"> <li>– Permitir el acceso al servidor web HTTPS (Puerto TCP 443)</li> <li>– SNMP (UDP 161)</li> <li>– ICMP</li> </ul> </li> </ul>	10.0.1.4 (Control y Operación)	172.16.0.3 (CPU S7-1516)
2	Cortafuegos basado en IP	<ul style="list-style-type: none"> <li>• Impedir todos los demás protocolos</li> </ul>		

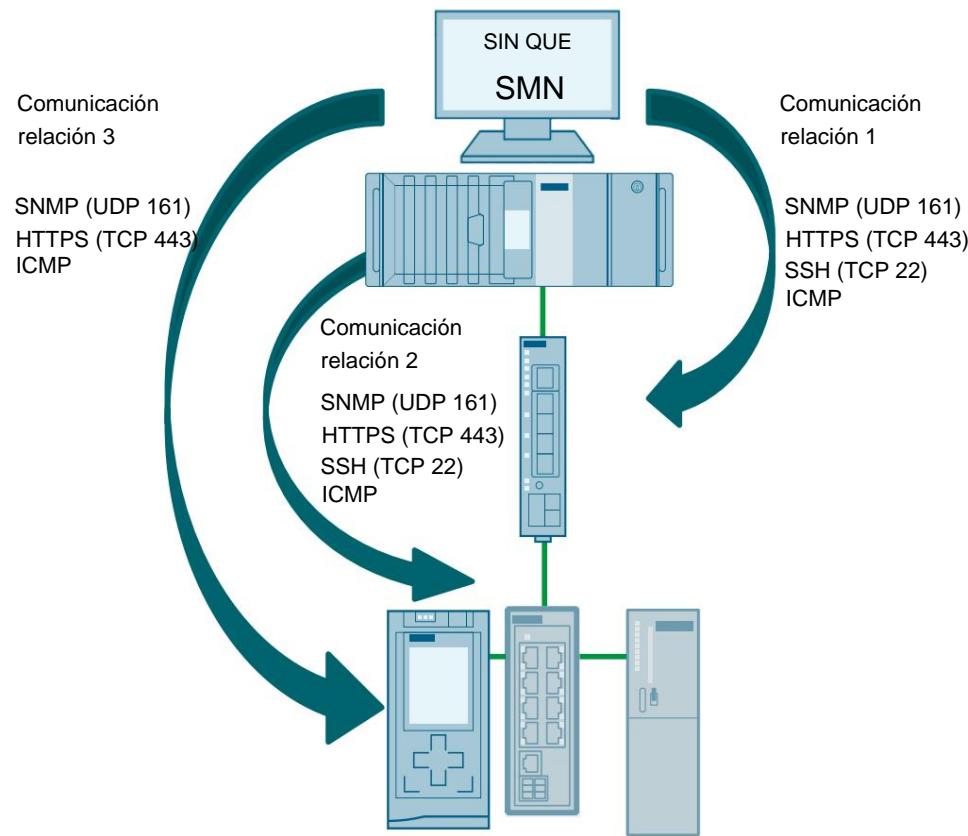
**Nota**

Tenga en cuenta que el usuario primero debe configurar la relación de comunicación 1. Esto permite el acceso permanente al firewall con SINEC NMS. Tan pronto como se haya creado la relación de comunicación 1, se pueden agregar más reglas de firewall al firewall utilizando otras relaciones de comunicación.

En la relación de comunicación 2, la celda se escanea una vez. Los dispositivos encontrados se pueden utilizar más adelante para la configuración.

En la relación de comunicación 3 se restringe el acceso a la celda con los respectivos servicios.

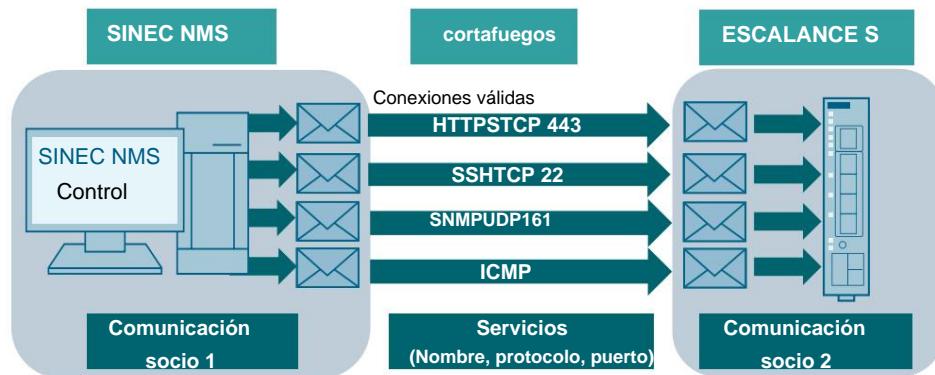
Figura 3-10



### 3.3 Configuración del acceso al cortafuegos

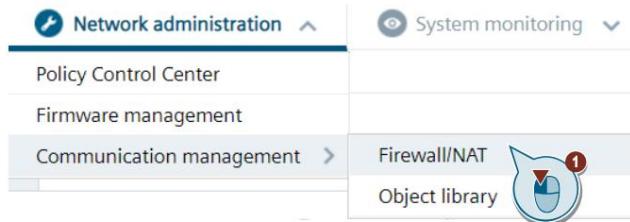
En la siguiente sección se configura el acceso de SINEC NMS a SCALANCE S a través de HTTPS, SSH, SNMP e ICMP.

Figura 3-11



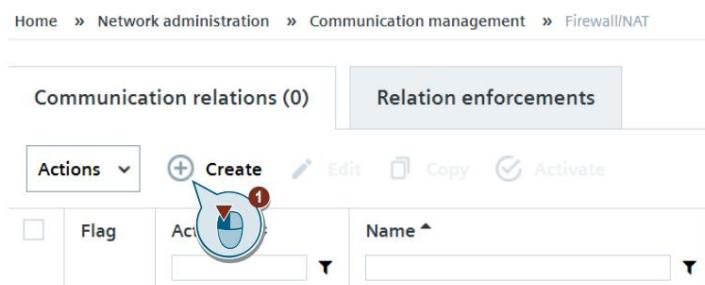
1. Abra el menú "Administración de red > Gestión de comunicación > Cortafuegos/NAT" en el Control.

Figura 3-12



2. Haga clic en el botón "Crear" para crear una nueva relación de comunicación.

Figura 3-13

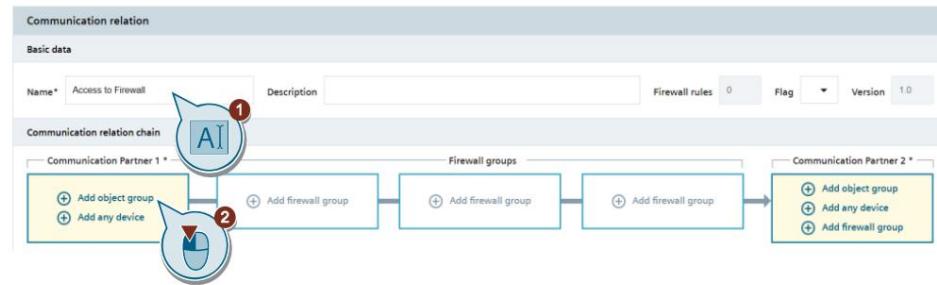


Irrestrictivo

3 Ingeniería

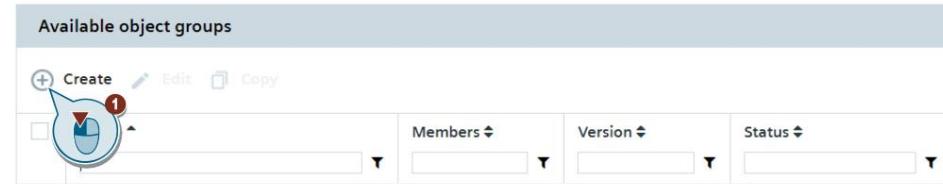
3. Asignar un nombre en la relación de comunicación. Haga clic en el botón "Agregar grupo de objetos" en "Socio de comunicación 1".

Figura 3-14



4. Haga clic en el botón "Crear" para crear un nuevo grupo de objetos.

Figura 3-15



5. Asigne un nombre al grupo de objetos. Haga clic en el botón "Agregar dispositivos monitoreados".

Con esta opción, agrega dispositivos que son monitoreados por SINEC NMS. Para los dispositivos monitoreados, SINEC NMS muestra la información de monitoreo detectada en el grupo de objetos y detecta los cambios realizados en el dispositivo fuera de SINEC NMS.

Alternativamente, también puede seleccionar la función "Agregar direcciones IP de dispositivos". Con esta función se pueden incluir dispositivos que no son monitorizados por SINEC NMS.

Figura 3-16

de uso gratuito

3 Ingeniería

6. Seleccione la estación de gestión para SINEC NMS. Haga clic en el botón "Agregar".

Figura 3-17

Add monitored devices			
IP address internal	Device name	Device type	Operation
<input type="checkbox"/> 192.168.0.2	SCALANCE XB208	SCALANCE XB208 PN (OBA00-2...	
<input type="checkbox"/> 10.0.1.1	Scalance XM408/8C L3	SCALANCE XM408-8C (8GR00-...	
<input checked="" type="checkbox"/> 10.0.1.4	-	Management Station	WIN10Blank
<input type="checkbox"/> 10.0.1.1	SCALANCE S615	SCALANCE S615 (OAA00-2AA2)	WIN10Blank
<input type="checkbox"/> 192.168.0.2	SCALANCE XB208	SCALANCE XB208 PN (OBA00-2...	WIN10Blank

**Cancel** **Add**

7. Haga clic en el botón "Guardar".

Figura 3-18

Object group			
Name*	Description	Version	
SINEC NMS		1.0	

Member			
<input type="button" value="Add monitored devices"/> <input type="button" value="Add device IP addresses"/> <input type="checkbox"/> Delete <input checked="" type="checkbox"/> Apply member changes		<input type="button" value="Edit"/>	
<input type="checkbox"/> IP address internal	Device name	Monitored	Status
<input type="checkbox"/> 10.0.1.4	-	Yes	OK

**Cancel** **Save**

de uso gratuito

3 Ingeniería

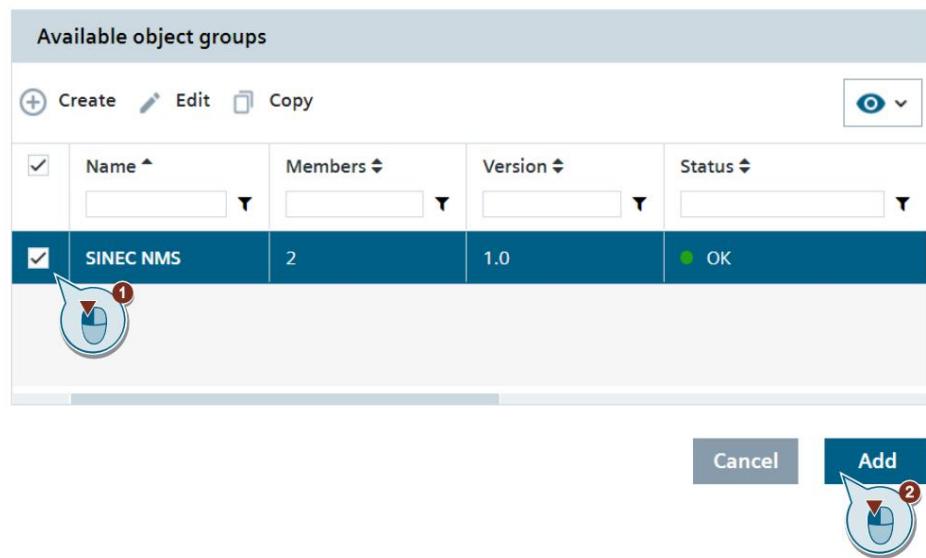
8. Introduzca un motivo para la acción que ha realizado. Haga clic en el botón "Guardar". La entrada se ingresa en el [registro de auditoría](#).

Figura 3-19



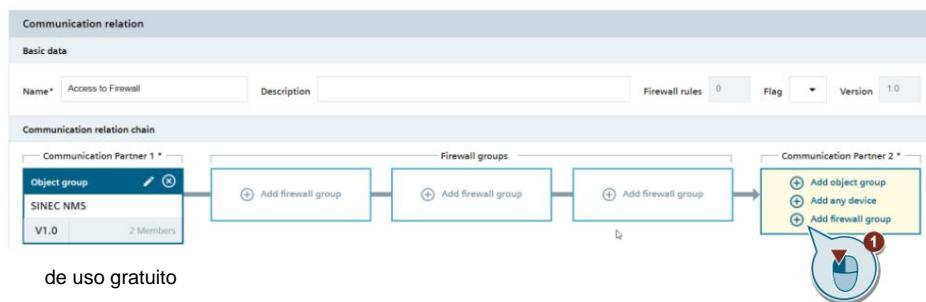
9. Seleccione el grupo de objetos recién creado "SINEC NMS". Haga clic en el botón "Agregar".

Figura 3-20



10. Haga clic en el botón "Agregar grupo de cortafuegos" en "Socio de comunicación 2".

Figura 3-21

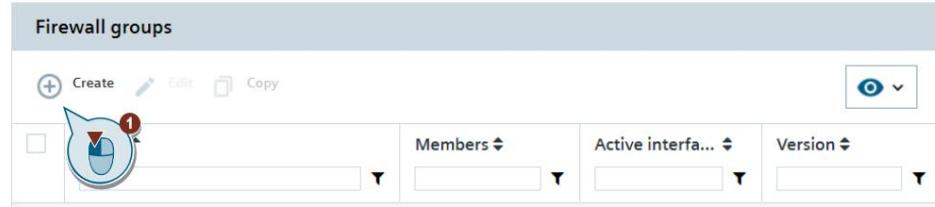


---

3 Ingeniería

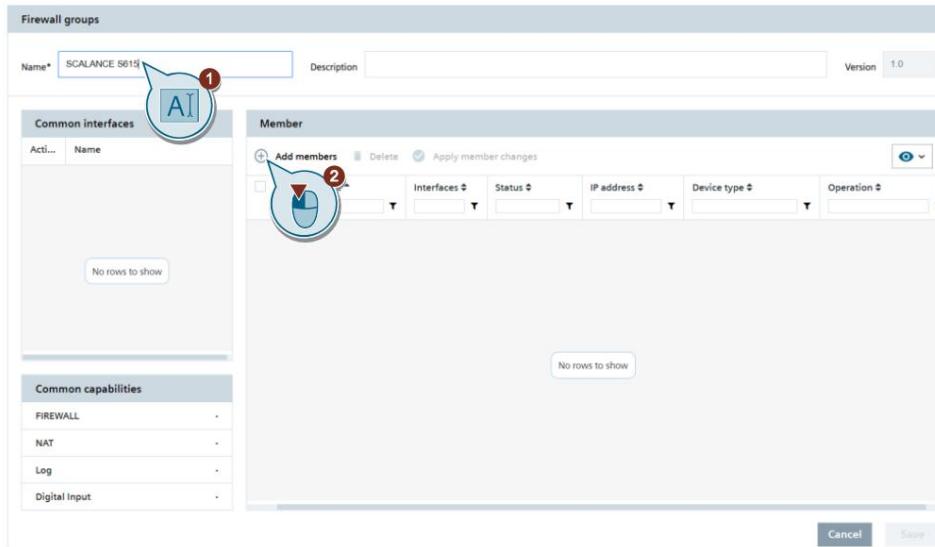
11. Haga clic en el botón "Crear" para crear un grupo de cortafuegos.

Figura 3-22



12. Asigne un nombre al grupo de cortafuegos. Haga clic en el botón "Agregar miembros".

Figura 3-23



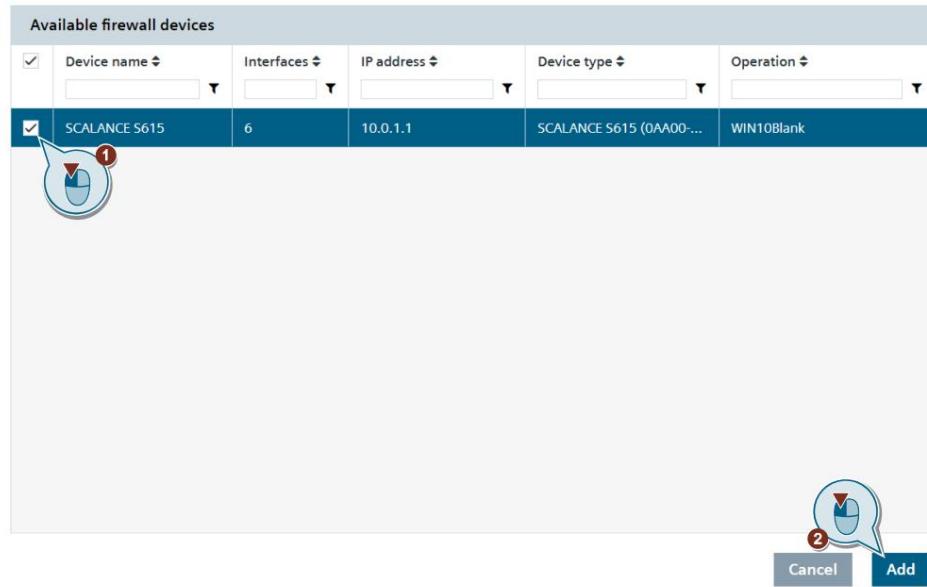
de uso gratuito

de uso gratuito

3 Ingeniería

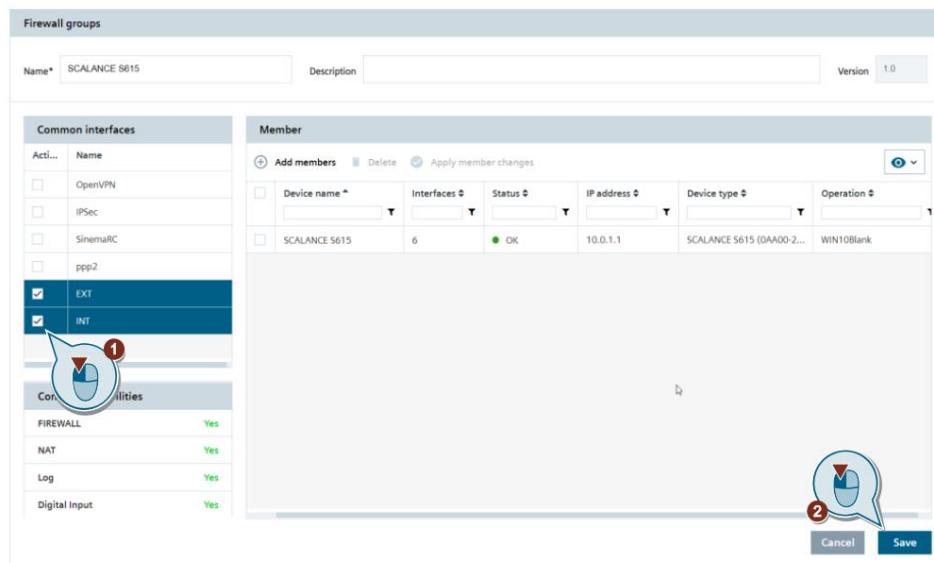
13. Seleccione el dispositivo de cortafuegos. Haga clic en el botón "Agregar".

Figura 3-24



14. Para utilizar las interfaces en un enlace de comunicación, debe estar habilitado. Seleccione las interfaces "EXT" e "INT". Haga clic en el botón "Guardar".

Figura 3-25



de uso gratuito

## 3 Ingeniería

15. Introduzca un motivo para la acción que ha realizado. Haga clic en el botón "Guardar". La entrada se ingresa en el registro de auditoría.

Figura 3-26



16. Seleccione el grupo de cortafuegos recién creado. Haga clic en el botón "Agregar".

Figura 3-27

Firewall groups				
	<input type="button" value="Create"/>	<input type="button" value="Edit"/>	<input type="button" value="Copy"/>	<input type="button" value=""/>
	Name	Members	Active interface	Version
<input checked="" type="checkbox"/>	SCALANCE S615	1	2	1.0 OK

At the bottom right of the table, there are 'Cancel' and 'Add' buttons, with 'Add' being highlighted and a red circle with the number '2' above it.

de uso gratuito

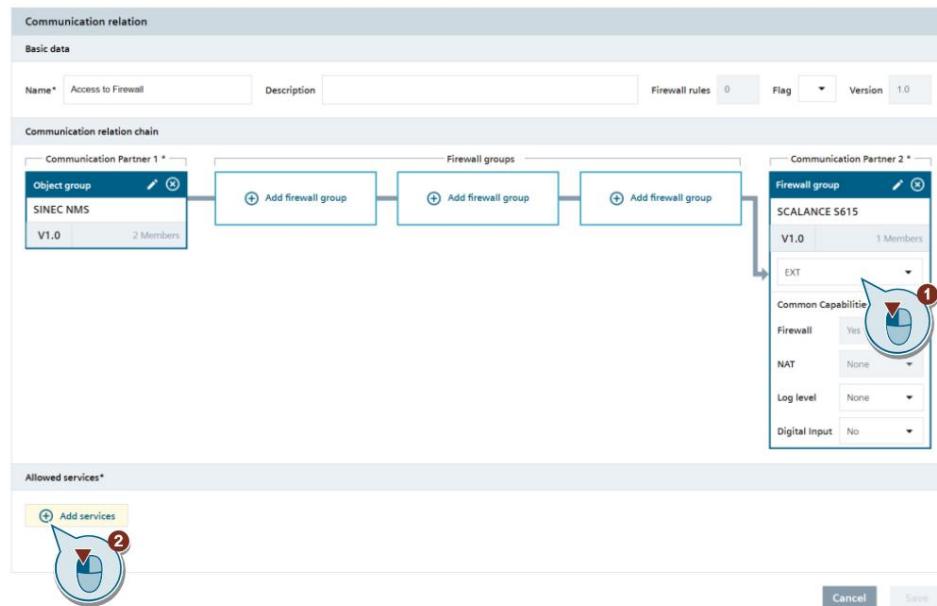
## 3 Ingeniería

17. Seleccione la interfaz "EXT". Haga clic en el botón "Agregar servicios".

Para cada grupo de cortafuegos, se pueden seleccionar las funciones de dispositivo comunes que se utilizarán. Las siguientes opciones están disponibles:

- Cortafuegos: determina si se crean reglas de cortafuegos para este cortafuegos a través de relaciones de comunicación.
- NAT: es posible configurar una traducción de direcciones (NAT) en un relación de comunicación además de las reglas del cortafuegos. Se puede encontrar más información en la Sección [NAT](#).
- Nivel de registro: define el nivel de registro hasta el cual los eventos son registrados por el dispositivos de seguridad. Por ejemplo, si se selecciona el nivel de registro "Advertencia", se registran los eventos de los niveles de registro "Crítico" y "Advertencia", pero no se registran eventos del nivel de registro "Info".
- Entrada digital: al configurar la propiedad "Entrada digital", las reglas del firewall no están permanentemente activas, sino solo si la entrada digital está activada en el dispositivo.

Figura 3-28



## 3 Ingeniería

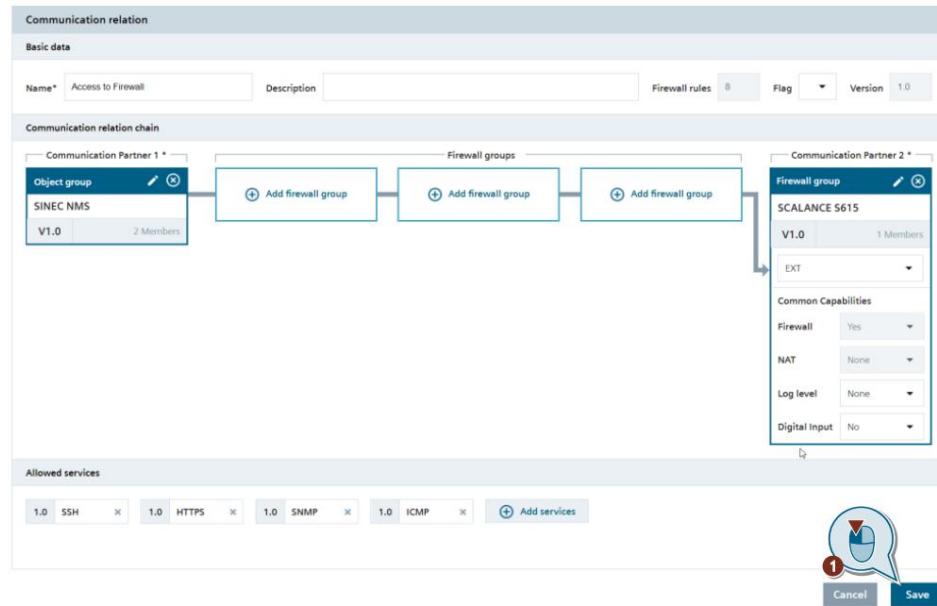
18. Para dispositivos SCALANCE, los servicios SNMP, HTTPS, SSH e ICMP son necesario. Para RUGGEDCOM, son necesarios los servicios SNMP, NETCONF-over-SSH e ICMP. Los servicios se seleccionan de la lista predefinida o se pueden agregar nuevos servicios. Seleccione los servicios. Haga clic en el botón "Agregar".

Figura 3-29



19. Haga clic en el botón "Guardar".

Figura 3-30



20. Introduzca un motivo para la acción que ha realizado. Haga clic en el botón "Guardar". La entrada se ingresa en el registro de auditoría.

Figura 3-31

Confirmation

Reason for change

Configuration Access to Firewall complete

de uso gratuito

Cancel Save

3 Ingeniería

21. Seleccione la relación de comunicación recién creada y haga clic en "Activar" botón.

SINEC NMS genera reglas de firewall/NAT a partir de las relaciones de comunicación activadas. Estas reglas se pueden mostrar en la página "Cumplimiento de la relación" y cargarse en los dispositivos de firewall participantes. Haga clic en la pestaña "Cumplimiento de la relación".

Figura 3-32

22. Antes de ejecutar, haga clic en el botón "Detalles del dispositivo" para ver las diferencias entre las reglas de firewall recién creadas y las reglas de firewall que están presentes en el dispositivo.

Figura 3-33

de uso gratuito

3 Ingeniería

23. Haga clic en el nombre del firewall para ver la comparación entre las reglas NAT y firewall configuradas y ya existentes en el dispositivo. Haga clic en el botón "Cerrar".

Figura 3-34

The screenshot shows the 'Device details - SCALANCE S615' interface. It has tabs for 'Firewall' and 'NAT'. Below them are two tables: 'Generated rules' and 'Online rules'. The 'Generated rules' table lists rules with columns: Priority, Action, SRC IP address, DST IP address, IP protocol, Protocol restrict., and Service name. The 'Online rules' table shows additional differences in the configuration. A callout bubble with the number '1' points to the 'Close' button at the bottom right.

Priority	Action	SRC IP address	DST IP address	IP protocol	Protocol restrict.	Service name
0	Accept	10.0.1.4	10.0.1.1	TCP	DST-22	SSH
1	Accept	10.0.1.4	10.0.1.1	TCP	DST-22	SSH
2	Accept	10.0.1.4	10.0.1.1	TCP	DST-443	HTTPS
3	Accept	10.0.1.4	10.0.1.1	TCP	DST-443	HTTPS
4	Accept	10.0.1.4	10.0.1.1	UDP	DST-161	SNMP
5	Accept	10.0.1.4	10.0.1.1	UDP	DST-161	SNMP
6	Accept	10.0.1.4	10.0.1.1	ICMP	Type8	ICMP
7	Accept	10.0.1.4	10.0.1.1	ICMP	Type8	ICMP

Priority	Action	SRC IP address	DST IP address	IP protocol	Protocol restrict.	Service name
0	Accept	Any	172.16.0.1			HTTP(grade)
1	Accept	Any	172.16.0.1			HTTP(grade)
2	Accept	Any	10.0.1.1			HTTP(grade)
3	Accept	Any	172.16.0.1			DN(grade)
4	Accept	Any	172.16.0.1			SNMP(grade)
5	Accept	Any	10.0.1.1			SNMP(grade)
6	Accept	Any	172.16.0.1			SNMP(grade)
7	Accept	Any	10.0.1.1			SNMP(grade)

24. Se debe seleccionar un rol antes de realizar la acción "Aplicar en el dispositivo". Seleccione el firewall y haga clic en el botón "Aplicar en el dispositivo".

Figura 3-35

The screenshot shows the 'Communication relations (1)' screen in the SINEC NMS interface. It includes tabs for 'Actions', 'Device details', and 'Enforce on device'. A callout bubble with the number '1' points to the 'Role' dropdown menu. Another callout bubble with the number '2' points to the 'Enforce on device' button. A third callout bubble with the number '3' points to the 'Device details' tab.

de uso gratuito

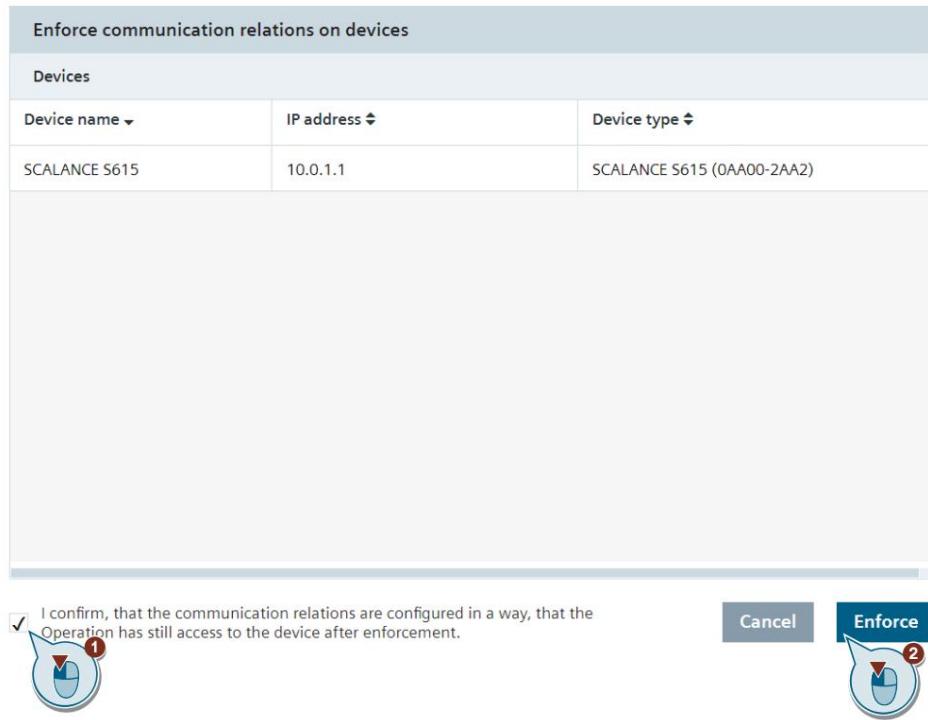
---

### 3 Ingeniería

25. Cierre la ventana de información. Haga clic en el botón "Aplicar" para cargar el relación de comunicación con el dispositivo.

**Nota** Cuando se ejecuta la relación de comunicación, se sobrescriben todas las reglas anteriores en el cortafuegos.

Figura 3-36



de uso gratuito

3 Ingeniería

26. Verifique la aplicación. El estado del dispositivo y el último estado de ejecución fueron exitosos. La sincronización entre SINEC NMS y las reglas de firewall/NAT generadas por el dispositivo de firewall coinciden con las reglas de firewall/NAT en el dispositivo de firewall.

**Nota** La sincronización entre SINEC NMS y SCALANCE S/RUGGEDCOM se actualiza en el Control después de un breve período de tiempo.

Figura 3-37

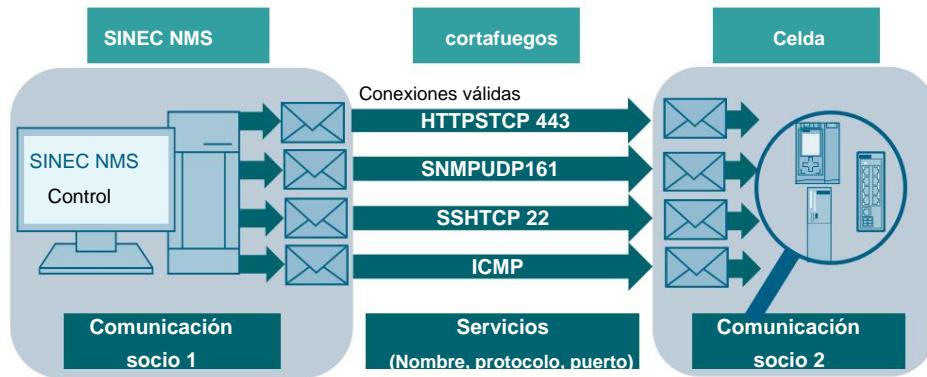
The screenshot shows the Siemens SINEC NMS interface under the 'CONTROL' tab. In the top navigation bar, 'Network administration' is selected. Below it, the path 'Home > Network administration > Communication management > Firewall/NAT' is visible. The main content area has two tabs: 'Communication relations (1)' and 'Relation enforcements'. The 'Communication relations (1)' tab is active. It displays a table with columns: 'Actions', 'Device details', and 'Enforce on device'. The table contains one row for a device named 'SCALANCE S615' with IP address '10.0.1.1'. The 'Device state' and 'Last enforcement state' columns both show a green status icon followed by the text 'Synchronised' and 'Success'. The entire row for this device is highlighted with a red border.

de uso gratuito

### 3.4 Configuración del acceso único a la celda

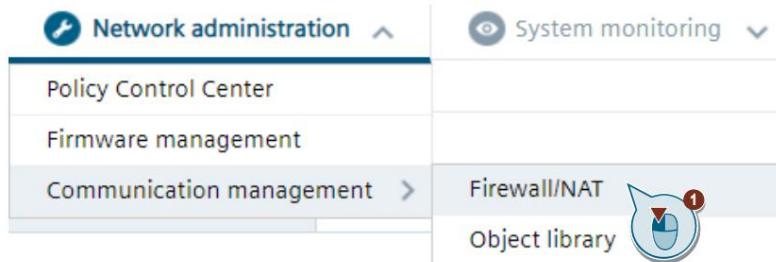
En el siguiente apartado se configura el acceso desde SINEC NMS al celular vía HTTPS, ICMP, SSH y SNMP. Esto permite un escaneo de red de la celda para agregar estaciones accesibles. El acceso se desactiva de nuevo después de leer la celda.

Figura 3-38



1. Abra el menú "Administración de red > Gestión de comunicación > Cortafuegos/NAT" en el Control.

Figura 3-39



Irrestricto

3 Ingeniería

2. Haga clic en el botón "Crear" para crear una nueva relación de comunicación.

Figura 3-40

**SIEMENS**

**CONTROL**

Home Network monitoring Network administration

Home » Network administration » Communication management » Firewall/NAT

Communication relations (1) Relation enforcements

Actions Create Edit Copy Activate

Flag	Name
<input type="checkbox"/>	Activated Access to Firewall

3. Asignar un nombre en la relación de comunicación. Haga clic en el botón "Agregar grupo de objetos" en "Socio de comunicación 1".

Figura 3-41

**Communication relation**

**Basic data**

Name*	Access to Cell	Description	Firewall rules	0	Flag	<input type="button" value="▼"/>	Version	1.0
-------	----------------	-------------	----------------	---	------	----------------------------------	---------	-----

**Communication relation ch**

Communication Partner 1

Communication Partner 2 \*

Add object group

Add device

Add firewall group

Add firewall group

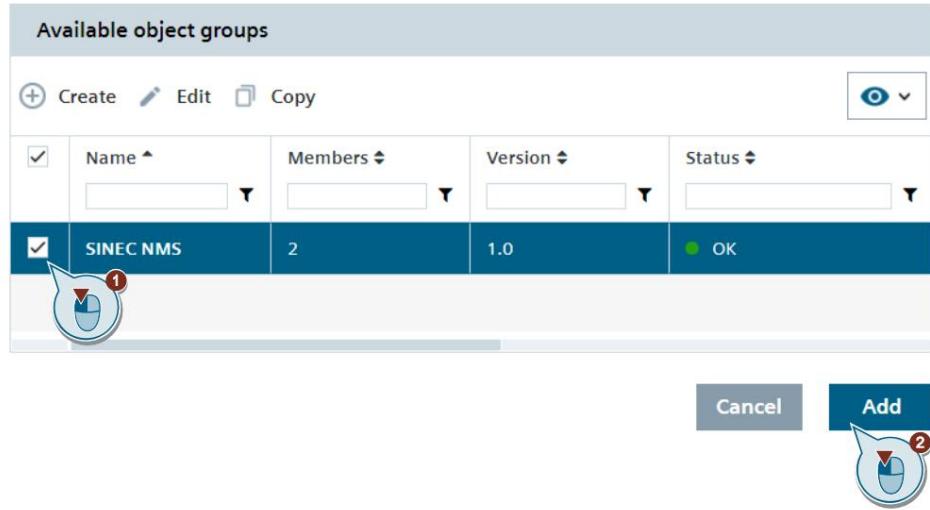
Add firewall group

Add firewall group

## 3 Ingeniería

4. Seleccione el grupo de objetos creado previamente "SINEC NMS". Haga clic en "Agregar" botón.

Figura 3-42



5. Haga clic en el botón "Agregar cualquier dispositivo" en "Socio de comunicación 2".

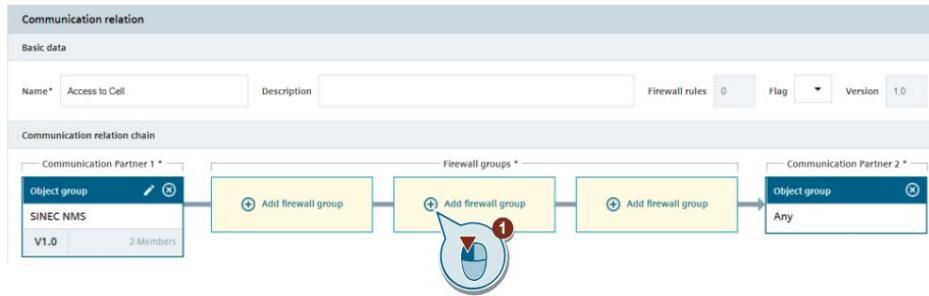
Figura 3-43



3 Ingeniería

6. Haga clic en el botón "Agregar grupo de cortafuegos".

Figura 3-44



7. Seleccione el grupo de cortafuegos recién creado "SCALANCE S615". Haga clic en "Agregar" botón.

Figura 3-45

The screenshot shows the 'Firewall groups' configuration screen. At the top, there are buttons for 'Create', 'Edit', and 'Copy'. Below is a table with columns: Name, Members, Active interfa..., Version, and Status. One row is selected, showing 'SCALANCE S615' with 1 member, 2 active interfaces, version 1.0, and status 'OK'. The bottom right of the table has 'Cancel' and 'Add' buttons, with the 'Add' button highlighted with a red circle.

<input checked="" type="checkbox"/>	Name	Members	Active interfa...	Version	Status
<input checked="" type="checkbox"/>	SCALANCE S615	1	2	1.0	OK

---

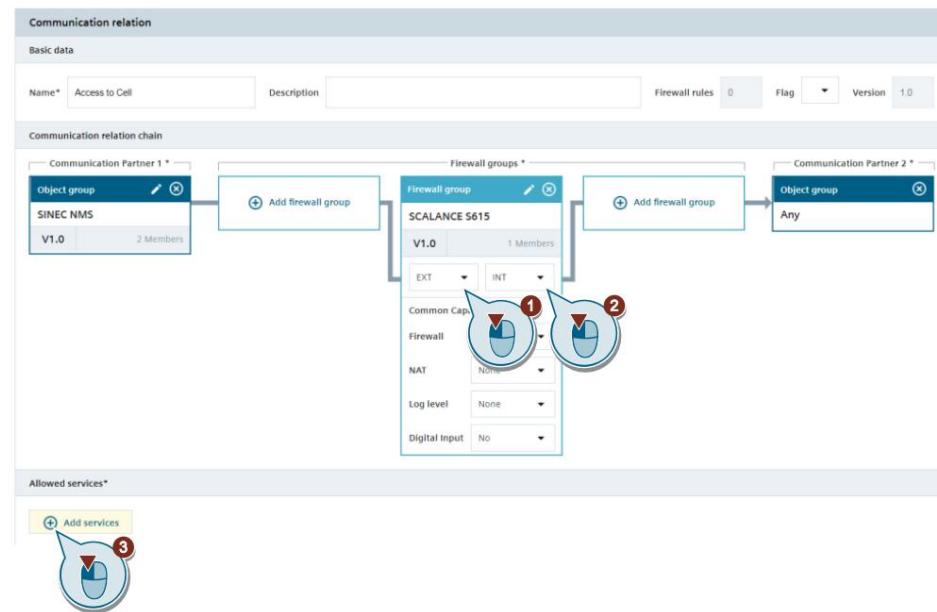
3 Ingeniería

8. Seleccione las interfaces "EXT" e "INT". Haga clic en el botón "Agregar servicios".

Para cada grupo de cortafuegos, también se pueden seleccionar las funciones comunes del dispositivo que se utilizarán. Las siguientes opciones están disponibles:

- Cortafuegos: determina si se crean reglas de cortafuegos para este cortafuegos a través de relaciones de comunicación.
- NAT: es posible configurar una traducción de direcciones (NAT) en un relación de comunicación además de las reglas del cortafuegos. Se puede encontrar más información en la Sección [NAT](#).
- Nivel de registro: define el nivel de registro hasta el cual los eventos son registrados por el dispositivos de seguridad. Por ejemplo, si se selecciona el nivel de registro "Advertencia", se registran los eventos de los niveles de registro "Crítico" y "Advertencia", pero no se registran los eventos del nivel de registro "Info".
- Entrada digital: al configurar la propiedad "Entrada digital", las reglas del firewall no están permanentemente activas, sino solo si la entrada digital está activada en el dispositivo.

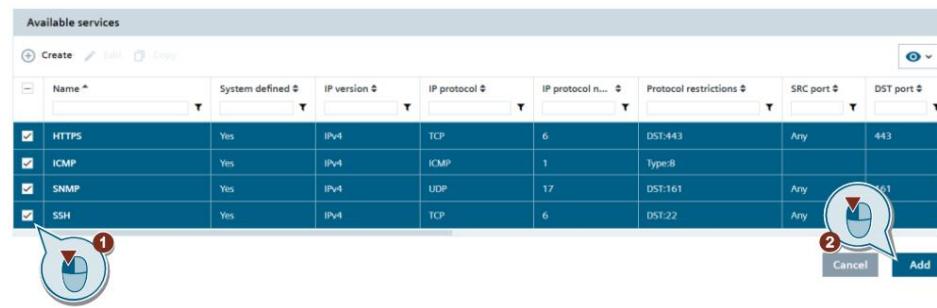
Figura 3-46



## 3 Ingeniería

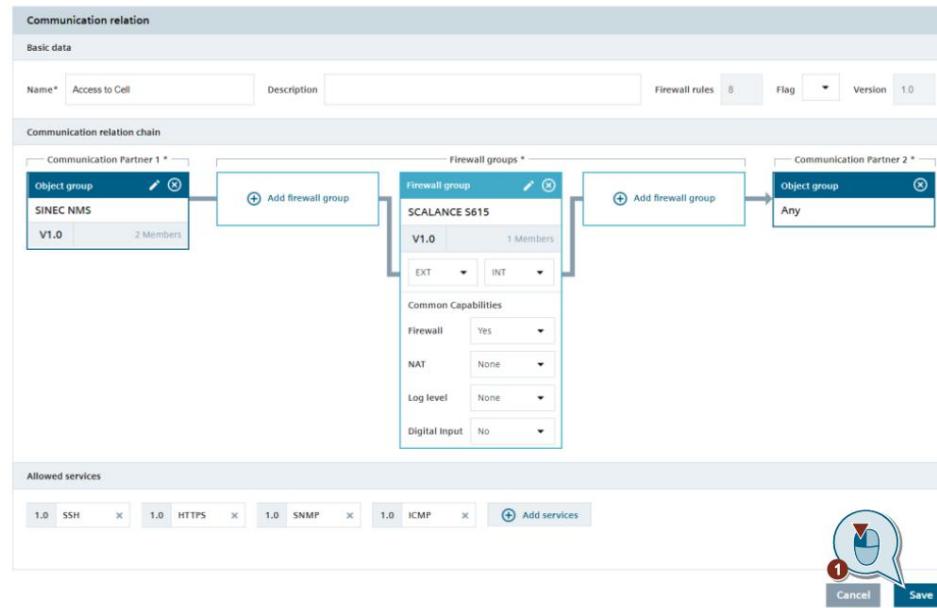
9. Seleccione los servicios "HTTPS", "ICMP", "SSH" y "SNMP". Haga clic en "Agregar" botón.

Figura 3-47



10. Haga clic en el botón "Guardar".

Figura 3-48



11. Introduzca un motivo para la acción que ha realizado. Haga clic en el botón "Guardar". La entrada se ingresa en el registro de [auditoría](#).

Figura 3-49

Confirmation

Reason for change

Configuration Access to Cell complete

de uso gratuito

Cancel Save

## 3 Ingeniería

12. Seleccione la relación de comunicación recién creada y haga clic en el botón "Activar".  
Haga clic en la pestaña "Cumplimiento de la relación".

Figura 3-50

**SIEMENS**

**CONTROL**

Home Network monitoring Network administration System monitoring

Home » Network administration » Communication management » Firewall/NAT

**Communication relations (2)** **Relation enforcements**

**Actions** Create Edit Copy Activate

Flag	Activated	Name	Status
<input checked="" type="checkbox"/>	Deactivated	Access to Cell	OK
<input type="checkbox"/>	Activated	Access to Firewall	OK

13. Antes de ejecutar, haga clic en el botón "Detalles del dispositivo" para ver las diferencias entre las reglas de firewall recién creadas y las reglas de firewall que están presentes en el dispositivo.

Figura 3-51

**SIEMENS** **SINEC NMS**

**CONTROL** Help SuperAdmin

Menu

Home » Network administration » Communication management » Firewall/NAT

**Communication relations (2)** **Relation enforcements**

**Actions** Device details Enforce on device

Device name	IP address	Device type	Device state
SCALANCE S615	10.0.1.1	SCALANCE S615 (0AA00-2AA2)	Enforcement required

de uso gratuito

3 Ingeniería

14. Haga clic en el nombre del cortafuegos. Haga clic en el nombre del cortafuegos para ver el comparación entre las reglas NAT y firewall configuradas y ya existentes en el dispositivo. Haga clic en el botón "Cerrar".

Figura 3-52

Priority	Action	SRC IP address	DST IP address	IP protocol	Protocol restriction	Service name
8	Accept	10.0.1.4	0.0.0.0	TCP	dst:22	SSH
9	Accept	10.0.1.4	0.0.0.0	TCP	dst:22	SSH
10	Accept	10.0.1.4	0.0.0.0	TCP	dst:443	HTTPS
11	Accept	10.0.1.4	0.0.0.0	TCP	dst:443	HTTPS
12	Accept	10.0.1.4	0.0.0.0	UDP	dst:161	SNMP
13	Accept	10.0.1.4	0.0.0.0	UDP	dst:161	SNMP
14	Accept	10.0.1.4	0.0.0.0	ICMP	Type:8	ICMP
15	Accept	10.0.1.4	0.0.0.0	ICMP	Type:8	ICMP

Priority	Action	SRC IP address	DST IP address	IP protocol	Protocol restriction	Service name
0	Accept	10.0.1.4	10.0.1.1	TCP	dst:22	SSH
1	Accept	10.0.1.4	10.0.1.1	TCP	dst:22	SSH
2	Accept	10.0.1.4	10.0.1.1	TCP	dst:443	HTTPS
3	Accept	10.0.1.4	10.0.1.1	TCP	dst:443	HTTPS
4	Accept	10.0.1.4	10.0.1.1	UDP	dst:161	SNMP
5	Accept	10.0.1.4	10.0.1.1	UDP	dst:161	SNMP
6	Accept	10.0.1.4	10.0.1.1	ICMP	Type:8	ICMP
7	Accept	10.0.1.4	10.0.1.1	ICMP	Type:8	ICMP

15. Se debe seleccionar un rol antes de realizar la acción "Aplicar en el dispositivo".  
Seleccione el firewall y haga clic en el botón "Aplicar en el dispositivo".

Figura 3-53

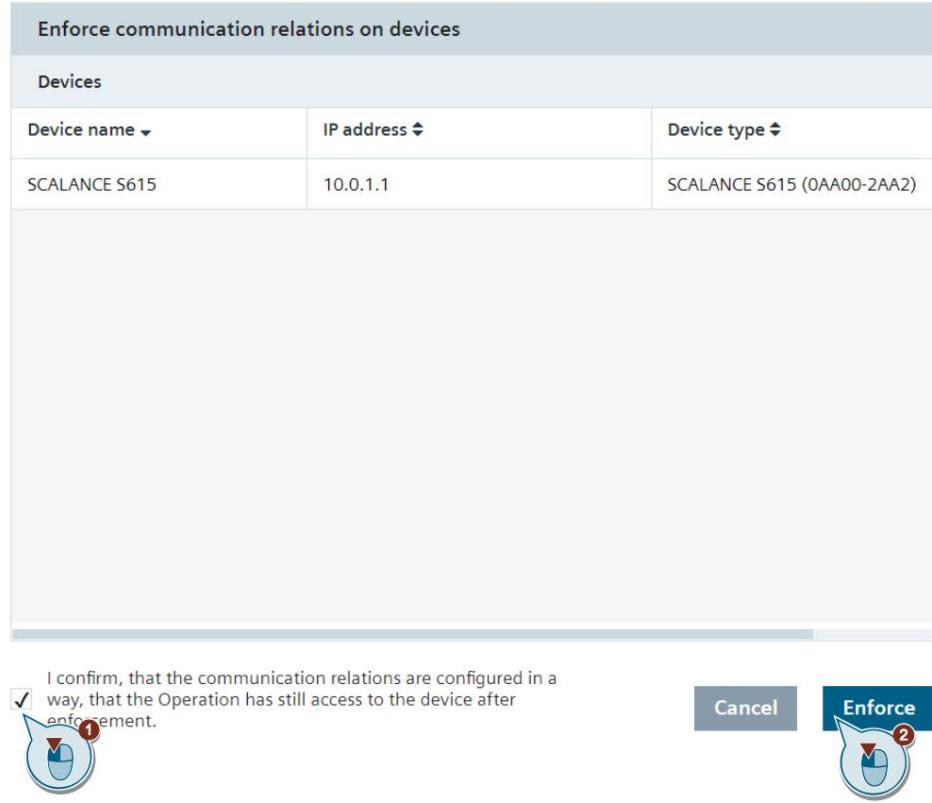
Actions	Device details	Enforce on device	Role*	Enforced on	Enforce
<input checked="" type="checkbox"/>	Device name: SCALANCE S615   IP address: 10.0.1.1   Device type: SCALANCE S615 (0AA00-2AA2)	<input type="button" value="Enforce on device"/>	Super Admin	mmddyyyy	<input type="button" value="Enforce"/>

## 3 Ingeniería

16. Confirme el cuadro de diálogo de que SINEC NMS aún puede acceder al cortafuegos después de desplegado Haga clic en el botón "Aplicar".

**Nota** Cuando se ejecuta la relación de comunicación, se sobrescriben todas las reglas anteriores en el cortafuegos.

Figura 3-54



de uso gratuito

## 3 Ingeniería

17. Verifique la aplicación. El estado del dispositivo y el último estado de ejecución fueron exitosos.

La sincronización entre SINEC NMS y las reglas de firewall/NAT generadas por el dispositivo de firewall coinciden con las reglas de firewall/NAT en el dispositivo de firewall.

**Nota**

La sincronización entre SINEC NMS y SCALANCE S/RUGGEDCOM se actualiza en el Control después de un breve período de tiempo.

Figura 3-55

Device name	IP address	Device type	Device state	Last enforcement state
SCALANCE S615	10.0.1.1	SCALANCE S615 (0AA00-2AA2)	Synchronised	Success

18. Abra el menú "Administración del sistema > Operaciones" en el Control.

Figura 3-56

19. Seleccione la operación y haga clic en el botón "Editar rangos de escaneo"

Figura 3-57

de uso gratuito

## 3 Ingeniería

20. Haga clic en el botón "Crear" para agregar una nueva área de escaneo.

Figura 3-58



21. Asigne un nombre y un rango de direcciones IP al área de escaneo. Haga clic en "Activar" botón. Haga clic en el botón "Aceptar" para completar la configuración.

Figura 3-59

Name of scan range\* Production Cell

First IP address\* 172.16.0.1

Last IP address\* 172.16.0.5

Devices in scan ranges 5

Enable

Operation\* WIN10Blank

Cancel OK

22. Haga clic en el botón "Aceptar".

Figura 3-60

Status	First IP address	Last IP address	Operation	Name
<input type="checkbox"/> Enabled	10.0.1.1	10.0.1.5	WIN10Blank	Cell
<input type="checkbox"/> Enabled	172.16.0.1	172.16.0.5	WIN10Blank	Production Cell

Cancel OK

3 Ingeniería

23. Haga clic en el botón "Iniciar análisis de red".

Figura 3-61

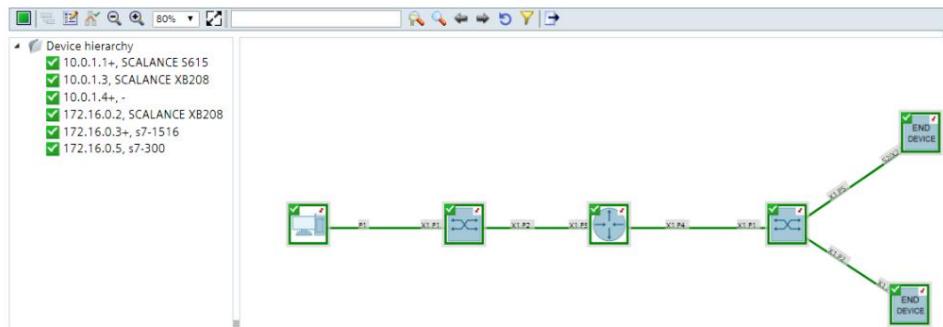


24. Se detectaron 3 nuevos dispositivos después del escaneo de red.

Figura 3-62

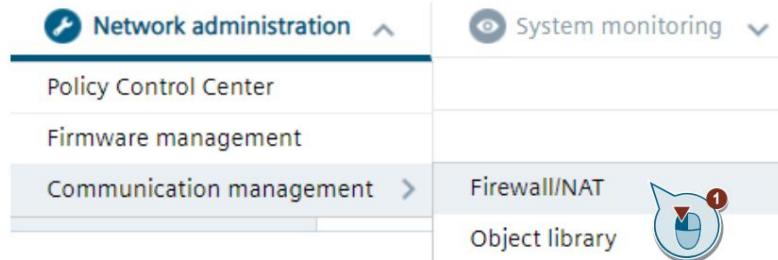


Figura 3-63



25. Abra el menú "Administración de red > Gestión de comunicación > Firewall/NAT" en el Control.

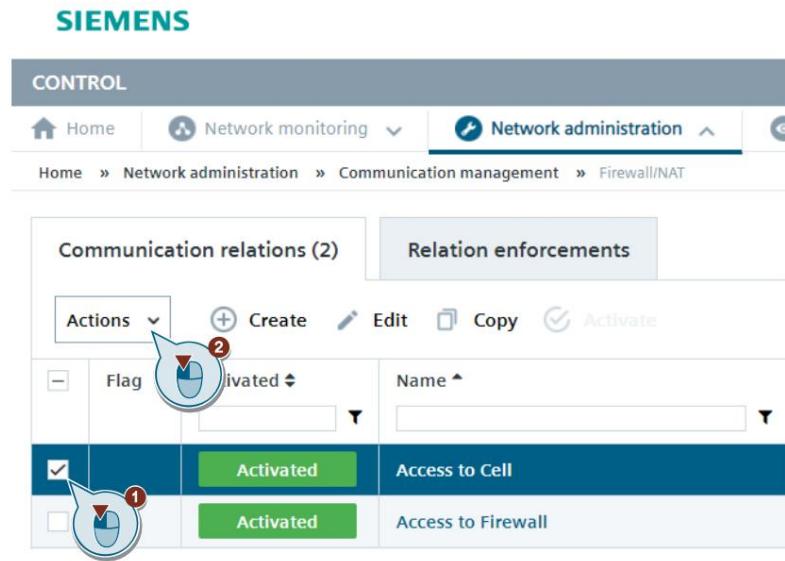
Figura 3-64



3 Ingeniería

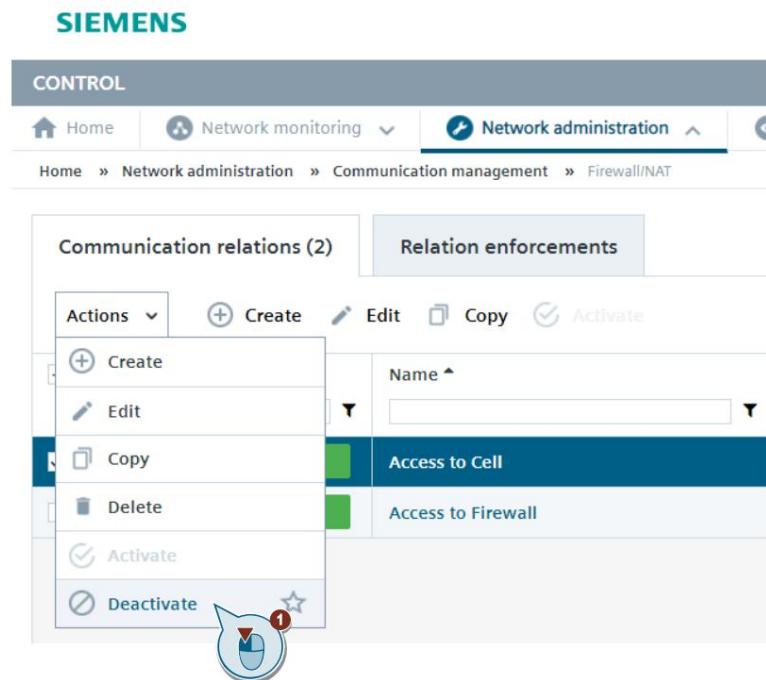
26. Seleccione la relación de comunicación recién creada. Haga clic en el botón "Acciones".

Figura 3-65



27. Haga clic en el botón "Desactivar". La relación de comunicación recién creada ya no es necesaria después de escanear. El acceso a los componentes individuales de la celda se explica en la siguiente sección.

Figura 3-66

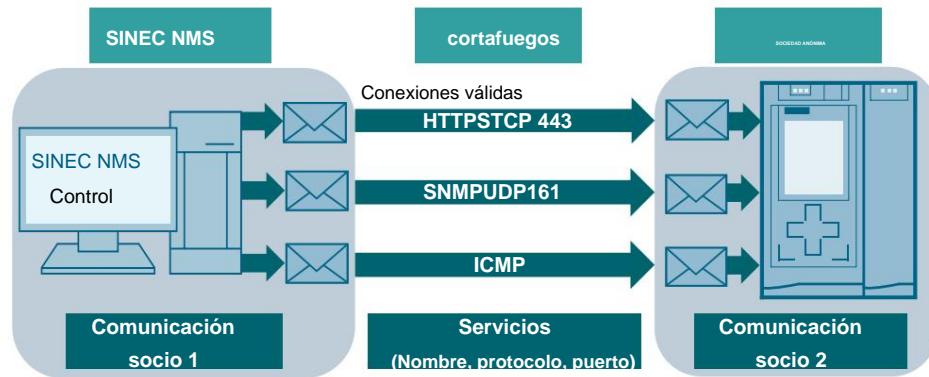


## 3 Ingeniería

### 3.5 Acceder a los datos del PLC

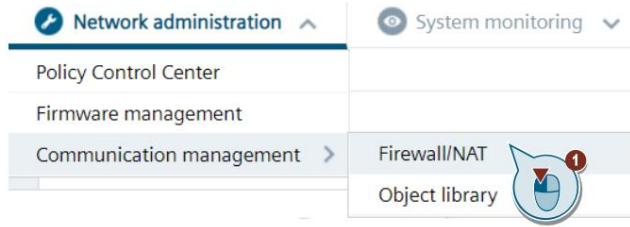
En la siguiente sección, se restringe el acceso a dispositivos individuales en la celda. En el siguiente ejemplo, se configura el acceso de SINEC NMS al PLC a través de HTTPS, ICMP y SNMP.

Figura 3-67



1. Abra el menú "Administración de red > Gestión de comunicación > Cortafuegos/NAT" en el Control.

Figura 3-68



Irrestricto

3 Ingeniería

2. Haga clic en el botón "Crear" para crear una nueva relación de comunicación.

Figura 3-69

The screenshot shows the SIMATIC Manager interface under the 'CONTROL' tab. The navigation path is Home > Network administration > Communication management > Firewall/NAT. The main area displays a table titled 'Communication relations (2)' with two rows. The first row has a status of 'Deactivated' and the second row has a status of 'Activated'. The top toolbar includes buttons for Home, Network monitoring, Network administration (highlighted), and other network-related functions. A prominent 'Create' button is highlighted with a red circle and a number '1'.

Communication relations (2)			Relation enforcements
Actions			
<input type="checkbox"/>	Flag	Activ	Name
<input type="checkbox"/>		Deactivated	Access to Cell
<input type="checkbox"/>		Activated	Access to Firewall

3. Asignar un nombre en la relación de comunicación. Haga clic en el botón "Agregar grupo de objetos" en "Socio de comunicación 1".

Figura 3-70

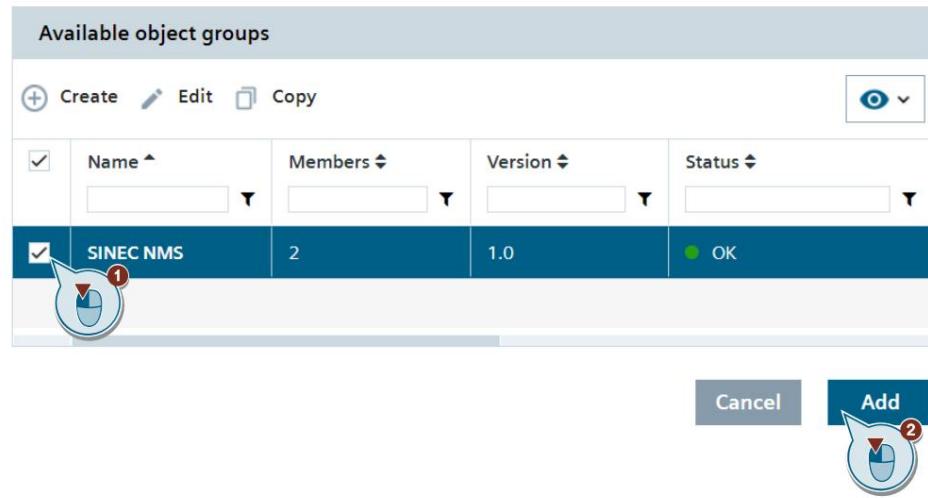
This screenshot shows the 'Communication relation' configuration page. It includes sections for 'Basic data' (Name: Access to S7-1500, Description: blank, Firewall rules: 0, Flag: off, Version: 1.0) and 'Communication relation chain'. The 'Communication Partner 1' section is highlighted with a yellow box and a red circle around the 'Add object group' button. The 'Communication Partner 2' section also has a red circle around its 'Add object group' button. The 'Firewall groups' section is shown in the middle.

de uso gratuito

3 Ingeniería

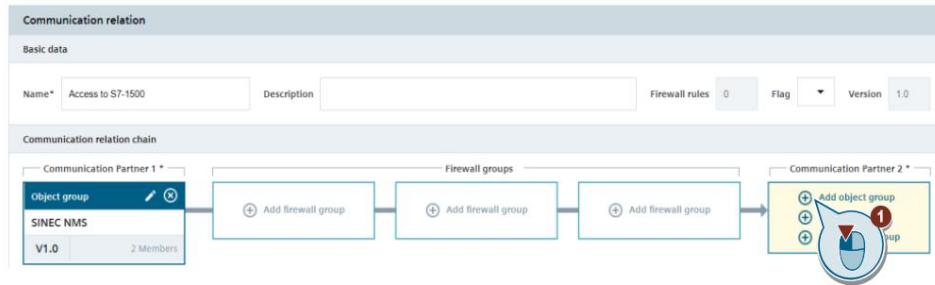
4. Seleccione el grupo de objetos creado previamente "SINEC NMS". Haga clic en "Agregar" botón.

Figura 3-71



5. Haga clic en el botón "Agregar grupo de objetos" en "Comunicador 2".

Figura 3-72



de uso gratuito

3 Ingeniería

6. Haga clic en el botón "Crear" para crear un nuevo grupo de objetos.

Figura 3-73

Available object groups			
<input type="button" value="Create"/>	<input type="button" value="Edit"/>	<input type="button" value="Copy"/>	
Name	Members	Version	Status
<input type="checkbox"/> SINEC NMS	2	1.0	<span style="color: green;">OK</span>

7. Asigne un nombre al grupo de objetos. Haga clic en el botón "Agregar dispositivos monitoreados".

Con esta opción, agrega dispositivos que son monitoreados por SINEC NMS. Para los dispositivos monitoreados, SINEC NMS muestra la información de monitoreo detectada en el grupo de objetos y detecta los cambios realizados en el dispositivo fuera de SINEC NMS.

Alternativamente, también puede seleccionar la función "Agregar direcciones IP de dispositivos". Con esta función se pueden incluir dispositivos que no son monitorizados por SINEC NMS.

Figura 3-74

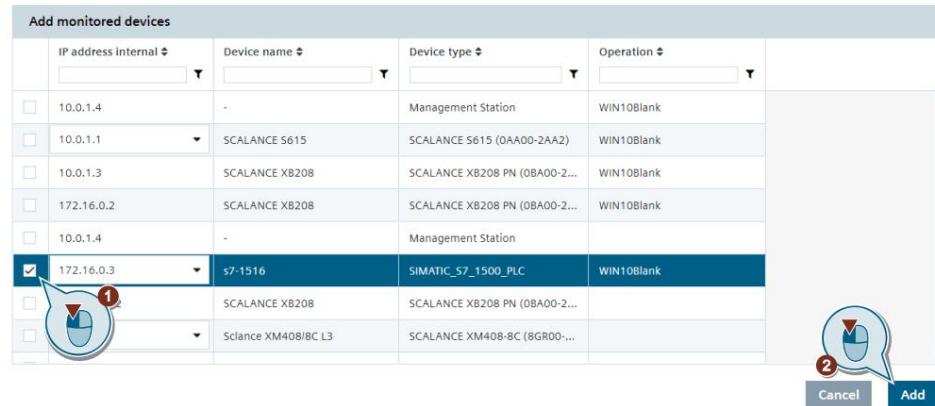
Object group	
Name*	S7 1500
Description	
Member	
<input type="button" value="Add monitored devices"/>	<input type="button" value="Add device IP addresses"/>
<input type="button" value="Delete"/>	<input checked="" type="checkbox"/> Apply member changes
Address internal	Device name
<input type="checkbox"/>	<input type="checkbox"/>
Monitored	

de uso gratuito

3 Ingeniería

8. Seleccione el controlador S7-1500. Haga clic en el botón "Agregar".

Figura 3-75



de uso gratuito

3 Ingeniería

9. Haga clic en el botón "Guardar".

Figura 3-76

IP address internal	Device name	Monitored	Status
172.16.0.3	s7-1516	Yes	OK

10. Introduzca un motivo para la acción que ha realizado. Haga clic en el botón "Guardar". La entrada se ingresa en el registro de [auditoría](#).

Figura 3-77

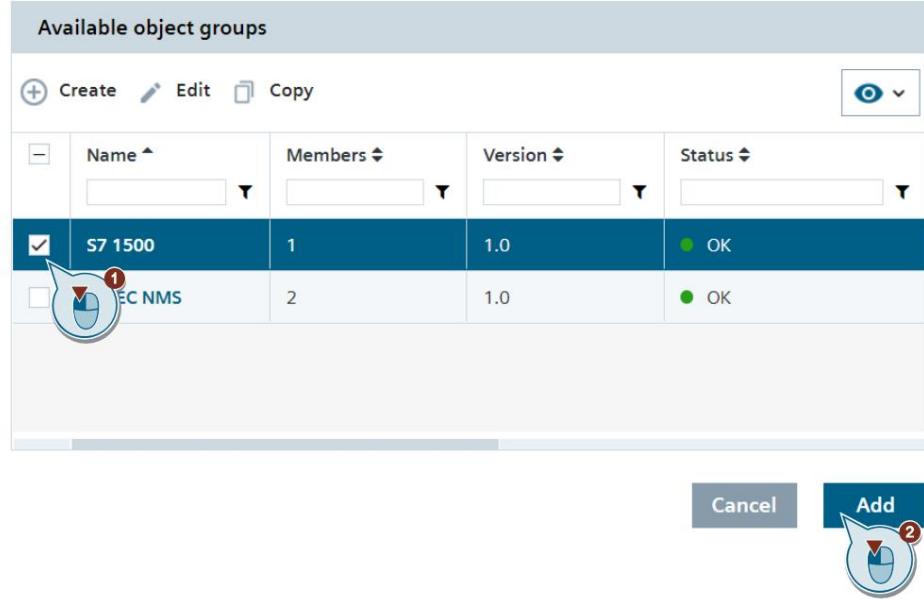
Provide a reason for this action  
Communication Partner 2 PLC

de uso gratuito

## 3 Ingeniería

11. Seleccione el grupo de objetos recién creado "PLC". Haga clic en el botón "Agregar".

Figura 3-78



12. Haga clic en el botón "Agregar grupo de firewall".

Figura 3-79



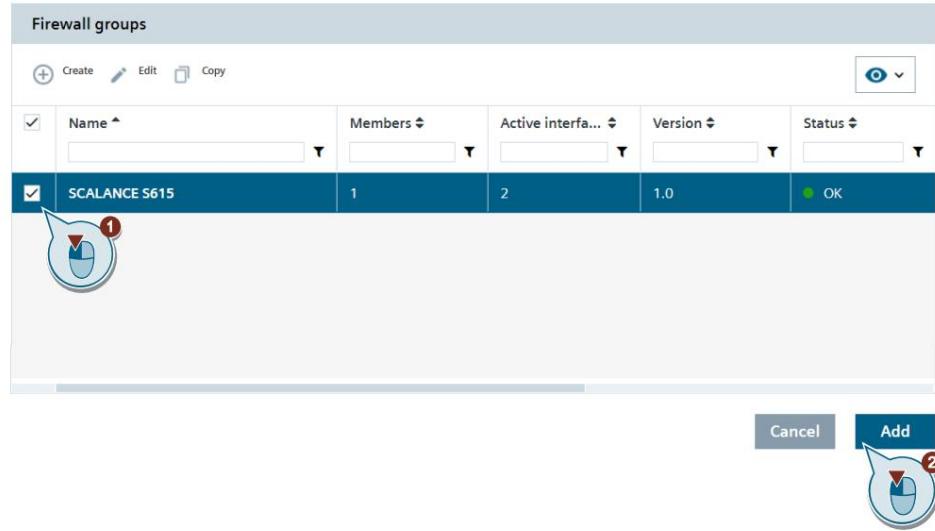
de uso gratuito

---

### 3 Ingeniería

13. Seleccione el grupo de cortafuegos recién creado "SCALANCE S615". Haga clic en "Agregar" botón.

Figura 3-80



The screenshot shows a software interface titled "Firewall groups". At the top, there are buttons for "Create", "Edit", and "Copy". Below the header is a table with columns: Name, Members, Active interfa..., Version, and Status. A row for "SCALANCE S615" is selected, highlighted in blue. The table shows the following data for the selected row:

Name	Members	Active interfa...	Version	Status
SCALANCE S615	1	2	1.0	OK

Two red numbered callouts are present: callout 1 points to the "SCALANCE S615" row, and callout 2 points to the "Add" button located at the bottom right of the interface.

de uso gratuito

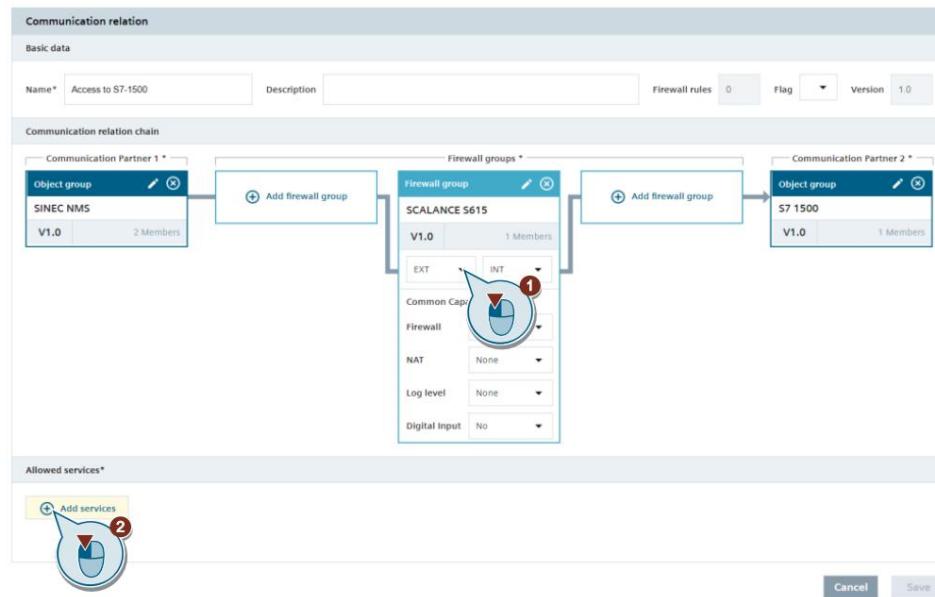
3 Ingeniería

14. Seleccione las interfaces "EXT" e "INT". Haga clic en el botón "Agregar servicios".

Para cada grupo de cortafuegos, también se pueden seleccionar las funciones comunes del dispositivo que se utilizarán. Las siguientes opciones están disponibles:

- Cortafuegos: determina si se crean reglas de cortafuegos para este cortafuegos a través de relaciones de comunicación.
- NAT: es posible configurar una traducción de direcciones (NAT) en un relación de comunicación además de las reglas del cortafuegos. Se puede encontrar más información en la Sección [NAT](#).
- Nivel de registro: define el nivel de registro hasta el cual los eventos son registrados por el dispositivos de seguridad. Por ejemplo, si se selecciona el nivel de registro "Advertencia", se registran los eventos de los niveles de registro "Crítico" y "Advertencia", pero no se registran los eventos del nivel de registro "Info".
- Entrada digital: al configurar la propiedad "Entrada digital", las reglas del firewall no están permanentemente activas, sino solo si la entrada digital está activada en el dispositivo.

**Figura 3-81**



3 Ingeniería

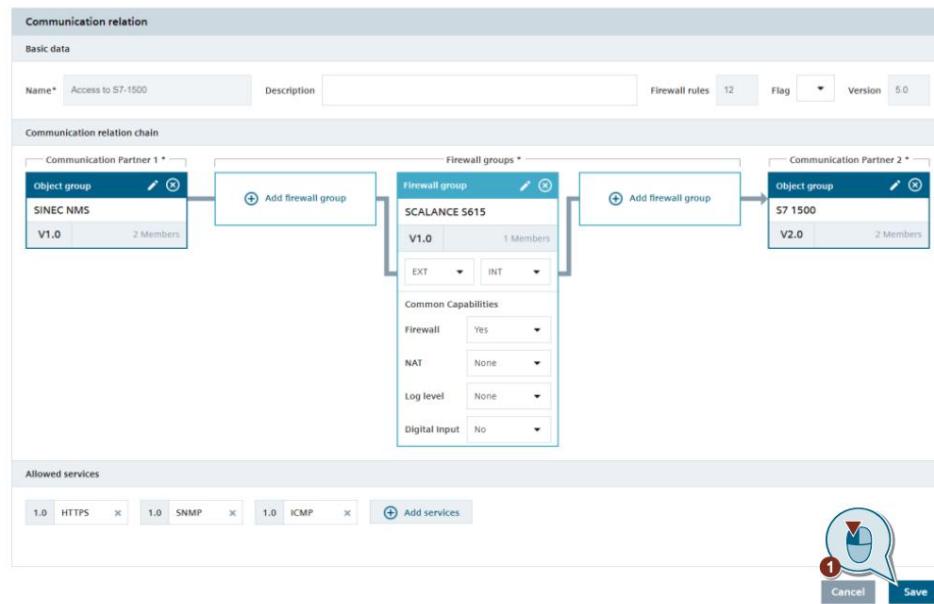
15. Seleccione los servicios "HTTPS"; "ICMP" y "SNMP". Haga clic en el botón "Agregar".

Figura 3-82



16. Haga clic en el botón "Guardar".

Figura 3-83



17. Introduzca un motivo para la acción que ha realizado. Haga clic en el botón "Guardar". La entrada se ingresa en el registro de [auditoría](#)

Figura 3-84

Confirmation

Reason for change

Configuration Access to Cell complete

de uso gratuito

Cancel Save

## 3 Ingeniería

18. Seleccione la relación de comunicación recién creada y haga clic en el botón "Activar".  
Haga clic en la pestaña "Cumplimiento de la relación".

Figura 3-85

Flag	Activated	Name	Status
<input type="checkbox"/>	Deactivated	Access to Cell	OK
<input type="checkbox"/>	Activated	Access to Firewall	OK
<input checked="" type="checkbox"/>	Deactivated	Access to S7-1500	OK

19. Antes de ejecutar, haga clic en el botón "Detalles del dispositivo" para ver las diferencias entre las reglas de firewall recién creadas y las reglas de firewall que están presentes en el dispositivo.

Figura 3-86

Device name	IP address	Device type	Device state
<input checked="" type="checkbox"/> SCALANCE S615	10.0.1.1	SCALANCE S615 (0AA00-2AA2)	Enforcement required

de uso gratuito

3 Ingeniería

20. Haga clic en el nombre del cortafuegos. Haga clic en el nombre del cortafuegos para ver el comparación entre las reglas NAT y firewall configuradas y ya existentes en el dispositivo. Haga clic en el botón "Cerrar".

Figura 3-87

Priority *	Action *	SRC IP address *	DST IP address *	IP protocol *	Protocol restriction *	Service name
4	Accept	10.0.1.4	10.0.1.1	UDP	DST:161	SNMP
5	Accept	10.0.1.4	10.0.1.1	UDP	DST:161	SNMP
6	Accept	10.0.1.4	10.0.1.1	ICMP	Type:8	ICMP
7	Accept	10.0.1.4	10.0.1.1	ICMP	Type:8	ICMP
8	Accept	10.0.1.4	172.16.0.3	TCP	DST:443	HTTPS
9	Accept	10.0.1.4	172.16.0.3	TCP	DST:443	HTTPS
10	Accept	10.0.1.4	172.16.0.3	UDP	DST:161	SNMP
11	Accept	10.0.1.4	172.16.0.3	UDP	DST:161	SNMP

Priority *	Action *	SRC IP address *	DST IP address *	IP protocol *	Protocol restriction *	Service name
0	Accept	10.0.1.4	10.0.1.1	TCP	DST:22	SSH
1	Accept	10.0.1.4	10.0.1.1	TCP	DST:22	SSH
2	Accept	10.0.1.4	10.0.1.1	TCP	DST:443	HTTPS
3	Accept	10.0.1.4	10.0.1.1	TCP	DST:443	HTTPS
4	Accept	10.0.1.4	10.0.1.1	UDP	DST:161	SNMP
5	Accept	10.0.1.4	10.0.1.1	UDP	DST:161	SNMP
6	Accept	10.0.1.4	10.0.1.1	ICMP	Type:8	ICMP
7	Accept	10.0.1.4	10.0.1.1	ICMP	Type:8	ICMP

21. Se debe seleccionar un rol antes de realizar la acción "Aplicar en el dispositivo".  
Seleccione el firewall y haga clic en el botón "Aplicar en el dispositivo".

Figura 3-88

Actions	Device details	Enforce on device	Role*	Enforce
<input checked="" type="checkbox"/>	Device name: SCALANCE S615   IP address: 10.0.1.1   Device state: SCALANCE S615 (0AA00-2AAZ)	Enforcement required	Super Admin	<input checked="" type="checkbox"/> mm/dd/yyyy 09/25/2020 20:36 SuperAdmin

**Nota**

No se puede acceder a la celda en el momento en que se configuran las reglas del firewall.

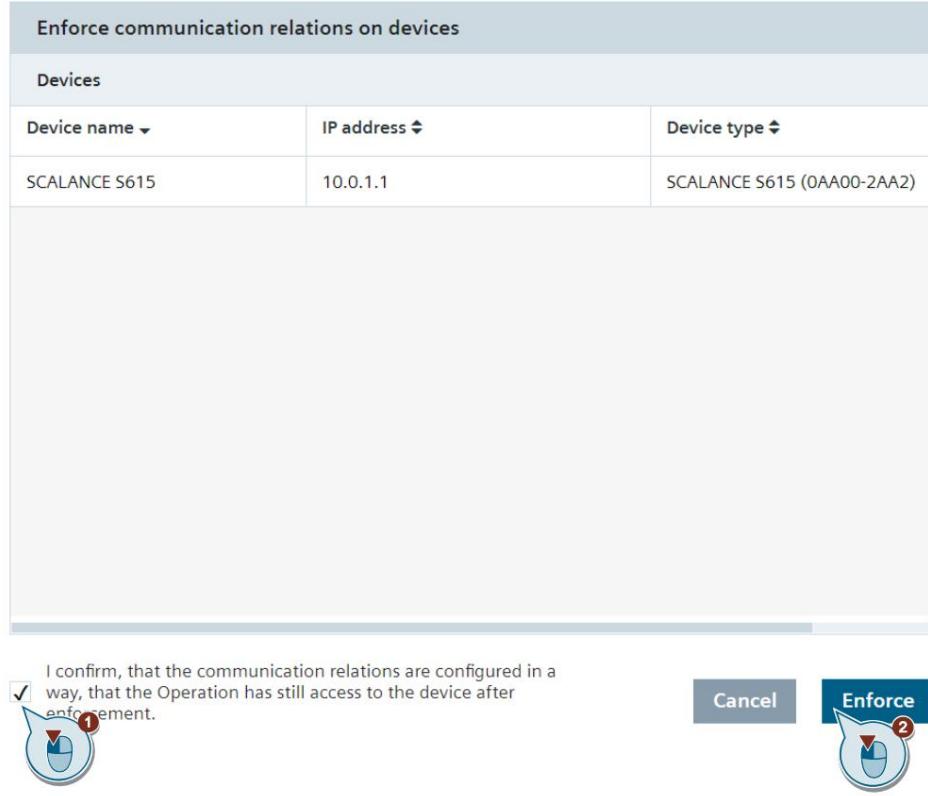
de uso gratuito

## 3 Ingeniería

22. Confirme el cuadro de diálogo de que SINEC NMS aún puede acceder al cortafuegos después de desplegado Haga clic en el botón "Aplicar".

**Nota** Cuando se ejecuta la relación de comunicación, se sobrescriben todas las reglas anteriores en el cortafuegos.

Figura 3-89



de uso gratuito

3 Ingeniería

23. Verifique la aplicación. El estado del dispositivo y el último estado de ejecución fueron exitosos. La sincronización entre SINEC NMS y las reglas de firewall/NAT generadas por el dispositivo de firewall coinciden con las reglas de firewall/NAT en el dispositivo de firewall.

**Nota** La sincronización entre SINEC NMS y SCALANCE S/RUGGEDCOM se actualiza en el Control después de un breve período de tiempo.

Figura 3-90

Device name	IP address	Device type	Device state	Last enforcement state
SCALANCE S615	10.0.1.1	SCALANCE S615 (0AA00-2AA2)	Synchronised	Success

de uso gratuito

---

### 3 Ingeniería

#### 3.6 Resultado

Se puede acceder al servidor web del SIMATIC S7-1500 a través del PC en el que se encuentra SINEC NMS Control and Operation.

Figura 3-91



de uso gratuito

### 3.7 Manejo de errores

Las razones del fracaso de una relación de comunicación pueden ser muy diversas. Con la ayuda del informe de ejecución, los ajustes parametrizados incorrectamente pueden identificarse y corregirse.

1. Puede encontrar un informe de ejecución detallado sobre las posibles causas de los errores en la aplicación de políticas. Para ver este informe, abra la página "Administración de red > Centro de control de políticas > Cumplimiento de políticas". Seleccione el informe de ejecución fallida.

Figura 3-92

The screenshot shows the SIMATIC Manager interface under the 'CONTROL' tab. In the top navigation bar, 'Network administration' is selected. Below it, the 'Policy Control Center' is active. On the left, there are tabs for 'Policies (4)' and 'Policy enforcements'. The 'Policy enforcements' tab is highlighted. To its right is a table titled 'Enforcement report' with the following data:

Name	Last enforcement state	Last enforcement steps	Role	Enforcement report
Firewall NAT Enforcement 2...	Success	2 (0 / 2 / 0 / 0)	Super Admin	1 (09/25/2020 18:04)
Firewall NAT Enforcement 2...	Success	1 (0 / 1 / 0 / 0)	Super Admin	1 (09/26/2020 18:04)
Firewall NAT Enforcement 2...	Failed	2 (0 / 0 / 1 / 1)	Super Admin	1 (09/25/2020 17:45)
Firmware Update XB208 V4_2	Success	4 (0 / 4 / 0 / 0)	Super Admin	2 (07/13/2020 18:04)

2. El resultado de la ejecución muestra la causa del error.

Figura 3-93

The screenshot shows the 'Enforcement report' dialog box. It contains two sections of policy details. The second section, for rule 2, has a red box around the 'Enforcement result' column, which displays 'Error : Authorization Error'.

Device	Device type	Enforcement order	Port	Task	Parameters	Value	Enforcement result
sysName Not Set (10.0.1.1)	SCALANCE S615 (0A00-2AA2)	1	-	Load Firewall Configuration	-	-	Error : Authorization Error
Name:	NAT Rule						
Rule:	2						
Description:	NAT Rule						
Rule type:	Device Rule						
Summary:	Number of Matching Devices : 1						
Conditions:	Conditions: ((IPADDR_V4 EQUALS 10.0.1.1 and OPERATION_NAME EQUALS WIN10Blank))						
Required capabilities:	Firewall						
Device conditions:	(IPADDR_V4 IN (10.0.1.1))						
Rule strategy:	Path based						
Rule error handling:	On Error Stop For All Devices						

Irrestricto

### 3 Ingeniería

Los siguientes errores durante la configuración se pueden corregir con los siguientes pasos de manejo de errores.

Tabla 3-5

errores	Manejo de errores
Error de autorización	Compruebe si se permite el acceso de escritura al cortafuegos. SNMP de solo lectura debe estar deshabilitado en el dispositivo.
USMError	Compruebe los datos de inicio de sesión de SNMPv3.
Se acabó el tiempo	Actualmente no se puede acceder al cortafuegos. Compruebe si todavía puede llegar al cortafuegos con las relaciones de comunicación ejecutadas.
dispositivo cero	El cortafuegos permanece en estado de ejecución, elimínelo y vuelva a leerlo.

## 3.8 Pista de auditoría

La funcionalidad "Audit Trail" permite realizar un seguimiento de todos los cambios en la gestión del cortafuegos. Registra qué usuario realizó qué cambios, cuándo y en qué dispositivo. Tanto las entradas de Audit Trail como los mensajes de alarma del sistema se pueden reenviar a un servidor syslog externo.

Las entradas de Audit Trail se pueden encontrar en el Control en "Monitorización del sistema > Audit Trail".

Figura 3-94

The screenshot shows the SIMATIC Manager interface with the following navigation path: Home > System monitoring > Audit trail. The main content area displays a table of audit trail entries:

Class	Initiated by	Initiated on	Message	Details
Information	User: Super/Admin	09/26/2020 17:54	Communication relation: Access to Cell Created	Version: 1.0 Reason: Configuration Access to Cell complete
Information	User: Super/Admin	09/26/2020 17:47	Object group: S7 1500 created	Version: 1.0 Reason: Communication Partner 2 PLC

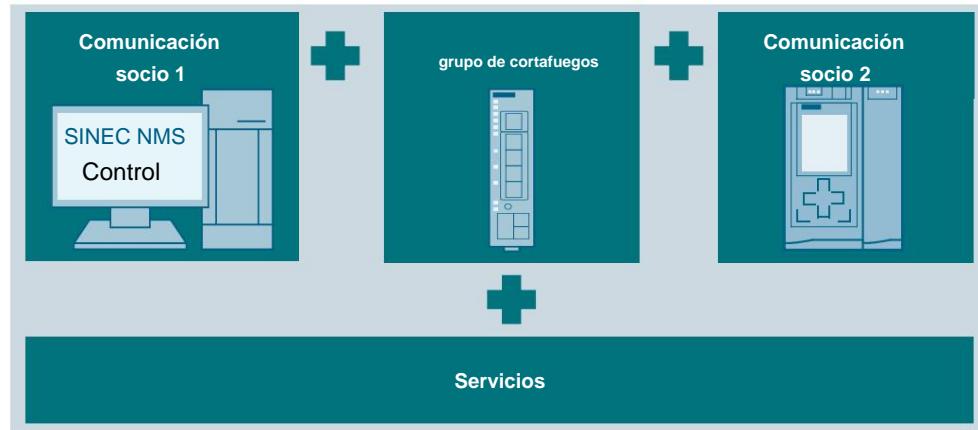
Irrestricto

## 4 Información útil

### 4.1 Estructura de una Relación de Comunicación en SINEC NMS

Las reglas de firewall se crean en SINEC NMS en las relaciones de comunicación. Una relación de comunicación describe qué socios de comunicación pueden comunicarse entre sí a través de qué servicios, así como qué dispositivos de seguridad se utilizan para asegurar esta comunicación. El sistema genera una política en base a la configuración realizada en la relación de comunicación.

Figura 4-1



#### Grupos de comunicación/grupos de objetos

Un grupo de objetos puede contener cualquier cantidad de dispositivos monitoreados, direcciones IP o rangos de IP. En lugar de un grupo específico de objetos, también se puede seleccionar el grupo predefinido "Cualquiera". Esto crea reglas de firewall sin direcciones IP de destino específicas.

Communication Partner 1 es el nombre del grupo de objetos cuyos dispositivos establecen comunicación con Communication Partner 2.

Communication Partner 2 es el nombre del objeto o grupo de cortafuegos con cuyos dispositivos se establece la comunicación.

#### Grupos de cortafuegos

Se pueden seleccionar hasta 3 grupos de cortafuegos en una relación de comunicación, que se ubican entre los dos grupos de comunicación. Para cada grupo de cortafuegos, se debe seleccionar la interfaz de comunicación entrante y saliente. Solo se pueden seleccionar las interfaces que son comunes a todos los cortafuegos dentro del grupo de cortafuegos.

En lugar de Communication Partner 2, también se pueden seleccionar grupos de cortafuegos para restringir el acceso al propio cortafuegos.

Irrestricto

---

## 4 Información útil

### Servicios

Define los protocolos con los que los dos socios de comunicación pueden comunicarse. Además de los servicios predefinidos, el usuario puede crear nuevos servicios con los protocolos y puertos IP requeridos.

### Dirección

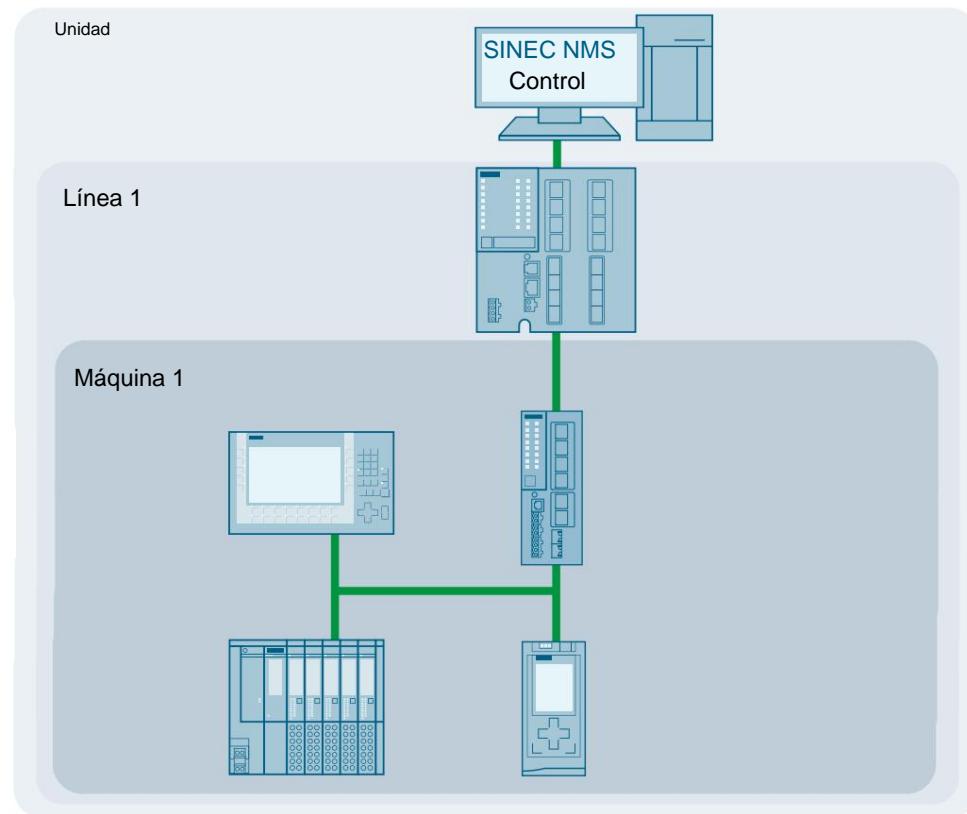
Muestra la dirección de la comunicación. El firewall está configurado para que la comunicación siempre se pueda establecer desde el Socio de comunicación 1 al Socio de comunicación 2. Se debe configurar una relación de comunicación separada para una configuración de comunicación en la dirección opuesta.

## 4 Información útil

### Ejemplo 1

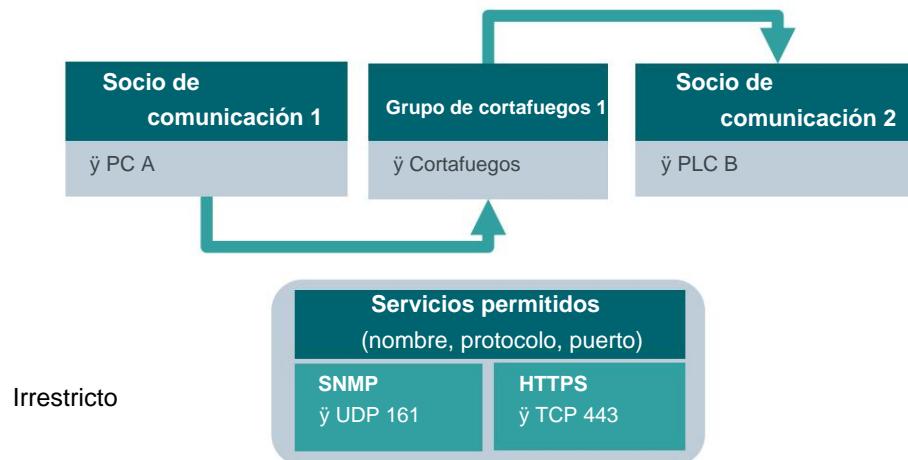
Un IPC debería poder acceder a un PLC a través de HTTPS y el protocolo SNMP. En este ejemplo ya se ha creado la relación de comunicación entre SINEC NMS y el cortafuegos.

Figura 4-2



En SINEC NMS esto se vería así:

Figura 4-3

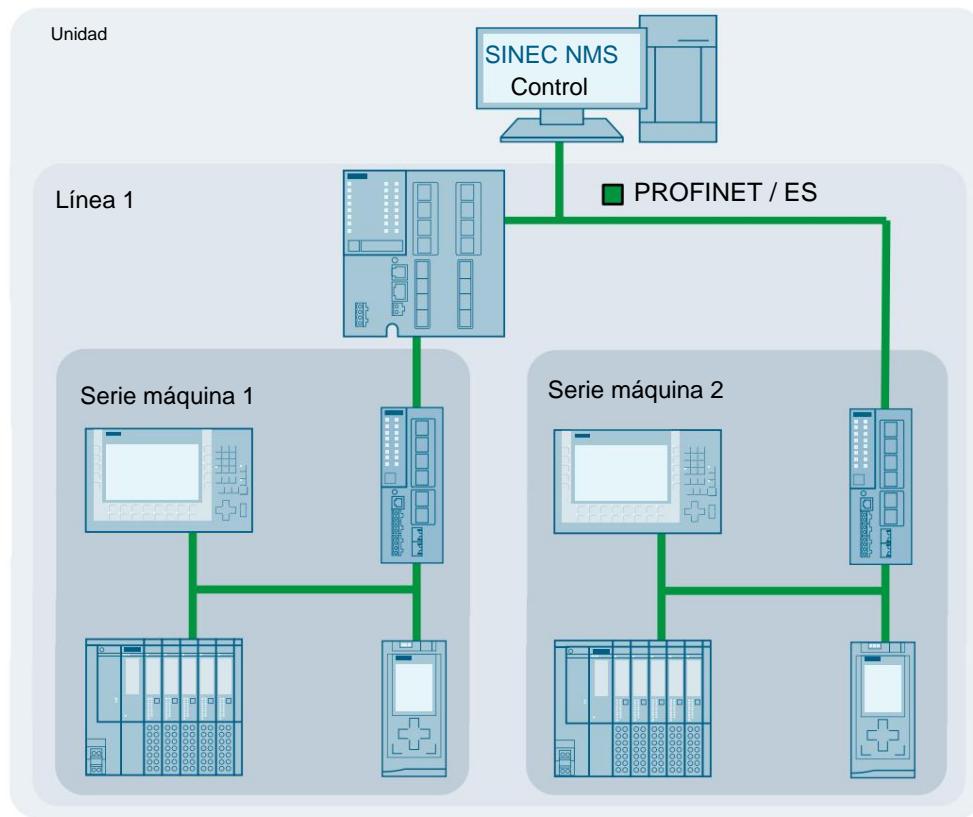


## 4 Información útil

### Ejemplo 2

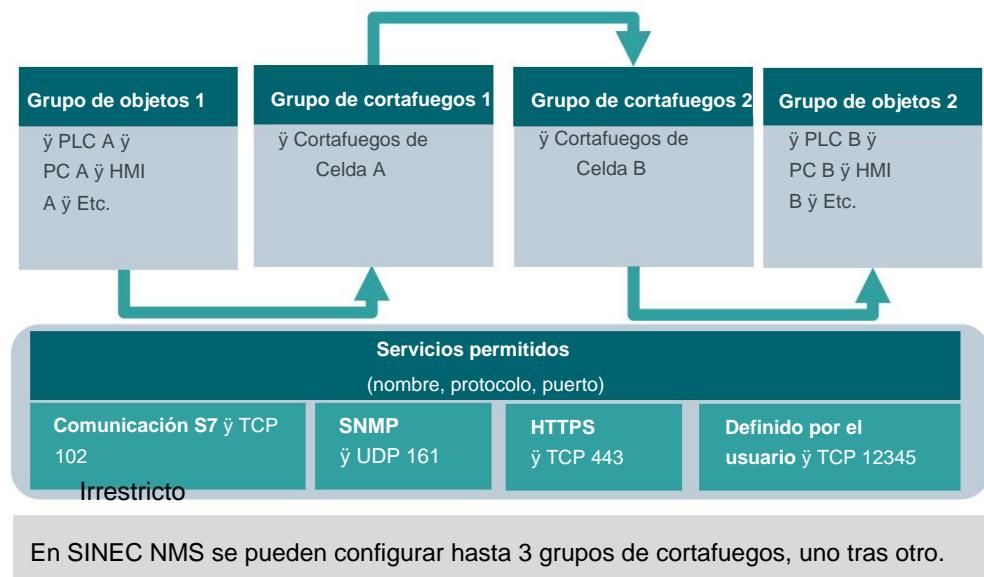
Los servicios de comunicación S7, SNMP, HTTPS y un protocolo definido por el usuario deben intercambiarse entre 2 celdas. En este ejemplo ya se ha creado la relación de comunicación entre SINEC NMS y el cortafuegos.

Figura 4-4



En SINEC NMS esto se vería así:

Figura 4-5

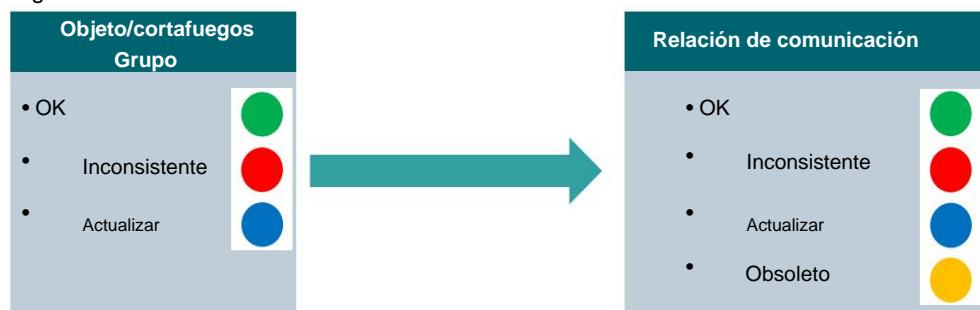


## 4 Información útil

**4.1.1 Estado de las Relaciones de Comunicación en SINEC NMS**

El estado de una relación de comunicación puede cambiar debido a la configuración en el proyecto o en el firewall. El estado de cada firewall o grupo de objetos afecta el estado general de la relación de comunicación.

Figura 4-6



El grupo objeto/cortafuegos o la relación de comunicación puede tener los siguientes estados:

- OK:

Todos los dispositivos en todos los grupos de objetos y cortafuegos están bien. La relación de comunicación puede ser ejecutada.

- Inconsistente:

Uno (o más) cortafuegos o grupos de objetos están en el estado "Incoherente". Esto sucede, por ejemplo, si el sistema NMS ya no puede acceder a un dispositivo o cortafuegos.

- Actualizar:

Uno (o más) cortafuegos o grupos de objetos se encuentran en el estado "Actualizar". Esto sucede, por ejemplo, cuando se cambia el nombre del dispositivo de un dispositivo o un firewall. El requisito para esto es que el dispositivo monitoreado se haya agregado a un grupo de objetos.

- Obsoleto:

Dentro de la relación de comunicación, existe una nueva versión para uno o más cortafuegos o grupos de objetos. Esto sucede, por ejemplo, cuando se agrega un nuevo dispositivo o firewall a un grupo que ya forma parte de la relación de comunicación.

Irrestricto

## 4 Información útil

**4.2 NOCHE**

La "traducción de direcciones de red" o "NAT" es un procedimiento que reemplaza la información de direcciones en los paquetes de datos con otra información.

**NAT en automatización**

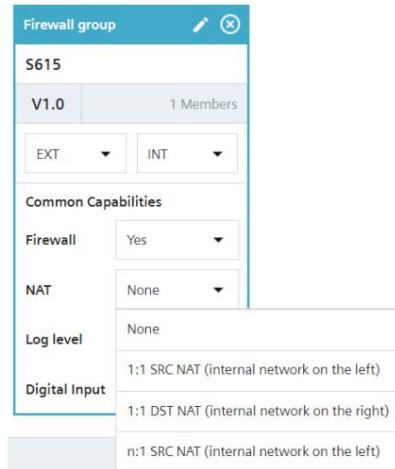
En el campo de la automatización, NAT se usa a menudo para conectar máquinas estándar a las que siempre se les asignan las mismas direcciones IP a una red de nivel superior en un rango de direcciones diferente. Esto simplifica la configuración para el fabricante de la máquina y, al mismo tiempo, permite el direccionamiento selectivo de los dispositivos individuales.

**NAT de origen y NAT de destino**

En general, se hace una distinción entre NAT de origen y NAT de destino, según la dirección del paquete IP que se traduzca. Si se cambia la dirección IP de origen del paquete, esto se denomina "Traducción de NAT de origen". Si, por el contrario, se cambia la dirección IP de destino, esto se denomina "Traducción de NAT de destino".

Las configuraciones de NAT se realizan en el grupo de cortafuegos.

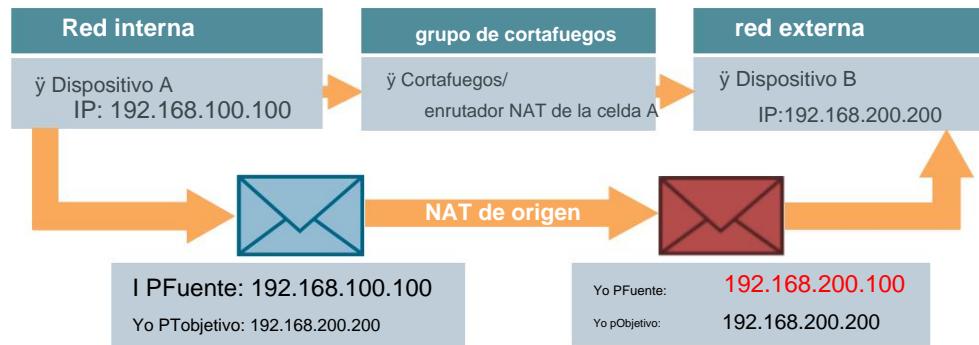
**Figura 4-7**



## 4 Información útil

### 4.2.1 NAT de origen

Figura 4-8



#### 1: 1 Fuente NAT

La dirección IP de origen de un paquete es reemplazada por el enrutador NAT durante la transmisión desde la red interna a la red externa. Una dirección IP de la red interna se asigna exactamente a una dirección IP en la red externa. La dirección de destino no se cambia.

La dirección adicional se introduce en la tabla NAT en "Inicio > Administración de redes > Gestión de comunicaciones > Biblioteca de objetos > NAT".

#### n: 1 Fuente NAT

El enrutador NAT reemplaza las direcciones de origen de todos los paquetes de más de un dispositivo en la red interna con una dirección de origen común. En la red externa, todos los paquetes parecen enviarse desde la misma dirección IP. Con SINEC NMS, esta dirección es la dirección de la interfaz externa del enrutador NAT.

#### Nota:

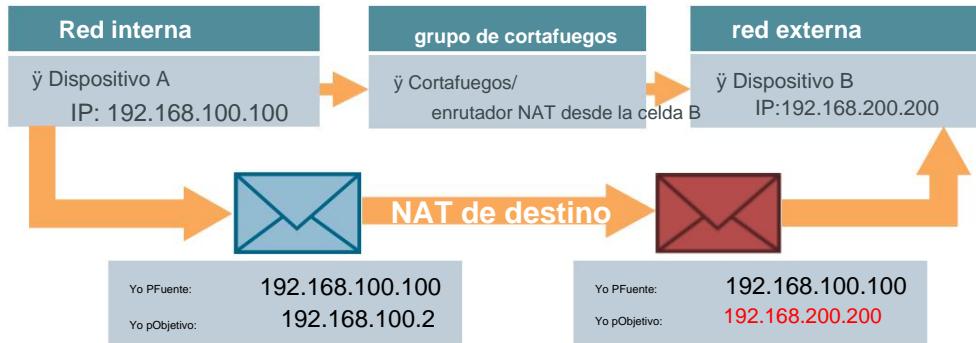
Para ambos tipos de NAT de origen, SINEC NMS siempre define la red izquierda en la relación de comunicación como la red interna.

Irrestricto

## 4 Información útil

## 4.2.2 NAT de destino

Figura 4-9



## 1: 1 Destino NAT

La dirección IP de destino del paquete es reemplazada por el enrutador NAT durante la transmisión desde la red externa a la interna. Una dirección IP de la red externa se asigna exactamente a una dirección IP en la red interna. Si el NAT de destino está activado, el enrutador NAT tiene direcciones IP adicionales en el lado externo. La dirección de origen no se modifica.

La dirección adicional se introduce en la tabla NAT en "Inicio > Administración de redes > Gestión de comunicaciones > Biblioteca de objetos > NAT".

Irrestricto

---

## 5 Apéndice

# 5 Apéndice

## 5.1 Servicio y soporte

### Soporte en línea de la industria

¿Tiene alguna pregunta o necesita ayuda?

Siemens Industry Online Support ofrece acceso las 24 horas a todo nuestro servicio, soporte y conocimientos técnicos y cartera.

Industry Online Support es la dirección central para obtener información sobre nuestros productos, soluciones y servicios.

Información de productos, manuales, descargas, preguntas frecuentes, ejemplos de aplicación y vídeos: toda la información está accesible con unos pocos clics del ratón: [support.industry.siemens.com](http://support.industry.siemens.com)

---

### Apoyo técnico

El Soporte técnico de Siemens Industry le brinda un soporte rápido y competente con respecto a todas las consultas técnicas con numerosas ofertas a medida, que van desde soporte básico hasta contratos de soporte individuales.

Envíe sus consultas al Soporte Técnico a través del formulario web:

[support.industry.siemens.com/cs/my/src](http://support.industry.siemens.com/cs/my/src)

### SITRAIN – Academia de la Industria Digital

Le apoyamos con nuestros cursos de formación disponibles en todo el mundo para la industria con experiencia práctica, métodos de aprendizaje innovadores y un concepto que se adapta a las necesidades específicas del cliente.

Para obtener más información sobre nuestras capacitaciones y cursos ofrecidos, así como sus ubicaciones y fechas, consulte nuestra página web:

[siemens.com/sitrain](http://siemens.com/sitrain)

### oferta de servicio

Nuestra gama de servicios incluye lo siguiente:

- Servicios de datos de planta
- Servicios de repuestos
- Servicios de reparación
- Servicios in situ y de mantenimiento
- Servicios de reacondicionamiento y modernización
- Programas y contratos de servicios

Puede encontrar información detallada sobre nuestra gama de servicios en la página web del catálogo de servicios:

[support.industry.siemens.com/cs/sc](http://support.industry.siemens.com/cs/sc)

### Aplicación de soporte en línea de la industria

Recibirá un soporte óptimo esté donde esté con la aplicación "Siemens Industry Online Support". La aplicación está disponible para iOS y Android: [support.industry.siemens.com/cs/ww/en/sc/2067](http://support.industry.siemens.com/cs/ww/en/sc/2067)

---

---

## 5 Apéndice

### 5.2 Enlaces y literatura

Tabla 5-1

No.	Sujeto
\1\	Asistencia en línea de la industria de Siemens <a href="https://support.industry.siemens.com">https://support.industry.siemens.com</a>
\2\	Enlace a la página del artículo del ejemplo de aplicación <a href="https://support.industry.siemens.com/cs/ww/en/view/109762792">https://support.industry.siemens.com/cs/ww/en/view/109762792</a>
\3\	

### 5.3 Cambiar documentación

Tabla 5-2

Versión	Fecha	Cambio
V1.0	12/2020	Primera edición