## SIEMENS

# Configurare firewall su base utente, digital input e time triggered

ноw то



## Contents

Configurare firewall su base utente, digital input e time triggered	3
Premessa	3
Configurazione degli utenti per utilizzo nelle regole di firewall	3
Configurazione regole di firewall con attivazione su base utenti	5
Configurazione regole di firewall con attivazione su base digital input	10
Configurazione di regole di firewall con attivazione su base utente e digital input	13
Configurazione di regole di firewall con attivazione su base durata temporale	15

# Configurare firewall su base utente, digital input e time triggered

#### Premessa

La seguente guida illustra le funzionalità relative ai firewall su base utente, Digital Input e Time Triggered sui modelli Siemens Scalance S e M e come queste possono essere configurate mediante la gestione web (WBM).

Queste funzionalità permettono di inserire delle regole di firewall che possono essere attivate mediante l'inserimento di credenziali (username e password) per un tempo limitato, tramite l'attivazione di un ingresso digitale sullo Scalance o sulla base di una definizione temporale.

La guida è valida per le versioni firmware fino alla 7.1 per Scalance S615/M800 e 2.3 per Scalance SC600. Per l'utilizzo di queste funzionalità si raccomanda l'aggiornamento firmware dei vecchi dispositivi in quanto introdotte di recente.

# Configurazione degli utenti per utilizzo nelle regole di firewall

Per utilizzare la funzionalità User Specific, che consente di abilitare regole di firewall su base utente, occorre prima configurare degli utenti. Questi possono essere creati dal menu Security → Users. Inserire le credenziali (username e password), specificare il ruolo (user = accesso in sola lettura o admin= accesso in lettura e scrittura) e cliccare su "Create".



Una volta creato l'utente, questo va indicato come utente in grado di effettuare l'accesso da remoto. Sotto la voce "Remote Access", selezionare dal menu a tendina il parametro:

- "only" se si intende creare un utente che ha il solo accesso alle regole di firewall
- "additional" se si intende creare un utente che ha accesso sia alle regole di firewall che al WBM dello Scalance

Al termine della scelta, cliccare "Set Values".

	S615 WEB Manageme 🗙	+			$\checkmark$ -
$\leftarrow \   \rightarrow \   G$	▲ Non sicuro	https://192.168.1.1			< ৫☆ \$
SIEMENS	192.168.1.1/	SCALANCE	S615		01/01
Welcome admin	Local Users	omatically in 51 seconds Pr	ess 'Write Startun Confie' to save imm	sdiately	
Logout	Changes will be saved auto		ess white startup comig to save innin		
▶Wizards	Local Users Roles Group	55			
► Information	User Account:				
▶System	Password Policy: Password:	high			
Interfaces	Password Confirmation:				
▶Layer 2	Role:	select User Account	Role	Description	Remote Access
▶Layer 3 (IPv4)		admin	admin	System defined local user	none ~
N aver 3 (IPv6)		Linda	user		none 🗸
▼Security	Create Delete Set Va	2 entries.			additional

**N.B:** anche l'utente di default admin ha la possibilità di essere utilizzato per le regole di firewall ma ovviamente è sempre meglio evitare di diffondere le credenziali amministrative preferendo l'uso di utenze ad hoc.

# Configurazione regole di firewall con attivazione su base utenti

Successivamente in Security → Firewall → Dynamic Rules bisogna creare dei "Rule Set" assegnando un nome identificativo nel campo "Name" e cliccando "Create".



La validità della regola ha un tempo limitato, al default: 30 minuti.

E' possibile modificare la durata sotto la voce "Timeout". A seguito di modifiche, è necessario cliccare su "Set Values".

SCALANCE	S615 WEB Manageme × +
$\leftarrow \   \rightarrow \   G$	△ A Non sicuro   https://192.168.1.1
SIEMENS	192.168.1.1/SCALANCE S615
Welcome admin	Dynamic Rules
Logout	Changes will be saved automatically in 3 seconds Press "Write Startup Config" to save immediately.
▶Wizards	General Predefined Dynamic Rules IP Services ICMP Services IP Protocols IP Rules
► Information	Rule Set
▶System	Name: Select No. Name Comment Timeout (min)
Interfaces	Image     Image     Image       1     RegolaTest     40
▶Laver 2	1 entry.
▶I aver 3 (IPv4)	
▶Laver 3 (IPv6)	Rule Set Assignment
=Socurity	User Account V
<ul> <li>♦Users</li> </ul>	Linda user - None - Force Deactivate
▶Passwords	Create Delete Set Values Refresh
►AAA	
▶Certificates	

Per definire una regola su base utente, nella tabella relativa al Rule Set Assignement, verificare di avere selezionato "User Account" in corrispondenza della voce "Type".

Per l'utente corrispondente alla voce "User Account" assegnare dal menu tendina "Rule Set" la regola definita in precedenza. Cliccare **"Set Values".** 

Così facendo, nel caso specifico in esempio, per l'utente Linda risulterà valida la regola RegolaTest.

SCALANCE	S615 WEB Manageme × +
$\leftarrow \  \  \rightarrow \  \  \mathbf{G}$	▲ Non sicuro   https://192.168.1.1
SIEMENS	192.168.1.1/SCALANCE S615
Welcome admin	Dynamic Rules
Logout	
▶Wizards	General Predefined Dynamic Rules IP Services ICMP Services IP Protocols IP Rules
►Information	Rule Set
▶ System	Select No. Name Comment Timeout [min]
▶ Interfaces	1 RegolaTest 30
▶Layer 2	1 entry.
►Layer 3 (IPv4)	
▶Layer 3 (IPv6)	Rule Set Assignment Type: User Account
✓Security	User Account Role Rule Set Combined Remaining Time Force Deactivate
▶Users	Linda user RegolaTest V None V - Force Deactivate
▶ Passwords	Create Delate Sat Values Refrech RegolaTest
►AAA	

Se sono stati creati più utenti e più regole, prestare attenzione ad effettuare le associazioni corrette, secondo le proprie necessità.

SCALANCE	S615 WEB Manageme × +
$\leftarrow \   \rightarrow \   {\tt G}$	▲ Non sicuro   https://192.168.1.1
SIEMENS	192.168.1.1/SCALANCE S615
Welcome admin	Dynamic Rules
1 and 1	Changes will be saved automatically in 57 seconds.Press 'Write Startup Config' to save immediately
Logour	General Predefined Dynamic Rules IP Services ICMP Services IP Protocols IP Rules
►Wizards	
►Information	Rule Set
▶ Svetom	Name:
P System	Select No. Name Comment Timeout [min]
►Interfaces	2 Regola2 30
▶Layer 2	2 entries.
▶Laver 3 (IPv4)	
· Edjor o (ii vi)	
►Layer 3 (IPv6)	Rule Set Assignment
✓Security	Type: User Account 🗸
▶Users	User Account Role Rule Set Combined Remaining Time Force Deactivate
▶Passwords	Linda user Regola lest V None V - Force Deactivate
►AAA	
▶Certificates	Create Delete Set Values Refresh
Firewall	

Nel Tab "IP Rules" selezionare la regola dal menu a tendina in corrispondenza della voce "Rule Set". Cliccare sul tasto "Create".

SCALANCE	S615 WEB Manageme × +
$\leftarrow \   \rightarrow \   {\tt G}$	▲ Non sicuro   https://192.168.1.1
SIEMENS	192.168.1.1/SCALANCE S615
Welcome admin	Internet Protocol (IP) Rules
<u>Logout</u>	Changes will be saved automatically in 9 seconds.Press 'Write Startup Config' to save immediately
►Wizards	General Predefined Dynamic Rules IP Services ICMP Services IP Protocols IP Rules
►Information	IP Version: IPv4 V
▶System	Rule Set: - v - RepolaTest
▶ Interfaces	Regola2 Action From To Source (Range)
►Layer 2	4
▶Layer 3 (IPv4)	0 entries.
►Layer 3 (IPv6)	Create Delete Refresh
▼Security	
▶Users	

Impostare i campi della tabella a seconda della regola di firewall da implementare (From, To, Source Range, Destination Range, Service). Per una spiegazione dettagliata si rimanda allo specifico manuale.

Successivamente spuntare la casella "Assign to" in modo da assegnare la regola di firewall al Rule Set selezionato. Sotto la voce "Assigned" apparirà il nome del Rule Set al quale la regola di firewall è stata assegnata.

SCALANCE	S615 WEB Managemi × +			~ - 0 >
$\leftarrow \   \rightarrow \   {\tt G}$	▲ Non sicuro   https://192.168.1.1		Q	8 🖈 🖪 😩
SIEMENS				English 🗸 Go
	192.168.1.1/SCALANCE S615			01/01/2000 02:39:53
Welcome admin	Internet Protocol (IP) Rules			
Logout	Changes will be saved automatically in 27 seconds Press Write Startup Config' to save immediately			□?≞★
▶Wizards	General Predefined Dynamic Rules IP Services ICMP Services IP Protocols IP Rules			
Information	IP Version: IPv4 🗸			
▶System	Rule Set: RegolaTest  Show all			
Interfaces	Action From To Source (Range)	Destination (Range)	Service Log Precedence	Assign to Assigned
▶Layer 2	Accept Viant (INT) Vian2 (EXT) VIANIC	192.168.2.33/32	VNC VInone V	Regola lest
►Layer 3 (IPv4)	1 entry.			
►Layer 3 (IPv6)	Create Delete Set Values Refresh			
✓Security ►Users				

Eseguire la stessa operazione per tutte le regole necessarie. Al termine cliccare su "Set Values".

SCALANCE	S615 WEB Manageme 🗙	+							$\sim$	-	0
$\leftarrow \   \rightarrow \   {\tt G}$	▲ Non sicuro	https://192.168	3.1.1					Q	6 \$	*	
SIEMENS										E	inglish 🗸 😡
SIEWIENS	192.168.1.1/5	SCALANC	CE S615							01/01/200	0 03:12:58
Welcome admin	Internet Protocol (IP	) Rules									
Logout	Changes will be saved autor	natically in 57 second	ds.Press "Write Startup	Config' to save immediately							■ <b>?</b> ≞ ★
₩izards	General Predefined Dynam	nic Rules IP Service	ces ICMP Services IP	Protocols IP Rules							
Information	IP Version: IPv4 🗸										
▶System	Rule Set: _	<b>~</b>									
▶Interfaces	Action	From	То	Source (Range)	Destination (Range)	Service	Log F	recedence	Assign to	Assigned	
▶Layer 2	Accept	vlan1 (INT)     vlan1 (INT)	<ul> <li>✓ vlan2 (EXT)</li> <li>✓ vlan2 (EXT)</li> <li>✓</li> </ul>	DYNAMIC DYNAMIC	192.168.2.33/32 192.168.2.20/32	VNC	✓ none ✓ 0 ✓ none ✓ 1			RegolaTe Regola2	st
▶Layer 3 (IPv4)	4			2							•
▶Layer 3 (IPv6)	2 entries. Create Delete Set Value	Refresh		-							

Qualora la stessa regola di firewall venga assegnata a tutti i rule set disponibili, nella colonna "Assigned" compare la voce "all", come riportato in immagine.

Lo stesso accade se è stato definito un solo rule set.

SCALANCE	S615 WEB Managem ( X	+								~ -	- 0	
$\leftarrow \   \rightarrow \   {\tt G}$	▲ Non sicuro	https://192.168.1.1							QB	☆ 🛔	- 🗆 😩	
											English 🗸 🤇	0
SIEWIENS	192.168.1.1/	SCALANCE S	615							01/01	/2000 03:13:53	3
Welcome admin	Internet Protocol (IF	) Rules										
Logout											E ? 占 🕇	3
▶Wizards	General Predefined Dynar	nic Rules IP Services ICM	P Services IP Protocols IP Rules									
Information	IP Version: IPv4 🗸											
▶System	Rule Set: RegolaTest	~										
Interfaces	То	Source (Range)	Destination (Range)	Service	Log	Precedence	Assign to	Assigned		▲Lat	bel	
▶Layer 2	vlan2 (EXT)	DYNAMIC     DYNAMIC	192.168.2.33/32 192.168.2.20/32	VNC	<ul> <li>none</li> <li>none</li> </ul>	✓ 0 ✓ 1		RegolaTest all		•		
▶Laver 3 (IPv4)	4										÷	
▶Layer 3 (IPv6)	2 entries.	es Refresh						2				
▼Security	Service Service											

Il campo "Source(Range)", se precedentemente impostato a 0.0.0.0/0, assume valore DYNAMIC. Questo significa che il "Source(Range)" corrisponde all'indirizzo IP del device da cui l'utente si collega.

Per utilizzare le regole di firewall, l'utente dovrà prima accedere alla pagina web del firewall scegliendo "switch to firewall login"

SCALANCE	S615 WEB Manageme × +
$\leftrightarrow$ $\rightarrow$ G	△ A Non sicuro   https://192.168.1.1
SIEMENS	
Name Password Login	
	LOGIN Name: Password:
	Login Switch to firewall login 년까 For information about browser compatibility please refer to the manual

SCALANCE	S615 WEB Manageme 🗙	+			
$\leftarrow \   \rightarrow \   G$	▲ Non sicuro	https://192.168.1.1			
SIEMENS					
Name Password Login					
			<b>F</b> I F Nar Pas	REWALL	
			<u>Swi</u> For information	witch to login n about browser compatibility please refer to the manual	
				₹J	

Nella pagina che si apre, inserire le credenziali dell'utente e cliccare su login.

A questo punto la regola funzionerà per il timeout impostato.

SCALANCE	S615 WEB Manageme × +
$\leftarrow \   \rightarrow \   G$	▲ Non sicuro   https://192.168.1.1/#
SIEMENS	192.168.1.1/SCALANCE S615
Welcome Linda <u>Logout</u>	Dynamic Firewall Rules Information
	Firewall Ruleset "RegolaTest" activated. Expires in 00h 39m 48s Reset Timeout Refresh

Se si vuole rinnovare il tempo di utilizzo della regola, è possibile resettare il timeout. In questo modo l'utente otterrà nuovamente il tempo iniziale per l'utilizzo della regola.

### Configurazione regole di firewall con attivazione su base digital input

Per definire delle regole di firewall attivabili sulla base di un ingresso digitale, procedere in Security → Firewall → Dynamic Rules e creare il "Rule Set" assegnando un nome identificativo nel campo "Name" e cliccando "Create". Modificare l'eventuale tempo di Timeout, come spiegato nel capitolo precedente.

Una volta creato il rule set, nella tabella relativa al "Rule Set Assignment", selezionare "Digital Input" dal menu a tendina in corrispondenza della voce "Type".

	SCALANCE S615 WEB Manageme X				+
$\leftarrow$	$\rightarrow$	C	合	A Non sicuro	https://192.168.1.1

#### SIEMENS

SIEWIENS	192	168	1 1/9		E \$615					
	102.	. 100	. 1. 1/C							
Welcome admin	Dynan	n <mark>ic Ru</mark>	les							
	Changes	will be s	aved autom	atically in 56 seconds	Press 'Write Start	up (	<u>Config' to save im</u>	mec	liately	
Logout						1.1.5				
▶ Wizards	General	Predefin	ed Dynami	ic Rules IP Services	ICMP Services	IP	Protocols IP Ru	lles		
, mzaras										
►Information		Rule Se	t							
1 Custom	Name:									
▶ System		Select	No.	Name	Comment			Ti	meout [min]	
▶Interfaces			1	RegolaTest				4(	)	
			2	Regola2				30	)	
►Layer 2			3	RegolaDI				30	)	
N avor 3 (IDv/I)		3 entries	S.							
►Layer 3 (IPv6)										
		Rule Se	t Assignmer	nt						
Security	Type:	User Ar	ccount 🗸							
▶Users		User Ac	ccount	Role	Rule Set		Combined		Remaining Time	Force Deactivate
▶Passwords			S role	user	RegolaTest	~	None	~	-	Force Deactivate
►AAA		RADIU	S user	user	Regola2	~	None	~	-	Force Deactivate
▶Certificates		Time tri	iggered							
▶Firewall	Create	Delete	Set Value	s Refresh						
▶IPsec VPN										

A questo punto assegno il Rule Set al Digital Input selezionando la regola dal menu a tendina in corrispondenza della colonna "Rule Set".

SCALANCE SE	515 WEB Manageme × +
$\leftrightarrow$ $\rightarrow$ C $\alpha$	▲ Non sicuro   https://192.168.1.10
SIEMENS	192.168.1.10/SCALANCE S615
Welcome admin	Dynamic Rules Changes will be saved automatically in 15 seconds.Press 'Write Startup Config' to save immediately
►Wizards	General Predefined Dynamic Rules IP Services ICMP Services IP Protocols IP Rules
►Information	Rule Set Name:
▶System	Select No. Name Comment Timeout [min]
▶ Interfaces	1 RegolaTest 40
	2 Regola2 30
▶Layer 2	3 RegolaDI 30
▶Layer 3 (IPv4)	3 entries.
▶Layer 3 (IPv6)	
-Socurity	Rule Set Assignment
◆Security	Type: Digital Input 🗸
▶ Osers	Digital Input Rule Set Dynamic Source (Range) Status
▶ Passwords	1 RegolaDI V 192.168.1.55/32 disabled
AAA	- RenolaTest
▶ Certificates	Create Delete Set Values Regola2
▶Firewall	RegolaDI
▶IPsec VPN	N N

E' possibile specificare gli indirizzi IP autorizzati all'attivazione del digital input, inserendoli nel campo "Dynamic Source (Range)".

Al termine della configurazione, cliccare "Set Values".

Nella colonna "Status" è possibile verificare l'attivazione della regola (disabled/enabled).

Il resto della configurazione è del tutto similare al firewall su base utente.

Procede nel tab **"IP Rules"**. Selezionare la regola corrispondente nel menu a tendina "Rule Set" e cliccare su **"Create"**. Dopo aver definito i campi della regola, inserire la spunta in corrispondenza della colonna "Assign to". Cliccare su **"Set Values**".

SCALANCE	S615 WEB Manageme × +					$\checkmark$	- 0 ×
$\leftrightarrow$ $\rightarrow$ G	△ A Non sicuro   https://192.168.1.1					익 년 ☆	* 🖬 😩 🗄
SIEMENS							English 🗸 😡
SILINEIUS	192.168.1.1/SCALANCE S	615					01/01/2000 03:32:24
Welcome admin	Internet Protocol (IP) Rules						
Logout							<b>□ ?</b> ≞ ★
▶Wizards	General Predefined Dynamic Rules IP Services ICM	P Services IP Protocols IP Rules					
►Information	IP Version: IPv4 V						
▶System	Rule Set: RegolaDI						
Interfaces	Action From To	Source (Range)	Destination (Range)	Service	Log Prece	dence Assign to	Assigned
▶Layer 2	Accept Vian1 (INT) Vian2	2 (EXT) V DYNAMIC	192.168.2.33/32	VNC ~	none V 0		RegolaTest Regola2
▶Layer 3 (IPv4)	Accept Vian1 (INT) Vian2	2 (EXT) V DYNAMIC	0.0.0.0/0	all	none V 2		RegolaDI
►Layer 3 (IPv6)	3 entries.				a contraction of the second se		
-Security	Create Delete Set Values Refresh						

Se il "Source(Range)" era stato definito con 0.0.0/0, questo valore viene sostituito dalla voce DYNAMIC e vale quanto specificato in tabella "Rule Set Assignment", come mostrato in precedenza.

Questa regola viene attivata esclusivamente quando viene fornita tensione all'ingresso digitale disponibile sul dispositivo. E' possibile verificare lo status dell'ingresso digitale dal WBM cliccando sul tasto indicato dalla manina nell'immagine qui sotto. Se il quadratino in corrispondenza della dicitura DI è verde, significa che l'ingresso riceve tensione.



In alternativa è possibile impostare nel menu System → Events la spunta sulla colonna "Digital Out" in corrispondenza della riga "Digital In". Al termine della configurazione cliccare "Set Values".

In questo modo viene restituito un feedback sottoforma di tensione sui morsetti del DO. La stessa informazione è disponibile sul led DO del dispositivo.

SCALANCE S6	15 WEB Manageme × +								~ -	- 0	×
$\leftrightarrow$ $\rightarrow$ C (	A Non sicuro   http://www.sicuro	<del>s</del> ://192.168.1.10						E	2 🖈 🖠		:
SIEMENS									Er	glish 🗸 <u>Go</u>	
	192.168.1.10/	SCALANCE S615							01/01/2000	01:13:01 🔁	
Welcome admin	<b>Event Configuration</b>										
Logout									t	• ? = *	
and grows	Configuration Severity Filter	rs									
▶ vvizards											
► Information	Log Table Alarm Threshold:	: 350								Cloud	
-System			E-mail	Trap	Log Table	Syslog	Fault	Digital Out	VPN Tunnel	Cioud	
► Configuration		All Events	No Change 🗸	No Change	✓ No Cha	n					
▶General		<								)	÷
▶Restart											
▶Load&Save		Event	E-mail	Тгар	Log Table	Syslog	Fault	Digital Out	VPN Tunnel	Cloud Connect	0
►Events		O al d Marra Ohart			-						
▶SMTP Client		Cold/Warm Start			✓						
		Link Change									
▶SNMP		Link Change Authentication Failure									
►SNMP►System Time		Link Change Authentication Failure Fault State Change									
▶SNMP ▶System Time ▶Auto Logout		Cold/Warm Start Link Change Authentication Failure Fault State Change Security Logs									
<ul> <li>SNMP</li> <li>System Time</li> <li>Auto Logout</li> <li>Button</li> </ul>		Colorivarm Start Link Change Authentication Failure Fault State Change Security Logs Firewall Logs									
<ul> <li>►SNMP</li> <li>►System Time</li> <li>►Auto Logout</li> <li>►Button</li> <li>►Syslog Client</li> </ul>		Colorivarm Start Link Change Authentication Failure Fault State Change Security Logs Firewail Logs DDNS Client Logs									
SNMP System Time Auto Logout Button Syslog Client Fault		Colorivarm Start Link Change Authentication Failure Fault State Change Security Logs Firewail Logs DDNS Client Logs System General Logs System Generation Status									
SNMP System Time Auto Logout Button Syslog Client Fault Monitoring		Colorivarm Start Link Change Authentication Failure Fault State Change Security Logs Firewall Logs DDNS Client Logs System General Logs System Connection Status Diotata in									
SNMP System Time Auto Logout Button Syslog Client Fault Monitoring PLUG		Colorivarm Start Link Change Authentication Failure Fault State Change Security Logs Firewall Logs DDNS Client Logs System General Logs System Connection Status Digital in VPN Tunnel								C	
SNMP     System Time     Auto Logout     Button     Syslog Client     Fault     Monitoring     PLUG     Ping		Colorivarm Start Link Change Authentication Failure Fault State Change Security Logs Firewall Logs DDNS Client Logs System General Logs System Connection Status Digital in VPN Tunnel Secure NTP									
SNMP     SNMP     System Time     Auto Logout     Button     Syslog Client     Fault     Monitoring     PLUG     Pling     DCP Discovery		Colorivarm Start Link Change Authentication Failure Fault State Change Security Logs Firewail Logs DDNS Client Logs System General Logs System Connection Status Digital in VPN Tunnel Secure NTP									-
SNMP     System Time     Auto Logout     Button     Syslog Cilent     Fault     Monitoring     PLUG     Plug     DCP Discovery     DNS		Colorivarm Start Link Change Authentication Failure Fault State Change Security Logs Firewail Logs DDNS Client Logs System General Logs System Connection Status Digital In VPN Tunnel Secure NTP									

## Configurazione di regole di firewall con attivazione su base utente e digital input

E' possibile definire delle regole di firewall attivabili solo se contemporaneamente soddisfatti i requisiti di un corretto login da parte di un utente e di attivazione di un ingresso digitale.

Per configurare questa opzione, riprendere passo-passo le istruzioni riportate nel paragrafo "Configurazione regole di firewall con attivazione su base utenti" trattato in precedenza, dopo aver correttamente definito gli utenti (vedi paragrafo: "Configurazione degli utenti per utilizzo nelle regole di firewall").

Oltre ai passaggi precedentemente descritti, selezionare dal menu a tendina in corrispondenza della colonna "Combined" la voce **"Digital Input"** per quei rule set per i quali entrambi i criteri, utente e digital input, devono essere soddisfatti contemporaneamente per l'attivazione della regola. Cliccare su **"Set Values"**.



Per l'attivazione della regola, procedere sulla pagina del WBM e cliccare su "switch to firewall login", come già indicato in precedenza.

Inserire le credenziali corrette.

Se l'ingresso digitale non è alimentato mentre viene effettuato il login, viene generato un messaggio "Invalid username/password".

SCALANCE SE	15 WEB Managem E 🗙 🕂			$\vee$	-		$\times$
$\leftrightarrow$ $\rightarrow$ C f	Non sicuro   https://192.168.1.1	0/#	È	☆	* 0		÷
SIEMENS					Englis	sh ∨ G	٥
Name Password Login	Errort					? -	5
	Invalid user	name/password					
	Nar	ne: Linda					
		k La	<u>ogin</u>				
	Swi	to login					
	For information	about browser compatibility please refe	er to the ma	nual			

L'attivazione della regola avviene correttamente quando entrambi i requisiti vengono verificati, utente e ingresso digitale!

E' quindi opportuno procedere con il login sul firewall garantendo la tensione sui morsetti dell'ingresso digitale.



### Configurazione di regole di firewall con attivazione su base durata temporale

Per definire delle regole di firewall attivabili su base temporale procedere in primo luogo con la sincronizzazione dell'orario del dispositivo. Questo è un prerequisito fondamentale per la corretta attivazione delle regole. Procedere dal menu System → System Time.

E' possibile assegnare il tempo del PC al dispositivo cliccando su "Use PC Time" e poi applicare le modifiche cliccando su "Set Values".

Questa scelta, seppur pratica, non è l'ottimale. Per ulteriori dettagli, consultare la guida dedicata.



Dopo aver correttamente impostato il tempo del dispositivo, procedere alla creazione del rule set, come visto in precedenza.

Accedere al menu Security → Firewall → Dynamic Rules.

Inserire un nome identificativo in corrispondenza del campo "Name" e cliccare su "Create".

SCALANCE S615 WEB Manageme × +											
$\leftrightarrow$ $\rightarrow$ C (	Non sicuro   h	ttps://192.168.1.10									
SIEMENS	SIEMENS 192.168.1.10/SCALANCE S615										
Welcome admin	Dynamic Rules Changes will be saved au	omatically in 45 secor	nds.Press 'Write Startup C	Config' to save immed	<u>liately</u>						
▶Wizards	General Predefined Dyn	amic Rules IP Servi	ces ICMP Services IP	Protocols IP Rules							
▶ Information	Rule Set Name: RegolaTempora	e)									
▶System	Select No.	Name RegolaTest	Comment	Ti 4	meout [min] D						
►Layer 2	2 3	Regola2 RegolaDI		31	0						
▶Layer 3 (IPv4)	3 entries.										
▶Layer 3 (IPv6)											
-Security	Rule Set Assign	ment									
▶Users	Liser Account	Role	Rule Set	Combined	Remaining Time	Force Deactivate					
▶Passwords	Linda	user	RegolaTest V	Digital Input V	-	Force Deactivate					
►AAA	Utente	user	Regola2 V	None ~	]-	Force Deactivate					
▶ Certificates											
Firewall	Create Delete Set Va	Refresh									
▶IPsec VPN	13										

Selezionare la voce "Time Triggered" dal menu "Type" in corrispondenza della tabella "Rule Set Assignment".

SCALANCE SE	15 WEB Managem 🗧 🗙	+				
$\leftrightarrow$ $\rightarrow$ C $\epsilon$	A Non sicure	https://192.168.1.10				
SIEMENS	192.168.1	.10/SCALAN	ICE S615			
Welcome admin	Dynamic Rules Changes will be save	automatically in 55 secon	ds.Press 'Write Startup C	<u>onfig' to save immedi</u>	iately	
▶ Wizards	General Predefined	Dynamic Rules IP Servio	ces ICMP Services IP F	Protocols IP Rules		
►Information	Rule Set Name:					
▶System	Select N	o. Name	Comment	Tin	neout [min]	
Interfaces	1	RegolaTest		40		
▶Layer 2		RegolaDI		30		
▶Layer 3 (IPv4)	4 entries.	RegolaTemporale		30		
▶Layer 3 (IPv6)						
-Security	Rule Set A	signment				
▶Users	Type: User Acco					
▶ Passwords	User Acco	unt Role	Rule Set	Combined	Remaining Time	Force Deactivate
►AAA	Digital Inp	ut user	RegolaTest V	Digital Input	-	Force Deactivate
▶ Certificates	RADIUS	ser user	Regola2 V	None V	-	Force Deactivate
▶Firewall	Time trigg	ered				
▶IPsec VPN	Create Delete	Set Values Refresh				

E' possibile definire fino a tre regole temporali differenti andando a personalizzare le righe della tabella. I trigger temporali possono essere eseguiti su base giornaliera, settimanale o mensile: specificare con il menu a tendina in corrispondenza della colonna "Cycle" la ripetizione del trigger temporale.

• Selezionando "Daily", l'intervallo temporale viene definito per ogni giorno

- Selezionando "Weekly", l'intervallo temporale viene definito per i giorni della settimana specificati in corrispondenza della colonna "Days". Possono essere assegnati valori da 1 a 7, dove 1 indica il lunedì e 7 la domenica. Per una selezione di più giorni, intervallare i valori numerici con una virgola.
- Selezionando "Monthly", l'intervallo temporale viene definito per i giorni del mese specificati in corrispondenza della colonna "Days". Possono essere assegnati valori da 1 a 31. Per una selezione di più giorni, intervallare i valori numerici con una virgola.

In corrispondenza delle colonne "Start Time" ed "End Time" specificare rispettivamente l'orario di inizio e di fine dell'intervallo temporale in questione.

Nel caso riportato in immagine, la riga 1 della tabella definisce l'intervallo di tempo che va dalle 7:59 alle 18 di ogni giorno, la riga 2 definisce l'intervallo di tempo che va dalle 11 alle 14:30 dei giorni lunedì e martedì della settimana, la riga 3 definisce l'intervallo di tempo che va dalle 13 alle 17:00 dei giorni 7, 14 e 21 del mese.

SCALANCE SE	515 WEB Managem  K	+								~ -	
$\leftrightarrow$ $\rightarrow$ C f	♪ 🔺 Non sicuro   ŧ	https://192.168.1.10						Ê	☆	<b>*</b> ≡	
SIEMENS 192.168.1.10/SCALANCE S615											
Welcome admin	Dynamic Rules										
Logout											
▶ Wizards	General Predefined Dyn	namic Rules IP Servi	ces ICMP Services	IP Protocols IP R	ules						
> Information	Rule Set										
Finiomation	Name:										
▶System	Select No.	Name	Comment		Timeout [min]						
Interfaces	1	RegolaTest			40						
	2	Regola2			30						
▶Layer 2	3	RegolaDI			30						
Naver 3 (IPv4)	4	RegolaTemporale			30						
PLayer 0 (II V+)	4 entries.										
►Layer 3 (IPv6)											
Coourity											
◆Security	Rule Set Assign	nment									
▶ Users	Type: Time triggered	~									
▶Passwords	Time triggered	Rule Set	Combined	Cycle	Days	Dynamic Source (Range)	Start Time	End Time	Acti	vate	
►AAA	1	- ~	None 🗸	Daily 🗸		0.0.0/0	07:59	18:00			
▶Certificates	2	- ~	None 🗸	Weekly 🗸	1,2	0.0.0/0	11:00	14:30			
▶Firewall	3	- ~	None 🗸	Monthly ~	7,14,21	0.0.0/0	13:00	17:00			
▶IPsec VPN				Daily							
▶OpenVPN	Create Delete Set V	alues Refresh		Monthly							
				ar ar							

Assegnare la riga di interesse al rule set precedentemente creato selezionandolo dal menu a tendina in corrispondenza della colonna "Rule Set".

Cliccare "Set Values".

SCALANCE S615 WEB Manageme × +												
$\leftrightarrow$ $\rightarrow$ C (	Non sicuro   h	<del>ttps</del> ://192.168.1.10						L#	2 1	*	⊧≡ſ	
SIEMENS 192.168.1.10/SCALANCE S615 06/21/2022												Englis 22 18
Welcome admin Logout	Dynamic Rules Changes will be saved automatically in 57 seconds.Press "Write Startup Config" to save immediately											
▶Wizards	General Predefined Dyn	amic Rules IP Servi	ces ICMP Services	IP Protocols IP R	ules							
►Information	Rule Set											
▶System	Name: Select No.	Name	Comment		Timeout [min]							
▶ Interfaces		RegolaTest			40							
▶Layer 2		RegolaDI			30							
▶Layer 3 (IPv4)	4	RegolaTemporale	•		30							
▶Laver 3 (IPv6)	4 entries.											
Security ▶Users	Rule Set Assign	ment										
▶ Passwords	Type: Time triggered	×	0	0	5		01-17-1					
►AAA	Time triggered	Rule Set	Combined	Cycle	Days	Dynamic Source (Range)	Start Time	End Time		Activate	e	
▶Certificates	2	-	None ¥	Weekly Y	1.2	0.0.0.0/0	11:00	14:30				
Firewall	3	RegolaTest	None ~	Monthly ~	7,14,21	0.0.0/0	13:00	17:00				
▶IPsec VPN		RegolaDI		· · · · ·	ar 1							
▶OpenVPN	Create Delete Set V	RegolaTemporale										

N.B: Per poter correttamente utilizzare la regola definita è necessario abilitare la spunta in corrispondenza della colonna "Activate"! e cliccare "Set Values".

I campi della riga attivata assumeranno colore giallo e non potranno essere modificati se non disabilitando la spunta.

SCALANCE SE	15 WEB Ma	anageme X	+								$\vee$	-
$\leftrightarrow$ $\rightarrow$ C f		Non sicuro   Ħ	1001101102.168.1.10	)					E	2 2		⊧ ≡J
SIEMENS	192.	.168.1.1	0/SCALAI	NCE S61	ō						06	E 6/21/2022
Welcome admin Logout	Dynamic Rules     Changes will be saved automatically in 55 seconds.Press 'Write Startup Config' to save immediately											
▶Wizards	General I	Predefined Dyr	namic Rules IP Serv	vices ICMP Service	IP Protocols IP F	Rules						
►Information		Rule Set										
▶System	Name:	Select No.	Name	Comment		Timeout [min]						
▶ Interfaces			RegolaTest			40						
▶Layer 2		3	RegolaDI			30						
Laves 2 (IDu4)		4	RegolaTempora	le		30						
PLayer 5 (IFV4)		4 entries.										
►Layer 3 (IPv6)												
-Security		Pulo Set Accion	mont									
▶Users	Type:	Time triggered										
▶Passwords		Time triggered	Rule Set	Combined	Cycle	Davs	Dynamic Source (Range)	Start Time	End Time		Activat	P
►AAA		1	RegolaTemporal V	None	Daily V	Dayo	0.0.0.0/0	07:59	18:00			
▶Certificates		2	- ~	None	• Weekly ~	1,2	0.0.0.0/0	11:00	14:30			J
▶Firewall		3	- ~	None N	Monthly ~	7,14,21	0.0.0/0	13:00	17:00			
▶IPsec VPN	-											
▶OpenVPN	Create	Delete Set V	Refresh									

E' possibile specificare gli indirizzi IP autorizzati per la comunicazione quando la regola viene attivata, inserendoli nel campo "Dynamic Source (Range)".

E' altresì possibile combinare l'utilizzo delle regole su base temporale con quelle legate all'attivazione dell'ingresso digitale.

Per creare una regola che richieda il verificarsi contemporaneo di queste due condizioni, selezionare dal menu a tendina in corrispondenza della colonna **"Combined"** la voce **"Digital Input**". Al termine della configurazione, cliccare **"Set Values".** 

SCALANCE SE	515 WEB M	anageme ×	+							$\sim$	-	
$\leftrightarrow$ $\rightarrow$ C $\epsilon$	<u>ک</u>	Non sicuro   h	ttps://192.168.1.10						Ê	☆	<b>*</b> =	
SIEMENS	192	.168.1.1	0/SCALAN	ICE S615	)					(	06/21/20	
Welcome admin	Dynar	nic Rules										
Logout												
▶ Wizards	General	Predefined Dyn	amic Rules IP Servi	ces ICMP Services	IP Protocols IP R	ules						
► Information		Rule Set										
Finiornation	Name	Name:										
▶ System		Select No.	Name	Comment		Timeout [min]						
▶Interfaces		1	RegolaTest			40						
		2	Regola2			30						
▶Layer 2		3	RegolaDI			30						
N aver 3 (IPv4)		4	RegolaTemporale	•		30						
PLayer o (II V+)		4 entries.										
►Layer 3 (IPv6)												
-Security		Dulo Cot Accian	mont									
▶Users	Tuno	Time triggered	ment									
▶ Passwords	Type	Time triggered	<b>~</b>									
۲۵۵		Time triggered	Rule Set	Combined	Cycle	Days	Dynamic Source (Range)	Start Time	End Time	Activa	ate	
► Certificates		1	Regola lempora V	None V	Daily V	1.0	0.0.0/0	07:59	18:00			
Foertinoates		2	Regola lempora V	None V	Vveekiy V	7.14.01	192.108.1.55/32	11:00	14:30		4	
Firewall		5	- *	Digital Input	wonuny V	1,14,21	0.0.0.0/0	13.00	17.00			
▶IPsec VPN	Creat	e Delete Set V	alues Refresh	2								
▶OpenVPN	S. State	2011										

Il resto della configurazione è del tutto similare a quanto riportato per i casi precedenti. Procede nel tab **"IP Rules"**. Selezionare la regola corrispondente nel menu a tendina "Rule Set" e cliccare su **"Create"**. Dopo aver definito i campi della regola, inserire la spunta in corrispondenza della colonna "Assign to". Cliccare su **"Set Values"**.

SCALANCE S6	515 WEB Managem 🤄 🗙	+							$\sim$	-	٥	>
$\leftarrow \rightarrow$ C $\triangle$ Non sicuro   https://192.168.1.10									₽ ☆	<b>a</b> ≡r		1
SIEMENS 192.168.1.10/SCALANCE S615 06/21/2022 18:53:1											inglish ∨ 2 18:53:1	] <u>Go</u> 8@
Welcome admin	Internet Protocol (IP) Rules Changes will be saved automatically in 9 seconds Press Write Startup Config' to save immediately Canaral Prodefined Dunamic Pulse   IP Services   ICMP Services   IP Protocols   IP Pulse											
▶Wizards	General Predenned D	ynamic Rules   IF Sei	VICES ICIMIF SELVICES	IF FIOLOCOIS IF Rules								
<ul><li>► Information</li><li>► System</li></ul>	IP Version: IPV4 V Rule Set: RegolaTempoi V											
Interfaces		То	Source (Range)	Destination (Rang	e) Servio	ce I	_og	Precedence	Assign to	Assigne	d	
▶Layer 2	(INT)   (INT)	Vlan2 (EXT) Vlan2 (EXT) Vlan2 (EXT)	DYNAMIC     DYNAMIC	192.168.2.33/32 192.168.2.20/32		× •	none V	0		Regola <sup>1</sup> Regola <sup>1</sup>	ïest lest, Rego	ola2
▶Layer 3 (IPv4)		Vian2 (EXT)		192.108.2.00/32	all	~	none V	3		Regola	JI Temnorale	4
▶Layer 3 (IPv6)	4			102.100.2.11102	an		none -			rtegola	omporaio	•
<ul> <li>Security</li> <li>▶Users</li> <li>▶Passwords</li> </ul>	4 entries.	Values Refresh										

La regola viene attivata automaticamente al verificarsi delle condizioni temporali specificate.

Con riserva di modifiche e salvo errori.

Il presente documento contiene solo descrizioni generali o informazioni su caratteristiche non sempre applicabili, nella forma descritta, al caso concreto o che possono cambiare a seguito di un ulteriore sviluppo dei prodotti. Le caratteristiche desiderate sono vincolanti solo se espressamente concordate all'atto di stipula del contratto.

Tutte le denominazioni dei prodotti possono essere marchi oppure denominazioni di prodotti della Siemens AG o di altre ditte fornitrici, il cui utilizzo da parte di terzi per propri scopi può violare il diritto dei proprietari.