



ноw то

# Configurazione di base del firewall

#### Contents

Configurazione di base del firewall	3
Premessa	3
Attivazione del Firewall e parametrizzazione di default	3
Creazione di regole di comunicazione IP	5
Creazione di servizi basati su porte TCP/UDP	8
Creazione di servizi basati su ICMP	10
Servizi predefiniti su Scalance S/M	11
Configurazione automatica del firewall da Sinema RC	12
Configurazione automatica del firewall per regole di NAT	13

## Configurazione di base del firewall

#### Premessa

La seguente guida illustra le funzionalità relative ai firewall dei modelli Siemens Scalance S e M e come queste possono essere configurate mediante la gestione web (WBM)

La guida è valida per le versioni firmware fino alla 7.1 per Scalance S615/M800 e 2.3 per Scalance SC600.

Per funzionalità aggiuntive quali firewall bridge (solo Scalance SC600), regole di firewall su base utente, digital input o trigger temporale così come altre informazioni di base relative agli Scalance, fare riferimento alle guide apposite.

### Attivazione del Firewall e parametrizzazione di default

Gli Scalance S/M sono dotati di firewall Stateful Inspection su base L3/L4 (L2 disponibile solo per Scalance SC-600, vedere guida specifica) abilitato di default.

Questo significa che fra le diverse interfacce (es: VLAN1 e VLAN2 per lo Scalance S615) non è possibile comunicare alcun tipo di dato senza una configurazione del firewall che lo permetta.

Il firewall funziona con la politica di Whitelist (tutto è proibito, fuorché ciò che è permesso) e si gestisce dalla schermata Security/Firewall nella pagina web del dispositivo.

	192.168.1.1/SCALANCE S615
Welcome admin	Firewall General
Logout	Changes will be saved automatically in 23 seconds.Press 'Write Startup Config' to save immediately
Logout	General Predefined Dynamic Rules IP Services ICMP Services IP Protocols IP Rules
▶Wizards	
▶ Information	✓ Activate Firewall
	TCP Idle Timeout [s]: 86400
▶ System	UDP Idle Timeout [s]: 300
▶ Interfaces	ICMP Idle Timeout [s]: 300
▶Layer 2	
▶Layer 3 (IPv4)	Set Values Refresh
▶Layer 3 (IPv6)	
-Security	
▶Users	
▶Passwords	
►AAA	
▶Certificates	
►Firewall	

#### SIEMENS

È possibile, disabilitando la spunta nel tab "General", disattivare il firewall e permettere qualsiasi tipo di comunicazione fra le interfacce, se necessario. Questa disabilitazione del firewall è fortemente sconsigliata!

In fase di prima configurazione non sono inserite regole, di conseguenza nessuna comunicazione è permessa a firewall attivo.

SCALANCE S	615 WEB Manageme × +							$\sim$		٥	×	-
$\leftrightarrow$ $\rightarrow$ C .	△ A Non sicuro   https://192.16	8.1.1					Ŕ	☆	*	•	•	
SIEMENS	192.168.1.1/SCAL/	ANCE S615						01/0	En	glish ~	<u>60</u> 01 <b>%</b>	
Welcome admin	Internet Protocol (IP) Rules											
Logout									C	□? -	; <b>*</b>	
▶ Wizards	General Predefined Dynamic Rules IF	Services ICMP Services	IP Protocols IP R	ules								
<ul> <li>Information</li> <li>&gt;System</li> </ul>	IP Version: IPv4 V Rule Set: V Show all											
Interfaces	Select Protocol Act	ion From	То	Source (Range)		Destination (Range)	Service	Lo	g	Pre	ced	
▶Layer 2	4 4 0 entries.										*	
<ul> <li>Layer 3 (IPv6)</li> </ul>	Create Delete Refresh											
-Security												
▶ Users												
▶Passwords					3							
►AAA												
Certificates												
FileWall												

#### Creazione di regole di comunicazione IP

Le regole di comunicazione vanno inserite nella tab "IP Rules". Per inserire la prima regola bisogna cliccare su "Create".

SCALANCE S6	15 WEB Managem∈ ×	+			
$\leftrightarrow$ $\rightarrow$ C (	A Non sicuro   h	<del>ttps</del> ://192.168.1.1			
SIEMENS	192.168.1.1	/SCALANCE	S615		
Welcome admin	Internet Protocol (	IP) Rules			
Logout					
▶Wizards	General Predefined Dyn	amic Rules IP Services	ICMP Services IP	Protocols IP Rules	
▶ Information	IP Version: IPv4 🗸				
▶System	Rule Set: -	~			
►Interfaces	Select Pro	otocol Action	From	То	Source (Range)
▶Layer 2	4				
▶Layer 3 (IPv4)	0 entries.				
▶Layer 3 (IPv6)	Create Delete Refre	esh			
-Security					

Viene quindi inserita automaticamente una regola dummy di default che può essere poi modificata

SCALANCE S6	515 WEB Manageme × +						~ -	Ð	
$\leftrightarrow$ $\rightarrow$ C (	▲ Non sicuro   https://	92.168.1.1				Ê	☆ 🗯		
SIEMENS							[	English 🗸	<u>30</u>
	192.168.1.1/SC	ALANCE S615					01/01/20	00 00:07:35 <sup>¢</sup>	23
Welcome admin Logout	Internet Protocol (IP) Ru Changes will be saved automatica	Iles Illy in 55 seconds.Press 'Write Star	tup Config' to save ir	nmediately				<b>?</b> .	
▶Wizards	General Predefined Dynamic R	ules IP Services ICMP Services	IP Protocols IP F	Rules					
►Information	IP Version: IPv4 V								
▶System	show all								
►Interfaces	Select Protocol	Action From	То	Source (Range)	Destination (Range)	Service	Log	Prece	d
▶Layer 2	IPv4	Drop V vlan1 (INT) Drop	✓ vlan1 (INT)	▶ 0.0.0.0/0	0.0.0/0	all	✓ none	✓ 0	
▶Layer 3 (IPv4)	1 entry.	Reject							
▶Layer 3 (IPv6)	Create Delete Set Values I	Refresh							

Per creare una regola di comunicazione in genere si seleziona l'Action su "Accept", dopodiché si modificano gli altri parametri per realizzare la comunicazione desiderata.

Selezionando le interfacce in corrispondenza delle voci "From" e "To", è possibile definire fra quali di queste stabilire le regole di comunicazione.



#### SIEMENS

#### 192.168.1.1/SCALANCE S615

Welcome admin	Intern	Internet Protocol (IP) Rules							
Logout									
▶Wizards	General	Predefined	Dynamic Rules	IP Services	ICMP Services	IP Protocols	IP Rules		
▶ Information	IP Ver	sion: IPv4 🗸	•						
▶System	Rule	Set: _	✓						
▶ Interfaces		Select	Protocol /	Action	From	То		Source (Range)	Destir
▶Layer 2		•	IPv4	Drop 🗸	<ul> <li>vlan1 (INT)</li> <li>vlan1 (INT)</li> <li>vlan2 (EXT)</li> </ul>	✓ vlan1 (I	NT) 🗸	0.0.0.0/0	0.0.0.
▶Layer 3 (IPv4)		1 entry.			ppp2	45			
▶Layer 3 (IPv6)	Creat	e Delete S	et Values Refre	sh	Device OpenVPN (all) SINEMA RC				
-Security					IPsec (all)				
▶Users									

**N.B.:** oltre alle VLAN/Subnet **è possibile utilizzare anche la stessa interfaccia del device, le interfacce mobili** su Scalance M(usb0) **e le interfacce VPN** come "SINEMA RC" per filtrare il traffico in entrata e in uscita dalla VPN. In questo ultimo caso, occorre però disabilitare l'auto firewall (vedere capitolo successivo relativo all'argomento).

Ad esempio, se si vuole permettere qualsiasi trasmissione (accesso web, ping...) dalla rete esterna verso il device è necessario stabilire una regola dalla VLAN 2 al "Device".

SCALANCE SE	515 WEB Manageme × +	
$\leftrightarrow$ $\rightarrow$ C $\epsilon$	△ A Non sicuro   https://192.168.1.1	
SIEMENS		
	192.168.1.1/SCALANCE 5615	
Welcome admin	Internet Protocol (IP) Rules	
Logout		
▶Wizards	General Predefined Dynamic Rules IP Services ICMP Services IP Protocols IP Rules	
▶Information	IP Version: IPv4 V	
▶System	Rule Set:	
Interfaces	Select Protocol Action From To Source (Range)	Destination (Range)
▶Layer 2	IPv4 Accept vlan2 (EXT) Device 0.0.0.0/0	0.0.0.0/0
▶Layer 3 (IPv4)	1 entry.	
▶Layer 3 (IPv6)	Create Delete Set Values Refresh	
Security		

Sul campo "Source (Range)" e "Destination (Range)" è invece possibile restringere il campo degli indirizzi che possono comunicare fra le 2 interfacce utilizzando la notazione CIDR (ad esempio /32 per definire un singolo indirizzo o /24 per definire una subnet mask 255.255.255.0)

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

#### SIEMENS

192.168.1.1/SCALANCE S615

Welcome admin	Internet Protocol (IP) Rule	s				
Logout						
Wizards	General Predefined Dynamic Rule	s IP Services ICMP Se	ervices IP Protocols	IP Rules		
FTTZAIGS						
►Information	IP Version: IPv4 🗸					
► Sustem	Rule Set: - 🗸					
▶System	🗹 show all					
►Interfaces	Select Protocol	Action From	То	Source (Range)	Destination (Range)	
	IPv4	Accept Vlan2 (	EXT) V Device	▶ 192.168.2.110/32	192.168.1.0/24	
▶Layer 2						
▶Layer 3 (IPv4)	1 entry.					
	Create Delete Set Values Ret	rech			N	
►Layer 3 (IPv6)	Create Delete Set values Re	CSII			2	
0 11						

Infine, è possibile anche selezionare il protocollo o servizio abilitato per la specifica regola. Al termine della creazione della regola cliccare su "Set Values".

SCALANCE	S615 WEB Manageme 🗙	+						
$\leftrightarrow$ $\rightarrow$ G	▲ Non sicuro	https://192.168.1	.1				(	Q
SIEMENS	192.168.1.1/	SCALANCI	E S615					
Welcome admin	Internet Protocol (II	P) Rules						
► Wizards	General Predefined Dyna	mic Rules IP Services	ICMP Services	P Protocols IP	Rules			
►Information	IP Version: IPv4 🗸							
▶ System	Rule Set: _	~						
Interfaces	Select Prote	ocol Action	From	То	Source (Range)	Destination (Range)	Service	Log
►Layer 2	IPv4	4 Accept	✓ vlan2 (EXT)	✓ Device	▶ 192.168.2.110/32	192.168.1.0/24	all 🗸	none
▶Layer 3 (IPv4)	1 entry.						S7 DNS	
►Layer 3 (IPv6)	Create Delete Set Val	lues Refresh					FTP NTP	
✓Security							SSH	
▶Users							VNC HTTP	
▶Passwords							SMTP	
►AAA							TFTP	
▶Certificates							HTTPS IPSec	
Firewall							Telnet	
►IPSEC VPN							IPSec_tnat	
►Brute Force Prevention							protocollo OpenVPN_TCP	

**N.B.:** i servizi vanno prima definiti nella tab IP Services (vedere capitolo successivo) per essere selezionati dal menu a tendina.

#### Creazione di servizi basati su porte TCP/UDP

Per sfruttare le funzionalità Layer 4 del firewall, legate al filtraggio sulla base del protocollo di comunicazione, è necessario creare dei servizi nel tab "IP Services".

Inserire un nome a piacere per denominare il servizio in corrispondenza di "Service Name" e cliccare su "Create".

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

#### SIEMENS

	192.168.1.1/SCALANCE S615
Welcome admin	Internet Protocol (IP) Services
Logout	
▶Wizards	General Predefined Dynamic Rules IP Services ICMP Services IP Protocols IP Rules
► Information	Service Name: protocollo
▶System	Select         Service Name         Transport         Source Port (Range)         Destination Port (Range)           0 entries.         0
►Interfaces	Create Delata Refresh
▶Layer 2	
▶Layer 3 (IPv4)	
▶Layer 3 (IPv6)	
-Security	
▶Users	
▶Passwords	
►AAA	
▶Certificates	
Firewall	

Una volta creato, è possibile definire il protocollo in base alla tipologia TCP/UDP e la porta di destinazione o sorgente (il carattere \* indica qualsiasi porta). Al termine della modifica, cliccare su "Set Values".

SCALANCE S615 W	VEB Manageme × +	
$\leftarrow$ $\rightarrow$ C $\triangle$	A Non sicuro   https://192.168.1.1	

#### SIEMENS

SIENIENS											
	192.16	68.1	.1/SCAL		E S6	15					
Welcome admin	Internet F	Protoc	ol (IP) Servi	ces							
<u>Logout</u>											
	General Prec	lefined	Dynamic Rules	IP Services	ICMP S	ervices	IP Protoco	ols IP Rules			
▶Wizards											
Information	Service Na	ime:									
		Se	lect	Service Nam	-	Transpor	+	Source Port	(Range)	Destination Port (Range	e)
▶Svstem		00			<b>C</b>	тапэрон		Source Fort	(Range)	Descritation Fort (rearies	c)
r oʻyotom				protocollo		TCP	~	. ·		26351	
Latorfaces		1 e	ntrv.			TCP					
▶ IIIIeIiaces						UDP	43				
	Create		Pot Values Defre	ch							
▶Layer 2	Create	elete	Set values Refre	sn							
►Layer 3 (IPv4)											

N.B.: Se il servizio in questione è definito da un intervallo di porte è possibile usare il carattere "-" fra la porta iniziale e quella finale per definire l'intervallo

I	SCAL	ANCE	S615 V	VEB N	lanageme 🗙	+
$\leftarrow$	$\rightarrow$	C	合	▲	Non sicuro	https://192.168.1.1

SIEMENS

#### 192.168.1.1/SCALANCE S615

Welcome admin	Internet Pro	Internet Protocol (IP) Services					
Logout							
Mizordo	General Predefin	ed Dynamic Rules	IP Services ICMP	Services IP Protoc	ols IP Rules		
▶ WIZards							
►Information	Service Name:						
		Select	Service Name	Transport	Source Port (Range)	Destination Port (Range)	
▶System			protocollo	TCP 🗸	*	24221 - 27338	
▶Interfaces		1 entry.					
▶Layer 2	Create Delete	e Set Values Refre	esh				

E' possibile inserire diversi tipi di servizi, sia noti che personalizzati. Riportiamo qui alcuni esempi.

	SCAL	ANCE	S615 V	VEB Manageme 🗙	+
$\leftarrow$	$\rightarrow$	C		A Non sicuro	https://192.168.1.1

#### SIEMENS

#### 192.168.1.1/SCALANCE S615

Welcome admin	Internet Prot	Internet Protocol (IP) Services					
Logout	Changes will be s	aved automatically in	n 46 seconds.Pre	ess 'Write Startu	<u>up Config' to</u>	save immedia	<u>tely</u>
•Wizards	General Predefin	ed Dynamic Rules	IP Services IC	CMP Services	IP Protoco	Is IP Rules	
F WIZUIUS							
►Information	Service Name:						
▶ System		Select	Service Name	Transport	t	Source Port (Range)	Destination Port (Range)
			S7	TCP	~	*	102
▶ Interfaces			DNS	UDP	~	*	53
▶Laver 2			FTP	TCP	~	*	21
Lujoi L			NTP	UDP	~	*	123
▶Layer 3 (IPv4)			RDP	TCP	~	*	3889
			SSH	TCP	~	*	22
►Layer 3 (IPv6)			VNC	TCP	~	*	5900
Security			HTTP	TCP	~	*	80
Alleere			SMTP	TCP	~	*	25
▶ Users			SNMP	UDP	~	*	162
▶Passwords			TFTP	TCP	~	*	69
►AAA			HTTPS	TCP	~	*	443
▶Certificates			IPSec	UDP	~	*	500
▶Firewall			Telnet	TCP	~	*	23
▶IPsec VPN			OpenVPN	UDP	~	*	1194
NOpen//PN			IPSec_tnat	UDP	~	*	4500
			protocollo	TCP	~	*	24221 - 27338
Prevention			OpenVPN_TCF	P TCP	~	*	5443
		18 entries.					
	Create Delete	e Set Values Refre	esh				

#### Creazione di servizi basati su ICMP

All'elenco del paragrafo precedente fanno eccezione i servizi ICMP, come il ping che, non essendo un servizio basato su TCP/UPD, va definito a parte nella tab "ICMP Services".

Inserire il nome scelto in corrispondenza di "Service Name" e cliccare su "Create"

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

#### SIEMENS

#### 192.168.1.1/SCALANCE S615

Welcome admin	Internet Control Message Protocol (ICMP) Services						
Logout							
▶ Wizards	General Predefined Dynamic Rules IP Services ICMP Services IP Protocols IP Rules						
F WIZUIUS							
►Information	Service Name: PING						
▶ System	Select Service Name Protocol Type Code						
▶Interfaces	o entries.						
, mondoos	Create Delete Refresh						
▶Layer 2	43						
►Layer 3 (IPv4)							

Definire il tipo di ping (in caso di dubbio lasciare "Any Type") e cliccare "Set Values".

SCALANCE S615 W	VEB Managem∈ ×	+
$\leftrightarrow$ $\rightarrow$ $C$ $\Delta$	A Non sicuro	https://192.168.1.1

#### SIEMENS

#### 192.168.1.1/SCALANCE S615

Welcome admin	Internet Control Message Protocol (ICMP) Services				
Logout	Changes will be saved automatically in t	56 seconds.Press 'Write Star	tup Config' to save immediately		
Wizards	General Predefined Dynamic Rules	IP Services ICMP Services	IP Protocols IP Rules		
F WIZUIUS					
Information	Service Name:				
. Ourstand	Select Service Nan	ne Protocol	Туре	Code	
▶ System	PING	ICMPv4	- Any Type -	- Any Code - V	
▶Interfaces	1 entry.		- Any Type -	<u> </u>	
Fintendees			Destination Unreachable (3)		
▶Layer 2	Create Delete Set Values Refres	h	Source Quench (4)		
			Redirect Message (5)		
▶Layer 3 (IPv4)			Alternate Host Address (6)		
			Echo Request (8)		
►Layer 3 (IPv6)			Router Solicitation (10)		
- C it -			Time Exceeded (11)		
Security			Parameter Problem (12)		
▶Users			Timestamp (13)		
▶Passwords			Timestamp Reply (14)		
►AAA			Information Request (15)		
			Address Mask Request (17)		
▶Certificates			Address Mask Reply (18)		
Firewall			Traceroute (30)		
▶IPsec VPN			Datagram Conversion Error (31)		
▶OpenVPN			Mobile Host Redirect (32)	<b>•</b>	

#### Servizi predefiniti su Scalance S/M

Nel tab "Predefined" del menu Firewall è anche possibile attivare dei servizi IP predefiniti. Questi servizi riguardano solamente quelli che possono <u>accedere al device</u> (cioè lo Scalance). Non è quindi necessario utilizzare queste impostazioni per impostare regole di comunicazione fra dispositivi esterni che insistono su subnet diverse e devono comunicare attraverso lo Scalance! Per queste si procede con la tab IPServices, come già precedentemente illustrato.

SCALANCE	S615 WEB Managen	ne × +														$\vee$	-
$\leftarrow \   \rightarrow \   {\tt G}$	☆ ▲ Non s	icuro   <del>https:</del> ,	//192.168.	1.1											Q 🖻 ☆	*	≡J
SIEMENS	SIEMENS 192 168 1 1/SCALANCE S615 01/01/200																
Welcome admin	Predefined																
▶Wizards	General Predefined	Dynamic Rules	IP Service	s ICMP Se	ervices IP	Protocols	IP Rules										
►Information	Allow device sen	vices:															
▶System	Interface <del>▼</del> vlan2 (EXT)	IP Version IPv4	All	HTTP	HTTPS	DNS	SNMP	Telnet	TCP Event	IPsec VPN	SSH	DHCP	Ping	System Time	Cloud Connector	VRRP	J
▶Interfaces	vlan2 (EXT) vlan1 (INT)	IPv6 IPv4															J
▶Layer 2	vlan1 (INT) SINEMA RC	IPv6 IPv4															
►Layer 3 (IPv4)	ppp2	IPv4															
+Layer 3 (IPv6) ▼Security	ppp2 Set Values Refr	IPv6 esh															

Di default la maggior parte dei servizi può lavorare sulla rete interna (VLAN 1) mentre il device è inaccessibile dall'esterno (VLAN 2 o interfaccia mobile USBO).

#### Configurazione automatica del firewall da Sinema RC

In caso dell'utilizzo del Sinema Remote Connect, non è necessario effettuare alcuna configurazione del firewall. Al default è attivato l'auto-firewall.

SCALANCE	S615 WEB Manageme × +	
$\leftarrow \   \rightarrow \   G$	▲ Non sicuro   http://www.sicuro   http://wwwwwwwwwwwwwwwwwwwwwww.sicuro   http://www.sicuro   http://wwwwwwwwwwwwww.sicuro   http://www.sicuro   http://www.sicur	<del>ps</del> ://192.168.1.1
SIEMENS	192.168.1.1/SC	ALANCE S615
Welcome admin	SINEMA Remote Conne	ct (SINEMA RC)
₩izards		Enable SINEMA RC
Information		Server Settings
▼System	SINEMA RC Address:	
▶Configuration	SINEMA RC Port.	443
▶General		
▶Restart		Server Verification
▶Load&Save	Verification Type:	Fingerprint ~
▶Events	Fingerprint:	
►SMTP Client	CA Certificate:	- ~
►SNMP		
▶System Time		Device Credentials
♦Auto Logout	Device ID:	0
▶Button	Device Password:	
▶Syslog Client	Device Password Confirmation:	
Fault Monitoring	_	Optional Settings
▶PLUG		Auto Firewall/NAT Rules
▶Ping	Type of connection:	Auto 🗸
►DCP Discovery	Use Proxy:	none ~
▶DNS	Autoenrollment Interval [min]:	60
DHCPv4	Timeout[min]:	0
CRSP / SRS		
. onor rono		

Questo significa che **le regole di firewall, che permettono il passaggio di dati dalla VPN Sinema Remote Connect alle reti configurate sul Sinema Remote Connect Server, sono automaticamente inserite** (così come le regole di NAT). **N.B.:** se si vuole filtrare i dati che dalla VPN passano verso le macchine, è necessario disabilitare questa spunta e inserire le regole a mano come riportato nella restante parte della guida.

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									
Logout										
▶Wizards	General Predefined Dynamic Rules IP Services ICMP Services IP Protocols IP Rules									
►Information	IP Version: IPv4 🗸									
▶System	Rule Set: ✓ show all									
▶Interfaces	Select Protocol Action From To Source									
▶Layer 2	□ IPV4 Accept V SINEMARC V   vian1 (INT) V 0.0.000									
►Layer 3 (IPv4)	1 entry.									
▶Layer 3 (IPv6)	Create Delete Set Values Refresh									

#### Configurazione automatica del firewall per regole di NAT

Anche configurando regole di NAT, dalla versione firmware 6.1, è possibile configurare automaticamente le corrispondenti regole di firewall in caso di uso della modalità Netmap (non in NAPT o Source NAT): Basta infatti inserire le regole di NAT e selezionare la **spunta "Auto Firewall Rule"** 



Andando sulla pagina del firewall è infatti possibile osservare che è stata inserita la regola coerente

SCALANCE	S615 WEB Manageme 🗙	+					~ -	- 0 ×
$\leftrightarrow$ $\rightarrow$ G	▲ Non sicuro	https://192.168.1.1				Q	. @ ☆ <b>*</b>	- 🖬 😩 E
SIEMENS								
	192.168.1.1/S	CALANCE S6	15				01/01	2000 01:57:23
Welcome admin	Internet Protocol (IP)	Rules						
Logout	Changes will be saved automa	atically in 59 seconds.Press 'W	rite Startup Config' to save imme	adiately.				🖿 <b>?</b> 🗄 🗡
▶Wizards	General Predefined Dynami	ic Rules IP Services ICMP S	ervices IP Protocols IP Rule	S				
▶Information	IP Version: IPv4 🗸							
▶Svstem	Rule Set:	~						
Nintorfacos	Soloct Protoco	al Action From	То	Source (Bange)	Doctination (Pango)	Service Log	Procodonco	Assign to
<ul> <li>Layer 2</li> </ul>	IPv4	Accept Vlan2	(EXT) Vlan1 (INT) V	<ul> <li>0.0.0.0/0</li> </ul>	192.168.2.100/32	all v none	✓ 0	Assign to 7
►Layer 3 (IPv4)	1 entry.							
▶Layer 3 (IPv6)	Create Delete Set Value	s Refresh						
-Security	5							

Tale regola è solo parzialmente modificabile (è possibile restringere gli IP sorgenti e cambiare i servizi) e non cancellabile in quanto legata alla regola di NAT. Di conseguenza per cancellare la regola di firewall occorre cancellare la corrispondente regola di NAT. 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.