



ноw то

Configurare routing NAT

SIEMENS

Contents

Config	Configurare routing (NAT)						
Premes	sa	3					
1.	STANDARD ROUTING	5					
2.	DESTINATION NAT (1:1)	6					
3.	NAPT (1:N) o PORT FORWARDING	7					
4.	SOURCE NAT o NAT MASQUERADING (1:N)	8					
5.	DOUBLE NAT (1:1)	9					
Esempi	di Programmazione	11					
1.	STANDARD ROUTING	11					
2.	DESTINATION NAT (1:1)	13					
3.	NAPT (1:N) o PORT FORWARDING	16					
4.	SOURCE NAT o NAT MAQUERADING (1:N)	19					
5.	DOUBLE NAT (1:1)	21					
6.	SETTAGGI NETMAP con BIDIRECTION RULE attiva	23					

Configurare routing (NAT)

Premessa

Gli scalance S (S615/SC600) e M (M87x) sono devices che incorporano le funzionalità di FIREWALL e ROUTING (LAYER 3). Tutti questi dispositivi al default di fabbrica nascono con due sottoreti distinte:

VLAN1 (rete interna),

VLAN2 (rete esterna, chiamata USBO nel caso degli M dove coincide con la rete mobile).

Le comunicazioni che possono transitare tra queste due sottoreti vengono decise in base alla programmazione dello scalance.

Al default le due subnet sono completamente separate grazie al FIREWALL attivo.

Sarà cura del programmatore settare opportunamente lo Scalance con le regole di ROUTING (NAT) e FIREWALL. Oltre alle VLAN di default, 1 e 2, con opportuna programmazione si possono creare anche altre VLAN, e le comunicazioni tra tutte le N VLAN dovranno poi essere definite in fase di programmazione come avviene per quelle al default di fabbrica, 1 e 2 (USBO per gli Scalance M).

La presente guida ha lo scopo di far comprendere quale tipo di programmazione (quale NAT) va programmato in funzione dei requisiti di partenza.

La guida è stata redatta con le seguenti versioni HW/FW ma valida anche per le successive.

	нพ	FW						
Scalance S615	6GK5 615-0AA00-2AA2	V06.03.00						
N.B.: Guida e programmazione valida anche per Scalance M87x.(*) e SC600.								
Scalance M87x	6GK5 87x (x=2,3,4)	V06.04.00						
Scalance SC600	6GK5 6xy (x=3,4; y=2,6)	V02.01.01						

*: Negli scalance M87x la VLAN 2 è la rete mobile, Ma nulla vieta previa programmazione opportuna di creare nuove VLAN e di ricondursi in questo modo alla funzionalità standard degli scalance S.

Lo schema di principio del **ROUTING** è il seguente: due dispositivi in due sottoreti diverse devono essere messi in comunicazione.



Figura 1: Schema base Routing

All'interno di una stessa sottorete i vari devices comunicano tra di loro sfruttando gli indirizzi MAC Address (LAYER 2 struttura ISO/OSI).

Gli indirizzi IP (LAYER 3 struttura ISO/OSI) entrano in gioco solo quando dobbiamo mettere in comunicazione oggetti in sottoreti diverse.

Lo scalance S/M avendo una connessione su entrambe le VLAN può fare da ROUTER, consentendo tale comunicazione.

All'inizio di ogni comunicazione il device chiamante controlla se l'indirizzo di destinazione è nella sua sottorete:

=>Se SI inoltra il pacchetto sfruttando il MAC ADDRESS di destinazione.

=>Se NO deve sapere quale è l'elemento che fa da interfaccia verso l'altra subnet (ROUTER) a cui spedirà il pacchetto per la successiva elaborazione.

Anche senza default gateway in uno o entrambi gli oggetti che devono comunicare tra loro è possibile instaurare un collegamento, ma per la corretta programmazione dello scalance è indispensabile conoscere:

- 1. Quali sono i settaggi a livello di default gateway (standard router) in questi dispositivi.
- 2. Chi inizia la comunicazione e chi risponde.

Vediamo quindi tutte le possibili casistiche:

1.STANDARD ROUTING

Entrambi i dispositivi, CHIAMANTE e CHIAMATO, hanno settato il default gateway pari alle relative interfacce dello scalance S.





Se il PC 192.168.2.10 chiama la CPU 192.168.1.20 indirizza il pacchetto verso il suo default gateway, il 192.168.2.1, interfaccia VLAN2 dello scalance S615.

Il router prende il pacchetto, verifica che la destinazione è nella VLAN 1 a lui connessa, e lo inoltra qui lasciando come sorgente l'indirizzo originale del PC chiamante.

Una volta arrivato ed elaborato dalla CPU, la risposta fa il percorso inverso esattamente con le stesse modalità: la CPU capisce che deve rispondere verso un'altra sottorete e lo fa grazie al default gateway settato verso 192.168.1.1, interfaccia VLAN 1 dello scalance S615 che a sua volta completa la comunicazione inoltrando la risposta verso il PC.

Questa modalità è detta STANDARD ROUTING: entrambi i devices si vedono con i loro indirizzi reali, non abbiamo necessità di indirizzi di appoggio nattati.

2. DESTINATION NAT (1:1)

Solo il device CHIAMATO ha settato il default gateway pari alla relativa interfaccia dello scalance S, il CHIAMANTE no.





In questo caso il PC chiamante non ha settato il default gateway verso lo scalance S.

Non è quindi in grado di indirizzare correttamente il pacchetto con destinazione le CPU nella VLAN1 nel caso le cerchi con il loro indirizzo reale.

Dato che il PC non può che comunicare con indirizzi in VLAN2 l'unico modo per permettere la comunicazione è di "presentare" le CPU in VLAN2 con appositi indirizzi nattati di appoggio.

Fatto questo, il pacchetto indirizzato verso 192.168.2.2 viene preso in carico dallo scalance che poi sa che va indirizzato verso la CPU 1 sostituendo in uscita dalla sua porta in VLAN1 l'indirizzo di destinazione con quello reale della CPU 1.

L'indirizzo sorgente di questo pacchetto è sempre quello del PC e la CPU avendo il default gateway è in grado di rispondere correttamente.

Per il DESTINATION NAT (1:1) condizione necessaria è avere N indirizzi di appoggio nella subnet del device CHIAMANTE per gli N device da raggiungere.

Con una singola regola di DESTINATION NAT è possibile poi rendere disponibile l'indirizzo di appoggio anche a più devices della sottorete chiamante (non al solo al PC come nell'esempio), dipende dalla programmazione del FIREWALL

3.NAPT (1:N) o PORT FORWARDING

Solo il device CHIAMATO ha settato il default gateway pari alla relativa interfaccia dello scalance S, il CHIAMANTE no.



Figura 4: NAPT (Network Address Port Translation)

Una possibile alternativa al DESTINATION NAT visto precedentemente è il NAPT.

Qui a differenza del DESTINATION si può sfruttare direttamente l'indirizzo esterno in VLAN2 del S615 senza dover necessariamente aver bisogno di altri indirizzi aggiuntivi.

Si opera una traslazione sulla porta (servizio): nell'esempio il PC vuole raggiungere la WEB page della CPU1. Manda quindi la richiesta direttamente allo scalance VLAN 2 utilizzando una porta di appoggio TCP 8080. Lo scalance opportunamente programmato indirizza la richiesta verso la CPU 1 alla porta effettiva del servizio, la TCP 80 (http). La risposta ritorna al PC grazie al default gateway settato in ogni CPU.

Analogamente, sfruttando un'altra porta di appoggio diversa, esempio TCP 8081, si può raggiungere la pagina WEB sempre in http (TCP 80) anche della seconda CPU.

Questa traslazione è possibile se il servizio, in questo caso la pagina WEB, consente l'uso di una porta variabile di appoggio.

Se invece la porta d'ingresso dovesse essere fissa (esempio S7/TIA, TCP 102) non sarebbe possibile gestire più di una CPU alla volta.

Ricapitolando con il NAPT è possibile raggiungere più devices con un solo indirizzo di appoggio nella VLAN di partenza, che può essere lo stesso impiegato per lo scalance. Deve essere possibile operare traslazioni di porta se si vuole gestire lo stesso servizio su più devices.

4.SOURCE NAT o NAT MASQUERADING (1:N)

Solo il device CHIAMANTE ha settato il default gateway pari alla relativa interfaccia dello scalance S, il CHIAMATO no.



Figura 5: SOURCE NAT

In questo caso è la CPU che inizia la comunicazione verso il PC.

La CPU ha settato il default gateway quindi il pacchetto con indirizzo di destinazione 192.168.2.10 viene spedito allo scalance in VLAN 1.

In uscita dallo scalance in VLAN 2, nel pacchetto viene sostituito l'indirizzo sorgente della CPU, 192.168.1.20, con l'indirizzo in VLAN 2 dello scalance: in questo modo il PC sa poi dove inoltrare la risposta (non avendo gateway il PC non può che gestire indirizzi nella sua stessa sottorete).

Il SOURCE NAT può essere 1:1 (la CPU può comunicare solo con il PC come nell'esempio sopra), oppure anche 1:N (la CPU può iniziare la comunicazione verso tutti i device in VLAN 2), dipende dalla programmazione dello scalance e non necessita di indirizzi di appoggio aggiuntivi.

N.B.: SOURCE & DESTINATION NAT vengono usati contemporaneamente nel caso la comunicazione possa essere iniziata sia dalla CPU che dal PC.

5.DOUBLE NAT (1:1)

Nessuno dei due devices, CHIAMANTE e CHIAMATO, ha settato il default gateway.



Figura 6: DOUBLE NAT

La comunicazione viene iniziata dalla CPU 2 in VLAN 2 verso la CPU 1 che risponde.

Entrambi i dispositivi non hanno default gateway, quindi sono in grado di gestire solo pacchetti con indirizzi nelle rispettive subnet locali.

La CPU 2 chiamante necessita di un indirizzo di appoggio e cerca la CPU 1 con 192.168.2.2.

Il pacchetto con questo indirizzo di destinazione viene preso in carico dallo scalance VLAN 2.

Lo scalance invia poi in VLAN 1 lo stesso pacchetto apportando due modifiche: cambia l'indirizzo di destinazione con quello reale della CPU 1 e modifica anche l'indirizzo sorgente con quello dello scalance stesso VLAN 1, 192.168.1.1.

A questo punto la CPU 2 è in grado conoscere il percorso della risposta e reinvia il pacchetto allo scalance che poi completerà la risposta inoltrandolo alla CPU 1.

Con il DOUBLE NAT non è possibile rendere disponibile l'indirizzo di appoggio a più devices della sottorete chiamante: con una regola di DOUBLE NAT solo la CPU2 può comunicare con la CPU1.

Nel caso ci siano altri devices in VLAN2 che devono essere messi in comunicazione con la CPU1 in VLAN1 vanno inserite altre regole di DOUBLE NAT.

Possiamo così riassumere tutte le casistiche di ROUTING nella tabella seguente:

Tipo di Routing/NAT	Impostazione gateway nel Device 1 CHIAMANTE: →	SI	NO
Impostazione gateway nel Device 2 CHIAMATO:			
t			
		STANDARD	DESTINATION NAT
51		ROUTING	NAPT
			DOUBLE NAT
NU		SOURCE NAT	(*)

(*): Con il NAT MASQUERADING abilitato nella VLAN CHIAMATA ci si riconduce a DESTINATION NAT.

Nelle pagine seguenti sono dettagliati esempi di programmazione dello scalance.

Viene anche spiegato, in funzione del tipo di ROUTING adottato, come il pacchetto viene modificato per permettere la comunicazione da MITTENTE a DESTINATARIO e conseguente risposta:

Il pacchetto IP:	PAYLOAD	Altro header TCP/UDP	Source TCP/UDP Port	Destination TCP/UDP Port	resto header IP	Source IP Address	Destination IP Address

• Source IP : l'indirizzo IP del Source, ovvero chi inizializza la connessione/invia il pacchetto

• Destination IP : l'indirizzo IP del Destination, ovvero di chi deve accettare la connessione/ricevere il pacchetto

• Source Port: la porta logica TCP o UDP del Source, solitamente è una porta dinamica e scelta casualmente.

Destination Port: la porta di trasmissione TCP o UDP del Destination, solitamente dipende dal protocollo superiore

• Altri Header: altri dati degli header TCP/UDP/IP non rilevanti per il NAT/NAPT

• Payload: i veri dati trasportati con eventuali header di protocolli a livello superiore (es: livello applicativo, HTTP...)



Figura 7: Schema comunicazione tra due devices in sottoreti diverse

Esempi di Programmazione

1.STANDARD ROUTING



Figura 8: STANDARD Routing: Principio comunicazione

Come programmazione dobbiamo solo aprire la comunicazione a livello di FIREWALL, visto che gli indirizzi con cui si vedono i devices rimangono quelli reali grazie ai default gateway correttamente settati su entrambi.

IMPORTANTE: il FIREWALL è di tipo STATEFUL: basta configurare solo la direzione di chiamata, la risposta passa in AUTOMATICO (non va quindi settata anche la regola duale in direzione opposta).

Nell'esempio sotto in figura 9 abbiamo aperto (ACTION=ACCEPT) la comunicazione dal MITTENTE(FROM) in VLAN2 (solo questo device con l'indirizzo IP specificato /32 in SOURCE RANGE) ad un solo DESTINATARIO (TO) in VLAN1 (avendo anche qui specificato il suo indirizzo IP con /32 in DESTINATION RANGE).

Welcome admin	Internet Protocol (IP) Rules									
Logout										
♦ Wizards	General Predefined IPv4 User Specific 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)	Service L							
▶Layer 2	IPv4 Accept Vian2 (EXT) Vian1 (INT) 192.168.2.1/32	192.168.1.1/32	all 🗸							
▶Layer 3	Create Delete Cot Valuer Bofrech									
-Security										
▶Users										
▶Passwords										
►AAA										
▶ Certificates										
Firewall										

Figura 9: Settaggio IP FIREWALL Rules da solo Device1 a solo Device 2 su tutti i servizi.

Lasciando nei campi **SOURCE e/o DESTINATION** il parametro al default "0.0.0.0/0" significherebbe invece permettere qualsiasi indirizzo IP come sorgente e/o destinatario.

Nella colonna **SERVICE** lasciando "all" tutti i servizi sono consentiti.

Potremmo anche decidere di far transitare solo uno o un range di servizi specificandoli prima nelle IP SERVICES.

Per fare questo è sufficiente inserire un acronimo nel campo **SERVICE NAME**, cliccare CREATE, inserire il numero di porta nella colonna **DESTINATION PORT** selezionando anche se **TCP o UDP**, ed infine cliccare SET.

Nell'esempio di figura 10 sono stati previsti una serie di servizi riferiti ad una sola porta ed un range di porte da TCP 50 a TCP 60.

Welcome admin	Internet Protoc	ol (IP) S	ervices				
Logout							
♦ Wizards	General Predefined	IPv4 User	Specific IP Services	ICMP Services	IP Prot	ocols IP Rules	
Information	Service Name:						
	Se	lect	Service Name	Transport		Source Port (Range)	Destination Port (Range)
▶ System			S7	TCP	~	ż	102
L Interfaces			https	TCP	~	*	443
Fintenaces			IPSEC1	UDP	~	*	500
▶Layer 2			IPSEC2	UDP	~	*	4500
			Range1	TCP	~	*	50 - 60
▶Layer 3	5 e	ntries.					
✓Security							
▶Users	Create	Set Values	Refresh				
▶Passwords							
▶ AAA							
▶ Certificates							
Firewall							

Figura 10: Esempio settaggio IP Services

Infine nelle IP RULES questi servizi possono essere selezionati dal menù a tendina nella colonna SERVICES.

Nell'esempio di figura 11 si consente la comunicazione da PC (192.168.2.1) a CPU (192.168.1.1) per i soli servizi S7 e HTTPS. Viene anche consentita una comunicazione instaurata da qualsiasi device in VLAN1 a tutta la VLAN 2 per il range di servizi TCP da 50 a 60.

Welcome admin	Internet Prot	Internet Protocol (IP) Rules										
Logout												
▶Wizards	General Predefine	ed IPv4 User S	Decific IP Servi	ces ICMP Servic	es IP Protocols	IP Rules						
► Information	IP Version: IPv	4 🛩										
▶System	Rule Set: -	Rule Set:										
►Interfaces	Sele	ect Protocol	Action	From	То	Source (Range)	Destination (Range)	Service		Log	F	Prece
		IPv4	Accept •	 vlan2 (EXT) 	✓ vlan1 (INT)	✓ 192.168.2.1/32	192.168.1.1/32	S7	~	none	~ (0
▶Layer 2		IPv4	Accept •	 vlan2 (EXT) 	 vlan1 (INT) 	✓ 192.168.2.1/32	192.168.1.1/32	https	~	none	v '	1
▶Layer 3		IPv4	Drop	 vlan1 (INT) 	 vlan2 (EXT) 	✔ 0.0.0.0/0	0.0.0/0	Range1	~	none	~ :	2
-Security	3 en	tries.										
►Users	Create Delete	Set Values R	efresh									
▶Passwords												
►AAA												
▶Certificates												
Firewall												

Figura 11: Esempio settaggio IP FIREWALL Rules

2. DESTINATION NAT (1:1)



Figura 12: DESTINATION NAT Principio comunicazione

Il MITTENTE senza default gateway manda il pacchetto all'indirizzo di appoggio 192.168.2.2 nella stessa subnet.

Questo indirizzo di appoggio viene inserito nel campo DESTINATION IP SUBNET (unico indirizzo con /32).

Il **TRANSLATED DESTINATION IP SUBNET** deve contenere l'indirizzo reale in VLAN 1 del DESTINATARIO (<u>sempre unico</u> indirizzo con /32).

Welcome admin	NETMAP							
Logout								
Mizarde	Masquerading	NAPT	Source NAT	NETM/	NP .			
• WIZdrus								
► Information			Type:	Destina	tion		~	
• System	Source Interface: vlan2 (EXT)						~	
<i>y</i> oystom			~					
►Interfaces		Sour	ce IP Subnet:	192.168	.2.1/32			
▶Laver 2	Translat	ed Sour	ce IP Subnet:					
	0)estinati	on IP Subnet:	192.168	2.2/32			
⋆Layer 3	Translated D)estinati	on IP Subnet:	t 192.168.1.1/32				
Static Routes						Bidirectional Rule		
▶Subnets				🗸 Auto	Firewall Ru	lle		
►NAT				Select	Туре	Source Interfac	е	
▶VRRPv3				0 entries	L.			

Select	Туре	Source Interface	Destination Interface	Source IP Subnet	Translated Source IP Subnet	Destination IP Subnet	Translated Destination IP Subnet
	Destination	vlan2	vlan1	192.168.2.1/32	-	192.168.2.2/32	192.168.1.1/32
1 entry.							

Figura 13: DESTINATION NAT Settaggio NETMAP da solo Device1 a Device 2

Il FLAG attivo su "AUTO FIREWALL RULE" consente il settaggio in automatico delle FIREWALL IP Rules:

Select	Protocol	Action	From	То	Source (Range)	Destination (Range)	Service	Log	Precedence	Assign
	IPv4	Accept 🗸	vlan2 (EXT) 🛛 💙	vlan1 (INT) 🛛 🗸	192.168.2.1/32	192.168.1.1/32	all 🗸	none 🗸	0	
1 entry.										

Figura 14: DESTINATION NAT Settaggio Automatico regola di Firewall da solo Device1 a Device 2 su tutti i servizi

Anche qui ovviamente poi la risposta da DESTINATARIO a MITTENTE ritorna in automatico senza necessità di ulteriori settaggi né lato NETMAP né lato FIREWALL.

Settando nel campo SOURCE IP SUBNET :0.0.0/0, con il **DESTINATION NAT** abbiamo la possibilità di permettere la comunicazione tra tutti i device in VLAN2 (quindi da più MITTENTI) verso il device RICEVENTE in VLAN1.

Questa applicazione trova particolare impiego in caso di teleassistenza remota passando da una VPN di terze parti che consente la connessione verso la VLAN2, dove sono presenti anche gli indirizzi di appoggio NATTATI.

In questi casi non è solitamente possibile predeterminare con quale indirizzo si presenterà il MITTENTE dall'altro capo della VPN.

Masquerading	NAPT	Source NAT	NETMAP	
		Type:	Destination	~
	Sou	irce Interface:	vlan2 (EXT)	~
	Destina	tion Interface:	vlan1 (INT)	~
	Sour	ce IP Subnet:	0.0.0/0	
Translat	ed Sour	ce IP Subnet:		
[)estinati	on IP Subnet:	192.168.2.2/32	
Translated [)estinati	on IP Subnet:	192.168.1.1/32	
			Bidirectional Rule	
			Auto Firewall Rule	

Select	Туре	Source Interface	Destination Interface	Source IP Subnet	Translated Source IP Subnet	Destination IP Subnet	Translated Destination IP Subnet
	Destination	vlan2	vlan1	0.0.0/0	-	192.168.2.2/32	192.168.1.1/32
1 entry.							

Figura 15: DESTINATION NAT Settaggio NETMAP da tutta VLAN 2 a Device 2

Protocol	Action	From	То	Source (Range)	Destination (Range)	Service	Log	Precedence
IPv4	Accept 🗸	vlan2 (EXT) 🗸 🗸	vlan1 (INT) 🗸 🗸	0.0.0/0	192.168.1.1/32	all 🗸	none 🗸	0
				A				

Figura 16: DESTINATION NAT Settaggio Automatico regola di Firewall da tutta VLAN 2 a Device 2 su tutti i servizi

Nel campo **SOURCE IP SUBNET** si può inserire anche un sottogruppo di indirizzi di rete, esempio 192.168.2.40/27 (quindi tutti devices dall'indirizzo 192.168.2.33 a 192.168.2.62 sono autorizzati a raggiungere il device 2).

Ovviamente il DESTINATION IP SUBNET, che rimane un indirizzo singolo, /32, deve essere fuori da questo intervallo.

Esiste infine la possibilità di poter instaurare questo tipo di comunicazione anche senza il default gateway settato nel Device 2 Destinatario.

Bisogna in questi casi abilitare il NAT MASQUERADING su VLAN1 (VLAN del device DESTINATARIO).

Così facendo qualsiasi pacchetto uscente dallo scalance S615 ha come suo indirizzo sorgente lo scalance in quella VLAN ed in questo modo ogni device sa a chi deve rispondere perché il MITTENTE risulta nella sua stessa subnet.

Welcome admin	Internet Proto	col (IP) Masquerading
Logout		
♦ Wizards	Masquerading NA	PT Source NAT NETMAP
►Information	Interface	Enable Masquerading
▶System	vlan1 (INT) vlan2 (EXT)	
►Interfaces	ppp2	✓
►Layer 2	Set Values Ref	resh
-vLayer 3		
▶Static Routes		
▶Subnets		
►NAT		

Figura 17: NAT MASQUERADING abilitato su VLAN 1

In ogni caso i vari parametri di rete, quindi anche il default gateway, dei devices connessi in VLAN 1 possono essere visionati e cambiati direttamente dal menù **SYSTEM-DCP DISCOVERY** dello scalance.

E' sempre raccomandabile ove possibile settare i gateway (operazioni che nelle CPU va eseguita con questa nello stato di STOP).

Welcome admin	Discover	y and Set	via PROFINET	Discovery and Co	onfiguration Pro	otocol (DCP)						
Logout												
Wizards	Timeout[s]:	5 🗸										
Information		Blink Own L	EDs									
System	Interface	vlan1 🗸										
General		Discover										
▶Restart						0						
▶Load&Save		Port	MAC Address	Device Type	Device Name	IP Address	Mask Address	Gateway Address	Name Status	IP Status	Timeout[s]	Blink
· Evente		P2	00-1b-1b-81-0f-4b	SIMATIC-PC	centrocontrollo	192.168.1.99	255.255.255.0	192.168.1.55	Discovered	Discovered/IP	5 🗸	Blink
▶ Events		P3	00-1b-1b-e7-c6-36	SCALANCE XB-200		172.16.100.87	255.255.255.0	172.16.100.1	None	Discovered/IP	5 🗸	Blink
▶SMTP Client		2 entries.										
▶ SNMP												
▶System Time	Set Values	Refresh										
► Auto Logout												
▶Button												
► Syslog Client												
Fault Monitoring												
▶ PLUG												
▶Ping												
DCP Discovery												

Figura 18: SYSTEM – DCP Discovery

3.NAPT (1:N) o PORT FORWARDING



Figura 19: NAPT Principio comunicazione

Con il **NAPT** (Network Address Port Translation) è possibile traslare una porta (servizio) in ingresso dalla VLAN del MITTENTE in un'altra porta nella VLAN del DESTINATARIO.

Con la traslazione quindi con un solo indirizzo di appoggio sulla VLAN 2, che corrisponde allo stesso del 615 in quella VLAN (non servono indirizzi aggiuntivi in VLAN2), è possibile raggiungere più device remoti.

Nell'esempio della figura 20 seguente abbiamo 3 dispositivi in VLAN1 di indirizzo 192.168.1.1, 192.168.1.2 e 192.168.1.3, dei quali è possibile raggiungere dalla VLAN2 le rispettive Web pages (servizio HTTPS porta TCP 443) grazie agli indirizzi **192.168.2.254:8081, 192.168.2.254:8082, 192.168.2.254:8083.**

Welcome admin	IP Network Address Port Translation (NAPT) (Port Forwarding)									
Logout										
Mizarde	Masquerading NAPT Source NAT	NETMAP	·							
▶ WIZdius										
►Information	Source Interface:	vlan2 (E	XT) 🗸							
• Sustam	Traffic Type:	TCP 🗸]							
Poystem		🗸 Use Ir	terface IP from Sou	urce Interface						
►Interfaces	Destination IP Address:	192.168.	2.254							
NL OWOF 2	Destination Port:	8083								
FLayer 2	Translated Destination IP Address:	0.0.0.0								
-Layer 3	Translated Destination Port:	443								
▶Static Routes		Select	Source Interface	Traffic Type	Interface IP	Destination IP	Destination Port	Translated Destination IP	Translated Destination Port	
▶ Subnets			vlan2	TCP		192.168.2.254	8081	192.168.1.1	443	
NAT			vlan2	TCP		192.168.2.254	8082	192.168.1.2	443	
			vlan2	TCP		192.168.2.254	8083	192.168.1.3	443	
▶VKKPV3		3 entries								

Figura 20: NAPT Esempio settaggio con DESTINATION IP = indirizzo IP S615 Source

Ricordo che oltre al settaggio del **NAPT** è necessario consentire come solito la comunicazione nel **FIREWALL** nella sola direzione da MITTENTE a DESTINATARIO.

Nella figura 21 seguente si è "semplicemente" aperta la comunicazione da tutti i devices in VLAN2 a tutti devices in VLAN 1 e su tutti i servizi. Agendo diversamente sul FIREWALL si possono introdurre le limitazioni volute tra devices e servizi.

Welcome admin	Internet Protocol (IP) F	Rules							
Logout									
►Wizards	General Predefined IPv4 User	r Specific IP Service	s ICMP Services	IP Protocols IP Ru	les				
►Information	IP Version: IPv4 🗸								
▶System	Rule Set: - 🗸]							
►Interfaces	Select Protocol	Action	From	То	Source (Range)	Destination (Range)	Service	Log	Prec
▶Layer 2	IPv4 1 entry.	Accept 🗸	vlan2 (EXT) 🗸	vlan1 (INT) 🗸	0.0.0.0/0	0.0.0.0/0	all 🗸	none 🗸	• 0
►Layer 3	Create Delete Set Values	Refresh							
-Security									
▶Users									
▶Passwords									
▶AAA									
▶Certificates									
Firewall									

Figura 21: Settaggio FIREWALL da VLAN 2 a VLAN 1

Nel caso di servizi ove la traslazione con cambio di porta non è possibile (esempio da PC con TIA il servizio viene iniziato da TCP 102 e deve essere necessariamente traslato sulla stessa porta 102) non è possibile gestire più devices DESTINATARI allo stesso momento.

In questo caso è possibile definire più indirizzi di appoggio nella VLAN del MITTENTE (che sono da dichiarare nella schermata SUBNET e non possono essere più di 5) o più semplicemente adottare la soluzione DESTINATION NAT già discussa precedentemente.

Nell'esempio di figura 22 è possibile raggiungere con il TIA (servizio TCP 102) da un PC in VLAN 2 le tre CPU in VLAN 1, cercandole con gli indirizzi **192.168.2.254, 192.168.2.2 e 192.168.2.3**.

I NAPT portforwordano il servizio TCP 102 verso gli indirizzi interni in VLAN 1 delle rispettive CPU.

Welcome admin	IP Network Address Port 1	Transla	tion (NAPT) (I	Port Forwa	rding)						
	Changes will be saved automatically	in 59 seco	onds.Press "Write S	tartup Config' t	o save immed	liately					
Logout											
	Masquerading NAPT Source NAT	NETMAR)								
♦ Wizards											
►Information	Source Interface:	vlan2 (E	X T) V								
. Ourban	Traffic Type:	TCP 🗸]								
▶ System		Use Interface IP from Source Interface									
►Interfaces	Destination IP Address:	192.168.	2.3								
	Destination Port:	102									
▶Layer 2	Translated Destination IP Address:	192.168.	1.3								
	Translated Destination Port:	102									
▶Static Routes		Select	Source Interface	Traffic Type	Interface IP	Destination IP	Destination Port	Translated Destination IP	Translated Destination Port		
▶ Subnets			vlan2	TCP		192.168.2.254	102	192.168.1.1	102		
			vlan2	TCP		192.168.2.2	102	192.168.1.2	102		
► NAT			vlan2	TCP		192.168.2.3	102	192.168.1.3	102		
▶VRRPv3		3 entries									

Figura 22: NAPT Esempio settaggio con anche DESTINATION IP diverso da indirizzo IP S615

Nella figura 23 seguente è riportato il settaggio degli indirizzi di appoggio nella schermata SUBNET.

Welcome admin	Connected Subnets Overview												
Logout													
▶Wizards	Overview Configura	Overview Configuration											
³ ► Information	Interface: VLAN1	~											
▶ System	Select	Interface	TIA Interface	Status	Interface Name	MAC Address	IP Address	Subnet Mask	Address Type	IP Assgn. Method			
► Interfaces		vlan1	yes	enabled	INT	20-87-56-97-16-91	192.168.1.254	255.255.255.0	Primary	Static			
		vlan2		enabled	vlan2-1	20-87-56-97-16-91	192.168.2.2	255.255.255.0	Secondary	Static			
▶Layer 2		vlan2		enabled	vlan2-2	20-87-56-97-16-91	192.168.2.3	255.255.255.0	Secondary	Static			
Lavor 2		vlan2	-	enabled	EXT	20-87-56-97-16-91	192.168.2.254	255.255.255.0	Primary	Static			
▼Layer 3		ppp2	-	disabled	ppp2	00-00-00-00-00	0.0.0.0	0.0.0	Primary	Static			
 Static Routes 	5 entrie	S.											
Subnets													

Figura 23: Definizione degli indirizzi IP 192.168.2.2 e 192.168.2.3 in VLAN 2

Infine si ricorda che è possibile settare un **NAPT** su un range di porte, come nella figura 24 seguente.

In caso di range, DESTINATION e TRANSLATED DESTINATION PORT devono avere gli stessi valori, non è possibile traslare un **RANGE** di porte.

Anche in questo bisogna ricordarsi di aprire detti servizi lato FIREWALL.

				(1 (3.1.5 00 000 (1						
	Welcome admin	IP Network Address Port 1	ransla	tion (NAPT) (I	Port Forwa	rding)				
		Changes will be saved automatically	in 38 sec	onds.Press 'Write S	tartup Config' t	o save immed	iately			
	Logout									
		Masquerading NAPT Source NAT	NETMA	P						
►Wiza	ards									
► Infor	rmation	Source Interface:	vlan2 (E	XT) 🗸						
		Traffic Type:	TCP 🗸]						
►Syst	tem			⊥ starfasa ID fram Ca	urse Interfese					
			Osei	nteriace in irom 50	urce mienace					
► Inter	rfaces	Destination IP Address:	192.168	.2.2						
		Destination Port:	50 - 60							
►Laye	er 2	Translated Destination IP Address:	192,168	.1.2						
		Translated Destination Port:	50 60							
-Laye	er 3	Translated Destination Fort.	50-00							
►S	tatic Routes		Select	Source Interface	Traffic Type	Interface IP	Destination IP	Destination Port	Translated Destination IP	Translated Destination Port
►S	ubnets			vlan2	TCP		192.168.2.2	50 - 60	192.168.1.2	50 - 60
	doneto		1 entry							
► N	AI									
►V	RRPv3	Create Delete Refresh								
		Cleate Delete Reliesh								

Mizarda	General Predefined IPv	v4 User Specific	IP Services ICM	IP Services	IP Protocols	IP Rules				
• Wizarus										
►Information	IP Version: IPv4 🗸									
▶ Svstem	Rule Set: -	~								
	🗹 show a	all								
►Interfaces	Select F	Protocol Actin	on From		То	Source (Range)	Destination (Ra	inge) Service		Log
▶Laver 2		IPv4 Acc	cept 🗸 vlan2	(EXT) 🗸	vlan1 (INT)	▶ 192.168.2.2/32	192.168.1.2/32	Range	1 🗸	none 🗸
	1 entry.									
►Layer 3	Create Delete Sat									
-Security	Create Delete Oet	Values								
▶Users										
▶Passwords										
▶AAA										
▶Certificates										
Firewall										

Figura 24: NAPT Esempio settaggio su un range di indirizzi

4.SOURCE NAT o NAT MAQUERADING (1:N)



Figura 25: SOURCE NAT Principio comunicazione

Con la programmazione di esempio in figura 26 abilitiamo la comunicazione dalla CP in VLAN 1 verso tutta la sottorete VLAN 2, quindi con i due PC di indirizzo 192.168.2.1 e 192.168.2.2.

Avendo lasciato fleggato ON la spunta "Use Interface IP from Destination interface", quando il pacchetto attraversa lo scalance S615 questo gli cambia l'indirizzo sorgente con il suo in VLAN 2: in questo modo i PC senza default gateway sapranno di dover reindirizzare le risposte al S615 che completerà così la comunicazione.

Welcome admin	IP Source	Netwo	ork Add	Ires	s Ti	ranslation (SNAT)		
Logout								
• Wizards	Masquerading	NAPT	Source N	TAI	NET	МАР		
► Information		Source	e Interface	vla	n1 (ll	NT)	~	
Svetom	De	stination	n Interface	vla	n2 (E	EXT)	~	
Poystern	Sour	ce IP Ad	dress(es)	192	.168	.1.1/32		
Interfaces				21	Jse Ir	nterface IP from Destinati	on Interfa	се
Laure 2	Translated S	Source I	P Address	192	.168	2.254		
FLayer 2	Destinati	on IP Ad	ddress(es)	0.0	0.0/0			
←Layer 3				Sel	ect	Source Interface	C.	Dest
▶ Static Routes				0 e	ntries			
▶Subnets		_						
►NAT	Create	lete	efresh					

Select	Source Interface	Destination Interface	Source IP Address(es)	Use Interface IP	Translated Source IP Address	Destination IP Address(es)
	vlan1	vlan2	192.168.1.1/32		192.168.2.254	0.0.0/0
1 entry.						

Figura 26: SOURCE NAPT Esempio settaggio

Anche qui è necessario consentire come solito la comunicazione nella sola direzione da MITTENTE a DESTINATARIO nel FIREWALL, in questo caso da VLAN 1 a VLAN 2.

Vista l'applicazione si potrebbe optare di consentire la comunicazione solo dalla CP di indirizzo 192.168.1.1/32, inibendola per tutti gli altri devices in VLAN 1.

Welcome admin	Internet Protocol (IP) Rules					
Logout						
►Wizards	General Predefined IPv4 User Specific IP Services	ICMP Services IP Protocols IP	Rules			
►Information	IP Version: IPv4 🗸					
▶System	Rule Set: - V					
►Interfaces	Select Protocol Action	From To	Source (Range)	Destination (Range)	Service	Log P
▶Laver 2	IPv4 Accept 🗸	vlan1 (INT) Vlan2 (EXT)	▼ 192.168.1.1/32	0.0.0/0	all	✓ none ✓ 0
	1 entry.					
►Layer 3	Create Delete Set Values Refresh					
-Security						
▶Users						
▶Passwords		Ν				
AAA		45				
▶ Certificates						
Firewall						

Figura 27: Settaggio FIREWALL da VLAN 1 (solo CP 192.168.1.1/32) a VLAN 2 (tutta)

5.DOUBLE NAT (1:1)

► NAT

Con il DOUBLE NAT è possibile mettere in comunicare devices senza default gateway.



Figura 28: DOUBLE NAT Principio comunicazione

Il PC che inizia la comunicazione vede la CPU con l'indirizzo di appoggio 192.168.2.1 La CPU risponde mandando i pacchetti all'indirizzo dell'interfaccia dello scalance 192.168.1.254.

Welcome admin	NETMAP						
Logout							
Mizordo	Masquerading	NAPT	Source NAT	NETMA	NP .		
WIZarus							
Information			Type:	Destina	tion		~
Sustam		Sou	rce Interface:	vlan2 (E	EXT)		~
System	1	Destinat	tion Interface:	vlan1 (I	NT)		~
Interfaces		Sour	ce IP Subnet:	0.0.0.0/0)		
Laver 2	Translate	ed Sour	ce IP Subnet:				
Layer 2	D	estinati	on IP Subnet:	192.168	.2.1/32		
Layer 3	Translated D	estinati	on IP Subnet:	192.168	.1.1/32		
▶Static Routes				Bidire	ctional Rule		
▶Subnets				🗸 Auto I	Firewall Rule		
►NAT				Select	Туре	Source Interfa	ace
Welcome admin	NETMAP						
Logout							
Wizards	Masquerading	NAPT	Source NAT	NETM	AP		
. Information			Type	Course			
mormauon		0.0	urea Interface	Source			-
System		50	urce internace	vlan2 (EXT)		~
to be designed as		Destina	ation Interface	vlan1 (INT)		~
Interfaces		Sou	rce IP Subnet	192.16	8.2.100/32		
Layer 2	Transla	ted Sou	rce IP Subnet	192.16	8.1.254/32		
		Destinat	ion IP Subnet	0.0.0.0	0		
∗Layer 3	Translated I	Destinat	ion IP Subnet				
 Static Routes 				Bidir	ectional Rule		
				-			

Select	Туре	Source Interface	Destination Interface	Source IP Subnet	Translated Source IP Subnet	Destination IP Subnet	Translated Destination IP Subnet
	Destination	vlan2	vlan1	0.0.0/0		192.168.2.1/32	192.168.1.1/32
	Source	vlan2	vlan1	192.168.2.100/32	192.168.1.254/32	0.0.0.0/0	-
2 entries.							

Select Type Source Interface

Figura 29: DOUBLE NAT Esempio settaggio

																				_
▶Wizards	General	Predef	ined IP	v4 Use	r Specific	IP Serv	vices	ICMP	Services	s IF	P Protocols	IP Ru	les							
►Information	IP Ver	rsion:	Pv4 🗸																	
▶System	Rule	e Set: 💶	show	~	•															
Interfaces		S	elect	Protocol	Actio	on	Fr	rom			То		Source (Rano	ie)	Destir	ation (Range))	Service		
				IPv4	Acc	ept	✓ v	rlan2 (E	XT)	~	vlan1 (INT)	~	192.168.2.10	0/32	0.0.0.	0/0	, 	all	~	n
▶Layer 2				IPv4	Acc	ept	٧V	rlan2 (E	XT)	~	vlan1 (INT)	~	0.0.0/0		192.1	58.1.1/32		all	~	n
►Layer 3		2	entries.																	
-Security	Creat	te Dele	ete Se	t Values	Refresh															
▶Users																				
▶Passwords																				
►AAA																				
▶Certificates																				
Firewall																				

Grazie al flag AUTO FIREWALL RULE on, il FIREWALL viene settato in automatico come di seguito:

Figura 30: DOUBLE NAT Settaggio FIREWALL in automatico.

II DOUBLE NAT consiste in due regole di DESTINATION e SOURCE entrambe nella stessa direzione.

La comunicazione DOUBLE NAT non può che essere 1:1, come evidenziato anche dal FIREWALL, dove solo il PC 192.168.2.100/32 viene autorizzato verso la VLAN1 (tutta), mentre tutte le comunicazioni instaurate dalla VLAN 2 verso la VLAN 1 possono transitare solo se verso la CP 192.168.1.1/32.

6. SETTAGGI NETMAP con BIDIRECTION RULE attiva

Dalla versione FW 6.1.x per lo scalance S615/M800 e FW 2.1.x scalance SC600, nelle NETMAP è possibile configurare in automatico anche una comunicazione in direzione opposta rispetto a quella consentita dalla regola settata.

Bidirectional Rule	
🗸 Auto Firewall Rule	

Grazie a questa funzionalità, se viene abilitata una comunicazione di DESTINATION NAT da VLAN 2 a VLAN 1, in automatico viene prodotta anche la regola per la direzione opposta, un SOURCE NAT. da VLAN 1 a VLAN 2.

In modo analogo si potrebbe creare una regola di SOURCE e la regola in direzione opposta di DESTINATION verrà prodotta in automatico.

E' sempre consigliato lasciare fleggato ON anche l'AUTO FIREWALL RULE.

Così facendo con un singolo settaggio potremo fare in modo che entrambi i device possono iniziare una comunicazione verso il partner, creando quindi un **SOURCE & DESTINATION NAT**.

Questo schema di comunicazione è consentito quando uno dei due device ha il gateway impostato correttamente, come nello schema sotto.



Figura 31: SOURCE & DESTINATION NAT Principio comunicazione.

Nell'esempio di programmazione della schermata sotto quindi si esegue semplicemente il settaggio del DESTINATION da VLAN 2 a VLAN 1 ed il SOURCE da VLAN 1 a VLAN 2 viene prodotto in automatico, così come le due regole di FIREWALL.

Welcome admin	NETMAP Changes will be saved automatically	in 7 sec	onds.Press	Write Startup Confi	<u>g' to</u>
Wizards	Masquerading NAPT Source NAT	NETM	AP		
► Information	Type:	Destina	ation		~
Sustam	Source Interface:	vlan2 (EXT)		~
Voyatom	Destination Interface:	vlan1 (l	NT)		~
Interfaces	Source IP Subnet:	0.0.0/	0		
Laver 2	Translated Source IP Subnet:				
	Destination IP Subnet:	192.168	8.2.1/32		
-Layer 3	Translated Destination IP Subnet:	192.168	8. <mark>1.1/32</mark>		
▶ Static Routes		Bidire	ectional Rul	e	
▶ Subnets		🗸 Auto	Firewall Ru	le	
► NAT		Select	Туре	Source Interface	
▶VRRPv3		0 entries	S.		

Select	Туре	Source Interface	Destination Interface	Source IP Subnet	Translated Source IP Subnet	Destination IP Subnet	Translated Destination IP Subnet
	Source	vlan1	vlan2	192.168.1.1/32	192.168.2.1/32	0.0.0/0	-
	Destination	vlan2	vlan1	0.0.0/0	-	192.168.2.1/32	192.168.1.1/32
2 entries.							

Figura 32: SOURCE & DESTINATION NAT Esempio settaggio

▶ Wizards	General Pre	defined l	Pv4 User Sp	ecific IP Se	rvice	s ICMP Service	es	IP Protocols	P Ru	les						
Information	IP Version	IDv4 N														
▶ mornation		11-14 4														
▶ System	Rule Set	-	~													
	Show all															
Interfaces		Select	Protocol	Action		From		То		Source (Range)	Destination (Range)	Service		Log	P	re
a Lawrence D			IPv4	Accept	~	vlan1 (INT)	~	vlan2 (EXT)	~	192.168.1.1/32	0.0.0/0	all	~	none	v ()
▶Layer 2			IPv4	Accept	\sim	vlan2 (EXT)	\sim	vlan1 (INT)	\sim	0.0.0/0	192.168.1.1/32	all	~	none	♥ 1	
▶Laver 3		2 entrie	S.													
-Security	Create	Delete	et Values Re	fresh												
►Users																
▶Passwords																
►AAA																
▶ Certificates																
Firewall										N .						
Firewall										2						

Figura 33: SOURCE & DESTINATION NAT Settaggio FIREWALL in automatico.

Nel caso invece in cui nessuno dei due device abbia settato correttamente il default gateway ed entrambi possano iniziare la comunicazione verso il partner, non ci resta che settare un double NAT per ognuna delle due direzioni.

Anche in questo caso la funzionalità di BIDIRECTIONAL RULE ci viene in aiuto, consentendo la programmazione di un **DOUBLE NAT BIDIREZIONALE**:

Ricordiamoci che non avendo default gateway, è necessario avere un indirizzo di appoggio in entrambe le VLAN, nell'esempio sotto:

Il PC di indirizzo 192.168.2.100 vedrà la CPU con l'indirizzo di appoggio 192.168.2.1

La CPU di indirizzo 192.168.1.1 vedrà il PC con l'indirizzo di appoggio 192.168.1.100



Entrambi i partner possono inizializzare la comunicazione e ricevere risposte

Figura 34: DOUBLE NAT Bidirezionale Principio comunicazione

A livello di programmazione dobbiamo semplicemente programmare un double NAT lasciando fleggati a ON sia il **BIDIRECTIONAL RULE** che l'**AUTOFIREWALL RULE**.

N.B.: In questo caso in cui il DOUBLE NAT è bidirezionale risulta necessario identificare due indirizzi liberi e univoci in ciascuna VLAN.

Mentre in un DOUBLE NAT in una sola direzione nella regola di SOURCE come TRANSLATED SOURCE IP SUBNET si potrebbe anche sfruttare l'indirizzo già presente dell'interfaccia dello scalance in quella VLAN.

Welcome admin	NETMAP Changes will b	e savec	l automatically	<u>in 34 se</u>	conds.Pres	ss 'Write Startup Config
Wizards	Masquerading	NAPT	Source NAT	NETM	AP	
Information			Type:	Destina	ition	~
▶ Svstem		Sou	urce Interface:	vlan2 (I	EXT)	~
Interfaces		Destina	tion Interface:	vlan1 (I	NT)	~
N avor 2	Translat	Sour	ce IP Subnet: ce IP Subnet:	0.0.0.0/	J	
FLayer 2	C	Destinati	on IP Subnet:	192.168	.2.1/32	
▼Layer 3	Translated D	Destinati	on IP Subnet:	192.168	.1.1/32	
▶ Static Routes				Z Bidire	ectional Rul	le
▶ Subnets				🗹 Auto	Firewall Ru	lle
► NAT				Select	Туре	Source Interface

Welcome admin	NETMAP Changes will b	e savec	i automatically	in 15 se	conds.Pres	s 'Write Startup Config' to
. Minorda	Masquerading	NAPT	Source NAT	NETMA	AP	
▶ vvizarus						
►Information			Type:	Source	-	~
• Svetom		Sou	urce Interface:	vlan2 (B	EXT)	~
Poystem		Destina	tion Interface:	vlan1 (I	NT)	~
►Interfaces		Sour	ce IP Subnet:	192.168	2.100/32	
▶Laver 2	Translat	ed Sour	rce IP Subnet:	192.168	.1.100/32	
,	0	Destinati	on IP Subnet:	0.0.0/0	0	
-Layer 3	Translated E	Destinati	on IP Subnet:			
 Static Routes 				Bidire	ectional Rul	e
▶ Subnets				🗹 Auto	Firewall Ru	le
► NAT				Select	Туре	Source Interface

Select	Туре	Source Interface	Destination Interface	Source IP Subnet	Translated Source IP Subnet	Destination IP Subnet	Translated Destination IP Subnet
	Source	vlan1	vlan2	192.168.1.1/32	192.168.2.1/32	0.0.0/0	-
	Destination	vlan1	vlan2	0.0.0/0	-	192.168.1.100/32	192.168.2.100/32
	Destination	vlan2	vlan1	0.0.0/0		192.168.2.1/32	192.168.1.1/32
	Source	vlan2	vlan1	192.168.2.100/32	192.168.1.100/32	0.0.0/0	-
4 entries.							

Figura 35: DOUBLE NAT Bidirezionale Esempio settaggio

Welcome admin	Internet Pr	rotoc	ol (IP) Rul	es									
Logout													
♦ Wizards	General Prede	fined I	Pv4 User Sp	ecific IP Sen	ices ICN	AP Service	es IP P	rotocols IP	Rul	es			
▶ Information	IP Version: IPv4 v												
▶ System	Rule Set:	-	✓ ∕ all										
►Interfaces	5	Select	Protocol	Action	From		То			Source (Range)	Destination (Range)	Service	Log
			IPv4	Accept	✓ vlan2	2 (EXT)	✓ vla	in1 (INT)	\sim	192.168.2.100/32	0.0.0.0/0	all	none
▶Layer 2			IPv4	Accept	✓ vlan ²	1 (INT)	✓ vla	in2 (EXT)	\sim	0.0.0/0	192.168.2.100/32	all	 none
▶Laver 3			IPv4	Accept	✓ vlan ²	1 (INT)	✓ yla	an2 (EXT)	\sim	192.168.1.1/32	0.0.0/0	all	 none
			IPv4	Accept	✓ vlan.	2 (EXT)	✓ vla	an1 (INT)	\sim	0.0.0/0	192.168.1.1/32	all	 none
✓Security	4	4 entries	S.										
▶Users													
▶Passwords	Create Del	lete	et Values Re	efresh									
►AAA													
▶ Certificates													
► Firewall													
			г:,):		. ++		n automatica		

Figura 36: DOUBLE NAT Bidirezionale Settaggio FIREWALL in automatico

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.