HOW TO

Configurare routing NAT

SIEMENS

Contents

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 USB0 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 (USB0 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.

	HW	FW
Scalance S615	6GK5 615-0AA00-2AA2	V06.03.00

N.B.: Guida e programmazione valida anche per Scalance M87x.(*) e SC600.

	HW	FW
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.**

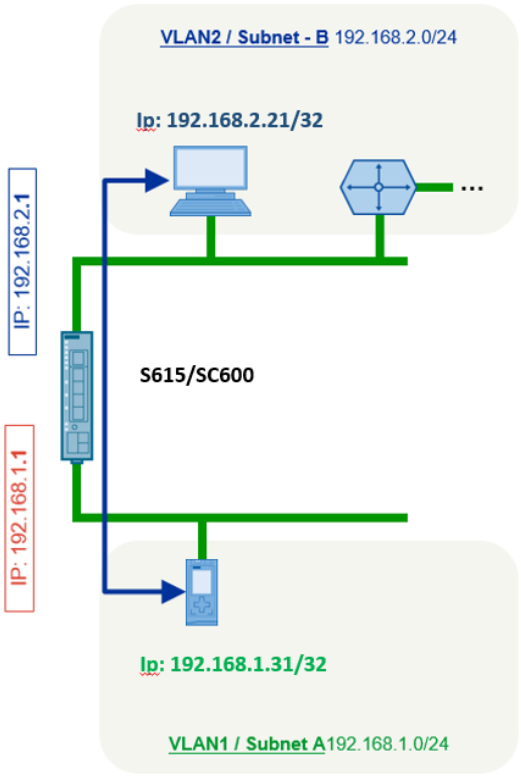


Figura 1: Schema base Routing

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.

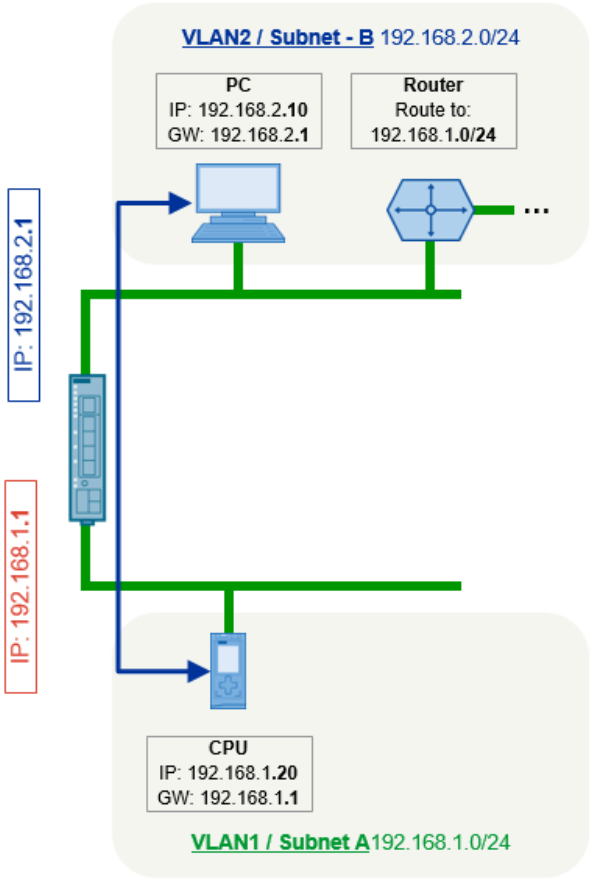


Figura 2: STANDARD routing

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.

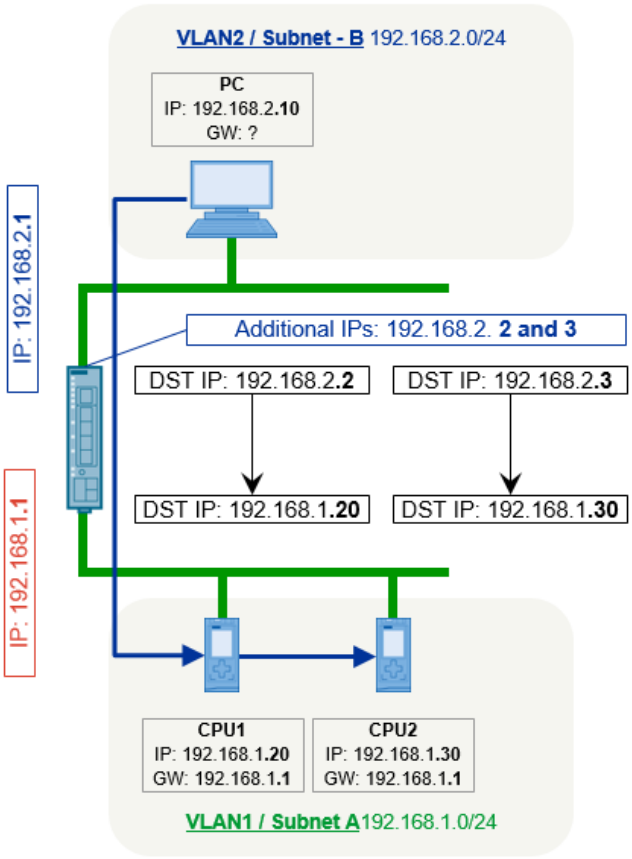


Figura 3: DESTINATION NAT

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.

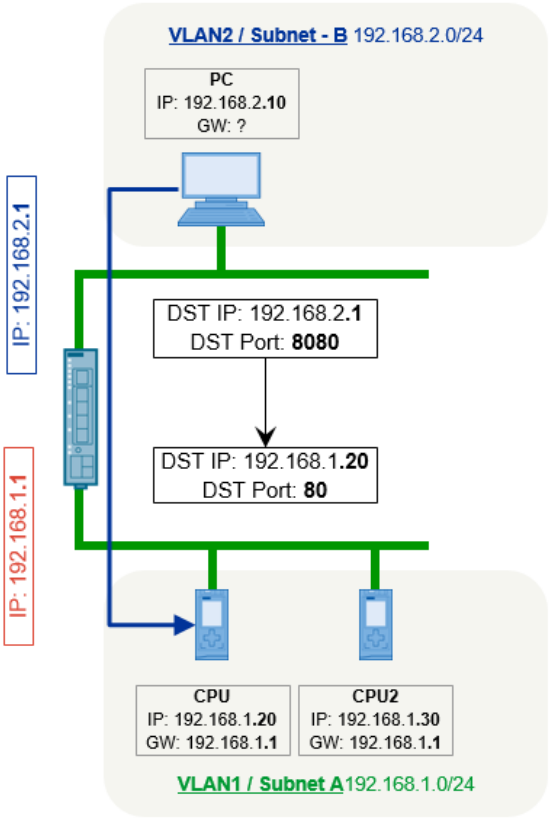


Figura 4: NAPT (Network Address Port Translation)

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.

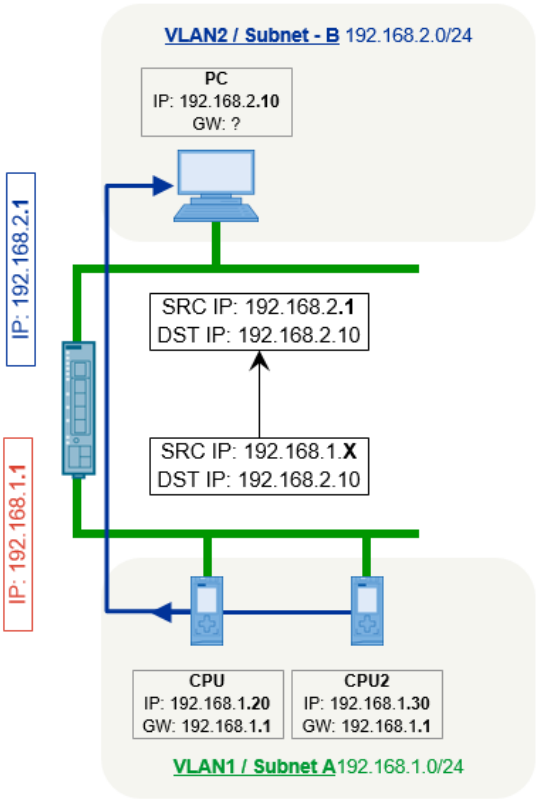


Figura 5: SOURCE NAT

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.

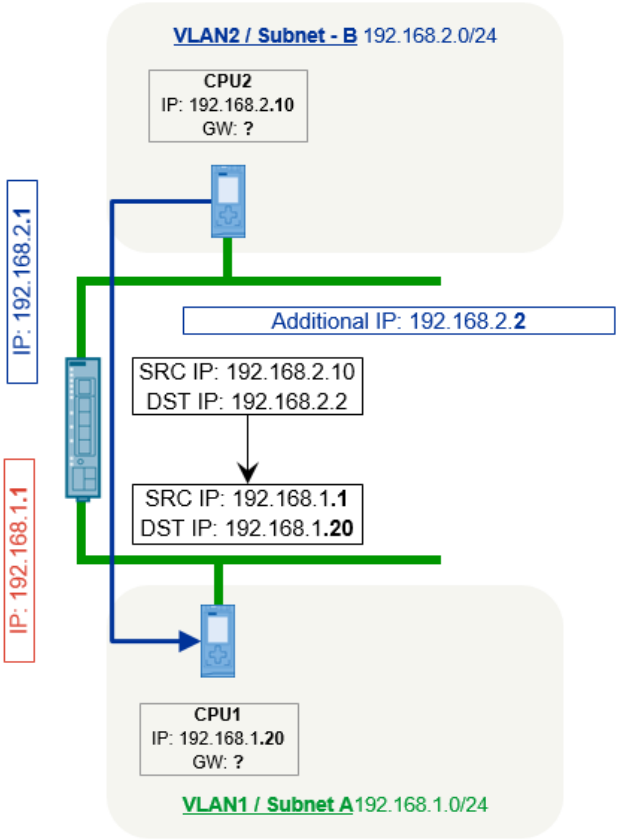


Figura 6: DOUBLE NAT

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: ↓			
SI		**STANDARD ROUTING**	**DESTINATION NAT NAPT**
NO		**SOURCE NAT**	**DOUBLE 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:

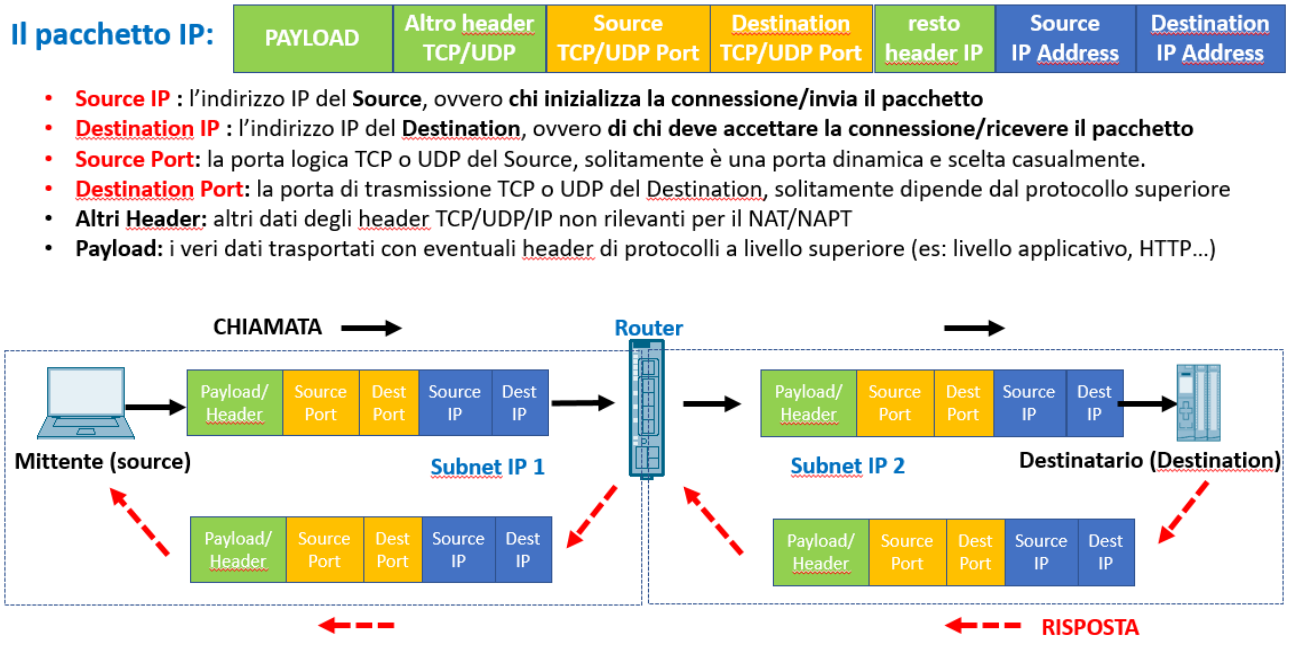


Figura 7: Schema comunicazione tra due devices in sottoreti diverse

Esempi di Programmazione

1.STANDARD ROUTING

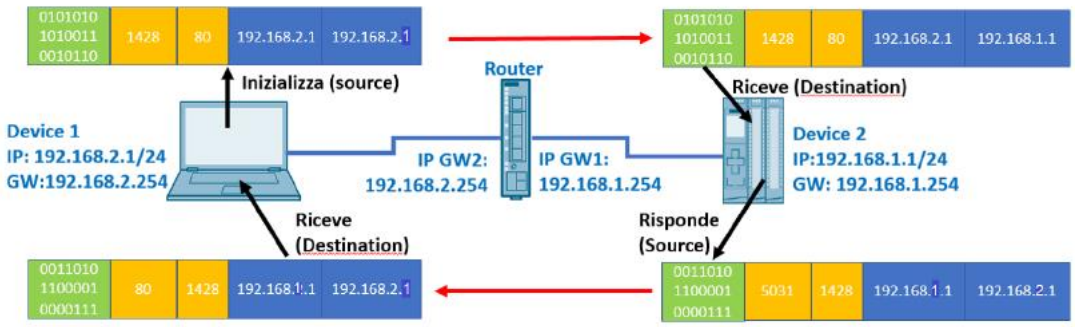


Figura 8: STANDARD Routing: Principio comunicazione

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**).

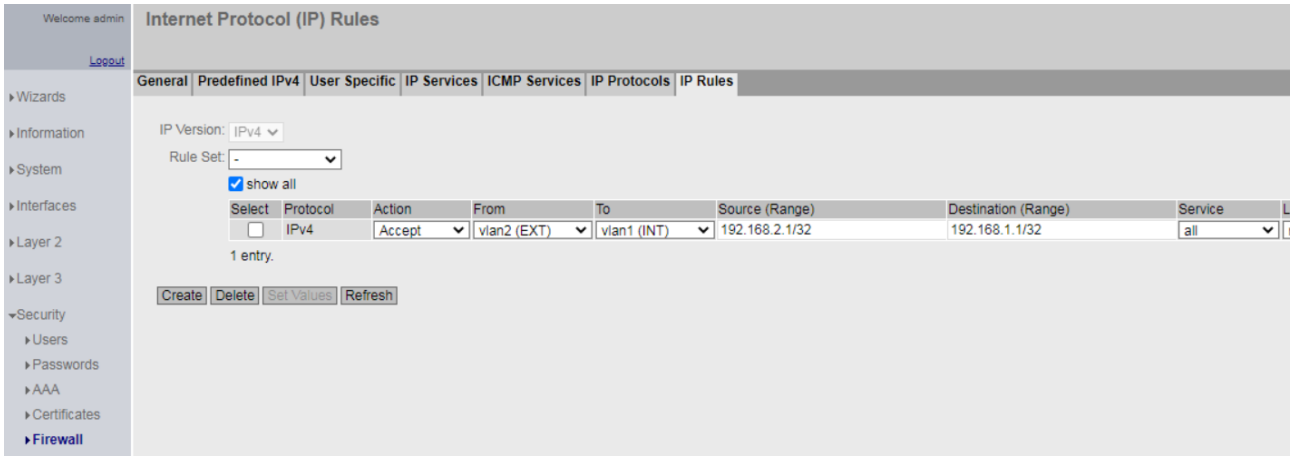


Figura 9: Settaggio IP FIREWALL Rules da solo Device1 a solo Device 2 su tutti i servizi.

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.

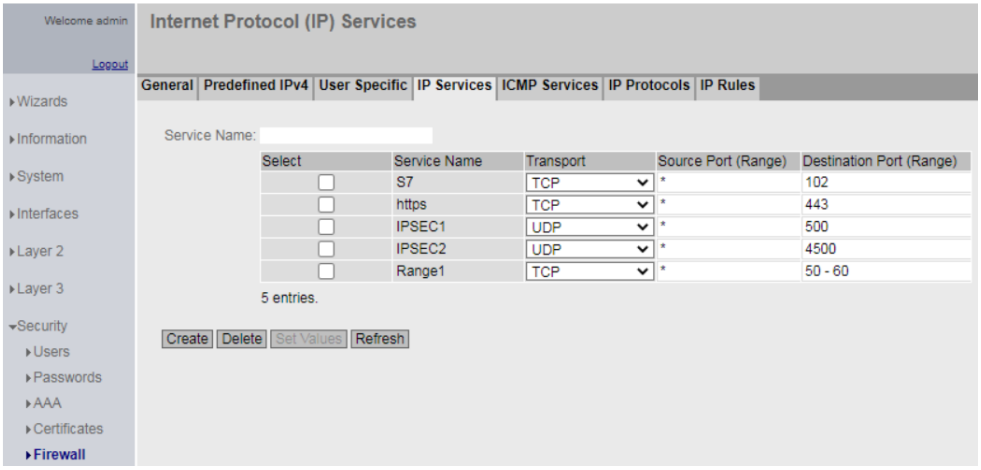


Figura 10: Esempio settaggio IP Services

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.

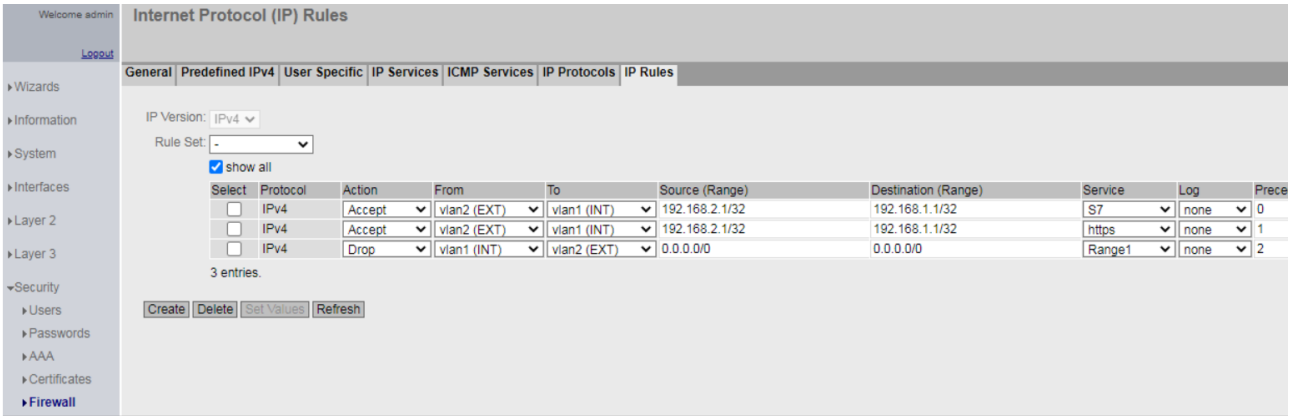


Figura 11: Esempio settaggio IP FIREWALL Rules

2.DESTINATION NAT (1:1)

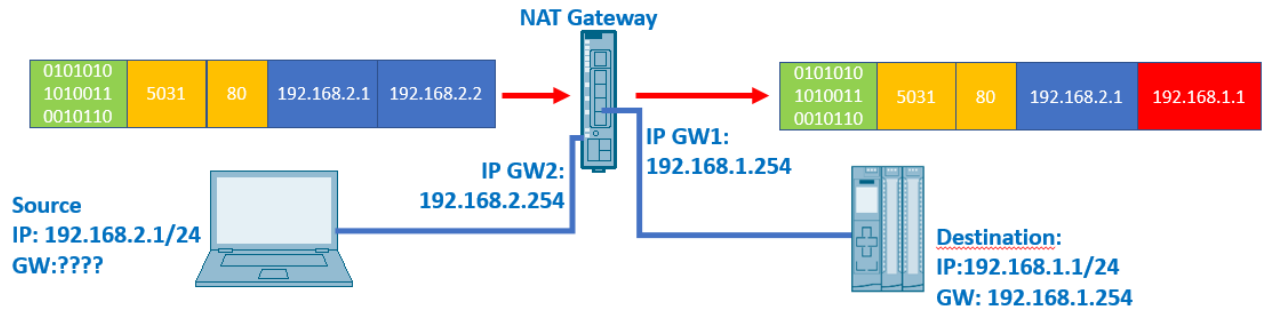
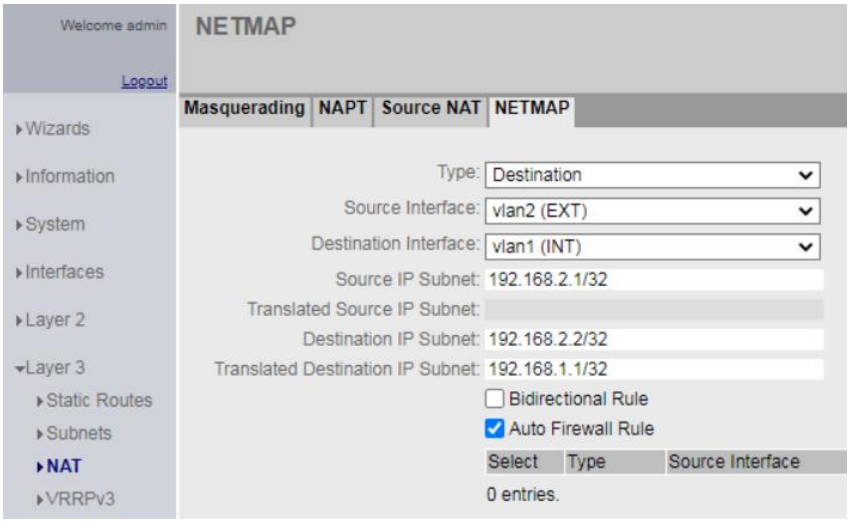


Figura 12: DESTINATION NAT Principio comunicazione

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 (sempre unico indirizzo con /32).



Select	Type	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	To	Source (Range)	Destination (Range)	Service	Log	Precedence	Assig
☐	IPv4	Accept	vlan2 (EXT)	vlan1 (INT)	192.168.2.1/32	192.168.1.1/32	all	none	0	

1 entry.

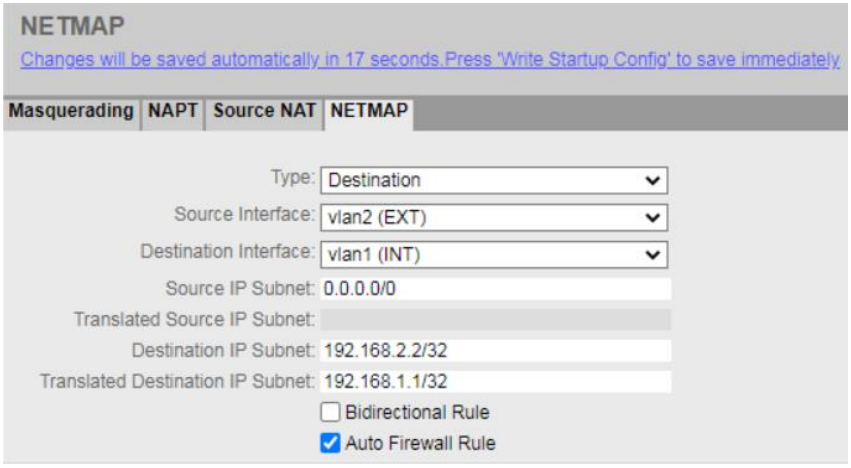
Figura 14: DESTINATION NAT Settaggio Automatico regola di Firewall da solo Device1 a Device 2 su tutti i servizi

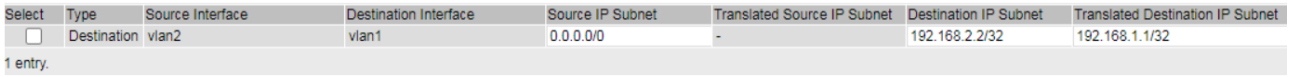
Anche qui ovviamente poi la risposta da DESTINATARIO a MITTENTE ritorna in automatico senza necessità di ulteriori settaggi né lato NETMAP né lato FIREWALL.

Settando nel campo SOURCE IP SUBNET :0.0.0.0/0, 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.





Select	Type	Source Interface	Destination Interface	Source IP Subnet	Translated Source IP Subnet	Destination IP Subnet	Translated Destination IP Subnet
☐	Destination	vlan2	vlan1	0.0.0.0/0	-	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	To	Source (Range)	Destination (Range)	Service	Log	Precedence
IPv4	Accept	vlan2 (EXT)	vlan1 (INT)	0.0.0.0/0	192.168.1.1/32	all	none	0

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.

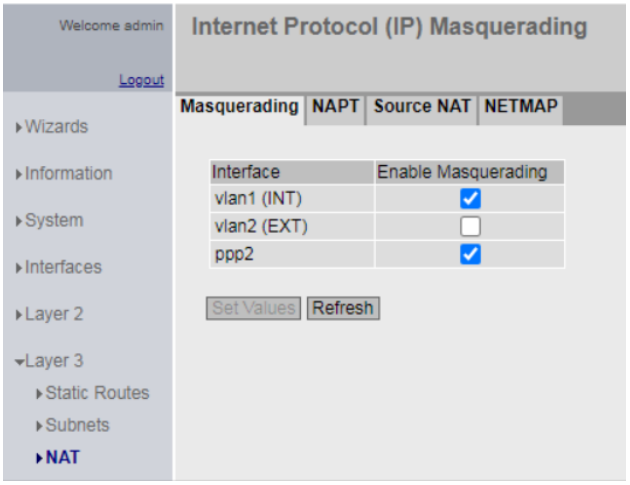


Figura 17: NAT MASQUERADING abilitato su VLAN 1

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).

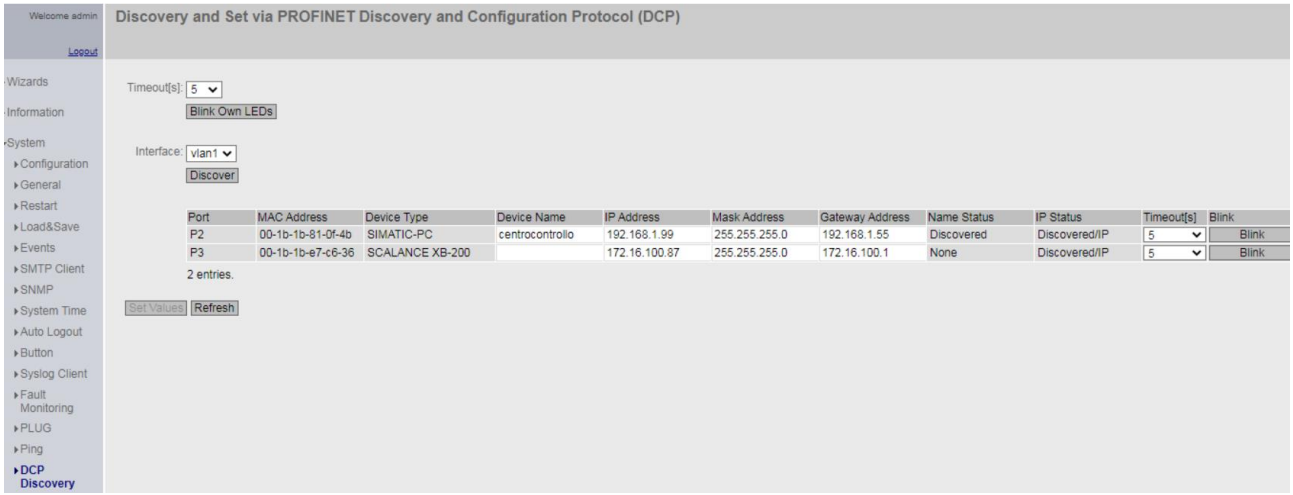


Figura 18: SYSTEM – DCP Discovery

3. NAPT (1:N) o PORT FORWARDING

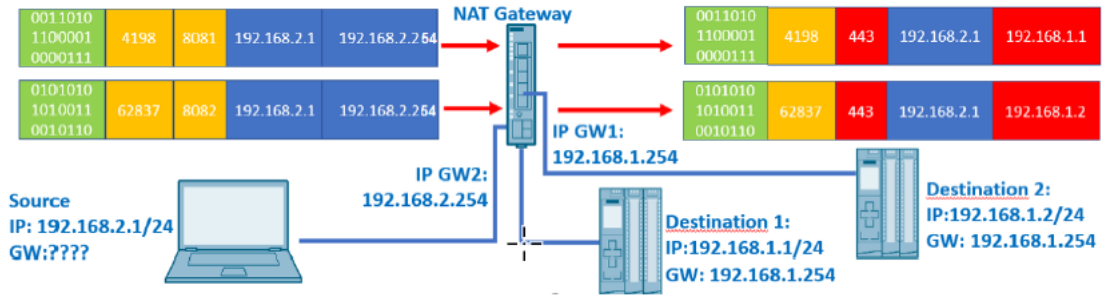


Figura 19: NAPT Principio comunicazione

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.**

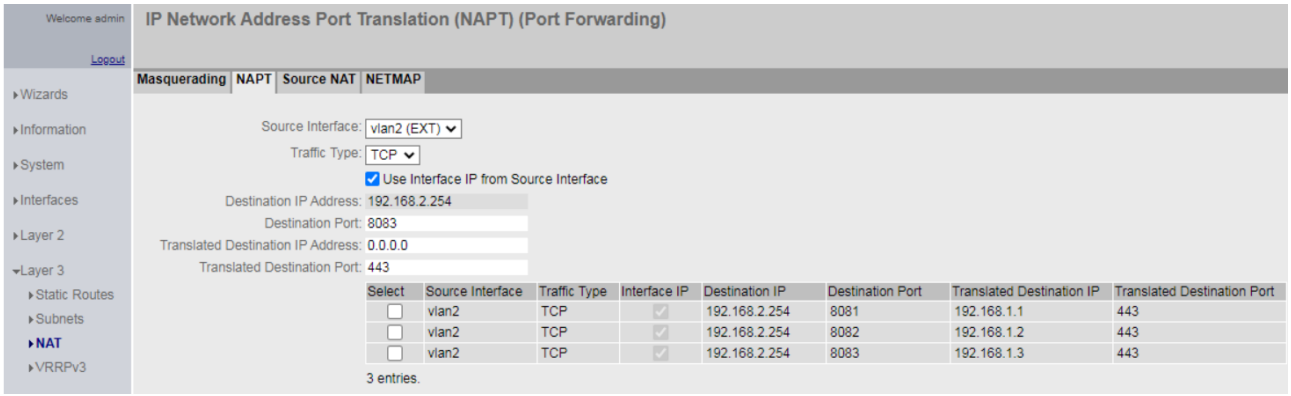


Figura 20: NAPT Esempio settaggio con DESTINATION IP = indirizzo IP S615 Source

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.

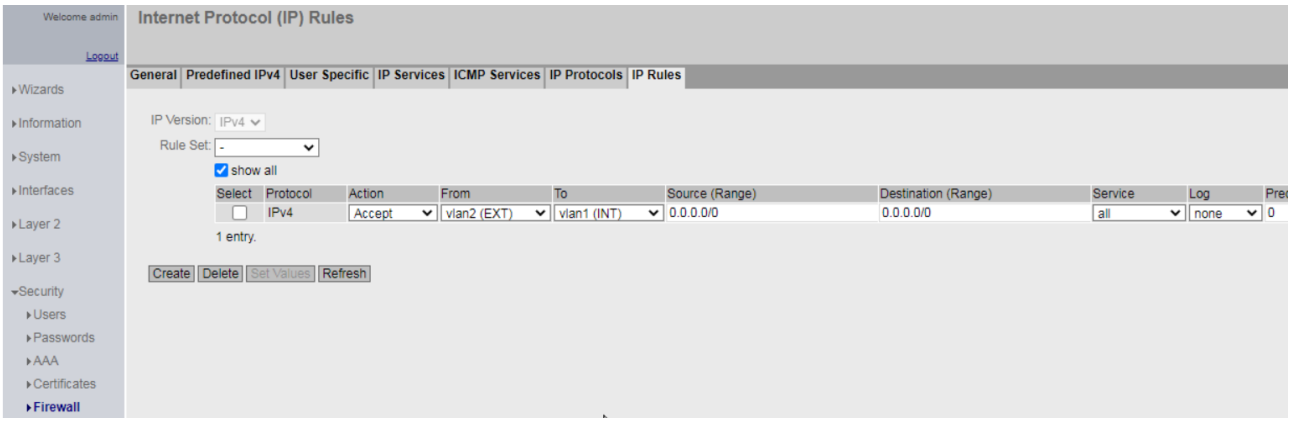


Figura 21: Settaggio FIREWALL da VLAN 2 a VLAN 1

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.

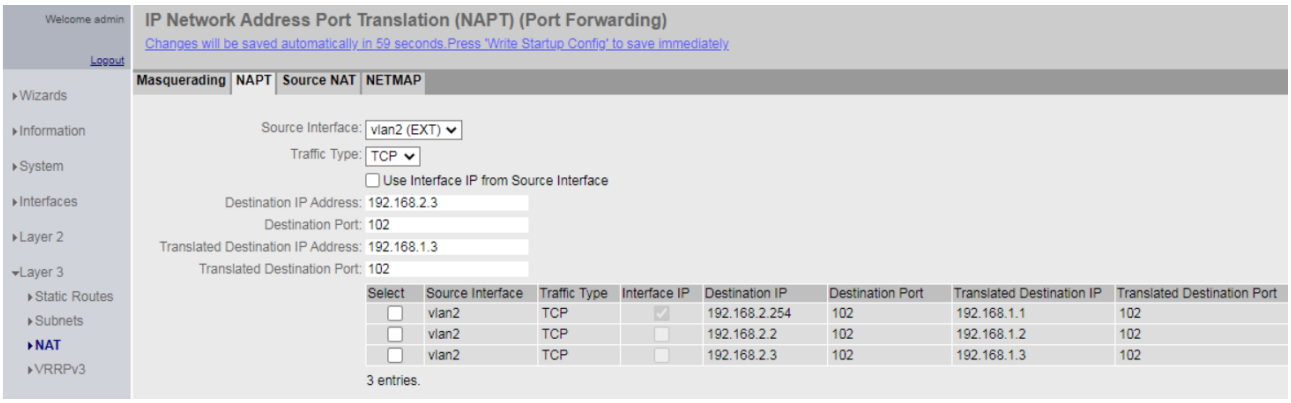


Figura 22: NAPT Esempio settaggio con anche DESTINATION IP diverso da indirizzo IP S615

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

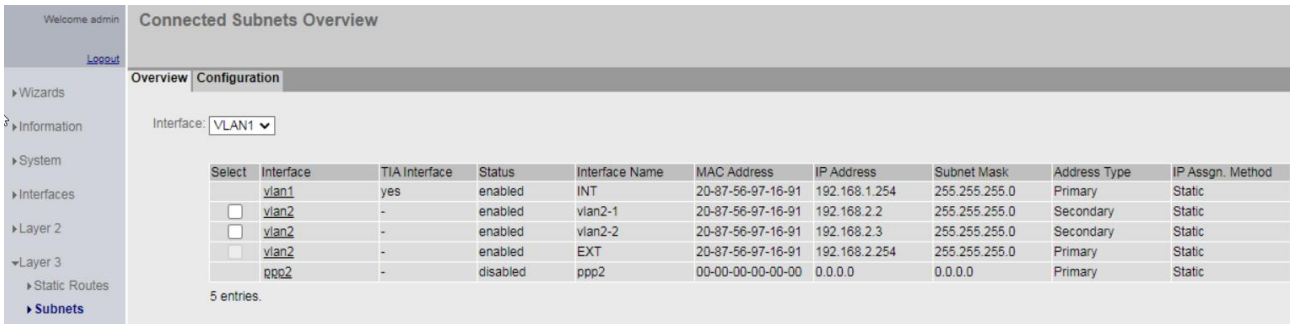


Figura 23: Definizione degli indirizzi IP 192.168.2.2 e 192.168.2.3 in VLAN 2

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.

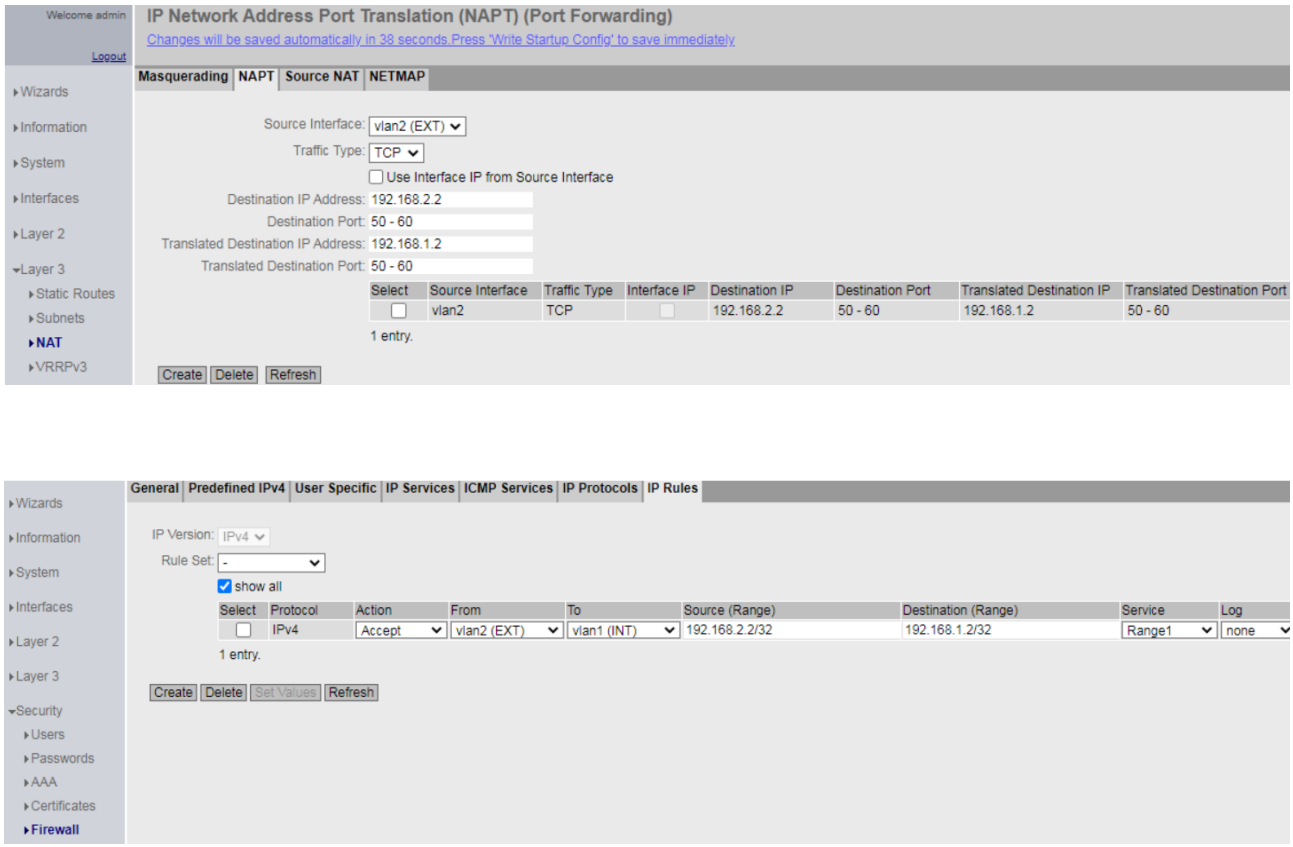


Figura 24: NAPT Esempio settaggio su un range di indirizzi

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

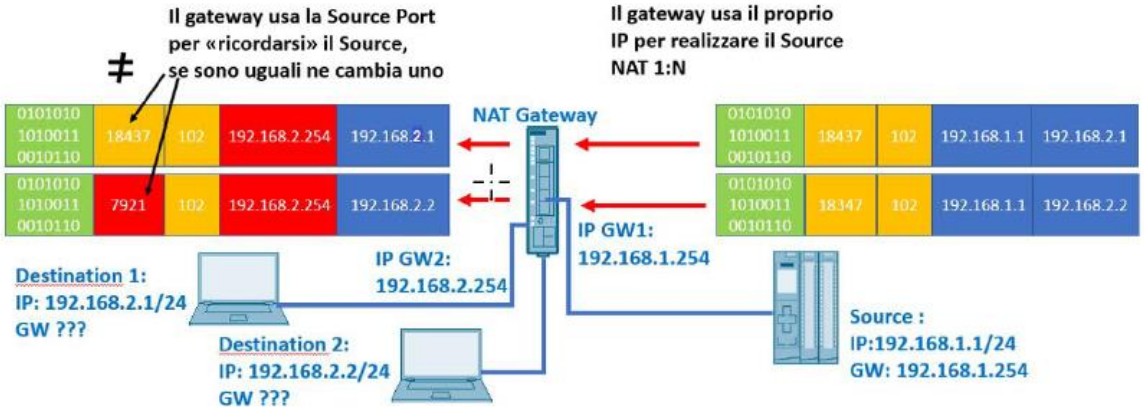
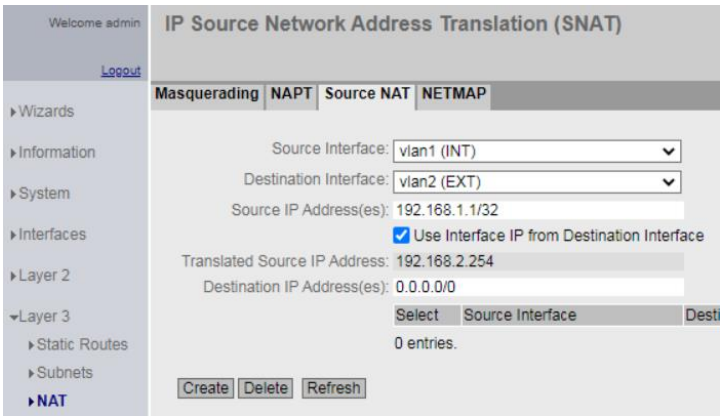


Figura 25: SOURCE NAT Principio comunicazione

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.



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	0.0.0.0/0

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.

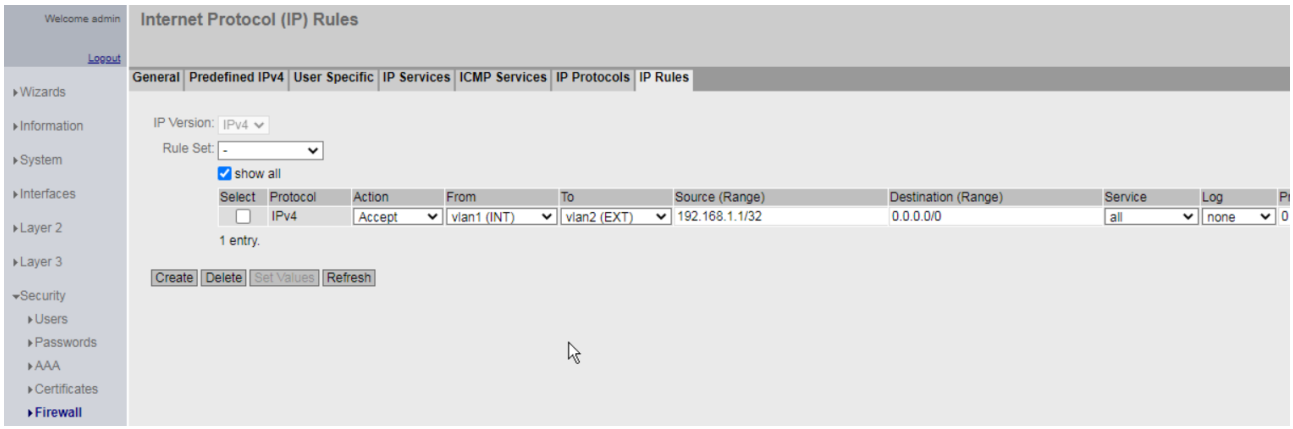


Figura 27: Settaggio FIREWALL da VLAN 1 (solo CP 192.168.1.1/32) a VLAN 2 (tutta)

5.DOUBLE NAT (1:1)

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

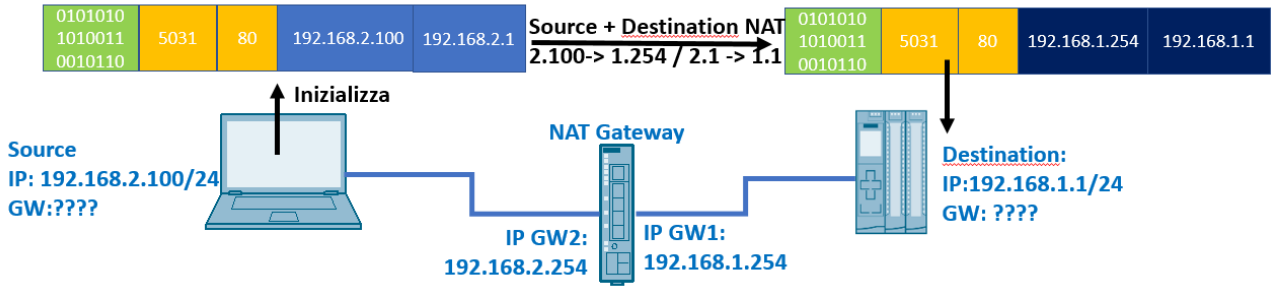
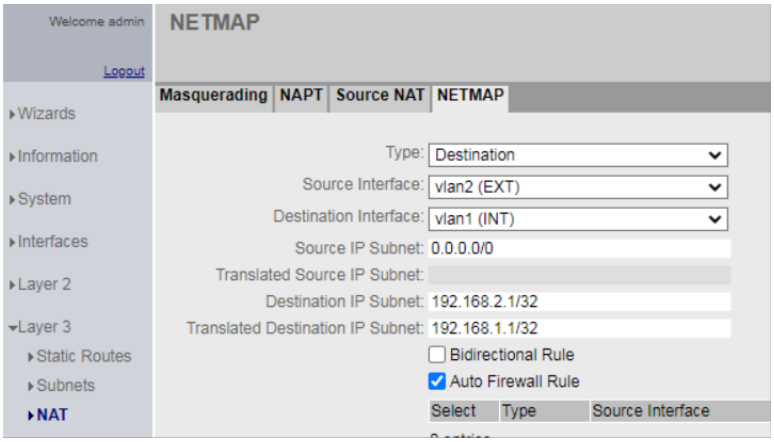
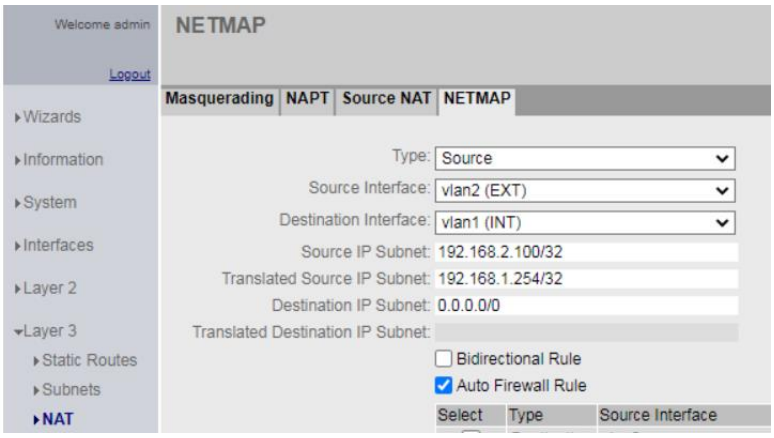


Figura 28: DOUBLE NAT Principio comunicazione

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.





Select	Type	Source Interface	Destination Interface	Source IP Subnet	Translated Source IP Subnet	Destination IP Subnet	Translated Destination IP Subnet
☐	Destination	vlan2	vlan1	0.0.0.0/0	-	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.

Figura 29: DOUBLE NAT Esempio settaggio

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

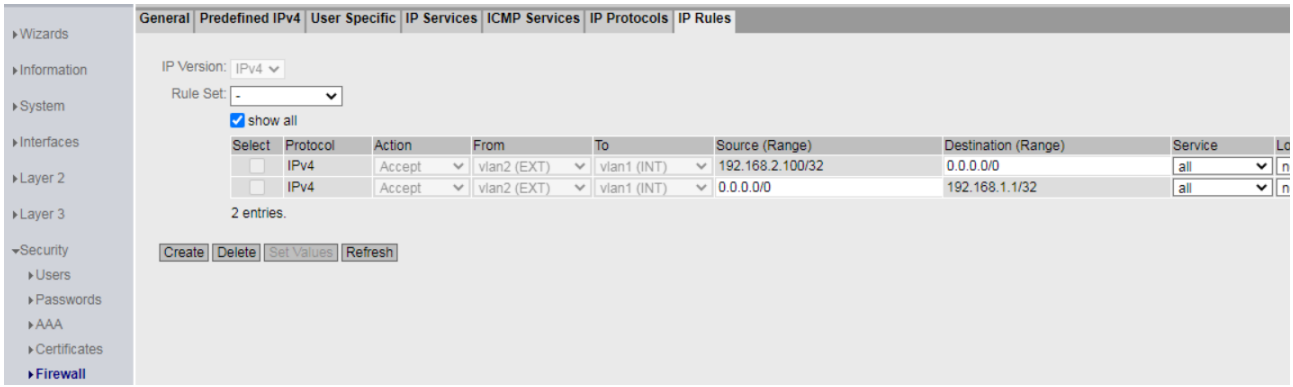


Figura 30: DOUBLE NAT Settaggio FIREWALL in automatico.

Il 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.

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.

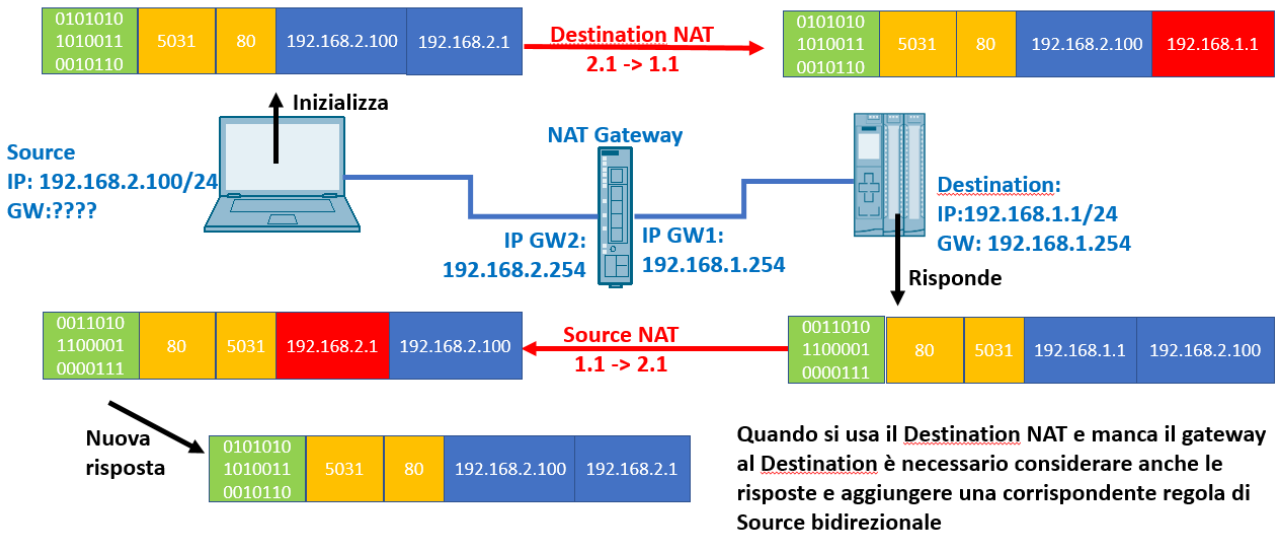
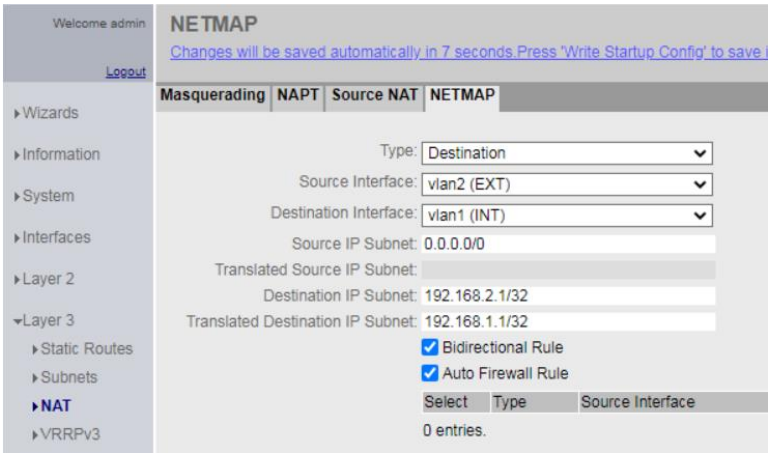


Figura 31: SOURCE & DESTINATION NAT Principio comunicazione.

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.



Select	Type	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	0.0.0.0/0	-
☐	Destination	vlan2	vlan1	0.0.0.0/0	-	192.168.2.1/32	192.168.1.1/32

2 entries.

Figura 32: SOURCE & DESTINATION NAT Esempio settaggio

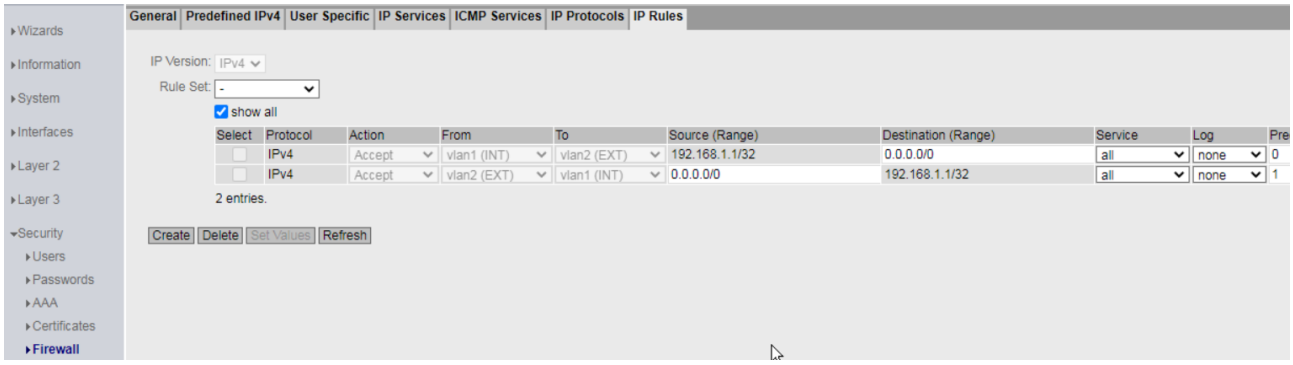


Figura 33: SOURCE & DESTINATION NAT Settaggio FIREWALL in automatico.

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

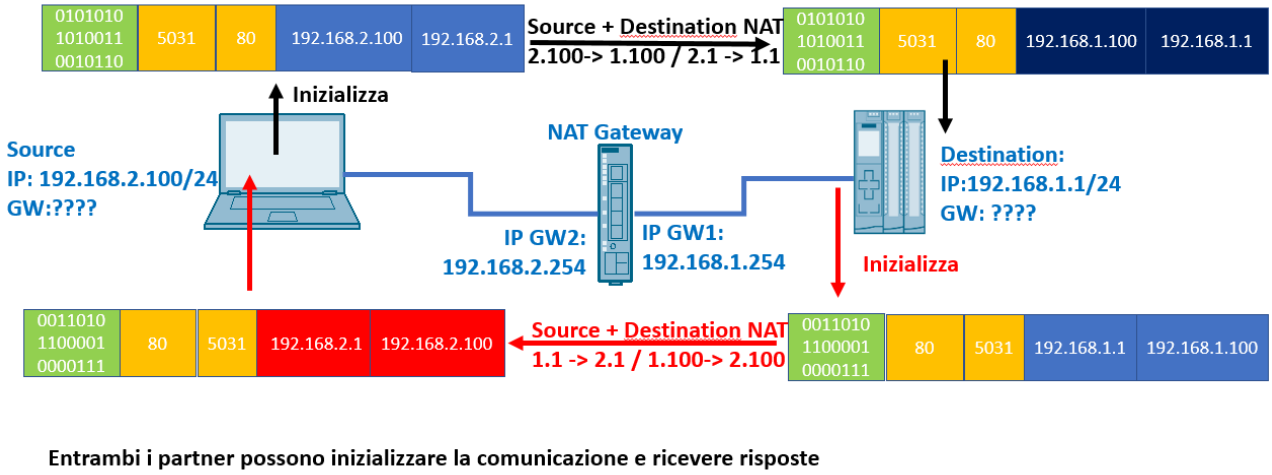
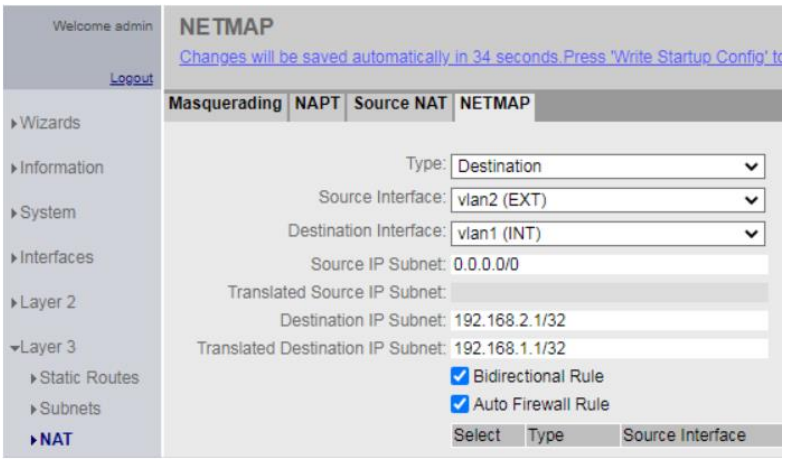


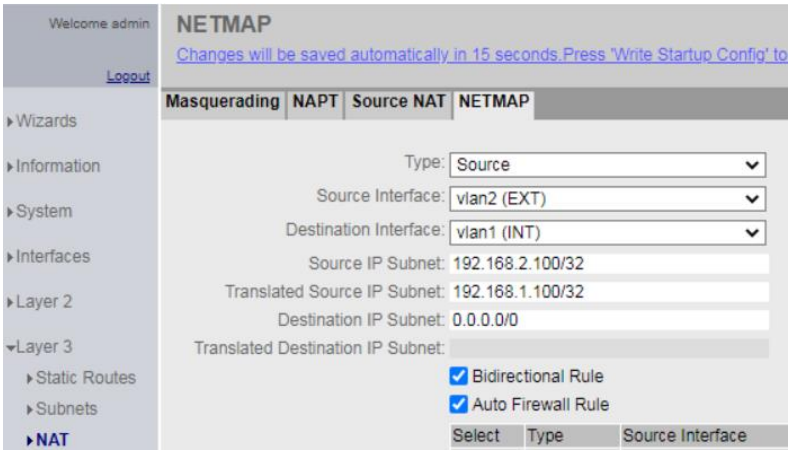
Figura 34: DOUBLE NAT Bidirezionale Principio comunicazione

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.





Select	Type	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	0.0.0.0/0	-
☐	Destination	vlan1	vlan2	0.0.0.0/0	-	192.168.1.100/32	192.168.2.100/32
☐	Destination	vlan2	vlan1	0.0.0.0/0	-	192.168.2.1/32	192.168.1.1/32
☐	Source	vlan2	vlan1	192.168.2.100/32	192.168.1.100/32	0.0.0.0/0	-

4 entries.

Figura 35: DOUBLE NAT Bidirezionale Esempio settaggio

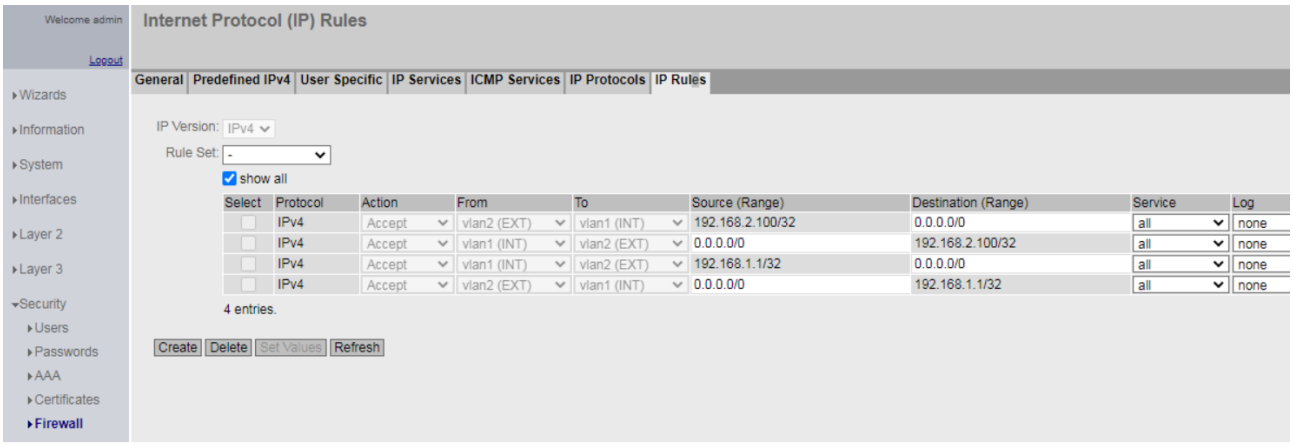


Figura 36: DOUBLE NAT Bidirezionale Settaggio FIREWALL in automatico