Come accedere alla rete di automazione da un PC (Rete cliente)

COM	IE ACCEDERE ALLA RETE DI AUTOMAZIONE DA UN PC (RETE CLIENTE)	1
1	INDICE	FINED.
2	INTRODUZIONE	2
3	COSA VI SERVE PER COMINCIARE	2
4	COME E DOVE COLLEGARE IL PLC	2
4.1 4.2	 Modo 1- Collegare il PLC direttamente sulla rete cliente Modo 2 – Collegare i PLC alla rete di macchina 	2 3
5	CONFIGURAZIONE DEL SITEMANAGER.	3
6	CONFIGURARE UNA ROUTE PER RAGGIUNGERE LA RETE DI AUTOMAZIONE	4
6.1	1 Modo1: Route statica configurata sul PC	4
6.2	2 MODO2: ROUTE STATICA CONFIGURATA NEL FIREWALL AZIENDALE	6
6.3	3 NOTE PER IL TROUBLESHOOTING	6
7	ACCESSO ALLA RETE MACCHINA CON REGOLA DI FORWARDING	7
7.1	1 CREAZIONE AGENT CUSTOM-FORWARDING	7
7.2	2 IMPOSTAZIONE REGOLA FORWARDING	9
7.3	3 ACCESSO ALLA WEB PAGE DEL PLC TRAMITE REGOLA DI FORWARDING	11



your partner

1 Introduzione

Questo documento vi spiega come accedere alla rete di automazione da un PC lato rete cliente, senza dipendere dalla connessione di teleassistenza, cioè anche se il gatemanager non è connesso ad internet.

Ciò può essere utile per esempio per realizzare una raccolta dati da uno Scada o se il cliente vuole da una postazione della sua azienda accedere via remote destkop (es. Vnc) ad un pannello operatore o al PC macchina. Per fornire al vs cliente invece un accesso dall'esterno è necessario che il cliente abbia la sua copia del software Linkmanager ed il suo certificato (Licenza 6041EU)

2 Cosa vi serve per cominciare

Prima di iniziare controllate che:

- Il SM sia stato configurato correttamente e i dispositivi di automazione siano attivi, collegati
 - e abbiano come Gateway l'indirizzo IP della porta DEV1 Del SiteManager
- Il Link Manager sia installato e possa connettersi ai dispositivi
- Il SM deve avere un indirizzo fisso e noto per la porta *uplink* tramite ip statico oppure tramite *DHCP*, assicurandosi che il DHCP assegni sempre il medesimo indirizzo al sitemanager

NOTA: annotatevi gli indirizzi IP delle interfacce di Uplink e Dev1 del Site Manager

3 Come e dove collegare il PLC

Esistono tre metodi per permettere un a PC lato cliente di raggiungere i dispositivi di automazione.

3.1 Modo 1- Collegare il PLC direttamente sulla rete cliente

Questo modo è sconsigliato e viene citato solo a titolo informativo. (normalmente lo si utilizza se non si è a conoscenza del modo N2). Infatti in questo modo si perde la separazione tra rete cliente e rete di automazione.

Si collegano tutti i dispositivi di automazione direttamente alla rete cliente sulla porta UPLINK, quindi la **porta DEV1 del Sitemanager rimane vuota.**

Si sfrutta, la possibilità del site manager di monitorare anche i dispositivi presenti sul lato cliente. Per utilizzare questa soluzione è sufficiente inserire nella pagina degli agents (*gatemanager->agents*) gli indirizzi IP (lato cliente) dei dispositivi



your partner



3.2 Modo 2 – Collegare i PLC alla rete di macchina

Questo metodo è quello più sicuro, perchè si mantiene la separazione tra rete cliente e rete di automazione. In questo caso i dispositivi di automazione sono su una rete diversa da quella cliente e sono collegati alla porta Dev1 del Sitemanager. (es. tramite uno Switch di macchina).

NOTA: Il PC lato cliente deve appartenere alla rete UPLINK e deve avere quindi un indirizzo IP appartenente alla stessa famiglia.

Supponiamo di avere configurato il Sitemanager nel seguente modo

Porta DEV1 IP: 128.127.60.4

Porta UPLINK1 IP: 192.168.26.93

Obiettivo: con il PC lato cliente che ha un indirizzo IP: 192.168.26.87, vogliamo raggiungere un pannello HMI, sulla rete di macchina che ha un indirizzo IP: 128.127.60.190.

4 Configurazione del SiteManager.

Il SiteManager come default, scarta tutto il traffico dalla rete macchina alla rete cliente e viceversa.

Al fine di mettere in comunicazione le due porte del Sitemanager occorre creare un Agent del tipo SCADA

- 1. Accedere all'interfaccia web del SiteManager e andare nella sezione GateManager \rightarrow Agents
- e creare un nuovo agente scegliendo come tipo Custom / Scada

Nota: E' possibile utilizzare solo un Agent Scada

		vaterianager i	nio - General • .	agenta - Device r	verays * 34		eo rioxy •	Junio	
				GateManager	Agents				
				Using 4 of 5 a	agents				
atus Disable	S/N D	evice Name	De	vice Type		Device IP & Par	ameters	c	omment
	#05 Sca	ia 👘	Custom	💙 Scada	×			C T T	
			10.00					in the second	





2. Inserire gli indirizzi IP, fino ad un massimo di nove, dei dispositivi che sono autorizzati ad attraversare il Sitemanager. Ciò permette di mantenere comunque un controllo e una certa sicurezza.

		GateManager	·Info • General • A	gents • Device R	elays + Server Rela	nys • Web Proxy • :	Status	
				GateManager	Agents			
				Using 4 of 5 a				
				Using 4 or 5 a	gents			
atus Disable	S/N	Device Name	Dev	ice Type	Device	IP & Parameters	Comment	
	#05	Scada	Custom	💉 Scada	192.168.26.8	7	e d	
			TP-1	The second second				

In questo modo autorizzo il PC ad accedere alla rete di macchina e quindi al pannello HMI

Il controllo è di tipo unidirezionale, per cui gli indirizzi IP inseriti potranno accedere alla rete automazione e non viceversa. Se invece vogliamo che un dispositivo presente nel lato automazione (es un pannello HMI) mandi dei dati ad un PC alla rete cliente, metteremo l'indirizzo IP del pannello HMI. In questo caso il PC potrà accedere al pannell HMI, ma non il contrario.

5 Configurare una route per raggiungere la rete di automazione

Il PC lato cliente deve sapere come raggiungere la rete macchina, a questo scopo è necessario "spiegargli" come raggiungere il PLC o altri dispositivi di automazione. Il site manager agisce come *router* tra la rete macchina e quella cliente. Ci sono due modi per implementare questa *route* permettendo questo tipo di comunicazione che normalmente il site manager blocca per ragioni di sicurezza.

5.1 Modo1: route statica configurata sul PC

Aggiungere una router statica da un prompt di ms-dos di un pc (WINXP/WIN7)

Nota: Con WinVista e Win7 è necessario aprire la finestra ms-dos con i diritti di Administrator.





Il comando è fatto da due parti:

1. l'indirizzo della rete macchina (DEV): è l'indirizzo del PLC con uno 0 come numero finale. Es. se il plc è 128.127.60.190 la rete sarà 128.127.60.0

2.	L'indirizzo della porta UPLI	NK del site	manager (Es.192.	168.26.93)
	Amministratore: Prompt dei comandi			
	Microsoft Windows EVersione 6.0 Copyright (c) 2006 Microsoft Co	0.6001] prporation. Tu	utti i diritti risen	•vati.
	C:\Users\PCLAB.DIREL>route add	128.127.60.0	mask 255.255.255.0	192.168.26.93
		1		1
	Dev Network	UPLI	NK IP Address	

A questo punto, dal PC dovrebbe essere possibile fare ping verso il pannello e comunicare normalmente.

- NOTA: il comando indicato non sopravvive ad un reboot del PC. E' quindi consigliabile inserirlo in un file batch oppure utilizzare l'opzione **-p** che lo rende persistente al reboot.
- ES. route -p add 128.127.60.0 mask 255.255.255.0 192.168.26.93

an Amministratore: Prompt dei comandi	8 24	B	
Minimo = 2ms, Massimo = 2ms, Me	dio = 2ms		
C:\Users\PCLAB.DIREL>route print			
Elenco interfacce 1100 25 b3 cf ab 35 Inte 1 Soft 1000 00 00 00 00 00 00 e0 6T04 1300 00 00 00 00 00 00 e0 isat IPv4 Tabella route	l(R) 82566DM-2 Gig ware Loopback Inte Adapter ap.DIREL.LOC	abit Network Co rface 1	nnection
Route attive: Indirizzo rete Mask 0.0.0.0 0.0.0.0 127.0.0.0 255.0.0.0 127.0.0.1 255.255.255.255	Gateway 192.168.26.5 On-link On-link	Interfaccia 192.168.26.87 127.0.0.1 127.0.0.1 127.0.0.1	====== Metrica 10 306 306
122.255.255.255.255.255.255.255.255.128.127.60.0 255.255.255.2	On-link 192.168.26.93	122.0.0.1	306
192.168.26.0 255.255.255.0	On-link	192.168.26.87	266

Attraverso una finestra Dos se digitiamo il comando **route print** possiamo vedere gli indirizzi della route aggiunta.



5.2 Modo2: route statica configurata nel firewall aziendale

Se invece del solo Pannello HMI, si vuole avere accesso a vari dispositivi di automazione, da diversi PC lato cliente, è possibile evitare di inserire il comando precedente su ogni PC. E' sufficiente chiedere al vostro responsabile IT di inserire questa route nel vs *router/firewall* aziendale.

5.3 Note per il Troubleshooting

A titolo di Troubleshooting, se andiamo nella finestra di Status del Sitemanager

Indirizzo 🧃	https://128.127.60.4	~
	SiteManager secomea	
	SETUP • System GateManager VPN Routing Maintenance Status Log •	HELP
	Status Info • System • Tunnels • GateManager • Network • Extended • Ping/Trac	e
	Status Information	
	System: View information about the appliance, including current firmware version and time.	
	Tunnels: View tunnel status. See the on-line help for details.	
	GateManager: View GateManager status.	
	Network : View information about the network interfaces , such as IP and MAC addresses, traffic statistics, and ARP table entries.	
	Extended: View various currently active settings in the system as an aid in advanced troubleshoo	ting.
	Ping/Trace : This is a tool that allows you to test connectivity using Ping or TraceRoute without having to leave the management interface.	

e selezioniamo la voce Extended,

		Sec	UB1 omec	101	hut	jer				
				SE	TUP .	System	GateManager	VPN Routing Mainten	ance Status Log • HELP	
					State	s Info • 5	System • Tunnels	• GateManager • Network	Extended • Ping/Trace	
14	840	ACCEPT	all		*	*	0.0.0.0/0	0.0.0/0	state RELATED . ESTABLISHED	
z	120	FWA forw	all		*	*	0.0.0.0/0	0.0.0/0		
2	120	SCA_forw	all		*	*	0.0.0.0/0	0.0.0/0		
Chain	OUTPU	(policy	ACCEPT	442	packet	.s, 98912	bytes)			
pkts	bytes	target	prot	opt	in	out	source	destination		
Chain	FWA E	orw (1 ref	ference	s)						
pkts	bytes	target	prot	opt	in	out	source	destination		
Chain	SCA f	orw (1 ref	terence	s)						
pkts	bytes	target	prot	opt	in	out	source	destination		
2	120	ACCEPT	all		*	*	192.168.26.87	0.0.0/0		
0	0	ACCEPT	all	-	*	*	128.127.60.4	0.0.0/0		
7	MANGLE	TABLE	_							
hain	MANGLE PRERO	TABLE	- Licy AC	CEPT	33918	packets,	3410K bytes)	10.00 M		
hain	MANGLE PRERO bytes	TABLE JTING (pol target	- licy AC prot	CEPT opt	33918 in	packets, out	3410K bytes) source	destination	_	
hain pkts 33918	MANGLE PRERO bytes 3410K	TABLE JTING (pol target IPSEC	- licy AC prot all	CEPT opt 	33918 in *	packets, out *	3410K bytes) source 0.0.0.0/0	destination 0.0.0.0/0		
hain pkts 33918 Chain	MANGLE PRERO bytes 3410K INPUT	TABLE JTING (pol target IPSEC (policy Å	- prot all LCCEPT	CEPT opt 3390	33918 in * 2 packs	packets, out *	3410K bytes) source 0.0.0.0/0 K bytes)	destination 0.0.0.0/0		
Chain pkts 33918 Chain pkts	MANGLE PRERO bytes 3410K INPUT bytes	TABLE JTING (pol target IPSEC (policy # target		CEPT opt 3390 opt	33918 in * 2 packs in	packets, out * ats, 3409 out	3410K bytes) source 0.0.0.0/0 K bytes) source	destination 0.0.0.0/0 destination		
Chain pkts 33918 Chain pkts Chain	MANGLE PRERO bytes 3410K INPUT bytes FORWA	TABLE JTING (pol target IPSEC (policy & target RD (policy		CEPT opt 3390 opt T 16	33918 in * 2 packs in packs	packets, out * ats, 3409 out :s. 960 b	3410K bytes) source 0.0.0.0/0 K bytes) source vtes)	destination 0.0.0.0/0 destination		
Chain pkts 33918 Chain pkts Chain pkts	MANGLE PRERO bytes 3410K INPUT bytes FORWA bytes	TABLE	- prot all CCEPT prot ACCEP prot	CEPT opt 3390 opt T 16 opt	33918 in * 2 packs in packet in	packets, out * ats, 3409 out is, 960 b out	3410K bytes) source 0.0.0.0/0 K bytes) source ytes) source	destination 0.0.0.0/0 destination destination		
Chain pkts 33918 Chain pkts Chain pkts 0	HANGLE PRERO bytes 3410K INPUT bytes FORWA bytes 0	TABLE	- prot all CCEPT prot ACCEP prot tep	CEPT opt 3390 opt T 16 opt 	33918 in * 2 packs in packet in *	packets, out * ats, 3409 out ss, 960 b out *	3410K bytes) source 0.0.0.0/0 K bytes) source ytes) source 0.0.0.0/0	destination 0.0.0.0/0 destination 0.0.0.0/0	tep flags:0x06/0x02 TCPMS8 clamp to PMTU	
Chain pkts 33918 Chain pkts Chain pkts O Chain	HANGLE PRERO bytes 3410K INPUT bytes FORWA bytes 0 . OUTPU	TABLE	- licy AC prot all CCEPT prot tcp ACCEPT	CEPT opt 3390 opt T 16 opt 227	33918 in * 2 packo in packet in * 14 pack	packets, out * ats, 3409 out ts, 960 b out * *	3410K bytes) source 0.0.0.0/0 K bytes) source ytes) source 0.0.0.0/0 3K bytes)	destination 0.0.0.0/0 destination destination 0.0.0.0/0	tep flags:0x06/0x02 TCPMSS clamp to PHTU	
Chain pkts 33918 Chain pkts Chain pkts 0 Chain pkts	HANGLE PRERO bytes 3410K INPUT bytes FORWA bytes 0 . OUTPU bytes	TABLE target IPSEC (policy & target RD (policy target TCPMSS F (policy target	- licy AC prot all CCEPT prot top ACCEPT prot	CEPT opt 3390 opt T 16 opt 227 opt	33918 in 2 packs in packet in * 14 pack	packets, out * ats, 3409 out cs, 960 b out * *	3410R bytes) source 0.0.0.0/0 K bytes) source ytes) source 0.0.0.0/0 Sk bytes) source	destination 0.0.0.0/0 destination destination 0.0.0.0/0 destination	tcp flags:0x06/0x02 TCPMSS clamp to PMTU	
Chain pkts 33918 Chain pkts Chain pkts 0 Chain pkts 22714	MANCLE PREROU bytes 3410K INPUT bytes FORWA bytes 0 . OUTPU bytes 1913K	TABLE target IPSEC (policy & target RD (policy target TCPMSS F (policy target IPSEC	- licy AC prot all ACCEPT prot tcp ACCEPT prot all	CEPT opt 3390 opt T 16 opt 227 opt 	33918 in * 2 packet in * 14 pack in *	packets, out * ats, 3409 out * * tets, 960 b * * tets, 191 out *	3410K bytes) source 0.0.0.0/0 K bytes) source ytes) source 0.0.0.0/0 3K bytes) source 0.0.0.0/0	destination 0.0.0.0/0 destination 0.0.0.0/0 destination 0.0.0.0/0	tcp flags:0x06/0x02 TCPNSS clamp to PHTU	
Chain pkts 33918 Chain pkts O Chain pkts 22714 Chain	MANGLE PREROU bytes 3410K INPUT bytes FORWA bytes 0 . OUTPU bytes 1913K	TABLE		CEPT opt 3390 opt T 16 opt 227 opt CCEP	33918 in * 2 packet in packet in * 14 pack in * T 22730	packets, out * out ss, 3409 out * * kets, 3409 out * * * * * * * * * * * * * * * * * * *	3410K bytes) source 0.0.0.0/0 K bytes) source ytes) source 0.0.0.0/0 3K bytes) source 0.0.0.0/0 , 1914K bytes)	destination 0.0.0.0/0 destination 0.0.0.0/0 destination 0.0.0.0/0	tep flags:0x06/0x02 TCPNSS clamp to PHTU	
Chain pkts 33918 Chain pkts 0 Chain pkts 22714 Chain pkts	MANCLE PRERO bytes 3410K INPUT bytes 0 0 0 0 0 0 0 0 0 0 0 0 0	TABLE JTING (pol target (policy & target RD (policy target TCPHSS ((policy target TPSEC DUTING (pol target		CEPT opt 3390 opt T 16 opt 227 opt CCEP opt	33918 in * 2 packet in * 14 pack in * 14 pack in *	packets, out * sts, 3409 out sts, 960 b out * tets, 191 out *	3410K bytes) source 0.0.0.0/0 K bytes) source source 0.0.0.0/0 3K bytes) source 0.0.0.0/0 , 1914K bytes) source	destination 0.0.0.0/0 destination 0.0.0.0/0 destination 0.0.0.0/0 destination	tcp flags:0x06/0x02 TCPMSS clamp to PHTU	
hain pkts 33918 Chain pkts Chain pkts 22714 Chain pkts	MANCLE PRERO bytes 3410K INPUT bytes 0 0 0 0 0 0 0 0 0 0 0 0 0	TABLE	- iicy AC prot all ACCEPT prot tcep ACCEPT prot all blicy A prot	CEPT opt 3390 opt T 16 opt 227 opt CCEP opt	33918 in * 2 packet in packet in * 14 pack in * T 22730	<pre>packets, out * ats, 3409 out cs, 960 b out * tets, 191 out * out *</pre>	3410K bytes) source 0.0.0.00 source source 0.0.0.0/0 3K bytes) source 0.0.0.0/0 , 1914K bytes) source	destination 0.0.0.0/0 destination 0.0.0.0/0 destination 0.0.0.0/0 destination	tep flags:0x06/0x02 TCPNSS clamp to PHTU	

Contatore pacchetti



your partner

Tel +390362-55.3265 <u>tecnico@gate-manager.it</u> www.direl.it Via Ferrini, 8 - 20031 Cesano Maderno (MI)

Pagina 6



possiamo vedere la regola aggiunta creando l'Agent Scada.

Se provo ad eseguire dei Ping dal PC (IP:192.168.26.87) al pannello HMI (IP:128.127.60.190), vedremo crescere il valore del contatore, in caso contrario occorre riguardare i passaggi inerenti la creazione della Route

6 Accesso alla rete macchina con regola di Forwarding

Come metodo alternativo è possibile accedere alla rete di automazione dalla rete del cliente anche attraverso un agent di tipo CUSTOM - FORWARDING.

Il vantaggio rispetto all'utilizzo dell'agent SCADA è che non è richiesta nessuna modifica sul PC cliente, in quanto non è necessario installare nessuna rotta da prompt di MS-DOS.

A titolo di esempio supponiamo di voler visualizzare tramite Browser la WEB Page ad un PLC dotato di interfaccia Web da un PC collegato alla porta *UPLINK*, cioè alla rete cliente.

6.1 Creazione Agent CUSTOM-FORWARDING

Una volta entrati nel Setup del SiteManager Selezioniamo alla voce *Device Agents* il pulsante *Fix*, nel caso non siano presenti *Agents* o *Edit*, nel caso sia già presente un agent.

About SiteManager 3429 - Setup Assistant 1. GateManager: 95.174.29.2 Connected to 95.174.29.2:443 (UPLINK) Edit 2. Uplink port: 192.168.26.84/24 Up Edit 3. Uplink2 (2G/3G/4G): Not Installed Edit 4. DE¥ port: 10.0.0.1/24 [default] Edit 5. Device Agents: No agents defined Fix 6. Chat / Scratchpad: Empty Edit				
SiteManager 3429 - Setup Assistant 1. GateManager: 95.174.29.2 2. Uplink port: 192.168.26.84/24 3. Uplink2 (2G/3G/4G): Not Installed 4. DE¥ port: 10.0.0.1/24 [default] 5. Device Agents: No agents defined 6. Chat / Scratchpad: Empty		-	lbout	
1. GateManager: 95.174.29.2 Connected to 95.174.29.2:443 (UPLINK) Edit 2. Uplink port: 192.168.26.84/24 Up Edit 3. Uplink2 (2G/3G/4G): Not Installed Edit 4. DEV port: 10.0.0.1/24 [default] Edit 5. Device Agents: No agents defined Fix 6. Chat / Scratchpad: Empty Edit		SiteManager 34	29 - Setup Assistant	
I. GateManager: 95.174.29.2 Connected to 95.174.29.2:443 (UPLINK) Edit 2. Uplink port: 192.168.26.84/24 · Up Edit 3. Uplink2 (2G/3G/4G): Not Installed Edit 4. DEV port: 10.0.0.1/24 [default] Edit 5. Device Agents: No agents defined Fix 6. Chat / Scratchpad: Empty Edit				
2. Uplink port: 192.168.26.84/24 Up Edit 3. Uplink2 (2G/3G/4G): Not Installed Edit 4. DEV port: 10.0.0.1/24 [default] Edit 5. Device Agents: No agents defined Fix 6. Chat / Scratchpad: Empty Edit	1. GateManager:	95.174.29.2	Connected to 95:174.29.2:443 (UPLINK)	Edit
3. Uplink2 (2G/3G/4G): Not Installed Edit. 4. DEV port: 10.0.0.1/24 [default] Edit. 5. Device Agents: No agents defined Fix. 6. Chat / Scratchpad: Empty Edit.	2. Uplink port:	192.168.26.84/24	Up	Edit
4. DEV port: 10.0.0.1/24 [default] Edit 5. Device Agents: No agents defined Fix 6. Chat / Scratchpad: Empty Edit	3. Uplink2 (2G/3G	/4G):	Not Installed	Edit
5. Device Agents: No agents defined Fix 6. Chat / Scratchpad: Empty Edit	4. DEV port:	10.0.0.1/24 [default]		Edit
6. Chat / Scratchpad: Empty Edit	5. Device Agents:		No agents defined	Fix
	6. Chat / Scratchp	ad: Empty		Edit





Selezioniamo il tasto New per creare e configurare un nuovo Agent

SiteManager sectmen	
SETUP • System GateManager VPN Routing Maintenance Status Log • HELP	
GateManager Agents - Setup Assistant	
You can configure an agent to monitor a device connected to the SiteManager Serial port and TCP/IP enabled devices located on either the DEV network or Uplink network of the SiteManager.	
Click [New], and give the Agent a name (this name will be what the LinkManager user will see), and select a suitable device type (first vendor, then model). Then click on 📇 to specify the device address and other relevant parameters.	
The SiteManager will instantly try to connect to the device, and if successful the Agent will go IDLE and appear on the GateManager and any LinkManager that have been granted access to the domain of the SiteManager.	
If not successful, the Agent will report an error, and the agent will not be registered on the GateManager and subsequently not on LinkManagers either. Help Continue Setup »	
Using 0 of 5 agents New SNMP >>	

Creiamo ora un agent di tipo Custom (Advanced) – Forwarding

	SiteMana	ger		<i>(</i>)						
SETUP • System GateManager VPN Routing Maintenance Status Log • HELP										
Autor										
GateManager Agents - Setup Assistant										
You can configure an agent to monitor a device connected to the SiteManager Serial port and TCP/IP enabled devices located on either the DEV network or Uplink network of the SiteManager.										
	Click [New], and select a	and give the Agent a name (this name will b suitable device type (first vendor, then mod	e what the LinkManager user will see), el). Then click on 🕵 to specify							
	the device a	ddress and other relevant parameters.								
	The SiteMan go IDLE and domain of th	ager will instantly try to connect to the devic appear on the GateManager and any LinkMa e SiteManager.	e, and if successful the Agent will inager that have been granted access to the							
	If not succe the GateMar	ssful, the Agent will report an error, and the ager and subsequently not on LinkManagers	agent will not be registered on either.							
Help Continue Setup >										
Using 1 of 5 agents										
Status Disable S/N	Device Name	Device Type	Device IP & Parameters	Comment						
new: 🔲 #00	Scada	CUSTOM (Advanced) 🔻 Forwarding	T	e to						
		Save New	SNMP >>							



Pagina 8



Selezioniamo il pulsante *edit* presente nell'*Agent* (icona con immagine foglio e manina) per impostare la regola di *Forwarding*:

s Disable	S/N	Device Name	Devic	е Туре		Device IP & Parameters	Comment
	#00	Scada	CUSTOM (Advanced)	Forwarding	•		
							7
	S	iteMana	ger		-		
	56	SETUP • 3	System GateManager	VPN Routing	Mainten	ance Status Log • HELP	
				About			
		0	evice "Scada" (Forv	varding Agent) Details	- Setup Assistant	
		When you or Uplink n	configure an agent to monit etwork of the SiteManager,	or a TCP/IP enable you must specify t	d devices lo ne device IP	cated on either the DEV network address below.	
		Click [Save] and then [Back] to make	the SiteManager in	stantly try t	o connect to the device.	
		If not succ the GateMa	essful, the Agent will report mager and subsequently no	an error, and the a t on LinkManagers	igent will not either.	t be registered on	
						Help Continue Setup *	
		Forwarding	Rule 1:				
		Forwarding	Rule 2:				
		Forwarding	Rule 3:				
		Forwarding	Rule 4:				
		Forwarding	Rule 5:				
		Forwarding	Rule 6:				
		Forwarding	Rule 7:				
		Forwarding	Rule 8:				
		Forwarding	Rule 9:				
		Forwarding	Rule 10:				
		Enable UPL	INK Source Translation:	6			
		Enable DEV	Source Translation:				
				[
		Custom Se	congs:	I			
			Save	Back	Ping	1	
				* = Mandatory f	ield		

6.2 Impostazione regola Forwarding

5

Come accennato all'inizio del capitolo supponiamo di voler accedere dalla rete del cliente alla WEB Page di un PLC con indirizzo 10.0.0.2

Per creare la regola di Forwarding è necessario sapere l'indirizzo IP e la porta di comunicazione che il dispositivo usa per comunicare. (es. vnc TCP 5900, WEB TCP 80, etc...) Nel nostro caso l'accesso alla WEB Page del PLC avviene sulla porta TCP = 80

La regola di forwarding sarà: **UPLINK*:TCP:80>>(Indirizzo IP PLC):80** Nel nostro caso sarà: UPLINK*:TCP:80>>10.0.0.2:80

Nel caso di porta UDP la regola sarà: UPLINK*:UDP:xx>>(Indirizzo IP PLC):xx







Nota: Se non conosco la porta di comunicazione che il dispositivo usa, posso specificare un Range di indirizzi (1-65535) in modo tale da inclutede tutte le porte di comunicazione. [UPLINK*:TCP:1-65535>>(Indirizzo IP PLC):1-65535]

SiteMana(ger		
SETUP · S	stem GateManager VPN Routing	Maintenance Status Log • HELP	
	About		
	GateManager Agents - Se	tup Assistant	
You can con and TCP/IP	igure an agent to monitor a device connected enabled devices located on either the DEV netw	to the SiteManager Serial port vork or Uplink network of the SiteManager.	
Click [New], and select a	and give the Agent a name (this name will be suitable device type (first vendor, then model)	what the LinkManager user will see), . Then click on 🏫 to specify	
the device a	ddress and other relevant parameters.		
The SiteMan go IDLE and domain of th	ager will instantly try to connect to the device, appear on the GateManager and any LinkMana e SiteManager.	and if successful the Agent will ger that have been granted access to the	
If not succes the GateMan	sful, the Agent will report an error, and the ag ager and subsequently not on LinkManagers ei	ent will not be registered on ther.	
		Help Continue Setup »	
	Using 1 of 5 agen	\$	
Status Disable S/N Device Name	Device Type	Device IP & Parameters	Comment
#00 Scada	CUSTOM (Advanced) Forwarding	UPLINK*:TCP:80>>10.0.0.2:80	r t
	Save New	SNMP >>	

Nota: Specificando l'intero range 1-65535 si esclude anche la porta 443, e quindi la possibilità di raggiungere la GUI del sitemanager dalla porta *Uplink*



6.3 Accesso alla WEB Page del PLC tramite regola di Forwarding

Abbiamo ora la seguente condizione -Indirizzo IP porta Uplink1: 192.168.26.84 -Indirizzo IP porta dev1: 10.0.0.1 -Indirizzo IP PLC: 10.0.0.2 -Porta di comunicazione Web Page PLC: TCP = 80

Dalla rete Cliente, via Browser WEB potremo accedere alla WEB Page del PLC digitando sul Browser l'indirizzo IP assegnato alla porta UPLINK1 (Nel nostro caso 192.168.26.84)



Nota: Nel caso di accesso tramite protocolo FTP o OPC è possibile utilizzare solo l'opzione con Agents SCADA



Pagina 11