# Operating principles of outsourcing or remote data copy.

To guarantee a secure link between 2 IDSboxes via Internet, the set up principle is as follows:

- The remote IDSbox comes to connect itself to the public IP address of the company's broadband access (ADSL, cable, fibre ...), at the scheduled time.
- If this public IP address is not fixed, this could be relayed by a DynDNS type address (the IP address is replaced in this case by a subdomain, which itself does not change). You should obtain a fixed public IP address from your Internet access provider.
- For security reasons, the entry into the company's network via the broadband line is limited to a certain number of services, thus blocking any intrusion attempt. Only some ports remain open. This is the method that is used to open ports to allow on-line games. You will find therefore that in some routers the menu "Gaming" is the menu by which router ports are opened.
- It is therefore necessary to open a port to allow a direct and exclusive connection between two IDSboxes.

is the reason why it does not call the DHCP (Random and dynamic IP attribution by a LAN server).

This constitutes the first element of security of the concept of transfer via the internet. The choice in the sense of the connection (Remote IDSbox towards Enterprise IDSbox) was chosen since the IT resources are found naturally in the company. This avoids the need to have technical constraints while installing and connecting the remote box. No remote LAN configuration is necessary during the installation of the remote unit.

The second element of security: in order to ensure the confidentiality of the transaction between the IDSboxes, an exchange procedure two of authentification keys is used through a SSL tunnel. This step is initiated by the remote IDSbox; since the receiving IDSbox has the same certificate of identification, it will authorize the connection and dialog between the two IDSboxes.



Deutschland:

Tel.: 0761 / 59 21 00 Fax: 0761 / 58 52 28

- The 52222 port is used since it is not used by any current services.
- Opening this port implies the attribution of a destination target which in this case is the Enterprise IDSbox. To identify this target precisely, the Enterprise IDSbox has a fixed local IP code. This

The third element of security: in order to ensure that it really is your remote IDSbox that is trying to connect to the enterprise IDSbox, we have put in place a password that provides an additional control that it is indeed your IDSbox that is requesting access.



#### www.hantzundpartner.com/idsbox





# Some examples of router configuration

### LIVEBOX - example model Inventel

- Go to the configuration space of your router as indicated in the quick installation guide or the user manual. You need a PC whose TCP/IP configuration is configured to « obtain an IP address automatically ».
- Den a Web browser and enter the IP address indicated in manufacturer's manual.
- □ Enter the username and password as mentioned in the manufacturer's manual.
- $\hfill\square$  Then select « Configuration », « Advanced » and lastly « Router » (1)
- $\hfill\square$  Enter a new Service with the following information (2) :
  - Service  $\rightarrow$  give a name of your choice
    - Protocol  $\rightarrow$  TCP
    - External port (Origin port) → 52222
    - Internal (Remote port) → 52222
    - $\circ$  Server IP Address (Destination IP address) ightarrow IP address of the Enterprise IDSbox
- Validate by clicking on « Add » (3)

livebox						
	Router - NAT					
My services Security	Port forwarding	g is used to	forward specific	incoming conne	ctions toward dedicate	ed PC on your network.
Configuration	Your computer	's IP addres	ss:10.0.0.32			
Update	Service	Protocol	External port	Internal port	Server IP address	Remove
Administrator	ADMINBOX65	TCP	52222	52222	10.0.0.65	P1
Assistance (1)	rioria io orico	1.01	af he be de be	JALLE .		
Advanced ADSL Wireless Router USB Host Port UPnP Dynamic DNS Network	[Add] Remov	/e	3			2
Save	DMZ setup					
System Information	The DMZ will o Warning : In th on this comput	pen all port ne DMZ, the er" to set it	ts on one chosen computer becon up.	computer. nes accessible fr	om the Internet and m	nore vulnerable to hackers. Click on the button "Configure DM2
	DMZ is configu	red for com	puter : 10.0.0.32	2		
	Warning : To	set the Di	MZ, you must fi	rst set the fire	wall level to "minim	um".
			Configure DM	Z on this comput	er Remo	we DMZ settings

**The configuration of your router for your IDSbox is now complete.** 



www.hantzundpartner.com/idsbox

Österreich: Tel.: 01/58 55 430 Fax: 01/58 55 460

Schweiz: Tel.: 061 / 27 311 - 31

Fax: 061 / 27 311 - 39

Deutschland:

Tel.: 0761 / 59 21 00 Fax: 0761 / 58 52 28

## Sitecom - example model DC-202

- Go to the configuration space of your router as indicated in the quick installation guide or the user manual. You need a PC whose TCP/IP configuration is configured to « obtain an IP address automatically ».
- $\hfill\square$  Open a Web browser and enter the IP address indicated in manufacturer's manual.
- $\hfill\square$  Enter the username and password as mentioned in the manufacturer's manual.
- □ Then select « Advanced Settings », first spot « Virt. Serv. » (1)
- □ Enter 52222 in the Service Ports zone(2)
- **Enter the IP address of your Enterprise IDSbox connected to the LAN (3) and tick the space (4)**
- As an option you can program a time to open the port, which you would have created before in « Schedule » (Opt)

Home Wizard Basic Settings Securit	v Settings Advanced Settings Toolbox Advanced Virt. Serv. Spec. AP Misc.	ogs / DDNS / SNMP / Ro	DC-202
	ID Service Ports	Server IP 192.168.1. XXX	Enable Use Rule#
2 INTERNET	2	192 108.1. 192.168.1.	0
	4 <b>3</b>	192.168.1. <b>4</b>	0
Con and	6 7	192.168.1. 192.168.1.	0
B	9	192.168.1. 192.168.1.	
100	10	192.168.1. 192.168.1.	
Broadband xI	DSL/Cable Router	102 169 1	
INTERNET NETWORK CONNEC	ΤΙΛΙΙΆ	EXP	SITECOM

Do not forget to validate your entries by clicking on the save button.

well known se	rvices - selectone -	Convito	
Schedule rule	(00)Always 👻	0009910	JID



**The configuration of the router for your IDSbox is now complete.** 



www.hantzundpartner.com/idsbox







#### Netgear - example model ProSafe<sup>™</sup> FVG318

- □ Go to the configuration space of your router as indicated in the quick installation guide or the user manual. You need a PC whose TCP/IP configuration is configured to « obtain an IP address automatically ».
- Dependence of the IP address indicated in manufacturer's manual.
- Enter the username and password as mentioned in the manufacturer's manual (by default this is generally Admin / Admin),
- Select « Services », in the « Security » option. (1)
- Click on « Add Custom Service » (2) to open the port 52222



Enter the requested values П

Services	-
Service Definition	
Name:	IDSBOX
Туре:	TCP 🔻
Start Port	52222
Finish Port:	52222
Default QoS Priority:	None -

- Service Name = give the name of your choice, e.g. IDSBOX
- Type = Protocol TCP
- Start port = 52222 0
- 0 Finish port (Destination port) = 52222

Click on « Apply » to validate.

- You will come back to the « Services » screen in « Security »
- Select « Rules » (4), in « Security »



www.hantzundpartner.com/idsbox



Tel.: 0761 / 59 21 00





NETGE ProSafe <sup>™</sup> B02.11g	NETGEAR settings ProSafe <sup>III</sup> 802.11g Wireless VPN Firewall FVG318															
• Setup Wizard	Rules     Rules     Rules     Rules											•				
Setup Basic Settings	Outbound Services											The Firewall will always block DoS (Denial of Service) attacks. A DoS attack does not attempt to steal data or damage your PCs, but overloads your internet connection so you can not use it - the service is unavailable.				
• Wireless Settings Security		De	# fault	Enable Yes	Service Name Any	Action	LAI	N Users Any	WAN Servers Any	Priority None	Log Always		As well, you can use this screen to create Firewall rules to block or allow specific traffic. This feature is for Advanced Administrators only! Incorrect configuration will cause serious problems.	ш		
<ul> <li>Logs</li> <li>Block Sites</li> <li>Rules</li> </ul>	Add Edit Move Delete										E	Outbound Services				
Services Schedule		0	# 1	Enable	Service Name IDSBOX	Action ALLOW Always	LAN Server	IP addres 3.1.90	s WAN Users Any	Priority None	Log Always		This lists all existing rules for outbound traffic. If you have not defined any rules, only the default rule will be listed. The default rule allows all outgoin traffic.			
E-mail		De	fault	Yes	Any	BLOCK always	-	-	Any	None	Always		To create a new rule:			
<ul> <li>VPN Wizard</li> <li>IKE Policies</li> <li>VPN Policies</li> <li>CAs</li> <li>CAs</li> </ul>	Add Edit Move Delete 4 4 4 1. Click the 'Add' buttor setected 2. The 'Outbound Servi own help file. 3. Complete the 'Outbound Servi own help file. 3. Complete the 'Outbound Servi own help file.									<ol> <li>Chick the Add buildin, it does not maker which radio buildin's selected;</li> <li>The "Outbound Service" screen will be displayed. This screen has its own help file.</li> <li>Complete the "Outbound Service" screen, and save the data. The new rule will be listed in the table when you return to this screen.</li> </ol>						
CRL VPN Status	5     6     To make changes to an existing rule:       7     1. Click the check box at the begining of the row and click Applyto disable of Enable the policy.															
Router Status	-											+	Click the button for the desired actions:     Click the button for the desired actions:     The desired actions:	+		

- You come back to the « Services » in « Security »
- Click on the « Add » button to add an association rule between the service created and the IP address of the Enterprise IDSbox.
- Select the service created previously and enter the IP address of the Enterprise IDSbox. (6)
- Then click « Enable » (7)
- The configuration of your router for the IDSbox is now complete.



www.hantzundpartner.com/idsbox

•

Schweiz: Tel.: 061 / 27 311 - 31 Fax: 061 / 27 311 - 39

Österreich: Tel.: 01/58 55 430 Fax: 01/58 55 460

# Linksys - example model RV042

- Go to the configuration space of your router as indicated in the quick installation guide or the user manual. You need a PC whose TCP/IP configuration is configured to « obtain an IP address automatically ».
- Open a Web browser and enter the IP address indicated in manufacturer's manual.
- □ Enter the username and password as mentioned in the manufacturer's manual. (By y default this is generally Admin / Admin),
- □ Select « Setup » (1), then « Forwarding » (2)
- □ Click on « Service Management » (3) to open the 52222 port

A Division of Cisco Systems, Inc.									Firmware \	Version: 1,3.9-q50
			¢.				10/100 4-р	ort VPN Rout	er	RV042
Setup	System Summary	Setup	DHCP	System Management	Port Management	Firewall	VPN Log	Wizard	Support	Logout
	Network	assword	Time	DMZ Host	Forwarding	UPnP	One-to-One NA	T   More	»	
Forwarding	പ്			$\sim$					4	SITEMAP
Port Range Forwarding	<u> </u>	Sei	rvice	2	IP Address	-	Enable		Port Rance	Forwarding
			Service Ma			Add to	list		1. Select th	e Service from
			+						the pull-dov 2. If the Ser	wn menu. rvice you need is
			4						click the Se Managemei	ervice nt button to add
			0						new Servic Protocol an	ce and enter the Id Port Range.
									button. 3. Enter the	P Address of
				Delete sele	cted application				the server the Internet	that you want tusers to
									entry. 4. Click the	Add to List
Port Triggering		Application	Name	Trigger P	ort Range	Incomi	ng Port Range	( I	button, and many entrie	l configure as es as you would
				t	0		to		selected ap	pplication.
				Ad	d to list				Port Trigger	ring:
									or games u ports to cor	net applications ise alternate mmunicate
									between si host.	erver and LAN
									More	
				Delete sele	cted application	1				
					Chow Tables	Cause Catti	ana Carrot	Changes		

Enter the requested values



www.hantzundpartner.com/idsbox

Österreich: Tel.: 01/58 55 430 Fax: 01/58 55 460

Schweiz: Tel.: 061 / 27 311 - 31

Fax: 061 / 27 311 - 39



- Service Name = give a name of your choice, 0 e.g. IDSBOX
- Protocol = TCP 0
- Port range (Origin port) = 52222 0
- to (destination port) = 52222 0

Click on the button « Add to list », then « Save setting » to validate

You will come back to « Setup » - « Forwarding » 

System Summary	Setup	DHCP	System Management	Port Management	Firewall	VPN	Log	Wizard
Network	Password	Time	DMZ Host	Forwarding	UPnP	One-to	-One NAT	More.
	Ser IDSBOX [TCP/	r <b>vice</b> /52222~5222 Service M	2] anagement	IP Address 10 . 168 . 1 . xxx	5 Add to	Enable Ist	6	7

- □ Select the service you have just created (4)
- Complete the field « IP Address » (5) with IP address value of your IDSbox
- Tick the « Enable » button (6) to activate the service
- Click on « Add to list » (7) to validate your input
- The configuration of your router for the IDSbox is now complete.



www.hantzundpartner.com/idsbox

•

Schweiz: Tel.: 061 / 27 311 - 31

Fax: 061 / 27 311 - 39

Österreich: Tel.: 01/58 55 430 Fax: 01/58 55 460

# 3Com Office Connect - example model 3CRWDR100A

- Go to the configuration space of your router as indicated in the quick installation guide or the user manual. You need a PC whose TCP/IP configuration is configured to « obtain an IP address automatically ».
- Open a Web browser and enter the IP address indicated in manufacturer's manual.
- □ Enter the username and password as mentioned in the manufacturer's manual. (By y default this is generally Admin / Admin),
- □ Select « Special Applications » (1), in « Firewall »
- Enter the port 52222 as « Trigger port » and « public port » as shown (2) and tick « Enabled » to activate



Deutschland:

Tel.: 0761 / 59 21 00

Fax: 0761 / 58 52 28

**The configuration of the router for the IDSbox is now complete.** 



www.hantzundpartner.com/idsbox

Schweiz: Tel.: 061 / 27 311 - 31

Fax: 061 / 27 311 - 39

Österreich: \_\_\_\_\_ Tel.: 01/58 55 430

Fax: 01/58 55 460

#### BT Voyager - example model 3CRWDR100A

- Go to the configuration space of your router as indicated in the quick installation guide or the user manual. You need a PC whose TCP/IP configuration is configured to « obtain an IP address automatically ».
- Den a Web browser and enter the IP address indicated in manufacturer's manual.
- □ Enter the username and password as mentioned in the manufacturer's manual. (By y default this is generally Admin / Admin),
- □ Select « Special Applications » (1), in « Firewall »
- □ Then select « Port Forwarding » (2) and click on « Add » (3)

🖉 Voyager 220V Configuratio	n Manager - Windows	Internet Explorer				- F 🛛
🔆 🖉 🗸 🖉 http://192.168.1	1.1/			¥ 49	Live Search	P -
🖌 🎄 🏀 Voyager 220V Config	guration Manager				🙆 • 📾 • 🖶 •	🔂 Page 🔹 🍈 Tools 🔹 🎇
			BT Voyager 220V Cor	figuration Manager	50	
вт	Virtual Serv	er Configuration	ALG			
Quick Start Troubleshooting Configuration Quick Setup	Port Forwarding	Help » 2	ertain applications or	server software		
Voice Local Network	to work on your c	omputers in the internet (	connection uses NAT.			
Internet Security Virtual Server	Application Name I	External Packet P Address Protocol I	Internal F Port IP Address	Host Delete Port		
IP Routing DNS Server Quality of Service				Add		
IGMP Proxy System Status						
				Ŭ		
Version 3.03c						
Done					😝 Internet	🔍 100% 🔹 💡
🦺 start 🔰 🖉 🙆 🔌	" 🔛 IDS Backup	🖉 Voyager 220V 🖳 🕅	Document1 - M EN	(Siscancia		S ▶ 📲 🧏 🧶 10:31

□ Enter the data as shown below

Add New Port Fo	rwarding Rul	le					
Application Name	:					0	Define an a
O Pre-defined:	Audio/Vide	30	Camerades	~		0	Enter the a
Oser defined:	ID Server						IDSbox in (
<b>rom</b> Internet Hos	t IP Address:	ALL	*	3			(4)
orward to Interna	al Host IP Ado	dress: 192.168	1.200	-	-	0	Indicate th
By using the rules	s: Externa	al Packet	Forward to	Internal Host		0	Click on «
Protocol	Port Start	Port End	Port Start	Port End		0	CHER OIL # 1
тср 🖌 5	2222	52222	52222	52222	<b>(</b> 5)		
тср 🗸					$\sim$		
A CONTRACTOR OF							

- Define an application name (3)
- Enter the address of the Enterprise
   IDSbox in « Internal Host IP address »
   (4)
- Indicate the 52222 port in all the fields linked to the TCP protocol (5)
- Click on « Apply » to validate (6)
- **D** The configuration of your router for the IDSbox is now complete.



### www.hantzundpartner.com/idsbox







### Ultimobyte - example model Halon SX-50

- Go to the configuration space of your router as indicated in the quick installation guide or the user manual. You need a PC whose TCP/IP configuration is configured to « obtain an IP address automatically ».
- Dependence of the Dependence o
- □ Enter the username and password as mentioned in the manufacturer's manual. (By y default this is generally Admin / Admin),
- □ Select « Services » (1), in « Firewalling »
- □ Choose « Custom Services » (2) and click on « new service » (3)
- Make for example the service IDSBOX, select TCP for the protocol and enter the port 52222 in « Source Ports » and « Destination ports » as shown below (4) then validate.

H/OS Extreme		0					Firewall / S
😭 Overview 💥 Management	Visual Filter:						No Filter
Schedule	Custom Se	vices Predefined	Services				
Network •	ID	Name	Protocol	Source/Type	Dest/Code	Forward	
🥥 Wireless	service:1	admin_services	ТСР	Any	22,80,443	Same As Dest	Dele
🛞 Applications 👻	service:2	Vnc	TCP, UDP	Any	5901	Same As Dest	Dele
🔋 Firewalling	service:3	SSH2	TCP, UDP	Any	122	22	Dele
Visual Filters	service:4	DMZ	TCP, UDP	Any	25.53	Same As Dest	Dele
Policies	service:5	DMZ_PROXY	TCP, UDP	Any	80,443,21,20	Same As Dest	Dele
Quality of Service	service:6	SSH	ТСР	Any	22	Same As Dest	Dele
Services	service:7	FTP_DATOS	TCP, UDP	Any	20,27200-27210	Same As Dest	Dele
Address Groups	service:8	SMTP2	ТСР	Any	2525	Same As Dest	Dele
Policy Routing	service:9	IDSBOX	ТСР	52222	52222	Same As Dest	Delet
UTM							
🔯 Inspection	Edit Custo	m Service #9 🔹					
Virtual Private Network •	Overvier	w Genera	What are s	ervices?			
UU Help	Advance	d Name	a: IDSBOX				
		Main Protoco	₫: ТСР		~		
		TCP/UDI	p l		4		
		Source Port	s: 52222		$\sim$		
		Destination Port	s: 52222	-			
	New Serv	ice)					

 $\Box$  Add an address group (4 – 5) to make known the Enterprise IDSbox IP Address (6)

H/OS Extreme	l	The firewall configuration has char	nged.	Firewall / Address Groups
Overview Management	Visual Filter:			No filter 👤
Schedule Reporting	Address Grou	ps Predefined Groups		
Network • Wireless	ID group:12	Name Aula_aceptado	Addresses/Networks 192.168.2.99	Delete
Applications     Firewalling     Visual Filters     Policies     Quality of Service     Services     Address Groups     Policy Routing     Options	group:13 Anti-spam		192.168.0.2	Delete
Inspection	Add Address	Group 🔻		
Virtual Private Network	Overview New Group Add Group	General Name: Ids-box Visual Filter: default (sf. 1) Item: 192.168.0.99	Negation: Delete	

Deutschland:

Tel.: 0761 / 59 21 00

Fax: 0761 / 58 52 28



www.hantzundpartner.com/idsbox

Schweiz:

Tel.: 061 / 27 311 - 31

Fax: 061 / 27 311 - 39

Österreich: Tel.: 01/58 55 430 Fax: 01/58 55 460 Now you need to create a rule via the menu « Policies » (7) and link it to the IDSBOX service created previously (8)

H/OS Extreme	The firewal	configuration has changed.		Firewall / Policie
Overview Management Schedule Reporting	Visual Filter: No filter Policies Logs	Advanced Mode is activated. /	Advanced policies are not interpreted i	n Basic Mode. Basic
Network     Wireless     Applications     Firewalling     Visual Filters     Policies     Quality of Service     Address Groups     Policy Routing     Olicy Routing	56 IDSBOX-Port-Forward Block	I IDSBOX (any → ether1:ip) any (any → any)	→ any 🖻 ⇔ any 🦻	Delete © 🗹 🗖
∰ UTM ☐ Inspection ∰ Virtual Private Network ▼ 99 Help ▼	Edit Policy #56 Stat Overview G Redirection Advanced New Group Flush States New Policy Save Policy	istics   eneral What can policies do? Condition Name: DSBOX-Port-Forwar Action: Allow Packet   From IP To IP t Flow  ->  any Interface Firewall	what are conditions?       ce:     IDSBOX       any     IDSBOX       (s):     any       ether1:     Implication       How does flows work?       sabled     Implication       2:nd Interface     Direction	

□ The last step consists of the redirecting of the service (port 52222)towards the Enterprise IDSbox address that was created as a group of addresses (9)

H/OS Extreme	The firewal	Il configuration has changed.		Firewall / Policies
Overview     Management     Schedule     Reporting     Applications     Firewalling     Visual Filters     Policies     Quality of Service     Services     Address Groups     Policy Routing     Options	Visual Filter: No filter Policies Logs	Advanced Mode is activated. Ad	dvanced policies are not interpreted in Basic Mod	e. Basic
	56 • IDSBOX-Port-Forward Block	d IDSBOX (any → ether1:ip) any (any → any)	⊶any ⊠ ⇔ary ⊠	Daiete
	Edit Policy #56 Stat	tistics +		
Virtual Private Network	Overview         Packet           Redirection         Destin           AdVanced         Sm           New Group         P           Flush States         Rout           New Policy         Save Policy	t Forwarding nation Address: Ids-box mart Balancing: Policy Routing ute(s) for "any": disabled te(s) for "none": disabled		

Deutschland: Tel.: 0761 / 59 21 00 Fax: 0761 / 58 52 28

**The configuration of your router for your IDSbox is now complete.** 



www.hantzundpartner.com/idsbox

Österreich: Tel.: 01/58 55 430 Fax: 01/58 55 460

Schweiz: Tel.: 061 / 27 311 - 31 Fax: 061 / 27 311 - 39