



Cloud managed & monitored
VoIP Gateways and Appliances

Come diventare Partner certificato beroNet



Indice

A proposito del beroNet technical training:.....	3
Presentazione del technical training	3
Connettere l'Appliance.....	6
Test 1: Chiamare via SIP.....	6
Configurazione del m0n0wall	6
Accedere all'interfaccia web dell'hypervisor	6
Accedere all'interfaccia web del router	7
Configurazione della porta del m0n0wall.....	8
Configurazione dei Gateways.....	11
Configurazione del gateway Integrato	11
Configurazione del Gateway Esterno.....	13
Test 1: Chiamate dall'Analogico a SIP	15
Test 2: chiamate via ISDN.....	16
Configurazione del Gateway Esterno.....	16
Configurazione della Connessione ISDN	16
Configurazione del Dialplan	17
Configurazione del Gateway Integrato.....	18
Configurazione delle Porte ISDN.....	18
Configurazione del Dialplan	18
Test 1: Chiamate dall'Analogico a ISDN	20
Connettere i dispositivi al beroNet Cloud	20
Connettere i Gateways al Cloud	21
Connettere l'Hypervisor beroNet al Cloud.....	21
Riepilogo del training	22

A proposito del beroNet technical training:

Il beroNet technical training ha l'obiettivo di insegnare ai partner beroNet come predisporre una effettiva installazione VoIP e scoprire il funzionamento della Telephony Appliance, i gateways e il cloud beroNet.

Il training richiede l'utilizzo dei dispositivi inclusi nel beroNet Starter Pack:

- Una BNTA20-2S02FXS-L
- Un BF4002S02FXSbox
- Un beroNet Cloud account

Attenzione: una macchina virtuale del m0n0wall (firewall / router) è già installata e funzionante sull'Appliance ai fini del training. **NON COLLEGATE LA PORTA LAN** (quella sulla sinistra) **AL VOSTRO NETWORK, COLLEGATE SOLO LA PORTA WAN.**

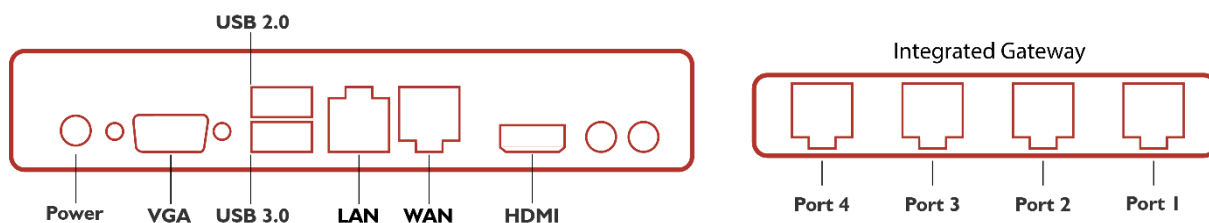


Diagramma: beroNet Telephony Appliance 2.0

Presentazione del technical training

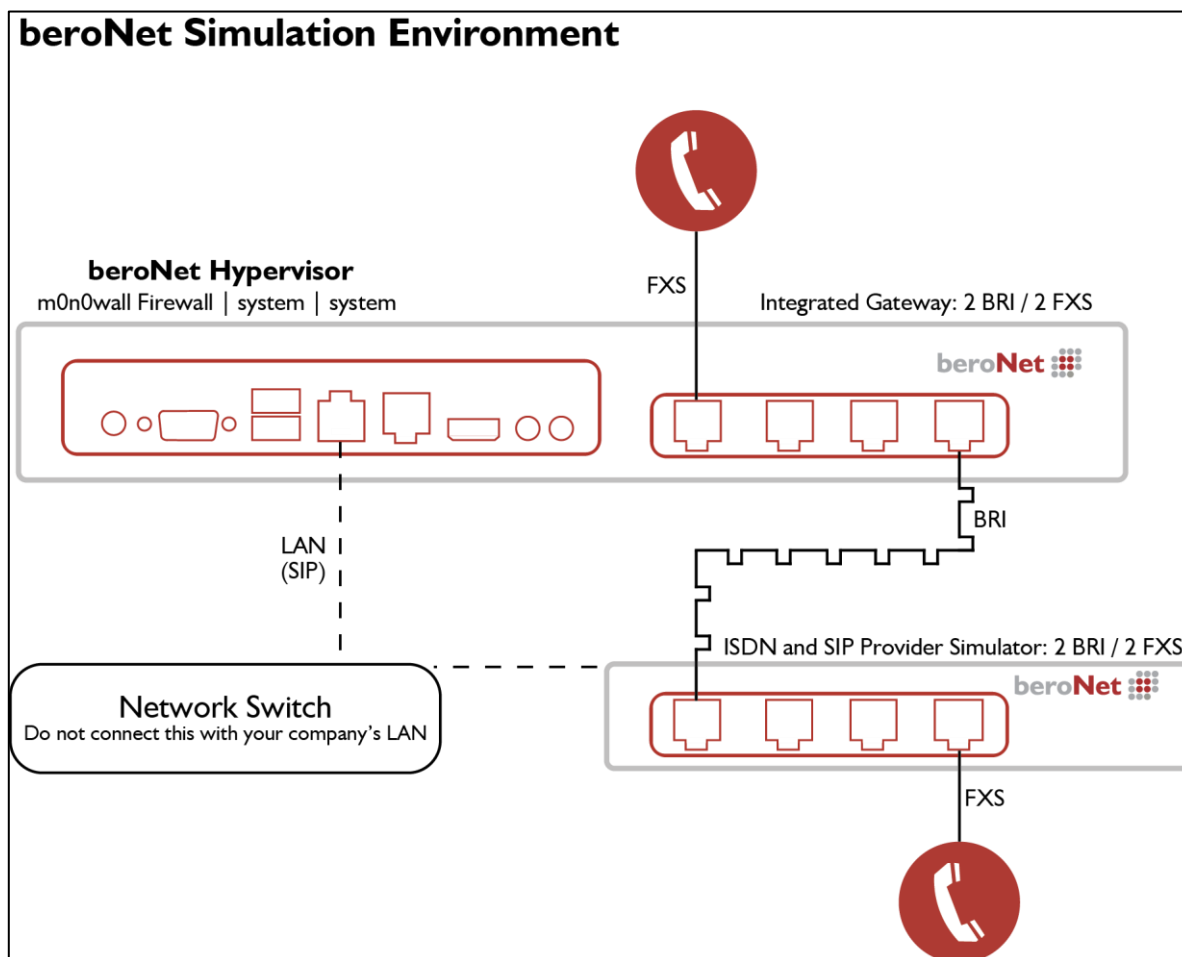
L'idea è di creare uno scenario con il quale i partners beroNet avranno spesso a che fare durante l'installazione di dispositivi VoIP presso i loro clienti. Come verranno utilizzati i dispositivi.

- Il gateway beroNet (BF4002S02FXSbox) simulerà un provider ISDN e SIP. Un telefono analogico sarà connesso a una delle porte FXS (porta 3 o 4) per inviare e ricevere chiamate.
- La beroNet appliance con un gateway integrato sarà utilizzata per simulare il network interno di un'impresa. Sull'appliance è preinstallato un hypervisor per consentire al dispositivo di eseguire diverse macchine virtuali contemporaneamente. Il dispositivo sarà utilizzato come segue:
 - Un router / firewall. Un m0n0wall preinstallato. Il m0n0wall consentirà al partner beroNet di distinguere l'ambiente interno dell'impresa (LAN) da quello esterno (WAN). L'indirizzo IP del m0n0wall è 10.0.0.1.
 - Un Gateway per connettere l'impresa all'esterno via ISDN e SIP. Un telefono analogico sarà connesso al gateway interno dell'appliance. Le chiamate saranno

effettuate dal gateway integrato nell'appliance verso l'esterno via SIP e ISDN.

- Entrambi i gateways e l'hypervisor saranno connessi al beroNet Cloud.

Rappresentazione grafica dello scenario:



Informazioni sulle impostazioni:

- Il gateway esterno funge da provider ISDN e VoIP
- Il m0n0wall è il router. Esso assegna l'indirizzo IP al simulatore dell'IP-PBX (gateway interno) e all'hypervisor (simulatore del data center)
- L'IP range del LAN è da 10.0.0.10 a 10.0.0.99.
- L'indirizzo IP del m0n0wall è 10.0.0.1 e quello sull'hypervisor è 10.0.0.4
- Entrambi i gateways sono configurati per ricevere un indirizzo IP dal server DHCP
- (il gateway interno ottiene un indirizzo IP dal m0n0wall e il gateway esterno dalla rete locale dell'impresa cliente).

Al termine di questo training potrete effettuare chiamate dall'appliance verso l'esterno via SIP e ISDN. Di seguito come procedere:

- Seguite passo dopo passo la guida per creare il vostro scenario
- Inviare ogni traccia realizzata durante il training a training@beronet.com
- Registrate entrambi i gateways e l'hypervisor al beroNet cloud

Connettere l'Appliance

Durante il training utilizzerete un network chiuso.

1. Connettete la porta WAN (quella sulla destra) al vostro network. Il m0n0wall otterrà un indirizzo IP WAN dal DHCP.
2. Connettete la porta LAN (quella sulla sinistra) al vostro computer.
3. Usate l'alimentatore per collegare l'appliance a una presa elettrica.

Test I: Chiamare via SIP

In questo scenario conatterete il gateway integrato nell'appliance a quello esterno via SIP. Per fare ciò, configurate il router preinstallato nel beroNet Hypervisor sull'appliance.

Configurazione del m0n0wall

Accedere all'interfaccia web dell'hypervisor

M0n0wall è un firewall/router open source eseguito su una Macchina Virtuale dell'hypervisor . L'appliance è preconfigurata ed include un server DHCP. Dopo aver connesso il vostro computer alla porta LAN (quella sulla sinistra), l'appliance otterrà un indirizzo IP con il subnet 10.0.0.x e vi permetterà di accedere alla WEB GUI del vostro hypervisor (10.0.0.4).

Lo sapevate che ? beroNet ha sviluppato uno strumento chiamato bfdetect per rilevare e gestire gli indirizzi IP dei dispositivi beroNet nel vostro LAN. Questo può essere scaricato da: <http://www.beronet.com/bfdetect>

1. Inserite l'indirizzo IP dell'hypervisor nel browser (consigliamo Mozilla Firefox o Microsoft Edge).
2. Le credenziali sono "admin / beronet"



Version: 0.8 Copyright © 2015 beroNet GmbH, Germany

3. Il dashboard dell'hypervisor apparirà. A questo punto noterete che il m0n0wall è già operativo.



Maggiori Info: Maggiori informazioni sul funzionamento dell'hypervisor beroNet sono disponibili al link: <http://www.beronet.com/products/telephony-appliance/> o http://wiki.beronet.com/index.php/BeroNet_Telephony_Appliance-v2

Accedere all'interfaccia web del router

Per accedere all'interfaccia web del m0n0wall avete bisogno del suo indirizzo IP.

1. Cliccate sul link "WEB-VNC (5901)". Un nuovo tab si aprirà. Cliccate su "connect" per accedere alla configurazione del firewall. Qui è possibile vedere gli indirizzi IP LAN e WAN del vostro m0n0wall. Le credenziali per il login sono: admin / beronet

```
*** This is m0n0wall, version 1.6.1
    built on Wed Jan 15 13:32:38 CET 2014 for generic-pc
    Copyright (C) 2002-2014 by Manuel Kasper. All rights reserved.
    Visit http://m0n0.ch/wall for updates.

LAN IP address: 10.0.0.1
WAN IP address: 172.20.29.102

Port configuration:
LAN    -> re0
WAN    -> re1

m0n0wall console setup
*****
1) Interfaces: assign network ports
2) Set up LAN IP address
3) Reset webGUI password
4) Reset to factory defaults
5) Reboot system
6) Ping host
Enter a number: █
```

Maggiori Info: Vi consigliamo di usare Mozilla Firefox o Microsoft Edge quando accedete alla Macchina Virtuale tramite il WEB-VNC.

2. Potete quindi accedere alla sua interfaccia web con le credenziali "admin / beronet":
 - a. Con l'indirizzo IP LAN quando siete connessi alla LAN dell'appliance
 - b. Con l'indirizzo IP WAN se il vostro computer non è connesso alla rete locale del m0n0wall. Per accedere al m0n0wall via WAN, sarà necessario configurare le porte inserendo "WANIP:2081". Es.: 172.20.29.102:2081

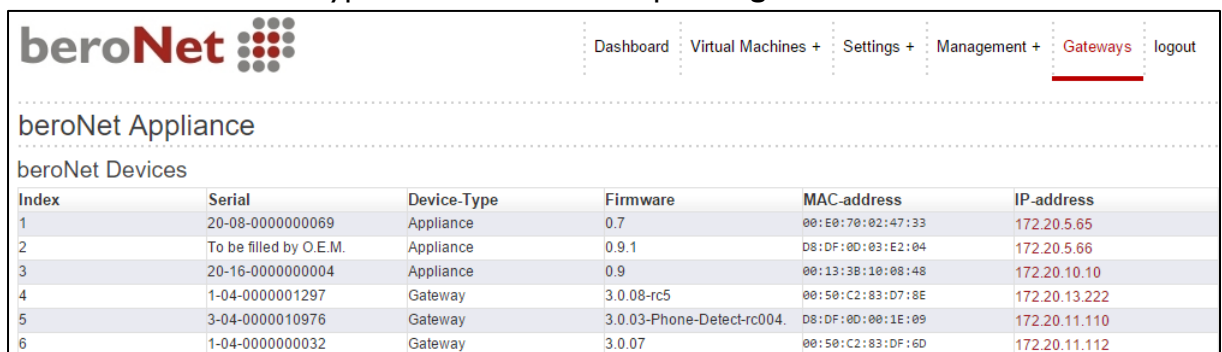
Informazioni sulla pre-configurazione del m0n0wall :

- Il DHCP è attivato sulla porta LAN. Il range del DHCP è impostato tra 10.0.0.10 e 10.0.0.99.
 - L'indirizzo IP LAN della porta LAN è 10.0.0.1
 - Le regole del NAT sono state configurate per l'hypervisor (porta 2084) e per il m0n0wall (porta 2081).
3. Accedete all'interfaccia web del m0n0wall usando il suo indirizzo IP LAN.

Configurazione della porta del m0n0wall

Per autorizzare le chiamate SIP provenienti dal provider, dovete per prima cosa configurare le porte del vostro firewall. Se questa fase non viene eseguita correttamente, il m0n0wall bloccherà tutte le chiamate che provengono dal provider.

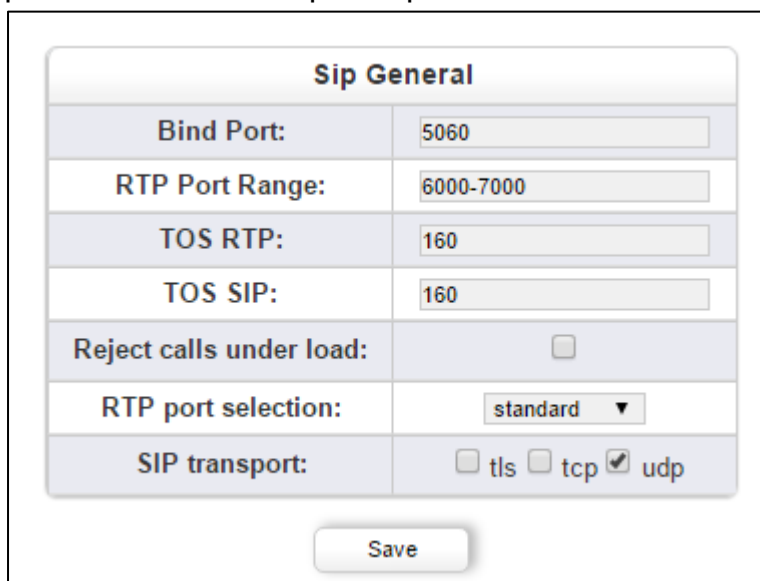
1. Usate una diversa finestra browser o tab per accedere all'interfaccia web del vostro gateway; potete rilevare l'IP del gateway tramite il bfdetect o cliccando su "Gateways" nell'interfaccia web dell'hypervisor. Le credenziali per il login sono: admin / admin



The screenshot shows the 'beroNet Appliance' web interface. At the top, there is a navigation menu with 'Gateways' highlighted. Below the menu, the page title is 'beroNet Appliance' and the section is 'beroNet Devices'. A table lists the following devices:

Index	Serial	Device-Type	Firmware	MAC-address	IP-address
1	20-08-0000000069	Appliance	0.7	00:E0:70:02:47:33	172.20.5.65
2	To be filled by O.E.M.	Appliance	0.9.1	D8:DF:0D:03:E2:04	172.20.5.66
3	20-16-0000000004	Appliance	0.9	00:13:3B:10:08:48	172.20.10.10
4	1-04-0000001297	Gateway	3.0.08-rc5	00:50:C2:83:D7:8E	172.20.13.222
5	3-04-0000010976	Gateway	3.0.03-Phone-Detect-rc004.	D8:DF:0D:00:1E:09	172.20.11.110
6	1-04-0000000032	Gateway	3.0.07	00:50:C2:83:DF:6D	172.20.11.112

2. Nel menu "SIP general", nella sezione "Sip+" dell'interfaccia web del gateway, è possibile vedere quali porte devono essere aperte nel firewall.



The screenshot shows the 'Sip General' configuration page. The fields are as follows:

Bind Port:	5060
RTP Port Range:	6000-7000
TOS RTP:	160
TOS SIP:	160
Reject calls under load:	<input type="checkbox"/>
RTP port selection:	standard ▼
SIP transport:	<input type="checkbox"/> tls <input type="checkbox"/> tcp <input checked="" type="checkbox"/> udp

Save

3. Ritornate alla finestra del browser o tab con il m0n0wall.
4. Andate nella parte “NAT” sotto “firewall” nell’interfaccia web del m0n0wall.
5. Aggiungete una regola cliccando sull’icona “+” e inserendo la seguente configurazione:
 - a. Interface: WAN
 - b. External address: interface address
 - c. Protocol: UDP
 - d. External Port range: scegliete la porta che desiderate (nell’esempio viene utilizzata la 2085 in quanto è più sicura della porta 5060, di solito usata come porta VoIP standard)
 - e. NAT IP: inserite l’indirizzo IP locale del gateway interno all’appliance, (10.0.0.10 nel nostro caso)
 - f. Local port: 5060 dal momento che è la porta configurata in “general SIP settings” all’interno del gateway
 - g. Scegliete **“Auto-add a firewall rule to permit traffic through this NAT rule”** per aggiungere una regola del firewall appropriata
 - h. Salvate e attivate le configurazioni

Firewall: NAT: Edit

Interface	<input type="text" value="WAN"/> <p><small>Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.</small></p>
External address	<input type="text" value="Interface address"/> <p><small>If you want this rule to apply to another IP address than the IP address of the interface chosen above, select it here (you need to define IP addresses on the Server NAT page first).</small></p>
Protocol	<input type="text" value="UDP"/> <p><small>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</small></p>
External port range	from: <input type="text" value="(other)"/> <input type="text" value="2085"/> to: <input type="text" value="(other)"/> <input type="text"/> <p><small>Specify the port or port range on the firewall's external address for this mapping. Hint: you can leave the 'to' field empty if you only want to map a single port</small></p>
NAT IP	<input type="text" value="10.0.0.10"/> <p><small>Enter the internal IP address of the server on which you want to map the ports. e.g. <i>192.168.1.12</i></small></p>
Local port	<input type="text" value="(other)"/> <input type="text" value="5060"/> <p><small>Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). Hint: this is usually identical to the 'from' port above</small></p>
Description	<input type="text" value="Configuration of port 5060 for SIP calls"/> <p><small>You may enter a description here for your reference (not parsed).</small></p>

Auto-add a firewall rule to permit traffic through this NAT rule

6. Una seconda regola NAT deve essere aggiunta per autorizzare l'audio in entrambi i sensi. Di seguito le configurazioni da scegliere in questa seconda regola:
 - a. Interface: WAN
 - b. External address: interface address
 - c. Protocol: UDP
 - d. External Port range: da 6000 a 7000
 - e. NAT IP: inserite l'indirizzo IP locale del gateway interno (10.0.0.10 nel nostro caso)
 - f. Local port: 6000
 - g. Scegliete **“Auto-add a firewall rule to permit traffic through this NAT rule”** per aggiungere una regola del firewall appropriata
 - h. Salvate e attivate le configurazioni

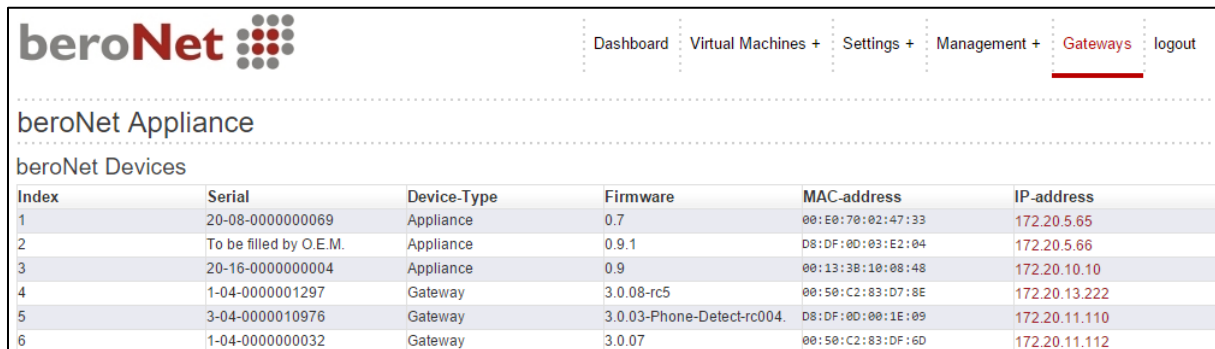
Firewall: NAT: Edit	
Interface	<input type="text" value="WAN"/> Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.
External address	<input type="text" value="Interface address"/> If you want this rule to apply to another IP address than the IP address of the interface chosen above, select it here (you need to define IP addresses on the Server NAT page first).
Protocol	<input type="text" value="UDP"/> Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.
External port range	from: <input type="text" value="(other)"/> <input type="text" value="6000"/> to: <input type="text" value="(other)"/> <input type="text" value="7000"/> Specify the port or port range on the firewall's external address for this mapping. Hint: you can leave the 'to' field empty if you only want to map a single port
NAT IP	<input type="text" value="10.0.0.10"/> Enter the internal IP address of the server on which you want to map the ports. e.g. <i>192.168.1.12</i>
Local port	<input type="text" value="(other)"/> <input type="text" value="6000"/> Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). Hint: this is usually identical to the 'from' port above
Description	<input type="text" value="Rule for RTP port range"/> You may enter a description here for your reference (not parsed).
<input checked="" type="checkbox"/> Auto-add a firewall rule to permit traffic through this NAT rule	
<input type="button" value="Save"/>	

Configurazione dei Gateways

Lo scopo di questo test è di effettuare chiamate da un gateway all'altro via SIP. Il gateway esterno funge da provider SIP. Per questo, aggiungete un SIP trunk in ciascun gateway. Dovete registrare il dispositivo interno su quello esterno e viceversa. Basta inserire l'indirizzo IP dell'altro gateway nel campo "server address".

Configurazione del gateway Integrato

1. Accedete all'interfaccia web del vostro gateway tramite il bfdetect o semplicemente cliccando su "Gateways" nell'interfaccia web dell'hypervisor.



The screenshot shows the beroNet web interface. At the top left is the beroNet logo. To the right is a navigation menu with items: Dashboard, Virtual Machines +, Settings +, Management +, Gateways (highlighted with a red underline), and logout. Below the navigation is the text "beroNet Appliance" and "beroNet Devices". A table lists the devices with columns: Index, Serial, Device-Type, Firmware, MAC-address, and IP-address.

Index	Serial	Device-Type	Firmware	MAC-address	IP-address
1	20-08-0000000069	Appliance	0.7	00:E0:70:02:47:33	172.20.5.65
2	To be filled by O.E.M.	Appliance	0.9.1	D8:DF:0D:03:E2:04	172.20.5.66
3	20-16-0000000004	Appliance	0.9	00:13:3B:10:08:48	172.20.10.10
4	1-04-0000001297	Gateway	3.0.08-rc5	00:50:C2:83:D7:8E	172.20.13.222
5	3-04-0000010976	Gateway	3.0.03-Phone-Detect-rc004.	D8:DF:0D:00:1E:09	172.20.11.110
6	1-04-0000000032	Gateway	3.0.07	00:50:C2:83:DF:6D	172.20.11.112

2. Cliccate sul link nell'hypervisor o inserite l'indirizzo IP nel vostro browser ed effettuate il login all'interfaccia web usando le credenziali: admin / admin

Configurazione dell'account SIP

1. Andate in "SIP" nella sezione "SIP+".
Qui potete aggiungere un account SIP.
Inserite le seguenti informazioni:
 - a. Name: scegliete un nome
 - b. Server Address: inserite l'indirizzo IP del gateway esterno
 - c. User: scegliete un user di vostro gradimento, questo dovrà essere lo stesso anche nell'altro gateway
 - d. Secret: create una password
 - e. NAT-options: scegliete l'opzione "extern IP" – il WAN del m0n0wall (172.20.29.102 nel nostro caso)
 - f. Register: spuntate il riquadro "Register"
2. Salvate

Name:	Provider
Server Address:	172.20.29.167
User:	Tech-training
Authentication user:	
Displayname:	
Secret:	
Match type:	<input checked="" type="checkbox"/> IP Address <input type="checkbox"/> From User <input type="checkbox"/> To User <input type="checkbox"/> Contact User <input type="checkbox"/> Request-URI User <input type="checkbox"/> Manual
SIP transport:	udp
NAT options:	<input type="radio"/> No-NAT <input type="radio"/> STUN-Server <input checked="" type="radio"/> Extern-IP
Extern-IP:	172.20.29.102
Register:	<input checked="" type="checkbox"/>
Registration interval:	300
Register option:	no-validate
Keepalive-Interval:	0

more...

Save Close

Configurazione delle porte analogiche

1. Andate in "Analog FXS" nella sezione "PSTN+".
2. Aggiungete un gruppo e inserite le seguenti informazioni:
 - a. Name: inserite un nome a vostra scelta
 - b. Ports: scegliete una o entrambe le porte
 - c. Tones: scegliete il tono relativo al vostro Paese
 - d. CLIP and CNIP: inserite il numero di telefono che la porta FXS simulerà
3. Salvate
4. Premete su "Activate"

Group Name:	FXS
Ports:	LI0(bf2S02FXS) LI1() Port 1 <input checked="" type="checkbox"/> Port 2 <input checked="" type="checkbox"/>
Interdigit timeout initial:	15
Interdigit timeout:	3
Overlap Dialing:	<input type="checkbox"/>
Tones:	[de]
CLIP:	0302593890
CNIP:	0302593890
ChanSel:	standard
ChanSel direction:	ascending
Message waiting method:	stutter

more...

Save Close



PSTN + Hardware
ISDN BRI
ANALOG FXS

Configurazione del dialplan









Bisogna creare 2 regole nel dialplan:


1. Aggiungete una regola che invia tutte le chiamate dalle porte analogiche verso SIP
2. Aggiungete una seconda regola che invia tutte le chiamate provenienti da SIP verso le porte analogiche

Sotto un esempio delle 2 regole:

DIALPLAN Languages:  

Direction: all Search: Entries per page: 15

<input type="checkbox"/> Check all	Direction	From ID	To ID	Destination	New destination	Source	New source	Position	
<input type="checkbox"/>	sip-analog	Provider	FXS	(.*)	\1	(.*)	\1	1 <input type="text"/> ▲ ▼	   
<input type="checkbox"/>	analog-sip	FXS	Provider	(.*)	\1	(.*)	\1	2 <input type="text"/> ▲ ▼	   

 [activate](#) , [deactivate](#) , [delete](#)

3. Attivate le impostazioni che avete configurato.

Configurazione del Gateway Esterno

Accedere all'interfaccia web del gateway

Dal momento che il gateway esterno non è connesso alla rete LAN del m0n0wall, dovete attenervi alle seguenti indicazioni per scoprire l'indirizzo IP del gateway.

1. Connettete il vostro computer alla rete LAN della vostra impresa
2. Usate il bfdetect per rilevare l'indirizzo IP del gateway esterno
3. Riconnettete il vostro computer alla rete LAN del m0n0wall
4. Usate il vostro browser per cercare l'indirizzo IP del gateway e usate le seguenti credenziali per effettuare il login all'interfaccia web del gateway: admin / admin

Configurazione dell'account SIP

- Andate in "SIP" nella sezione "SIP+".
Qui potete aggiungere un account SIP. Inserite le seguenti informazioni:
 - Name: scegliete un nome
 - Server Address: inserite l'indirizzo IP WAN del m0n0wall e la porta definita per il gateway – 2085. Nel nostro caso
172.20.29.102:2085
 - User: scegliete un nome di vostro gradimento, questo dovrà essere lo stesso anche nell'altro gateway
 - Secret: create una password
 - NAT Options: lasciate l'opzione di default "No-NAT"
 - Register: selezionate questa opzione
- Salvate
- Premete su "Activate"

Name:	sip-provider
Server Address:	172.20.29.102:2085
User:	Tech-training
Authentication user:	
Displayname:	
Secret:
Match type:	<input checked="" type="checkbox"/> IP Address <input type="checkbox"/> From User <input type="checkbox"/> To User <input type="checkbox"/> Contact User <input type="checkbox"/> Request-URI User <input type="checkbox"/> Manual
SIP transport:	udp
NAT options:	<input checked="" type="radio"/> No-NAT <input type="radio"/> STUN-Server <input type="radio"/> Extern-IP
Register:	<input checked="" type="checkbox"/>
Registration interval:	300
Register option:	no-validate
Keepalive-Interval:	0

Configurazione delle porte analogiche

- Andate in "Analog FXS" nella sezione "PSTN+".
- Aggiungete un gruppo e inserite le seguenti informazioni:
 - Name: scegliete un nome
 - Ports: scegliete una o entrambe le porte
 - Tones: scegliete il tono relativo al vostro Paese
- CLIP and CNIP: inserite il numero di telefono che la porta FXS simulerà
- Salvate
- Premete su "Activate"











Group Name:	FXS
Ports:	Li0(bf2S02FXS) Li1() Port 1 <input checked="" type="checkbox"/> Port 2 <input checked="" type="checkbox"/>
Interdigit timeout initial:	15
Interdigit timeout:	3
Overlap Dialing:	<input type="checkbox"/>
Tones:	[de]
CLIP:	0302593890
CNIP:	0302593890
ChanSel:	standard
ChanSel direction:	ascending
Message waiting method:	stutter


Configurazione del dialplan

Bisogna creare 2 regole nel dialplan:

1. Aggiungete una regola che invia tutte le chiamate dalle porte analogiche verso SIP
2. Aggiungete una seconda regola che invia tutte le chiamate provenienti da SIP verso le porte analogiche

Sotto un esempio delle 2 regole:

DIALPLAN										Languages:  	
Direction: all Search: <input type="text"/> Entries per page: 15											
<input type="checkbox"/> Check all	Direction	From ID	To ID	Destination	New destination	Source	New source	Position			
<input type="checkbox"/>	sip-analog	Provider	FXS	(.*)	\1	(.*)	\1	1 <input type="text"/> ▲ ▼	   		
<input type="checkbox"/>	analog-sip	FXS	Provider	(.*)	\1	(.*)	\1	2 <input type="text"/> ▲ ▼	   		

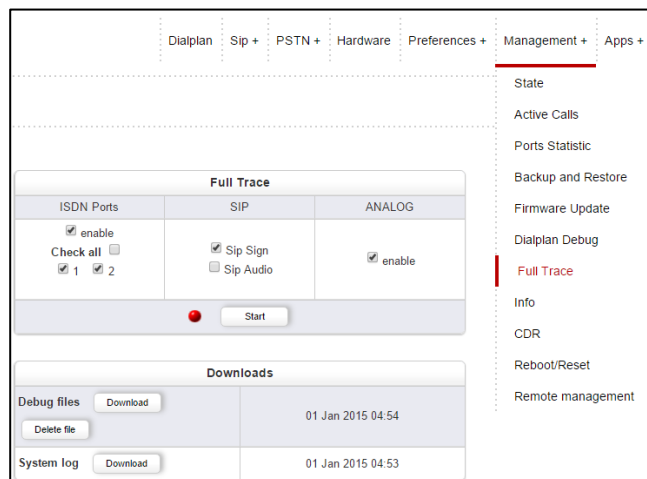
 activate , deactivate , delete

1. Attivate le impostazioni che avete configurato.

Test I: Chiamate dall'Analogico a SIP

Ora che entrambi i dispositivi sono configurati, potete effettuare una chiamata dall' analogico a SIP.

1. Andate in “Fulltrace” nella sezione “Management +”. Avviate la traccia.
2. Fate una chiamata dal telefono analogico connesso all’appliance al telefono connesso al gateway esterno usando il numero inserito nel campo “CLIP” del telefono analogico.
3. Fate una chiamata dal telefono analogico connesso al gateway esterno, al telefono connesso all’appliance usando il numero inserito nel campo “CLIP” del telefono analogico.
4. Interrompete la “Fulltrace” e, se le chiamate sono andate a buon termine, scaricate il file. L’estensione del file dovrebbe essere “.tar.gz”. Se le chiamate non sono andate a buon termine, controllate le vostre configurazioni e provate di nuovo.



Test 2: chiamate via ISDN

In questa parte apprenderete come creare regole ISDN e come funziona il dialplan beroNet.

Configurazione del Gateway Esterno

Il gateway esterno simulerà il provider ISDN. Accedete di nuovo alla sua interfaccia WEB e configurate le porte ISDN come segue:

Configurazione della Connessione ISDN

Per prima cosa, dal momento che questo gateway funge da provider ISDN, dovete impostare la giusta configurazione hardware per le sue porte.

1. Andate nel tab “hardware” e scegliete la modalità “NT” (il gateway integrato nell’appliance avrà la modalità “TE”).

Card Type: bf2S02FXS Line Interface: 0 Master: master Synchronization port: 1						
Port: 1	Port type: BRI	Type: nt	Protocol: PTP	Termination: <input checked="" type="checkbox"/>	Permanent1: <input type="checkbox"/>	
Port: 2	Port type: BRI	Type: te		<input checked="" type="checkbox"/>	Permanent1: <input type="checkbox"/>	
Port: 1						
Port: 2						

Possible values for ISDN Mode are:

- TE (Terminal Endpoint) to connect to a ISDN Line
- NT (Network Terminator) to connect ISDN devices

2. Dopo andate in “ISDN BRI” nella sezione “PSTN+” e configurate le porte come segue:
 - a. Assegnate un nome al gruppo
 - b. Scegliete le porte da aggiungere al gruppo
 - c. Impostate il tono relativo al vostro Paese
 - d. Impostate il “country code” (49 in Germania)
 - e. Impostate il “city code” (es. 030 per Berlino)
 - f. Save
3. Premete su “Activate”

Configurazione del Dialplan

Bisogna creare 2 regole nel dialplan:

1. Le chiamate provenienti da ISDN devono essere inviate alle porte analogiche.
2. Le chiamate provenienti dalle porte analogiche devono essere inviate a ISDN..

		Direction: all	Search:			Entries per page: 15			
<input type="checkbox"/> Check all	Direction	From ID	To ID	Destination	New destination	Source	New source	Position	
<input type="checkbox"/>	isdn-analog	BRI	FXS	(*)	\1	(*)	\1	1	
<input type="checkbox"/>	analog-isdn	FXS	BRI	(*)	\1	(*)	\1	2	

activate , deactivate , delete

3. Attivate le configurazioni che avete modificato.

Configurazione del Gateway Integrato

Configurerete questo gateway in maniera tale che le chiamate verso la Germania (chiamate locali) saranno inviate via ISDN, e le restanti via SIP.

Configurazione delle Porte ISDN

1. Effettuate la stessa configurazione delle porte usata per il gateway esterno. Assicuratevi che la modalità hardware delle porte sia impostata su “TE”.
2. Usate il cavo ISDN arancione in dotazione con il training kit per connettere entrambi i gateways. **NON USATE UN NORMALE CAVO ETHERNET !!!**

Configurazione del Dialplan

Informazioni sul dialplan beroNet

Dovrete aggiungere altre due regole e differenziarle. Di seguito le informazioni più importanti da sapere sul dialplan:

- Utilizza espressioni regolari (per saperne di più consultate il seguente link: <http://www.zytrax.com/tech/web/regex.htm>)
- Funziona dall'alto verso il basso. Questo significa che le regole generiche devono essere collocate sotto regole più specifiche. Quando c'è una chiamata in entrata, il dialplan esaminerà ogni regola iniziando dall'alto. Appena la chiamata passa attraverso il dispositivo, la prima regola che rispecchia i parametri di tale chiamata (tecnologia da cui proviene, “CalledID” o DAD – numero chiamato, e “CallerID” o CID – numero chiamante) sarà applicata.

Regole specifiche del dialplan

Al momento, le due regole esistenti inviano tutte le chiamate provenienti da SIP alle porte analogiche e viceversa. Ora dovete assicurarvi che le chiamate verso la Germania siano inviate via ISDN. Essendo questa regola più specifica, deve essere collocata sopra alle altre, nella parte più alta del dialplan.

1. Cliccate su “add” e selezionate le seguenti configurazioni:
 - a. From: Analog
 - b. To: ISDN
 - c. Destination: inserite 0049(.*), questo significa che tale regola sarà applicata a tutte le chiamate effettuate digitando numeri che iniziano con 0049

- d. New destination: \1 significa che le informazioni all'interno della parentesi del campo "destination" saranno mantenute
- e. Source e new source possono essere lasciati vuoti

DIALPLAN ✕

From direction:	ANALOG ▼	To direction:	ISDN ▼
From ID:	g:FXS ▼	To ID:	g:ISDN ▼
Destination:	0049(*)	New destination:	\1
Source:	(*)	New source:	\1
Comments:			
Activ:	<input checked="" type="checkbox"/>		

2. Cliccate save. Ora, quando chiamerete un numero che inizia con 0049, la chiamata sarà instradata via ISDN.
3. Andate in "dialplan debug" nella sezione "management+" per controllare il funzionamento della regola. Avviate un debug.
4. Provate a fare una chiamata. Dovreste visualizzare qualcosa del genere:

DIALPLAN DEBUG

State: ON

```

CDR,34,SIP:10.0.0.10,ISDN:1:1,"0302593890" "",_0302593890,123456789,15/01/01-06:26:29,15/01/01-06:26:32,-,-,SIP_NUA_I_CANCEL:200,-,-
S CANCEL|INDICATION: from="0302593890" 0302593890@10.0.0.10, to="" ISDNZUISDN54a5447b04be8123456789@10.0.0.10
CDR,33,ANALOG:1,SIP_0302593890,0049123456789,"0302593890",,15/01/01-06:26:23,15/01/01-06:26:32,-,-,ANALOG_ANALOG_EVENT_IDLE:0,-,-
S CANCEL|REQUEST: from="0302593890" 0302593890@10.0.0.10, to="" ISDNZUISDN54a5447b04be8123456789@10.0.0.10:5060
A ANALOG_EVENT_IDLE|INDICATION: port=1
I SETUP|REQUEST: port=1, channel=1, dad=123456789, oad=302593890
D INCOMING src:0302593890 dest:ISDNZUISDN54a5447b04be8123456789 -- OUTGOING src:0302593890 dest:123456789
S INVITE|INDICATION: from="0302593890" 0302593890@10.0.0.10, to=ISDNZUISDN54a5447b04be8123456789@10.0.0.10
S INVITE|REQUEST: from="0302593890" 0302593890@10.0.0.10, to="" ISDNZUISDN54a5447b04be8123456789@10.0.0.10:5060
D INCOMING aport:1, src:0302593890 dest:0049123456789 -- OUTGOING src:"0302593890" dest:
A ANALOG_EVENT_OFFHOOK|INDICATION: port=1
CDR,32,ANALOG:1,SIP_0302593890,4123,"0302593890",,15/01/01-06:25:04,15/01/01-06:26:17,15/01/01-06:25:10,15/01/01-06:26:17,ANALOG_ANALOG_EVENT_IDLE:0,-,-
S BYE|REQUEST: from="0302593890" Tech-training@172.20.29.167, to="" 4123@172.20.29.167
A ANALOG_EVENT_IDLE|INDICATION: port=1

```

Problema:

Se guardate attentamente la regola, noterete che il numero chiamato non è stato inviato correttamente alla linea ISDN. Il dialplan in realtà esclude il prefisso "0049". In base a quanto visualizzato nello screenshot sopra, avete chiamato il numero: **0049123456789** ma la linea ISDN riceve soltanto "dad= 123456789". Per mantenere il prefisso dovete quindi apportare una piccola modifica alla regola.

Modifiche della regola:

In base alla regola che avete creato, il dialplan stabilisce che tutti i numeri che iniziano con “0049” siano inviati verso ISDN. L’espressione \1 nel campo “New destination” mantiene ciò che è all’interno della parentesi. Potete notare che nel precedente screenshot il prefisso è posizionato prima delle parentesi e viene quindi escluso.

1. Aggiungete un’altra coppia di parentesi e “\2” nel campo “new destination”.

Fate riferimento allo screenshot sottostante:

Field	Value
From direction:	ANALOG
To direction:	ISDN
From ID:	g:FXS
To ID:	g:ISDN
Destination:	(0049)(.*)
New destination:	\1\2
Source:	(.*)
New source:	\1
Comments:	
Activ:	<input checked="" type="checkbox"/>

2. Cliccate su Save. Ora, quando chiamerete la Germania, il numero sarà mantenuto nel format corretto.

La stessa regola viene applicata al campo “Source” e “New source”. Per ottenere maggiori informazioni sul dialplan, [consultate l’articolo sul dialplan nel nostro blog](#).

Test I: Chiamate dall’Analogico a ISDN

1. Effettuate la traccia di una chiamata da analogico a ISDN in entrambe le direzioni.
2. Scaricate il file (Debug files). Questo è uno dei file che dovrete inviare a training@beronet.com alla fine del training.

Connettere i dispositivi al beroNet Cloud

Il beroNet Cloud vi consente di gestire e monitorare i vostri dispositivi da qualsiasi browser, da qualsiasi luogo.

Connettere i Gateways al Cloud

1. Andate in “Remote management” nella sezione “management+”.
2. Spuntate il riquadro “Cloud enable”.
3. Inserite la vostra Username e Password relative al Cloud e cliccate su Register.

The screenshot shows a web interface for configuring cloud settings. It is divided into two main sections. The top section, titled "Cloud", contains a "Cloud Username:" field with the value "usernameofyourcloud", a "Cloud password:" field with masked characters ".....", and a "Register" button. The bottom section contains a "Cloud enable:" checkbox which is checked, a "Cloud URL:" field with the value "berocloud.beronet.com", a "Load default" button, and a "Save" button at the bottom.

Connettere l’Hypervisor beroNet al Cloud

1. Andate in “Cloud settings” nella sezione “Settings” dell’interfaccia web dell’hypervisor.
2. Inserite la vostra Username e Password relative al Cloud e cliccate su Register

The screenshot shows the "beroNet Appliance" web interface. It has two main sections: "Register" and "Cloud Settings". The "Register" section includes a "Register" button and a "register" button. The "Cloud Settings" section includes a "Cloud Server:" field with the value "berocloud.beronet.com", an "Enable:" checkbox which is checked, and a "cloud_enable" button.

Riepilogo del training

Durante questo training, avete effettuato le seguenti configurazioni:

- Un sistema sistema VoIP interno basato sulla beroNet appliance, nella quale avete configurato un router e un gateway che simula un PBX.
- Invio di chiamate verso l'esterno via SIP o ISDN
- Un gateway esterno che funge da provider SIP e ISDN per simulare le chiamate

Per completare il training e diventare partner beroNet è necessario inviare diverse tracce a training@beronet.com:

- Una traccia di due chiamate SIP: da e verso il gateway esterno
- Una traccia di due chiamate ISDN: da e verso il gateway esterno