

Traffic collector



User manual

Product version: 2.3 Copyright: 5gFuture Inc., 2011-2017

www.5gFuture.com

Table of Contents

1. Introduction	2
1.1. Overview	2
1.2. Collection methods	2
2. Signaling collector	4
2.1. Overview	4
2.2. Signaling logs menu	4
2.3. Signaling logs	5
2.4. Leg list	6
2.5. Call list	6
2.6. Call flow	6
2.7. Packet viewing	7
3. Media collector	9
3.1. Overview	9
3.2. Media conf	9
3.3. Media calls	10
3.4. Media logs	10
4. IP whitelist	12
4.1. Overview	12
4.2. Collected IPs	12
4.3. Whitelist config	13

1. Introduction

5gVision Traffic collector is part of the 5gVision suite of products for monitoring, alerting, packet sniffing, and rate management that share a common web interface: quick, intuitive, and flexible.

1.1. Overview



The **Traffic collector** is part of the **5gVision** suite of products. Its main function is to gather SIP/H.323 signaling logs and media packets in real time. It then allows you to quickly view any signaling logs or Call flows from the past in an easy and convenient way, listen to the recorded media for pre-defined IP addresses and number masks, and detect intrusions to your VoIP system. A good way to start with the Traffic collector and understand its main concepts is to view this sales presentation:

5gVision Traffic Collector Modules

The 5gVision interface principles are described in a separate manual: User interface

You may download a PDF version of the manual here:

User interface

If you are new to 5gVision, we would recommend to go through at least the beginning of the Interface manual first.

The Traffic collector comprises three separate modules:

- Signaling collector
- Media collector
- IP whitelist

that are described in further sections of this manual.

1.2. Collection methods

There are 4 main methods of getting signaling and media packets:

• Method 1 requires setting up a mirrored port on the Ethernet switch the VoIP softswitch is connected to. This mirrored port should be linked to a NIC on a 5gVision server to let it grab signaling and media packets passing through the network.

The main advantage is that this scheme doesn't affect the softswitch performance at all, is invisible to softswitch vendor's support team, and usually allows to collect huge amounts of traffic without drops. However, a customer has to reconfigure its Ethernet switch and add another NIC card to a 5gVision server. Not all Ethernet switches support mirroring too, and it won't work if a customer does not have physical access to the softswitch server (rented servers, VPS, etc.), or can't install just another server for 5gVision in the same LAN as the VoIP softswitch.

Method 2 allows collection of traffic remotely via an SSH connect to each of customer's VoIP softswitches with a user that is only
allowed to run one application - tcpdump. All packets are grabbed locally on the softswitch and are sent to 5gVison via SSH.

The benefit of this scheme is that there are no additional hardware requirements, logs can be collected from any servers without a physical access, and from geographically distributed servers. Also, this scheme doesn't affect the "Do not install the third-party software" agreement with the softswitch vendor, because ssh and tcpdump are a basic tools of every Linux system.

Local packet sniffing consumes some extra CPU resources and memory on the softswitch, although the increase is usually negligible and is within 5-10%. HDD is not affected at all, as no packets are written to a local drive of the softswitch.

- Method 3 can be used if you already collect .pcap files yourself. 5gVison may then upload and process these files over SFTP or other protocols. It is preferred that the files are rotated every 2-5 minutes or so, to make the collector closer to real time.
- Method 4 requires installation of a very simple script on each node (server) of your softswitch. This script will run the tcpdump and write traffic into files. The files will rotate and will never use more space than was allocated on each HDD. We will then upload files to a 5gVision server for processing.

This scheme will deliver unprecedented performance for large distributed systems. For instance, if you have 8 nodes (servers) in your softswitch, doing mirroring of 8 ports to just one NIC card on the 5gVsion server may result in enormous traffic (especially if media is collected) that we will not be able to read from the NIC without drops. However, if traffic is dumped into files on each of the 8 nodes, it will not be a problem to copy and process them on one or several 5gVision servers.

There would be an extra load on CPU and HDD of each node in this case, we would need to investigate your node load and your softswitch type to make a decision to install this scheme.

2. Signaling collector

The signaling collector gathers SIP/H.323 logs in real time and let you view their contents and Call flows.

2.1. Overview

The Signaling collector gathers, stores and conveniently displays SIP and H.323 messages sent and received via the predefined ports of your network.

Traffic colle	ctor C — Cust 1m 10m 1h 4h 12h 24h 1d-3	2d 2d-3d GO Share R	CDR S	ignaling	logs Media ca Fetch: 10 100	lls Medialog 300 1k 3k Fil	s Me e-PCA	edia co	onf Mo	re ? 🖉 ▽ 🗖 8
	(Import PCAP or 5g log) (Leg	list) (Call list) (Call flow) (I	fo X							
selected	V 2020042007_12030440		DST	55	Customer from CDR	Vendor from CDR	Leg	Dir	Packet size	Packet data
alastad	X 738148.73.79.108	8 0010ec1e208.108.108.30	.190.3	30			1	src->	1131	INVITE sip:
selected			1.127	7.52			2	src->	1364	INVITE sip:
n Offset from	5060 5060	5050	5060	30			2	<-dst	719	SIP/2.0 100 Trying Via: SI
	3000 3000 3000	3000	.70.10	09			1	<-dst	315	SIP/2.0 100 Trying Via: SI
0.000000			.190	30			2	<-ast	1255	SIP/2.0 183 Progress Via
0 0.027830			wiewe	38			2	<-dst	1345	SIP/2.0 200 OK Via: SIP/2
7 0.004807				09 90			1	<-dst	996	SIP/2.0.200 OK Via: SIP/2
8 0.167751	100 Trying		Daw log	ctod pa	ckata Calact	red logs (1)	All los	10	Coll fly	
0 0.166722		18: Select all	Kaw iog Sele	cted pa	ickets Select	ed legs (1)	All leg	JS	Call IK	- +
1 0.001701	183 Progress (G729)	2015-12-16 19:4	1.57 1599/1	0.0270	830 === Log	2 SPC-	>Det			
5 10 474694	<	INVITE sip:	1.57.155641	0.0270	user=pt	none SIP/2.0	-031		Sector Sector	
0 000000	200 01/ (0720)	Via: SIP/2.0/UDF	60.000	60;rpor	t;branch=	40K-8046500	0042	41164	91635	sig=110f
8 0.001193	< 200 OK (G729)	Via: SIP/2.0/UDF	10.100 .00:50	60;rpor	rt;branch=	406-8046543	Halls	ane	591038	4073810ec10;sig=890
6 0.000808		Via: SIP/2.0/UDF	50	61;rpor	rt=5061;branch	edihG4bK-a	Note	404.4	241765	91b3549/3510ec1c
0 0.029084	ACK	From: <sip:< td=""><td>C2148C7_088.788.</td><th>190.00</th><th>:5061;user=ph</th><td>one>;tag=Hg</td><td>qtOul</td><td>=Yxr4</td><td>eE8Xh</td><td>WMa+HhPEyDV2wQAc</td></sip:<>	C2148C7_088.788.	190.00	:5061;user=ph	one>;tag=Hg	qtOul	=Yxr4	eE8Xh	WMa+HhPEyDV2wQAc
3 0.002083	INVITE (G729)	10: <sip.< td=""><td></td><th></th><th>user=pnor</th><td>ie></td><td></td><td></td><td></td><td></td></sip.<>			user=pnor	ie>				
3 0.002140	200 OK (G729)	CSeq: 1 INVITE	CALCULATION OF TAXABLE		and a second second	100.00				
4 0.022261	ACK	Contact: <sip:< td=""><td>ACCESSION NAMES OF</td><th>1. TANK</th><th>:5061;user=</th><td>phone></td><td></td><td></td><td></td><td></td></sip:<>	ACCESSION NAMES OF	1. TANK	:5061;user=	phone>				
1 136 007137		Content-Type: a	oplication/sdp							
5 0.004574		Allow: ACK, BYE	CANCEL, INFO, IN	NVITE, O	OPTIONS, REF	FER, REGIST	ER, L	IPDAT	ΓE	
0.0015/4		Max-Forwards: 6	9							
6 0.000961	BYE	User-Agent: TS-	/4.6.0-116W	201 24	44448027 800	301468				
7 0.025811	200 OK	Content-Length:	200	501-244	44440927-090	00 (400				
		Record-Route: <	sip:	1000	NOL IN TRANS	0.4.2 Million (2010)	198	199.3	:lr>	

There are several ways for accessing this feature:

- through CDRs (see CDR pop-up menu) which frees you from entering Call ID manually, and lets you see call flow for 2 call legs at once).
- through your current screen by opening the Signaling logs module.
- by adding a new Traffic collector screen (see Menu tree for information on how to add it).

2.2. Signaling logs menu

The menu on top of the Signaling logs table consists of the Table menu, the Interval strip, the Row count strip, the Row limit strip, the Export 5g log button, the Import PCAP or 5g log button, the Leg list, the Call list and the Call flow button.

Traffic collector	CD	R Signaling logs	Media calls	Media logs	Media conf
C C C Cust 1m 10m 1h 4h 12h 24h 1d-2d 2d-3d	GO Share Rows: 17 / 17 1-1	7 Fetc	h: 10 100 300) 1k 3k File-I	PCAP
Export 5g log Import PCAP or 5g log Leg list Cal	I list Call flow Info)		

The interval selector allows you to limit the number of packets fetched from the DB to those belonging to the latest period (1m, 10m, 1h, etc) or custom period only, while the row count selector limits them to only the top X rows.

To apply the settings of the selectors, click GO. The Rows label shows the current number of rows displayed with filters applied.

To create a shared link based on the information displayed at the current screen, click Share. For more information see Shared links.

To export the currently displayed packets into a text file, click **Export log file**. To export packets for a certain interval into a PCAP file, choose an interval in the Interval strip, click **File PCAP** on the Row limit strip and then **GO**. To import logs from a text file or Wireshark-readable PCAP format, click **Import PCAP or 5g file**. You can also drag and drop a PCAP file right to the window. Please note that the import function affects the web interface only and doesn't change the DB. That is why imported data will disappear once you reload or leave the screen.

To view the full list of legs recognized in the current log, click Leg list. The system will open a new Leg list window.

To view the full list of 1-leg and 2-leg calls based on the current log, click **Call list**. The system will open a new Call list window.

To view the packets of a particular one- or multi-leg call in a timely organized flow form, click Call flow.

2.3. Signaling logs

Once signaling packets are loaded, they are displayed in a table with the predefined sort. By default, the sort is done by the **Capture time** column, this organizes packets correctly on the timeline. All 5gVision table capabilities are supported (like **Filtering**, **Column selection**, **Column resizing**, **Export**. See more in User interface).

Export 5g log Impo	rt PCAP or 5g lo	og Leg	list Call list Call flow	Info	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,						
			=42294474bd2e11e4b75								
Capture time, J GMT	offset from first, sec	Offset from prev, sec	Call ID	SRC address	DST address	Customer from CDR	Vendor from CDR	Leg	Dir	Packet size	Packet data
015-02-25-20:38:30 752389	0.000000	0.000000	42294474bd2e11e4b7580 10.2	20.30.40	10.10.10.10	1		1	src->	1043	INVITE sip:1515151515151
015-02-25 20:38:30.800189	0.046800	0.046800	42294474bd2e11e4b7580(10.	10.10.10	10.20.30.40			1	<-dst	410	SIP/2.0 100 Trying Via: S
015-02-25 20:38:30.834953	0.081564	0.034764	427a80f Niew in Call flow	N	11.11.11.11			2	src->	1376	INVITE sip:1515151515151
015-02-25 20:38:30.880189	0.126800	0.045236	427a80f V Add to filter		10.10.10.10			2	<-dst	915	SIP/2.0 100 Trying v: SIP
015-02-25 20:38:30.888081	0.134692	0.007892	427a80f		10.10.10.10			2	<-dst	764	SIP/2.0 603 Declined v: \$
015-02-25 20:38:30.888385	0.134996	0.000304	427a80f		11.11.11.11			2	src->	465	ACK sip:151515151515
015-02-25 20:38:30.893506	0.140117	0.005121	4283750 View selected p	backet(s)	22.22.22.22			3	src->	443	Setup Q.931 { CallRefer
015-02-25 20:38:30.894150	0.140761	0.000644	4283750 View selected l	eg(s)	10.10.10.10			3	<-dst	139	CallProceeding Q.931 {
015-02-25 20:38:30.897753	0.144364	0.003603	4283750 🖒 View all legs		10.10.10.10			3	<-dst	117	ReleaseComplete Q.93
015-02-25 20:38:39.443636	8.690247	8.545883	479c280 Export to Excel		33.33.33.33			4	src->	1313	INVITE sip:151515151515
015-02-25 20:38:39.449817	8.696428	0.006181	479c280 Colort coll cont	anta	10.10.10.10			4	<-dst	721	SIP/2.0 100 Trying Via: S
015-02-25 20:38:40.762174	10.008785	1.312357	479c280	ents	10.10.10.10			4	<-dst	1211	SIP/2.0 183 Progress Vi
015-02-25 20:38:40.764414	10.011025	0.002240	422944 Select col conte	ents	10.20.30.40			1	<-dst	708	SIP/2.0 183 Progress Vi
015-02-25 20:38:41.165816	10.412427	0.401402	479c280 🔀 Cnt: 2		10.10.10.10			4	<-dst	1301	SIP/2.0 200 OK Via: SIP/
015-02-25 20:38:41.167477	10.414088	0.001661	422944 💥 Remove all high	hlights	10.20.30.40			1	<-dst	1128	SIP/2.0 200 OK Via: SIP/
015-02-25 20:38:41.168310	10.414921	0.000833	479c280	72	33.33.33.33			4	src->	880	ACK sip:151515151515
015-02-25 20:38:41.169538	10.416149	0.001228	422944		10.10.10.10			1	src->	696	ACK sip:151515151515
015-02-25 20:38:45.815047	15.061658	4.645509	422944		10.10.10.10			1	src->	750	BYE sip:15151515151515
015-02-25 20:38:45.816974	15.063585	0.001927	42294474bd2e11e4b7580(10.1	10.10.10	10.20.30.40			1	<-dst	529	SIP/2.0 200 OK Via: SIP/
015-02-25 20:38:45.818098	15.064709	0.001124	479c280ebd2e11e4a85b0(10.	10.10.10	33.33.33.33			4	src->	928	BYE sip:151515151515(
2015-02-25 20:38:45.823737	15.070348	0.005639	479c280ebd2e11e4a85b0(33.3	33.33.33	10.10.10.10			4	<-dst	761	SIP/2.0 200 OK Via: SIP/

To view the contents of an individual packet, right-click on the required row and choose View selected packet(s). Another way to do it is to click the packet content in the Packet data column. This will open the Packet viewing window containing information of the required packet. You can ctrl-click several rows to select them all at once and then use the View selected packet(s) option to view the selected packets in one window. You can also ctrl-click in the Packet data column of the required packets to open several windows with the packet info which might be handy if you want to compare several packets.

To view all packets forming a call leg, right-click on a packet belonging to a required leg and choose View selected leg(s). You can also ctrlselect several packets, belonging to different legs, and view all their packets in the same window (same as multiple selection of packets above).

To view the call flow figure, click the Call flow button. This will open the Call flow viewing window. The result will depend on the value in the Call ID column filter and the selection of packets in the table.

If a Call ID filter is present in a filter field above the respective column:

- If no table rows are selected show a Call flow for all packets belonging to filtered Call IDs.
- If one row is selected same as above, show a Call flow for all packets belonging to filtered Call IDs.
- If several rows are selected show a Call flow for all packets with the same Call IDs as the chosen ones. This way you may choose to show only certain legs out of several present in a log table. No need to choose all the packets in a leg, one packet will be enough to show a full leg.

If the **Call ID** filter is empty:

- If no table rows are selected show a Call flow for the leg with the Call ID of the first packet in a table.
- If one row is selected show a Call flow for all packets with the same Call ID as the selected packet.
- if several rows are selected show a Call flow for all packets with the same Call IDs as the chosen ones.

Please note that it is possible to filter SRC/DST IPs using whole networks, like this: =10.20.30.55/24. Network filtering works only with = or != signs.

2.4. Leg list

To view all legs in the currently displayed log, click the Leg list button. The system will open a new window showing Call ID, leg SRC and DST addresses and the list of packets constituting a leg.

			Click 12294474bd2e11e4t	075	1						_	_
S List of all call legs					A.				(Leg list	?	S.
First packet	Call ID	SRC address	DST address	SRC)ST mber	Click for Call flow	No of packs	Packets	Call dur	PDD	T
2015-02-25 20:38:30.753389	42294474b	10.20.30.40	10.10.10.10	View in Call flow	N	51515	Completed	7	INVITE, 100, 183, 200, ACK, BYE, 200	4.6	10.0	1
2015-02-25 20:38:30.834953	427a80fabd	10.10.10.10	11.11.11.11	Y Add to filter	1	51515	Rejected	4	INVITE, 100, 603, ACK			
2015-02-25 20:38:30.893506	42837502b	10.10.10.10	22.22.22.22	🦙 Clear filter	1	51515	Completed	3	Setup, CallProceeding, ReleaseComple	te		_
2015-02-25 20:38:39.443636	479c280ebc	10.10.10.10	33.33.33.33	View all legs	1	51515	Completed	7	INVITE, 100, 183, 200, ACK, BYE, 200	4.6	1.3	
				Export to Excel								
				Select cell cont	ents							
				Select col conte	ents							
				X Remove all high	hliahts							

You may open the Call Flow window for the desired leg using the link in the leg status column or with the help of the pop-up menu.

To view the leg's packets (see Packet viewing), you may use the pop-up menu or click the content of the Packets column.

2.5. Call list

To view all 1 and 2-legged calls in the currently displayed log, click the **Call list** button. The system will open a new window showing leg parameters, such as Call ID, legs' SRC and DST addresses and the list of packets constituting the first and the second leg.

raffic collector						CDR	Signaling log	s) Medi	a calls Media logs	Media conf Mo	ore ?	$\varnothing \otimes \square$
C C Cust	1m 10m 1b	4h 12h 24	h 1d-2d 2d-3d	(GO) (S	hare Rows	: 17 / 17 1-17	Fet	ch: 10	100 300 1k 3k File	-PCAP		
Export 5g log Impo	rt PCAP or 5 <u>0</u>	log	Leg list C	all list Call	flow Info							
			=2526087	738_85291CK@								
🖉 🔀 List of all 1- or	2-leg calls									Call list ?	⊘ ᠿ ९	⁄ ଛ]
1 - 😿 C - Rows: 1												
1 First packet capture time, GM		D Call ID	SRC address	DST address	SRC number	DST number	Click for Call flow	No of leas	Packets Leg 1	Packets Leg 2	Call dur	Call dur P
2015-12-16 19:11:28.7	50380 25260)87 cf458f7a	1401020308	RELEVAN	View in 🤇	Call flow	Completed	2	VITE, 100, 183, 200	INVITE, 100, 183, 2	00 522.4	522.5 0
1					Add to fi	Iter						
1					View all	leas						
1					Export to	Excel						
1					Select ce	ell contents						
1					Select co	ol contents						
1					🔀 Remove	all highlights						
1						@2						
1						4) <u>@</u> 5						

You may open the Call Flow window for the desired leg using the link in the leg status column or with the help of the pop-up menu.

To view the first or the second leg's packets (see Packet viewing), you may use the pop-up menu or click the content of the Packets Leg N column.

2.6. Call flow

The Call flow window graphically presents the call as a series packet exchanges between switches.



5gVision parses the packets and automatically divides the call into a number of legs, taking into account Call IDs and IPs involved. The system forms a new leg whenever any address or port in a SRC IP - DST IP pair is changed. Clicking on the Call ID link on top of the leg column or on the individual packet name will open a new Packet viewing window showing all packets that comprise the leg or a single packet respectively.

You may also remove the undesired packets from the displayed call flow by clicking the red cross next to the leg ID.

You may also resize the window to display all legs at the same time. Double click on the resize icon to revert the window to the default height and width.

The window contains the **Share selected** button which allows you to share the required legs (marked with checkboxes) as a **Shared link** (see **Shared links**). This feature comes the additional benefits on top of the usual ones of the shared links - you may hide your partners and send these logs to your vendor and vice versa which is much more convenient than editing the required bits out of raw logs.

There is also the **PCAP selected** button that lets you export the selected legs to a pcap file.

2.7. Packet viewing

The packet viewing window presents packet content in textual form. The amount of information depends on where and how the window was invoked: it is possible to view a single packet, all packets pertaining to a single leg or the whole call.

L	Select all Raw log Selected packets (1) I Selected legs All legs Call thow C - C +	
20	115-02-25 20:38:30.834953 === 0.081564 === Leg 2 === SRC->DST === 10.10.10.10 ==> 11.11.11.11	-
IN	VIIE SID:1515151515151500(11.11.11.11)USER=phone SIP/2.0	
	a. SIP/2.0/0DP 10.10.10.10.10.0000,1001,01a1011-2911G40K-427a0340002011e4a641001b21603010,SIQ-10111606	l
Vi	a: SIP/2.0/0DF 10.10.10.10.11.5063;mort=5063;hranch=z0hG/bk/.427ab/f8hd2e11e4a641001b216c3d18,sig=c0b5216	l
F	rom: <sin:1717171717171717@10.10.11.15063;user=nbone>:tag=427kGOEO75sEE8fbl/O+bBBPEAtn6ggAg</sin:1717171717171717@10.10.11.15063;user=nbone>	l
Тс	v <sip:15151515151515515011.11.11.11.11.vser=phone></sip:15151515151515515011.11.11.11.11.vser=phone>	l
C	all-ID: 427a80fabd2e11e4a641001b216c3d18@10.10.10.11	l
C	Seg: 1 INVITE	l
C	ontact: <sip:1717171717170210.10.10.11:5063:user=phone></sip:1717171717170210.10.10.11:5063:user=phone>	l
С	ontent-Type: application/sdp	l
AI	Iow: ACK, BYE, CANCEL, INFO, INVITE, OPTIONS, REFER, REGISTER, UPDATE	l
М	ax-Forwards: 69	l
U	ser-Agent: TS-v4.6.0-10b	
Ci	sco-Guid: 1041351716-3173913060-2593287266-1842828445	I.
С	ontent-Length: 322	ľ
R	ecord-Route: <sip:aqeaecjtkf+u36or4emssdo1+6udaar0ig0b@10.10.10.10;ir></sip:aqeaecjtkf+u36or4emssdo1+6udaar0ig0b@10.10.10.10;ir>	Ľ
R	ecord-Route: <sip:aqeaelvvvxqtg7pfckgzljbgldidaaq0vvcd@10.10.10.11;ir></sip:aqeaelvvvxqtg7pfckgzljbgldidaaq0vvcd@10.10.10.11;ir>	
V=	0	
0=	1424896710 1424896710 IN IP4 10.10.10.10	
S=		l
C=	IN IP4 10.10.10	l
t=	00	l
m	audio 31448 RTP/AVP 18 4 0 8 101	l
a=	mpmap:18 G729/8000	l
a		l
a=	-11µ11dp.4 G7207000	
a=	-mmp.4 ammt.a-ycs	l
a-		

The toolbar at the top of the window allows the user to do the following:

- Select the whole text (for subsequent copying) with the help of the Select all button.
- Disable or enable text formatting with the help of the Raw log/Formatted button.
- Show the selected packet(s) (Selected packets), the leg to which the packet(s) belong (Selected legs) or all legs in the Signaling logs (All legs, up to 1000 packets in total).
- Switch to viewing the call in the Call flow window.

For your convenience it is possible to change the font size using the +/- buttons.

It is possible to expand or collapse a packet body in a packet viewer window by clicking on its header (INVITE, etc.).

3. Media collector

The media collector gathers media packets in real time and lets you listen to conversations in any codec.

3.1. Overview

The Media collector module gathers media packets in real time for pre-defined IP addresses and number masks, either fully or randomly, and allows users to listen to the recorded media in most commonly-used codecs.

Capturing can work in 2 modes:

- You may set up signaling IPs and number masks for which the media will be recorded randomly. To insure that small customers, vendors, or areas get a certain number of calls recorded each hour, you may set this minimal number of calls per each object. Thus, small objects will have at least the minimum, large object with a lot of traffic will have hundreds or thousands of calls recorded every hour.
- You may force the system to record the next 5/10/20 calls in a row for specific IPs/numbers, for instance, if you are making a call and want to be sure it will be recorded.

Since media is recorded randomly and only for a short initial interval (we recommend 60-120 seconds) - it won't create too much additional load to the system, even if you want to monitor quality for all your customers and vendors.

Usually, 10-20 calls per hour is enough to understand what is going on with a specific vendor->area combination, there is no need to record absolutely every call.

The Media collector module requires the Signaling collector module installed to function.

IPs and number masks to collect media for are configured in the Media conf table.

The resulted raw packets can be viewed in the Media logs table, and full recorded calls can be listened to in the Media calls table.

3.2. Media conf

The Media conf table allows you to set up the SRC/DST signaling IP addresses and/or number masks to record only the calls that match these criteria.

The system will filter the signaling logs first, figure out the media IPs, and then start recording of the media stream for the configured calls in a random or full mode.

Rew	Status	SRC signaling address / net	DST signaling address / net	SRC number pattern	DST number pattern	Min recorded calls per hour	Count conn.	Record time per call, sec	Capture each of next X calls	Comment
4	1			987654321	123456789	10	V	60	Next 5 calls	
3	1	3.3.3.3	4.4.4.4			10	1	60	Next 20 calls	
2	1		2.2.2.2			5	1	30	Random mode	
1		1.1.1.1		123456789		10	V	60	Random mode	

The user may define the following settings:

- SRC/DST signaling address / net the calls from/to these addresses will be considered for media recording.
- SRC/DST number pattern the calls with these SRC/DST number patterns will be considered for media recording.
- Min recorded calls per hour the sniffer will try to record this number of calls each hour. Without this setting, objects with small traffic
 may not have enough calls recorded in a random mode, as they will be competing for the recording slots with much larger objects.
- Record time per call, sec the duration of a sample to be recorded, we recommend 60-120 seconds. The longer are the recorded calls, the less calls will be recorded per hour.
- Capture each of next X calls when recording calls, the system may work in two modes. In the Random mode calls to be recorded will
 be chosen randomly. In the Next 5/10/20 calls mode the system will record the next 5, 10, or 20 calls in a row once the setting is applied,
 and then switch to the Random mode again.

Please note that if you change the settings, it may take up to a minute for a sniffer to pick them up.

With the help of a right-click menu, you may view pre-filtered recorded calls by clicking on the View in Media calls menu option.

3.3. Media calls

The Media calls table contains recorded calls in a playback-ready format. You may easily find a call you need filtering by IPs or numbers.

ie, 🖵	Call ID	SRC signaling	DST signaling	SRC	DST		Codecs	Packet	Lost	Captured	Early media	Connect	Media	Audio	Audio
9 429017	402878847	autress 8 81 2 128 196	88 198 190 30	77751895708 1	25#99893	20836	8 G 711a	83	packets 0	25	25		uelecteu	piay	get file
1576427	402878909	1 81.2.128.196	88,198,190,30	77752635015 12	25#99890	98791	8: G.711a	2663	2	32.1	32.1			play/pause, ctrl-click to jum	get file
1.975213	402878988	3 81.2.128.196	88.198.190.30	77754307876 1	25#99890	59552	18: G.729	4109	3	41.1	41.1			play/pause, ctrl-click to jum	get fil
3.959021	402879048	1 81.2.128.196	88.198.190.30	View in Media	aloge	2785	8: G.711a	1215	0	14.6	14.6			play/pause, ctrl-click to jum	get fil
6.126221	402879106	1 81.2.128.196	88.198.190.30		a iogs	5169	8: G.711a	434	0	5.3	5.3				get fil
3.525727	402879122_	6 81.2.128.196	88.198.190.30	View in Signa	uing logs	7959	18: G.729	3382	0	33.8	33.8			play/pause, ctrl-click to jum	get fil
8.589387	402879135_	1 81.2.128.196	88.198.190.30	View in Call fi	low	7044	18: G.729	5926	2	59.3	59.3			play/pause, ctrl-click to jum	get fil
4.473290	402879315_	1 81.2.128.196	88.198.190.30	Add to filter		3516	8: G.711a	245	0	7.3	7.3			play/pause, ctrl-click to jum	get fil
9.823112	402882584_	3 81.2.128.196	88.198.190.30	🙀 Clear filter		7959	18: G.729	3299	1	33.0	33.0				get fil
1.301528	402882643_	1 81.2.128.196	88.198.190.30	Export to Exc	el	2347	8: G.711a	1448	0	43.4	43.4			play/pause, ctrl-click to jum	get fil
5.687776	402882746_	1 81.2.128.196	88.198.190.30		ntents	2347	8: G.711a	1329	0	39.8	39.8			play/pause, ctrl-click to jum	get fil
9.071047	402882782_	7 81.2.128.196	88.198.190.30		-teete	7409	8: G.711a	2876	0	34.5	34.5			play/pause, ctrl-click to jum	get fil
7.055170	402882914_	2 81.2.128.196	88.198.190.30	Select col col	ntents	0071	8: G.711a	1054	1	31.6	31.6				get fil
7.577698	402883013_	1 81.2.128.196	88.198.190.30	💥 Remove all h	ighlights	7975	18: G.729	5914	4	59.2	15.8	yes			get fil
2.581946	402883104_	7 81.2.128.196	88.198.190.30	[@1]	@2	9587	18: G.729	325	0	3.2	3.2			play/pause, ctrl-click to jum	get fil
1.728602	402883117_4	4 81.2.128.196	88.198.190.30	@3 @4	@5	8791	3: G.711a, 18:	1907	0	21.1	11.8	yes		play/pause, ctrl-click to jum	get fil
1.686772	402883200_	3 81.2.128.196	88.198.190.30			2882	18: G.729	692	0	6.9	6.9			play/pause, ctrl-click to jum	get fil

To display the recorded calls, click the period you want to investigate in the interval selector.

You may play back the call by clicking the **play/pause** button in the **Audio play** column. The system will display the graphical representation of a sound stream. To pause the file, click the field again. **Ctrl-click** on the sound bar will jump playback to a click position.

You may also download the file by clicking the Get file link in the Audio get file column.

With the help of a right-click menu, you may view the call in Media logs or Signaling logs and display the Call flow for its signaling packets.

3.4. Media logs

This table contains data on raw media packets collected by the system.

Capture time, U GMT	Call ID	SRC address	DST address	SSRC	Seq	RTP timestamp	Codec	Packet
2015-12-16 19:51:00.010443	ACCESSION, DESCRIPTION (C.	8.98.98.00	81.2 XXX XXX	24775b55	54595	420148416	8: G.711a	214
015-12-16 19:51:00.018209	ACCESSION, TOPOTHE SQUALE.	HAD KIN PHO	66,706,700,00	10084	25447	1481362244	18: G.729	74
2015-12-16 19:51:00.026447	ACCESSION, DESCRIPTION OF	H. H. H. K. M.	81.2 XXX XX4	24775b55	54596	420148576	8: G.711a	214
2015-12-16 19:51:00.037790	ACCESSION, DESCRIPTION (C.	84.2 CB 864	61,701,701,00	10084	25448	1481362404	18: G.729	74
2015-12-16 19:51:00.051266	ACCESSION, DESCRIPTION OF	68, 108, 108, 201	81.2 X 83 X 84	24775b55	54597	420148736	8: G.711a	21
2015-12-16 19:51:00.057409	ACCESSION, TOPOTHE SQUALE.	HAD KIN PHO	66,706,700,00	10084	25449	1481362564	18: G.729	74
2015-12-16 19:51:00.067224	ACCESSION, DESCRIPTION OF	61.100.100.20	81.2 XXX XX4	24775b55	54598	420148896	8: G.711a	21
2015-12-16 19:51:00.077640	ACCESSION, TOPOTHE SQUALE.	84.2 KB 864	68,708,709,00	10084	25450	1481362724	18: G.729	74
2015-12-16 19:51:00.090891	ACCESSION, DESCRIPTION (C.	66, 106, 106, 20	81.0 XXX XX4	24775b55	54599	420149056	8: G.711a	21
2015-12-16 19:51:00.097277	ALCOHOL, DESCRIPTION (84.2 CB 864	61,701,701,20	10084	25451	1481362884	18: G.729	7
2015-12-16 19:51:00.107201	ACCESSION, DESCRIPTION OF	61.100.100.20	81.2 XXX XX4	24775b55	54600	420149216	8: G.711a	21
2015-12-16 19:51:00.118067	ACCEPTED, DESCRIPTION, D	81.2 CB 810	61,701,701,20	10084	25452	1481363044	18: G.729	7
2015-12-16 19:51:00.131620	ADDRESS, DESCRIPTION (66, 106, 106, 20	81.0 XXX XX4	24775b55	54601	420149376	8: G.711a	21
2015-12-16 19:51:00.138556	ACCORDENCE, TOPOTHE SQUALS.	64.2 KR 864	68,708,709,00	10084	25453	1481363204	18: G.729	7
2015-12-16 19:51:00.147775	ACCESSION, DOTATING SQUALE.	68,108,106,00	84.01.038 X 84	24775b55	54602	420149536	8: G.711a	214
2015-12-16 19:51:00.159022	ACCESSION, TOPOTHER SPICE, D	84.2 CB 894	61,701,701,20	10084	25454	1481363364	18: G.729	74
2015-12-16 19:51:00.171559	ADDRESS, DESCRIPTION (66,106,106,20	81.0 XXX XXX	24775b55	54603	420149696	8: G.711a	21
2015-12-16 19:51:00.178396	AND REAL TO STRENG DE LA	84.2 CB 884	66,706,706,20	10084	25455	1481363524	18: G.729	7
2015-12-16 19:51:00.187592	ACCESSION, DESCRIPTION OF	65, 105, 105, 201	81.2 XXX XX4	24775b55	54604	420149856	8: G.711a	21
015-12-16 19:51:00.198783	ACCESSION, TOPOTHER SPICE, D	84.2 CB 894	61,701,701,20	10084	25456	1481363684	18: G.729	7
2015-12-16 19:51:00.211579	ACCESSION, DESCRIPTION OF	66,106,106,20	61.0 XXX XX4	24775b55	54605	420150016	8: G.711a	21
2015-12-16 19:51:00.219453	ACCESSION, TOPOTHER SPIRE	84.2 CB 884	66,706,706,20	10084	25457	1481363844	18: G.729	7
2015-12-16 19:51:00.227876	ADDRESS, DESCRIPTION (68,498,496,20	81.2 XXX XX4	24775b55	54606	420150176	8: G.711a	21
2015-12-16 19:51:00.240305	ACCEPTED TO STRENGT ALL	H 2 CB FM	66,106,100,00	10084	25458	1481364004	18 [:] G 729	7

To export the filtered data for the chosen interval into a Wireshark-readable PCAP format, please choose File-PCAP in the row count selector and click GO.

4. IP whitelist

The IP whitelist helps you detect intrusions to your VoIP network analyzing all the IP addresses collected from the signaling packets.

4.1. Overview

The IP whitelist module collects all IPs that send H.323 setups or SIP invites to your switch, independently of switch CDRs, from raw packets, and in case a number of per hour occurrences of new IPs that are not in the whitelist exceeds a preset threshold, you will be alerted. IP whitelist can be accessed by adding a IP whitelist screen.

This feature might be useful to catch any unauthorized traffic originating from your server, either from your own VoIP switch, if it is cracked and the config is changed, or from a new switch installed by intruders. In the latter case, it could take a carrier several days till they catch the extra traffic that is originating from their IPs open at their vendors. No such traffic will be visible in carrier's switch or billing. This is why this whitelist should be created independently, on a different server (a 5gVision logging server) the intruders have no access too, as any precautions at your switch will be bypassed, if this server with a VoIP switch is compromised.

If an IP whitelist module is purchased, log collection via mirroring is a more preferred method of setting up the logger (see Collection methods), as in case of collecting logs over SSH, the attackers can block logs collection, once the softswitch server is compromised. This is not possible with mirroring, as 5gVision will be able to get and analyze all the packets traveling through your network.

The main table of the IP whitelist module is Collected IPs, where you can see all collected IPs with showing leg, direction, customer, vendor.

Configuration of the IP whitelist module is made via the corresponding Whitelist config tables.

4.2. Collected IPs

All collected IPs are added to the Collected IPs table.

IP collected from traffic packets	Port	Dir SRC/DST	Leg and direction	from the White List	Customer, Vendor or own switch	SIP	H.323 setups
0.0000.00	5060	0: SRC	Leg 1, Customer SRC	Customer IP NOT FOUND!		922	
10.712474	5060	0: SRC	Leg 1, Customer SRC	A REAL PROPERTY.	Training Talanger	607	
10.00	5060	0: SRC	Leg 1, Customer SRC	0.070120	084	510	
1 C 1 C 1 C 1 C 1 C 1 C 1 C 1 C 1 C 1 C	5060	0: SRC	Leg 1, Customer SRC	10.101.00.005	873	3362	
1 (1) (1) (1) (1) (1)	5060	0: SRC	Leg 1, Customer SRC	10.100.00.000	873	31	
2 (C. 1997)	5060	0: SRC	Leg 1, Customer SRC	11.000071	Telepali .	38	
10-00-00 MB	5060	0: SRC	Leg 1, Customer SRC	12,1040,10	TRACEOR - Again	9	
10-00-00 Add	5060	0: SRC	Leg 1, Customer SRC	12,1040,10	TRACE UNIT - Again	8	
(b) (75, 168, 20)	5060	0: SRC	Leg 1, Customer SRC	NUMBER OF CONTRACTOR	TRACE UNIT - Design Tall	109276	
(C) 40,460,824	5060	0: SRC	Leg 1, Customer SRC	51,75,000,004	Level 3	290	
(1) 40 403 403	5060	0: SRC	Leg 1, Customer SRC	51.15.100 MB	Level 3	26	
10 X 10 K 10 K 10 K	5060	0: SRC	Leg 1, Customer SRC	50.00 147 148	07	26	
B-C 80-800.8	5060	0: SRC	Leg 1, Customer SRC	50.000.000.000	Interdisting Telephone	7454	
40.00 40 400.00	5060	0: SRC	Leg 1, Customer SRC	50.000.000.000	Interdition Telecom	8495	
400.001-00.001	5060	0: SRC	Leg 1, Customer SRC	N. 179, 199, 199	Interdisting Telephone	8096	
8-00-00-m	5060	0: SRC	Leg 1, Customer SRC	54.000.000.000	Dime.	522	
8.98.03.28	5060	0: SRC	Leg 1, Customer SRC	56,100,100,014	Televali	47	
8,300-68,40	5060	0: SRC	Leg 1, Customer SRC	50 (199 (199 (199	Perigram Development	18	
00.841-000	5060	0: SRC	Leg 1, Customer SRC	50 (19) (90) (90)	Perigen Designers	12	
0.00.01.00	5060	0: SRC	Leg 1, Customer SRC	50 190 194 198	TRACTORIA - Design Call- Name 2	52108	
8.06.01 HT	5060	0: SRC	Leg 1, Customer SRC	50,100,104,107	TRACEORE - Design Call- Name 1	52406	
88-000 HR	5060	0: SRC	Leg 1, Customer SRC	64,075,003,764	Level D	1485	
100.8307	5060	0: SRC	Leg 1, Customer SRC	4 10 10 10 10 10	Francisco	184	
104 per 04 per 04	5060	0: SRC	Leg 1, Customer SRC	08.08004.00°	100	212473	

The system distinguishes packets on basis of several parameters:

- IP collected from traffic packets source or destination IP address of the packet.
- **Port** source or destination port of the packet.
- Dir SRC/DST source or destination information of the packet was taken into account.

So if the system collects packets with an identical IP and port there are still can be 2 records in the table differentiated by direction.

The table contains records with the following information included:

• Leg and direction - leg number and direction of the packet, detected on basis of correlation of the Dir SRC/DST and Customer,

Vendor or own switch parameters.

- IP net match from the White List IP or IP net against which the collected IP was matched. If the collected IP does not match any defined pattern, the red label IP NOT FOUND! is displayed.
- Customer, Vendor or own switch entity to which the matched IP is supposed to belong.
- SIP invites and H323 setups Number of SIP INVITEs or H.323 SETUPs that have sent to/arrived from the collected IP within the specified interval.

For your convenience, it is possible to add the desired IP(s) into whitelist from this screen by selecting the required row or rows, invoking the pop-up menu and selecting Add selected to White List.

CD	R Traffic logs Collected	IPs WL customers WL vendors WL	own switc
30d 60d G(C Rows: 244		
and direction	IP/net mat from the Whi	tch Customer, ite List or own s	Vendor witch
mer SRC	Customer IP NOT FOU	View in CDRs	
mer SRC	04/70/04/10	View in Traffic logs	
mer SRC	0.00.00.00	- Add colocted to White Liet	
mer SRC	19.115-09.505	Add selected to white List	
mer SRC	10.110.001	Add all customers to White List	
mer SRC	FD-609-6071	I Add all vendors to White List	
mer SRC	PT 10411.00	Add to filter	
mer SRC	PT 10411.94	Ver Clear filter	
mer SRC	10,111,141,00		
mer SRC	ST 10488.554	Export to Excer	
mer SRC	ST 10 100 140	Select cell contents	
mer SRC	55/00/54P/548	Select col contents	
mer SRC	10.018 10.046	X Remove all highlights	
mer SRC	55-028° 103, 048		
mer SRC	10.018-02.019		
mer SRC	10.12108-10		

4.3. Whitelist config

IP whitelist configuration consists of several tables:

- WL customers needed to detect unauthorized traffic not originating from your customer.
- WL vendors needed to detect unauthorized traffic terminating to vendors.
- WL own switch needed to detect pirate switches installed on the same server as your own switch.
- Own nets needed to detect which IPs belong to customers/vendors and can never be assigned to a pirate switch in your network.

By default all users can edit these tables. But it is possible to allow access only for certain users to add/edit/remove customers, vendors, own switches and nets from the whitelist. Please send a request to 5gVision support for this purpose. You may manually add IPs and nets against which the collected IPs are matched in the WL customers, WL vendors and WL own switch tables. All auto-added IPs via the Collected IPs screen will also appear in the former two tables.

To add an allowed IP or IP net to the WL customers table, please click the green plus.

CC C C C C C C Cancel GO Rows: 124								
Row	Status	Whitelist Customer IP/net	Whitelist Customer port range	Customer name	Last change, GMT	Change mode	Last editing user	Comment
							[
135		100.50 101.001	8664	Class Telecome	2015-05-04 16:16:47	Edited manualy	9	
134	1	64, 16, 16, 16, 14, 14, 14, 14, 14, 14, 14, 14, 14, 14	8660	13	2015-04-28 16:53:34	Edited manualy	9	
133	1	6170126	8660	CMP	2015-04-28 16:52:03	Edited manualy	9	
132	1	A 10.712 104	890	One Bourds	2015-04-28 16:52:28	Edited manualy	9	
131	V	100.00.000	800	Testings Party	2015-04-28 16:46:22	Added manualy	9	
130	V	100.100.00100	800	Testings Party	2015-04-28 16:46:02	Edited manualy	9	
129	1	101144120140	890	Testing Colorida	2015-04-28 16:45:14	Edited manualy	9	
128	1	200 AR 200 100	9000 - 000 F	Testing (204 (2008))	2015-04-28 16:18:52	Added manualy	9	
127	1	66,000,000,000		Carta	2015-03-12 13:28:17	Added manualy	9	
126	V	5 THE REPORT		Tohers	2015-03-12 13:27:58	Added manualy	9	
125	V	60,000,000,004		Temp car	2015-03-12 13:27:28	Added manualy	9	
124	1	66.009.009.000		Rentified Transports	2015-03-12 13:26:56	Added manualy	9	
123	1	198.5425079		Charle Statistics and	2015-03-12 13:25:57	Added manualy	9	
122	1	1988, 998, 2002, 989		PhoneBine	2015-03-12 13:22:24	Added manualy	9	
121	1	4/2014 (227		PhoneBine	2015-03-12 13:22:24	Edited manualy	9	
120	1	201.01.40/140		Tellin Content of California	2015-03-12 13:13:15	Added manualy	9	
119	1	2011 S 82 S 82 S		Telecove Statedor CTE	2015-03-12 13:11:16	Added manualy	9	
118	1	12,1040,18		TRACTORE-Auto	2015-03-11 21:42:45	Added manualy	9	
117	1	12,10403,58		TRACTORE-Auto	2015-03-11 21:42:31	Added manualy	9	
116	1	11.49(040)71		Tempolar	2015-03-11 21:42:07	Added manualy	9	
115	1	200.40.000.000	8990	Testine (254 (2008))	2015-03-11 21:13:55	Added manualy	9	
114	1	200 AU (200 SU)	1000+ 30FE1	Teamor (Che (PRPC))	2015-03-11 21:12:33	Added manualy	9	
113	1	200 AU (94 PT)	10004-00701	Testing and a provide	2015-03-11 21:11:24	Added manualy	9	

A new record will be added to the table, with the following parameters:

- Status whether the record is enabled (and takes part in IP matching) or disabled.
- Whitelist Customer IP/net define the IP or net against which the collected IPs will be tested.
- Whitelist Customer port range define the port or port range against which the collected ports will be tested.
- Customer name optional information about the customer, to which the IP belongs.
- Last change, GMT date and time when the record was added or edited the last time.
- Change mode If the IP was added through this screen, the system will show Added manually in this column. If the IP was added from the Collected IPs screen with the help of a pop-up menu, the column will have the Added from collected text.
- Last editing user ID of a user who edited the record at the latest.
- Comment.

To save the added row, click **Save**. To discard the changes before they are saved, click **Cancel**.

To edit or remove a record, select it in the table and click the pen or red cross button respectively.

The WL vendors and WL own switch tables have the similar parameters.

In the Own nets you should just enter full owned networks where your VoIP switches are located.