

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 coll		2d 2d-3d GO Share Rows: 17 /		g logs Media ca Fetch: 10 100				f More 🦓 🖉 🗖 🤇
Califyit		list) (Call list) (Call flow) (Info			1			м
selected			DST ddress	Customer from CDR	Vendor from CDR	Leg	Dir P	acket Packet size data
selected	X 738048-73.79.708	X 0010ec1s@d8.108.108.30	.19 0.30			1	src->	1131 INVITE sip:
			1.127.52			2	src->	1364 INVITE sip:
n Offset from et prev. packet	5060 5060	5060 5060	.190.30				<-dst	719 SIP/2.0 100 Trying Via: SI
0.000000		3000	.70.109				<-dst	315 SIP/2.0 100 Trying Via: SII 1255 SIP/2.0 183 Progress Via
-		- Cit	. 190.30				<-dst	929 SIP/2.0 183 Progress Via
0 0.027830	-	Packet						1345 SIP/2.0 200 OK Via: SIP/2
0.004807	-	A Trung Palcker	70 409			1	<-dst	996 SIP/2.0.200 OK Via: SIP/2
8 0.167751	100 Trying	Select all Raw log	Selected p	ackets Select	ted legs (1)	All leg	. [Call flow - +
0 0.166722		18 Select all Raw log	Belected p	derees Select	leu legs (1)	Airieg	>	
1 0.001701	183 Progress (G729)	2015-12-16 18:41:57 159	841 === 0.027	7830 === Leg	2 === SRC-	>пят	1	0.190.100.00 ==> 140.251
5 19.474684		INVITE sip:						instant - Prisant
8 0.001193	200 OK (G729)	Via: SIP/2.0/UDP	5060;rpc	ort;branch=	340K-8046580	0.0424	antes:	11.0549735106114;sig=1101
-	<hr/>							1008400810ec10;sig=890
6 0.000808	-							411e591b3549/3518ec1c
0.029084	ACK	From: <sip: To: <sip:< td=""><td></td><td></td><td></td><td>qtOu⊢</td><td>Yxr4e</td><td>E8XhWMa+HhPEyDV2wQAc</td></sip:<></sip: 				qtOu⊢	Yxr4e	E8XhWMa+HhPEyDV2wQAc
3 0.002083	INVITE (G729)	Call-ID:						
3 0.002140	200 OK (G729)	CSeg: 1 INVITE						
4 0.022261	АСК	Contact: <sip:110040000< td=""><td>1.944,000,000</td><td>:5061;user=</td><td>phone></td><td></td><td></td><td></td></sip:110040000<>	1.944,000,000	:5061;user=	phone>			
1 136.007137		Content-Type: application						
5 0.001574		Allow: ACK, BYE, CANCE	L, INFO, INVITE,	OPTIONS, REI	FER, REGIST	ER, U	PDATE	
0.001074		Max-Forwards: 69 User-Agent: TS-v4.6.0-11	oW					
0.000004	BYE	Cisco-Guid: 2940891100			004400			
6 0.000 961			-2753827301-24	44448927-890	301468			
6 0.000961 7 0.025811	200 OK	Content-Length: 299	-2753827301-24	44448927-890	301468			
-	200 OK						100.30	;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		CDR Signaling lo	gs Media calls	Media logs	Media conf
C E C Cust 1m 10m 1h 4h 12h 24h 1d-2d 2d-3	d GO Share Rows: 17 / 17	1-17	etch: 10 100 30	1k 3k File-I	PCAP
Export 5g log Import PCAP or 5g log Leg list	Call 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).

C B C Cust	m 10m 1h 4h	12h 24h 1d	2d 2d-3d GO Share Rows	: 21 / 21 1-21	Fetch: 10 100	300 1k 3k File	e-PCAP		
Export 5g log Import	PCAP or 5g lo	g 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 Packe size	t Packet data
2015-02-25-20:38:30 752389	0.000000	0.000000	42294474bd2e11e4b7580 10.20.30.40	10.10.10.10			1 s	c-> 1043	INVITE sip:15151515151515
2015-02-25 20:38:30.800189	0.046800	0.046800	42294474bd2e11e4b758010.10.10.10.10	10.20.30.40			1 <	dst 410	SIP/2.0 100 Trying Via: SI
2015-02-25 20:38:30.834953	0.081564	0.034764	427a80f View in Call flow	11.11.11.11			2 s	c-> 1376	INVITE sip:151515151515
2015-02-25 20:38:30.880189	0.126800	0.045236	427a80f Y Add to filter	10.10.10.10			2 <	dst 915	SIP/2.0 100 Trying v: SIP/2
2015-02-25 20:38:30.888081	0.134692	0.007892		10.10.10.10			2 <	dst 764	SIP/2.0 603 Declined v: SI
2015-02-25 20:38:30.888385	0.134996	0.000304	427a80f	11.11.11.11			2 s	c-> 465	ACK sip:1515151515156
015-02-25 20:38:30.893506	0.140117	0.005121	4283750 View selected packet(s)	22.22.22.22			3 s	c-> 443	Setup Q.931 { CallRefere
2015-02-25 20:38:30.894150	0.140761	0.000644	4283750 View selected leg(s)	10.10.10.10			3 <	dst 139	CallProceeding Q.931 { C
2015-02-25 20:38:30.897753	0.144364	0.003603	4283750 View all legs	10.10.10.10			3 <	dst 117	ReleaseComplete Q.931
2015-02-25 20:38:39.443636	8.690247	8.545883	479c280 Second to Excel	33.33.33.33			4 s	c-> 1313	INVITE sip:151515151515
2015-02-25 20:38:39.449817	8.696428	0.006181		10.10.10.10			4 <	dst 721	SIP/2.0 100 Trying Via: SI
2015-02-25 20:38:40.762174	10.008785	1.312357	479c280	10.10.10.10			4 <	dst 1211	SIP/2.0 183 Progress Via
2015-02-25 20:38:40.764414	10.011025	0.002240		10.20.30.40			1 <	dst 708	SIP/2.0 183 Progress Via
2015-02-25 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/2.
015-02-25 20:38:41.167477	10.414088	0.001661	422944 💥 Remove all highlights	10.20.30.40			1 <	dst 1128	SIP/2.0 200 OK Via: SIP/2
2015-02-25 20:38:41.168310	10.414921	0.000833	479c280	33.33.33.33			4 s	c-> 880	ACK sip:1515151515156
015-02-25 20:38:41.169538	10.416149	0.001228		10.10.10.10			1 s	c-> 696	ACK sip:1515151515156
015-02-25 20:38:45.815047	15.061658	4.645509	422944	10.10.10.10			1 s	c-> 750	BYE sip:151515151515
015-02-25 20:38:45.816974	15.063585	0.001927	42294474bd2e11e4b7580 10.10.10.10	10.20.30.40			1 <	dst 529	SIP/2.0 200 OK Via: SIP/2
015-02-25 20:38:45.818098	15.064709	0.001124	479c280ebd2e11e4a85b0(10.10.10.10	33.33.33.33			4 s		BYE sip:151515151515
015-02-25 20:38:45.823737	15.070348	0.005639	479c280ebd2e11e4a85b0(33.33.33.33	10.10.10.10			4 <	dst 761	SIP/2.0 200 OK Via: SIP/2

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.

			Lick 12294474bd2e11e4t	075	1							_	_
S List of all call legs					A					Le	eg list	?.	S.
First packet	Call ID	SRC address	DST address	SRC		ST nber	Click for Call flow	No of packs		С	all dur	PDD	T
2015-02-25 20:38:30.753389			10.10.10.10	View in Call flow		51515	Completed	7	INVITE, 100, 183, 200, ACK, BYE, 200	D	4.6	10.0	1
2015-02-25 20:38:30.834953	427a80fabd		11.11.11.11	Add to filter		51515	Rejected	4	INVITE, 100, 603, ACK				_
2015-02-25 20:38:30.893506			22.22.22.22	🙀 Clear filter		51515	Completed	3	Setup, CallProceeding, ReleaseCon				-
2015-02-25 20:38:39.443636	479c280ebc	10.10.10.10	33.33.33.33	View all legs	18	51515	Completed	7	INVITE, 100, 183, 200, ACK, BYE, 200	D	4.6	1.3	
				Export to Excel									
				Select cell cont	ents								
				Select col conte	ents								
				👷 Remove all high	hlights								
					2								

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.

Export 5g log Import PCAP or 5	log Leg list Ca	all list Call f	flow Info							
	=2526087	38_8 52115K @								
🖉 🔀 List of all 1- or 2-leg calls								Call list 🖁	ፇ ᠿ ♡	/ 🗖 🖾
01 👿 C Rows: 1										
01										
D1 First packet Call Capture time, GMT leg		DST address leg2	SRC number	DST number	Click for Call flow	No of legs	Packets Leg 1	Packets Leg 2	Call dur leg1	Call dur P leg2 le
2015-12-16 19:11:28.750380 2526		iegz	View in C	all flow	Completed		2	Leg 2 200 INVITE, 100, 183, 20	_	
01			Add to file	er						
01			🛛 🏹 Clear filte	r						
01			View all le	gs						
01			Export to	Excel						
01			Select ce	ll contents						
01			Select co	contents						
01			👷 Remove a	all highlights						

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) Selected legs All legs Call flow - +	
	115-02-25 20:38:30.834953 === 0.081564 === Leg 2 === SRC->DST === 10.10.10.10 ==> 11.11.11.11	-
	VITE sip:151515151515@11.11.11.11;user=phone SIP/2.0 a: SIP/2.0/UDP 10.10.10.10.5060;rport;branch=z9hG4bK-427ad348bd2e11e4a641001b216c3d18;siq=fdf1f8b6	
	a: SIP/2.0/UDP 10.10.10.10.10.5060;rport;branch=z9hG4bK-427ad546bd2e11e4a641001b216c3d18;sig=c6b52f8 a: SIP/2.0/UDP 10.10.10.11:5060;rport;branch=z9hG4bK-427acd62bd2e11e4a641001b216c3d18;sig=c6b52f8	l
	a: SIP/2.0/UDP 10.10.10.11:5063;rport=5063;branch=z9hG4bK-427acd62bd2e11e4a641001b216c3d18;sig=c6b5216 a: SIP/2.0/UDP 10.10.10.11:5063;rport=5063;branch=z9hG4bK-427ab4f8bd2e11e4a641001b216c3d18	l
	om: <sip:17171717171717170200;port=0000;sirain0=2510401427a041052201144044001221005000< td=""><td>l</td></sip:17171717171717170200;port=0000;sirain0=2510401427a041052201144044001221005000<>	l
): <sip:151515151515150;0:1.11.11.11:user=phone></sip:151515151515150;0:1.11.11.11:user=phone>	l
	all-ID: 427a80fabd2e11e4a641001b216c3d18@10.10.10.11	l
	Seq: 1 INVITE	l
	ontact: <sip:17171717171717@10.10.10.11:5063;user=phone></sip:17171717171717@10.10.10.11:5063;user=phone>	l
	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.
	ontent-Length: 322	ľ
	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
	IN IP4 10.10.10	l
	00	l
	audio 31448 RTP/AVP 18 4 0 8 101	l
	rtpmap:18 G729/8000	l
	fmtp:18 annexb=no	l
	rtpmap: <mark>4 G723/8000</mark> :fmtp:4 annexa=ves	
	imp.4 annexa=yes intpmap: <mark>0 PCMU/8000</mark>	l
	rtpmap:8 PCMA/8000	

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	s SRC signaling address / net	DST signaling address / net	SRC number pattern	DST number pattern			Capture each of next X calls	Comment
4		addrooornot	durocornic	987654321	123456789	10	60	Next 5 calls	
3		3.3.3.3	4.4.4.4			10	60	Next 20 calls	
2			2.2.2.2			5	30	Random mode	
1		1.1.1.1		123456789		10	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.

	Call ID	SRC signaling address	DST signaling	SRC	DST number		Codecs				Early media	Connect		Audio	Audio
.429017	402878847 8		address 88.198.190.30	number 77751895708 12	25#998932	_	8: G.711a	83	packets 0	duration 2.5	duration 2.5		detected	play	get file
	402878909_1		88,198,190,30				8: G.711a	2663	2	32.1	32.1			play/pause, ctrl-click to jum	-
	402878988_8		88.198.190.30		25#998905 25#998905		18: G.729	4109	2	41.1	41.1			play/pause, ctrl-click to jum	
	402879048 1		88.198.190.30				8: G.711a	1215	0	14.6	14.6			play/pause, ctrl-click to jum	
	402879106 1		88.198.190.30	View in Media	alogs		8: G.711a	434	0	5.3	5.3				aet fil
	402879122_6		88,198,190,30	View in Signa	lina loas i		18: G.729	3382	0	33.8	33.8			play/pause, ctrl-click to jum	-
	402879135 1		88,198,190,30	View in Call f	0.11	7044	18: G.729	5926	2	59.3	59.3			play/pause, ctrl-click to jum	-
.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
.823112	402882584_3	81.2.128.196	88.198.190.30	V Clear filter		7959	18: G.729	3299	1	33.0	33.0				get fil
.301528	402882643_1	81.2.128.196	88.198.190.30	Export to Exce	el	2347	8: G.711a	1448	0	43.4	43.4			play/pause, ctrl-click to jum	get fil
6.687776	402882746_1	81.2.128.196	88.198.190.30	Select cell co		2347	8: G.711a	1329	0	39.8	39.8			play/pause, ctrl-click to jum	get fil
0.071047	402882782_7	81.2.128.196	88.198.190.30			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 cor	ntents	0071	8: G.711a	1054	1	31.6	31.6			• • • • • • • •	get fil
.577698	402883013_1	81.2.128.196	88.198.190.30	💥 Remove all hi	ighlights	7975	18: G.729	5914	4	59.2	15.8	yes			get fil
.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
.728602	402883117_4	81.2.128.196	88.198.190.30		@5	87918	: G.711a, 18:	1907	0	21.1	11.8	yes		play/pause, ctrl-click to jum	get fil
1.686772	402883200_8	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 file

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.

Traffic collector	m 10m 1h 4h 12h 24h 1d-2d	2d-3d GO R	ows: 300 / get 1-300	DR Signaling logs	Media calls		more g Ø	• ∞
Capture time, J GMT	Call ID	SRC address	DST address	SSRC	Seq	RTP timestamp	Codec	Packet size
2015-12-16 19:51:00.010443	ACCESSION, DOWNERS, D.	64,104,106,20	84.01 XXX XX4	24775b55	54595	420148416	8: G.711a	214
2015-12-16 19:51:00.018209	ACCESSION, TOPOTAL SQUARE.	64.2 KBB 864	66,706,700,00	10084	25447	1481362244	18: G.729	74
2015-12-16 19:51:00.026447	ACCESSION, NUMBER OF A	66.106.100.00	64.01.038.03H	24775b55	54596	420148576	8: G.711a	214
2015-12-16 19:51:00.037790	ACCESSION, DESCRIPTION (C	64.2 K/8 FM	61,701,703,20	10084	25448	1481362404	18: G.729	74
2015-12-16 19:51:00.051266	ACCESSION, DOTOR ADDRESS.	66, 106, 106, 20	81.0 XXX XX4	24775b55	54597	420148736	8: G.711a	214
2015-12-16 19:51:00.057409	ACCESSION, TOPOTRATION, C.	64.2 K/8 FM	64,704,704,20	10084	25449	1481362564	18: G.729	74
2015-12-16 19:51:00.067224	ADDRESS, DODRESS, D.	66, 106, 106, 20	81.2 XXX XX4	24775b55	54598	420148896	8: G.711a	214
2015-12-16 19:51:00.077640	ACCESSION, TOYOTHE SQUALS.	84.2 K/8 864	61,701,701,00	10084	25450	1481362724	18: G.729	74
2015-12-16 19:51:00.090891	ADDRESS, DEDRESS, D.	66,106,106,20	44.01X38.004	24775b55	54599	420149056	8: G.711a	214
2015-12-16 19:51:00.097277	ACCESSION, TOPOTHERDON, D.	64.2 CB 864	66,106,106,00	10084	25451	1481362884	18: G.729	74
2015-12-16 19:51:00.107201	ACCESSION, DOTATING STREET, D	65,106,106,20	64.01.038.004	24775b55	54600	420149216	8: G.711a	214
2015-12-16 19:51:00.118067	ACCESSION, TOPOTHERDON, C.	64.2 CB 864	68,708,709,00	10084	25452	1481363044	18: G.729	74
2015-12-16 19:51:00.131620	ADDRESS, DESCRIPTION C.	66,106,106,20	64.01X38.004	24775b55	54601	420149376	8: G.711a	214
2015-12-16 19:51:00.138556	ACCESSION, TOPOTHERDON, D.	64.2 CB 864	66,709,709,00	10084	25453	1481363204	18: G.729	74
2015-12-16 19:51:00.147775	ADDRESS, DESCRIPTION, D	66,106,106,20	64.01.038.004	24775b55	54602	420149536	8: G.711a	214
2015-12-16 19:51:00.159022	ACCESSION, TOYOTHE SQUALE.	84.2 K/8 864	61,701,701,00	10084	25454	1481363364	18: G.729	74
2015-12-16 19:51:00.171559	ADDRESS, DODRESS, D	66, 106, 106, 20	61.0 XXX XX4	24775b55	54603	420149696	8: G.711a	214
2015-12-16 19:51:00.178396	ACCESSION, TOYOTHE SQUALE.	64.2 K/8 FM	66,706,700,00	10084	25455	1481363524	18: G.729	74
2015-12-16 19:51:00.187592	ADDRESS, DODRESS, D	66,106,106,20	81.2 XXX XX4	24775b55	54604	420149856	8: G.711a	214
2015-12-16 19:51:00.198783	ACCESSION, TOYOTHE SQUALS.	84.2 K/8 864	61,701,701,20	10084	25456	1481363684	18: G.729	74
2015-12-16 19:51:00.211579	ACCESSION, DOTOR ADDRESS.	66, 106, 106, 20	61.0 XXX XX4	24775b55	54605	420150016	8: G.711a	214
2015-12-16 19:51:00.219453	ACCESSION, TOPOTHERDON, D.	64.2 K/m #84	66,709,709,00	10084	25457	1481363844	18: G.729	74
2015-12-16 19:51:00.227876	ADDRESS, DEDRESS, D	66,106,106,20	81.2 XXX XX4	24775b55	54606	420150176	8: G.711a	214
2015-12-16 19:51:00.240305	ACCEPTED TO STREET, STREET, ST	H 2 CB Phi	61,101,101,00	10084	25458	1481364004	18: G.729	74

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.

	1	1		1	1	() () () () () () () () () ()	
IP collected from traffic packets	Port	Dir SRC/DST	Leg and direction	ID/not match 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	
121212	5060	0: SRC	Leg 1, Customer SRC	A REAL PROPERTY.	Training Internet	607	
17.85.10	5060	0: SRC	Leg 1, Customer SRC	0.0001.00	084	510	
1 C 2 C 1 C 2 C 2 C 2 C 2 C 2 C 2 C 2 C	5060	0: SRC	Leg 1, Customer SRC	11,101,08,105	87%	3362	
10 CO 10 CO	5060	0: SRC	Leg 1, Customer SRC	11,101,08,100	87%	31	
200.20071	5060	0: SRC	Leg 1, Customer SRC	12.40(040(71)	Internal	38	
2-040.00	5060	0: SRC	Leg 1, Customer SRC	11,1040,10	TRACEORD - Agric	9	
2-048.88	5060	0: SRC	Leg 1, Customer SRC	12.10405.54	TRACEORD - Agric	8	
B-171-142.20	5060	0: SRC	Leg 1, Customer SRC	54.7073.7043.005	PROPERTY Interpretation	109276	
C - 10 - 10 - 10 - 10 - 10 - 10 - 10 - 1	5060	0: SRC	Leg 1, Customer SRC	64.76488.804	Level 3	290	
C - H ACA H D	5060	0: SRC	Leg 1, Customer SRC	54.76/100/146	Level 3	26	
10 TO 1 1 TO 1 1	5060	0: SRC	Leg 1, Customer SRC	54.00 THE THE	or	26	
B-C-ND-B/C-B	5060	0: SRC	Leg 1, Customer SRC	56.009.009.000	Interdition Telephone	7454	
8.208-64.240-	5060	0: SRC	Leg 1, Customer SRC	56.009.009.000	Interdition Telephone	8495	
400.40 400.8	5060	0: SRC	Leg 1, Customer SRC	54.009.009.009	Interdisting Telephone	8096	
8-02-02-0	5060	0: SRC	Leg 1, Customer SRC	64,783,784,784	Ove	522	
8-98-0752-8	5060	0: SRC	Leg 1, Customer SRC	56,756,785,854	Televali .	47	
8,200 148,400	5060	0: SRC	Leg 1, Customer SRC	50.000 (Web.99)	Perigen Desire as	18	
8,200 148 100	5060	0: SRC	Leg 1, Customer SRC	55 (196 (196 (196))	Parigan Desirana	12	
8.04.02.08	5060	0: SRC	Leg 1, Customer SRC	00,100,104,109	TRACE SHIE - Design East- Name 2	52108	
8,06,03,07	5060	0: SRC	Leg 1, Customer SRC	50,100,104,107	TRACTOR - Design Date: Name 1	52406	
8.3H8.300-H8	5060	0: SRC	Leg 1, Customer SRC	94,075,000,794	Level 3	1485	
100.6.00	5060	0: SRC	Leg 1, Customer SRC	4004.007	Phaneline	184	
3649066 AUX	5060	0: SRC	Leg 1, Customer SRC	08.08004.007	(ED)	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		IPs WL customers WL vendors WL own switch
30d 60d G(C Rows: 244	
and direction	IP/net mate from the Whit	
mer SRC	Customer IP NOT FOUN	View in CDRs
mer SRC	64/2010-0110-	View in Traffic logs
mer SRC	0.0000	
mer SRC	75 175 (St. 56)	Add selected to White List
mer SRC	79 175 20 101	Add all customers to White List
mer SRC	7040340171	Add all vendors to White List
mer SRC	70,000,00	Add to filter
mer SRC	72,2342,34	Clear filter
mer SRC	10.111.141.00	Export to Excel
mer SRC	ST 10 88 714	
mer SRC	57 YE NOT 140	Select cell contents
mer SRC	55 (E 547 548	Select col contents
mer SRC	10.000 00.046	💥 Remove all highlights
mer SRC	10.010104.040	
mer SRC	N-018-104.009	
mer SRC	56 TO: 100 TO	

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.

		Click						
Row	Status	Whitelist Customer IP/net	Whitelist Customer port range	Customer name	Last change, GMT	Change mode	Last editing user	Comment
	\checkmark							
135	1	200.00 W1227	8667	Case Network	2015-05-04 16:16:47	Edited manualy	9	
134	1	51.76-80.044	890	13	2015-04-28 16:53:34	Edited manualy	9	
133	1	0100120	890	CHP	2015-04-28 16:52:03	Edited manualy	9	
132	1	810.710104	890	One Brance	2015-04-28 16:52:28	Edited manualy	9	
131	V	100.00.000	890	Teather Party	2015-04-28 16:46:22	Added manualy	9	
130	1	100.100.00100	890	Testing Party	2015-04-28 16:46:02	Edited manualy	9	
129	1	10034030030	880	Teamor Dolonicol	2015-04-28 16:45:14	Edited manualy	9	
128	\checkmark	200 AU 200 100	4004-00767	Teams (254 (2000)	2015-04-28 16:18:52	Added manualy	9	
127	\checkmark	N. 101 104 10		Cores	2015-03-12 13:28:17	Added manualy	9	
126		5 100 100 10		Toherry	2015-03-12 13:27:58	Added manualy	9	
125		00,700,700,004		Tempose	2015-03-12 13:27:28	Added manualy	9	
124	1	PA 2018 TO 1 (199		Harmond Pandomy	2015-03-12 13:26:56	Added manualy	9	
123	1	1991 S (200) FB		Charte Statistics and	2015-03-12 13:25:57	Added manualy	9	
122	1	100 PC (127 PC		Phonetone	2015-03-12 13:22:24	Added manualy	9	
121	1	A1004 (117		PhoneBille	2015-03-12 13:22:24	Edited manualy	9	
120		100.00.00.000		Traffic Contempore Callored	2015-03-12 13:13:15	Added manualy	9	
119	1	101.007.000.0		Telecon Standor CTE	2015-03-12 13:11:16	Added manualy	9	
118	1	12,1040,10		TRACTORE-Auto	2015-03-11 21:42:45	Added manualy	9	
117	1	12,1040,10		TRACTORE-Auto	2015-03-11 21:42:31	Added manualy	9	
116	1	12.49.040.01		Tempolar	2015-03-11 21:42:07	Added manualy	9	
115		200.00.000.000	8990	Teams (254 (2008))	2015-03-11 21:13:55	Added manualy	9	
114	1	200.40.200.00	10084-00767	Testing State (PRPS)	2015-03-11 21:12:33	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.