Q1

The users could be seen registered after the configurations were in place and Jitsi was used to login. Configuring was troublesome and the fault in previous unsuccessful configurations was not pinpointed. A successful call was made from 9998 to 9999 while packets were captured from the server's interface towards 9998.

Q2

There are some ARP messages in the start to determine who has which address. The call session is first set up with SIP and SDP protocols after which the call itself consists of a large number of RTP packets. The IP addresses and used ports (port 5060) of the origin and destination can be seen in the capture communicating with the VoIP server. Even the usernames are visible in the SIP messages together with the addresses, in the form of *"9998@10.38.0.102"* and *"9999@10.38.0.103"*.

The RTP packets include two codecs, H264 and OPUS. The capture contains nine (9) SIP flows according to the Wireshark tools.

Q3

The registration was successful after moving user 9999 to the 10.38.10.0 network and to the second VoIP server but the call was **not**. It is because the first server does not know where to reach user 9999.

Q4

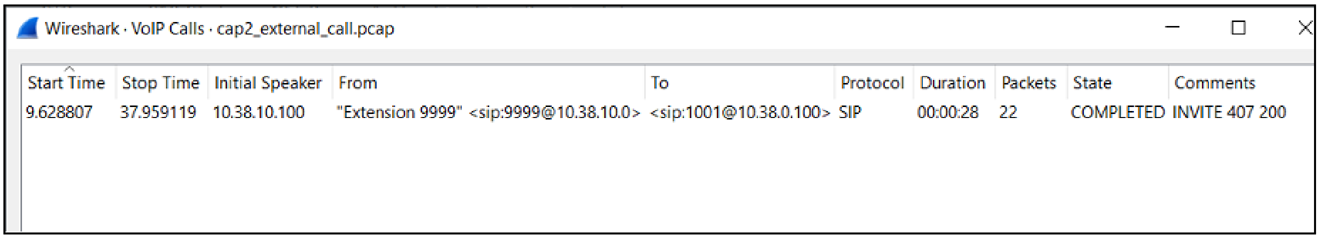
After configuring external calls successful calls were made between domains with the VoIP phone user 1019 and user 9998.

Q5

A SIP invitation is made between the servers. Different statuses are reported while the session is being set up.

- Status: 407 Proxy Authentication Required
- Status: 100 Trying
- Status: 183 Session Progress

You can see protocols SIP, SDP and RTP. This time the origin and destination **cannot** be seen, only the IP addresses of the two servers. The username of the other user is however visible in the SIP messages. The only codec used seems to be G.722. This could be because of a setting in the configuration files.



Wireshark · VoIP Calls · cap2_external_call.pcap

Start Time	Stop Time	Initial Speaker	From	To	Protocol	Duration	Packets	State	Comments
9.628807	37.959119	10.38.10.100	"Extension 9999" <sip:9999@10.38.10.0>	<sip:1001@10.38.0.100>	SIP	00:00:28	22	COMPLETED	INVITE 407 200

Image 1: Wireshark VoIP Calls feature

Q6

Both calls were made in the lab due to troubles with the configurations before the lab appointment. The captures were similar.

Q7

G.722 can be a good option when you have a lot of bandwidth as it delivers high quality audio but needs a wide bandwidth. In low bandwidth conditions you may consider *G.729* which uses higher compression. This lowers audio quality and sounds other than speech may sound especially poor.[1]

Q8

The codec setting was probably already enabled, as implied in Question 5, when every possible configuration was tried while attempting to get FreeSWITCH working. The value was set to "*G722*". Delay values of 0, 500 and 1000 ms were introduced. It is difficult to say when the calls became inaudible as no audio could be heard in any case due to other technical difficulties.

Q9

Yes, you can tap into the traffic. Wireshark seems to include a feature that even lets you play the audio transported by the RTP traffic.

Q10

TLS encryption was set up on both servers. It was implemented in *vars.xml* and the dialplan. An encryption key appeared in the */etc/freeswitch/tls* folder. However, calls did not work after these alterations despite several attempts. Packet capture showed no traffic between the servers and the cause of the problem was not discovered.

FQ1

A VoIP codec often determines voice signal quality, network compression, and encoding and decoding. There are various codecs, and each type is associated with a distinctive property. Typically, these characteristics are sampling rate, bit rate, and frame size, which ultimately impact the network's efficiency and voice quality. A few codecs and their properties are described below [2]:

G.711: The International Telecommunication Union has standardized this codec, which is known as a pulse code modulation audio codec. This codec is widely implemented in VoIP systems. The sampling rate of the G.711 codec is 8 kHz, and the bit rate is 64 kbps.

G.722: This codec is extensively used for high-quality voice and audio transmission, along with higher voice quality compared to the G.711 codec. The International Telecommunication Union has classified this codec as a standardized audio codec. This utilizes a sample rate of 16kHz - 24kHz and a Bit rate of 48 kbps - 64 kbps

G.729: This codec utilizes less bandwidth and produces high-quality audio. This is a low-bitrate codec; therefore, it is frequently used in VoIP applications for consumers and businesses. This is a frame-based code. Hence the frame size is 20 milliseconds, while the Sampling rate is 8kHz and a Bit rate of 8 kbps.

G.726: This is yet another low-bitrate codec that allows efficient and reliable voice transmission over the internet. This codec is also commonly used for real-time speech transmission, as its low latency makes it suitable for the function. It has a sampling rate of 8kHz and various bit rates - 6 kbps, 24 kbps, 32 kbps, and 40 kbps.

FQ2

No matter how safe a VoIP network is, it will always be open to security threats and loopholes. Some of the security risks in the VoIP network are listed below [3]:

DDoS (Denial of Service Attacks) - The main goal of DDoS attacks is to stop VoIP communications and networks from working. DDoS attacks cause VoIP servers to be overloaded, create massive amounts of disruption, increase latency and lower the call quality.

Virus and Malware - These are the most significant threats that can happen to a network over the internet, and VoIP can be infected with malware and end up letting sensitive information get out. Malware and viruses can be found on the internet and spread within an internal network, giving attackers access to the whole VoIP network. This also makes information about customers and businesses very vulnerable.

Packet Sniffing or Man-in-the-Middle attacks - Packet sniffing works in such a way that the attackers tend to intrude on the ongoing packets and stop the network packets from reaching the destination. As a result, attackers have the ability to get control over the entire network along with the physical networking devices over packet sniffing.

Vishing - Voice phishing, or vishing, is the same as phishing. It is the most common way to get information out of people. This is the most widely used method in VoIP. Attackers attempt to appear like legitimate services and usually ask for personal information like account information and other sensitive information over the phone.

FQ3

Like other IT systems, VoIP can be exploited, has vulnerabilities, and can be attacked. But VoIP is a good choice for most businesses because it has many benefits. VoIP, for example, reduces operational costs, improves scalability and accessibility, and provides great convenience. Therefore To keep VoIP secure, it must be protected from cyberattacks and hackers. [4]

By patching the system with security and vulnerable patches - Most loopholes are fixed by regularly patching the VoIP software and the associated operating system, lowering the risks of attacks.

Implementing Encryption: Encryption techniques, such as Transport Layer Security (TLS), are an excellent way to safeguard VoIP communications.

Using Firewalls: Firewalls ensure that services are safe from the internet and any potential threats that may be found between the internet and the VoIP network. A Firewall, either locally or in the cloud, can be set up to filter any traffic in real-time.

By using a virtual private work and regularly monitoring the VoIP network - A VPN creates a private, encrypted connection between the VoIP network and the internet, and it also monitors your network in real-time for any suspicious activity. This helps ensure the complete safety of VoIP communications, and so does routinely monitoring the VoIP network and fixing any suspicious vulnerabilities.

References

[1] https://www.nextiva.com/blog/voip-codecs.html Cited 2.2.2023.

[2] https://www.lifewire.com/voip-codecs-3426728 Cited 5.2.2023

[3] https://fitsmallbusiness.com/voip-security-threats/ Cited 5.2.2023.

[4] https://www.nextiva.com/blog/voip-security.html Cited 5.2.2023.