WORKSHOP GARR 2022

NET MAKERS

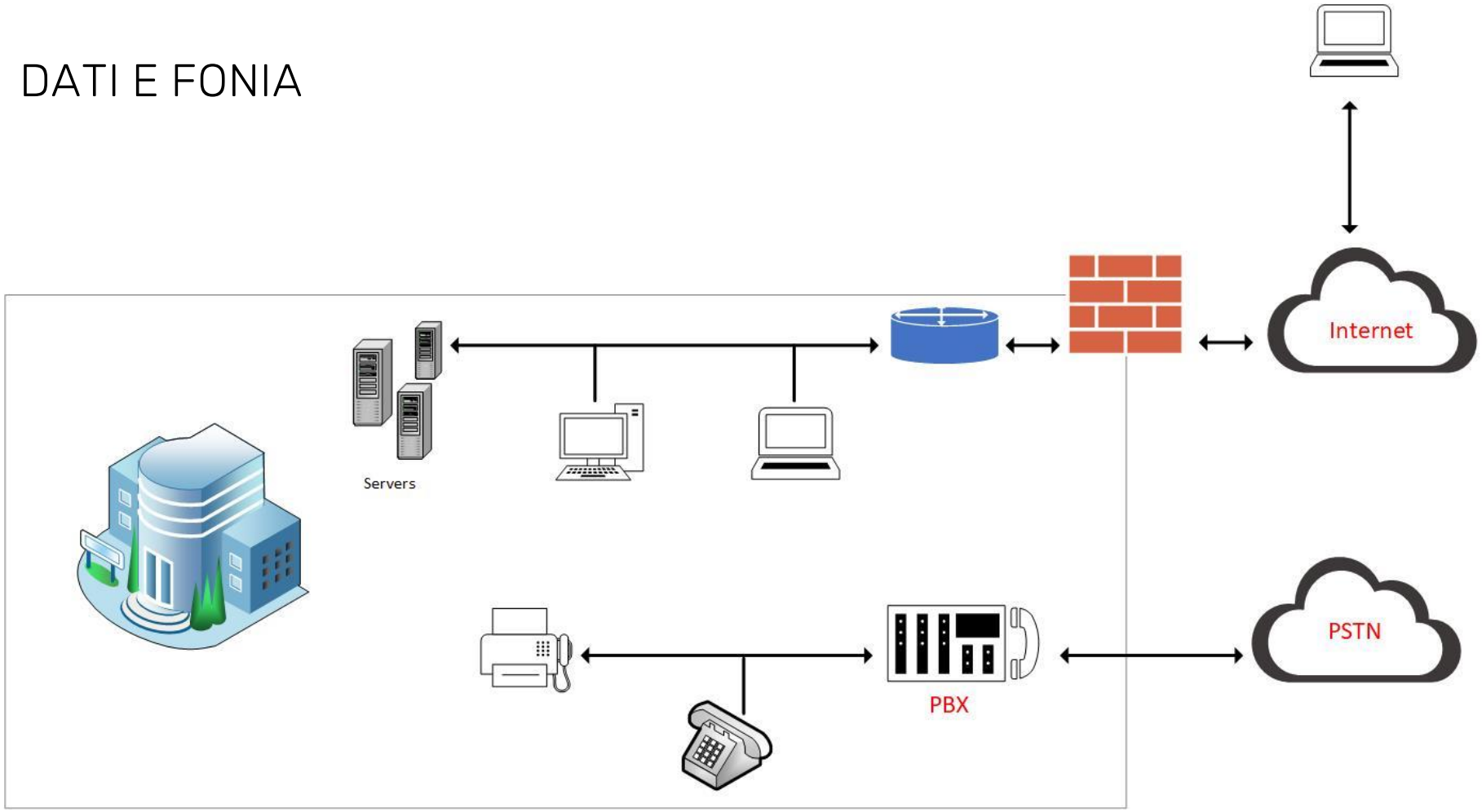
Riflessioni su un attacco alla sicurezza delle reti VoIP

Marco Nicoletti

Proge-Software S.r.l.

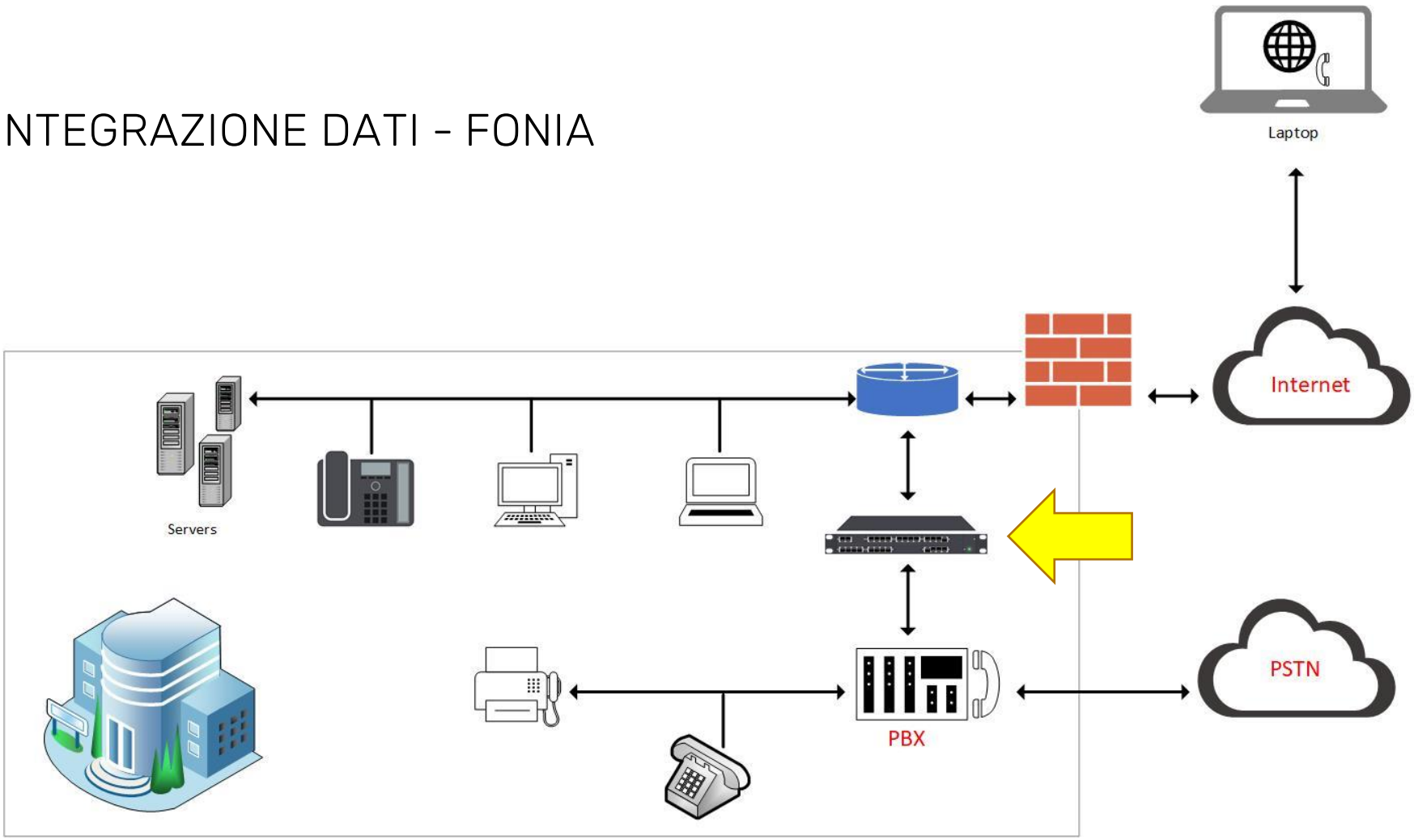
Evoluzione delle reti VoIP

DATI E FONIA



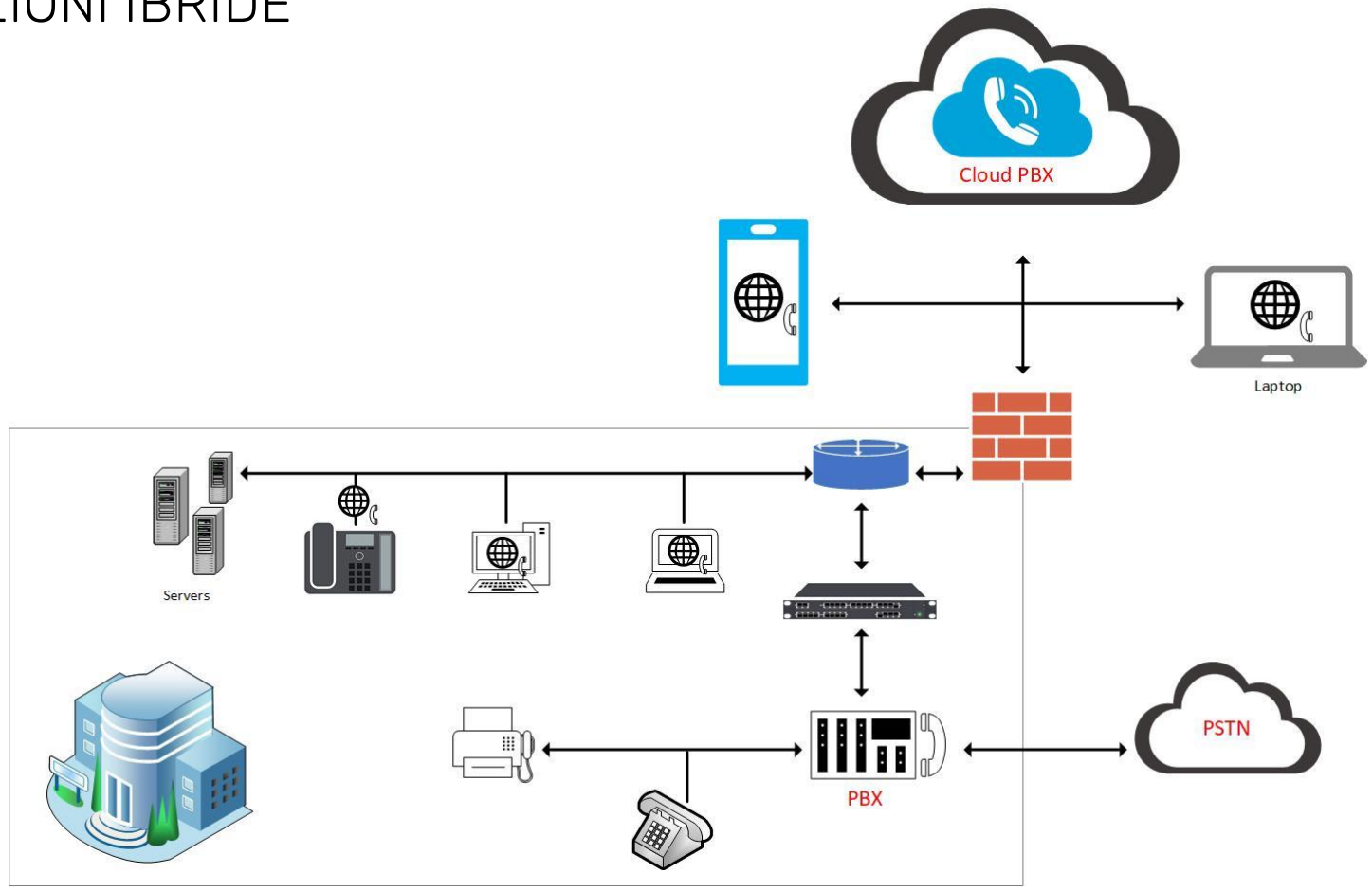
Evoluzione delle reti VoIP

INTEGRAZIONE DATI - FONIA



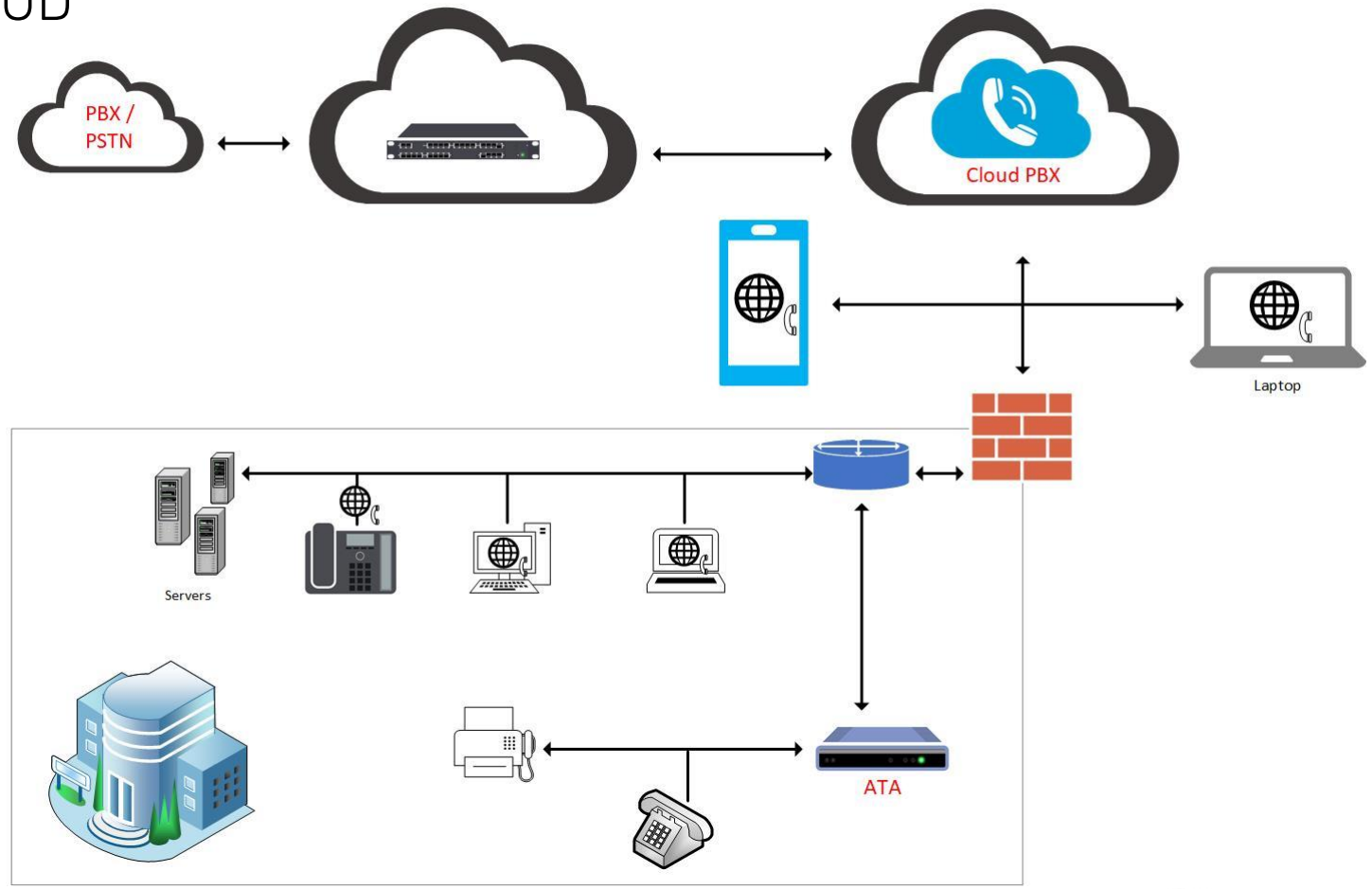
Evoluzione delle reti VoIP

SOLUZIONI IBRIDE

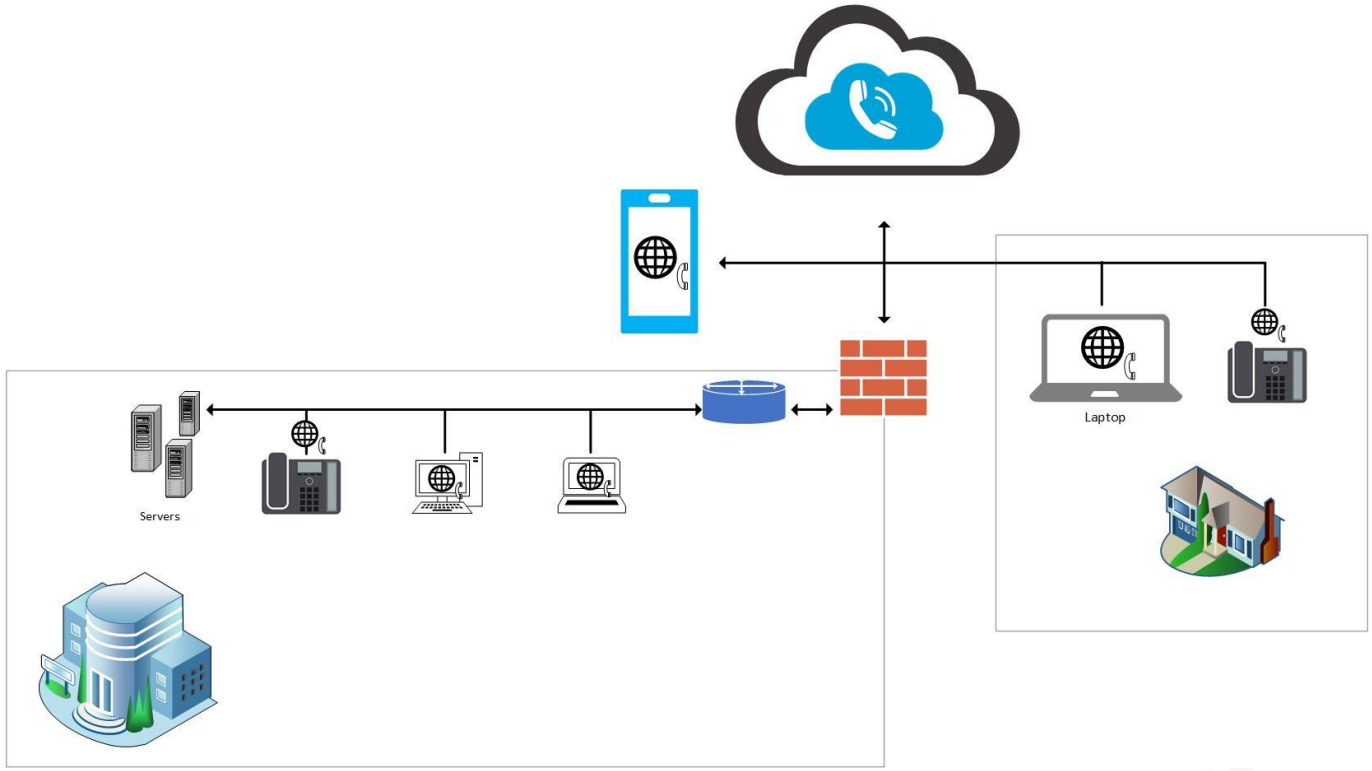


Evoluzione delle reti VoIP

IL CLOUD

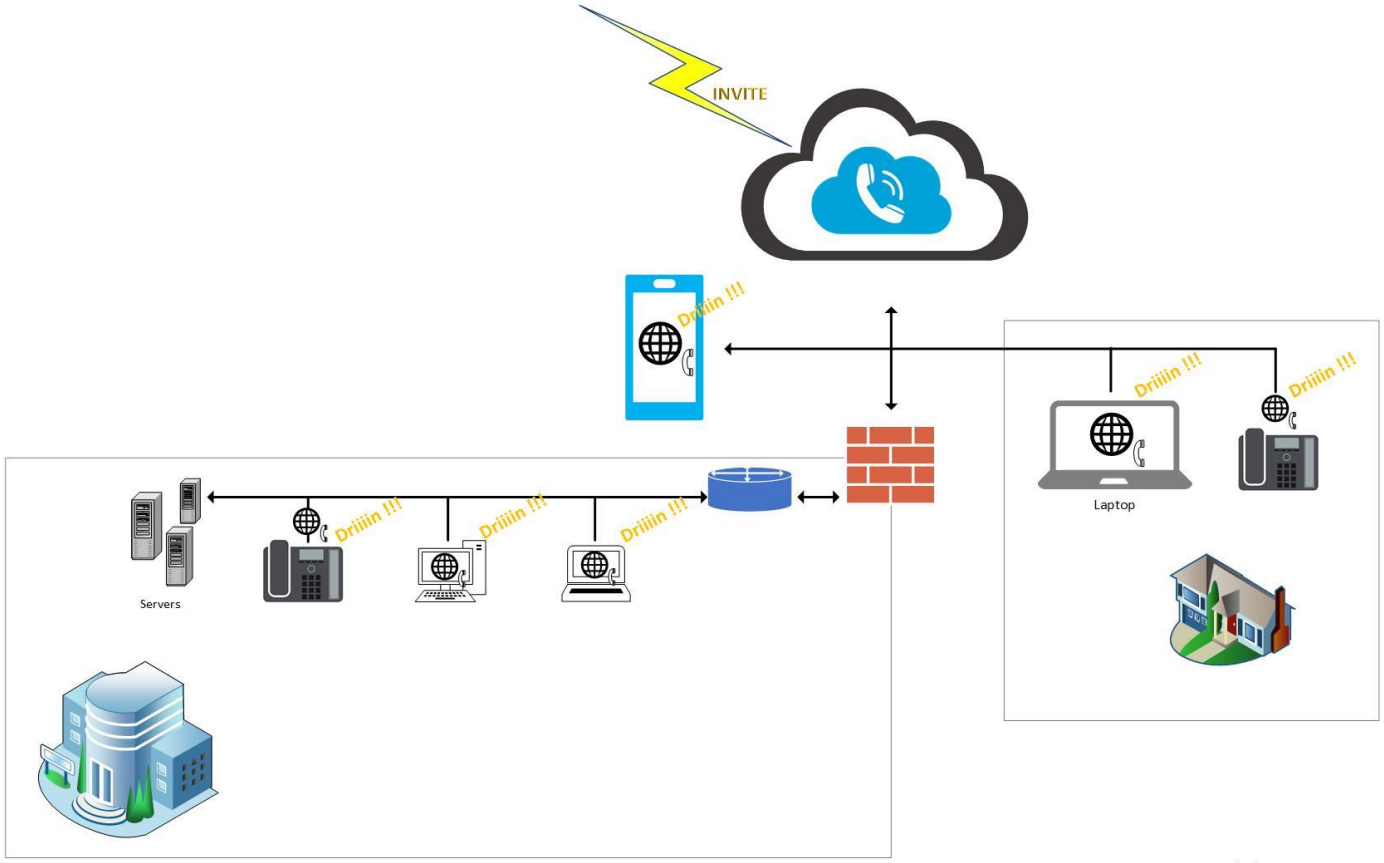


Il funzionamento del VoIP

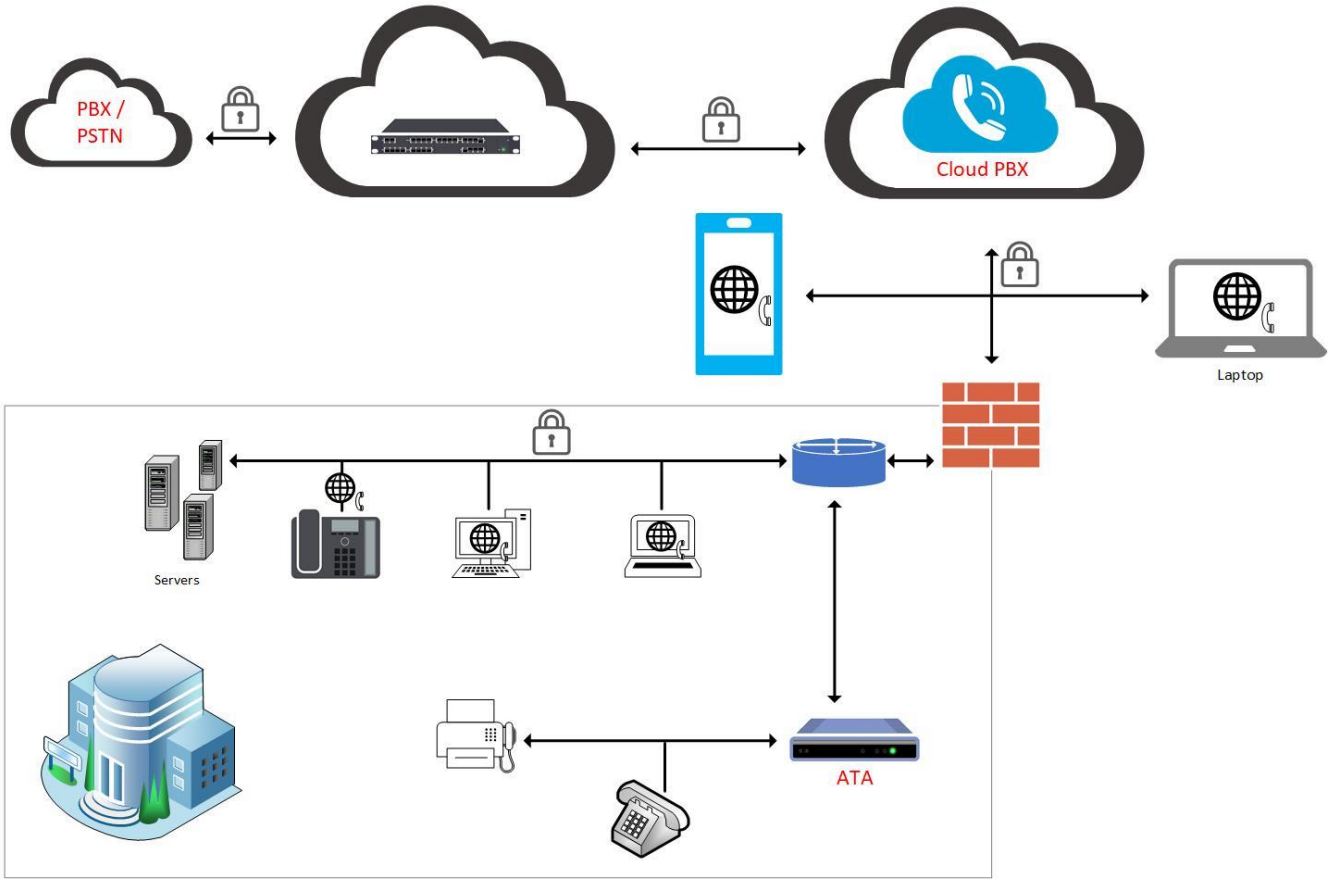


Il funzionamento del VoIP

- Il VoIP connette identità
- Ogni device autenticato invia informazioni su di sé

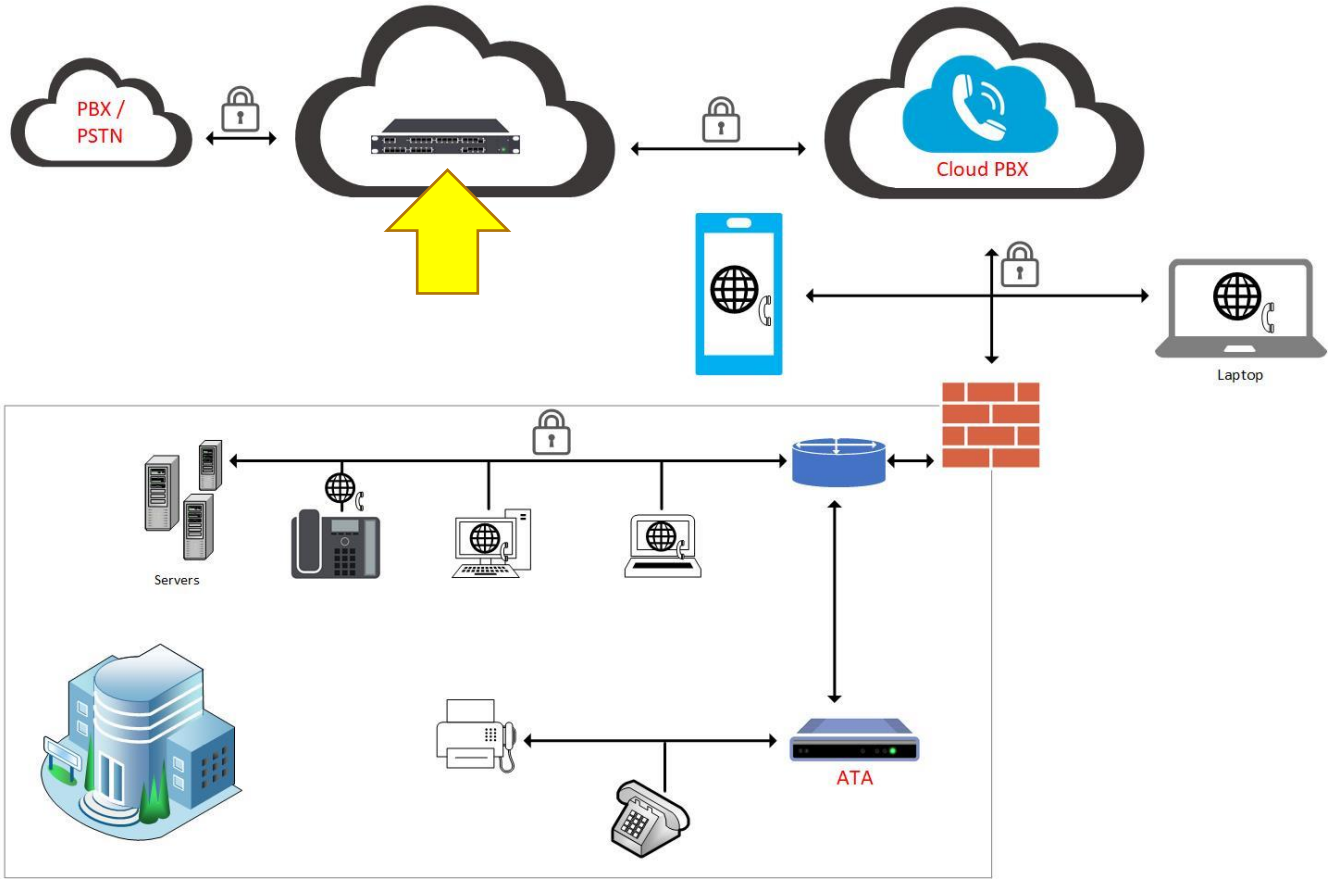


La gestione del VoIP



La gestione del VoIP

- Le responsabilità della gestione del VoIP

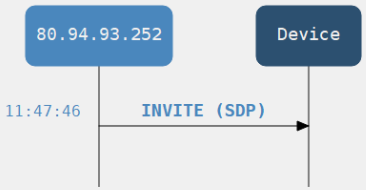


Caso reale

username:password
@
IP pubblico Alice

90017199377208

IP pubblico
Trudy



#	SID	Type	Time	From	To
1	ddb198:10:5252	INVITE	11:47:46	10001:1234@188.15.55.xx	90017199377208@188.15.55.xx

<< | Find | >> | Export | Refresh | Show: All | Calls: 1 Other: 0

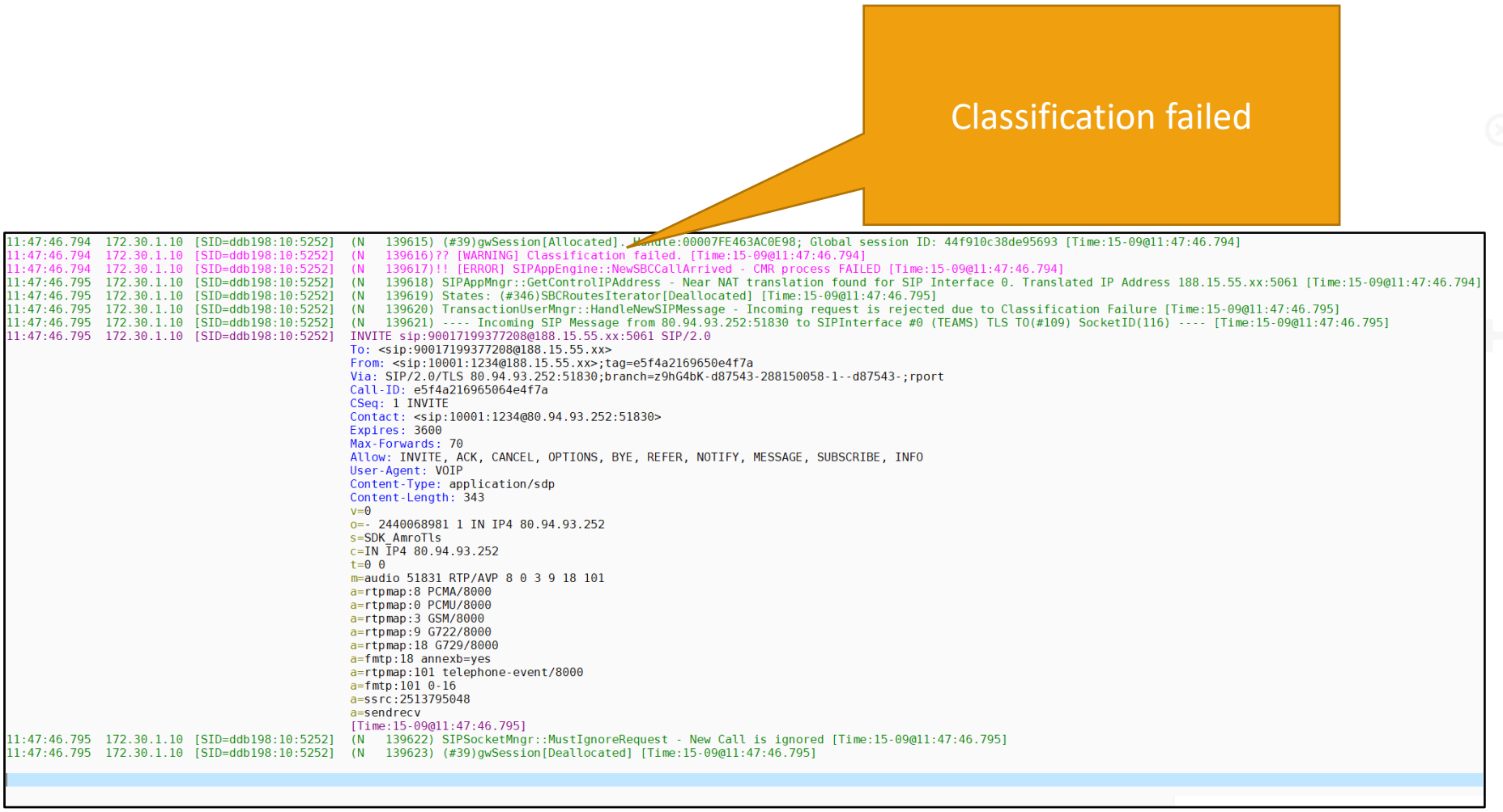
```
11:47:46.795  ---- Incoming SIP Message from 80.94.93.252:51830 to SIPInterface #0 (TEAMS) TLS TO(#109) SocketID(116) ---- [Time:1

INVITE sip:90017199377208@188.15.55.xx:5061 SIP/2.0
To: <sip:90017199377208@188.15.55.xx>
From: <sip:10001:1234@188.15.55.xx>;tag=e5f4a2169650e4f7a
Via: SIP/2.0/TLS 80.94.93.252:51830;branch=z9hG4bK-d87543-288150058-1--d87543-;rport
Call-ID: e5f4a216965064e4f7a
CSeq: 1 INVITE
Contact: <sip:10001:1234@80.94.93.252:51830>
Expires: 3600
Max-Forwards: 70
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
User-Agent: VOIP
Content-Type: application/sdp
Content-Length: 343
v=0
o=- 2440068981 1 IN IP4 80.94.93.252
s=SDK_AmroTls
c=IN IP4 80.94.93.252
t=0 0
m=audio 51831 RTP/AVP 8 0 3 9 18 101
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:3 GSM/8000
a=rtpmap:9 G722/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=yes
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ssrc:2513795048
a=sendrecv
```

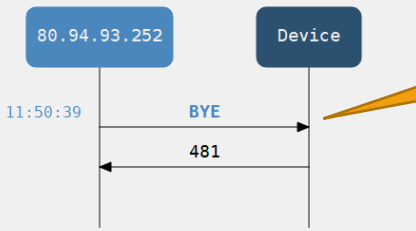
Un solo IP candidate

CODEC di Trudy

Caso reale


Classification failed
11:47:46.794 172.30.1.10 [SID=ddb198:10:5252] (N 139615) (#39)gwSession[Allocated]. Handle:00007FE463AC0E98; Global session ID: 44f910c38de95693 [Time:15-09@11:47:46.794]
11:47:46.794 172.30.1.10 [SID=ddb198:10:5252] (N 139616)?? [WARNING] Classification failed. [Time:15-09@11:47:46.794]
11:47:46.794 172.30.1.10 [SID=ddb198:10:5252] (N 139617)!! [ERROR] SIPAppEngine::NewSBCCallArrived - CMR process FAILED [Time:15-09@11:47:46.794]
11:47:46.795 172.30.1.10 [SID=ddb198:10:5252] (N 139618) SIPAppMngr::GetControlIPAddress - Near NAT translation found for SIP Interface 0. Translated IP Address 188.15.55.xx:5061 [Time:15-09@11:47:46.794]
11:47:46.795 172.30.1.10 [SID=ddb198:10:5252] (N 139619) States: (#346)SBCRoutesIterator[Deallocated] [Time:15-09@11:47:46.795]
11:47:46.795 172.30.1.10 [SID=ddb198:10:5252] (N 139620) TransactionUserMngr::HandleNewSIPMessage - Incoming request is rejected due to Classification Failure [Time:15-09@11:47:46.795]
11:47:46.795 172.30.1.10 [SID=ddb198:10:5252] (N 139621) ---- Incoming SIP Message from 80.94.93.252:51830 to SIPInterface #0 (TEAMS) TLS TO(#109) SocketID(116) ---- [Time:15-09@11:47:46.795]
11:47:46.795 172.30.1.10 [SID=ddb198:10:5252] INVITE sip:90017199377208@188.15.55.xx:5061 SIP/2.0
To: <sip:90017199377208@188.15.55.xx>
From: <sip:10001:1234@188.15.55.xx>;tag=e5f4a2169650e4f7a
Via: SIP/2.0/TLS 80.94.93.252:51830;branch=z9hG4bK-d87543-288150058-1--d87543-;rport
Call-ID: e5f4a216965064e4f7a
CSeq: 1 INVITE
Contact: <sip:10001:1234@80.94.93.252:51830>
Expires: 3600
Max-Forwards: 70
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
User-Agent: VOIP
Content-Type: application/sdp
Content-Length: 343
v=0
o=- 2440068981 1 IN IP4 80.94.93.252
s=SDK_AmroTls
c=IN IP4 80.94.93.252
t=0 0
m=audio 51831 RTP/AVP 8 0 3 9 18 101
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:3 GSM/8000
a=rtpmap:9 G722/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=yes
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ssrc:2513795048
a=sendrecv
[Time:15-09@11:47:46.795]
11:47:46.795 172.30.1.10 [SID=ddb198:10:5252] (N 139622) SIPSocketMngr::MustIgnoreRequest - New Call is ignored [Time:15-09@11:47:46.795]
11:47:46.795 172.30.1.10 [SID=ddb198:10:5252] (N 139623) (#39)gwSession[Deallocated] [Time:15-09@11:47:46.795]

Caso reale



#	SID	Type	Time	From	To
1	ddb198:10:5273	BYE	11:50:39	10001:1234@188.15.55.xx	900017199377208@188.15.55.xx

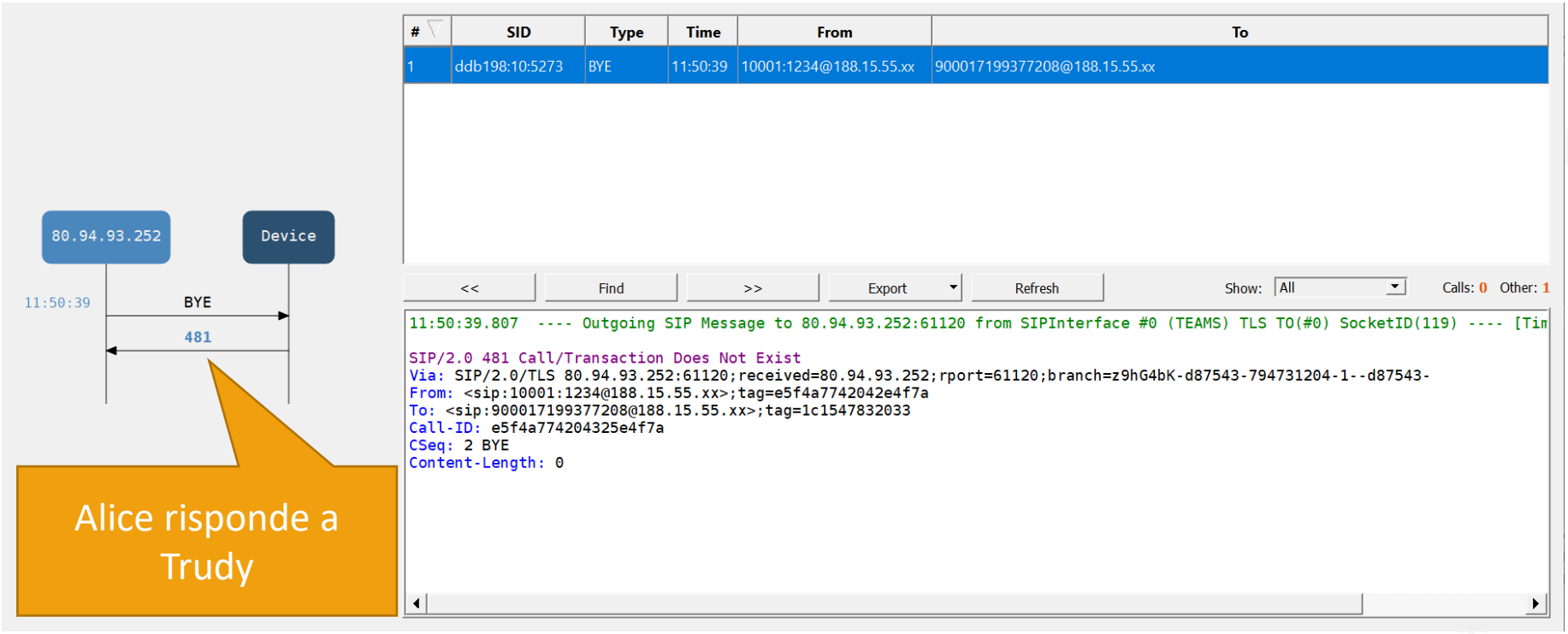
Trudy invia un BYE per una sessione SIP mai iniziata

<< | Find | >> | Export | Refresh | Show: All | Calls: 0 | Other: 1

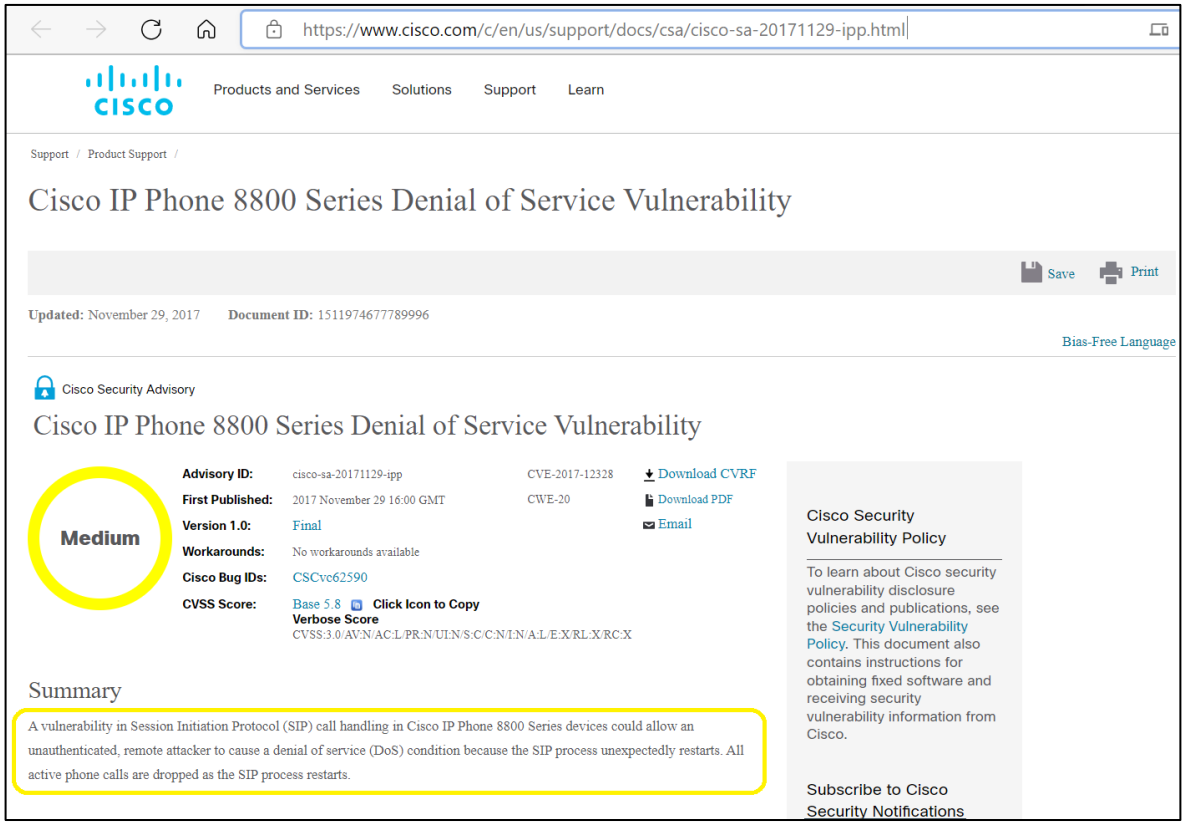
```
11:50:39.806  ---- Incoming SIP Message from 80.94.93.252:61120 to SIPInterface #0 (TEAMS) TLS TO(#106) SocketID(119) ---- [T

BYE sip:900017199377208@188.15.55.xx:5061 SIP/2.0
To: <sip:900017199377208@188.15.55.xx>
From: <sip:10001:1234@188.15.55.xx>;tag=e5f4a7742042e4f7a
Via: SIP/2.0/TLS 80.94.93.252:61120;branch=z9hG4bK-d87543-794731204-1--d87543-;rport
Call-ID: e5f4a774204325e4f7a
CSeq: 2 BYE
Contact: <sip:10001:1234@80.94.93.252:61120>
Expires: 3600
Max-Forwards: 70
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
User-Agent: VOIP
Content-Length: 0
```

Caso reale - BYE

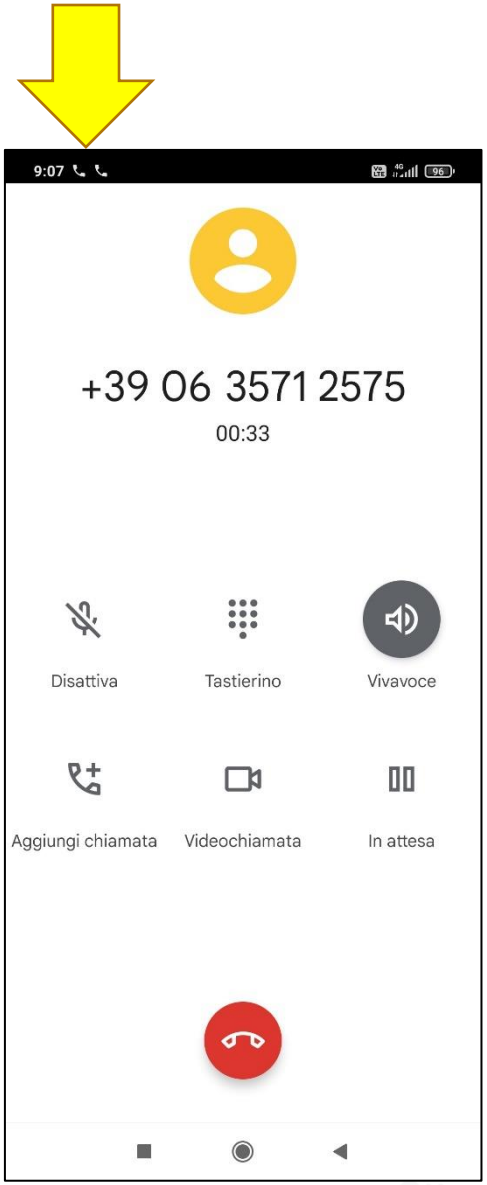


Caso reale - Vulnerabilità SIP di telefoni IP



"A vulnerability in Session Initiation Protocol (SIP) call handling … could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition …. …An attacker could exploit this vulnerability by sending a malformed SIP packet to a targeted phone.
Ref.: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171129-ipp

Una situazione di confine



Conclusioni e proposte

- La possibilità di comunicare a voce è uno dei servizi essenziali nelle emergenze;
- Negli ultimi due anni di pandemia si è registrato un aumento esponenziale nell'utilizzo delle comunicazioni VoIP;
- Le reti VoIP stanno diventando di crescente interesse per chi mira a sferrare attacchi informatici;
- Dobbiamo prepararci a proteggere le comunicazioni voce delle nostre utenze.

PROPOSTA

- Collaborare per configurare un honeypot VoIP che possa servire a documentare le strategie di attacco e fornire linee guida a chi deve applicare le contromisure.

GRAZIE!

Riferimenti

Forensic analysis of Microsoft Skype for Business
Digital Investigation, Volume 29
https://doi.org/10.1016/j.diin.2019.03.012

Forensics for Microsoft Teams
ArXiv, Cornell University
http://arxiv.org/abs/2109.06097