Cloud PBX (Private Branch Exchange) Security: The Future of Enterprise Communication

Siddarth Kaul Research Scholar Bhagwant University Rajasthan India
Dr. Anuj Jain Assistant Professor Bhagwant University Rajasthan India
Dr Rajesh Saini Assistant Professor Govt College Ateli Haryana India

Abstract

The paper proposes to clearly elaborate a solution for the understanding of cloud PBX security the future reality of enterprise communication it seeks to clearly underline the different scenarios of implementation of Communication hosted on the cloud in the different unified Communication environments whether Hybrid or complete cloud deployment it also describes the use of different components involved in the planning of Cloud PBX (Private Branch Exchange) hosted by service provider like the use of Active Directory , Database (SQL) , Internet security and Acceleration , Patch Management and certificate deployments to operate the cloud PBX (Private Branch Exchange). The solution itself involves many flavors like the use of Service Integrator certificate normally deployed on client machine to act as mediator for the services operated on the cloud and for software integration of Clients machine to the Hosted Cloud PBX (Private Branch Exchange) , Communication Services Provider (CSP) normally manages the hardware and software integration on their Private Cloud and a Public cloud so that the Core Business is never in the need of any resources or the resources are never less for any shared risk and responsibilities of minimized downtime. The overall cloud deployment reduces client infrastructure manageability and cost at the lowest level with maximum use of resources such as Calling (Voice & Video), Persistent Chat, call admission Control (CAC), Teleconferencing costs also reduce drastically. The large-scale scalability of the solution is nowadays achieved with use of clustering and virtualization of these servers and other tools in the cloud so the effective service operation is maintained at the highest standards.

Keywords

Cloud Computing, Private Branch Exchange (PBX), Communication Services Provider (CSP), Call admission Control (CAC).

Introduction

Cloud Private Branch Exchange (PBX) security is one of the key parameters of focus within all large and medium size business as Voice or Video Telephony and Teleconferencing fraud at any stage is the near cousin of the data fraud which does not come in attention of the public and rather takes a good amount understanding for the administrator to acknowledge the same it has major and catastrophic devastating effects on the organization and the end users[1] . In the Cloud environment attacks can come anywhere from the internet or attackers normally tend to exploit several vurnabilities. It is thus important to have a secure cloud with minimum risks of vurnabilities, the security of the Cloud Private Branch Exchange (PBX) is specific to the cloud services provider according to the various factors like size, cost and deployment and traffic management architecture [2].

Cloud Security Fraud

The Cloud Security Fraud is primarily focused on the customer resources or equation if a business tries to share some of the resources to its customers sometimes the customers become a threat for the business. Frauds

can take place in several ways like phishing schemes, money transfer scams, identity threats or malware attacks [3].

Examples of Banking Fraud in Cloud

Operation High Roller an international criminal ring targeted many commercial accounts across the European Banks the entire fraud was conducted through remote servers on the cloud the criminals had intimated the knowledge of Banking transaction systems to automate thefts , the fraud started like an email from the banking recipient once clicking the link a malware downloaded and stole all information required for bank transfers it is estimated by Mc Afee that around $ 2.5 Billion was stolen by this scam across European Banks[4].

Securing PBX (Private Branch Exchange) Voice

Eavesdropping in the phone calls normally offer a lucrative target to hackers as that normally compromises everything from the private business to events [5]. Intercepting voice communication in the cloud PBX (Private Branch Exchange) requires accessing the PSTN server nodes with some critical types of crypto encryption decryption algorithms to decrypt and intercept the voice traffic weather voice packets on premise or on cloud is susceptible to the attacks, the use of efficient architecture and better network and security tool manage us to control these attacks [6].

Knowledge gap has become increasingly converged sometime and it is very important that Cloud PBX (Private Branch Exchange) are secured to surrogate the best possible solution to avoid any suspected activity in the enterprise solutions [7].

OTT (Over the Top) Deployments in Cloud PBX (Private Branch Exchange) Voice

The over the Top deployment method is a way in which customer or end user has an access to a given cloud service from a secure Cloud PBX provider , a customer normally will have an access over the broadband services with sufficient control and QOS policy rendered in the best possible way in order the calls with messaging is available with ease from customer premises to the cloud service provider with a synchronous bandwidth of minimum 1 Mbps so that do voice or messaging traffic redundancy is felt [8].

Routers and Switches for Cloud PBX (Private Branch Exchange) need to be configured in a way as the voice, content and Video traffic is prioritized once it lands back to customer premises from Cloud service provider normally QOS (Quality of Service) marking is summarily done and plays an important role to optimize and prioritize the voice, content and Video traffic [9].

The optimization is normally done according to DSCP values as given below

Audio RTP DSCP 46 (EF Class)

UDP ports 1024 to 65355 and 5000 – 5499 range depending on phone type and Models.

Video RTP DSCP 34 (AF41)

UDP ports 1024 to 65355 and 5500 – 6000 range depending on phone type and Models.

SIP DSCP 26 (AF 31)

UDP port 5060, TCP port 5060, TLS and TCP port 5061.

Cloud PBX (Private Branch Exchange) working and Security Consideration

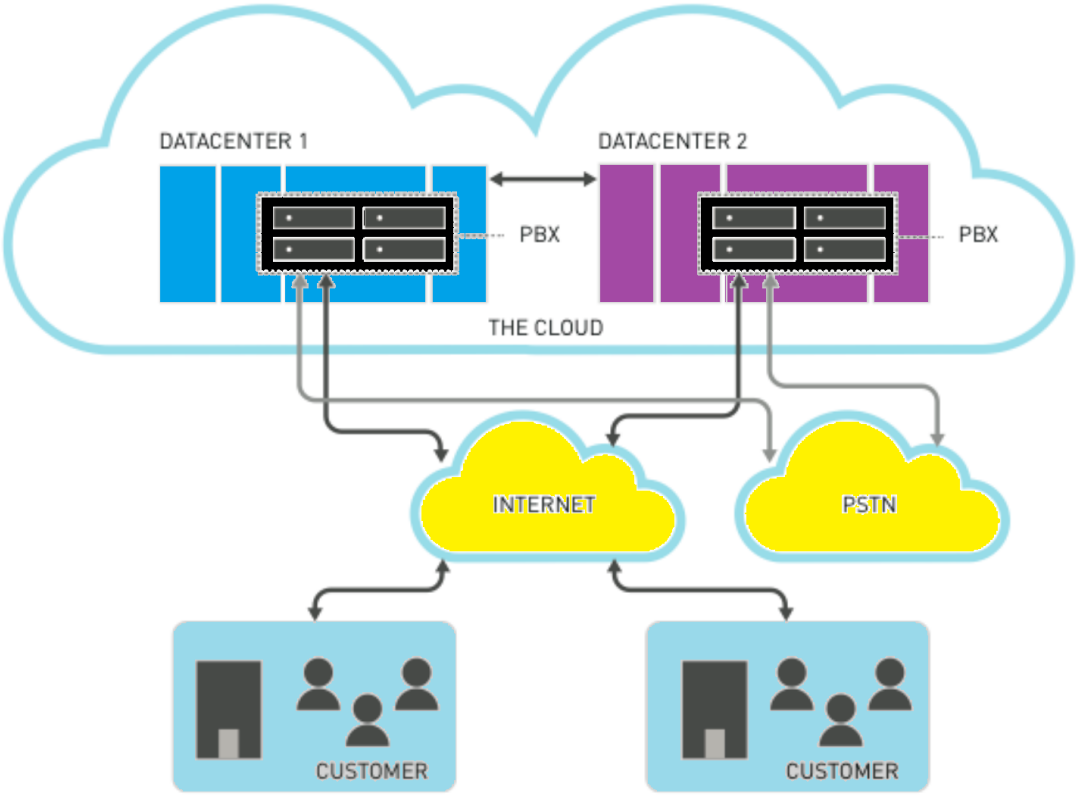

Figure 1. A Cloud PBX (Private Branch Exchange) Enviournment

The above Figure 1 shows a Cloud PBX (Private Branch Exchange) Enviournment in which two separate datacenters host two different Cloud servers depicting an failover enviournment in which if one Datacenter is effected or goes down the Voice , Content and Video traffic is not effected as automatic failover helps the traffic to flow to second datacenter and the Customer/ User is never aware if the failover has occurred if so the End user must allow certain firewall changes to its network in order to allow the Voice , Content and Video Traffic to flow in its network [4].

The optimization of Firewall Traffic is normally done according to DSCP values as given below

HTTP port 80 must be allowed.

Keep live native NAT messages must be allowed.

SIP multiple UDP port connections must be allowed on port 5060 and 5061.

RTP traffic allowance on UDP port 10000 – 65536 for audio and video.

NTP port 143 allowance for firewall configuration.

Environmental Readiness to Cloud PBX (Private Branch Exchange)

A Good Network Backbone Infrastructure is very important for real time voice, video and Content there are two options either an on premises infrastructure or an Cloud PBX infrastructure for a better Cloud PBX

(Private Branch Exchange) infrastructure there are certain enviournment Readiness factors depending on which an organization can be cloud PBX (Private Branch Exchange) ready for communication as under

a. A single installation resource of proper enviournment like racks, Cable space for Cloud PBX (Private Branch Exchange) integration.
b. Category 5 cable marking and end user closet to telco marking.
c. Secure Staging Room for proper environmental conditions to include appropriate levels of temperature, Humidity and Dust.
d. End user training and System Design Specification Conditions as per software supported Enviournment [10].

Functionality Requirements to Cloud PBX (Private Branch Exchange)

The different Functionality Requirements to Cloud PBX (Private Branch Exchange) are dependent on many factors apart from a secure enviournment. The requirements are grouped under various factors

1. Call Redirection
2. Two Factor Authentication (2FA)
3. Encryption and Traffic Protection
4. Free Communication
5. Hide a Phone number
6. Scenario execution
7. Conversation recording and data storage
8. Call Tracking
9. IVR (Interactive Voice Response)
10. Video Call
11. Reminder
12. API and AI (Artificial intelligence) and text Interaction [10]

QOS MARKING TABLE FOR CLOUD PBX (Private Branch Exchange)

Classification and Marking Design
QoS Baseline Marking Recommendations

Application	L3 Classification IPP	PHB	DSCP	L2 CoS
Routing	6	CS6	48	6
Voice	5	EF	46	5
Video Conferencing	4	AF41	34	4
Streaming Video	4	CS4	32	4
Mission-Critical Data	3	AF31*	26	3
Call Signaling	3	CS3*	24	3
Transactional Data	2	AF21	18	2
Network Management	2	CS2	16	2
Bulk Data	1	AF11	10	1
Best Effort	0	0	0	0
Scavenger	1	CS1	8	1

Table 1. QOS MARKING

The QOS marking as shown in Table 1. Depicts the various traffic markings required when the Cloud PBX (Private Branch Exchange) data is classified for marking when coming from Cloud to User or Customer the data packets is itself classified on different application types like routing data, Voice communication data, Call signaling, Video Conferencing data [11].

The QOS marking helps user to choose the adequate bandwidth required for segmentation of the data packets these data packets segmentation helps understand bandwidth in total required for a better cloud PBX setup [12].

The figure 2 above depicts a total bandwidth distribution in a Tunnel distribution method for segmentation of the different Traffic for Voice, Video and other traffic this representation helps us know that voice is always prioritized in Cloud communication followed by Video and other data packets email and File transfer [13].

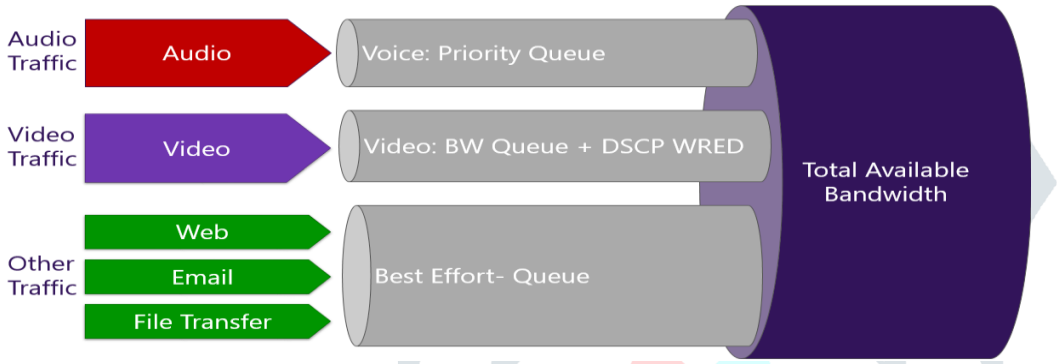

Figure 2. Representation of Bandwidth Distribution in Cloud PBX on User Premises

Conclusion

There are some concerns over the prevalence of cloud-based technologies on security and privacy, in fact in case of Cloud PBX (Private Branch Exchange) means you will have to entrust your service provider for your users or clients mostly the cloud service providers have specific privacy policies set out to govern client resources.

It is also a cloud service providers responsibility to offer good security their reputation is itself dependent on the type of security they offer to their end users.

Cloud PBX (Private Branch Exchange) helps an enterprise to be free from the spending of high value on infrastructure and resources it is through a better option in terms of minimal dependency on the infrastructure in terms of both hardware and software dependency and offers a better cost model to the current challenging business scenarios [14].

References

[1] https://www.microsoft.com/itshowcase/Article/Content/943/How-cloudbased-PBX-and-PSTN-save-Microsoft-more-than-120000-per-day-with-Skype-for-Business.

[2] Executive Considerations – Skype Cloud PBX (002) pdf.

[3]https://www.fonality.com/hubfs/Net_Fortris_May2017/Pdf/cloud_pbx_service_publication_netfortris_010917.pdf

[4] http://tech1p.com/dev/ctr/wp-content/uploads/2013/05/PBX-White-Label-Technical-Whitepaper.pdf (Figure 1).

[5] https://ico.encryptotel.com/assets/pdf/EncryptoTel_WP_v1.pdf

[6] https://www.sangoma.com/wp-content/uploads/2017/04/Disaster-Recovery-Webinar-Questions-English.pdf

[7] https://www.voip-info.org/cloud-pbx/

[8] https://medium.com/365uc/microsoft-teams-direct-routing-with-pure-ip-no-on-prem-infrastructure-7e3c92f8e865

[9] https://wiki.freepbx.org/display/FPG/Using+the+Backup+module

[10] https://arxiv.org/ftp/arxiv/papers/1205/1205.3319.pdf

[11] https://slideplayer.com/slide/6203781/ (Table 1).

[12] https://www.netcraftsmen.com/configuring-qos-on-the-nexus-50002000-part-2/

[13] https://www.nextiva.com/downloads/Cloud-Phone-Systems-eBook.pdf

[14] S. Black, D. Black, M Carlson, E Davies, Z Wang and W. Weiss "Architecture of Differentiated Services ", RFC 2475, December 1998. (Figure 2)