Genesys Engage cloud private edition

Architecture - EAP

Disclaimer

Genesys Engage cloud private edition is being released to pre-approved customers as part of the Early Adopter Program. This means that both the product and the documentation are still under development. As a result, documentation sections might require revision as the product develops. We advise that you use this documentation with care. Before you make changes that could affect the success of your deployment, verify them with your Genesys representatives.

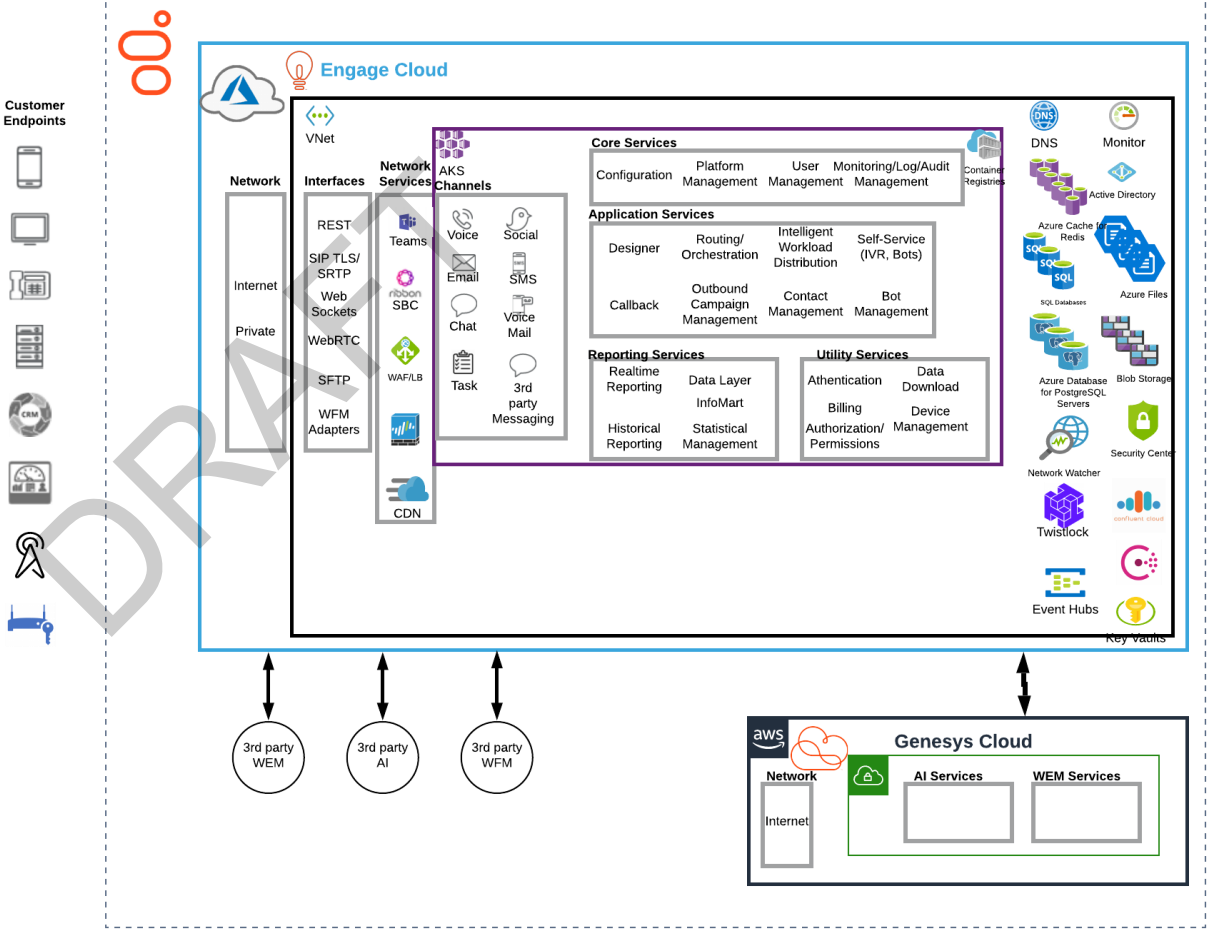
Next Gen Multicloud Platform – What's different

- **Modern Tech Stack** – Containerization and Kubernetes-first approach to abstract the cloud platform
- **Single, Multicloud Code base** – Same architecture and codebase for different arch types and environments

  This is a first in the industry that opens Genesys to a lot more opportunities

- **Network Connectivity Options** – Provides more software-based, open and flexible options (BYOC focus)
- **Automated Deployment Pipeline** – Standardized deployment pipeline enables velocity and consistency
- **Resiliency** – Scalability and observability-driven capacity in the platform and services
- **Security** – Shifting Left with enterprise-grade security via DevSecOps approach
- **Efficiency** – New technologies enable greater efficiency and cloud cost visibility
- **Auto-scaling** – Delivers superior resiliency and efficiency thru orchestration and Infrastructure as Code
- **Immutability** – Greater stability and less complexity
- **All the great features of the Engage Platform** – Build on Global contact center, flexible integration and other features that make Engage the platform of choice for large enterprises.

Functional Architecture



GENESYS

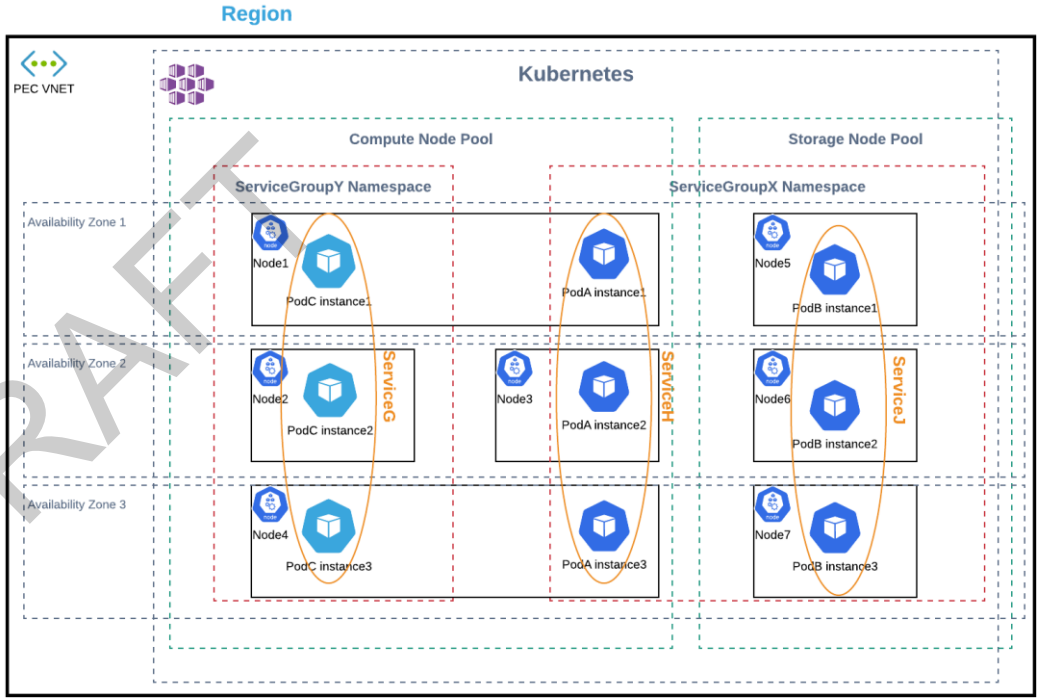
Engage on Azure Global Reach

Confirmed
Planned

Availability roadmap

Kubernetes and Genesys Terms

Kubernetes/Azure	Genesys
Region – A Group of Azure Availability Zones (i.e. data centers) in a geographic area.	
Availabiltiy Zone - A data center in a Region.	
Vnet – A logical isolation of the **Azure** cloud dedicated to your subscription	Unit – This encompass all the automation of the infrastructure in the Vnet within a region
Kubernetes (AKS) Cluster (K8s)	
Node – A VM or Physical Server which is used to run Pods	
Node pool – A group of Nodes that have the same physical characteristics (compute focus)	
Pod – The application that runs on K8s. It can contain multiple containers and run multiple components (processes)	Service – A microservice or a legacy component that has been containerized. e.g., Auth Service from GWS
Namespace – a logic separation of pods within the cluster and share the same access policies.	ServiceGroup – this what was called a product (e.g. GWS) or a group of products (e.g. voice=ors, sipproxy, sipcluster, etc.)

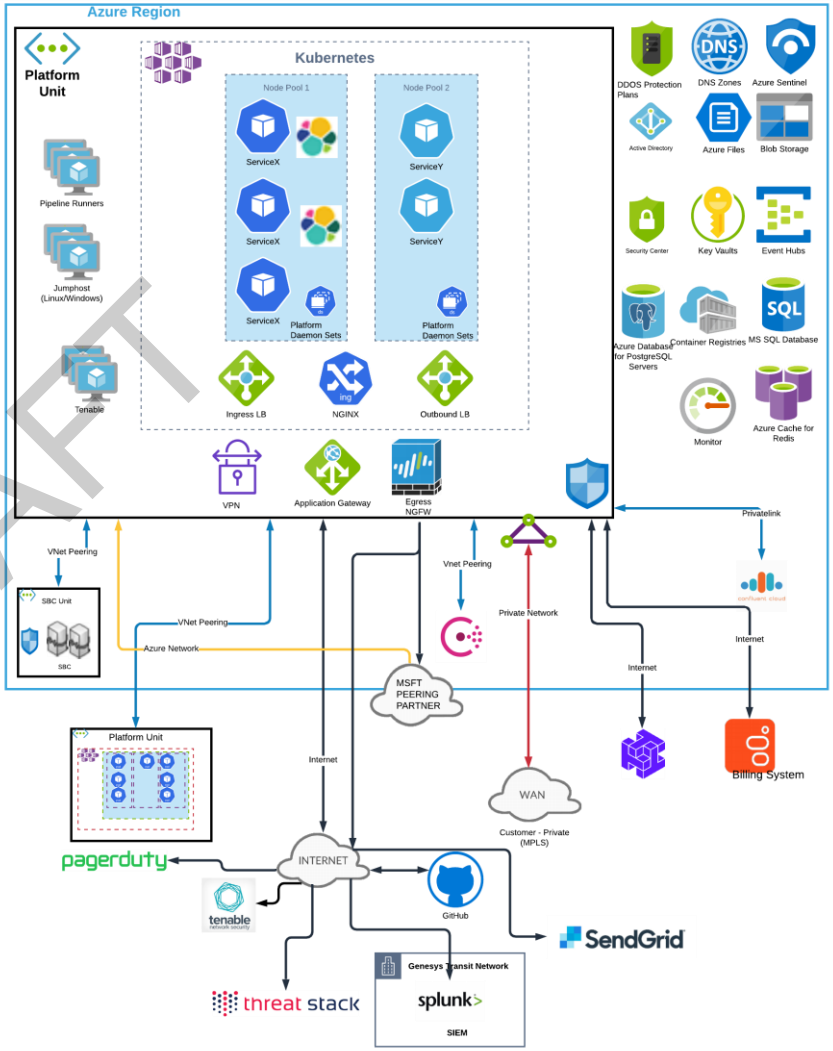


Multi-Region Distributed Architecture

- **Multi-Region** – Architecture supports distributing voice traffic and agents within geo-regions
  - Fits well with different premise-based data center architectures and as well as Cloud
  - Allows for a Global CX Center
  - Provides another level of redundancy with Region pairing in a Geo-Region
- **Multi-AZ** – Takes advantage of Cloud Platform Availability Zones
- **Cloud based Network Connectivity** – Private and Public Options

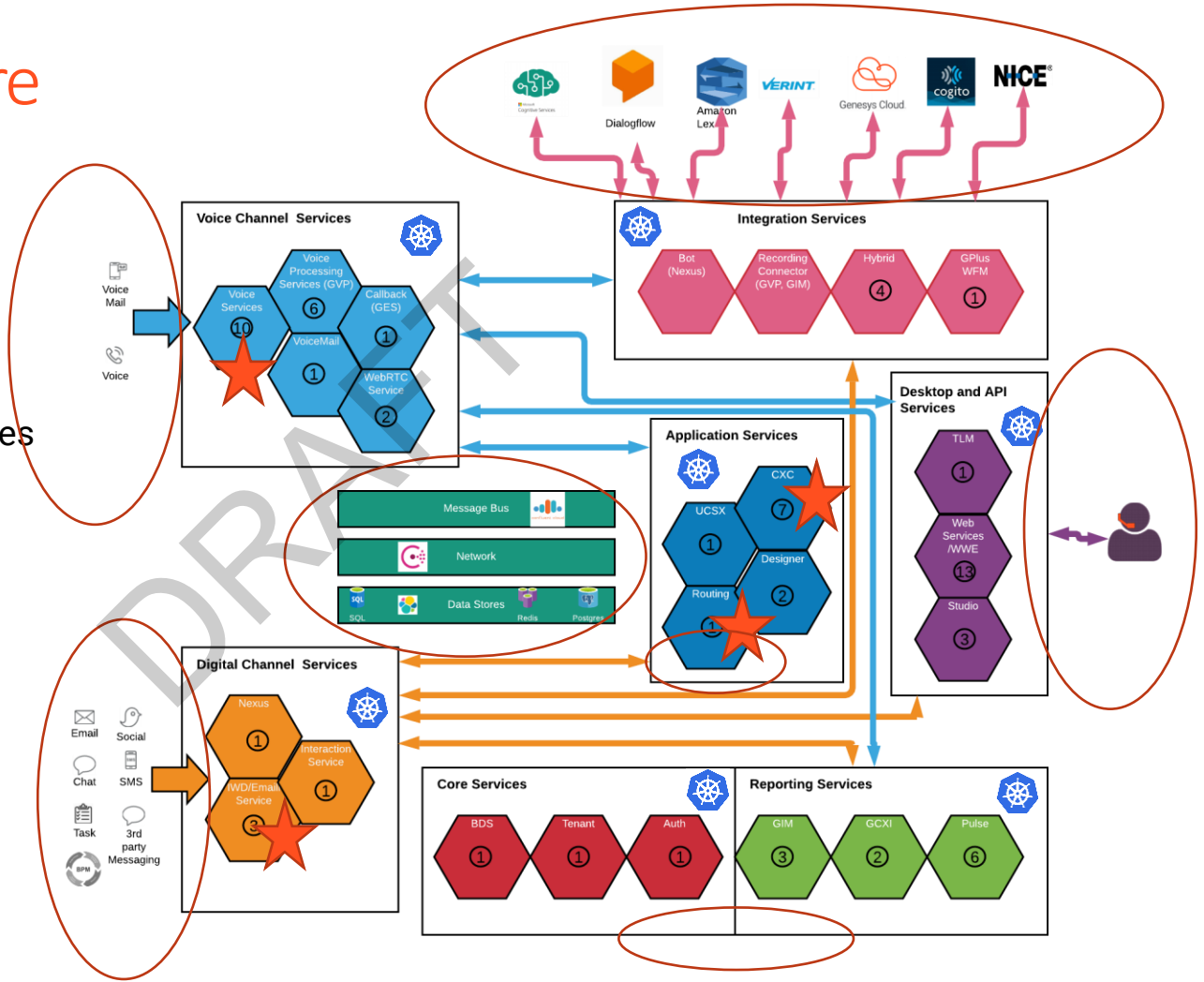
Platform Architecture

- Self contained
- Covers all the security aspects
- Flexible and scalable
- Utilizes managed services to improve reliability and feature velocity

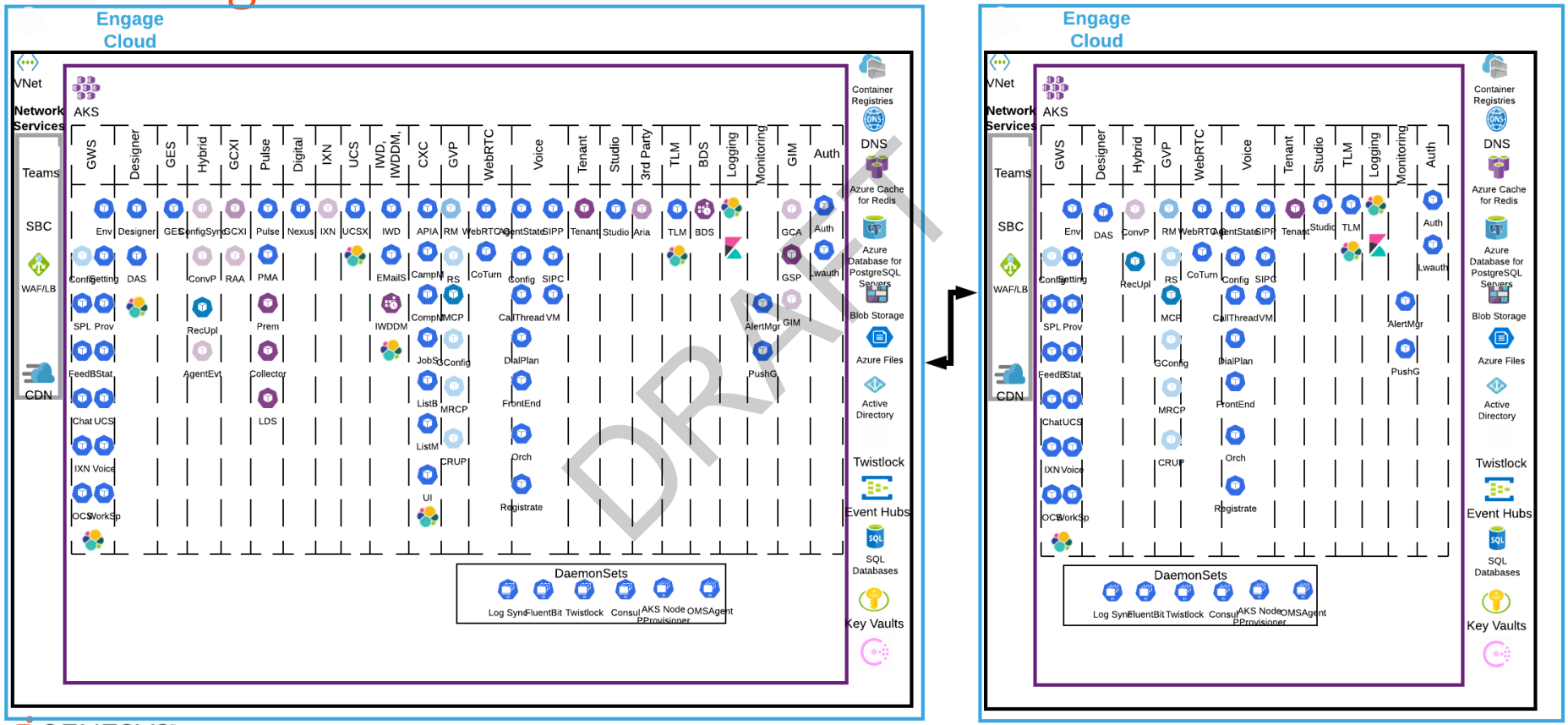


Service Architecture

- Kubernetes and Microservices
- Engage Features (Routing, Intelligent Workload Distribution, Scale)
- Extensive Integration Capabilities
- Multicloud 3rd party dependencies



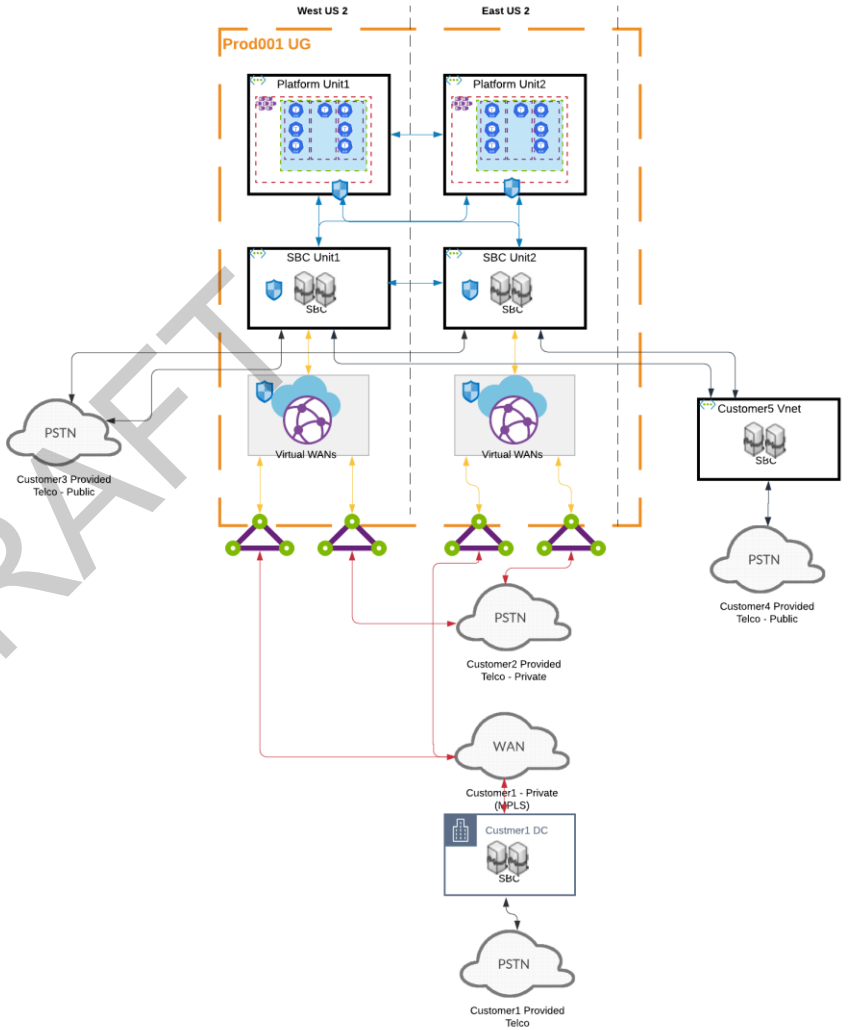
Multi-Region Service Architecture



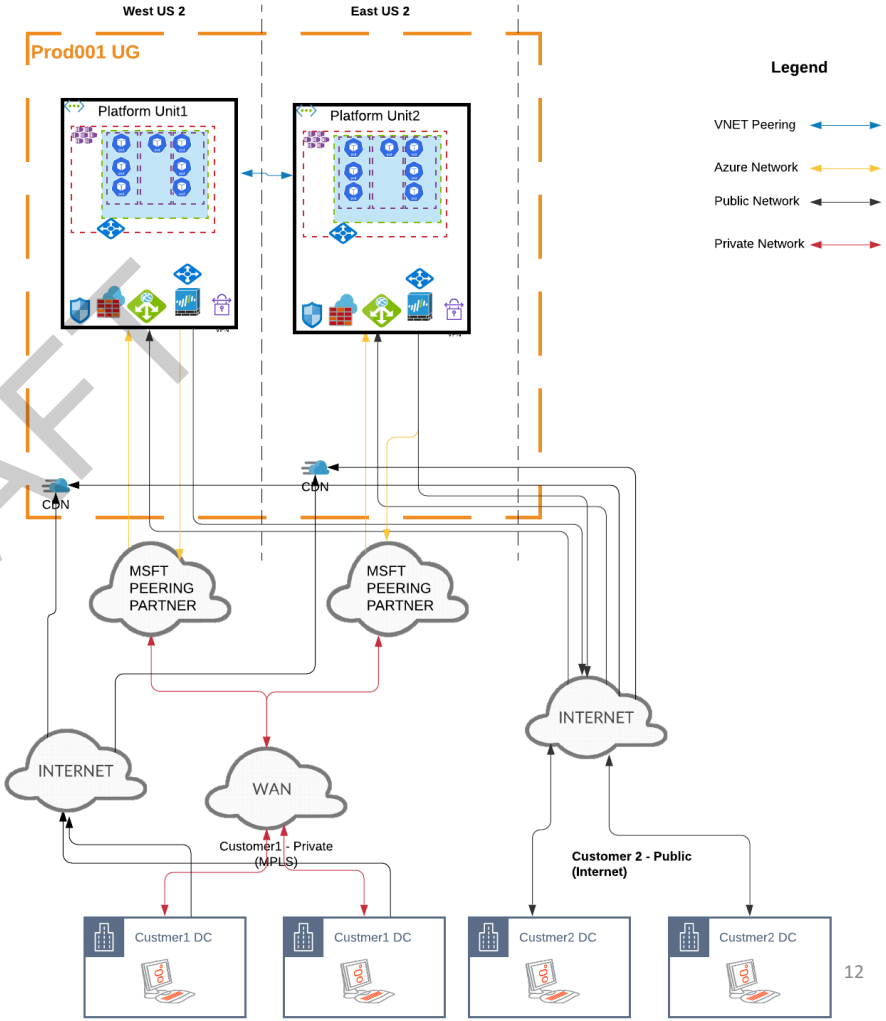
Shared Tenant Specific

3 AZs 2 AZs 1 AZs 3 AZs 2 AZs 1 AZs

Voice Network Architecture

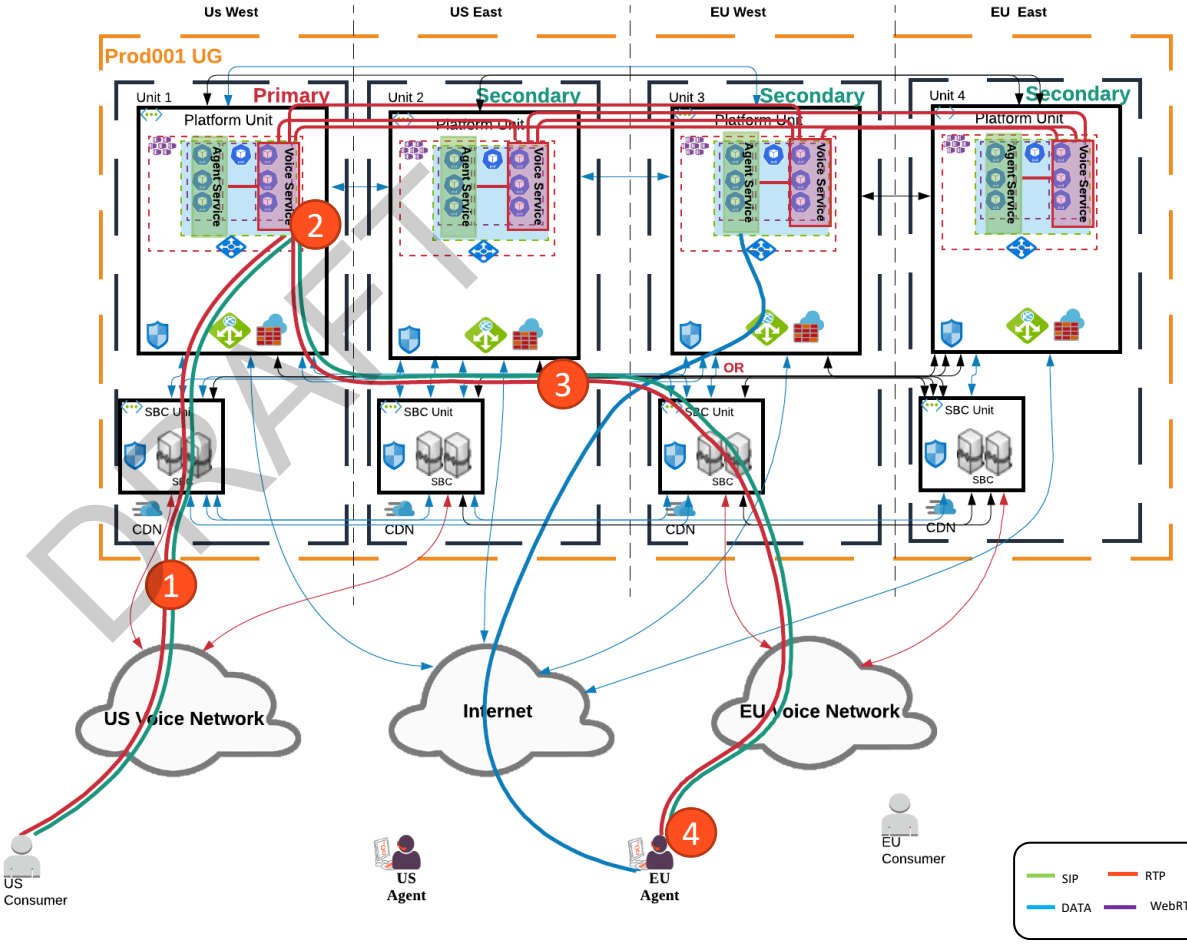


Data Network Architecture



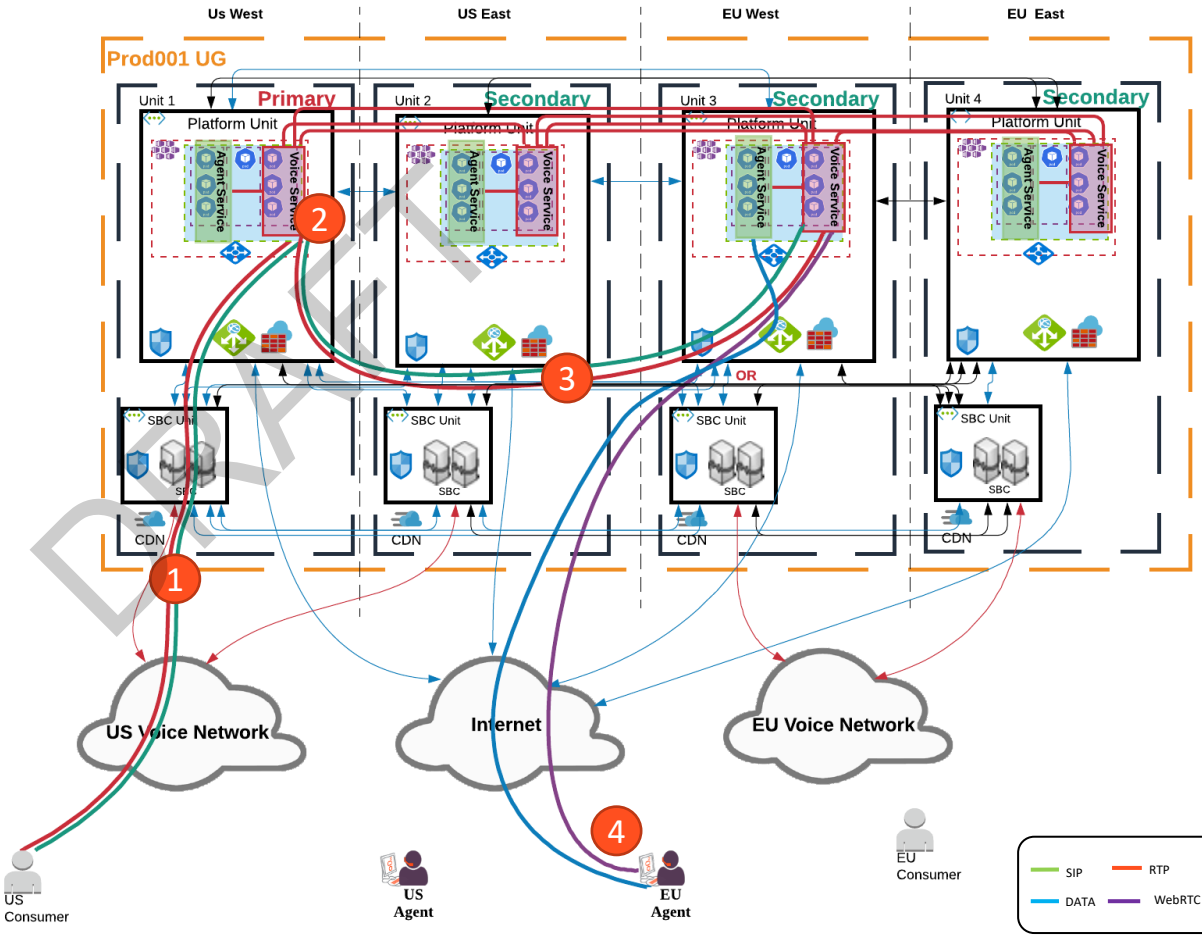
Telephony Architecture – SIP Phone

1) **A US customer** originates a call to the contact center. The US Carrier sends the call to Genesys US West SBC.
2) Genesys Engage **Advanced Routing engine** determines skills required.
3) **An agent in the EU** that meets the skills criteria becomes available. Genesys Engage connects the call with this agent via customer voice network in the EU.
4) EU Agent controls the call through the **WWE desktop** and softphone.



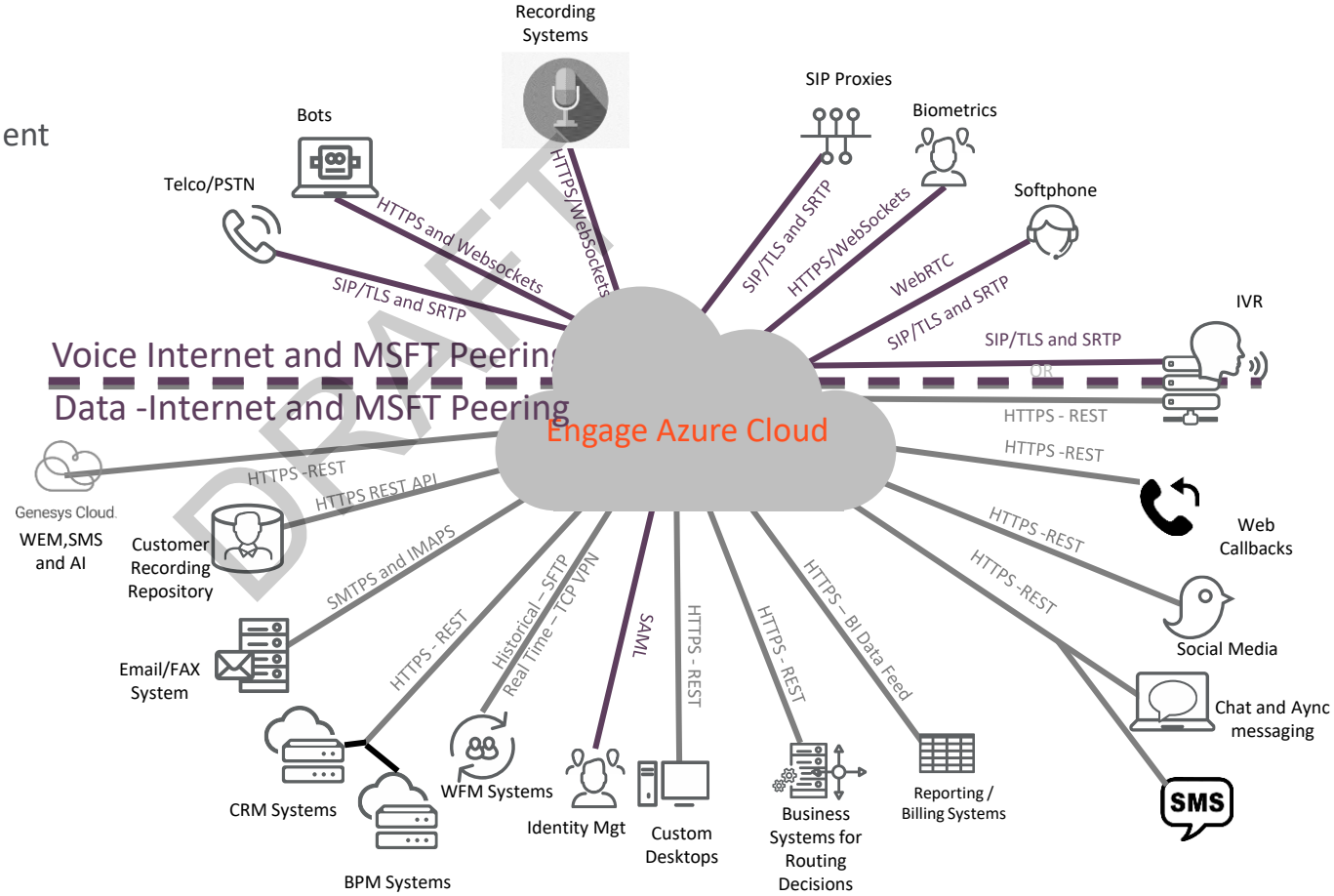
Telephony Architecture – WebRTC

1) **A US customer** originates a call to the contact center. The US Carrier sends the call to Genesys US West SBC.
2) Genesys Engage **Advanced Routing engine** determines skills required.
3) **An agent in the EU** that meets the skills criteria becomes available. Genesys Engage connects the call with this agent via internet and WebRTC in the EU.
4) EU Agent controls the call through the **WWE desktop** and WebRTC softphone.



Engage Azure Cloud Integration Points

- Integrations require engagement of Genesys PS or Partner



GENESYS

Bandwidth Sizing

Traffic	Bandwidth	Transport via	When
Voice (SIP/RTP)	100 kbps G.711, (40 kbps G.729)	SIP TLS/SRTP	Per call
WebRTC (Opus)	Variable 10 kbps to 160kbps	Internet (HTTPS/DTLS)	Per call
Web Service	Typically low	MPLS or Internet (HTTPS)	Varies based upon application
Desktop/ CTI	16 kbps	MPLS or Internet (HTTPS)	Per Call
Screen Recording		MPLS or Internet (HTTPS)	Per recorded call/screen. Can be scheduled
Call playback		MPLS or Internet (HTTPS)	User initiated
Report download	Varies	MPLS or Internet (HTTPS)	User initiated or may be scheduled (sFTP)

These two services are available from Genesys Cloud

User Desktop Requirements

- Cloud UIs are provided via a thin-client GUI in a web browser or via Citrix for a small set of administrative tasks. Other than the requirement to support Citrix a standard PC with the following specifications will suffice:
  - 1 GB RAM
    - Add X for Screen Recording
    - Add X for Softphone
  - Dual-core, 2GHz CPU
  - 1 GB hard drive
  - Windows - 7 or 8 32-bit or 64-bit
  - Citrix version supported on the PC: Citrix Receiver 3.3 and above
- Browsers:
  - Microsoft Internet Explorer® 10+
  - Chrome™ web browser 22+ except for GI2 is not supported.
- There are no drivers, applets or any other downloads that need to be made to the PC, with the possible exception of the Genesys Softphone and Screen Recording Client for users who are processing interactions (calls, emails, etc.).

Phone Support

SIP/WebRTC Softphone

In-browser WebRTC*

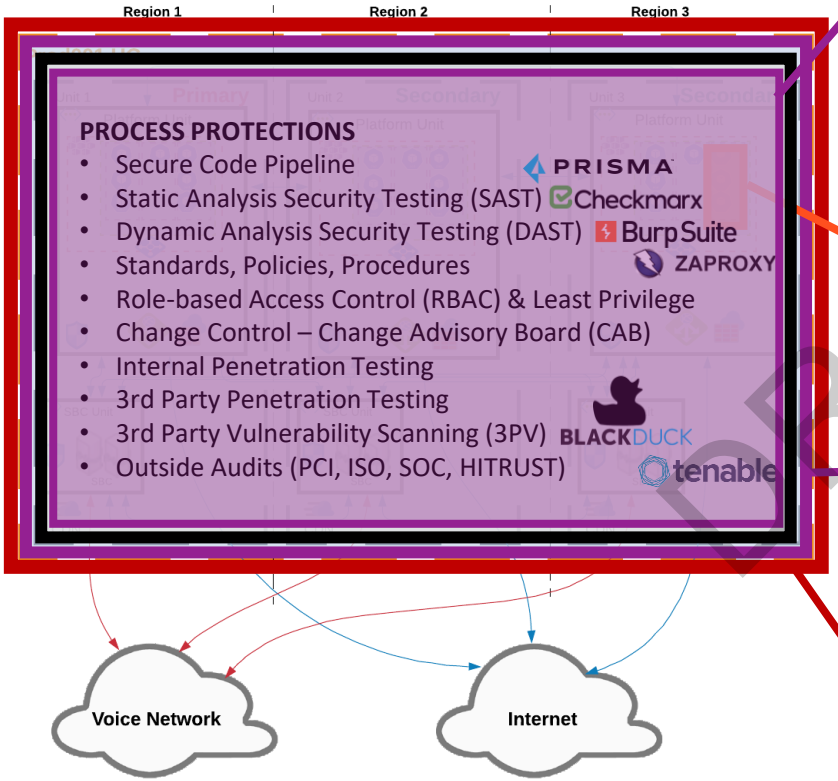
Genesys

Existing Phone

Remote agent capabilities with complete call control managed through desktop (hold, transfer, consult transfer, supervision, etc.)

* Requires open Internet connection with IP whitelisting

Engage Cloud Multi-Layered Security



Data and Access PROTECTIONS

- All Data encrypted at rest
- TLS 1.2 used for all external communications (voice and data)
- All UI and most APIs are authentication (SAML)
- RBAC Access Control
- Data Masking
- UI Security (security banners, inactivity timeouts, lock outs, masking)
- API Protection – Rate limiting, Application Keys)

HOST LEVEL PROTECTIONS

CROWDSTRIKE

tripwire

threat stack

- Host-based Intrusion Detection (HIDS)
- File Integrity Monitoring (FIM)
- Anti-malware

ENVIRONMENT OBSERVABILITY

splunk> phantom

splunk> siem

- Vulnerability Detection and Management
- Security Orchestration, Automation & Response (SOAR)
- Security Information & Event Management (SIEM)

PERIMETER SECURITY

Azure WAF & DDoS

- Web Application Firewall (WAF)
- Distributed Denial of Service (DDoS) Protection
- Intrusion Detection/Prevention System (IDS/IPS)
- Network Policy
- Whitelisting as needed

GENESYS

External Access Security

- UIs
  - WAF
  - Authentication
    - Genesys based
    - IDP (SAML)
  - Role based access control
  - IP whitelisting
  - TLS 1.2 (HTTPS, Websockets)
- Ingress APIs
  - WAF
  - Authentication
    - Web Tokens, Oauth, Application Key
    - Genesys based
    - IDP (SAML)
  - Role based access control
  - IP whitelisting
  - TLS 1.2 (HTTPS, Websockets)
- Egress APIs
  - Outbound Proxy (white/black listing)
  - Authentication
    - Web Tokens, Oauth, Application Key
  - Role based access control
  - TLS 1.2 (HTTPS, Websockets, SFTP, SMTPS, IMAPS)
  - VPN (for 3rd party WFM RTA connection)
- Voice Traffic
  - SBC - control point
  - WebRTC
    - Authentication
      - Genesys based
      - IDP (SAML)
    - Role based access control
    - TLS 1.2 (HTTPS, SIP TLS, SRTP)
  - Encryption
    - SRTP and SIP TLS
    - Private Connectivity via ExpressRoute

Understanding Failure Modes

What to expect when the system experiences failures

Availability Zone Failure

Functionality	Operational Impact	Representative Experinece	Customer Experience
Agent login	No impact	No Impact	No Impact
Callback	No impact	No Impact	No Impact
Historical data feed	Delayed Reporting BI feed is affected if the system that performs the upload is within the failed AZ into Blob storage. The data is not lost. The upload will resume later when the AZ is recovered; the data will be provided retroactively.	No Impact	No Impact
Designer applications	No impact	No Impact	No Impact
Call Routing	No impact	No Impact	No Impact
Agent and Queue Provisioning	No impact	No Impact	No Impact
Historical and real-time reporting/monitoring tools	Delayed Reporting BI feed upload is affected if the system that performs the upload is within the failed AZ into Blob storage. The data is not lost. The upload will resume later when the AZ is recovered; the data will be provided retroactively.	No Impact	No Impact
Recording playback and viewing	No impact	No Impact	No Impact
Genesys WFM	No impact	No impact	No impact
Voicemail	No impact	No Impact	No Impact
Digital (Chat, Email, etc.)	No impact	No impact	No impact
Outbound	No impact	No impact	No impact

Primary Region Failure

Functionality	Operational Impact	Representative Experience	Customer Experience
Agent login	Agent will be automatically re-login into Alternative (Secondary) region. SIP Phone will have to re-register.	Automatically reconnect Phone re-registers to secondary	Active Calls Dropped in primary region
Callback	The callbacks will not be executed until Primary is back up and running.	Automatically reconnect Phone re-registers to secondary	Delayed Callbacks
Historical data feed	You will not have access to historical data until the primary is back up and running.	Automatically reconnect Phone re-registers to secondary	No Impact
Designer applications	You will not be able to make any changes to the designer application until Primary is back up and running.	Automatically reconnect Phone re-registers to secondary	No Impact
Call Routing	Active calls that were associated with Primary are lost. All new calls will be send to the secondary Region by the Carrier and proceed through IVR; the calls will queue up until the agents log in and Ready. No impact to calls already be processed by the Secondary.	Automatically reconnect Phone re-registers to secondary	Active Calls Dropped in primary region
Agent and Queue Provisioning	You will not be able to make any provisioning changes (adding agents, groups, queues, etc.) until Primary is back up and running.	Automatically reconnect Phone re-registers to secondary	No Impact
Historical and real-time reporting/monitoring tools	You will not be able to access the real-time reporting tools until Primary is back up and running. The data is not lost. The upload will resume later when the Primary is recovered; the data will be provided retroactively. The secondary region keeps performing its background jobs (collecting reporting statistics). Statistics previously collected in the Primary region, as well as the statistics in the secondary region, will be utilized by the Reporting tools when Primary is back up and running	Automatically reconnect Phone re-registers to secondary	No Impact
Recording playback and viewing	You will not have access to recordings in primary until it is back up and running. Recordings in secondary will continue to be collected until the primary region is up and running and the recordings are synced with it.	Automatically reconnect Phone re-registers to secondary	No Impact
Genesys WFM	You will not be able to perform any WFM function until Primary is back up and running.	Logged out of WFM will not have access till primary recovers.	No Impact
Voicemail	You will not have access to an voicemails stored in Primary until Primary is up and running but will be able to access voicemails in the secondary.	Automatically reconnect Phone re-registers to secondary	Recovered on next call
Digital (Chat, Email, etc.)	You will not be able to perform any chat or email function until Primary is back up and running.	Automatically reconnect Phone re-registers to secondary but the ability to process chat and email interactions is not available.	Chat is unavailable to customers.
Outbound	You will not be able to perform any outbound Campaign function until Primary is back up and running.	Automatically reconnect Phone re-registers to secondary but the ability to process outbound Campaign interactions is not available.	Active Calls Dropped in primary region

Secondary Region Failure

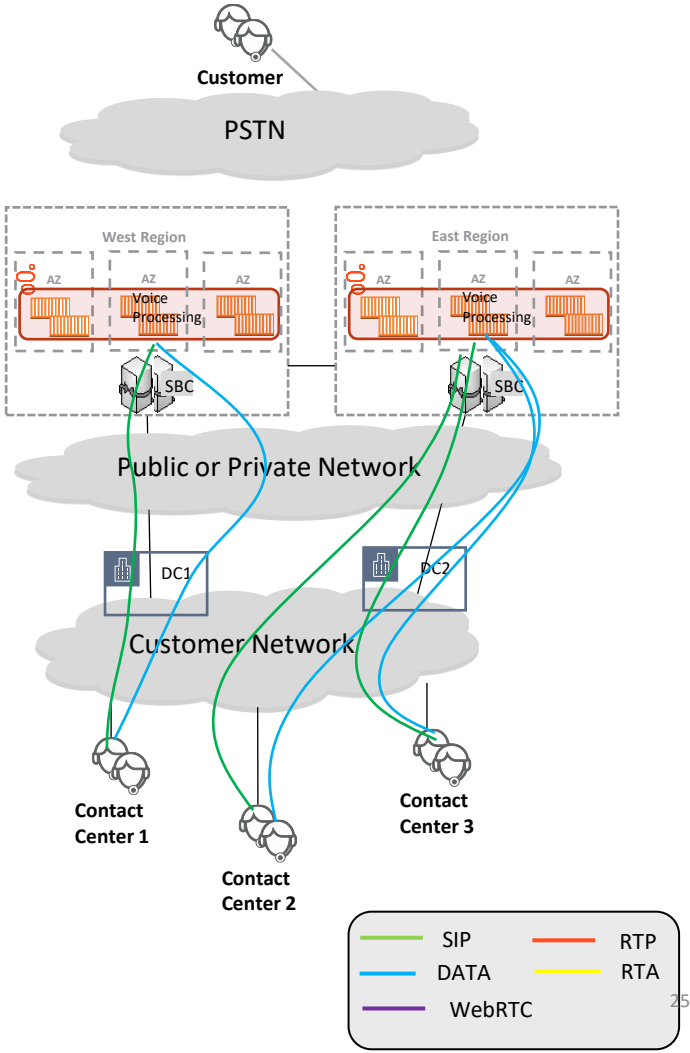
Functionality	Operational Impact	Representative Experinece	Customer Experience
Agent login	Agent will be automatically re-login into Alternative (Primary) region. SIP Phone will have to re-register.	Automatically reconnect Phone re-registers to primary	Active Calls Dropped in secondary
Callback	No impact	Automatically reconnect Phone re-registers to primary	In Queue Callback Dropped in Secondary region
Historical data feed	No impact	Automatically reconnect Phone re-registers to primary	No Impact
Designer applications	No impact	Automatically reconnect Phone re-registers to primary	No Impact
Call Routing	Active calls that were associated with Secondary are lost. All new calls will be send to the Primary Region and proceed through IVR; the calls will queue up until the agents log in and Ready. No impact to calls already be processed by the Primary.	Automatically reconnect Phone re-registers to primary	Active Calls Dropped in secondary region
Agent and Queue Provisioning	No impact	Automatically reconnect Phone re-registers to primary	No Impact
Historical and real-time reporting/monitoring tools	Will not be collect data from secondary region	Automatically reconnect Phone re-registers to primary	No Impact
Recording playback and viewing	No Impact	Automatically reconnect Phone re-registers to primary	No Impact
Genesys WFM	No Impact	Logged out of WFM will not have access till primary recovers.	No Impact
Voicemail	You will not have access to an voicemails stored in secondary until secondary is up and running but will be able to access voicemails in the primary.	Automatically reconnect Phone re-registers to primary	Recovered on next call
Digital (Chat, Email, etc.)	No Impact	Automatically reconnect Phone re-registers to primary	No impact
Outbound	No impact	Automatically reconnect Phone re-registers to primary	Active Calls Dropped in secondary region

SIP Endpoint Registration and Agent Login

The SIP endpoint will be registered to the Genesys SBCs. The DNS SRV record splits these registrations evenly.

Customer agents use Genesys WWE via a web browser, which will connect and allow a log in via the MPLS. Data connectivity will be encrypted via https.

Any agent can receive any call according to Customer's business rules for Skills Based Routing, regardless of where the call arrived, and where the agent is currently logged in.



Call Qualification/IVR

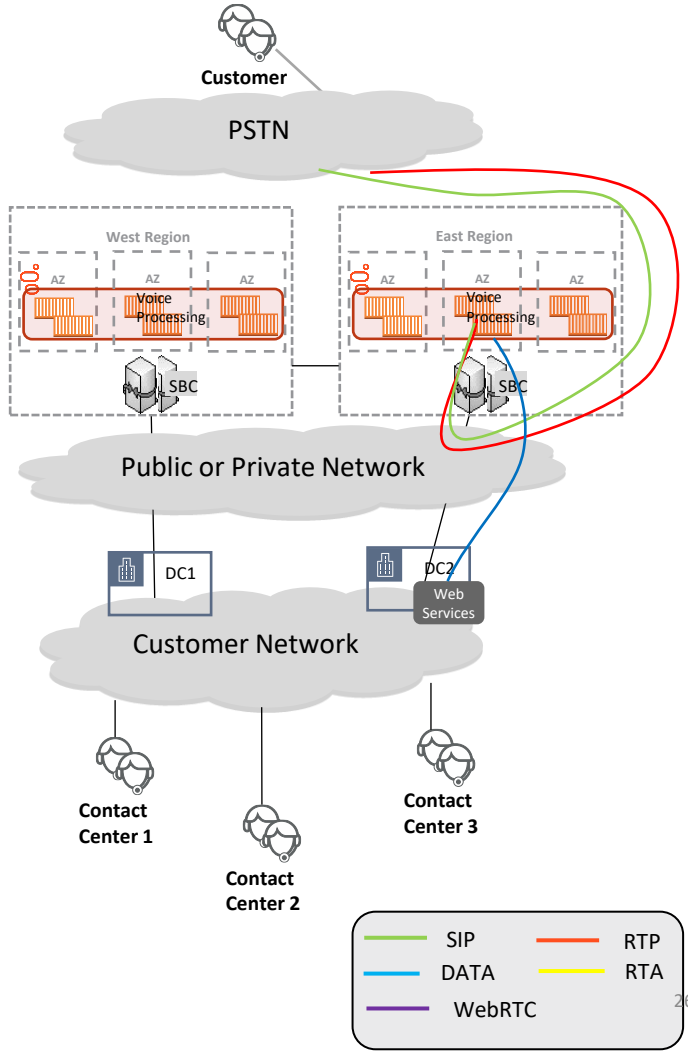
A caller originates a call to the contact center.

Calls are directed to East Region. This diagram shows Carrier sends the call to Genesys East SBC.

During the qualification of the call, the voice application may connect to the Customer's web services to retrieve customer data using REST.

Genesys routing engine determines skill requirements based on Customer's business rules.

Call is queued if an agent meeting skills criteria is not immediately available.



Call Routed to Agent

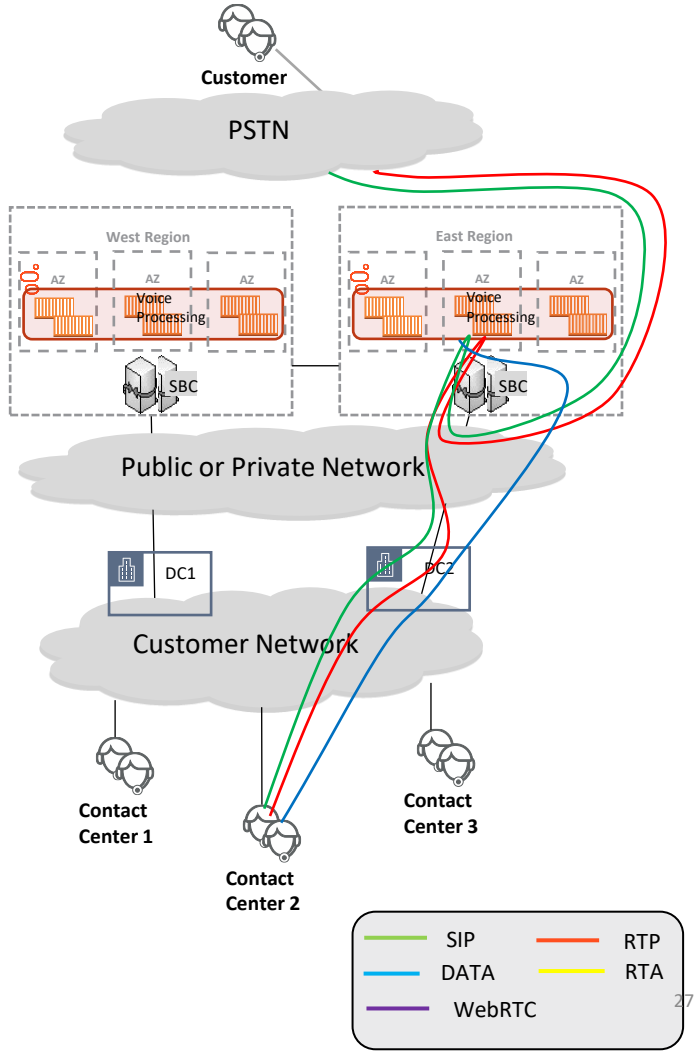
An agent meeting the skills criteria becomes available.

Genesys originates a second call leg to the agent. The call is delivered via East region

On answer, Genesys bridges the caller and agent legs.

If the call is to be recorded, RTP media remains anchored on Genesys Media Control Processor.

Agent controls the call through the WWE desktop.



Call Routed to Agent - WebRTC

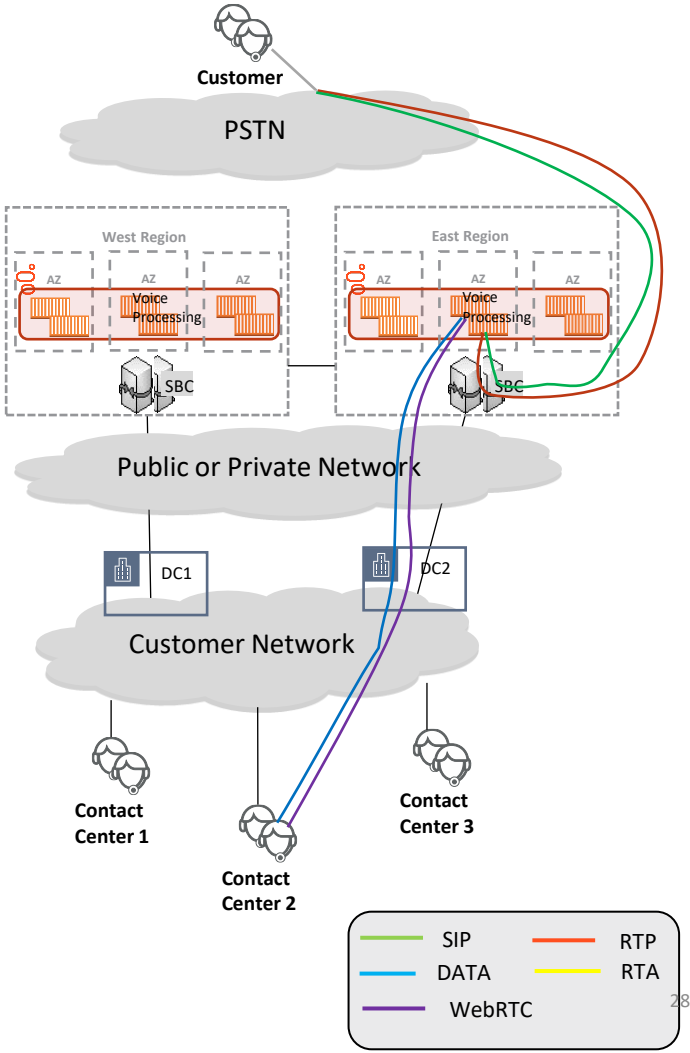
An agent meeting the skills criteria becomes available.

Genesys originates a second call leg to the agent. The call is delivered via East region

On answer, Genesys bridges the caller and agent legs.

If the call is to be recorded, RTP media remains anchored on Genesys Media Control Processor.

Agent controls the call through the WWE desktop.



Call Routed to Agent in other region - WebRTC

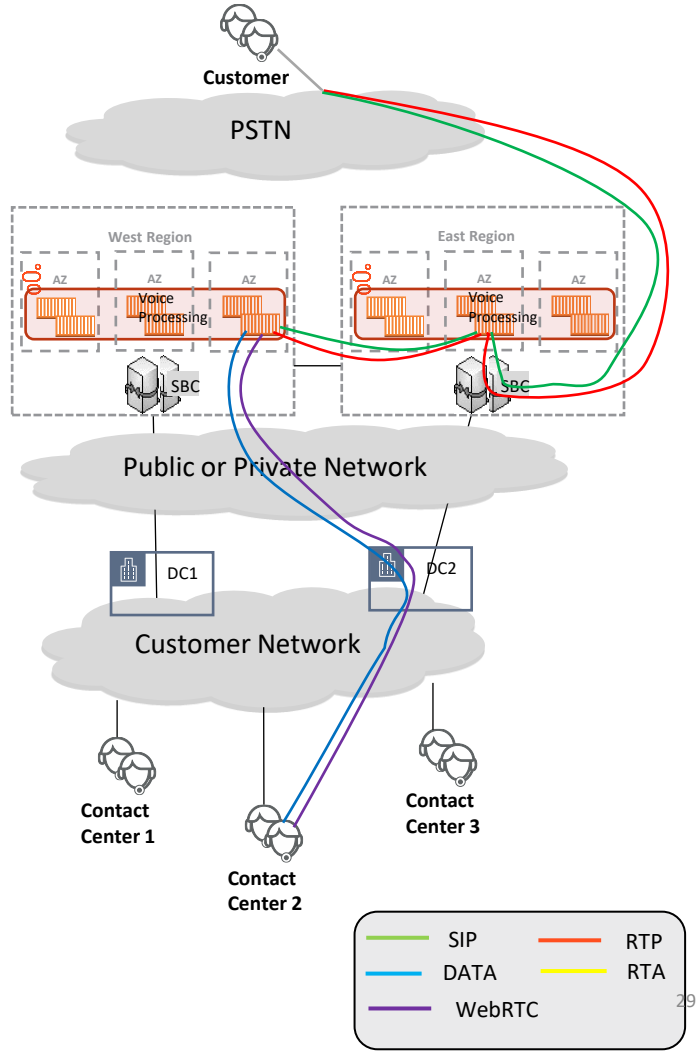
An agent in other region meeting the skills criteria becomes available.

Genesys originates a second call leg to the agent. The call is delivered through West region

On answer, Genesys bridges the caller and agent legs.

If the call is to be recorded, RTP media remains anchored on Genesys Media Control Processor in the East region.

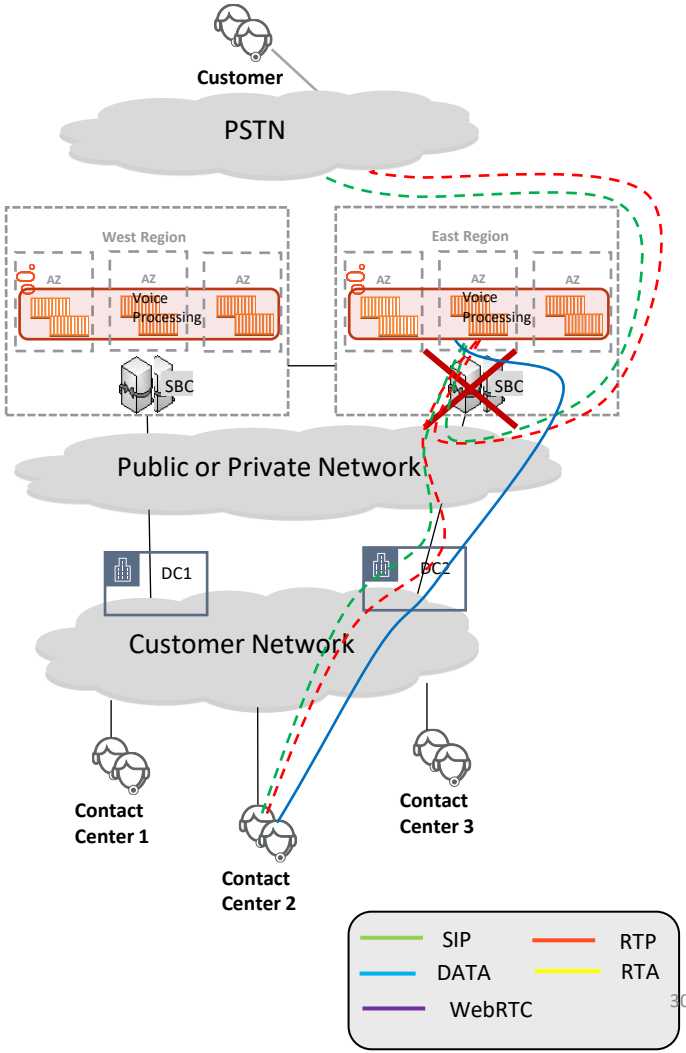
Agent controls the call through the WWE desktop.



Failure of SBC

In this scenario, a catastrophic incident takes the SBC out of service. As a consequence:

- Established calls from East region are dropped
- As SIP registrations are done via East region, they would be lost and the agents would be logged out.
- Carrier detects that East region SBC is not responding and sends all calls to West region.
- If the agent logged in through the East region, then the agent will lose access to Agent Desktop. In this case, the application will leverage ‘smart failover’ to log the agent back in via the West region.



Recovery of GTN AMS Failure

Smart Failover will automatically log the agents back in to WWE and set themselves ready the other region.

As the phone was registered through East region, the SIP phone would re-register, obtaining the IP address West region SBC via the SRV record

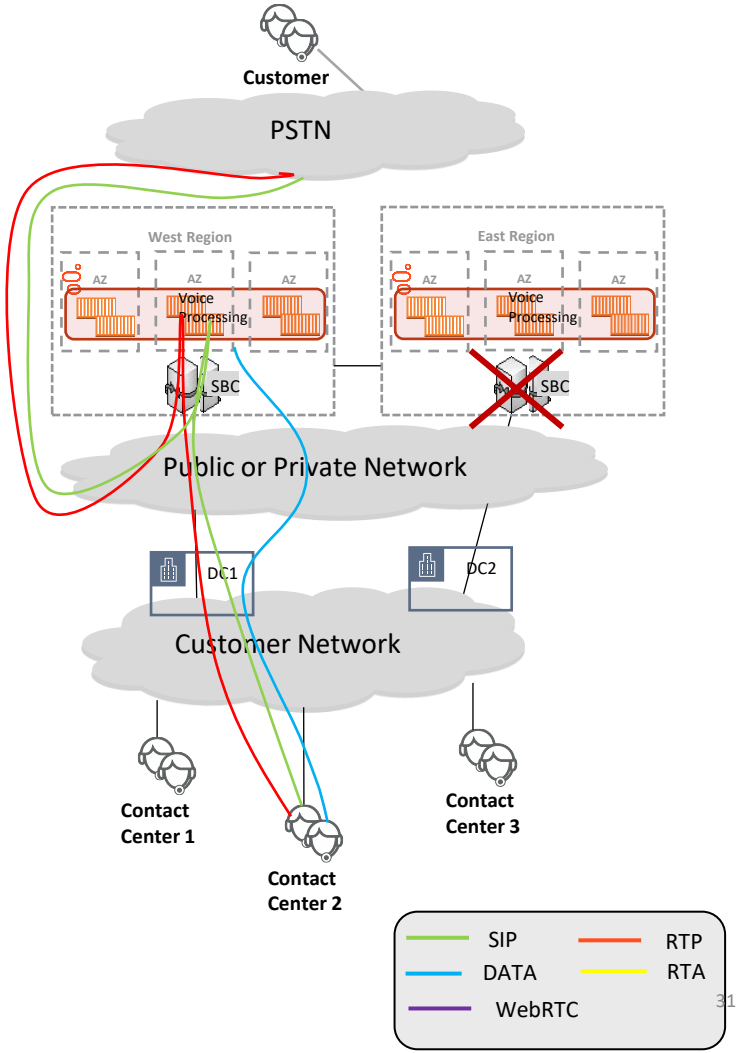
An agent meeting the skills criteria for the call becomes available.

Genesys originates a second call leg to the agent.

On answer, Genesys bridges the caller and agent legs.

Since the call is to be recorded, RTP media remains anchored on Genesys Media Control Processor.

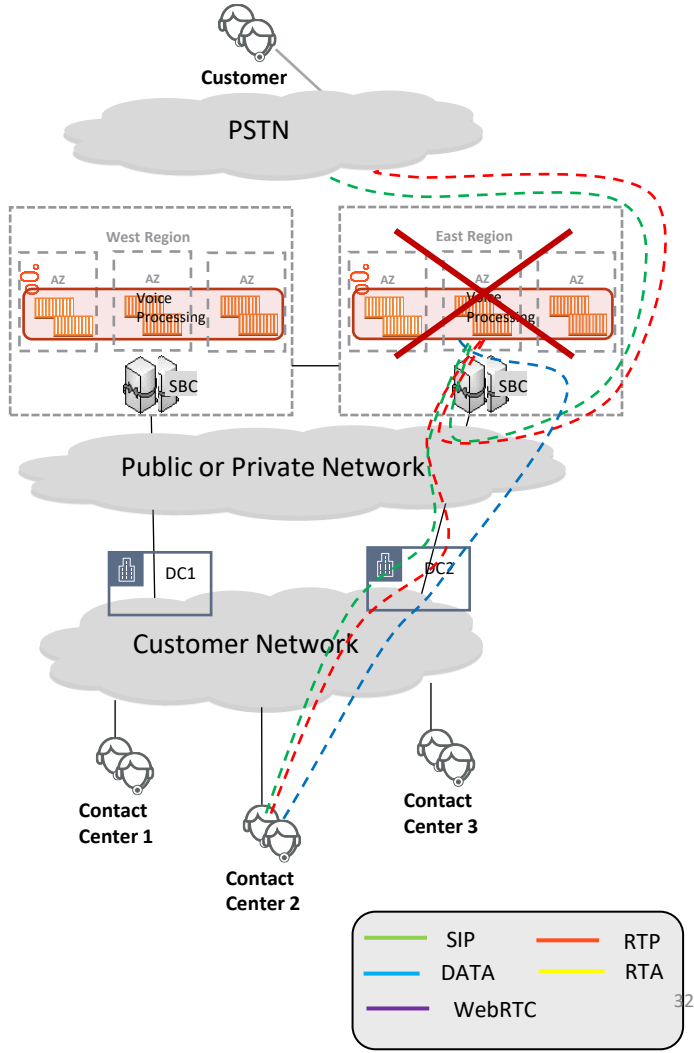
Agent controls the call through the Desktop.



Failure of REGION

In this scenario, a catastrophic incident takes the East Region out of service. As a consequence:

- Established calls from East region are dropped
- As SIP registrations are done via East region, they would be lost and the agents would be logged out.
- Carrier detects that Genesys SBC is not responding and sends all calls to the alternate SBC.
- If the agent logged in through the East region, then the agent will lose access to Agent Desktop.



Recovery of Region Failure

Smart Failover will automatically log the agents back in to WWE and set themselves ready the other region.

As the phone was registered through East region, the SIP phone would re-register, obtaining the IP address of the Genesys West region SBC via the SRV record

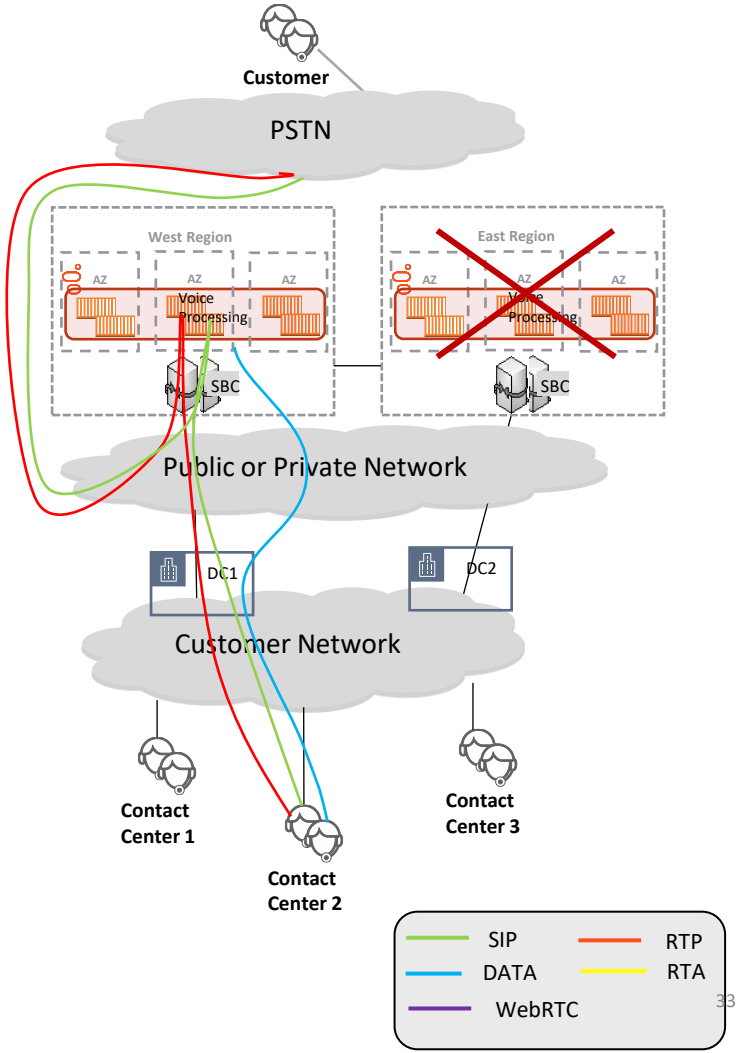
An agent meeting the skills criteria for the call becomes available.

Genesys originates a second call leg to the agent.

On answer, Genesys bridges the caller and agent legs.

Since the call is to be recorded, RTP media remains anchored on Genesys Media Control Processor.

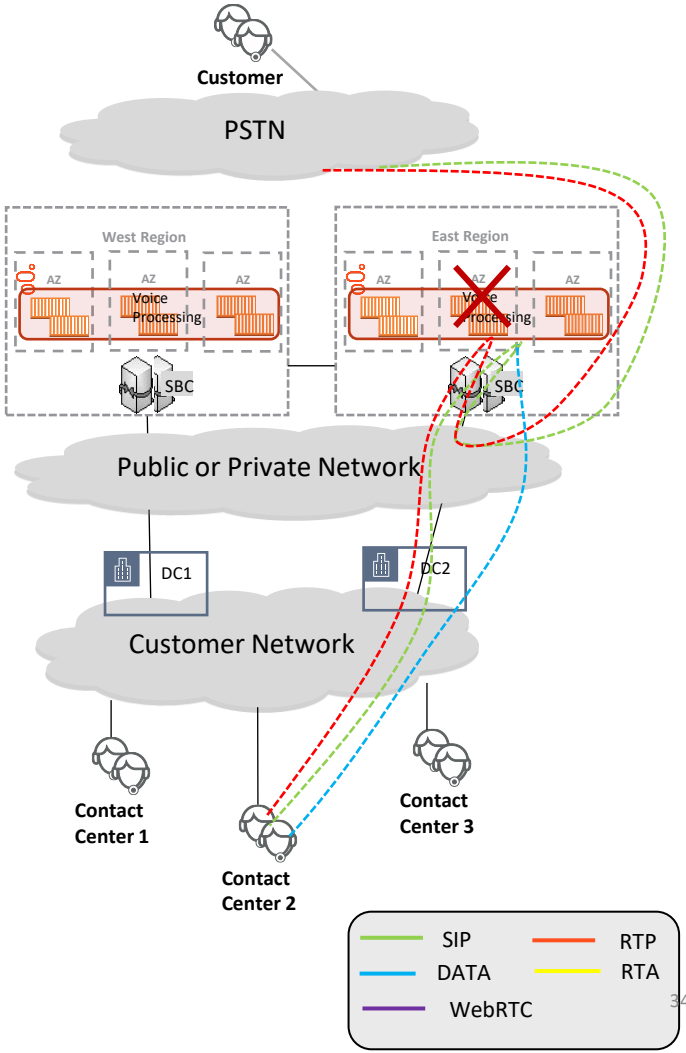
Agent controls the call through the Desktop.



AZ (Data Center) Failure

In this scenario, a catastrophic incident takes the active Availability Zone. The agents should not see a disruption but this failure on rare occasions could result in the following conditions:

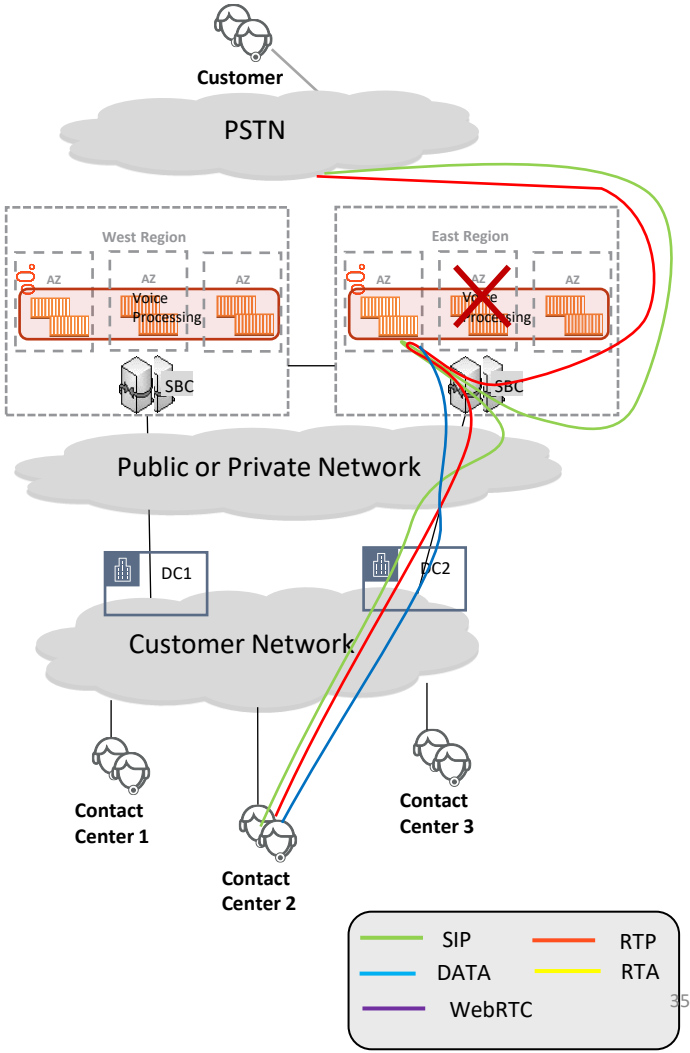
- Failure may temporarily disrupt voice conversation while the DR processes complete.
- Agents may detect application latency.



AZ (Data Center) Failure Recovery

Voice processing seamless continues to work:

- The voice processing fails over to the backup in the alternate AZ
- The AMS SBC recognizes failure of the impacted AZ and initiates communications with the voice processing in the alternate AZ.
- The desktop resumes normal processing.



India call flows

DRAFT

GENESYS

Genesys Cloud – **Domestic** Inbound Call Flow to Domestic based India Consumer using Customer PSTN and Customer MPLS

Call flow:

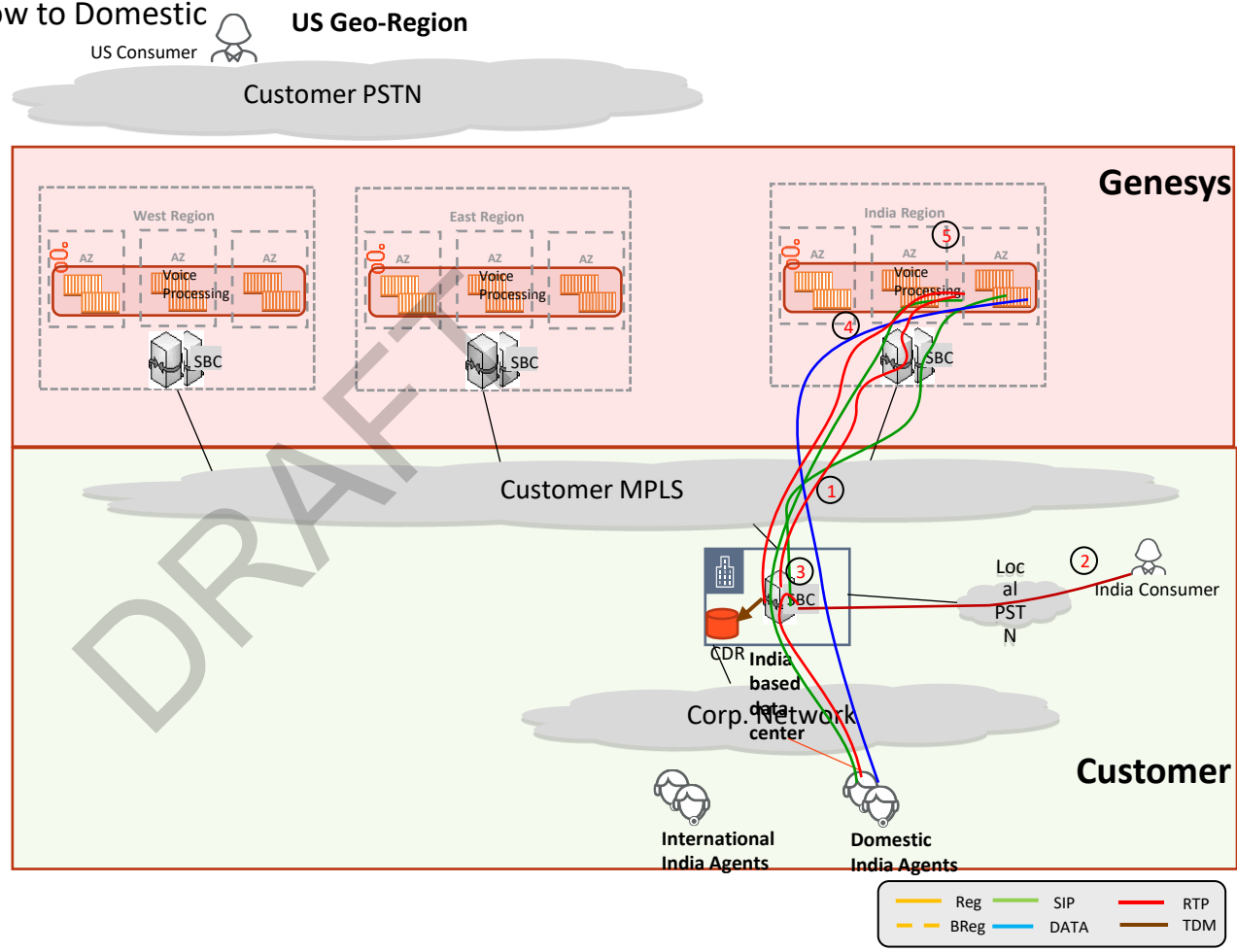
1) Domestic based India Agent logs into Genesys Cloud India based WWE from Agent desktop.

2) India based Consumer Dials India Toll Free Number (TFN) or Direct Inward Dial (DID) which uses Customer procured and managed PSTN.

3) Customer India based SBC receives the call and determines that it needs to be routed to the Genesys Cloud India Region. Genesys India region SBC receives the call, Genesys India region SBC forwards to Genesys India based voice processing, performs IVR treatment (if required) then Selects Agent, which in this case happens to be in India.

4) Genesys Cloud India based Voice Processing makes outbound call from Genesys India region to Agent in India over customer MPLS network through the Customer's SBC in India to the agent.

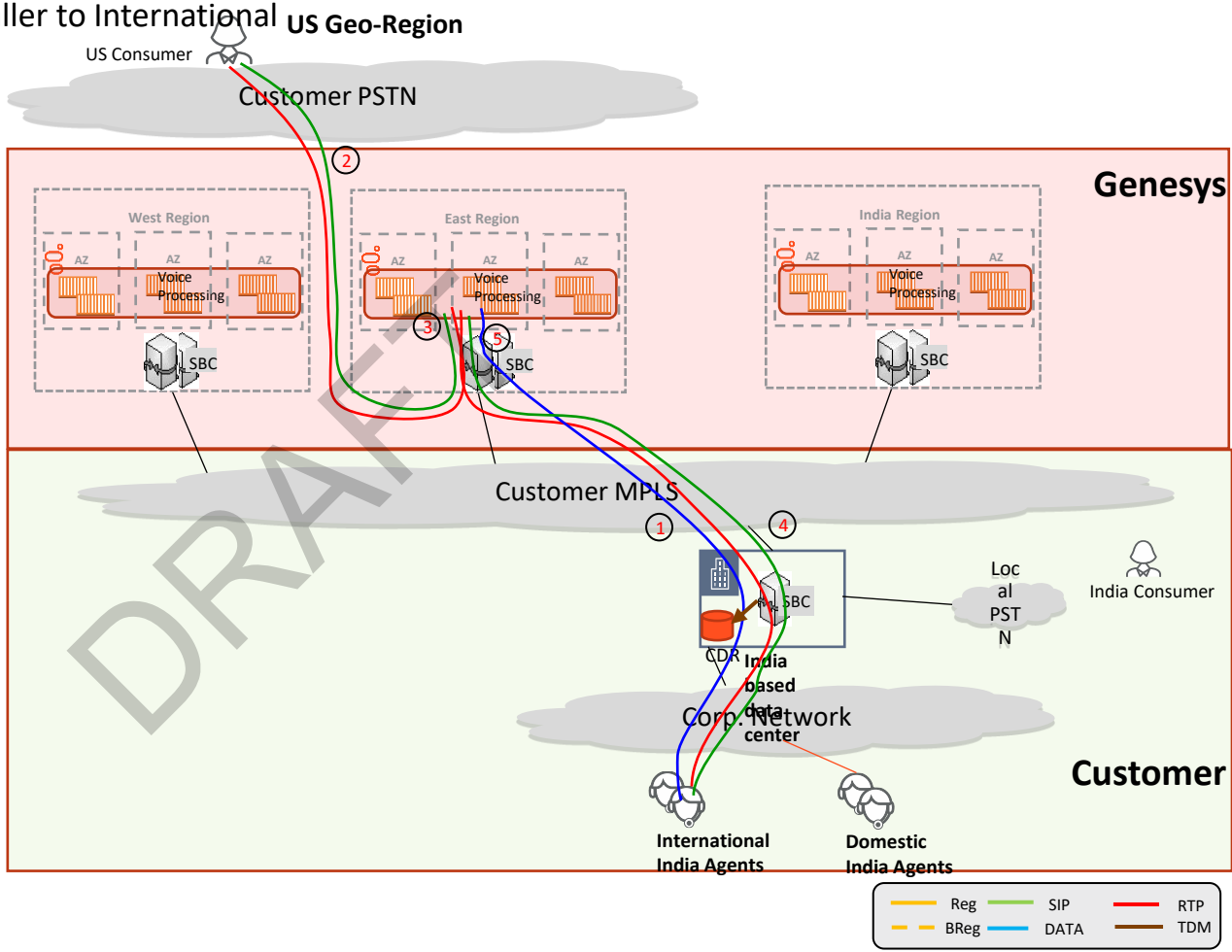
5) Once India Agent answers, both parties (India based Consumer and India Agent), then Genesys Cloud India based voice processing bridges the two parties together



International Inbound Call Flow from US Caller to International based India Agent
using Customer PSTN and Customer MPLS

Call flow:

1) International based India Agent logs into Genesys Cloud US based WWE from Agent desktop.
2) Caller Dials US Toll Free Number (TFN) or Direct Inward Dial (DID) which uses Customer procured and managed PSTN.
3) Genesys Cloud US based SBC and voice processing in East region receives call, performs IVR treatment (if required) then Selects Agent.
4) Genesys Cloud US based Voice Processing makes outbound call from East region to Agent in India over customer MPLS network to the through the Customer's SBC in India to the agent.
5) Once India Agent answers, both parties (US Consumer and India Agent), then Genesys Cloud based US voice processing bridges the two parties together



Security

GENESYS

Tenant Data

Data	Retention	How Tenant Data Isolation is handled	Security
Call / Screen Recording Data	30 days beyond that is charged extra	• Separate tenant Azure Blob storage accounts.	Recordings are encrypted using AES256 with unique data encryption keys. Data Encryption keys are RSA asymmetric encrypted in PKCS7 envelopes using key encryption keys provided by customer and locked in secured key store. Customer self-service manages own keys which are not handled by Genesys personnel. Full audit trail in place.
Voice Application and Treatments Data	As long as deployed	• Partitioned cluster of the Designer application servers, so that data can't be shared across tenants	File System level encryption. Does not contain any sensitive data
Routing and Orchestration Application	As long as deployed	• Partitioned cluster of the Designer application servers	File System level encryption. Does not contain any sensitive data

Tenant Data

Data	Retention	How Tenant Data Isolation is handled	Security
Configuration and Provisioning Data	As long as deployed	• Separate DB system per tenant	Azure Data Encryption. Plus - Only passwords are combined with salt and then combination is encrypted with SHA-2 256 bit.
Reporting Data	13 Months days	• Separate DB system per tenant • Blob Storage Account per tenant for data feed data (30 days)	Azure Data Encryption. Should not contain any sensitive data (filtered out before send to reporting components)
Contact, Interaction, Service, Suggested Response Data	90 days except for SRs which are as long as deployed. Also Contact records are keep until requested to remove.	• Separate DB system per tenant	Azure Data Encryption.

Tenant Data

Data	Retention	How Tenant Data Isolation is handled	Security
Chat Transcripts	90 days	• Separate DB system per tenant	Azure Data Encryption.
WFM Data	90 days for detailed interaction information 24 months for WFM data	• TBD	TBD
Outbound Data	As long as the Campaign is deployed	• Separate DB system per tenant • Same DB System partitioned based on tenantID column	Azure Data Encryption.

Tenant Data

Data	Retention	How Tenant Data Isolation is handled	Security
Survey Result data and Report	90 days	• Shared DB System partitioned based on tenantID column • Separate tenant DB Schemas (Tables) - No access to the DBMS system just the tables	Azure Data Encryption. Sensitive data is filtered out.
Voice Mail	90 days	• Separate Blob storage container per Tenant	Azure Data Encryption. Does not contain any sensitive – we require customer to play a message to the consumer to not put that data in a voicemail.
Callback	As long as the Callback request is Scheduled	Shared DB System partitioned based on tenantID column	Azure Data Encryption. Does not contain any sensitive data
Workload Mgt	As long as the tasks are being processed	• Shared DB System partitioned based on tenantID column • Separate DB System per Tenant	Azure Data Encryption. Does not contain any sensitive data

Tenant Data

Data	Retention	How Tenant Data Isolation is handled	Security
PD Logs	13 Months	• Shared Blob Storage Account	Azure Data Encryption. All sensitive data is masked out.
Security Log	13 Months	• There is really no tenant data – just infrastructure related data (VM data, network scan results)	The data store is encrypted.

Tenant Services

Process	How Tenant Isolation is handled	Security
Interaction and workload Processing (voice, email, chat, tasks, etc.)	• Separate trunks to isolate the traffic • Specific dialing plan to isolate the traffic • Separate email connections to isolate the traffic • Specific routing applications to control which agents can handle which interactions and where a interaction can go when it is transferred to or conferenced with another agent	External Interfaces (UI, Ingress/Egress API, Voice) – See External Access Security Internal Interfaces – No connection encryption Log files and UIs – sensitive data masking
Recording Processing	• TBD	TBD

Tenant Services

Process	How Tenant Isolation is handled	Security
Voice Application and Treatment Processing	• Appropriate set of rules determine which tenant the call is for and which script or treatment to fetch	External Interfaces (UI, Egress API, Voice) – See External Access Security Internal Interfaces – No connection encryption Log files and UIs – sensitive data masking
WFM Processing	• TBD	TBD
Outbound Processing	• Separate Outbound Execution Pod instances for each tenant (OCS)	External Interfaces (UI, Voice) – See External Access Security Internal Interfaces – No connection encryption Log files and UIs – sensitive data masking

Tenant Services

Process	How Tenant Isolation is handled	Security
Callback Processing	• Separation based on TenantID/Appl Key in the API requests	External Interfaces (Ingress API, UI) – See External Access Security Internal Interfaces – No connection encryption Log files and UIs – sensitive data masking
VoiceMail Processing	• Voicemail and their meta data are processed from tenant specific Blob storage accounts	External Interfaces (WWE, Voice) – See External Access Security Internal Interfaces – No connection encryption Log files and UIs – sensitive data masking
Survey Processing	• Specific survey applications to control which consumers get which surveys	External Interfaces (UI) – See External Access Security Internal Interfaces – No connection encryption Log files and UIs – sensitive data masking

Security related Controls for Customers

- User Authentication and Authorization
  - Must provision all the users, their passwords and roles/permissions
  - If custom roles and permissions are needed, you must SR request for Genesys to create it.
  - If using IDP (SAML), must provision IDP configuration via Agent Setup
- Recording Keys
  - Must create and manage the keys for encrypting and decrypting records via Agent Setup
- Agent Desktop
  - Create a local Cert for the connection between the WWE in the browser and Softphone (not required for the browser based WebRTC softphone)
- UI whitelisting (ingress)
  - Provide list of address ranges to whitelist
- External data dips
  - Provisioning outbound proxy
  - Provision Authentication and Authorization for these data dip APIs.
- Voice
  - Provision the necessary Certs for secure voice traffic (SRTP, SIP TLS) with a Service Request and NetOps team
- Voicemail
  - Must provide greeting message to indicate to the users that they should leave any sensitive data in their voice messages.
- Identify what data your team considers sensitive and should be masked out or encrypted so Genesys can do the necessary provisioning for it.
- Email
  - Provision a secure Connection to your Corporate Email Servers via Agent Setup
- CXC
  - Provision a secure Connection to your Corporate FTP System via CXC UI
- WFM Adapters
  - Provision a secure Connection to your Corporate FTP System via Agent Setup
  - Provision a secure VPN from your Corporate Data Center to the Genesys Platform (Vnet) – Done through Service Request and Ops team
- Historical Data Feed
  - Get and utilize the secure Keys/Tokens to access the Blob Storage from Genesys