ASSERTION®

a voice security company

Secure Voice

Voice security add-on for SBCs to protect your enterprise from scam, robocalls , toll fraud and cyber attacks through AI based Call & Registration screening in real-time.

It integrates using standard SIP with the SBCs off-the-shelf. Single point of connection to the voice ecosystem. Built in fail-back ensures that even if Secure Voice fails no calls will be disrupted.

July 2024

Index

Pain & Solution – Remote worker security

Enterprises live in fear that SBCs used for Remote Workers are constantly being attacked

Remote Worker SBCs that are internet-facing are often attacked within 5 minutes of going online, rendering them vulnerable to potential breaches and malicious activities.

Check every remote worker registration, detect the malicious ones and block the attacker automatically, making remote working safe

SBC logs are monitored in near real-time to check for each registration message and its source. Using AI and Assertion threat intel, attacks are detected and blocked.

Pain & Solution – Scam call

Enterprises worry about ransomware attacks (scam calls), Toll fraud, and TDoS attacks

Screen every incoming and outgoing call to detect malicious calls and block or redirect them automatically, making voice calls safe

293 million scams and robocalls were reported globally in 2021, making them the second most reported crime worldwide. Financial losses amounted to $55.3 billion in 2021 and $1.02 trillion in 2022. Contact center fraud increased by 40%.

Assertion Defender is the next hop after the SBC for calls. Each INVITE message is screened by AI for malicious patterns, updating the display and redirecting or blocking calls if needed. Defender is not in the media path. Keep-alive with the SBC ensures automatic failover to the next hop if Defender fails, preventing call loss.

Pain & Solution – VIP callers

VIP callers (such as CMS.gov auditors) getting poor treatment – long wait times, poor agent experience, etc.

VIP callers like Government auditors (CMS.gov) are very valuable and one negative feedback could reduce the call center’s rating from 5-star to 4-star, resulting in loss of millions of dollars in business.

Check every call to determine if it is from a CMS.gov auditor (VIP caller) and inform agent & supervisor so they can provide the best possible service.

Assertion screens every incoming call, looks up the ANI in our database of CMS auditor phone numbers, and notifies the agent and supervisor through a message on the Microsoft Teams group chat within 10 seconds of the call arriving. Our database is kept up to date in real-time because we screen millions of calls a month and by using feedback from agents who answer such calls.

Pain & Solution – DNC & Geo-fencing

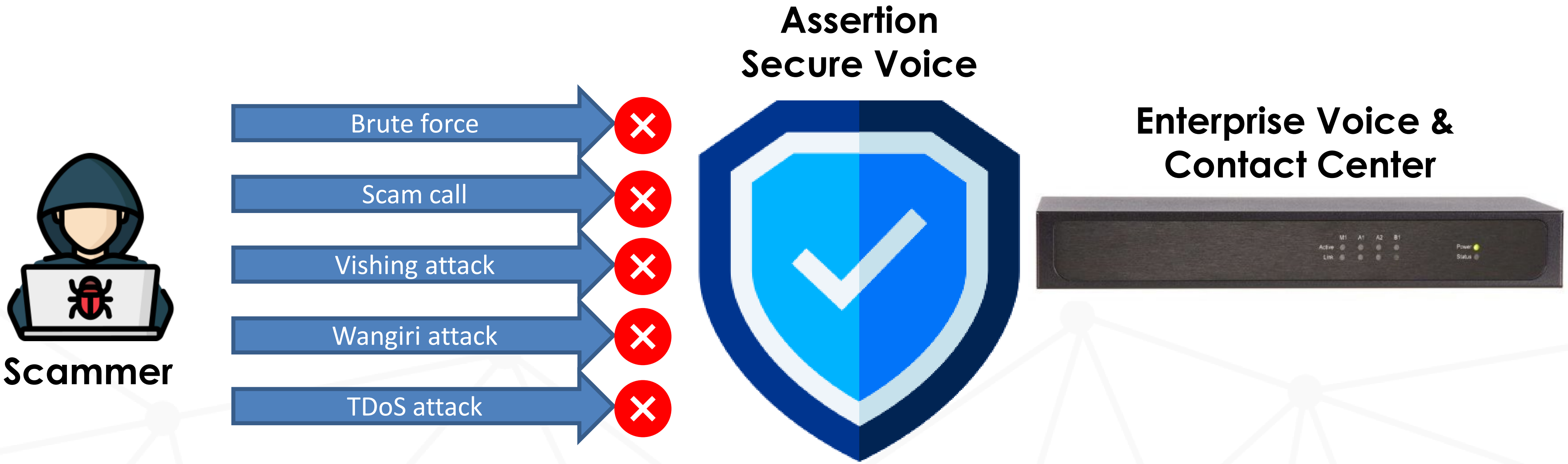
Enterprises do not have central tool to enforce compliance to DNC, Sanctions call barring, and Geo-fencing rules

In most countries, local regulations have requirements around enforcing do-not-call capabilities. These could be for regulatory reasons, geo-political, or to safeguard customer / employee interests. Failure to comply could cost fines or even loss of business.

Monitor every incoming and outgoing call and block or redirect calls that violate compliance rules

Assertion Defender is the next hop after the SBC for calls and screens incoming and outgoing calls from the call center as well as from UC applications like Teams and Zoom., making it the ideal place to enforce compliance rules.

Features of Secure Voice



REMOTE WORKER SECURITY

- Detect brute force, enumeration, time travel, and more attacks in near-real time
- Automatically block IP of attacker
- Geo-fence based on IP ranges / countries
- Get detailed attack analytics
- Get AI suggestions to tighten configuration

INCOMING CALL SCREENING

- Tag Scam calls with a Scam likely display
- Block or Redirect Scam and Robocalls
- Alert on VIP calls. Redirect if necessary.
- Block TDoS attack
- Block calls from premium rate numbers, geo-fenced and Sanctioned countries

OUTGOING CALL SCREENING

- Use local ANI on outbound calls to get more call connects
- Block calls to high-cost destinations to avoid toll fraud
- Enforce OFAC, DNC and geo-fencing rules
- Enforce calling restrictions to comply with local laws

Benefits

1. Detect and Block cyber attacks on SIP remote worker
2. Automatically block attacker IP on SBC or Firewall
3. Alert on VIP callers (e.g., CMS.gov auditor calls)
4. Protect from impersonation attempts (and ransomware attacks)
5. Block toll fraud attempts and TDoS attacks
6. Enforce DNC, OFAC, and Geo-fencing rules
7. Get traffic visibility across your entire voice network
8. Priced per call, billed monthly or annually

Success Story

Hosted Service Provider

The Telecom giant provides UCaaS and CCaaS services to SME customers. The SBC farm front-ending the deployment was constantly getting attacked, leading to huge toll frauds and service disruptions. They had a 24/7 NOC team to monitor logs to detect and block attackers but it took hours to detect and block an attack, was expensive, and was not accurate enough.

They implemented Assertion Secure Voice to automate the perimeter security and block all attacks in near real-time, ensuring a safer environment for their customers.

Healthcare

The Healthcare giant provides mission critical imaging systems that are used in hospitals worldwide. Their staff are in over 150 countries and are on the road, servicing the equipment. Their remote working infrastructure came under regular attack. They were also plagued by junk calls and feared that a telephony DoS attack could render their support center useless.

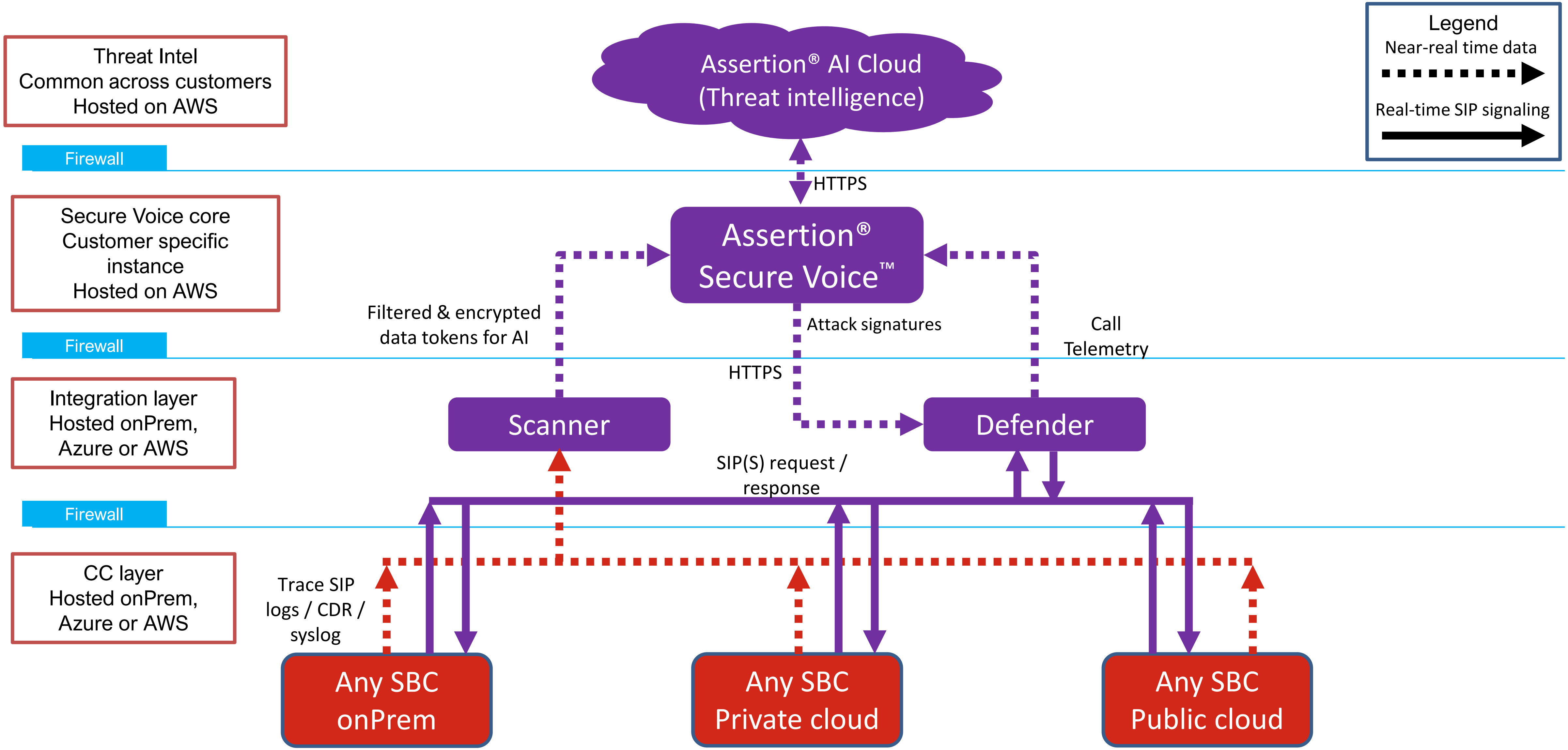
They implemented Assertion Secure Voice to detect and block cyber attacks (like brute force) and call-based attacks (like scam, robocall, TDoS) in real-time.

Outsourcers

The BPO, a major outsourcer in the Health Care industry, is a 5-star BPO. This 5-star rating allows them to bid for and win RFPs worth millions, where 5-star rating is a qualification criteria. CMS.gov’s auditors call periodically as “customers” to check the service levels. A negative feedback from them can reduce the star rating.

They implemented Assertion Secure Voice to detect these special calls and notify the agent and their supervisor on MS Teams about this call within 5 seconds. This allowed the agent and supervisor to provide great service to the VIP caller, thereby maintaining their 5-star rating.

Architecture - Remote worker security & Call screening for transformation customers

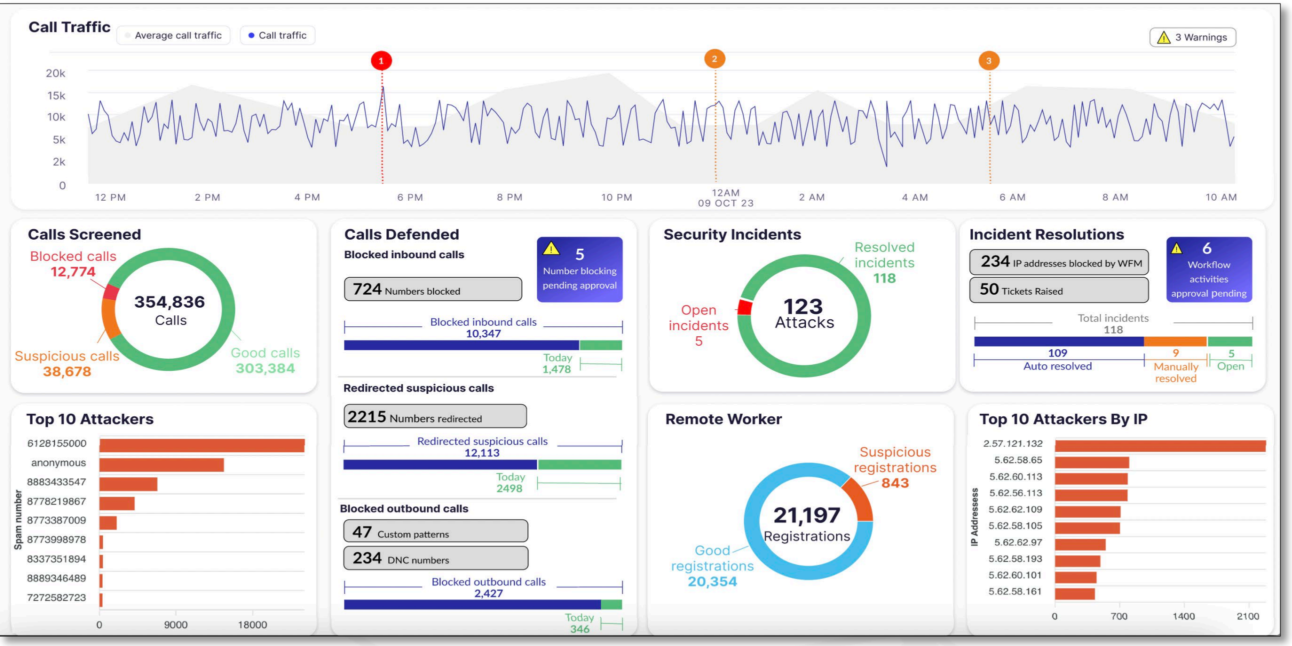


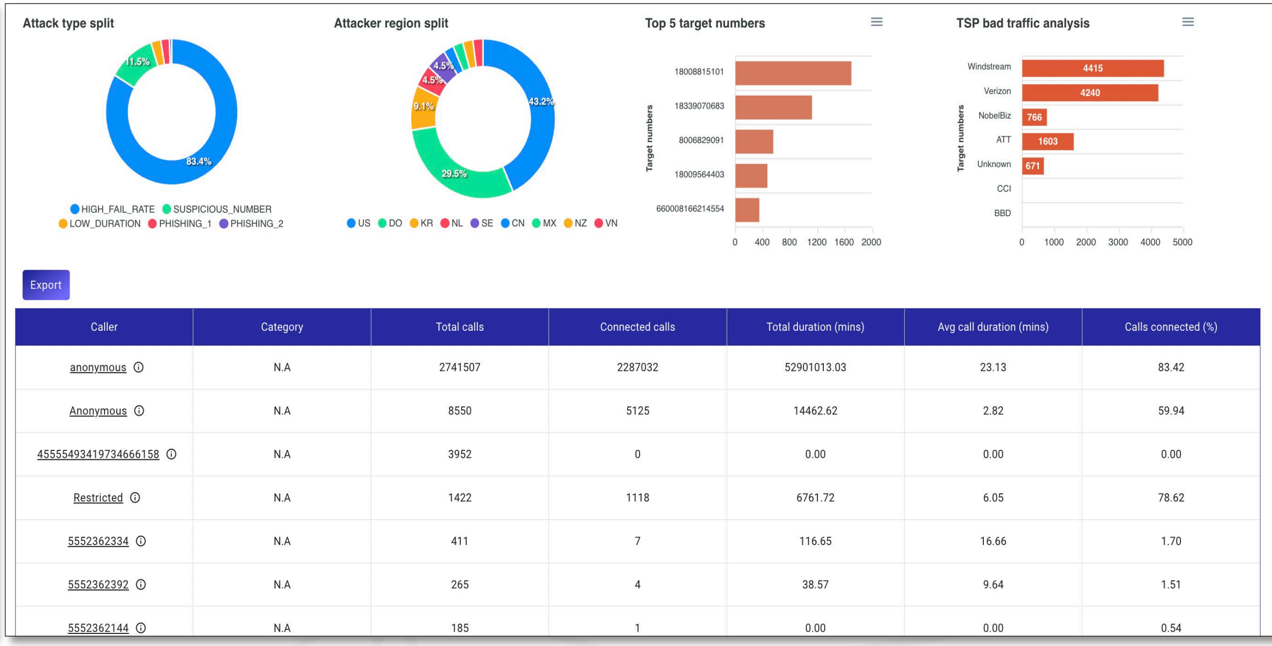
Defender is consulted during call setup and allows / redirects / blocks calls. It is not on signaling path of connected calls and is never in the media path.

Architectural considerations

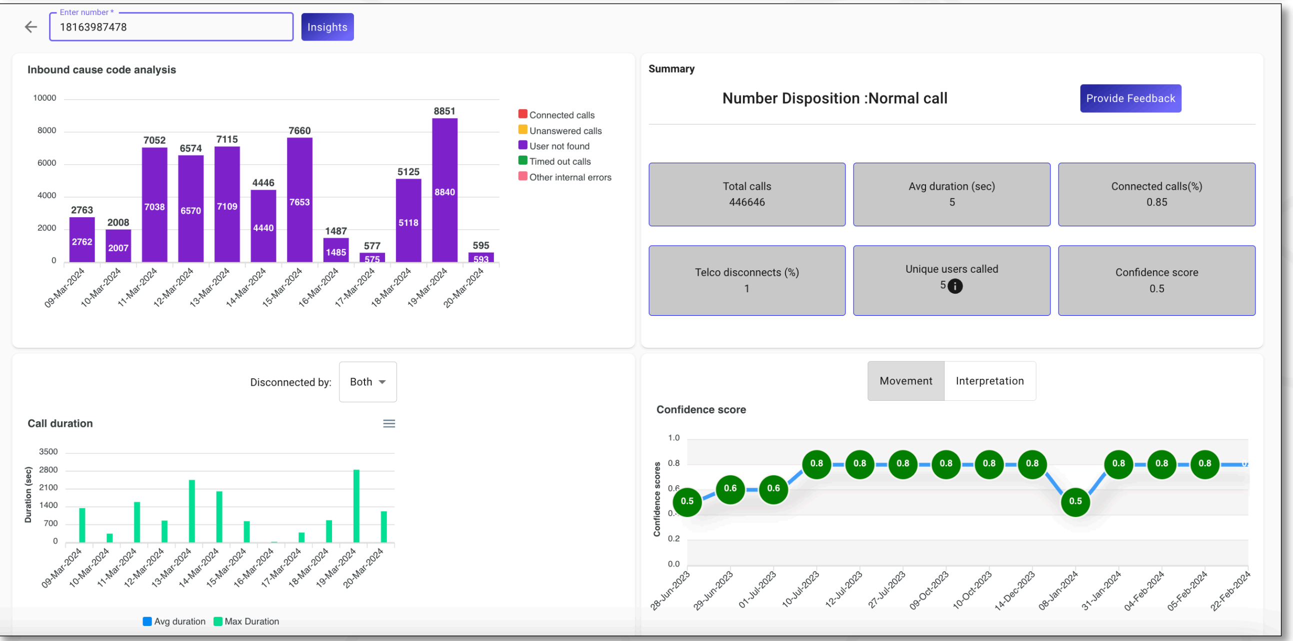
- Assertion Scanner supports geo-redundant HA
- Assertion Defender supports active-standby HA in the same site.
- Defender is never in the middle of media path (does not get RTP, ever). It redirects SIP INVITE using 3xx, 5xx or 6xx message.
- Defender does SIP keep alive with the SBC. If Defender fails or is slow to respond, SBC is configured to skip the Defender and move ahead with call processing.
- When Defender fails, there is no loss of call processing or delay in call processing.
- Defender is fast. It responds to each call within 10 milliseconds.
- It is highly scalable and can handle up to 500 calls / second / Defender node. Multiple Defender nodes can be stacked up, without any known limit.
- Threat intel is updated every minute to ensure best-in-class protection.
- The solution is vendor agnostic and uses RFC SIP signaling. Supports all major SBCs with no extra components.

Product Screens





Caller	Category	Total calls	Connected calls	Total duration (mins)	Avg call duration (mins)	Calls connected (%)
anonymous ⓘ	N.A	2741507	2287032	52901013.03	23.13	83.42
Anonymous ⓘ	N.A	8550	5125	14462.62	2.82	59.94
45555493419734666158 ⓘ	N.A	3952	0	0.00	0.00	0.00
Restricted ⓘ	N.A	1422	1118	6761.72	6.05	78.62
5552362334 ⓘ	N.A	411	7	116.65	16.66	1.70
5552362392 ⓘ	N.A	265	4	38.57	9.64	1.51
5552362144 ⓘ	N.A	185	1	0.00	0.00	0.54



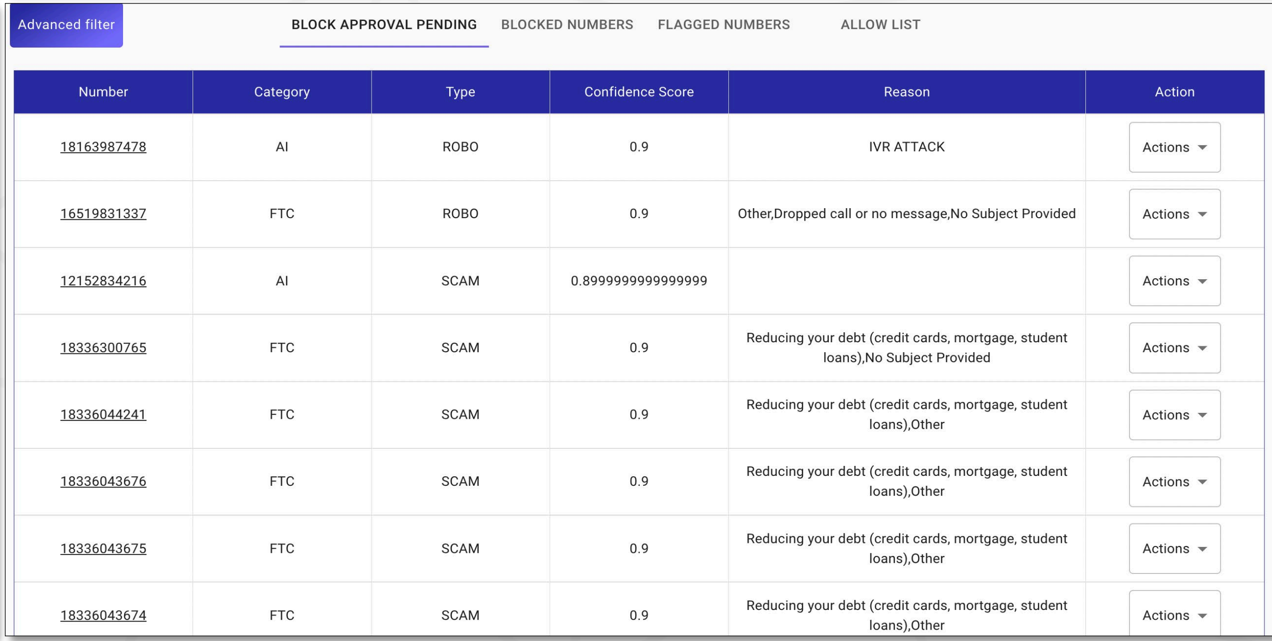
Enter number * 18163987478

Disconnected by: Both

Summary

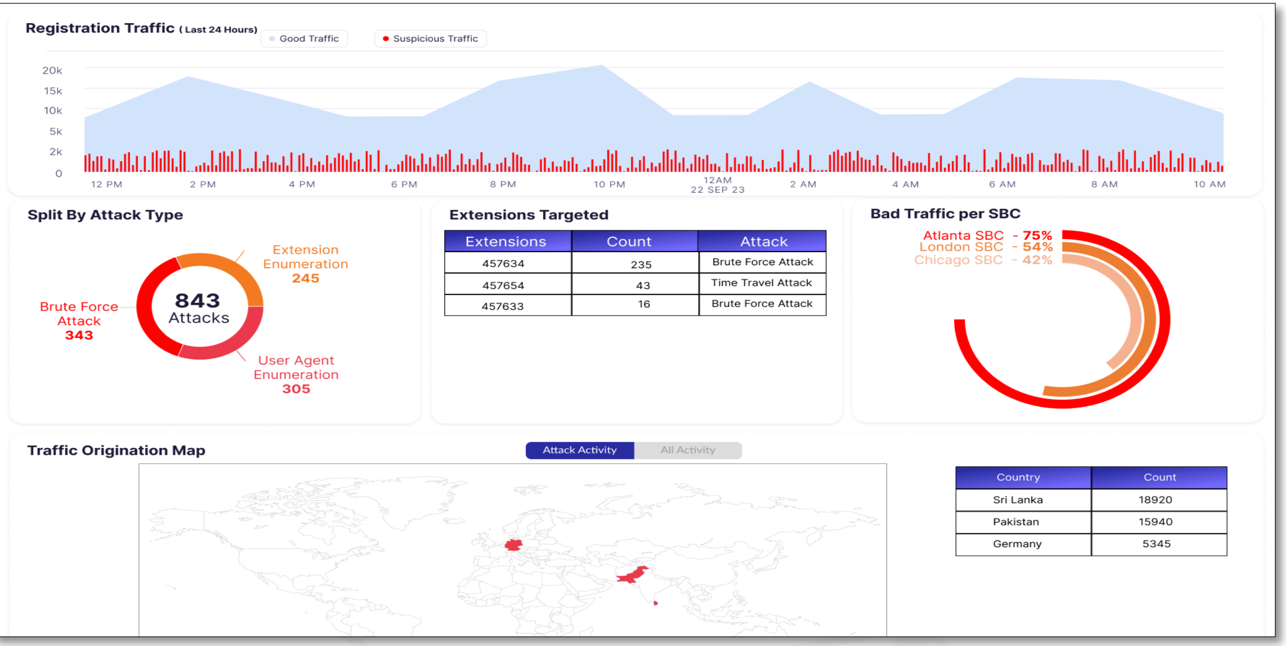
Number Disposition :Normal call

Total calls 446646	Avg duration (sec) 5	Connected calls(%) 0.85
Telco disconnects (%) 1	Unique users called 5	Confidence score 0.5



Number	Category	Type	Confidence Score	Reason	Action
18163987478	AI	ROBO	0.9	IVR ATTACK	Actions ▾
16519831337	FTC	ROBO	0.9	Other,Dropped call or no message,No Subject Provided	Actions ▾
12152834216	AI	SCAM	0.8999999999999999		Actions ▾
18336300765	FTC	SCAM	0.9	Reducing your debt (credit cards, mortgage, student loans),No Subject Provided	Actions ▾
18336044241	FTC	SCAM	0.9	Reducing your debt (credit cards, mortgage, student loans),Other	Actions ▾
18336043676	FTC	SCAM	0.9	Reducing your debt (credit cards, mortgage, student loans),Other	Actions ▾
18336043675	FTC	SCAM	0.9	Reducing your debt (credit cards, mortgage, student loans),Other	Actions ▾
18336043674	FTC	SCAM	0.9	Reducing your debt (credit cards, mortgage, student loans),Other	Actions ▾

Product Screens



Registration Traffic (Last 24 Hours)

Split By Attack Type

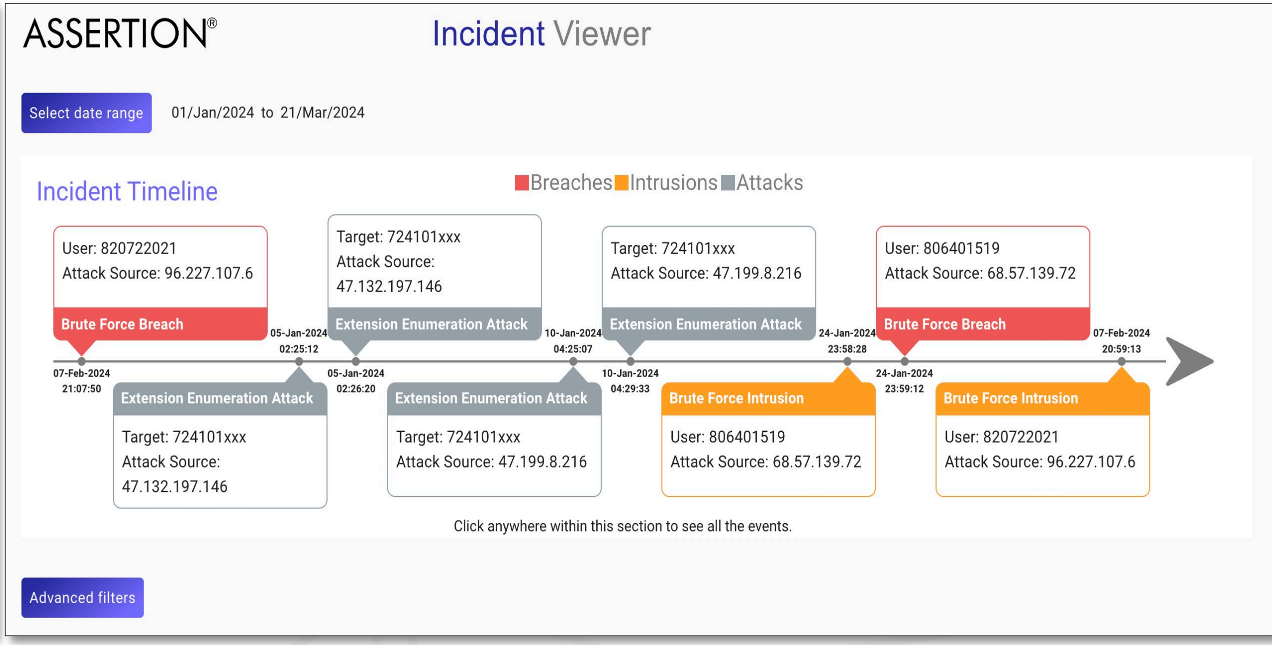
Extensions Targeted

Extensions	Count	Attack
457634	235	Brute Force Attack
457654	43	Time Travel Attack
457633	16	Brute Force Attack

Bad Traffic per SBC

Traffic Origination Map

Country	Count
Sri Lanka	18920
Pakistan	15940
Germany	5345



ASSERTION®

Incident Viewer

01/Jan/2024 to 21/Mar/2024

Incident Timeline

User: 820722021
Attack Source: 96.227.107.6
Brute Force Breach
07-Feb-2024
21:07:50

Extension Enumeration Attack
Target: 724101xxx
Attack Source:
47.132.197.146
05-Jan-2024
02:25:12

Target: 724101xxx
Attack Source:
47.132.197.146
Extension Enumeration Attack
05-Jan-2024
02:26:20

Extension Enumeration Attack
Target: 724101xxx
Attack Source: 47.199.8.216
10-Jan-2024
04:25:07

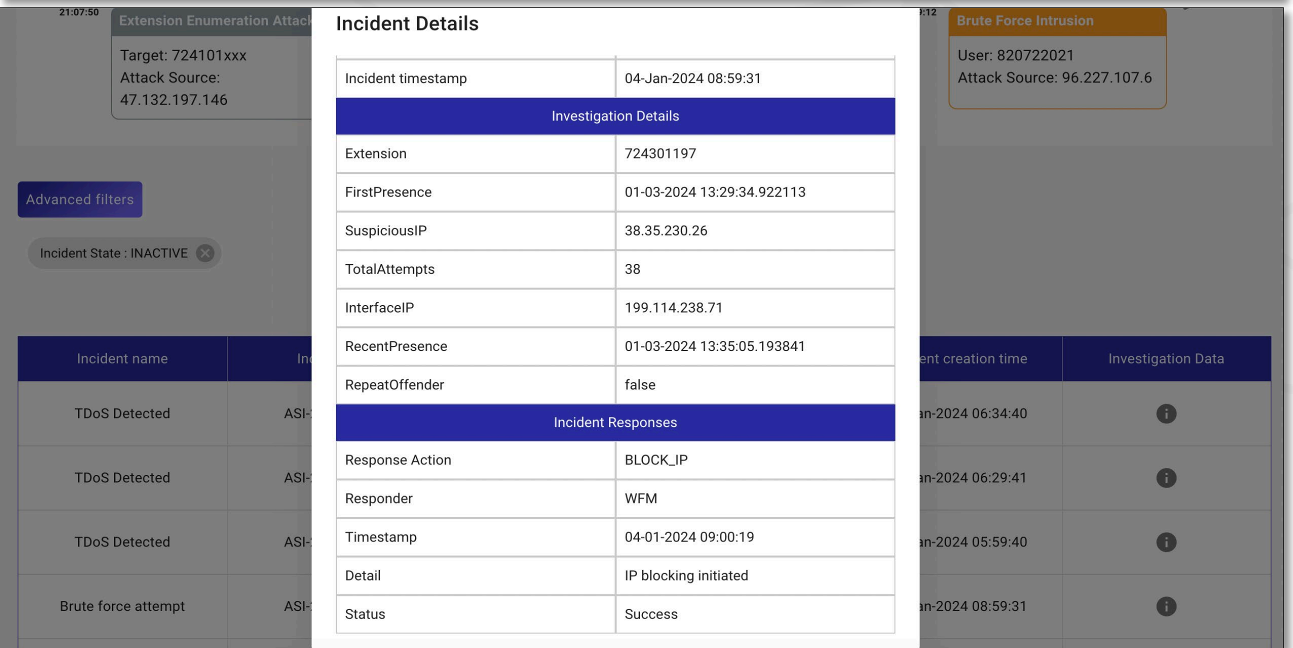
Target: 724101xxx
Attack Source: 47.199.8.216
Extension Enumeration Attack
10-Jan-2024
04:29:33

Brute Force Intrusion
User: 806401519
Attack Source: 68.57.139.72
24-Jan-2024
23:58:28

User: 806401519
Attack Source: 68.57.139.72
Brute Force Breach
24-Jan-2024
23:59:12

Brute Force Intrusion
User: 820722021
Attack Source: 96.227.107.6
07-Feb-2024
20:59:13

Click anywhere within this section to see all the events.



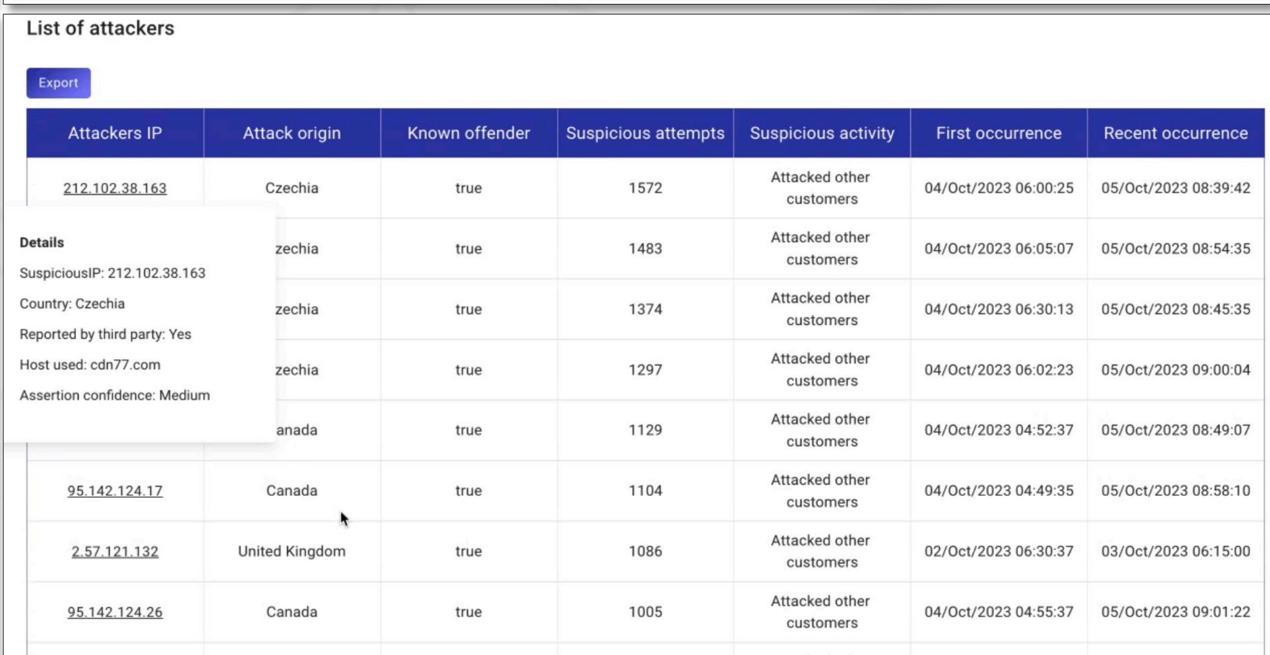
21:07:50
Extension Enumeration Attack
Target: 724101xxx
Attack Source:
47.132.197.146

:12
Brute Force Intrusion
User: 820722021
Attack Source: 96.227.107.6

Incident Details

Incident timestamp	04-Jan-2024 08:59:31
Investigation Details	
Extension	724301197
FirstPresence	01-03-2024 13:29:34.922113
SuspiciousIP	38.35.230.26
TotalAttempts	38
InterfaceIP	199.114.238.71
RecentPresence	01-03-2024 13:35:05.193841
RepeatOffender	false
Incident Responses	
Response Action	BLOCK_IP
Responder	WFM
Timestamp	04-01-2024 09:00:19
Detail	IP blocking initiated
Status	Success

Incident name	In	ent creation time	Investigation Data
TDoS Detected	ASI-	an-2024 06:34:40	i
TDoS Detected	ASI-	an-2024 06:29:41	i
TDoS Detected	ASI-	an-2024 05:59:40	i
Brute force attempt	ASI-	an-2024 08:59:31	i



List of attackers

Attackers IP	Attack origin	Known offender	Suspicious attempts	Suspicious activity	First occurrence	Recent occurrence
212.102.38.163	Czechia	true	1572	Attacked other customers	04/Oct/2023 06:00:25	05/Oct/2023 08:39:42
	zechia	true	1483	Attacked other customers	04/Oct/2023 06:05:07	05/Oct/2023 08:54:35
	zechia	true	1374	Attacked other customers	04/Oct/2023 06:30:13	05/Oct/2023 08:45:35
	zechia	true	1297	Attacked other customers	04/Oct/2023 06:02:23	05/Oct/2023 09:00:04
	anada	true	1129	Attacked other customers	04/Oct/2023 04:52:37	05/Oct/2023 08:49:07
95.142.124.17	Canada	true	1104	Attacked other customers	04/Oct/2023 04:49:35	05/Oct/2023 08:58:10
2.57.121.132	United Kingdom	true	1086	Attacked other customers	02/Oct/2023 06:30:37	03/Oct/2023 06:15:00
95.142.124.26	Canada	true	1005	Attacked other customers	04/Oct/2023 04:55:37	05/Oct/2023 09:01:22

Details

SuspiciousIP: 212.102.38.163
Country: Czechia
Reported by third party: Yes
Host used: cdn77.com
Assertion confidence: Medium

Hardware, Software and Network requirements

- Minimum 2 VMs - 1 Scanner and 1 Defender
- Assertion® Scanner has the following requirements:
    - Hardware requirements – VM with 8GB RAM, 4 vCPU * 2.2GHz, free disk space of 150 GB.
    - Software requirements – OVA provided with RHEL 8.x/9.x. Customer to provide license.
    - Network – 2 NIC cards, 1Gbps
- Assertion® Defender has the following requirements:
    - Hardware requirements – VM with 8GB RAM, 4 vCPU * 2.2GHz, free disk space of 150 GB.
    - Software requirements – OVA provided with RHEL 8.x/9.x. Customer to provide license.
    - Network – 2 NIC cards, 1Gbps

Pre-requisites and Implementation Process

Compatibility matrix

SBC Vendor	Version Supported
Avaya SBC	8.x, 10.x
AudioCodes SBC	7.2+
Oracle SBC	7.2.x, 7.4.x, 8.x
Ribbon SBC	10.x, 11.x for SBC SWe Lite, SBC 1K, SBC 2K
Cisco Cube	14.x+

PoC / Trial offer

We offer a 30-day Proof of Concept (PoC) for Assertion Secure Voice tailored to meet your business needs!

Opt for a no obligation PoC to test the system in your environment. Purchase only if the PoC is successful. This flexible approach allows you to experience the value of Assertion Secure Voice with confidence.

Competitive Analysis against Mutare & SecureLogix

Incoming Call Security	Assertion	Competition
AI/ML based scam call detection	✓	✓
Route / Block suspicious calls to specific numbers / agent based on dynamic reputation score	✓	✓
Scam call flagging with custom display update	✓	X
Fine grained control of the AI using 20+ levers	✓	X
Continuous learning using user feedback via agent disposition or admin portal	✓	X
Outgoing Call Security		
Block calls to premium rate numbers (toll fraud attempts)	✓	✓
Enforce DNC list, Sanctioned call barring (OFAC) and Geo-fencing	✓	✓
Block outbound calls based on state / local calling regulations	✓	X
Block calls to unfamiliar / suspicious numbers	✓	X

SIP Remote Worker Security	Assertion	Competition
Detect and block cyber attacks in real-time	✓	X
Continuously adapt your security posture to the threats (configurations)	✓	X
Geo-fencing of remote workers to specific countries	✓	X
Block calling permissions of compromised extensions	✓	X
Automated blocking of attacker IP (workflow)	✓	X
Unique Features	**Assertion**	**Competition**
Get AI powered insights about every caller	✓	X
Solve business problems with custom automation – e.g. detecting calls from CMS.gov auditors and informing agents	✓	X
CC process-wise & campaign-wise reporting	✓	X
Local ANI on outgoing calls	✓	X

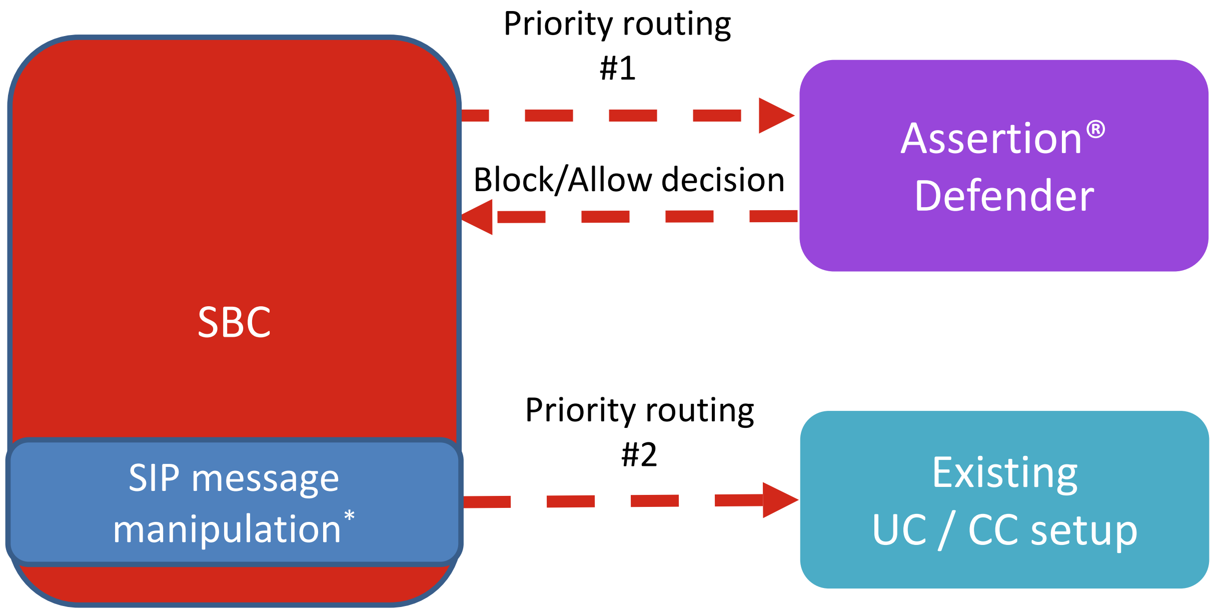
ASSERTION®
a voice security company

Thank you

Contact us today to discover how Assertion's innovative solutions can elevate your technology infrastructure and meet your evolving needs.

Defender call flow

Add Defender as the first routing point on all internal routes, pushing down the priority of existing destinations.



*SIP message manipulation rule is done to update the display that is presented to the endpoint. This is done based on the call reputation.

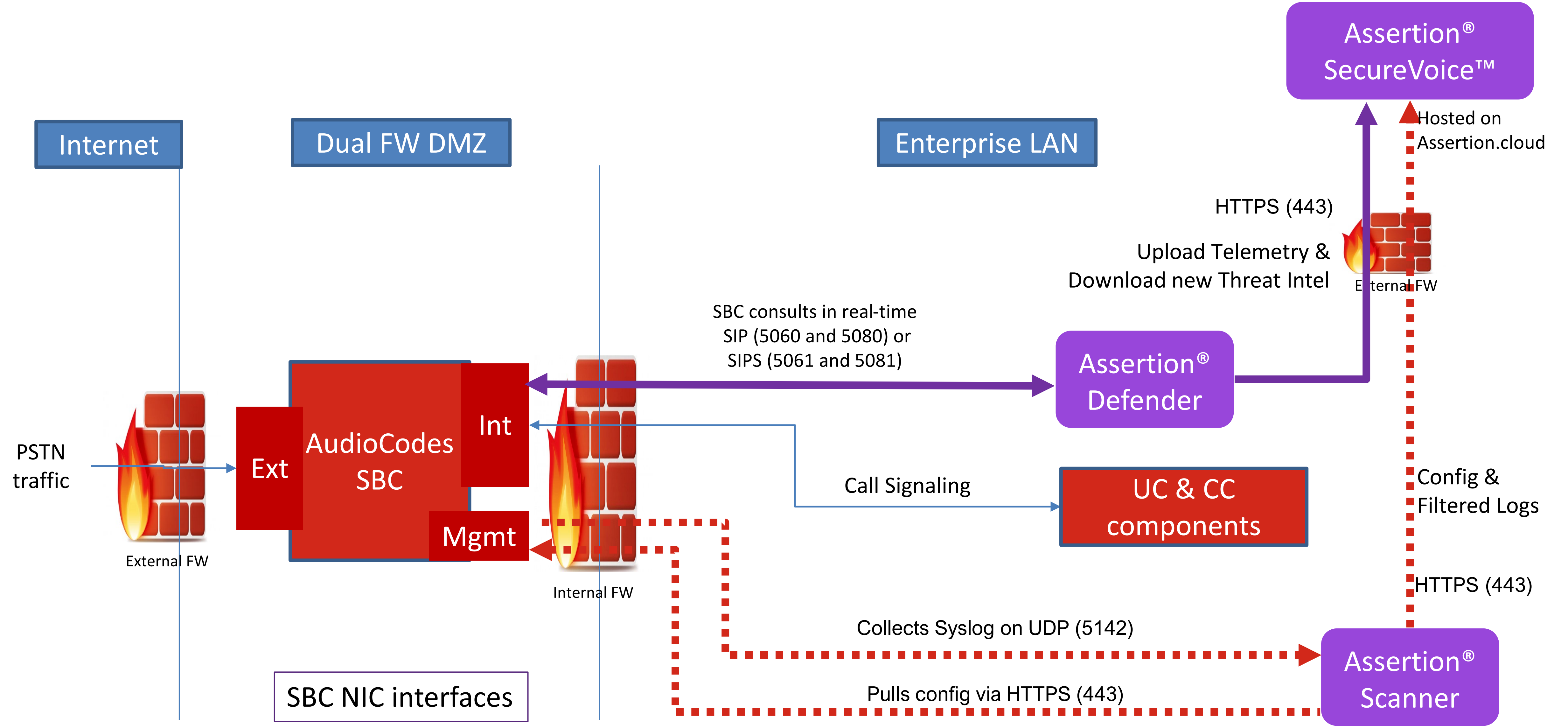
Defender response codes:

502 For allowed calls, Defender uses the failover routing capability of the SBC to move the call to the next hop (UC / CC setup).

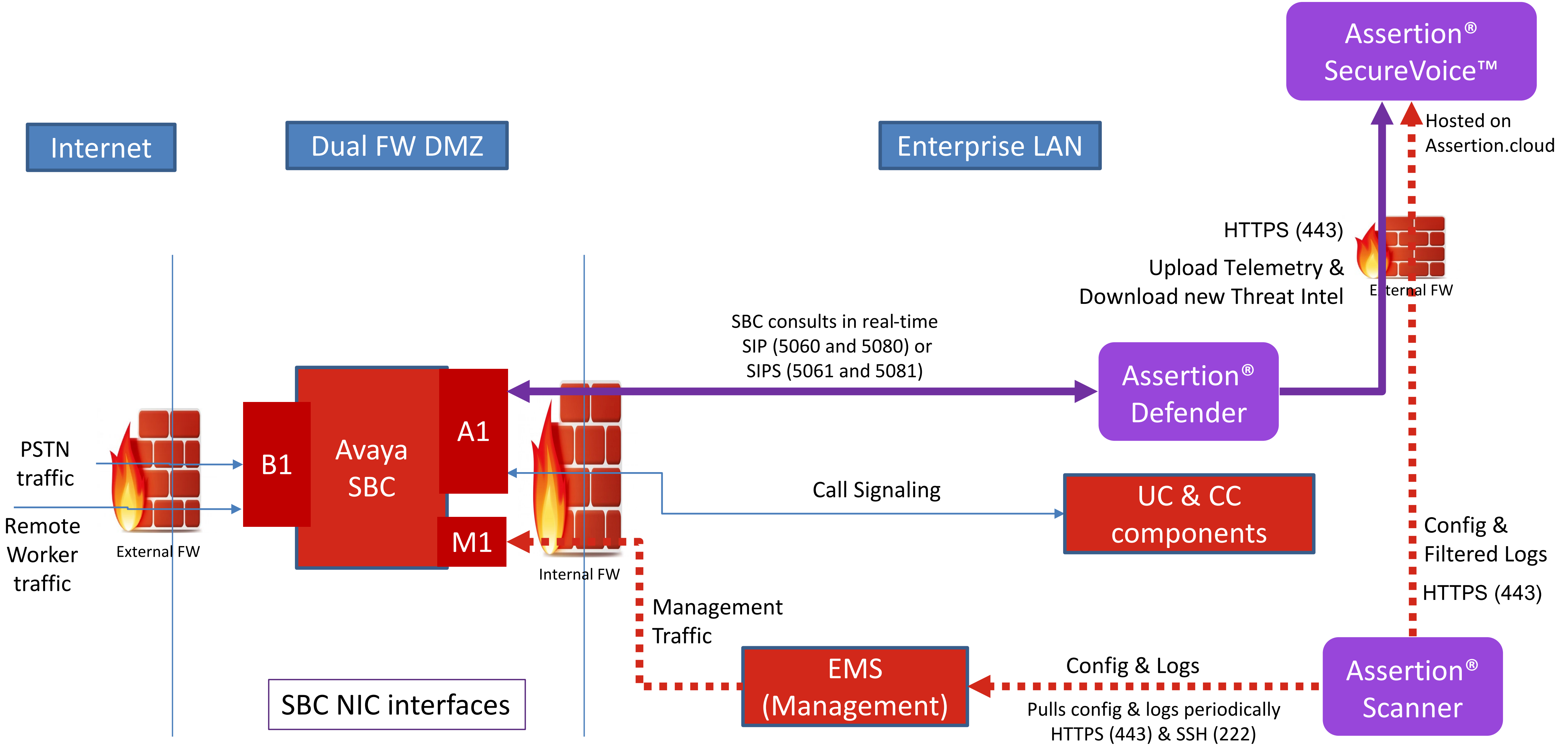
302 For calls that need to be flagged, Defender uses the 302 handling capability of the SBC to move the call to the next hop (UC / CC setup).

603 For calls that need to be blocked, Defender returns 603 so that SBC can reject the call.

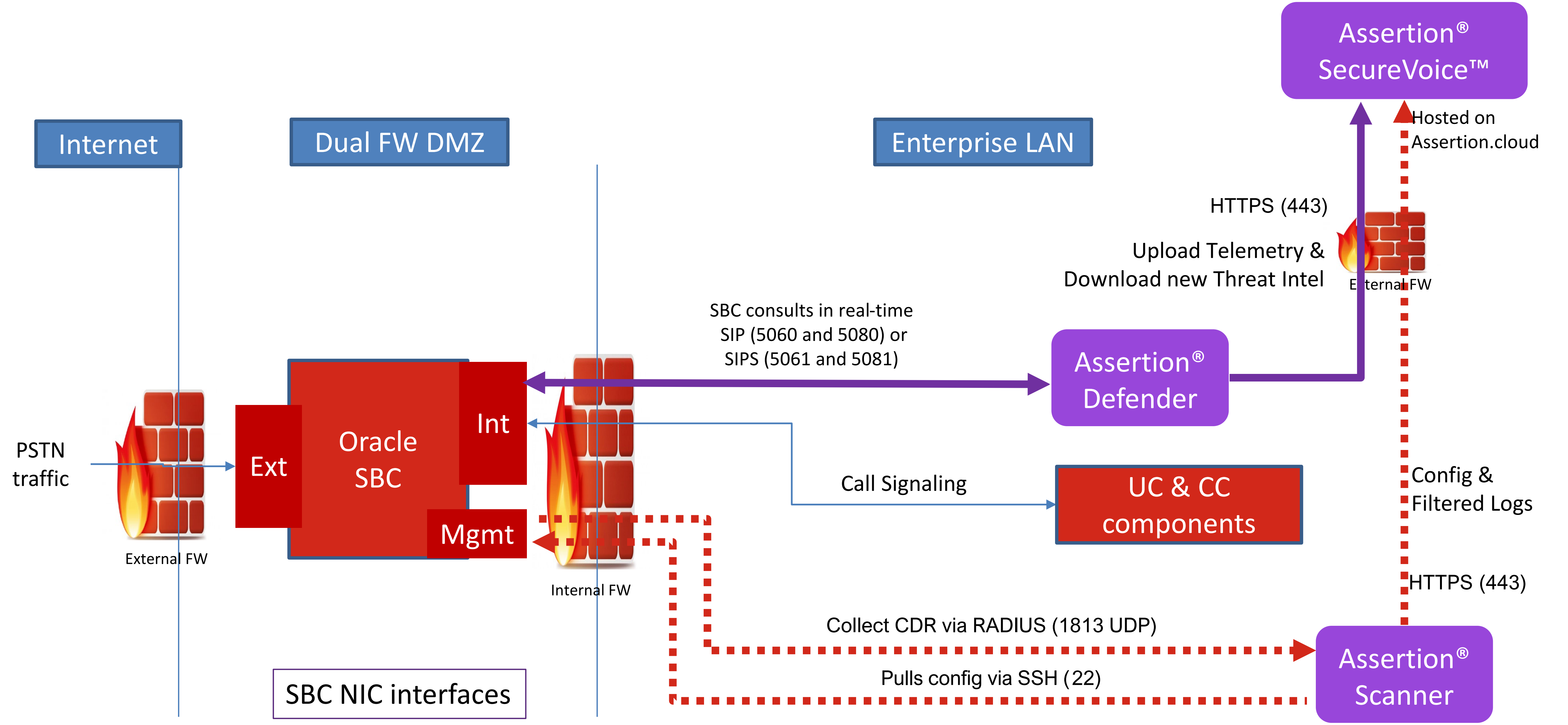
Deployment and Connectivity – Audiocodes onPrem (recommended)



Deployment and Connectivity – Avaya onPrem (recommended)



Deployment and Connectivity – Oracle onPrem (recommended)


Assertion® SecureVoice™
Hosted on Assertion.cloud
Internet
Dual FW DMZ
Enterprise LAN
HTTPS (443)
Upload Telemetry & Download new Threat Intel
External FW
SBC consults in real-time SIP (5060 and 5080) or SIPS (5061 and 5081)
Assertion® Defender
Int
Oracle SBC
Ext
PSTN traffic
Call Signaling
UC & CC components
Config & Filtered Logs
Mgmt
External FW
Internal FW
HTTPS (443)
Collect CDR via RADIUS (1813 UDP)
Pulls config via SSH (22)
Assertion® Scanner
SBC NIC interfaces