Secure Real-Time
Communications

ribbon

Secure SBC Deployment Guide

Deployment Guide

Document Overview

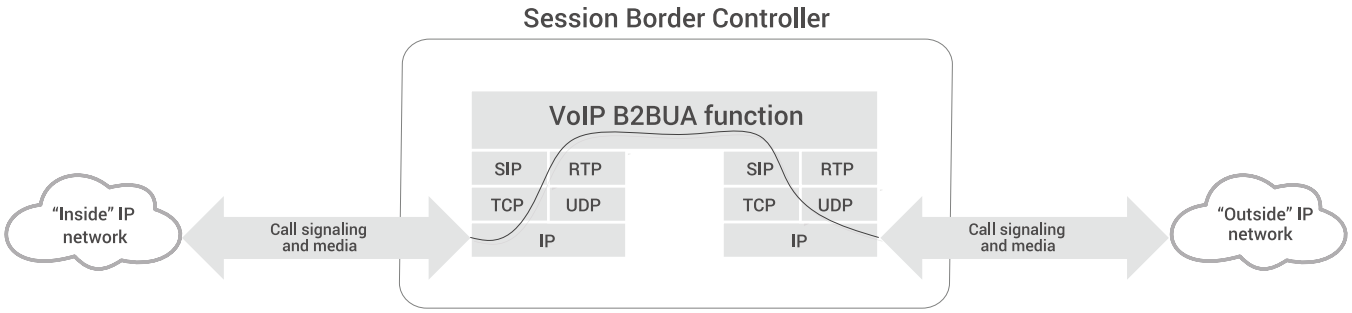
This document is for customers interested in deploying Ribbon Communications Session Border Controller (SBC) products. Prior knowledge of these Ribbon products is not required; however, general knowledge of IP networking, Voice over IP, and network security will help understand this material.
The document explains what SBCs are and where they are deployed, introduces the Ribbon SBC products, and describes the security protections that SBCs (and Ribbon SBC products) can provide.

What is an SBC?

"SBC" is an acronym for Session Border Controller. An SBC is a network device, typically deployed at the border of an administrative domain of a network to control certain types of network traffic. In particular, an SBC concerns itself with network traffic implementing session-oriented multimedia communications such as Voice over IP (VoIP). More succinctly, **a Session Border Controller sits at the border of a network domain and controls the flow of session-oriented traffic.**

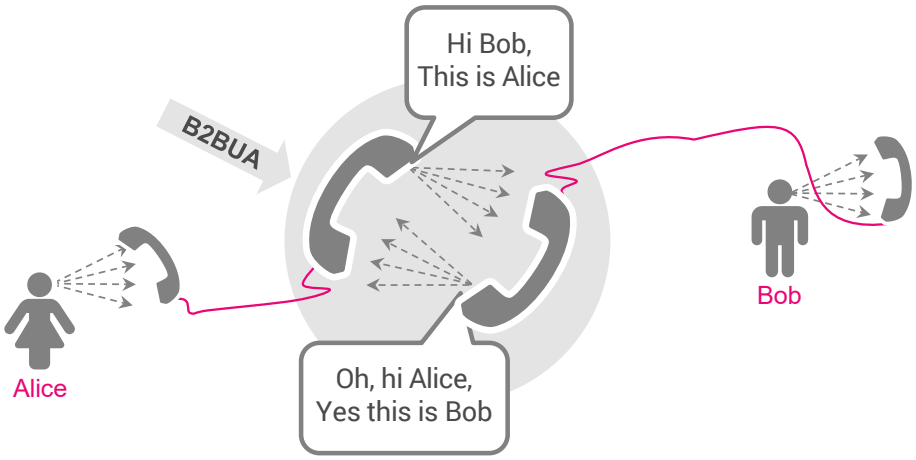
SBCs perform many essential functions aimed at enabling and enhancing multimedia communications. These functions include security, signaling protocol repair and interworking (such as IPv4 to IPv6 interworking), media transcoding, lawful intercept, and more. This particular document focuses on the security aspects.

The security functions of an SBC concerning VoIP traffic conceptually parallel those of a firewall for IP traffic. More specifically, the SBC's behavior is comparable to that of a proxy firewall – it terminates certain network protocol sessions. It then propagates the information carried therein onto corresponding sessions on the other side. In an SBC, the term Back to Back User Agent (B2BUA) is used to describe this structure, illustrated below. This fundamental approach underlies many of the security functions of the SBC by imposing a "permit what is understood and block the rest" architecture on the device.



Controlled relay of call signaling and media by an SBC acting as a Back-to-back User Agent

A more concrete, if whimsical, view of the B2BUA concept is that it connects two legs of a call with an "air gap" after the manner of two phones held together. In the VoIP world, a "UA" is a phone, and so a back-to-back UA is like a back-to-back pair of phones:



In addition to controlled relaying (or blocking) of the signaling and media information, an SBC may adjust the content, such as filtering SIP headers or transcoding the audio. Some SBCs can also provide more sophisticated services such as call routing.

The SBC B2BUA behavior happens at layer 5 of the protocol stack. From an IP perspective, an SBC is a network host; SBCs do not forward IP datagrams. Only the content of specifically selected signaling protocols (typically SIP) and media protocols (typically RTP) can be propagated by the SBC.

A Primer on Distributed Denial-Of-Service

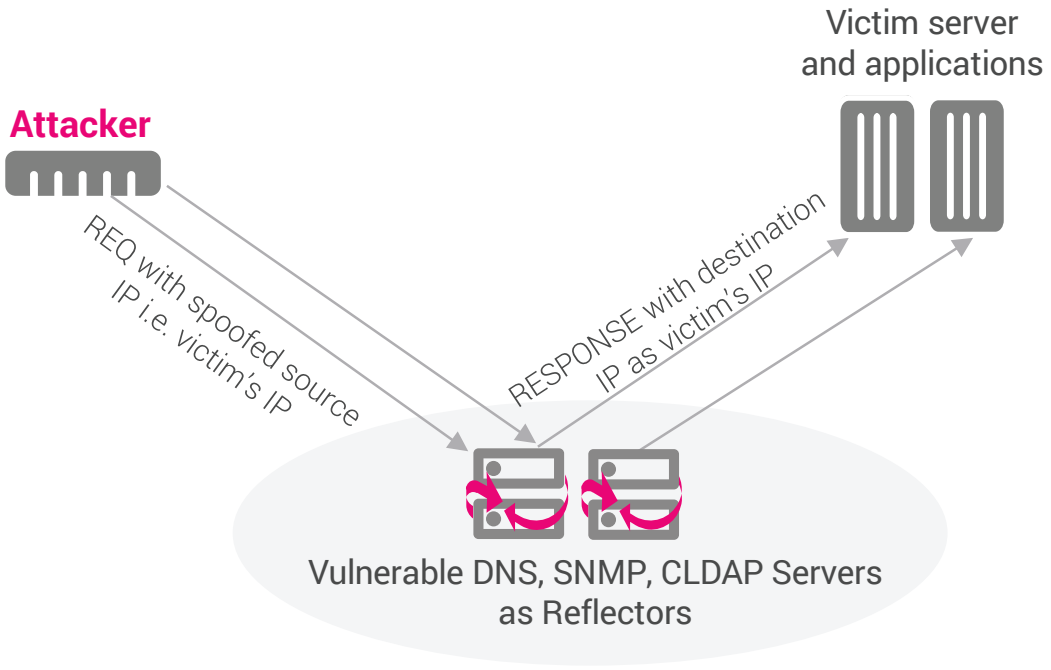
The focus of this section is to cover Denial-of-Service basic concepts, and to provide a brief description of distributed Reflective DOS attacks. There are plenty of educational material available on the internet for readers who are interested in learning about DDOS.

A Denial-of-Service DOS is a deliberate attempt by an individual or a group, referred to as attackers, to make services unavailable for legitimate users. An attack vector is a method or a scenario for conducting attacks on infrastructure and applications. A DNS reflection is an example of an attack vector. The attack surface area is the sum of all the exposed points of a target system through which an attacker can conduct DOS against the said system. An attacker uses a combination of attack vectors that exploit the attack surface; the larger the surface area, the more vulnerable the system is.

Here are a few key types of attack.

- Volumetric attacks that primarily target the depletion of available network bandwidth and compute resources for legitimate users. The most common type of volumetric attack is the ICMP flood and DNS, CLDAP, Memcached Reflections.
- The protocol-based attack targets to deplete the compute resources available on a server. The most well-known Protocol based attack is the SYN Flood, which causes a TCP server-side implementation to have many TCP connections in half-open states.

- Application Layer attacks target to take down the application by exploiting the weakness in the implementation. Attacks conducted using high volume of malformed PDU or malformed SIP Call flows are examples of Application Layer attacks.



Distributed Reflective Volumetric DOS

The diagram above describes the mechanics of a Distributed Reflective DOS. The attacker uses the spoofed IP as the source address in DNS, SNMPv2, CLDAP etc. Request messages to a server using UDP as the transport. The server sends the Responses, which many times larger than the Request to the victim. The ratio of the Response to the Request sizes is known as the Amplification factor. UDP-based Amplification attack on the network infrastructure has these properties.

- Response messages are much bigger than Request payload; Bandwidth Amplification Factor can range from single digit (e.g., SNMPv2) to hundreds of thousands (e.g., Memcached)
- Employs multiple attack vectors (e.g., combination of SNMPv2, DNS, CLDAP reflections etc.)
- Reflectors are trusted publicly accessible UDP servers and attacker could use thousands of reflectors.
- Identity of the attacker is concealed making it harder to blacklist.
- TCP is rarely used

Ribbon SBCs defend against these attacks and refer to Appendix A for details.

Ribbon Core Session Border Controller Portfolio

The Ribbon Core Session Border Controller (SBC) product portfolio includes two hardware-based options - SBC 5400 and SBC 7000 and the software-only option - Software Edition (SWe). The SBC SWe is a virtual SBC architected to enable and secure real-time communications in multiple virtual and private or public clouds. The SBC SWe features the same code base, resiliency, media processing, and security technology found in Ribbon's SBC 5400 and SBC 7000 appliances, adapted for resilient and efficient deployment in virtual and cloud environments.

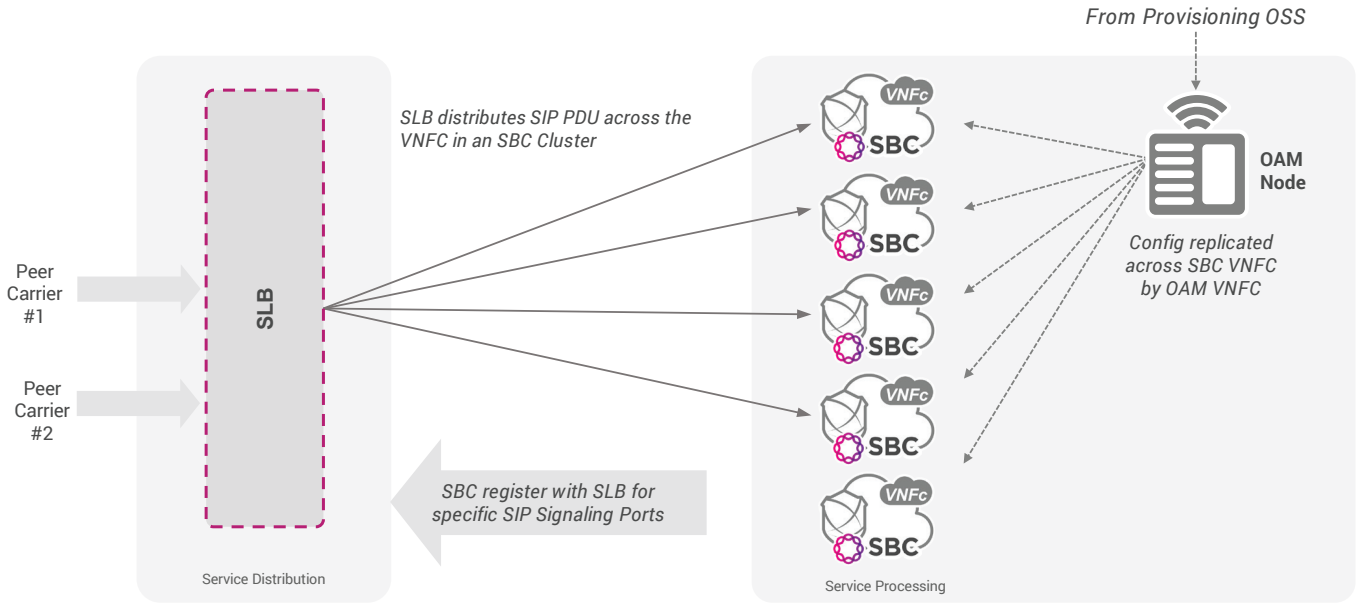
SBC Core Portfolio Shares a Common Software Base

When deploying the SBC Swe as a Virtual Network Function (VNF) on Virtual Machines (VMs) there is a practical capacity limitation for a single SBC instance. To address this, Ribbon's Core SBC portfolio also includes a session aware load balancer.

Session-aware Load Balancer (SLB)

Where the capacity required goes above that possible from one SBC instance, the Session-aware Load Balancer (SLB) can be introduced to maintain a single logical SBC for signaling, which distributes sessions evenly across multiple SBC instances delivering a call throughout up to 8,000 CPS.

The SLB is instantiated from the same software image as the SBC and is instructed to operate as an SLB, rather than as another SBC. **The SLB includes the main SBC security functions** integrated with the SBC for load distribution across the cluster of SBC instances.



SBC VNF with SIP-aware Load Balancer (SLB)

The SLB is implemented as a 1+1 HA pair that provide a service distribution layer in front of the cluster of N+1 SBC instances providing the service processing layer.
All SBCs in a cluster can serve the same set of SIP signalling ports (IP addresses), allowing the SLB to distribute traffic evenly across SBCs in the cluster. There is a feedback mechanism between the SLB and each SBC, so that traffic can be distributed evenly, taking into account of congestion or overload on any of the SBC. If an SBC rejects an INVITE, the SLB re-routes the INVITE to another SBC in the cluster.
The SLB has a consistently up to date view of the SBC in service because each SBC registers with the SLB when it is instantiated (either for scale-out events or when performing other lifecycle functions)

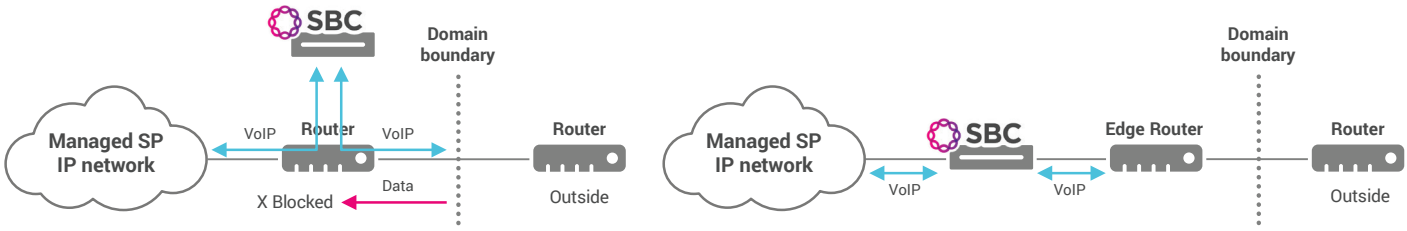
Deploying the Ribbon SBC

The Ribbon SBC is designed with suitable hardening to be deployed directly on unmanaged, “untrusted” networks such as the Internet. Most service providers deploying the SBC facing an untrusted network do indeed deploy it with its outward-facing network interfaces connected to that network, without a firewall (but typically with routers and switches in the path, for non-security reasons).

Service Provider Deployments

Different arrangements may be used at the service provider domain boundary to ensure that VoIP/multimedia traffic must traverse the SBC and that other traffic is blocked outright. Two such arrangements are shown below.

With the DMZ host model (left), a service provider’s edge router is configured to divert all incoming VoIP traffic to the SBC. With the more popular bastion host model (right), use of separate inside and outside network interfaces on the SBC ensures that VoIP traffic physically cannot enter the managed network without traversing the SBC. (In both models other non-VoIP types of traffic are blocked or directed to other appropriate handling.)

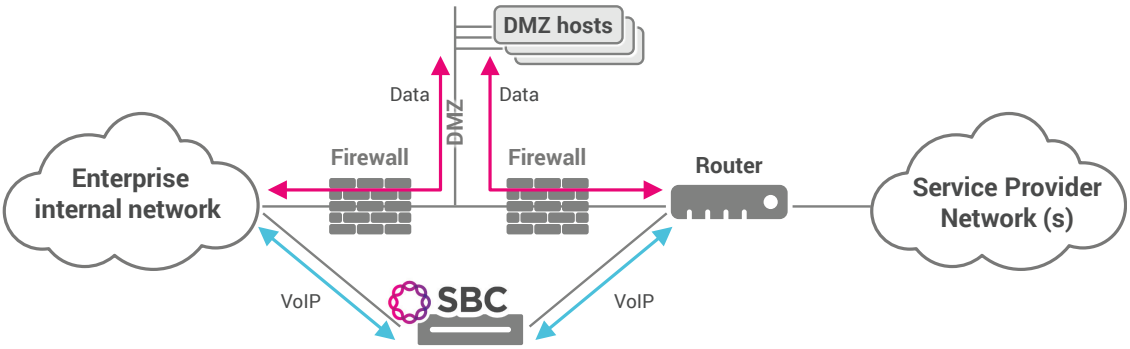


SP domain edge with SBC as a DMZ host

SP domain edge with SBC as a dual-homed bastion host

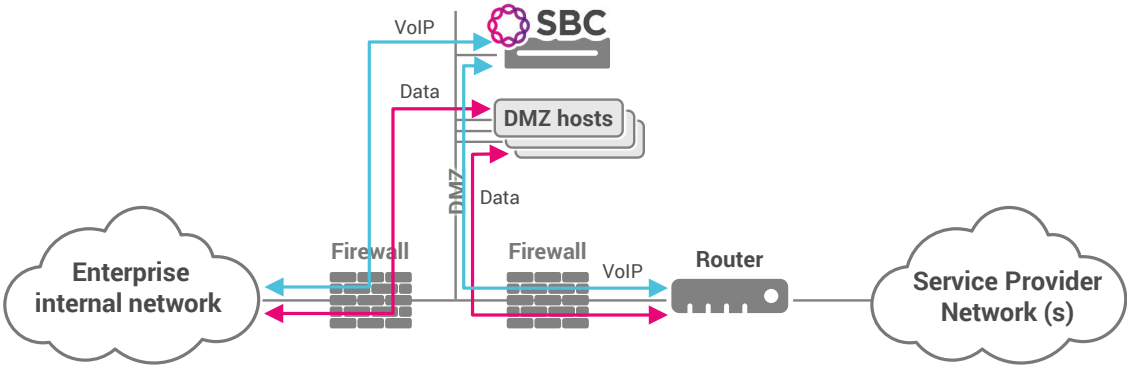
Enterprise Deployments

For enterprise scenarios some common arrangements are shown below. One approach is to position the SBC as a separate path between the protected and unprotected networks. The familiar firewall-DMZ-firewall path is used for data and a separate SBC path is used for VoIP. With this approach, the firewalls do not need to handle the VoIP traffic, alleviating some capacity and functional requirements for the firewalls:



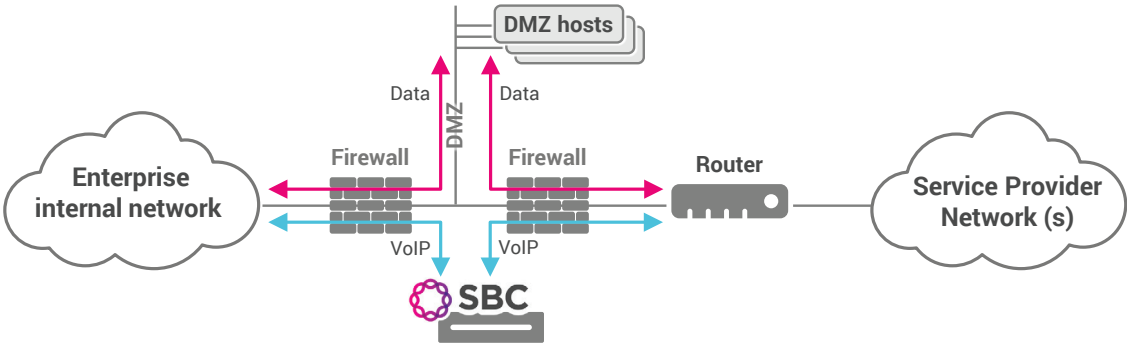
Enterprise edge with separate data and VoIP paths

Another enterprise approach is to deploy an SBC in the data DMZ, alongside the other DMZ hosts. The approach adds some security since more security boxes are in the VoIP path. But it comes at a cost: The firewalls must have additional bandwidth capacity to carry all the VoIP traffic. Also, the firewalls must either have the (rare and possibly fragile) functional capability to monitor the SIP signaling and dynamically open and close UDP pinholes for the RTP traffic flows, or the firewalls must be configured to statically open a wide range of UDP ports to and from the SBC.



Enterprise edge with integrated data and VoIP paths

A variation on this last approach is to deploy the SBC as a dual-homed device within the DMZ. This impacts similarly on the firewall requirements but allows for a bit finer control at the SBC:



Enterprise edge with integrated data and VoIP paths, dual-homed SBC

Note: SBCs are almost always deployed in High Availability configurations, with redundant SBC equipment as well as redundant surrounding network plumbing. Because the focus of this paper is security and not reliability, these details have been omitted here.

Ribbon SBC Security Mechanisms

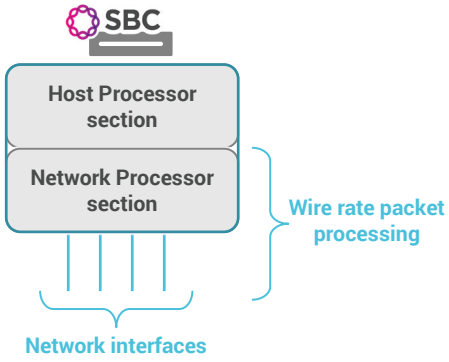
The high-level security goals of the SBC are to:

- Protect the availability and integrity of the SBC itself.
- Protect the managed network behind the SBC.
- Provide confidentiality and integrity protection services for the served VoIP and multimedia traffic.

The SBC achieves these goals through some fundamental architectural elements and a rich set of VoIP security features. The subsections following give brief overviews of the major aspects of the SBC that contribute to ensuring that the above security goals are met.

Specialized System Architecture

The system architecture of the SBC features a host processor portion and a network processor portion. The host processor is optimized for executing sophisticated software and is where the system management and call signaling functions are implemented. The network processor is optimized for very high-rate processing of network packets. Specifically, the network processor section can receive packets at wire rate on all network interfaces, recognizing and controlling those that are part of expected flows, and safely discarding the rest.



The SBC architecture consists of optimized host processor and network processor sections

The network processor portion is implemented using specialized hardware for SBC 5400 and SBC 7000 and using Intel DPDK technology for SBC SWe. The Network Processor is a key component of the DoS attack resistance of the SBC.

B2BUA Software Architecture

The Back-to-Back User Agent structure of the SBC has been introduced above. The fundamental security benefit of the B2BUA architecture is that it creates a "default deny" foundation for the device:

- IP packets are never forwarded by the SBC.
- Unrecognized protocols are always ignored.
- Media streams that are not associated with signaled sessions are blocked.

With the B2BUA model information forwarding from one interface to another happens only at the application layer. The B2BUA application completely terminates signaling and media transport connections on one side and relays certain of the received information onto new transport connections on another interface. Received information is parsed, filtered, limited, and selectively regenerated out the new interface. Messages with invalid syntax or seeking to use unauthorized services or capacity are discarded. In this way propagation of attacks from the outside to the inside domain is prevented.

Another effect of the B2BUA model is topology hiding. Because signaling and media messages are decapsulated on one side of the SBC and re-encapsulated on the other, the IP addresses and port numbers in the encapsulation are different on one side than the other. To complete the topology hiding capability the SBC can be configured to remove IP addresses pertinent to one side of the SBC from the SIP headers that are transmitted on the other side.

Wire Rate DoS Flood Protection

The SBC implements powerful capabilities to defend against packet flooding Denial of Service (DoS) attacks. All incoming IP packets are matched against either:

- IP 5-tuples of established communication flows with known signaling or media peers
- ACL (Access Control List) rules defining expected signaling packet flows

Packets that are so matched are considered expected but are rate limited to defend against abuse by known peers, or by attackers impersonating known peers. The imposed rate limits will not affect normal traffic but protect the system in the event of excessive incoming traffic. Received packets that do not turn up a match are discarded. All this can be done at whatever rate packets are received, up to full wire rate on all network interfaces.

The system keeps count of packets discarded by these DoS protection mechanisms and will automatically raise a security alarm if the rate of packet discards within any of several categories exceeds a set threshold.

IP Packet ACLs

The system has a configurable capability to filter arriving packets. SBC supports flexible rules that can match any combination of IP 5-tuple and incoming IP interface or interface group. Packets matching a rule may be accepted or discarded. This is very similar to the Access Control List features found in many popular routers, although the SBC adds an extra twist – rules that specify accepting packets can apply a rate limit simultaneously. E.g. a rule may permit packets arriving from a specified peer and addressed to a SIP signaling port of the SBC but allow only up to 100 such packets per second. Packets received more than the provisioned rate are counted and discarded.

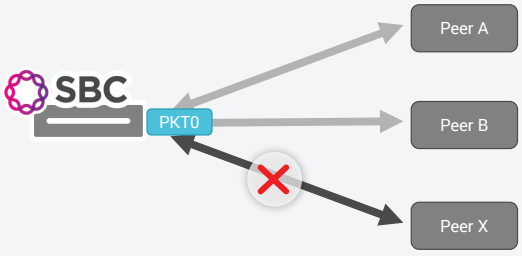
The IP ACLs are configurable, but the system automatically populates a default set of rules to ease product installation. One such rule, called SIP Unknown Peer IPACL, is automatically installed when the SIP signaling port is created on the SBC. The SIP Unknown Peer IPACL admits packets from any remote IP and port if the destination IP matches the SBC SIP IP address.

Although the default rules may be sufficient for many deployments, SBC operators are encouraged to examine these rules and augment them as appropriate for their specific network.

Ribbon recommends setting up the IPACL rule(s) for each SIP Trunk Remote Peer in Carrier Peering and Enterprise Access deployment scenarios as a Security Best Practice guideline to admit IP packets only from the known SIP peering gateways. The use of SIP Unknown Peer IP ACL in these deployments is discouraged. The operator can override the system installed SIP unknown peer IPACLs by configuring a "deny-all" rule to block packets from non-whitelisted sources to **reduce the DDOS attack surface significantly.**

Refer to Ribbon's Core SBC IP Access Control List CLI Documentation for details on setting up IPACL rules for both HW and virtual SBC.

The following example illustrates how to override SIP Unknown Peer IP ACL



Carrier Peering Deployment

IP ACL Rules by Precedence

User Rule 1, Precedence 1: action: allow, match on Peer - A as source IP, SBC SIP IP as destination IP, Interface: PKT0
User Rule 2, Precedence 2: action: allow, match on Peer - B as source IP, SB IP as destination IP, Interface: PKT0

User Rule 3, Precedence 3: action: discard, source and destination wild-carded, interface: PKT0

Rule 4, Precedence 1000 (system installed SIP Unknown Peer IP ACL): action: allow, match on SBC SIP IP as destination IP, any source address, interface: PKT0

An incoming IP packet could match more than one IP ACL rule. SBC uses the associated precedence value in case of multiple matches to select the rule and associated policy to be applied to the packet. The lower precedence value represents a higher priority.

In this example, the operator installs three rules, two allow-list IP ACLs (Rule 1 and 2) for Peer-A and Peer-B, and a deny-all for PKT0 interface. The user installed IP ACLs have higher priority than the system installed rules e.g., SIP Unknown IPACL rule. The IP ACLs for Peer-A and B have higher priority than the deny-all rule. Note that the deny-all rule has a higher priority than SIP Unknown IP ACL rule.

The SBC admits packets from peer-A and B by applying Rule1 and 2, respectively. The IP packets from peer-X match rule-3, the user-installed deny-all rule for PKT0 interface, and rule-4, system-installed SIP unknown peer IP ACL rule. SBC selects rule-3 as it has lower precedence than the one associated with rule-4 and drops all the packets from Peer-X. To admit traffic from Peer-X, the operator must install an IPACL rule using the Peer-X's SIP IP address(es).

Note, SBC performs IPACL lookup and applies the associated policer to non-media e.g., non-RTP/RTCP packets.

Dynamic Block-Listing DBL

Dynamic Block-Listing functionality deploys deny rules in reaction to an event and then removes the blocking policy after a certain period. The event could be the number of malformed PDUs from an endpoint exceeding a threshold in the desired user-defined time window. The DBL functionality allows users to configure the criteria that when matches trigger an automatic blocking rule. The DBL functionality allows the operator to configure actions other than blocking packets from a misbehaving endpoint, e.g., rejecting all SIP requests with 404. The DBL rules take a higher priority than user-defined allow-lists.

Ribbon recommends that a network operator set up a DBL profile on the untrusted side to detect malformed PDUs and block all traffic from offending sources. This serves as a deterrent to DOS induced by malformed PDU. Please refer to Core SBC Enhanced DBL Profile CLI documentation for more information.

Note, SBC applies DBL policy to non-media packets. The DBL rules take a higher priority than the operator-installed IPACL rules. For example, the DBL rule can override an allow rule established by the user for a peer.

Microflow Policing

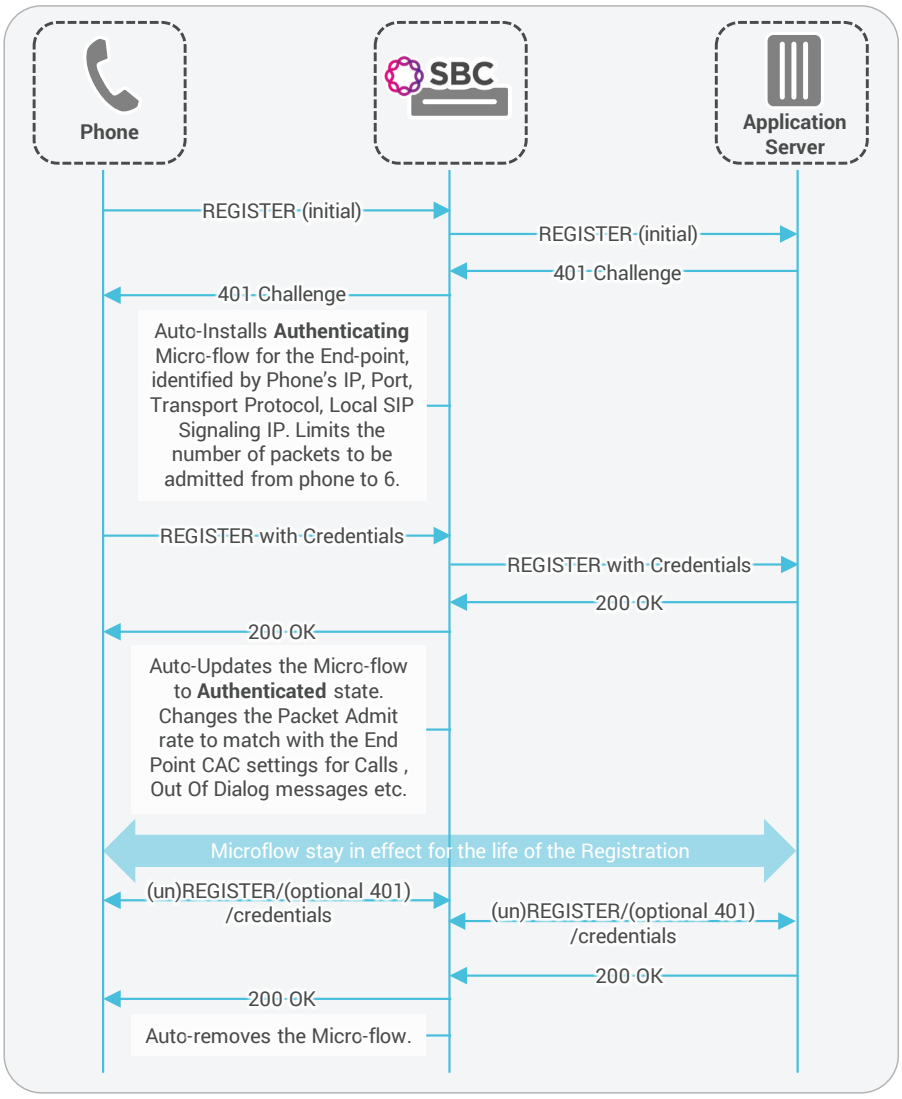
A microflow is defined as a single application-to-application packet flow typically characterized by endpoint IP addresses, next layer protocol, and transport-layer port numbers. Within SBC, a Microflow is identified by the following set of keys:

- Local SIP IP address
- Remote SIP IP and TCP/UDP/SCTP port number
- IPv4 Protocol field or IPv6 Next Header field
- Interface Group ID to disambiguate IP addresses in Overlap IP addressing deployment

A microflow entry is associated with

- 'accept' or 'discard' action
- Packet admit Rate policer
- Next stage aggregate policer selector and aggregate policer priority

The following diagram explains the microflow management based on endpoint Registration



End Point Registration and automated management of Microflows

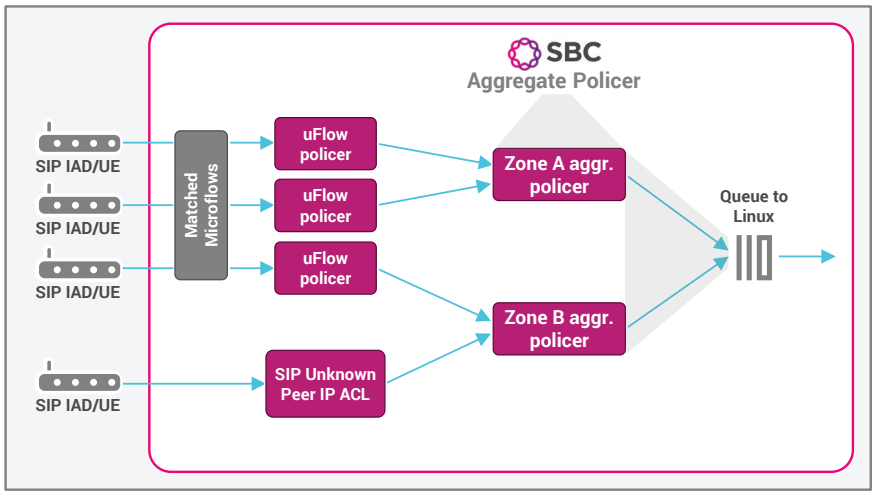
Note, SBC admits the very first SIP REGISTER message from the endpoint using SIP Unknown Peer IP ACL. The purpose of the Unknown Peer IP ACL is to facilitate end point discovery. The Unknown Peer IP ACL is never intended to be used in Carrier Peering and Enterprise Access deployments.

Once the SBC learns the IP address and UDP/TCP port of the endpoint (or NAPT device) from the first REGISTER message, SBC installs a microflow and admits subsequent packets from that endpoint using microflow. SBC limits the number of packets from an endpoint until the endpoint completes successful authentication with the application server. SBC uses the endpoint CAC profile to determine the admit rate for an authenticated endpoint.

Aggregate Policer

The aggregate policer functionality allows multiple flows to share a rate-limiter instance. The aggregate policer applies the second tier of rate limiting for a given packet, following per-microflow or per-ACL-rule policing.

The aggregate policing allows the operator to oversubscribe the first-tier policing and therefore obtain higher overall utilization while still limiting the overall load from a set of peers.



Here are a few notable aspects of aggregate policing.

- Packets from devices that belong to the same Zone get policed by the Zone Aggregate Policer
- Packets from Authenticated devices are given higher priority than the packets from unauthenticated devices i.e. packets matching a microflow have higher priority than packets matching Unknown Peer IP ACL

RTP Source Address Validation

The SBC decides for each received packet whether to process it as a RTP/RTCP packet or a non-RTP/RTCP packet. If the IPv4 Protocol field or IPv6 Next Header field is UDP, and the destination port number is in the “RTP port range” then SBC processes the packet as an RTP.

The RTP packets that fail to match a valid SIP session i.e., session state where media from remote peer is expected, are counted as rouge media, and discarded. A grace period for run-on media following a call is provided for an interval after a call is closed.

The SBC performs the following validation against a RTP packet that matches a valid SIP session.

- Match IP destination address and port with SBC own RTP IP address and port.
- RTP source address validation by matching the IP address and source UDP port in the packet with the IP and port signaled by the remote peer via SDP i.e., c= and m= lines, Offer-Answer during SIP session setup.

If there is any mismatch, the packet is counted as rouge media and discarded. The source address/port checking is disabled by default.

Ribbon strongly recommends that source IP and Port validation be enabled in all deployment models to protect audio sessions from a spectrum of DOS attacks such as Distributed Reflection DOS.

Please refer to the Core SBC SIP Trunk Group Media CLI for details on enabling Source Address Validation.

Further, SBC applies rate limiting to valid RTP packets using a media policer (used for RTP and RTCP together). The admit rate is set based on the selected codec and RTP packetization time. The SBC incorporates a hybrid policing scheme that rate limits RTP and RTCP packets using both bytes/sec and packets/sec policers.

SBC Operational Guidelines Policer Offender List and Alarms

SBC tracks the number of packets discarded by various policies such as Media, IPACL, and microflow policers. Besides, SBC keeps track of the sources whose packets were discarded and records them into the offender list. SBC raises the alarm when the discarded packet count in a specific category, e.g., IPACL policer, exceeds a configured threshold within a duration (also configurable).

There are ten categories of offender lists, e.g., IPACL offender list, rouge media offender list. SBC reports the top ten offenders within each type, i.e., source IP address, including the port that conducted the DOS. Please refer to the Core SBC IP Policing documentation for the details, including the commands to get the list of top ten offenders in each category.

SBC reports the following alarms based on the Alarm Profile configuration, described in detail in Core SBC IP Policing Alarm Profile CLI Documentation. A default Alarm Profile is seeded into the system for raising MAJOR, MINOR and Clearing IP Policing Alarms. Operators can override the default by their Alarm profile.

- setThreshold and setDuration – threshold where discard count must be greater than setThreshold for setDuration seconds to trigger sonusSbxNodePolicerMajorAlarmNotification and sonusSbxNodePolicerMinorAlarmNotification Alarms
- clearThreshold and clearDuration – threshold where discard count must be below than clearThreshold for clearDuration seconds to clear alarm sonusSbxNodePolicerClearAlarmNotification

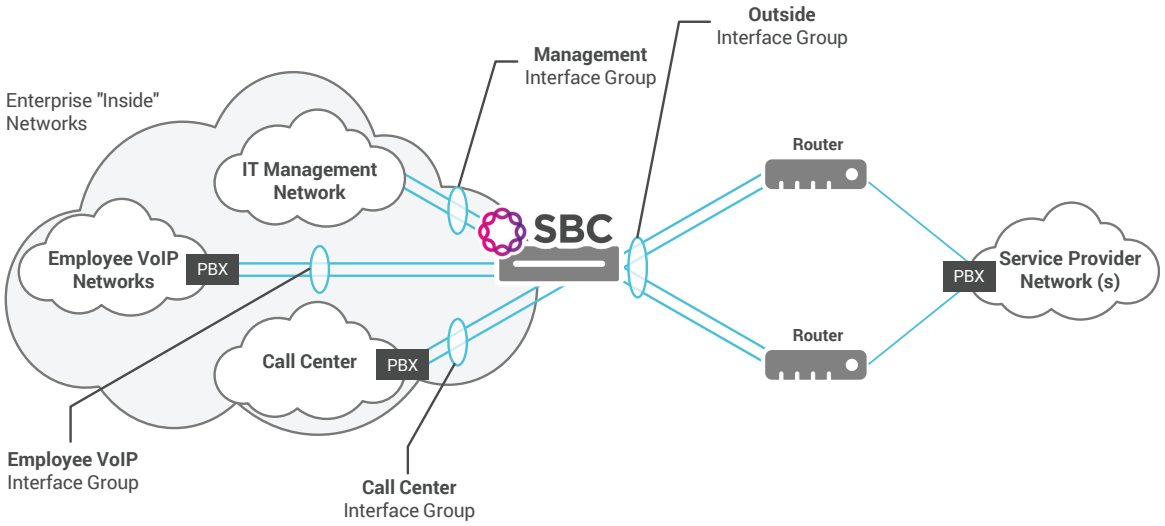
The System Interval Performance Statistics provides a wealth of historical information about the number of packets accepted, discarded and peak discard rate, the number of Major/Minor IP Policing alarm events in each interval. Please refer to IP Policing - System Current and Interval Statistics section in the Core SBC IP Policing documentation for details.

Disjoint Networking Controls

The SBC has flexible, configurable controls over which network interfaces may be used for sending and receiving signaling and media packets. The most common and basic deployment is to define an “Inside” and an “Outside” domain each with its own dedicated interfaces. Additional domains can be defined if desired. For example signaling and media may be kept isolated from each other at the same time as inside and outside are isolated, or several distinct inside and/or outside domains may be used.

Similarly, operations and management (OAM) traffic may be restricted to a certain set of interfaces and isolated from call signaling and media.

The diagram below shows an enterprise SBC deployment with four distinct interface groups defined, one each for connection to four disjoint network domains: the untrusted "Outside" network, the internal "IT management" network, an internal "call center" network, and an internal employee VoIP network. Configurable policies can control access to and amongst these domains as well as what peers the SBC may communicate with within each domain.



SBC Disjoint Networking Controls

Call Admission Controls (CAC)

Part of the security mission of the SBC is to protect and guarantee the level of service delivered. Achieving this requires applying limits to the system resources that any given user or VoIP peer may cause to be consumed. These controls are loosely referred to as Call Admission Controls (CAC) although they actually control much more than just call admission.

The SBC has flexible capabilities to identify individual VoIP devices (e.g. SIP phones, PBXs, SIP proxies, etc.) or groups of VoIP devices and apply CAC controls to those individual devices and overall groups. The CAC controls enforce limits on such metrics as:

- incoming calls per second
- outgoing calls per second
- total concurrent calls
- total concurrent media bandwidth
- etc.

Cryptographic Capabilities for VoIP Signaling and Media

As voice and other session-based multimedia communications move to IP-oriented implementations, the importance of protecting the integrity and confidentiality of these communications is increasing. The SBC provides robust cryptographic protections in several ways:

- Call signaling may be protected with either Transport Layer Security (TLS) or IPsec. These security protocols provide authentication of the peer device, confidentiality (privacy) of the call signaling, and integrity protection (detection of a changes made enroute) of the call signaling.
- Call media (RTP and RTCP) may be protected with Secure RTP (SRTP). SRTP provides confidentiality and integrity protection for the media.

In the SBC these protections can be enabled with minimal, or no performance impacts and Ribbon Communications strongly recommends using them.

Secure Management

Management of deployed SBC systems is cryptographically protected by several mechanisms. Access to command line (CLI) management is through ssh. Management of the system is through the netconf protocol protected by ssh. Ssh-based SFTP is used to transfer log files, software updates, etc. on and off the SBC. The built-in web-based GUI interface is accessed via https (http over TLS).

Ribbon's Core SBCs include several management daemons which operate in the background to handle various requests for services without user intervention. To prevent security loopholes and vulnerability from outside attacks, both the Linux and SBC management daemons are restricted to send and receive management traffic to/from management interfaces only.

In addition, this architecture prohibits packets received on packet interfaces from reaching management applications. For example, if the port scan (e.g. nmap) sends packets to packet interfaces, it does not discover the management daemons' ports as open state.

Secure Management Audit and Security Logs

Security analytics is dependent on centralized Syslog aggregation, with the expectation that the Syslog communication is secured. The primary Syslog security threats to address are:

- Masquerade
- Modification
- Disclosure

To eliminate these threats, RFC 5425 defines a TLS Transport Mapping for Syslog. The SBC supports the RFC 5425-compliant transport option in addition to the existing UDP, TCP, and RELP Syslog remote protocols.

The SBC supports Rsyslog method of sending event messages to the Syslog server, has the following capabilities.

- Send Syslog traffic to multiple Syslog servers
- support three Syslog servers per event log type
- offer support for the Linux logs

The Linux logs include the following:

- platformAuditLog - Platform Linux Audit log messages
- consoleLog - Console activity messages
- sftpLog - internal-sftp messages
- kernLog - kernel messages
- userLog - user-level messages
- daemonLog - system daemon messages
- authLog - auth and authpriv - security/authorization messages
- syslogLog - internally generated by syslog messages
- ntpLog - NTP subsystem messages
- cronLog - clock daemon messages
- fipsLog - fips messages

The SBC supports enabling or disabling the audit logs to start or stop the auditd service, which is used to write the audit logs. The SBC automatically adds an Access Control List (ACL) rule to send the audit logs to the remote server.

Secure Management Key Based Authentication

The SBC SSH public key authentication feature allows application management users to provision, delete, and display up to five SSH public keys for the purpose of accessing CLI (port 22), NETCONF(port 2022) and SFTP (port 2024).

This feature provides a user interface through which application management users can add, delete, and display authorized client public keys. Up to five keys are supported for each configured use

The system Admin command sshPublicKeyAuthenticationEnabled allows the user to enable or disable public key authentication.

Hardened System

In addition to the flooding-based DOS attack protection described earlier, the SBC system itself is hardened against intrusion attacks in a number of ways including:

- Protocol stacks are tested and hardened against software defects that could provide exploitation points for attackers.
- The system has robust, proven overload controls designed to gracefully shed load and maintain proper operation when overcapacity.
- The software is minimized to remove unused components and unnecessary network services.

Summary

Telecom network and service operators are now being targeted with more sophisticated DOS attacks. The distributed reflective DOS is an example where attackers utilize vulnerable UDP-based services as reflectors and target to deplete network bandwidth, compute resources, and impact services for legitimate users. The traditional technique to block the offending source is no longer effective for dealing with such DDOS attacks. And blocking a traffic class e.g. DNS may impact call routing and eventual service delivery. As a VOIP security device, an SBC has intelligent capabilities to detect and mitigate these DOS attacks. These capabilities ensure the availability and integrity of the SBC itself and managed network behind the SBC. SBCs also provide confidentiality and integrity protection services for the served VoIP and multimedia traffic using TLS for SIP and SRTP and SRTCP for media.

Ribbon recommends the following configurations to be applied on the SBC to protect SIP Signaling and RTP from DDOS attacks:

- SIP Unknown Peer ACL accepts packets from any remote IP and port, needed to admit the first few packets from Phones, i.e., TCP SYN-ACK, REGISTER. Ribbon recommends overriding the SIP Unknown Peer ACL with white-list IPACLs, one per known Peering Gateway.
- For over-the-top Access, use TCP/TLS on the Access interface and override the SIP Unknown Peer IP ACL with an IPACL restricted to admit TCP packets. Use SRTP for the over-the-top Access deployment.
- Install deny-ACL rules on packet interface to block IP packets from the well-known SNMP, DNS, CLDAP source ports to block UDP attack traffic from Reflectors
- Enable RTP Source Address Validation, which defends well against reflection attacks on media ports.

Appendix A – Attacks Protected Against

The following table lists SBC defense mechanism against some of the well-known attacks.

Attack Name	Attack Description	SBC Defense Mechanism
MAC Layer Attack		
	Unsupport Ethernet type	Discard
	ARP Flood	ARP Policing
Local Area Network Denial LAND Layer 4 Attack	Malformed IP Packet	Validate IP header and discard malformed packet
	Unsupported IP Protocol	Discard
	Unsupported IP Options	Discard
	IP Source Route attack	Discard source routed packets
	Packets with spoofed source IP = destination IP	Discard
Tear Drop, BONK and BOINK	IP Fragment Flood	IP Fragment Policing
	IP Fragment Reassmebly greater than 64KB	Hardened IP Fragment Reassembly
	Incomplete set of IP Fragments	Hardened IP Fragment Reassembly
SMURF, FRAGGLE	ICMP Request Flood	ICMP Policing
	ICMP Error Message	Discard
	IP Broadcast PING/ECHO Amplification with spoofed source address	Discard unexpected Broadcast and Multicast packets
PEPSI	UDP Malformed Header	Discard
	UDP Flood	Dark Grey Policing scheme
STREAM and SPANK TCP Layer Attacks	TCP SYN Flood	Linux SYN Cookie scheme
	TCP RST Attack	Hardened Linux TCP /IP implementation
	TCP FIN with no ACK	Discard
	TCP FIN and SYN in the same segment	Discard
XMAS TREE TCP Layer Attacks	More than one of SYN, FIN, RST set	Discard
	TCP segment with no flags set	Discard
	TCP connection hijacking	Initial SEQ number based on RFC 1948
Malicious Hosts	SNMP Flood	SNMP Policing
	SIP Flood from Known Peer	Whitelist policing
	SIP Flood from Registered device	Microflow policing
	Excessive Signaling traffic from untrusted sources	Unknown Peer Policing
	Excessive Signaling traffic on an IP Interface	IP Interface Policing
	RTP and RTCP Flood	Media Policing
	Rouge RTP and RTCP	Source RTP IP Validation
	Spoofed RTP and RTCP	Secure RTP and RTCP
	SIP REGISTER and INVITE Flood	Policing at IPTG and Zone Level
	SIP and SDP Malformed Packet	Hardened SIP Stack, Codenomicon validated
	Spoofed SIP	DIGEST Authentication
	Spoofed SIP Peer	TLS

Appendix B – Security Testing Performed by Ribbon

- Codenomicon SIP UAS
- Codenomicon SIP UAC
- Codenomicon SIPI
- Nessus scan
- Burp scan
- Qualys scan
- Rouge RTP simulator
- Ixia-Iexplorer based tests

Appendix C – SBC Network Ports Usage

Please refer to the Network Listener Ports Section in Core SBC Product guide.

Appendix D Glossary

ACL. Access control list
API. Application programming interface
AWS. Amazon Web Services
CAC. Call admission control

DoS. Denial of service
GCP. Google Cloud Platform
GUI. Graphical User Interface
HA. High Availability
IMS. IP Multimedia Subsystems
IP. Internet Protocol
IPACL. IP Access Control List
I-SBC. Integrated SBC, Integrated SBC
KVM. Kernel Virtual Machine
LTE. Long Term Evolution
NGN. Next generation network
OAM. Operations, Administration, and Maintenance
OTT. Over-the-top
PBX. Private Branch Exchange
PDU. Protocol data unit
RTC. Real-time communications
SBC. Ribbon Core Session Border Controller
SDP. Session Description Protocol
SIP. Session Initiation Protocol

SLB. Ribbon SIP-Aware Load Balancer
SWe. Ribbon SBC Software Edition
vCPU. Virtual Central Processing Unit
VIM. Virtual Infrastructure Manager
VM. Virtual machine
VNF. Virtual network functions
VNFC. Virtual Network Function Component
VoIP. Voice over Internet Protocol
VoLTE. Voice over LTE

Click Here to Get a Quote for One of Our SBCs https://rbbn.com/ribbon-sbc-quote

About Ribbon

Ribbon Communications (Nasdaq: RBBN) delivers communications software, IP and optical networking solutions to service providers, enterprises and critical infrastructure sectors globally. We engage deeply with our customers, helping them modernize their networks for improved competitive positioning and business outcomes in today's smart, always-on and data-hungry world. Our innovative, end-to-end solutions portfolio delivers unparalleled scale, performance, and agility, including core to edge software-centric solutions, cloud-native offers, leading-edge security and analytics tools, along with IP and optical networking solutions for 5G.

Copyright © 2022, Ribbon Communications Operating Company, Inc. ("Ribbon"). All Rights Reserved. v0122