Sangoma Session Border Controllers

Using DNS SRV to Provide High Availability Scenarios

Contents

1. SANGOMA SESSION BORDER CONTROLLERS - HIGH AVAILABILITY SOLUTION

SBCs are installed at the border of VoIP networks for VoIP security, NAT traversal, DDOS, call admission control, topology hiding, SIP mediation, RTP mediation, transcoding, DTMF, fax relay, port remapping, and secure remote access of VoIP users.

There are a number of applications that require a high availability (HA) solution that provides a resilient and fault tolerant network.

In each application, the solution is similar: to have multiple Sangoma Session Border Controllers manage all of the traffic from the public internet to a SIP server located on a secure LAN. There are two methods for providing high availability to the Sangoma Session Border Controllers. The first is by load balancing. The next is by failover. Both scenarios are quite valid to offer high availability.

2. WHAT IS DNS SRV?

The Domain Name System (DNS) associates various sorts of information with domain names; most importantly, it serves as the "phone book" for the internet by converting human-readable computer hostnames, e.g. *www.sangoma.com* into the IP addresses, e.g. *70.25.53.39* that networking equipment needs to convey information. It also stores other information, such as the list of mail exchange servers that accept email for a given domain. In providing a worldwide keyword-based redirection service, the Domain Name System is an essential part of contemporary internet use.

Above all, the DNS makes it possible to assign internet names to organizations, independently of the physical routing hierarchy represented by the numerical IP address. Because of this, hyperlinks and internet contact information can remain the same, whatever the current IP routing arrangements may be, and can take a human-readable, easier-to-remember form, such as *sangoma.com* when compared to the IP address *70.25.53.39*. People take advantage of this when they recite meaningful URLs and e-mail addresses without caring how the machine will actually locate them.

The Domain Name System distributes the responsibility for assigning domain names and mapping them to IP networks by allowing an authoritative server for each domain to keep track of its own changes, avoiding the need for a central registrar to be continually consulted and updated. An SRV record or Service record is a category of data in the Domain Name System specifying information on available services. It is defined in RFC 2782. Newer internet protocols, such as SIP and XMPP, often require SRV support from clients.

An SRV record has the form:

_Service._Proto.Name TTL Class SRV Priority Weight Port Target

Service:	The symbolic name of the desired service.
Proto:	The protocol of the desired service; this is usually either TCP or UDP.
Name:	The domain name for which this record is valid.
TTL:	Standard DNS time to live field.
Class:	Standard DNS class field (this is always IN).
Priority:	The priority of the target host, lower value means more preferred.
Weight:	A relative weight for records with the same priority.
Port:	The TCP or UDP port on which the service is to be found.
Target:	The canonical hostname of the machine providing the service.

An example SRV record might look like this using bind syntax:

_sip._udp.carrier.com. 86400 IN SRV 0 5 5060 sipserver.carrier.com

This points to a server named *sipserver.carrier.com* listening on UDP port 5060 for SIP protocol connections. The priority given here is 0, and the weight is 5.

With SIP telephony, a SIP call might start as *19054741990@sangoma.com* for the call to proceed, the phone needs to locate sangoma.com and it will use DNS to do this. Sangoma.com could be an IP-PBX, a soft switch or a proxy server.

3. FAILOVER SBCS WITH DNS SRV

The priority field is similar to an MX record's priority value. Clients always use the SRV record with the lowest-numbered priority value first, and only fall back to other records if the connection with this record's host fails. Thus, a service may have a designated "fallback" server, which will only be used if the primary server fails. Only another SRV record with a priority field value higher than the primary server's record is needed.

If a service has multiple SRV records with the same priority value, clients use the weight field to determine which host to use. The weight value is relevant only in relation to other weight values for the service, and only among records with the same priority value.

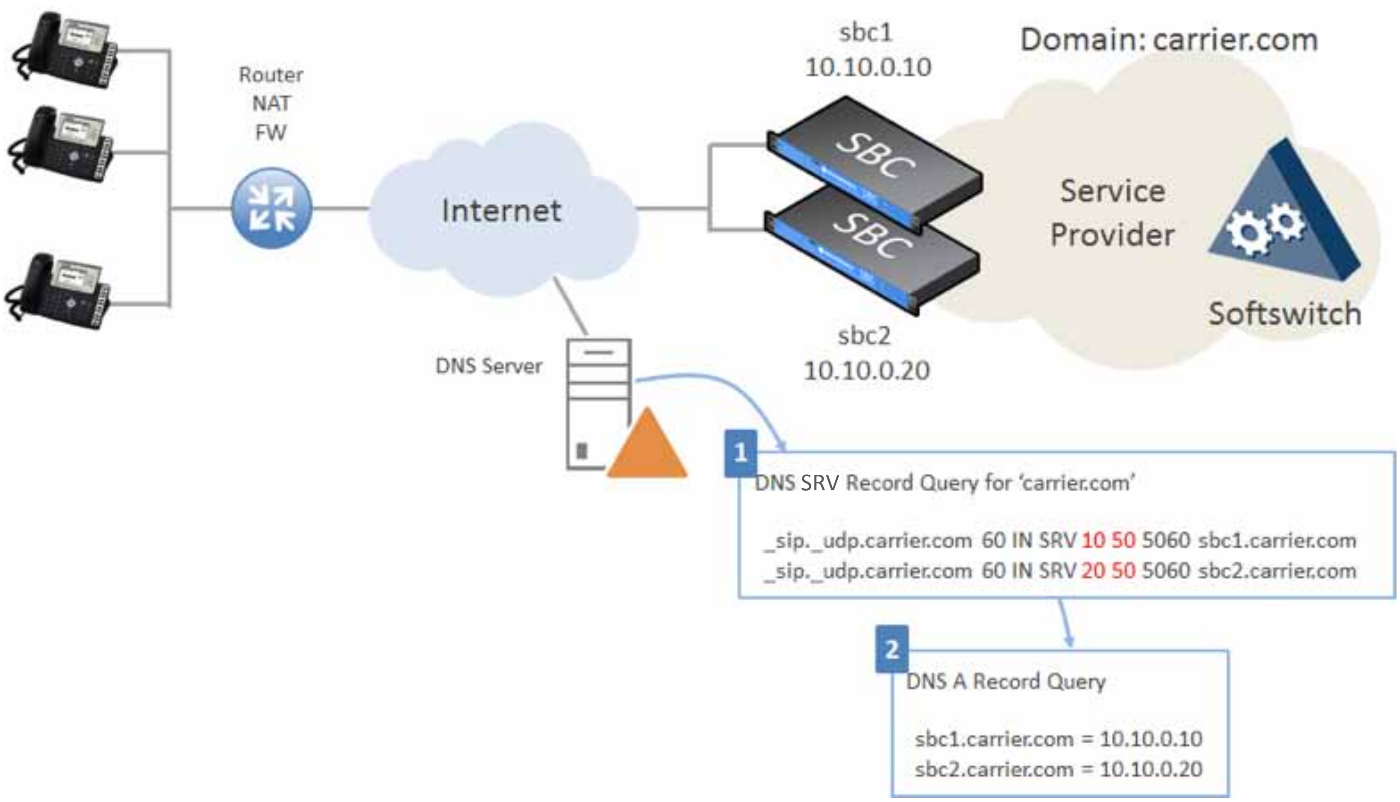
In failover, SBCs are set with different priorities. The lower priority SBC is tried first, and if that SBC is unavailable, the SBC with the higher priority is tried. Records with higher priority values are only tried if all records with a lower priority are considered unreachable.

In the following example, DNS SRV record query to carrier.com with both the priority and weight fields each with 50% of the traffic load is used to provide a failover service and would yield:

_sip._udp.carrier.com 60 IN SRV 10 50 5060 sbc1.carrier.com
_sip._udp.carrier.com 60 IN SRV 20 50 5060 sbc2.carrier.com

DNS A Record Query yields: **sbc1.carrier.com = 10.10.0.10**
sbc2.carrier.com = 10.10.0.20

If the server with the priority 10, *sbc1.carrier.com* is unavailable, the record with the next higher priority would be chosen, which would be *sbc2.carrier.com*.



4. LOAD BALANCING SBCS WITH DNS SRV

In the following example, a DNS SRV record query to carrier.com with both the priority and weight fields each with 50% of the traffic load is used to provide a load balancing and backup service and would yield:

_sip._udp.carrier.com 60 IN SRV 10 50 5060 sbc1.carrier.com
_sip._udp.carrier.com 60 IN SRV 10 50 5060 sbc2.carrier.com
_sip._udp.carrier.com 60 IN SRV 20 0 5060 backupbox.carrier.com

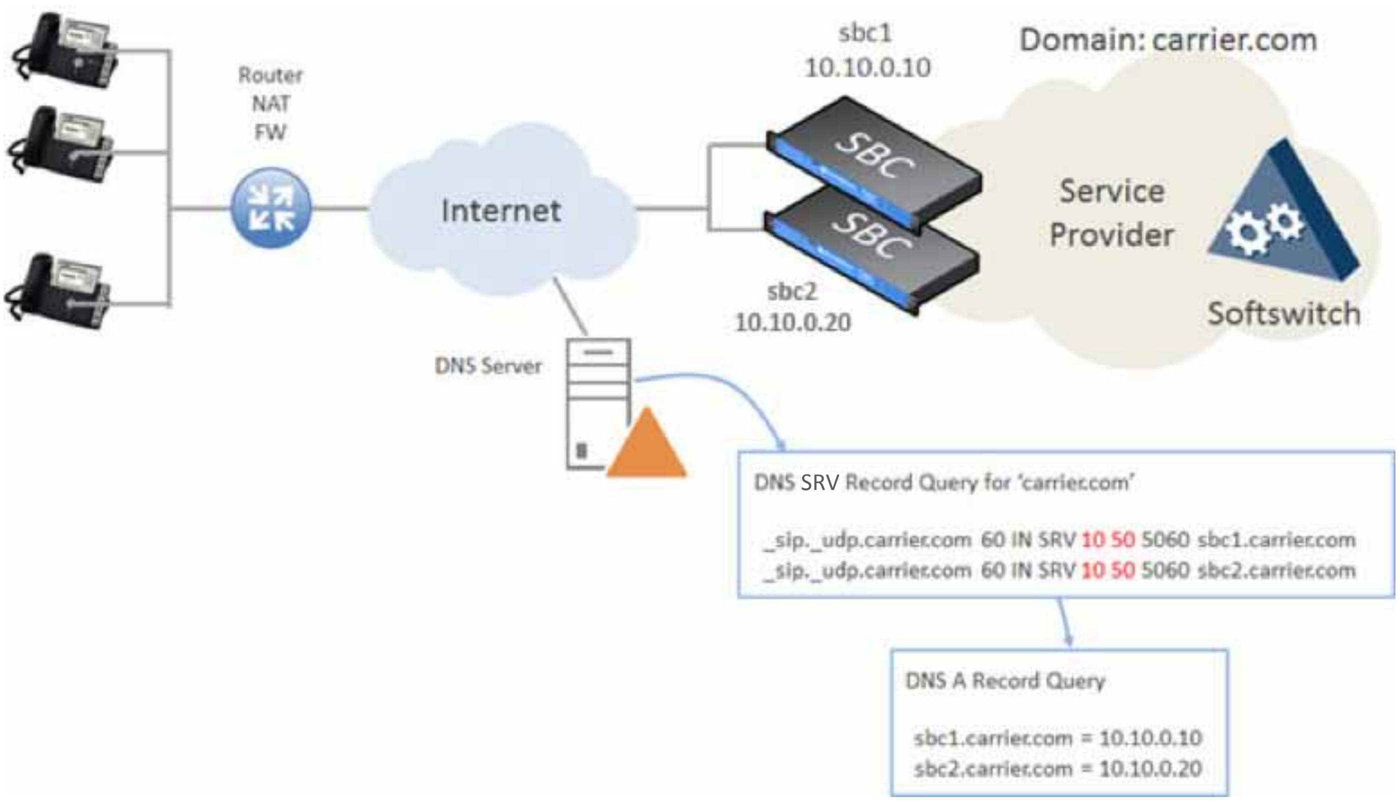
If one SBC becomes unavailable, the remaining machine takes the load.

The two records share a priority of 50, so the weight field's value will be used by clients to determine which server (host and port combination) to contact. The sum both values is 100, so sbc1.carrier.com will be used 50% of the time and sbc2.carrier.com will be used 50% of the time.

DNS A Record Query yields: **sbc1.carrier.com = 10.10.0.10**
sbc2.carrier.com = 10.10.0.20

If both servers with priority 10 are unavailable, the record with the next highest priority value will be chosen, which is *backupbox.carrier.com*. This might be a machine in another physical location, presumably not vulnerable to anything that would cause the first two hosts to become unavailable.

Several implementations relying on DNS also automatically update the DNS servers to optimize the load of servers or to remove servers due to service failures.



Please note this document does not describe network distribution, resiliency and failover scenarios in combination with having multiple Sangoma SBCs. If the solution is not properly distributed over a network, then it is possible that the Sangoma SBC may have some service degradation. Providing DNS Server updates with current network information will help in providing a resilient environment.

5. LOAD BALANCING SBCS VS. FAILOVER WITH DNS SRV

Both scenarios are quite valid to offer high availability. Load balancing, sometimes referred to as an Active-Active scenario, has some advantages. All equipment is active; it allows double the call rate, and accommodates traffic bursts. In a failover scenario, only one unit is active and traffic is limited to the capacity of that one device. This is sometimes referred to as Active-Standby Scenario.

With both types of DNS SRV high availability, if an SBC goes down the active calls on the network are dropped, but the new calls are taken care of by the remaining SBCs.

Although load balancing and failover is not stateful high availability, where all the calls remain up if an SBC fails and new SBC takes over, load balancing and failover high availability using two Sangoma SBCs are a small fraction of the cost of stateful solutions and are more than acceptable in most scenarios.

Both load balancing and failover SBC implementations using DNS SRV can be used with both carrier and enterprise SBCs and most VoIP endpoints support DNS SRV lookups, but it is advisable to verify with your supplier. Sangoma e-SBCs and Vega VoIP Gateways support DNS SRV lookups and responses.

Both methods can be used with hosted PBX service and with IP-PBX and SIP trunks. However, instead of SIP phones being configured to respond to DNS SRV answers, it would be the IP-PBX that is configured.

6. GEOGRAPHICAL DISTRIBUTION

All scenarios above described the solution with collocated SBCs. Another benefit of using DNS SRV, is it is very easy to distribute the SBCs to different locations in the case of multiple data centers providing the services, so in the event one data center experiences an outage, the other location(s) can provide the resiliency.

7. CONCLUSION

While there are other methods to provide high availability for SBCs, leveraging established and easy to use networking resources goes a long way.

FOR MORE INFORMATION:

+1 905 474 1990 ext. 2