DNS Setup Concepts for Session Border Controllers

By: Michael W. Picher

Date: January, 2009

This particular document isn't meant to be a tutorial on how to create DNS zones or add records to them. It is meant to help the reader understand the issues surrounding DNS configurations when a Session Border Controller (SBC) is in use and how to leverage DNS to configure redundant / load balanced SBC's.

Session Border Controllers allow for users to seamlessly connect to corporate SIP services. DNS setup can be tricky for a system setup where a user needs to be able to roam from inside the office to outside and then maybe even be on a VPN connection. To make this all work seamlessly, the PBX must be able to be referenced the same way no matter where the end-user is located.

Most of my work revolves around sipXecs (http://www.sipfoundry.org) systems so this document, while useful for any SBC setup, will be using sipXecs for the examples.

It is very important that network administrators understand DNS (most really don't). Here's a great reference to help get more comfortable with DNS: http://en.wikipedia.org/wiki/Domain_name_system

I've also written a separate document on setting up Microsoft DNS Services for use with sipXecs and published it in the sipXecs Wiki: http://sipx-wiki.calivia.com/index.php/Image:MSDNSConfigforsipX.pdf

For errors or omissions please contact me over at my blog: http://www.sipxecs.info or by e-mail at mpicher (at) gmail.com

DNS Records

It is important to understand the difference between A records and SRV records so let's get that out of the way first.

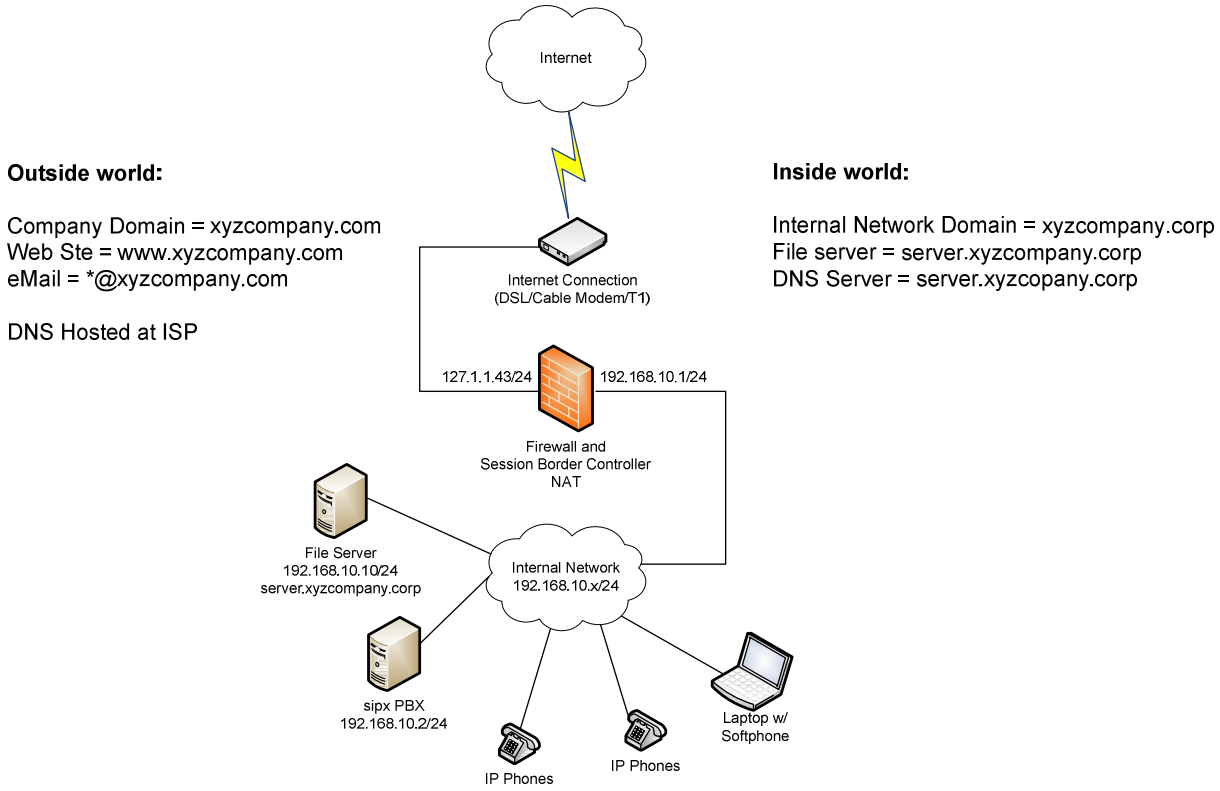
An A record is a typical host name pointer to an IP address. So, sipx.xyzcompany.com might be an A record that points to 127.1.1.43. In this example, sipx is the host name, xyzcompany.com is the domain name and sipx.xyzcompany.com is referred to as the fully qualified domain name (fqdn). We use A records because it's easier to remember computer names than a series of numbers (for most people anyway). Most Asterisk configurations the author has seen run with an A record setup for the PBX.

SRV records (service records) are used by newer Internet protocols to locate a type of service that might be available for a domain. MX records (mail exchange) work similarly to SRV records but are used specifically for mail. SRV records can be used for any number of services. A SIP service record will look like _sip._udp.xyzcompany.com. In this example a SIP device can query DNS for domain xyzcompany.com and find an IP address or host name for SIP services running on the UDP protocol. Similarly, _sip._tcp.xyzcompany.com would return an IP address or host name for SIP services running on the TCP protocol. So, a phone registering to the xyzcompany.com domain would lookup _sip._udp.xyzcompany.com and have the host name sipx.xyzcompany.com returned. Why not just cut to the chase and use the A record? You'll see why in a bit.

sipXecs PBX configurations are typically setup with SRV records.

The Typical Scenario

Ok, so most companies aren't hiding under rocks and they are already using DNS internally on their networks. Like many, the internal network DNS domain name may not be the same as their Internet facing domain. Consider the following network scenario:



With our fictitious company (sorry if it's not), the internal computer network has an existing DNS domain of xyzcompany.corp which is being used by Active Directory. If you were to setup your sipXecs pbx in the xyzcompany.corp domain, this domain is never going to be referable by domain name from the

Internet. Most Session Border Controllers do allow for some SIP domain name translation. It thus should be possible to setup your mobile users differently than your fixed position hard phone users and do a translation of xyzcompany.com to xyzcompany.corp.

In reality, the simplest approach should be used… Setup an internal DNS zone that mirrors the external domain and make the pbx participate in that DNS domain. A copy of the domain could be maintained on your internal DNS server but that wouldn't allow you to create your own records pointing to internal IP addresses.

For those who don't understand DNS domains setting up another DNS domain might sound like you are setting up another network domain. This simply isn't the case. A DNS domain is a name space that houses DNS records for resolving down to IP addresses. While Microsoft Active Directory utilizes DNS domains heavily, Active Directory domains and the security settings they impose on all members of the domain have nothing to do with DNS domains (of course if you mess up your Windows DNS server it will definitely adversely affect Active Directory).

So, using the above example, the sipXecs pbx would have a SIP domain of xyzcompany.com and a fully qualified domain name of sipx.xyzcompany.com if users are to access the PBX with the same name inside or outside the network. With this method, records can be added to the ISP's DNS zone files that point to the external interface of the firewall/SBC. Internally, records can be created in the DNS zone file that point directly at the sipXecs pbx.

Using A Records

As described above, A Records are simply name pointers to IP addresses. While A record naming is not typically recommended for sipXecs installations, A records can be utilized to locate the pbx. On a clean sipXecs system (before you add any users), under system administration, go into the System menu and select the Domain menu item. Change the domain name to the fully qualified domain name that you would like to use, click 'Apply' and then reboot.

Make sure your new A record is in your internal DNS server pointing to the internal IP address of the sipXecs pbx.

Internally DNS zone file for the xyzcompany.com domain would have an A record setup pointing to the IP of the PBX:

sipx	A	192.168.10.2

Have your ISP (or if you can do it yourself with a self-managed DNS hosting provider) add an A record for your pbx pointing at the external IP address of your firewall/SBC.

Externally, DNS would have an A record setup pointing to the external IP of the SBC:

sipx	A	127.1.1.43

Testing A Record Configuration

Verify that it all works properly by pinging the PBX by name from both inside the firewall and from outside the firewall using the same DNS domain name. For example:

```
ping sipx.xyzcompany.com
```

Should return something like:

```
Pinging sipx.xyzcompany.com [192.168.10.2] with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time=1ms TTL=64

Reply from 192.168.10.2: bytes=32 time=1ms TTL=64

Reply from 192.168.10.2: bytes=32 time=1ms TTL=64

Reply from 192.168.10.2: bytes=32 time=1ms TTL=64


Ping statistics for 192.168.10.2:

   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

   Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

From the Internet the results should be similar but the IP address will be the external IP address of the firewall/SBC (assuming of course that you are allowing ICMP traffic).

Using SRV Records

So, why are SRV records so much better? Well, they allow us to be contacted with the same address used to deliver e-mail and SRV records allow for server redundancy and load balancing.

Take for example the top salesperson for XYZ Company, Joe User. Joe's phone extension is 512 and he has an email address of joe.user@xyzcompany.com. SRV records allow Joe User to be contacted at sip:512@xyzcompany.com and if an alias is put on his user account he can also be called by phone at sip:joe.user@xyzcompany.com. If xyzcompany.com were using A records for their sipXecs installation, Joe's phone number and alias would have be sip:512@sipx.xyzcompany.com and sip:joe.user@sipx.xyzcompany.com respectively (unless of course the addresses are transformed by the SBC, but then we get into the whole problem of inside the network and outside the network).

SRV records also allow the administrator to have redundant and load balanced SBC computers (sipXecs also uses this method for locating PBX's in a clustered/high availability configuration). SRV records hold the following information:

Service: the symbolic name of the desired service.

- Protocol: this is usually either TCP or UDP.
- Domain name: the domain 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.
- 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 hostname of the machine providing the service.

An example SRV record might look like this in a DNS zone file:

```
_sip._udp.example.com 86400 IN SRV 0 5 5060 sipx.xyzcompany.com.
```

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

The priority field is similar to an MX record's priority value. Clients always use the SRV record with the lowest 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 the following example, both the priority and weight fields are used to provide a combination of load balancing and backup service.

_sip._udp.example.com 86400 IN SRV 10 60 5060 sipx.xyzcompany.com.

_sip._udp.example.com 86400 IN SRV 10 20 5060 sbc2.xyzcompany.com.

_sip._udp.example.com 86400 IN SRV 10 20 5060 sbc3.xyzcompany.com.

_sip._udp.example.com 86400 IN SRV 20 0 5060 sbc4.xyzcompany.com.

The first three records share a priority 10, so the weight field's value will be used by clients to determine which host to contact. The sum of all three values is 100, so sipx.xyzcompany.com will be used 60% of the time. The other two hosts, sbc2 and sbc3, will be used for 20% of requests each. If sipx.xyzcompany.com is unavailable, these two remaining machines will share the load equally, since they will each be selected 50% of the time.

If all three hosts with priority 10 are unavailable, the record with the next highest priority value will be chosen, which is sbc4.xyzcompany.com. This might be a machine in another physical location, presumably not vulnerable to anything that would cause the first three hosts to become unavailable.

Let's look at what these records look like on the internal DNS server and then on the external DNS server. We'll just concentrate on a single SBC and not a redundant configuration.

So, internally DNS zone file for the xyzcompany.com domain would have an A record setup pointing to the IP of the PBX:

sipx	A	192.168.10.2

And then the SRV records would be setup as follows:

_sip._udp.xyzcompany.com	86400	IN	SRV	10	100	5060	sipx.xyzcompany.com
_sip._tcp.xyzcompany.com	86400	IN	SRV	10	100	5060	sipx.xyzcompany.com

Externally, DNS would have an A record setup pointing to the external IP of the SBC:

sipx	A	127.1.1.43

And then the SRV records would be setup exactly as they were internally (note, if you are using OpenSBC it only needs the UDP record):

_sip._udp.xyzcompany.com	86400	IN	SRV	10	100	5060	sipx.xyzcompany.com
_sip._tcp.xyzcompany.com	86400	IN	SRV	10	100	5060	sipx.xyzcompany.com

Testing SRV Configuration

The dig command in Linux lets us test DNS.

At the command line enter: dig –t SRV _sip._udp.xyzcompany.com

The following will be displayed:

```
; <<>> DiG 9.3.4-P1 <<>> -t SRV _sip._udp.xyzcompany.com

;; global options:  printcmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48387

;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0


;; QUESTION SECTION:

;_sip._udp.xyzcompany.com.      IN      SRV


;; ANSWER SECTION:

_sip._udp.xyzcompany.com. 0     IN      SRV     0 0 5060 sipx.xyzcompany.com.


;; Query time: 3 msec

;; SERVER: 172.16.1.254#53(172.16.1.254)

;; WHEN: Sat Jan  3 15:46:12 2009

;; MSG SIZE  rcvd: 81
```

From the ANSWER: 1 in the returned information and the sipx.xyzcompany.com in the ANSWER SECTION we know that the SRV record is working properly.

From a Windows workstation the nslookup command can be used:

At the command prompt enter: nslookup

Default Server: UnKnown

Address: 172.16.1.254

> set type=srv (enter this)

> _sip._udp.xyzcompany.com (enter the SRV record to test)

Server: UnKnown

Address: 172.16.1.254

_sip._udp.xyzcompany.com SRV service location: (expected results)

priority = 0

weight = 0

port = 5060

svr hostname = sipx.xyzcompany.com

Dynamic DNS

Wondering what about the case where the external IP address may change like with a Cable Modem or DSL connection? Usually the only way you will be able to deal with SRV records is by owning your own domain. Drop $20 a year with a hosting provider like GoDaddy.com or similar (just make sure they let you have SRV records) and get yourself a domain name.

Once you have an domain name, get setup with DynDNS or one of the other dynamic DNS providers (I use DynDNS because it works with Vyatta firewall). If you don't have a firewall that does dynamic DNS updates, you can usually run software on an internal machine that helps the dynamic DNS provider figure out your external IP address.

The dynamic DNS provider will let you determine your own host name and tag it to one of their domain names. For instance, xyzpbx.dyndns.net might be a host name you could specify. We can then point to this dynamic DNS name from our own domain.

For pointing a host name at another host name we'll use a CNAME record (canonical name). So, externally the DNS would have a CNAME record setup pointing to the dynamic DNS name:

sipx	CNAME	xyzpbx.dyndns.net

And then the SRV records would be setup also pointing to the dynamic DNS name as follows:

_sip._udp.xyzcompany.com	86400	IN	SRV	10	100	5060	xyzpbx.dyndns.net
_sip._tcp.xyzcompany.com	86400	IN	SRV	10	100	5060	xyzpbx.dyndns.net