BUILDING A BETTER
ONLINE CANADA

USING TRANSACTION SIGNATURES (TSIG) FOR SECURE DNS SERVER COMMUNICATION

02-13-2017

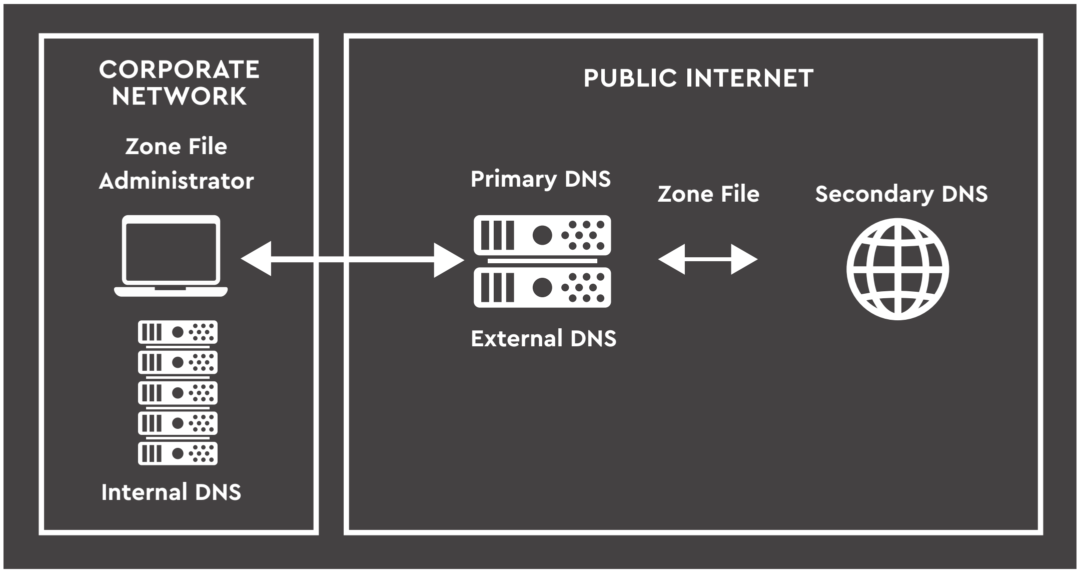
USING TRANSACTION SIGNATURES (TSIG) FOR SECURE DNS SERVER COMMUNICATION

Transaction Signatures (TSIG) provide a secure method for communicating from a primary to a secondary Domain Name server (DNS). It is a simple and effective method for organizations to enhance their security. TSIG is not a requirement and many organizations choose to specify IP address-based permissions between DNS name servers. However, as the DNS is increasingly targeted by bad actors on the Internet, TSIG is a recommended design consideration.

TSIG is used (optionally) by the D-Zone Anycast DNS service to communicate with an organization's primary DNS. This solution brief provides IT administrators a brief overview of a strong external DNS configuration using D-Zone, how TSIG is used, and the required configuration information. D-Zone users can get more details in the technical support documentation for D-Zone.

IMPLEMENTING A RESILIENT EXTERNAL DNS

Implementing a secondary DNS infrastructure for your external domain resolution improves the overall resiliency and performance of your external DNS and conforms to industry best practices. The ideal way to architect a secondary network is to maintain a hidden primary DNS server that is used for administration and management of the DNS. The secondary DNS consists of one or more name servers that are available to answer queries on the Internet which can be either Unicast or Anycast servers. Anycast technology uses multiple distributed servers that share the same IP address.



Typical DNS Architecture: Architecture of an authoritative DNS showing the corporate network, the primary DNS and a zone transfer to the secondary DNS.

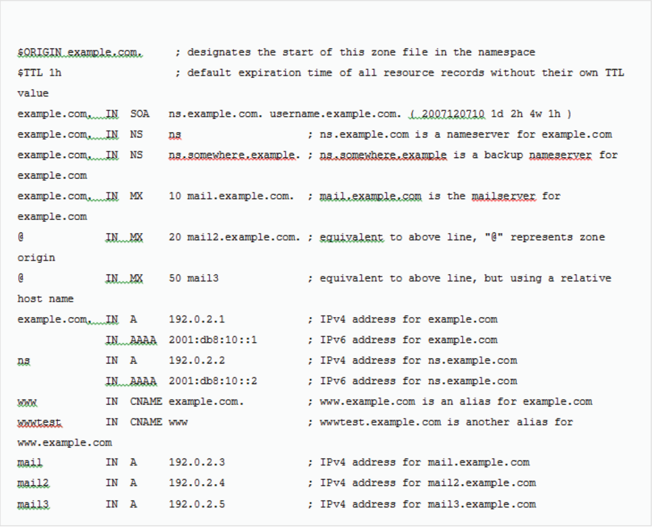
Combining a hidden primary DNS with an advanced Anycast DNS secondary solution provides the following benefits:

1) Easier maintenance of the primary DNS without without impacting public websites.
2) Increased security because the primary DNS is hidden.
3) Enhanced performance with a global network of servers that are close to customers.
4) Improved resilience because out of service nodes are removed from the routing tables.
5) Enhanced ability to soak up Distributed Denial-of-Service (DDoS) attacks against the DNS by soaking them up at the geographically closest node.

HOW DO I TRANSFER INFORMATION FROM MY PRIMARY DNS NAME SERVER TO A SECONDARY SERVICE

Now that you have made the decision to implement a more robust external DNS, how do you put it into action? Communication between name servers is done via zone files.

A zone file is a text file that describes a DNS zone. At its most basic it contains the mapping between IP addresses and domain names, organized in the form of resource records. In addition to providing the basic mapping it specifies a lot of other important details about the domain name including:



```
$ORIGIN example.com.      ; designates the start of this zone file in the namespace
$TTL 1h                   ; default expiration time of all resource records without their own TTL
value
example.com.  IN  SOA   ns.example.com. username.example.com. ( 2007120710 1d 2h 4w 1h )
example.com.  IN  NS    ns                    ; ns.example.com is a nameserver for example.com
example.com.  IN  NS    ns.somewhere.example. ; ns.somewhere.example is a backup nameserver for
example.com
example.com.  IN  MX    10 mail.example.com.  ; mail.example.com is the mailserver for
example.com
@             IN  MX    20 mail2.example.com. ; equivalent to above line, "@" represents zone
origin
@             IN  MX    50 mail3              ; equivalent to above line, but using a relative
host name
example.com.  IN  A     192.0.2.1             ; IPv4 address for example.com
              IN  AAAA  2001:db8:10::1        ; IPv6 address for example.com
ns            IN  A     192.0.2.2             ; IPv4 address for ns.example.com
              IN  AAAA  2001:db8:10::2        ; IPv6 address for ns.example.com
www           IN  CNAME example.com.          ; www.example.com is an alias for example.com
wwwtest       IN  CNAME www                   ; wwwtest.example.com is another alias for
www.example.com
mail          IN  A     192.0.2.3             ; IPv4 address for mail.example.com
mail2         IN  A     192.0.2.4             ; IPv4 address for mail2.example.com
mail3         IN  A     192.0.2.5             ; IPv4 address for mail3.example.com
```

Zone file

1) The Start of Authority (SOA) with the name of the authoritative servers (versus the caching servers online) which, in the examples in this paper, are the D-Zone secondary servers.
2) Time-to-live (TTL) which specifies how long the caching servers should keep the DNS record before reaching back to the authoritative servers.
3) The owner of the record.
4) Whether the address type is IPV4 or IPv6.

HOW IS THE PRIMARY EXTERNAL DNS ADMINISTERED?

The primary DNS of many organizations is administered by either the IT department or a supplier of web hosting, domain registration, primary DNS services, or other IT services. Regardless of the way the external DNS is administered, there are a few popular options for the underlying software infrastructure, including popular ones like BIND and Microsoft Windows Server.

UNDERSTANDING ZONE FILE TRANSFER AND TSIG

For maintaining strong security, the primary DNS is maintained as a hidden master only able to communicate with authorized secondary DNS servers with the correct IP address. This is a critical step in maintaining a secure, reliable and easy to maintain DNS.

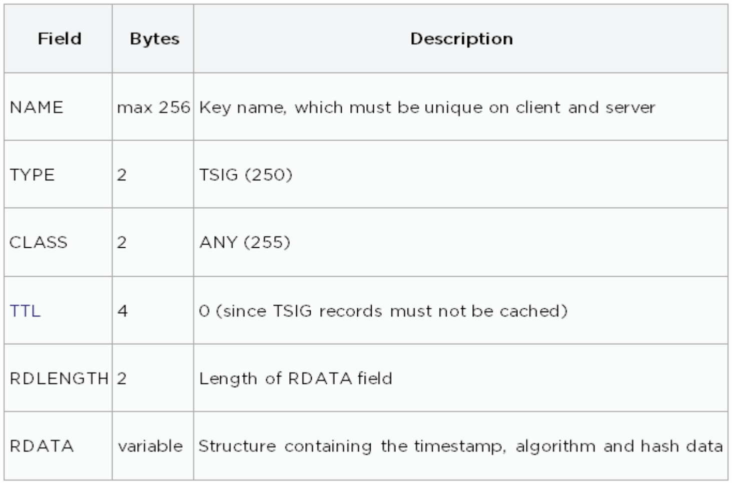
When any changes are made to the DNS in the primary name server it sends a "NOTIFY" DNS transaction to the secondary. If the secondary does not have the most up-to-date record it requests an update using a full zone transfer (AXFR) or an Incremental Zone Transfer (IXFR). The communication is over UDP or TCP as a client-server transaction and as a result is generally an open communication over an unsecured network (i.e. the Internet).

Since communication between name servers is open, authentication is critical because without it lasting changes to the DNS can be made that IT departments would have trouble overcoming. TSIG is a networking protocol that is defined in RFC2845 (Note: "RFC", or request for comment, is the nomenclature used by ICANN to make technical specifications and policy decisions) and it is used to provide authentication for dynamic DNS updates or communication between name servers.

When TSIG is used to secure communications between a primary and secondary name server, a cryptographic signature generated using a shared key and is added to all DNS packets exchanged between the servers. This ensures that the DNS packets originate from an authorized name server and have not been altered on route.

In addition to a key, the protocol includes a timestamp so that communications cannot be intercepted and used at a later time (and therefore requires that the systems use an accurate time source for their clocks).

A TSIG record is created and added to all DNS messages between the names servers. The following fields are included in a TSIG record:



Field	Bytes	Description
NAME	max 256	Key name, which must be unique on client and server
TYPE	2	TSIG (250)
CLASS	2	ANY (255)
TTL	4	0 (since TSIG records must not be cached)
RDLENGTH	2	Length of RDATA field
RDATA	variable	Structure containing the timestamp, algorithm and hash data

Fields in a transaction signature

CONFIGURATION USING TSIG

Notification between the servers must be enabled by specifying an IP address in "allow-notify" but not in "allow-transfer". If you configure both ends of the servers to "allow transfer" with an IP address and a TSIG then you are authorizing both TSIG and non-TSIG transfers. This allows an IP address **or** a TSIG when both are present. Notably, the interface to CIRA's D-Zone Anycast DNS secondary service will not allow incorrect configuration as D-Zone can be configured to allow open communications or TSIG communications, but not both.

Example zone entry with TSIG enabled
(correct secure configuration):

```
zone "example.ca" in {
        type master;
        file "master/example.ca";
        allow-transfer { key example-tsigkey. };
        also-notify { 162.219.53.35; 162.219.53.235; };
        };
};
```

Example zone entry with TSIG disabled
(correct but insecure configuration):

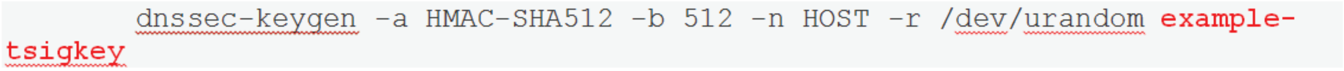
```
zone "example.ca" in {
        type master;
        file "master/example.ca";
        allow-transfer { 162.219.53.35; 162.219.53.235; };
        also-notify { 162.219.53.35; 162.219.53.235; };
        };
};
```

WHERE DO I GET THE TSIG AND IP ADDRESS

The signature can be generated on either your own DNS system or using the secondary DNS supplier's system. In the case of D-Zone, the capability to generate a TSIG is built into the interface and can be accomplished via point-and-click. The key signatures that D-Zone generates would then get copied onto your primary name server.

Example DNSSEC key generation using BIND

Using your primary DNS server to generate a key is a straightforward process. Generating a key in BIND uses a dnssec-keygen tool to generate both DNSSEC and TSIG keys. Notably, DNSSEC is a security protocol for the DNS that does not play a role in TSIG – the keys are simply generated from the same algorithm and command.



```
        dnssec-keygen -a HMAC-SHA512 -b 512 -n HOST -r /dev/urandom example-tsigkey
```

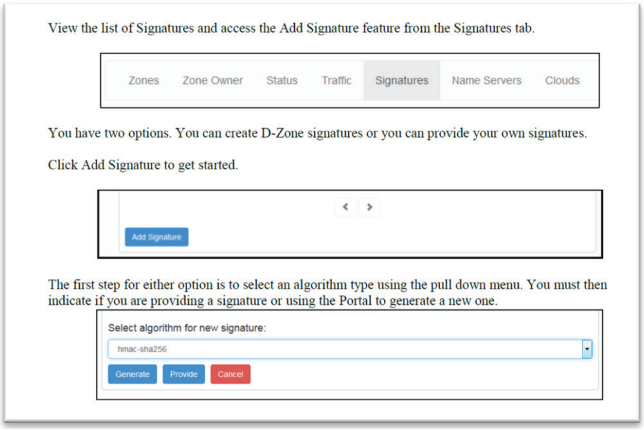
The name of the "example-TSIGkey" above must be unique to the organization and key.
This will generate a large key, or numbers and letters, which you will need to cut and paste into the BIND config file key section and copy to the secondary DNS service. Here is an example key section:

```
key "random-sig-1" { algorithm hmac-sha256; secret "dsdjflkjfkjk34u43430fgj3ifmi403jf3ijf="; };
server 162.219.53.35 {
        keys { random-sig-1; };
};
server 162.219.53.235 {
        keys { random-sig-1; };
};
```

Example key generation using D-Zone

Getting the key in D-Zone is a point-and-click activity rather than a command line task and generates an alphanumeric string that you copy into your primary DNS.

The task of copying the key into your primary name server depends on the platform you have chosen, or that your third party uses, and can be command line, point and click, or both. The support documentation of all common name servers covers this topic.



View the list of Signatures and access the Add Signature feature from the Signatures tab.

You have two options. You can create D-Zone signatures or you can provide your own signatures.

Click Add Signature to get started.

The first step for either option is to select an algorithm type using the pull down menu. You must then indicate if you are providing a signature or using the Portal to generate a new one.

Select algorithm for new signature: hmac-sha256

D-Zone interface showing how to generate a transaction signature.

WHERE DO I GET THE IP ADDRESS

The "allow transfer" IP address to supply to the secondary service will come from you or your primary DNS service provider. If you are using a service provider to configure and manage your primary DNS resolution you will need to provide them with the secondary service IP addresses for zone file transfer.

ORGANIZATIONAL WORKSHEET

Getting ready for configuring a secondary DNS and transferring a zone file using TSIG requires the following information be at hand. This table will help you to collect the information.

Setting up secure zone file transfer with TSIG is easy

Domain name(s)	Software Platform or supplier	Name	IP address of master server	IP address of secondary service	Transaction Signature
i.e .mysite.ca	BIND (internal) D-Zone (external)	Unique key name of server	162.xxx.xxx.123	232.xxx.xxx.789	FMP6jthr0OkmhHJUmj 32d1...

This paper contained quite a bit of detail and background material to help the reader understand the "why" and "how" for configuring secure zone transfers using TSIG and for helping you to avoid a common misconfiguration error. It is provided to help customers considering using the D-Zone Anycast DNS Service as a secondary service for their DNS.

The reality of actually setting up a secondary service with TSIG is a matter of a few clicks or command line prompts. Whether your organization is hosting its own primary DNS or using a third-party, the people at CIRA are here to help your organization build a more resilient DNS.

LEARN MORE ABOUT GETTING D-ZONE FOR YOUR ORGANIZATION

For information on ordering, finding a reseller, or becoming a reseller please contact info@d-zone.ca or visit cira.ca/d-zone.

ABOUT CIRA

The Canadian Internet Registration Authority (CIRA) manages Canada's .CA domain name registry as a 100 per cent up time service for Canadians and Canadian organizations.