Auth. DNS - Feature # 122: Optionally require TSIG signatures for zone transfers

Status:	New	**Priority:**	Normal
Author:	halleck	**Category:**	
Created:	2014-02-15	**Assigned to:**	
Updated:	2017-09-20	**Due date:**	
Subject:	Optionally require TSIG signatures for zone transfers		
Description:	Now that PowerDNS appear to support TSIG it would be nice to have it as an optional requirement for zone transfers. http://doc.powerdns.com/html/tsig.html		

History

2016-06-06 03:52 - halleck

Ok, time for a quick BIND tutotal, that now being what is running on a.authns.

TSIG signatures are based on a shared secret, and are used both to authenticate zone transfers as well as to protect the integrity of the zone transfer.

One way to generate is properly formated secret is to use the BIND dnssec-keygen tool.

```
dnssec-keygen -r /dev/urandom -a hmac-sha256 -b 256 -n HOST bitfolk-example
```

This will generate two files, _Kbitfolk-example.+163+*.key_ and _Kbitfolk-example.+163+*.private_; both containing the shared key.

The Secondary server will need two pieces of configuration; one which specifies the key, and one which specifies for which (master) ip address the key should be used.

```
key bitfolk-example {
    algorithm hmac-sha256;
    secret "lgCopLqhGqk12p2BdW3yKi+pJyExRznYJH6/nLfTVhA=";
};



server 2001:DB8::53:2 {
    keys { bitfolk-example; };
};
```

...where _bitfolk-example_ is the name of the key and _2001:DB8::53:2_ is the ip address of the DNS master. Note that the name of the key matters to the extent that both the Master server and the Secondary server need to use the same name.

2016-06-06 03:57 - halleck

The Master server is configured with the same _key_ directive as well as the equivalent _server_ directive. Then there are the _zone_ directives, which specifies keys rather than ip addresses for _allow-transfer_.

```
zone "example.net" {
    ...
    allow-transfer{ key "bitfolk-example"; };
    ....
};
```