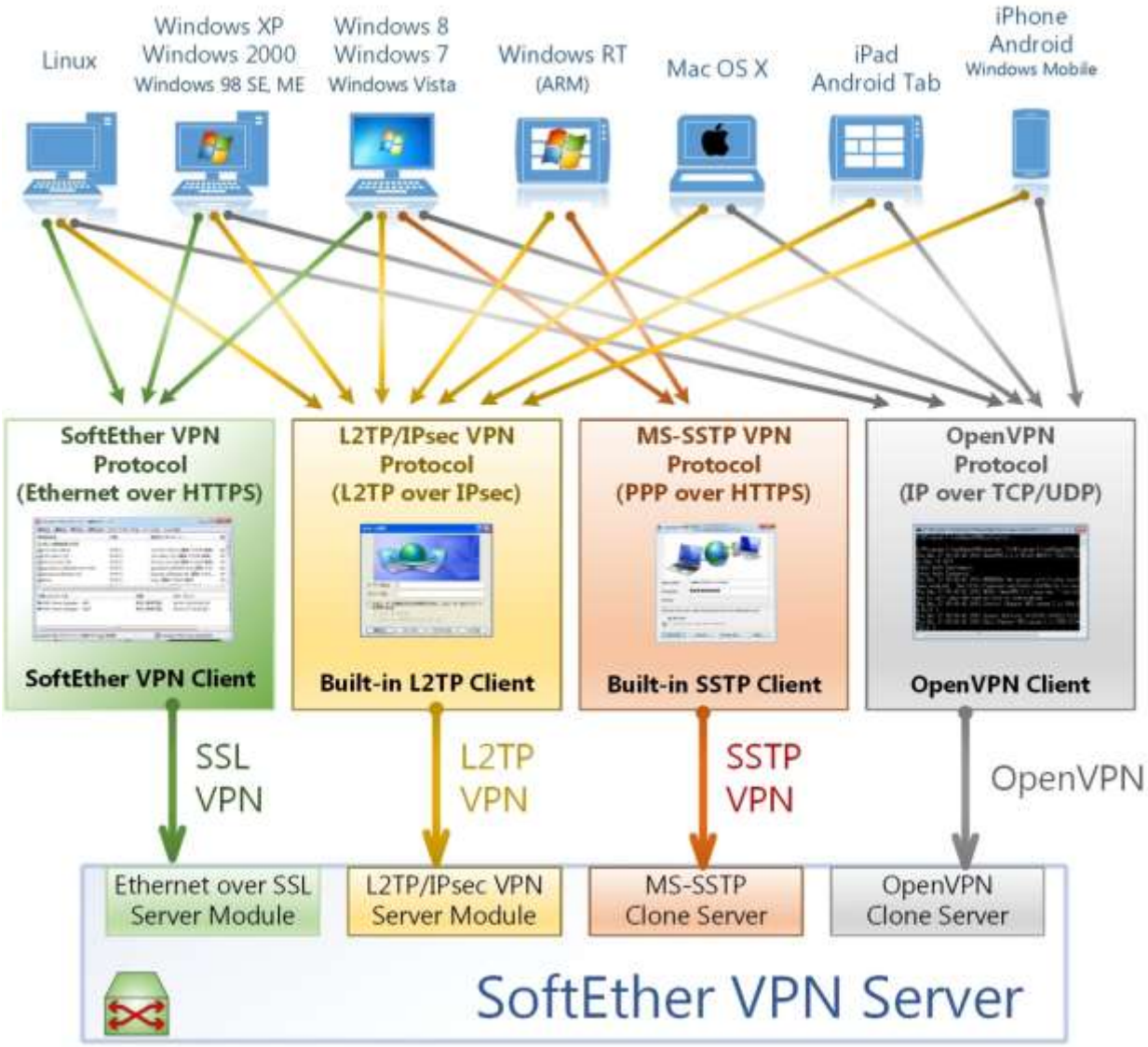
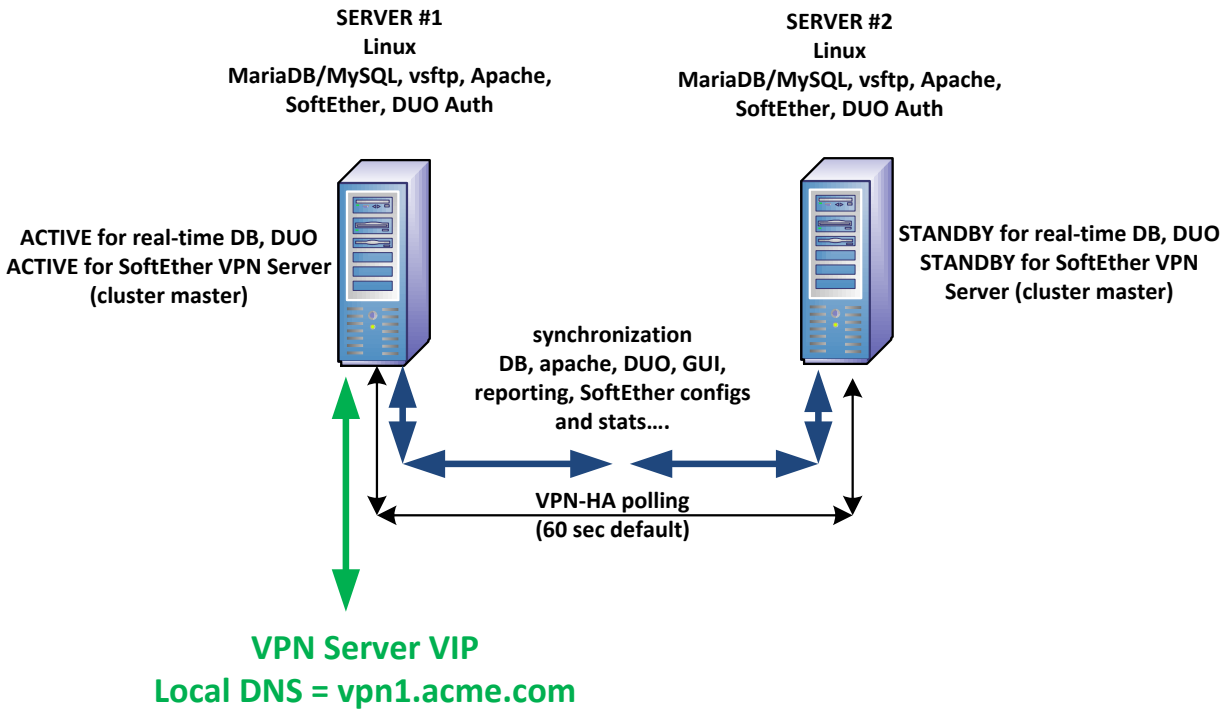
Basic SoftEther VPN Server Benefits - Work from Home / Remote Access Solutions

- SoftEther OPEN-SOURCE = no license fees
- AES-256 and RSA 4096 encryption
- >1Gbps throughput per server
- IPv4 and IPv6
- Excellent GUI
- 4096 session support per server
- Load balancing using clusters (up to 64 servers in cluster)
- Fault tolerance and high availability solutions for remote access and WFH
- Full specification of protection for DoS
- Very flexible multi-protocol VPN and security policies
- Support for multi-factor authentication
- Good solid testimonials

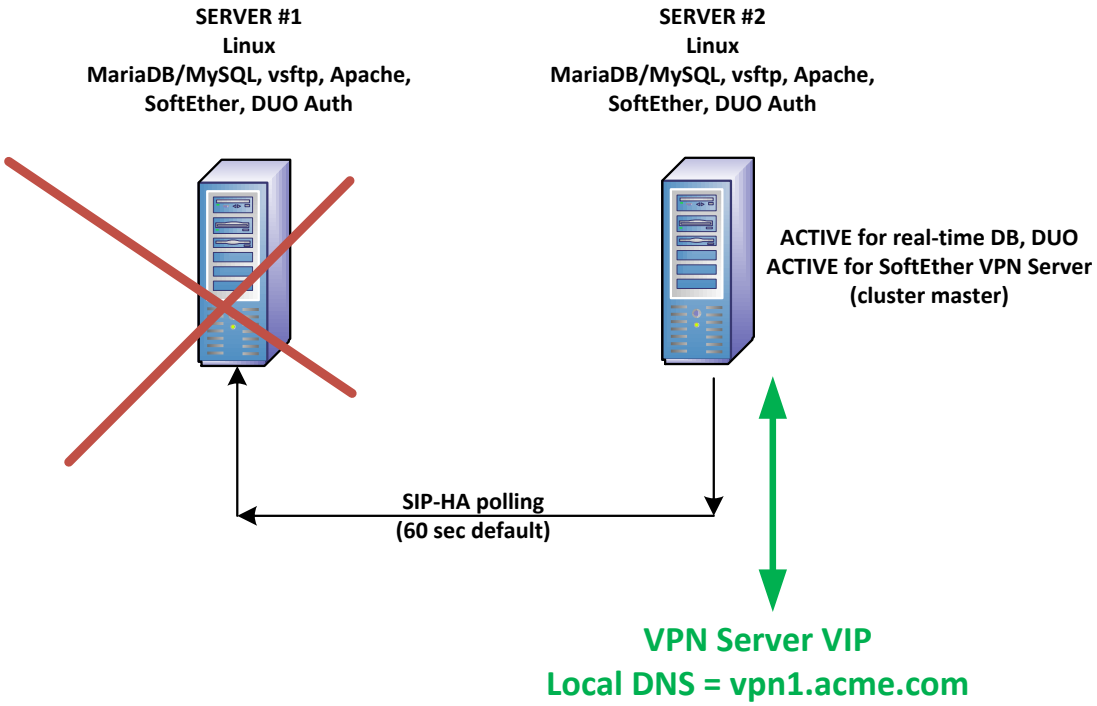


High Availability Provisions

- Very scalable (HA pair to 64 server cluster)
- Realtime failover and reporting
- Flexible public facing {DNS SRV, VRRP, VIP, NAT}
- Flexible inside DMZ connectivity
- IPv4 and IPv6
- Auto replication of databases, VPN Server configuration and http systems
- OSSEC, SNMP and email notification/support
- Support for complex PCI or FIPS compliance
- VM support



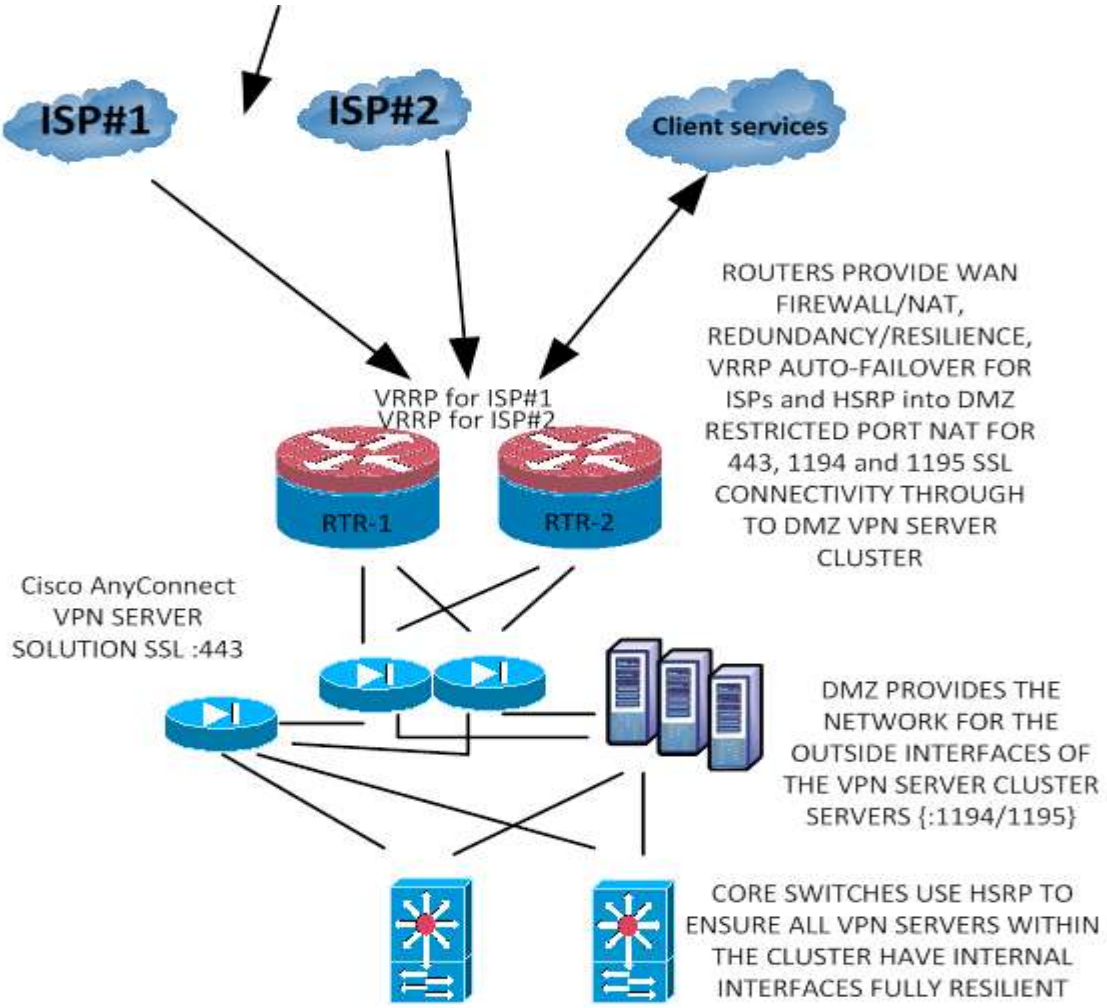
simple two server example



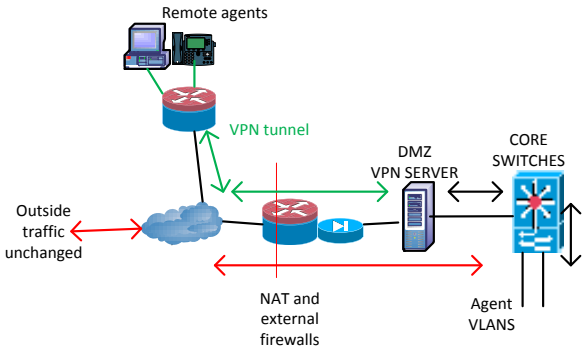
during any server, interface or software issues the second server becomes active

{server can be one of HA-pair or one of HA-pair of cluster controllers}

example integration in typical enterprise network



Minimum disruption and change required to existing network as the remote access uses the existing VLANs and ip networks = no changes to ACLs, Firewalls and routing



Remote agents are automatically allocated a DHCP address and routing configuration for their agent-group. The address will be within the agent group defined on the core switches, so that all services available within the main site will then be available for the remote agent. Outbound traffic will have the usual agent-group source address so that there are no changes required in any of the firewalls, ACLs and routing. Inbound traffic will also be routed through the core switches and onto the agent-group VLANs where they are routed back through the vpn server and to the remote agent PC.

The remote user can obtain the VPN-client application by browsing to the VPN sever using HTTPS {1194} this will allow the user to download the latest VPN client and then install on the local PC.

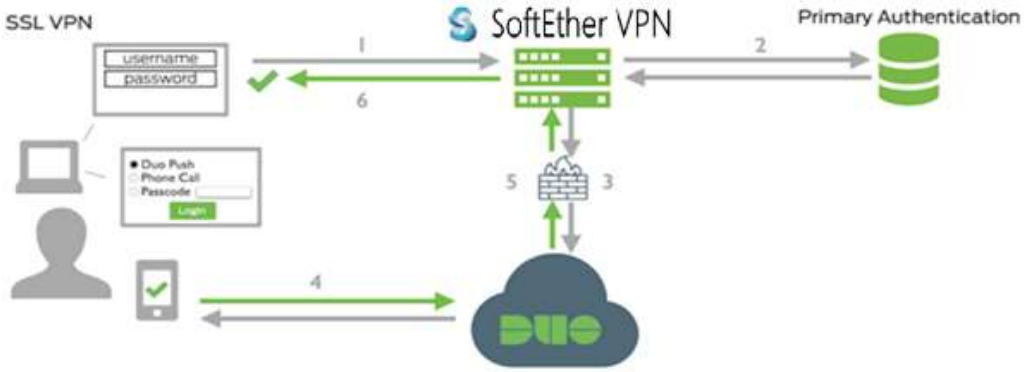
NOTICE – for maximum security and FIPS compliance, the WAN access database can be hosted on a different server from the SoftEther VPNServer. There can be 4 independent stages to secure the access to the client applications;

1 **WAN-Access** authentication of a username and password to initiate DUO
2 **DUO authentication** of a username and password with multi-factor options
3 **SoftEther authentication** of a username, group and password for VPN access
4 **Enterprise application authentication** of a username and passwords to access the applications

Each username/password/group combination can be independent and reside on different servers and databases OR can be synchronised to match the required security levels. The SoftEther VPNServer can make use of independent database or make use LDAP/RADIUS/CA security authentication options.

SoftEther user configuration allows users to be configured with or without DUO authentication.

Access can also be configured for less-secure applications using fewer combinations of authentication.



1 user login is performed to the secure browser using SSL
2 username and password verified on VPN Server WAN-Access database
3 API creates request for the user if the password is authenticated
   a. DUO alerts the user with a choice of communication methods
   b. User receives request on smartphone (push) or phone call (passcode) etc.
4 User acknowledges on smartphone
5 DUO verifies the response from approved source and username/password
   a. API send approval hash to server
   b. VPN server enables username VPN provision
6 User connects to VPN server using the vpn client

OPS will have to maintain the user authentication databases, administer the DUO multi-factor authentication user database and monitor the logs from each user group.

PCI v3 compliance is satisfied with the use of DUO and SoftEther independent database method as part of the multi-factor authentication process. Security logs are extensive and can be customised for the monthly PCI internal audits.

{see document showing the DUO authentication process for details on the options and screens seen during the initial and subsiquent user login attempts - ops need to be familiar with the process}

HIGH AVAILABILITY ROUTINES

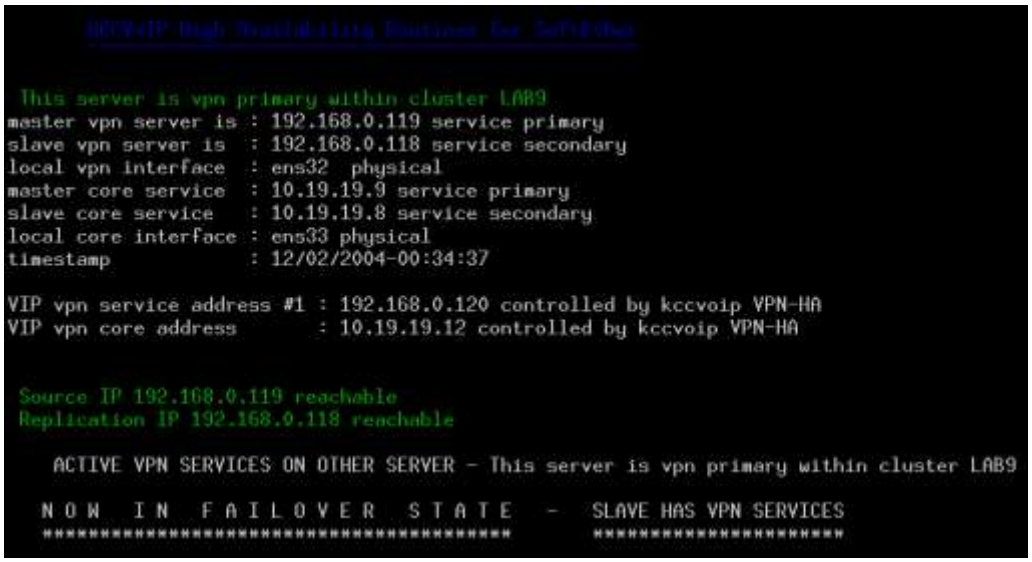
Customised command line scripts and OPS-GUI control and monitor the status of the HA-pairs of cluster controllers or pairs of non-cluster servers

```
       KCCVoIP High Availability Routines for SoftEther


 This server is vpn primary within cluster LAB9

master vpn server is : 192.168.0.119 service primary
slave vpn server is  : 192.168.0.118 service secondary
local vpn interface  : ens32  physical
master core service  : 10.19.19.9 service primary
slave core service   : 10.19.19.8 service secondary
local core interface : ens33 physical
timestamp            : 04/22/2020-10:56:53

VIP vpn service address #1 : 192.168.0.120 controlled by kccvoip VPN-HA
VIP vpn core address       : 10.19.19.12 controlled by kccvoip VPN-HA


 Source IP 192.168.0.119 reachable
 Replication IP 192.168.0.118 reachable

 ACTIVE VPN SERVICES ON THIS SERVER
  - This server is vpn primary within cluster LAB9
    - NOW IN NORMAL STATE -


 VPN-HA will replicate local vpn files to 192.168.0.118

sending incremental file list
vpn_server.config
```

Command line example showing HA status

example shows failure of primary server in the high-availability pair – during any interface and/or server issues the secondary server takes over all active services. When the primary server is back online, the secondary continues to be the main active server for all services and replicates the database and configuration to the standby servers until the operators make the switch back to primary server.

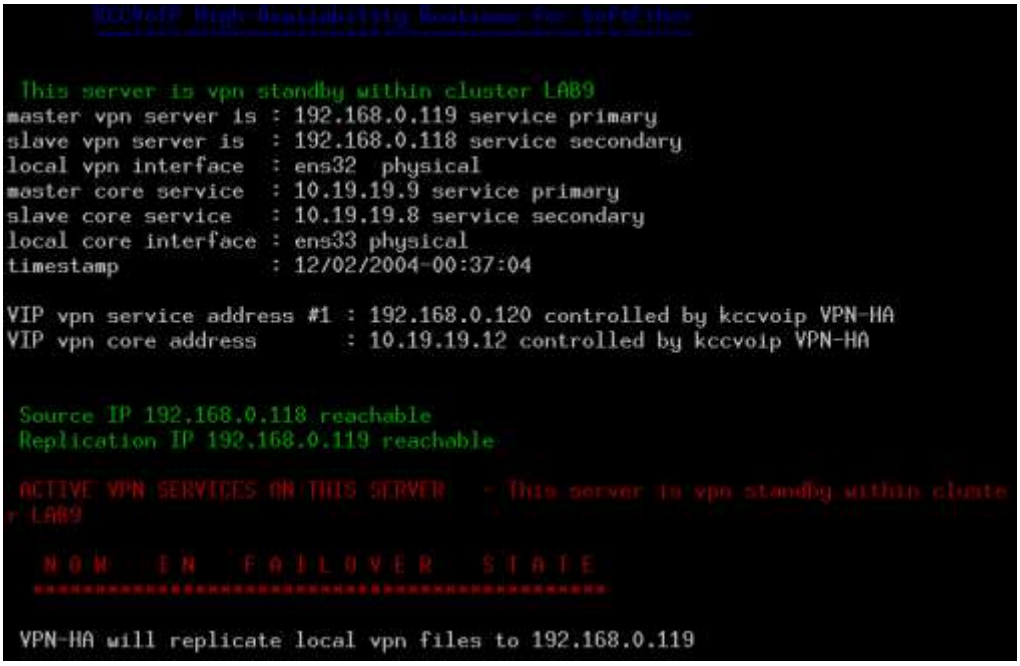
example command line during failover



During normal operation, the primary server will replicate database and configuration files to the standby servers so that they are always ready to take over during any issues.

Any SoftEther changes and additions are automatically maintained on all servers within the cluster.

Additional servers can be added to the cluster at any time to increase capacity and provide load balanced VPN service. Cluster controllers ONLY have the database replication and multi-factor {eg DUO} configuration - cluster members only need the SoftEther configuration.



DETAILED CONFIGURATION

{site = details to be documented}

SITE =

DMZ primary server =

DMZ secondary server =

DMZ VIP for VPN Server =

CORE SERVICE primary =

CORE SERVICE secondary =

VIP for CORE service =

CLUSTER MEMBERS =

PUBLIC ADDRESS ISP#1 VIP =

PUBLIC ADDRESS ISP#1 routers =

PUBLIC ADDRESS IPS#2 VIP =

PUBLIC ADDRESS ISP#2 routers =

PUBLIC DNS SRV GROUPS =

{drawing to show all details in here}