# DNS for Small Networks

Small networks typically do not require a dedicated internal DNS server. An external DNS server (often located at an ISP) can be used for address resolution on an External Network. If some internal hosts need to be referenced by name (for TCP/IP services), the use of a local "host file" on client systems may be utilized. The host file name and location vary depending upon the operating system. Host file locations for some common systems are:

- Windows 95/NT /Windows/Hosts
- Macintosh System Folder/Mac TCP DNR
- Unix/Linux /etc/hosts

***Note***

Sample host files are typically provided with these operating systems.

# Split DNS for Larger Networks

If DNS is used on a larger network, Split DNS can be used, with one server for users on the Protected Networks, and one for users on External Networks.

In Split DNS, an internal DNS server on the Protected Network makes DNS information available to the Protected Network and provides address resolution of the internal network addresses for external and internal hosts. Information about a PSN may also be provided for use by Protected Network hosts. (PSN hosts would not have access to this server unless you created a tunnel to a Protected Network from a PSN on port 53/UDP).

A separate DNS server is used to provide DNS information for users on an External Network. This external DNS server can reside anywhere that is accessible by external users: at your Internet Service Provider, on an external host (in the case of an intranet), or often on the PSN with Tunnels on port 53 for both TCP and UDP.

## Dual DNS

If Split DNS is desired, but the resources for two DNS servers are not available, a Dual DNS configuration can make it is possible to operate two separate DNS servers on the same host. As most DNS servers run on hosts using Unix or a Unix-like system such as Linux, this addresses only a Unix configuration.

The objective is configure system located on a PSN to provide name resolution about your domain for users on the External Network, and to provide DNS services for internal users on Protected Networks and PSNs.

### Internal DNS Server

Configure the host on the PSN as a normal DNS server, using your hidden/unregistered IP addresses. Your internal domain will most likely include at least two sets of networks (IP addresses from a Protected Network as well as from a PSN). The DNS server will typically contain information for hosts on a PSN, such as web and FTP servers (using their unregistered IP addresses).

Internal users should reference the host on a PSN as their DNS server to resolve all local addresses and external addresses. If an external address needs to be resolved, and that information does not reside in the DNS server's cache, a lookup on an External Network will be performed transparently.

### Configure an External DNS Server

List the domain's name server as a specific IP address for users from the Internet to reference DNS information about the domain, different from the IP address referenced by internal users.

Create a new directory for the external DNS server, e.g., `/etc/namedb2`

In the new directory, create the DNS domain and reverse lookup files. Only registered IP addresses should appear in these files. The IP addresses for email, web, FTP and DNS servers will be either an External Network interface IP address or IP alias, assuming tunnels have been created for these services.

In the **/etc** directory, create an additional DNS boot file (`/etc/named.boot2`) for your external DNS server. This file should be created as a normal "named.boot" file, yet reference files in the external DNS directory (`/etc/namedb2`).

In the appropriate **.rc** file, add an additional entry to start up a copy of the DNS server, typically called "`named`." This copy of the DNS server should be invoked with a port parameter of 54 (`-p 54`) and an alternative boot file name (`-f /etc/namd.boot2`).

Create two tunnels on the GTA Firewall for the external DNS server: one for DNS lookups (UDP/53) and one for zone transfers by a secondary DNS server (TCP/53). These tunnels should have the source side set for port 53 and the destination set for port 54.

Finally, create Remote Access Filters which will allow the tunnels to be accessed by the appropriate users, either by defaulting the filter set or by manually creating the appropriate filters.

#### GTA Firewall DNS Configuration Example

```
EXT: 199.120.225.2

PRO: 192.168.2.2

PSN: 192.168.3.2

DNS Server 192.168.3.20
```

#### Tunnels

```
UDP 199.120.225.2 53 192.168.3.20 54

TCP 199.120.225.2 53 192.168.3.20 54
```

#### Remote Access Filters

```
1. Allow DNS lookups from the Internet

Accept UDP EXT

From: 0.0.0.0/0.0.0.0 53

To: 199.120.225.2/255.255.255.255 53

2. Allow DNS zone transfers by our secondary

Accept TCP EXT

From: 204.96.116.2/255.255.255.255

To: 199.120.225.2/255.255.255.255 53
```