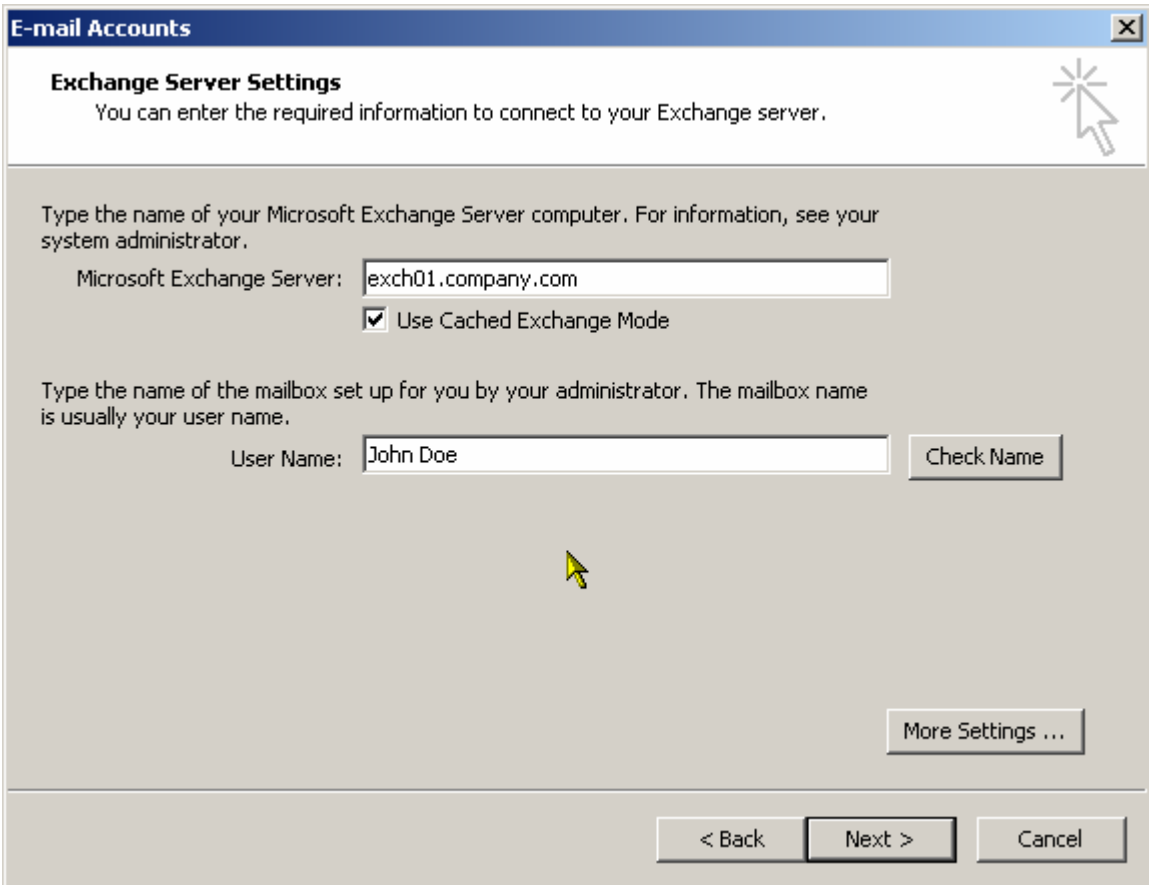
How to Configure Split DNS

Split DNS is a concept that allows a hostname to resolve to one IP address on the internal network, and another on the external network. An example is the G/On Server if it is to be used both internally and externally. If the hostname of the G/On Server is gon.company.com it might resolve to 10.0.0.10 on the internal network and 80.200.100.10 on the external network. The external IP address will then be Network Address Translated (NAT) through the firewall to the internal IP address of 10.0.0.10.

Any application client (like Outlook) that uses a hostname to connect to an application server (like Exchange) must be able to resolve this hostname to the loopback address 127.0.0.2 when connecting through G/On. This is because G/On uses the loopback interface to direct all traffic through the encrypted connection between the G/On Client and the G/On Server.

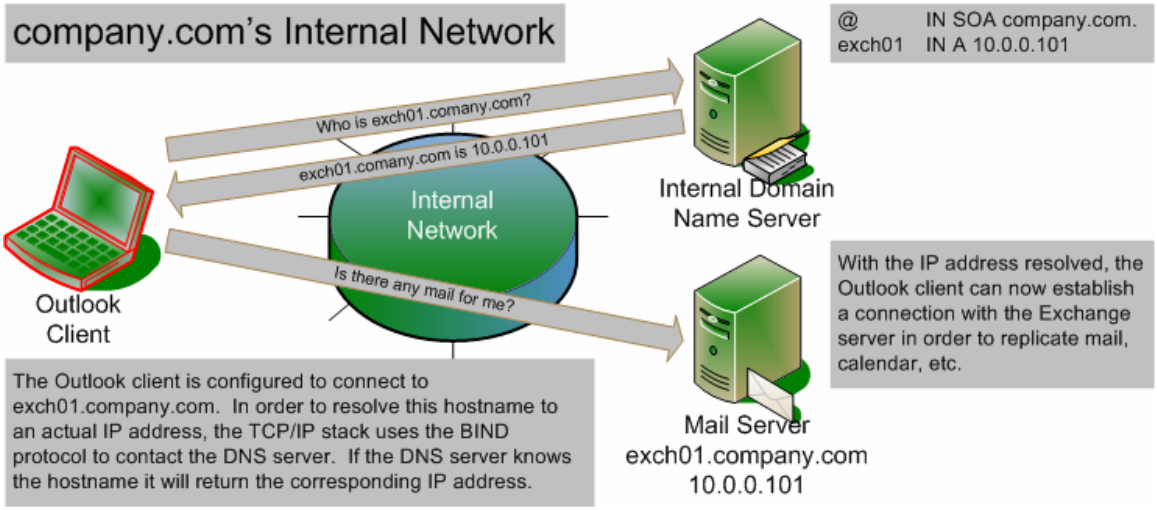
Outlook Client Setup

An example is an Outlook client that connects to an Exchange server using a hostname. If the hostname is exch01.company.com for user John Doe, the Exchange server settings will look as follows.

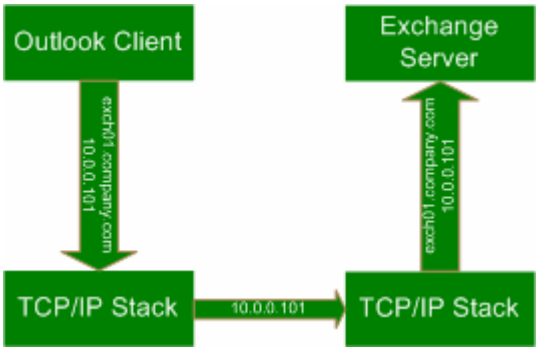


Internal DNS

The resolution of the hostname exch01.company.com to the IP address 10.0.0.101 and the subsequent connection between the Outlook client and the Exchange server will be accomplished as follows.

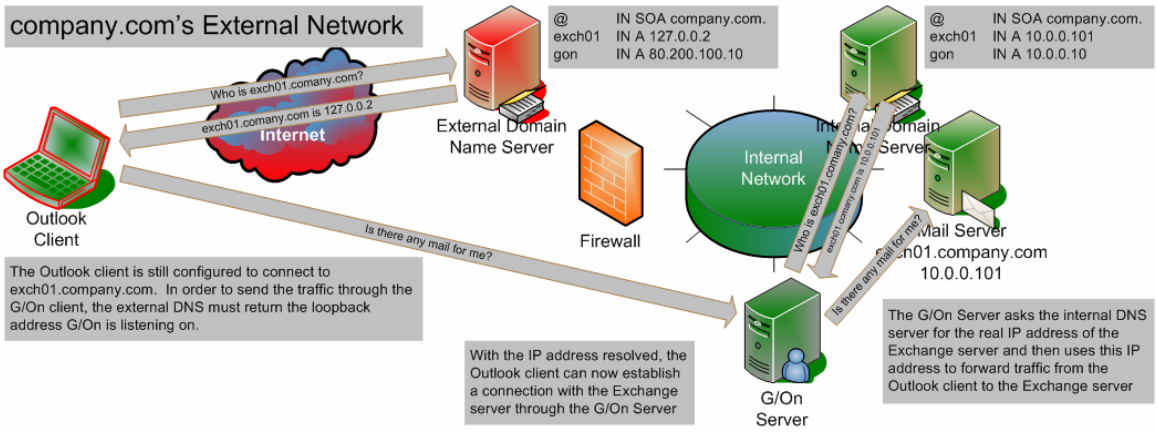


Since both the Outlook client and the Exchange server are on the same network, the Outlook client can easily resolve the hostname exch01.company.com to the correct IP address of 10.0.0.101. This results in the traffic flow below.

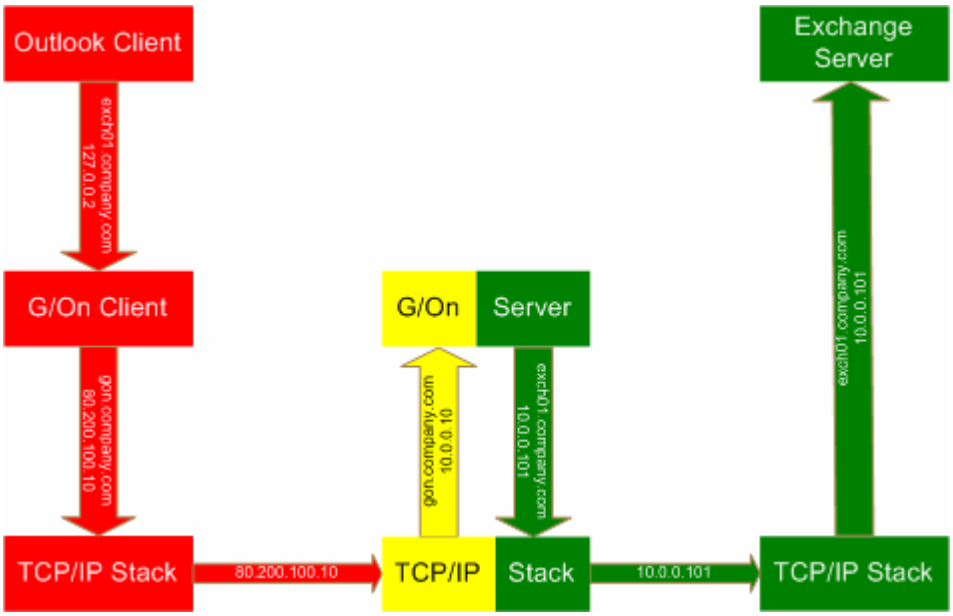


External DNS

When the Outlook client needs to connect through G/On, the connection can no longer be established directly to the Exchange server's internal IP address. Instead, the hostname exch01.company.com should now resolve to the loopback address the G/On Client is listening on. This requires that the external Domain Name Server resolves exch01.company.com to 127.0.0.2.



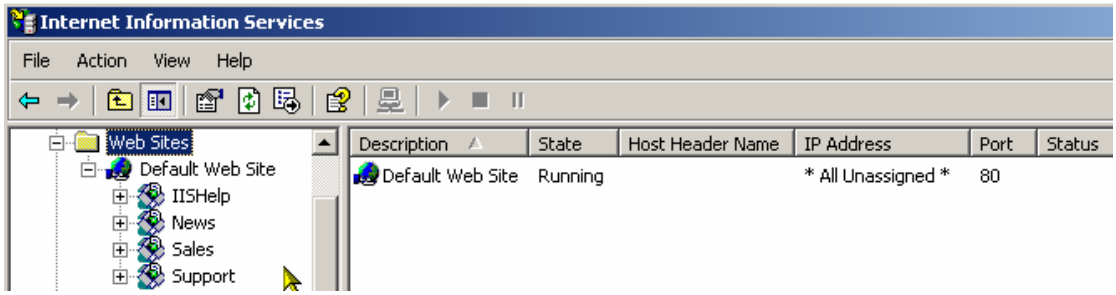
Since the Outlook client and Exchange server no longer are on the same network, the connection is now established through the connection between the G/On Client and the G/On Server. This results in the traffic flow below.



Web Server Access

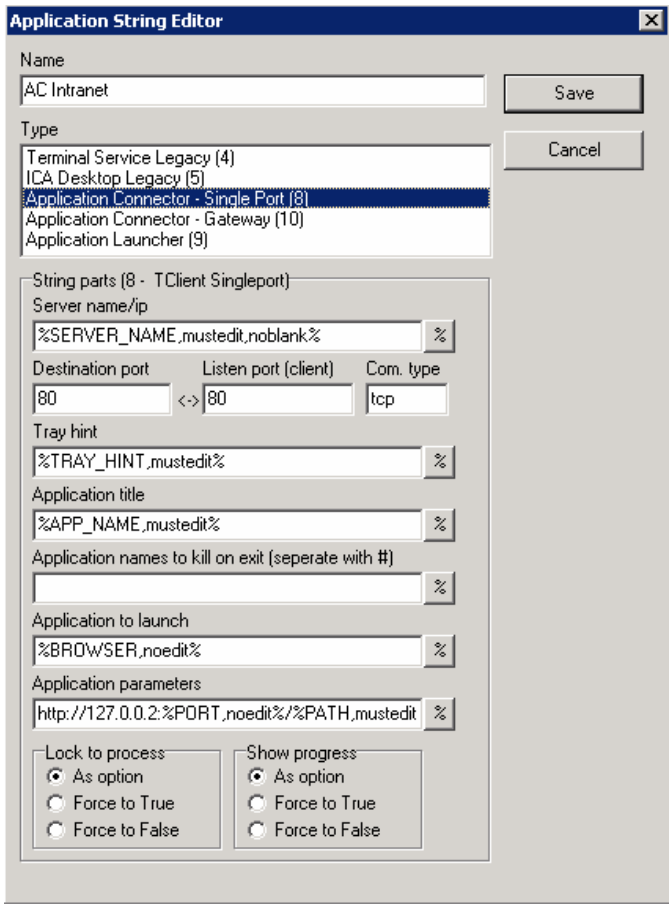
Another scenario where Split DNS sometimes is needed is Web Server access. If each website is on a separate web server, then Split DNS is not needed because the URL can be configured to go through the G/On Client by specifying http://127.0.0.2/

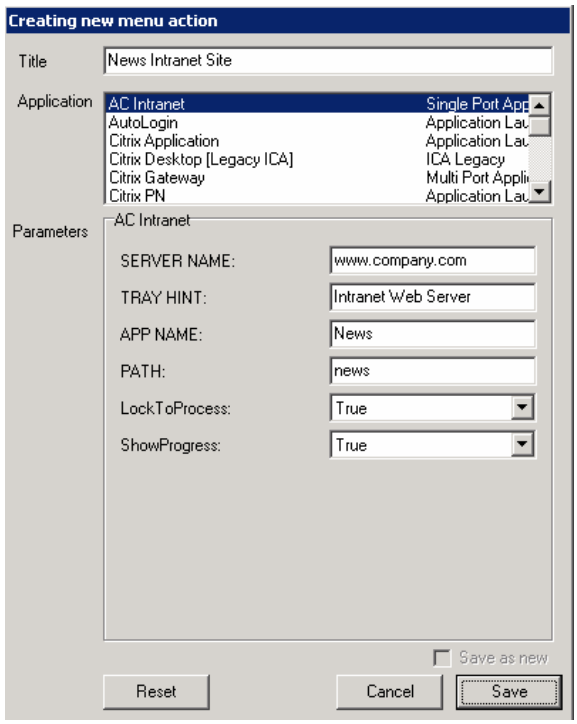
If several websites exists on one web server, it may be necessary to use Split DNS depending on how the web server is configured. If you have the following setup for www.company.com:



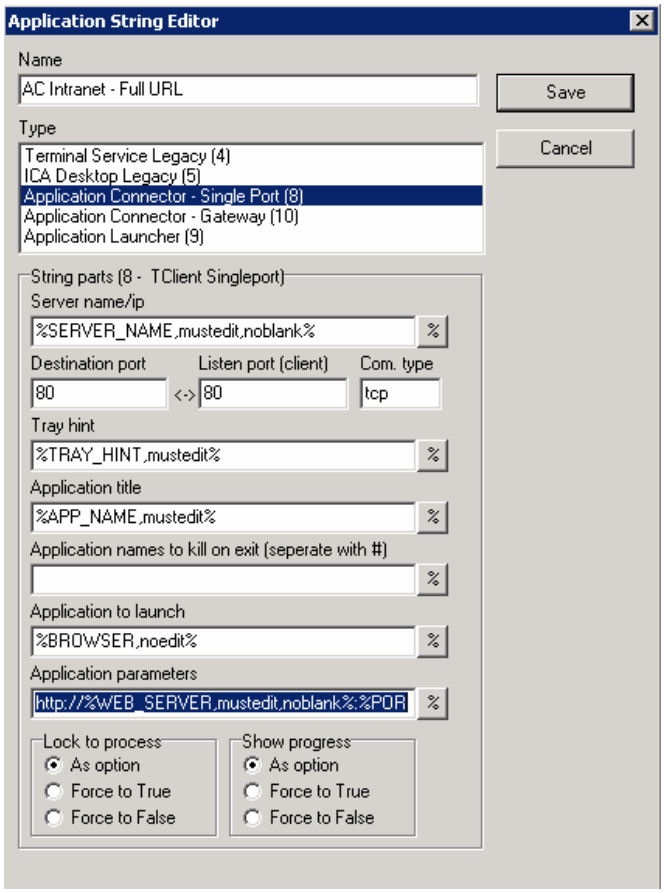
Then there are two different ways of accessing these websites either as http://www.company.com/news or http://news.company.com

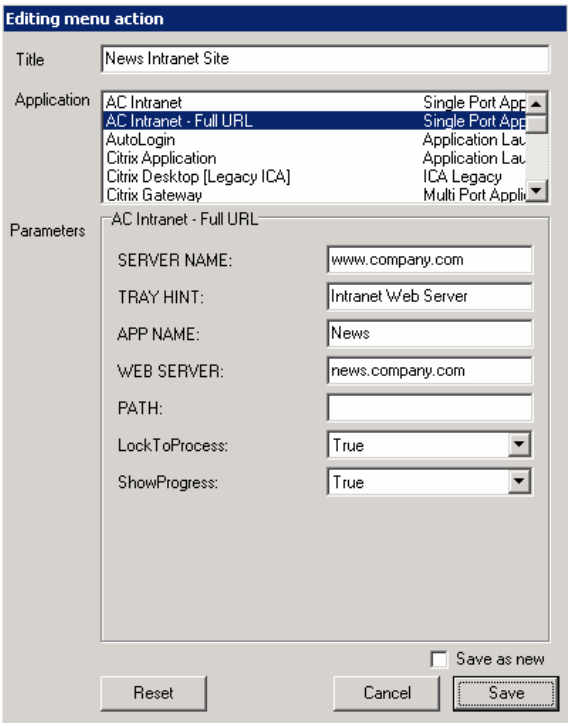
In the first scenario, G/On can be configured to connect to http://127.0.0.2/news and Split DNS is not needed.





In the second scenario G/On must be configured to connect to http://news.company.com which would require an external DNS to resolve news.company.com to 127.0.0.2.





DNS Configuration

In the above examples, the external DNS would be configured as follows:

```
@         IN SOA     company.com. support.isp.com. (
                     2007042401 ;serial
                     3600       ;refresh
                     300        ;retry
                     3600000    ;expire
                     86400      ;minimum
                     )
          IN NS      ns1.isp.com.
;
gon       IN A       80.200.100.10
exch01    IN A       127.0.0.2
www       IN A       127.0.0.2
news      IN A       127.0.0.2
sales     IN A       127.0.0.2
support   IN A       127.0.0.2
```

And the internal DNS would look as follows:

```
@         IN SOA     company.com. root.company.com. (
                     2007042401 ;serial
                     3600       ;refresh
                     300        ;retry
                     3600000    ;expire
                     86400      ;minimum
                     )
          IN NS      ns1.company.com.
;
gon       IN A       10.0.0.10
exch01    IN A       10.0.0.101
www       IN A       10.0.0.102
news      IN CNAME   www
sales     IN CNAME   www
support   IN CNAME   www
```

Security Concerns

The DNS server should be configured not to divulge the contents of the domain to anyone except the secondary DNS for the domain. This prevents a potential attacker from dumping the contents of the domain.

named.conf Example

```
#
# named.conf file for company.com master server
#
acl dns-slaves {
    80.200.100.6;
    80.100.100.3
};
options {
    directory "/etc";
    allow-transfer { dns-slaves; localhost; };
};
zone "company.com" in {
    type master;
    file "company.data";
};
zone "100.200.80.in-addr.arpa" in {
    type master;
    file "company.rev";
};
zone "0.0.127.in-addr.arpa" in {
    type master;
    file "company.local";
};
```

Loopback Hacking

Should an attacker manage to find out that the company.com domain contains a host called exch01 and the attacker decides to scan this server, what really happens is that the attacker will scan his/her own PC because the returned IP address corresponds to the attacker's own loopback interface.