Application Note

SIP Domain Management

28 March 2008

Table of Contents

Tested versions: Ingate Firewall/SIParator/MEDIAtor version 4.6.2

Revision History:

Revision	Date	Author	Comments
1	2008-03-28	Scott Beer	1st Release

1 What is a SIP Domain?

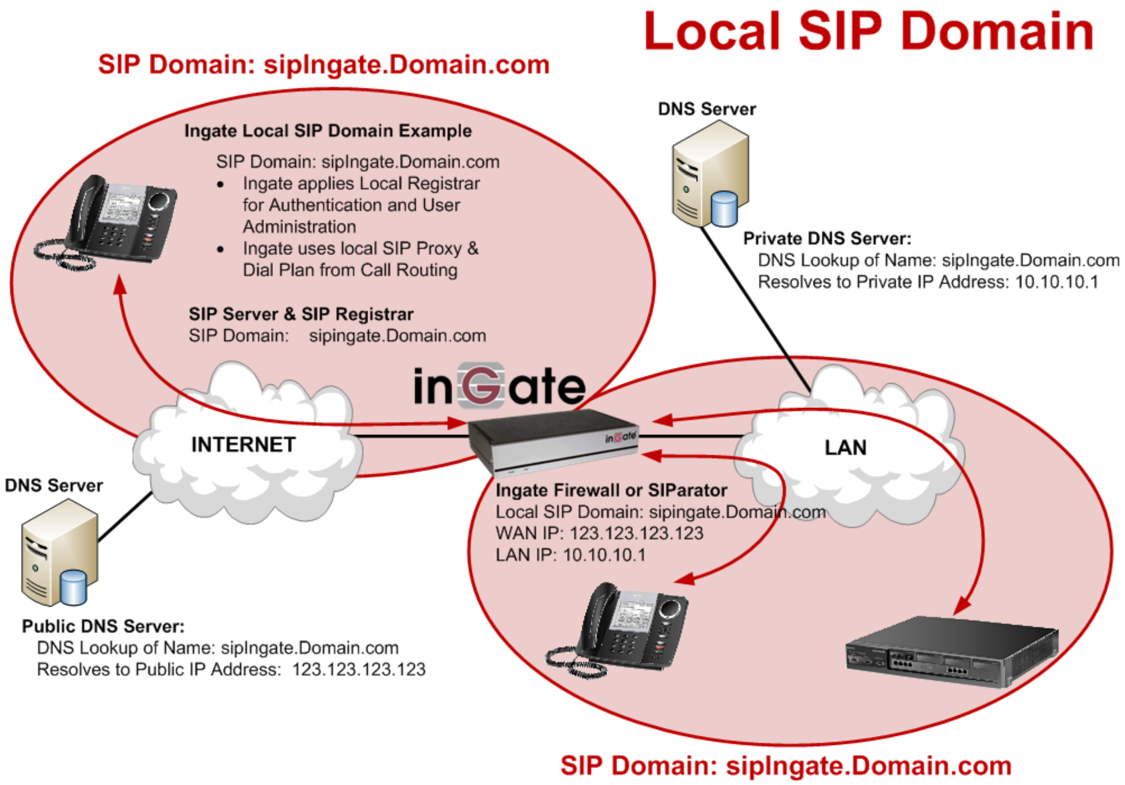
A SIP Domain is the distinguished part of an abstract or physical space where SIP devices exist, where they perform communication between each other, and are valid or authorized for communication. For example, the domain of SIP activity implies there is communication between SIP devices within the domain. The SIP domain may be the same or different then the domain for Web activity.

The most common types of domain names are hostnames that provide more memorable names to stand in for numeric IP addresses. They allow for any service to move to a different location in the topology of the Internet (or an intranet), which would then have a different IP address.

By allowing the use of unique alphabetical addresses instead of IP addresses, domain names allow Internet users to more easily find and communicate with SIP servers, web sites and other server-based services. The flexibility of the domain name system allows multiple IP addresses to be assigned to a single domain name, or multiple domain names to be assigned to a single IP address. This means that one server may have multiple roles, or that one role can be spread among many servers.

2 Local SIP Domain

As it applies to the Ingate products, the term “Local SIP Domain” are domains that the SIP registrar in the Firewall or SIParator should handle. Thus the Ingate is responsible for providing registration and authentication to SIP clients attempting to register with a SIP Server. These SIP clients will also send SIP Requests to the Local SIP Domain for the Ingate to process and direct using the Ingate SIP Proxy capabilities.

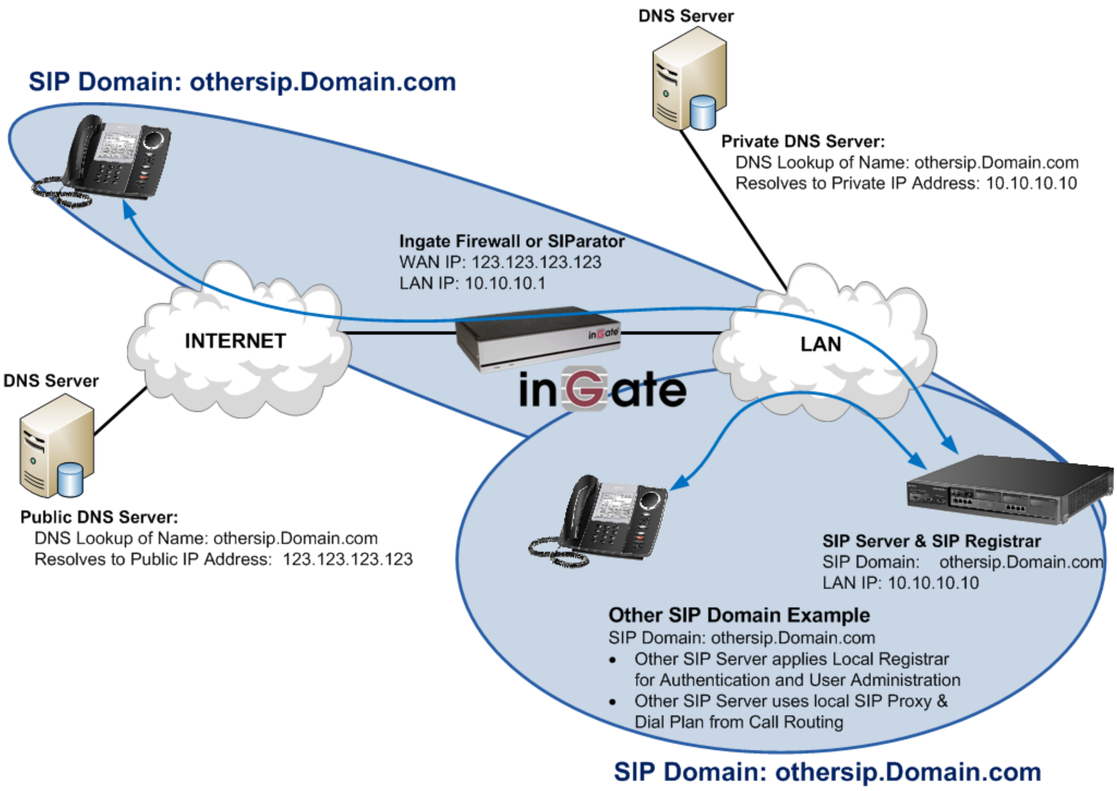


Local SIP Domain
SIP Domain: sipIngate.Domain.com
Ingate Local SIP Domain Example
SIP Domain: sipIngate.Domain.com
• Ingate applies Local Registrar for Authentication and User Administration
• Ingate uses local SIP Proxy & Dial Plan from Call Routing
SIP Server & SIP Registrar
SIP Domain: sipingate.Domain.com
inGate
INTERNET
DNS Server
Public DNS Server:
DNS Lookup of Name: sipIngate.Domain.com
Resolves to Public IP Address: 123.123.123.123
DNS Server
Private DNS Server:
DNS Lookup of Name: sipIngate.Domain.com
Resolves to Private IP Address: 10.10.10.1
LAN
Ingate Firewall or SIParator
Local SIP Domain: sipingate.Domain.com
WAN IP: 123.123.123.123
LAN IP: 10.10.10.1
SIP Domain: sipIngate.Domain.com

3 Other SIP Domain

Other SIP Domains are domains not handled by the Ingate products. Upon receiving a SIP Request for another SIP domain, the Ingate determines the location (by various means) of the other domain and sends the SIP Request along. Typically, DNS Lookups are used to determine the location of the other SIP Domains.

Other SIP Domain


DNS Server
SIP Domain: othersip.Domain.com
INTERNET
LAN
DNS Server
ingate
SIP Domain: othersip.Domain.com

Private DNS Server:
DNS Lookup of Name: othersip.Domain.com
Resolves to Private IP Address: 10.10.10.10

Ingate Firewall or SIParator
WAN IP: 123.123.123.123
LAN IP: 10.10.10.1

Public DNS Server:
DNS Lookup of Name: othersip.Domain.com
Resolves to Public IP Address: 123.123.123.123

SIP Server & SIP Registrar
SIP Domain: othersip.Domain.com
LAN IP: 10.10.10.10

Other SIP Domain Example
SIP Domain: othersip.Domain.com

- Other SIP Server applies Local Registrar for Authentication and User Administration
- Other SIP Server uses local SIP Proxy & Dial Plan from Call Routing

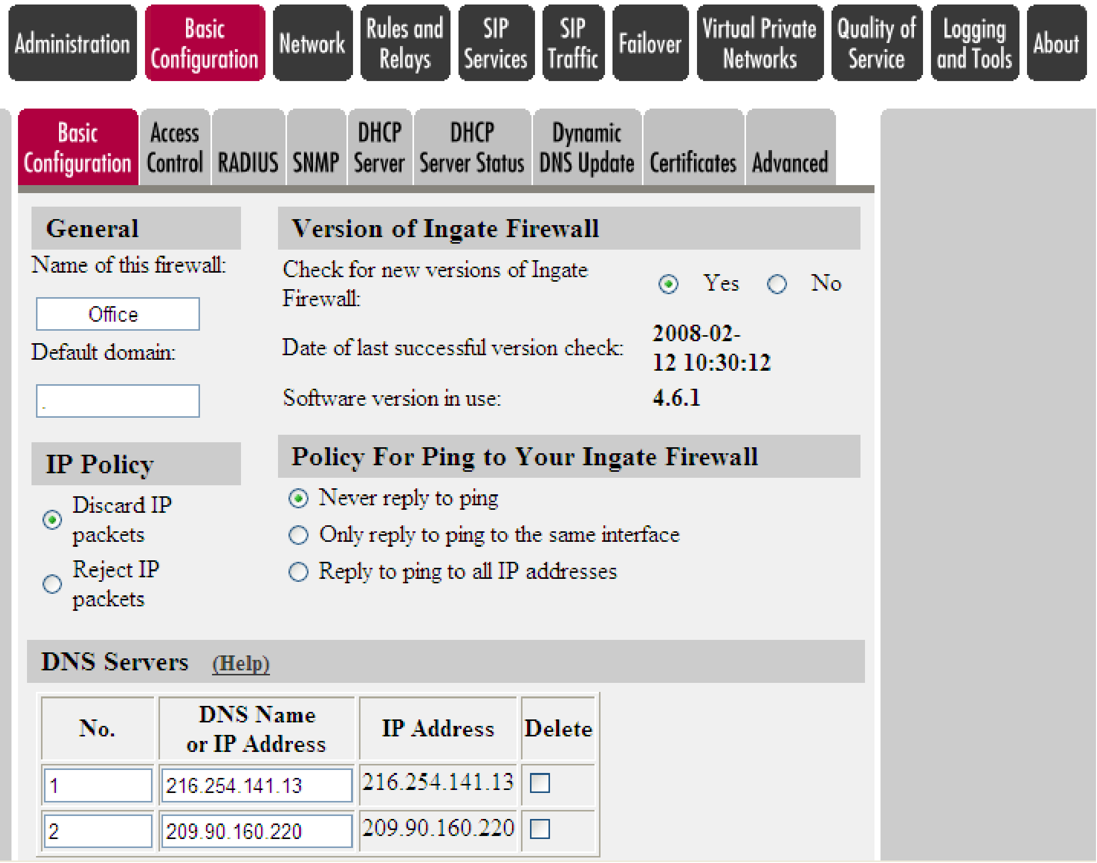
4 DNS Considerations

The Ingate Firewall needs to do DNS query for both incoming and outgoing traffic whenever it encounters a routing-participating header that contains a FQDN. This section highlights the DNS configuration items for a SIP call to get through the firewall from the SIP Servers perspective when using FQDNs with the Ingate Firewall. Please refer to the Ingate reference documentation for more detailed programming instructions.

Configuration Steps:

In the Basic Configuration page:

1. Assign the IP address of the DNS Server, whether a Private internal DNS Server or Public DNS Server.



General

Name of this firewall: Office

Default domain: .

Version of Ingate Firewall

Check for new versions of Ingate Firewall: ● Yes ○ No

Date of last successful version check: **2008-02-12 10:30:12**

Software version in use: **4.6.1**

IP Policy

● Discard IP packets

○ Reject IP packets

Policy For Ping to Your Ingate Firewall

● Never reply to ping

○ Only reply to ping to the same interface

○ Reply to ping to all IP addresses

DNS Servers (Help)

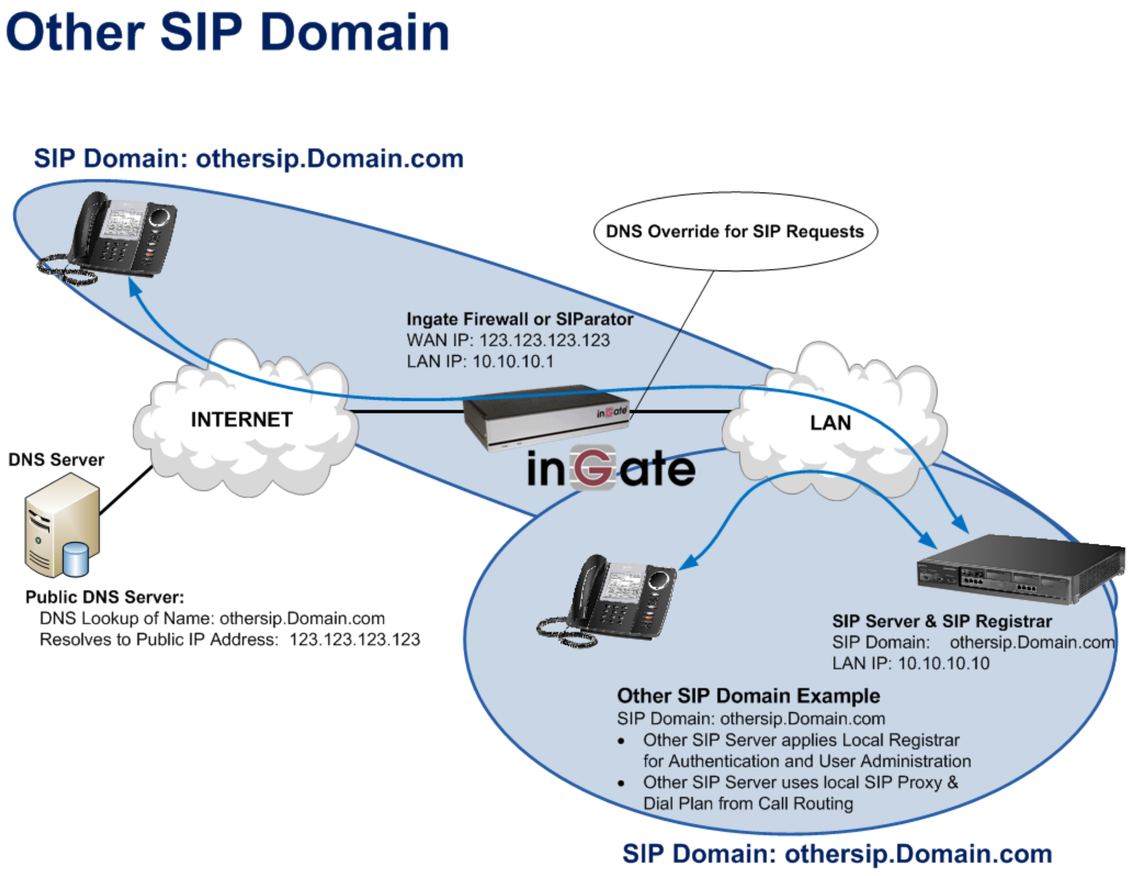
No.	DNS Name or IP Address	IP Address	Delete
1	216.254.141.13	216.254.141.13	□
2	209.90.160.220	209.90.160.220	□

5 Using a Public DNS

In a scenario where the Ingate must only use a public DNS Server, the Ingate Firewall has a table/function to take care of this. This configuration assumes that all DNS servers (regardless of location) in the environment resolve domain names to the same IP addresses (e.g., this is NOT a split-DNS configuration).

The SIP Server is located on a NAT'd network, and DNS queries for the FQDN of the SIP Server should point to the external IP address of the Ingate Firewall. The SIP Server on the LAN should be "authoritative" for that domain name and respond to SIP requests using that name when received. This means that the SIP Server must have a host name and a domain name. These names should be the same as the DNS name of the external WAN port of the Ingate firewall.

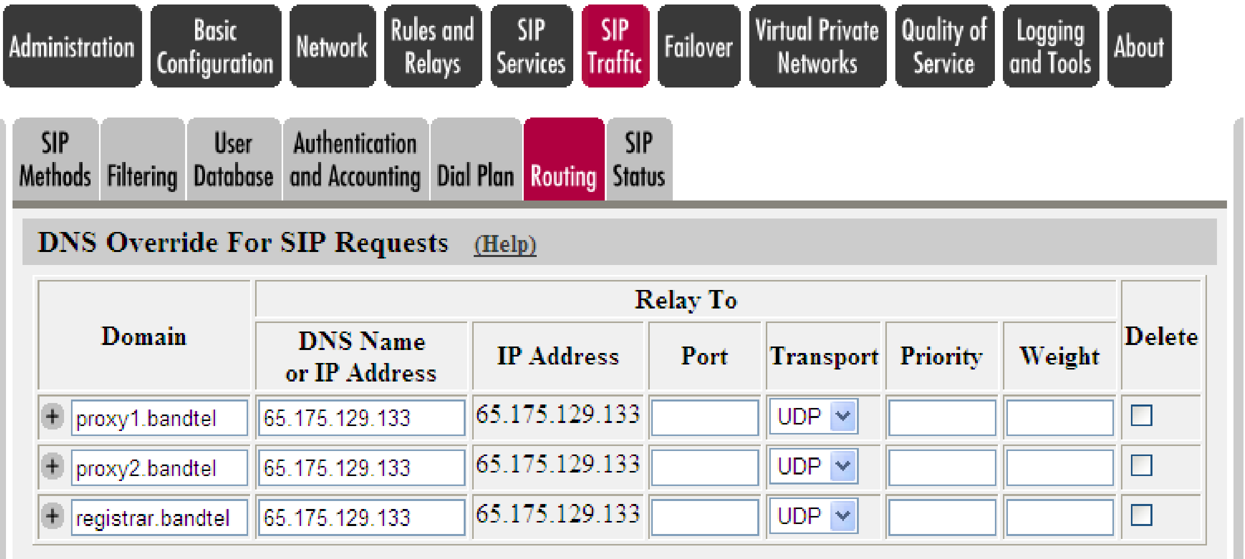
We will use an example of the FQDN "othersip.domain.com", where it publicly resolves to the external WAN IP of the Ingate. If the Ingate received a request for "othersip.domain.com", it would look it up and it would resolve to itself. Therefore, there would be a loop. Instead, under the SIP Traffic > Routing tab, you can use the "DNS Override For SIP Requests" table. There, you can specify that if the Ingate gets a request for a particular domain, the Ingate will not perform a DNS Lookup, the Ingate will send the SIP Request to the IP address and port listed in the table. It is like a static DNS table.


Other SIP Domain
SIP Domain: othersip.Domain.com
DNS Override for SIP Requests
Ingate Firewall or SIParator
WAN IP: 123.123.123.123
LAN IP: 10.10.10.1
INTERNET
LAN
DNS Server
inGate
Public DNS Server:
DNS Lookup of Name: othersip.Domain.com
Resolves to Public IP Address: 123.123.123.123
SIP Server & SIP Registrar
SIP Domain: othersip.Domain.com
LAN IP: 10.10.10.10
Other SIP Domain Example
SIP Domain: othersip.Domain.com
Other SIP Server applies Local Registrar for Authentication and User Administration
Other SIP Server uses local SIP Proxy & Dial Plan from Call Routing
SIP Domain: othersip.Domain.com

Configuration Steps:

In the Routing tab, in the "DNS Override for SIP Requests", enter the following;

1. Domain –Enter the full domain name that you wish to override.
2. DNS name or IP address –Enter the IP Address of UC Server.
3. Port – Enter 5060
4. Transport – Select UDP



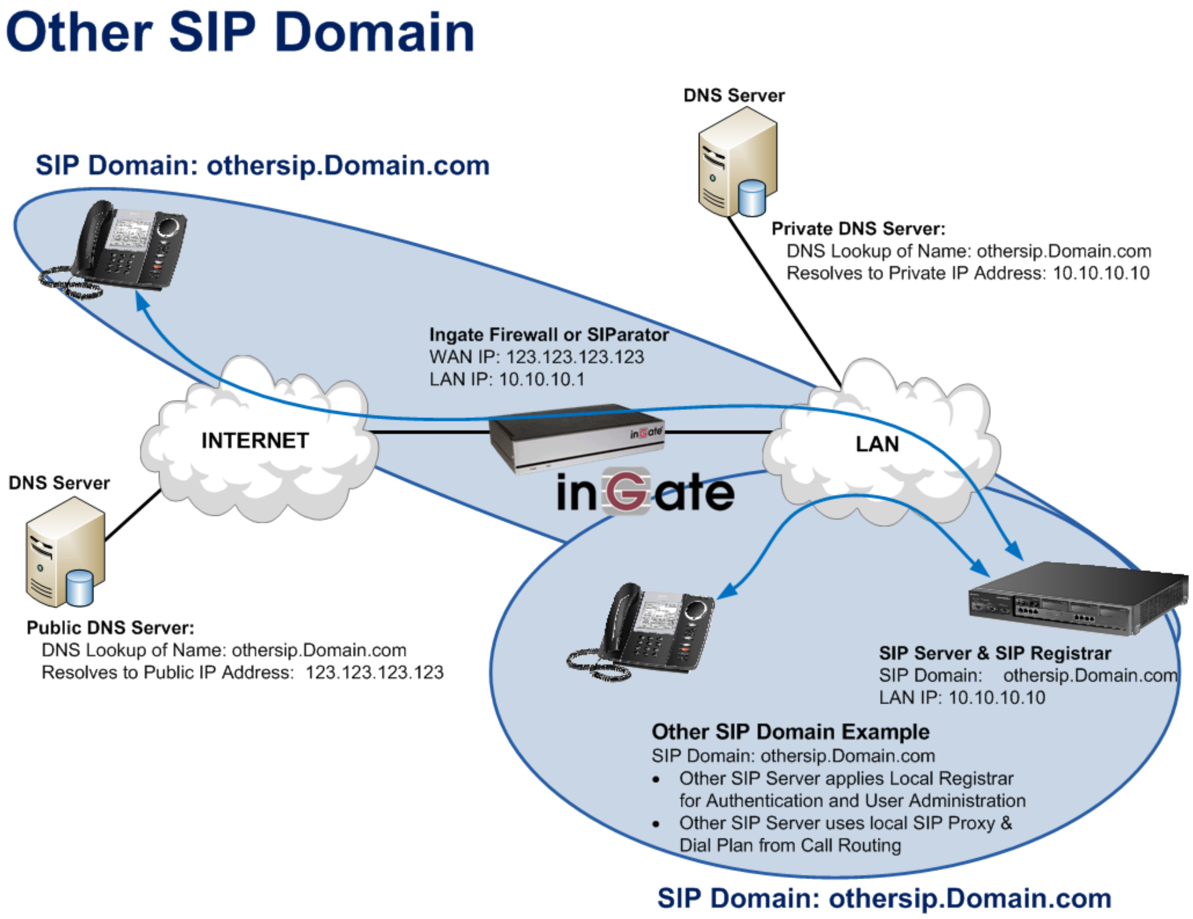
DNS Override For SIP Requests

Domain	Relay To						Delete
	DNS Name or IP Address	IP Address	Port	Transport	Priority	Weight	
+ proxy1.bandtel	65.175.129.133	65.175.129.133		UDP			□
+ proxy2.bandtel	65.175.129.133	65.175.129.133		UDP			□
+ registrar.bandtel	65.175.129.133	65.175.129.133		UDP			□

6 Split DNS Configuration

Another method is for the enterprise site to use a "Split DNS", meaning that they can point the Ingate to an internal DNS server that can resolve domain names differently than they are on a public DNS server. This requires the least configuration on the Ingate. For this method, it is recommended that all DNS queries for FQDNs are always directed to the DNS server on the Intranet side. All FQDN local to the Intranet side must be provisioned on the DNS server on the Intranet side. For outgoing traffic, the firewall needs to perform DNS query for FQDN resolvable on the Internet side. This is also done through the DNS server on the Intranet side that is trusted to an external DNS server. Within the Rules & Relays configuration page of the Ingate Firewall, the DNS Tunneling can be configured.

In the Basic Configuration tab in the Ingate Firewall configuration web page, the IP addresses of multiple DNS servers can be provisioned with each assigned a number. All servers provisioned are ordered according to the number assigned. The DNS server with the lowest number assigned is the first one to be queried. The Ingate firewall will not turn to the next DNS server in the list unless the first one is not reachable. Thus if the first DNS Server responds, but with no address for the initial query, this is deemed a successful response and the second DNS server is not queried. It is recommended that the DNS servers provisioned should reside inside the firewall.


Other SIP Domain
DNS Server
SIP Domain: othersip.Domain.com
Private DNS Server:
DNS Lookup of Name: othersip.Domain.com
Resolves to Private IP Address: 10.10.10.10
Ingate Firewall or SIParator
WAN IP: 123.123.123.123
LAN IP: 10.10.10.1
INTERNET
LAN
inGate
DNS Server
Public DNS Server:
DNS Lookup of Name: othersip.Domain.com
Resolves to Public IP Address: 123.123.123.123
SIP Server & SIP Registrar
SIP Domain: othersip.Domain.com
LAN IP: 10.10.10.10
SIP Domain: othersip.Domain.com

Other SIP Domain Example
SIP Domain: othersip.Domain.com

- Other SIP Server applies Local Registrar for Authentication and User Administration
- Other SIP Server uses local SIP Proxy & Dial Plan from Call Routing