Application Note

Ingate SIParator/Firewall for Remote Users in a Multitenant environment with

NEC UNIVERGE 3C As a Service

For the Ingate SIParator®/Firewalls using software release 6.1 or later

ingate
UNIVERGE BLUE

[April 2018]

Contents

1 Introduction 4

2 NEC UNIVERGE 3C – What is it? 5

3 Features and Values 5

4 The Initial Approach 6

4.1 How DNS override works? 6

4.2 Right solution using DNS override 7

5 More Advanced solution using GHM (Generic Header Manipulation) and Dial Plan. 8

5.1 What is Generic Header Manipulation 8

5.2 How GHM was used in our case? 9

6 Summary 10

Version: 01 Ingate SIParator/Firewall version 6.X

Revision History:

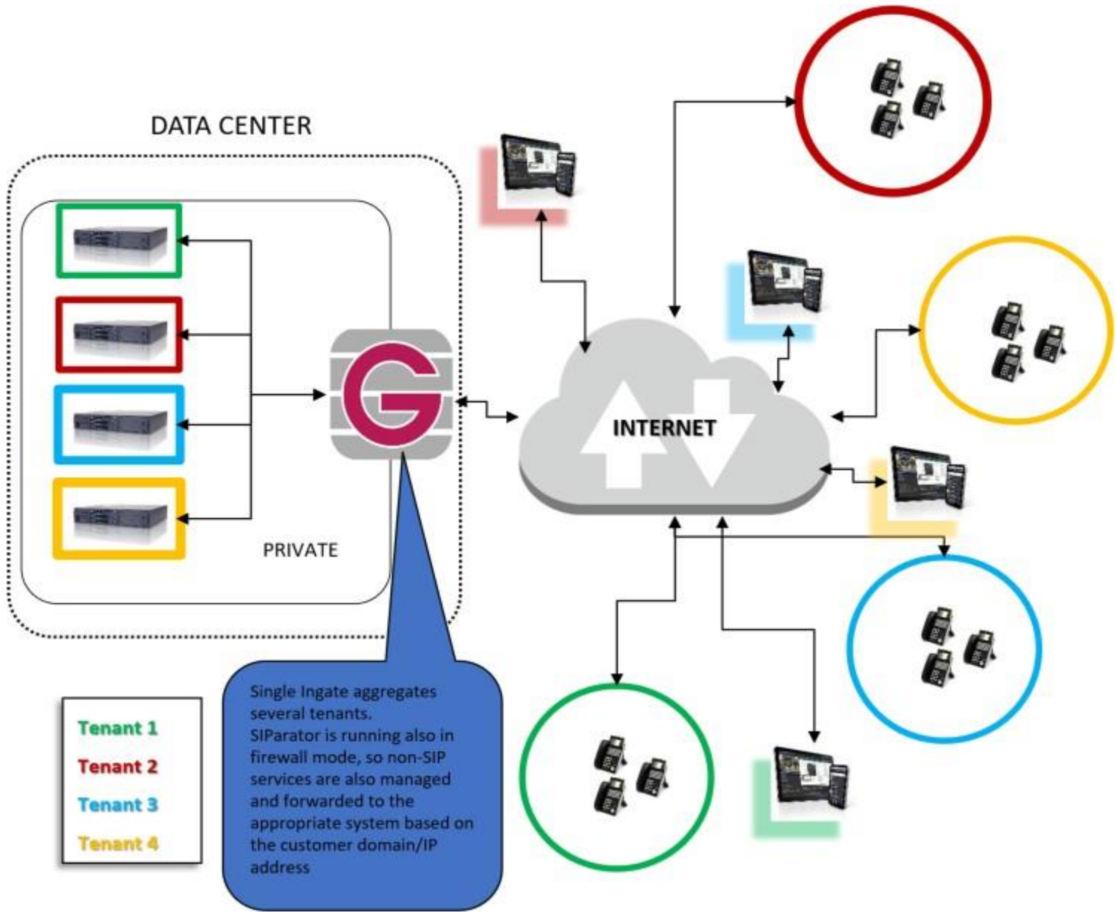
Revision	Date	Author	Comments
0.1	04-05-2018	Ernesto Casas	Approved

1 Introduction

The Topology:

The purpose of this document is to provide guidance on how to design and deploy Ingate SIParator SBC instance to provide remote access to NEC's UNIVERGE 3C services in a multitenant scenario.

One interesting concept introduced in this use case is the Multitenant scenario, where a single SIParator will be used to mediate connectivity between any remote user and its corresponding UNIVERGE 3C platform. Also, the SIParator will be mediating for more than one system.


DATA CENTER
PRIVATE
INTERNET
Tenant 1
Tenant 2
Tenant 3
Tenant 4
Single Ingate aggregates several tenants.
SIParator is running also in firewall mode, so non-SIP services are also managed and forwarded to the appropriate system based on the customer domain/IP address

The diagram above shows the typical use case we are covering in this application note.

We use colors to differentiate between 4 different Tenants (i.e. for different companies that want to use UNIVERGE 3C services hosted in the cloud/data center, having one dedicated System per enterprise customer.

Also, we show extensions or users remotely located using colors to identify which enterprise customer is associated with the corresponding Platform.

A single Ingate SIParator instance is being used to manage and mediate users and service platforms, providing each Tenant with the traditional SBC capabilities, including secure access, far end NAT traversal, QoS, Access Control, Encryption, Port forwarding, firewall, etc.

In our example:

a. Each customer (Tenant) is being hosted by a dedicated UNIVERGE 3C System
b. All users are remotely located, including offices, road warriors, home offices, etc.
c. Phones tested in this Proof of Concept (POC) lab are NEC DT and UT series as well as the UC Client.

2 NEC UNIVERGE 3C – What is it?

NEC UNIVERGE 3Cis an enterprise-grade, all-in-one communications solution: voice, mobility, messaging, presence, conferencing and more.

All your communications needs in a flexible, easy-to-use hosted cloud service, all for a single low monthly payment without massive up-front costs. NEC UNIVERGE 3C is Unified Communications as a Service (UCaaS).

NEC UNIVERGE 3C provides the rock-solid infrastructure so you unleash your people's creativity and productivity.

NEC UNIVERGE 3C takes the phone switching box out of a back closet and puts it into the cloud. Working smarter, faster and with more agility, UNIVERGE BLUE takes the burden of PBX hardware and maintenance off your shoulders and puts it into the cloud.

A single Ingate Instance or appliance could be mediating up to 20 thousand concurrent calls, even including Failover if necessary to provide business continuity.

3 Features and Values

Values obtained

a. Single point of access for multitenant services
b. Enables discriminated and distributed connectivity of Tenant endpoints to the appropriate designated servers in the cloud data center
c. Mediates signaling and media between endpoints and servers

d. Routes data port services to the appropriate servers based on Tenant (domain/IP)
e. Resolves far-end NAT traversal challenges occurring on customer premises and remote devices

SIParator features used

a. DNS override
b. Firewall rules and relays
c. Advanced dial plan and advanced header manipulation
d. Far-end NAT traversal (FENT)
e. IDS/IPS (security)

In order to implement the solution, any remote extension/user will use a unique domain name associated with the company (Tenant) it belongs to.

All Domain names (FQDN) will resolve on the same IP address, which is the Public IP address in the Ingate SIParator. For instance, if we want to provide service to 4 companies and we use domains such as company_1.com, company_2.com, company_3.com, company_n.com, all of them or any subdomain will always resolve to SIParator External/Public IP.

SIParator will distribute traffic to the designated 3C System based on the Domain name used in the signaling.

4 The Initial Approach

An initial approach is to take advantage of Ingate SIParator's DNS override functionality.

4.1 How DNS override works?

Here, you can register SIP domains to the unit which should be able to forward requests, but which for some reason cannot be resolved in DNS to a private IP address in the data center.

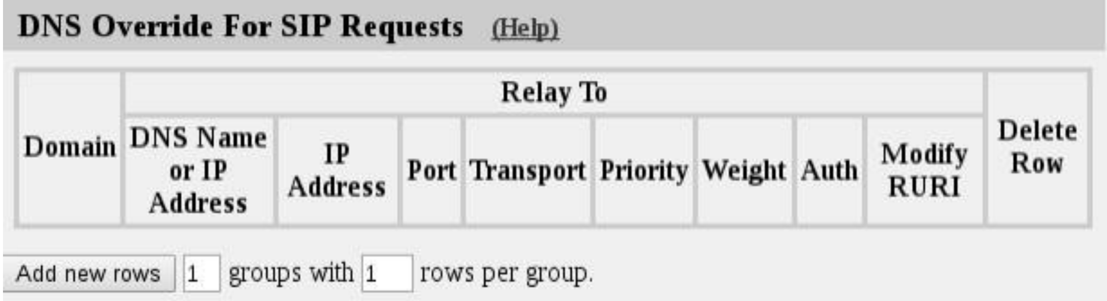
Enter an IP address and port to which the requests should be forwarded. You can also select to use a specific protocol.

The unit uses the Request-URI of the incoming SIP packet to match for the domains in this table.

When it matches a domain, the packet will be forwarded to the IP address entered here. Note that the Request-URI will not be rewritten!

You can also enter subdomains to Local SIP Domains, if you want the subdomain to be handled by a separate SIP proxy. This table has a higher priority than Local SIP Domains, which means that if you register a subdomain to a domain registered under Local SIP Domains, the unit will forward SIP requests to the subdomain instead of processing them itself.

You can enter more than one IP address or host name for a domain, and set weights and priorities for these, making this a powerful tool for failover of the System destination as well as use load balance approach if necessary. It is very similar to having DNS with SRV records, without the complexity of implementing a DNS server with split domains.



DNS Override For SIP Requests (Help)

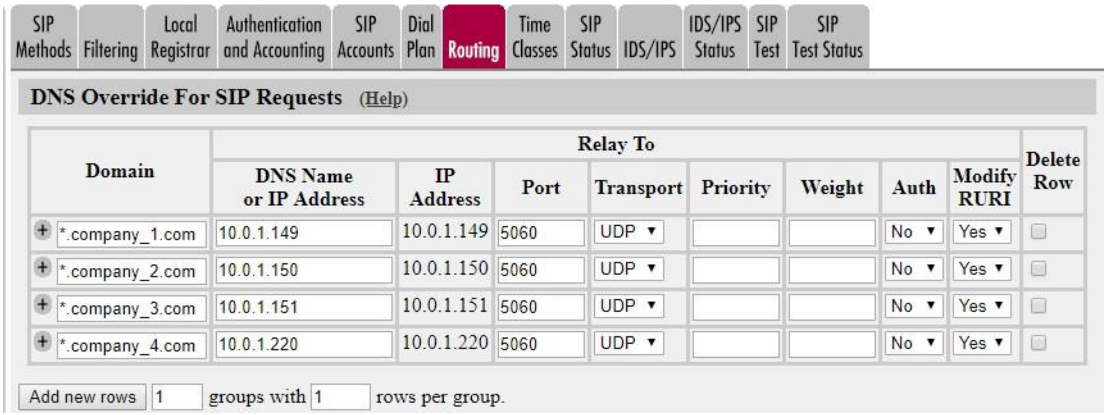
Domain	Relay To								Delete Row
	DNS Name or IP Address	IP Address	Port	Transport	Priority	Weight	Auth	Modify RURI	

Add new rows 1 groups with 1 rows per group.

For further details check section 10.7.1 in [Ingate SIParator Reference Guide]()

4.2 Right solution using DNS override

In our case the DNS Override may look like this:

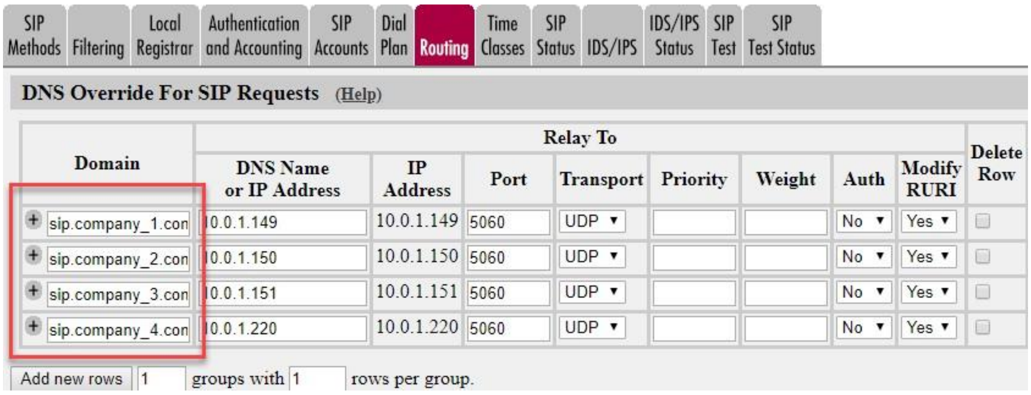


DNS Override For SIP Requests (Help)

Domain	Relay To								Delete Row
	DNS Name or IP Address	IP Address	Port	Transport	Priority	Weight	Auth	Modify RURI	
+ *.company_1.com	10.0.1.149	10.0.1.149	5060	UDP			No	Yes	□
+ *.company_2.com	10.0.1.150	10.0.1.150	5060	UDP			No	Yes	□
+ *.company_3.com	10.0.1.151	10.0.1.151	5060	UDP			No	Yes	□
+ *.company_4.com	10.0.1.220	10.0.1.220	5060	UDP			No	Yes	□

Add new rows 1 groups with 1 rows per group.

It can also use the specific subdomain name without the * wild card:

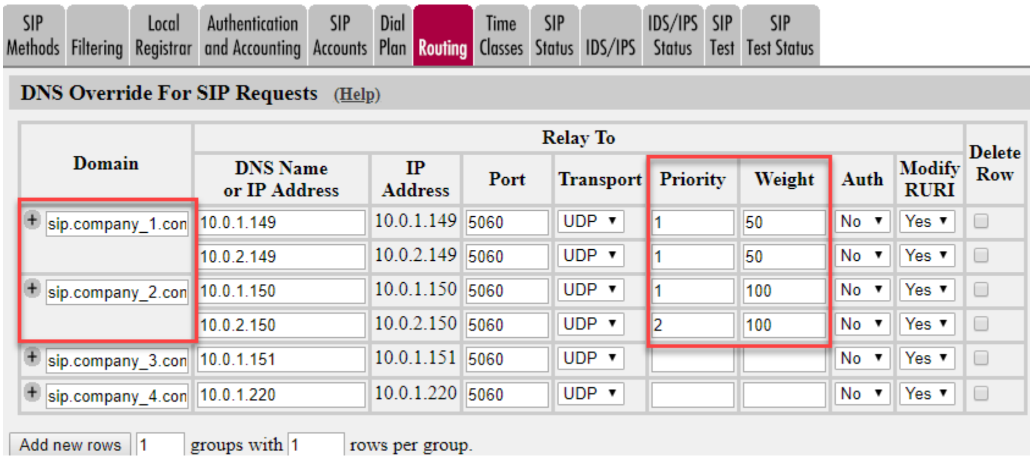


DNS Override For SIP Requests (Help)

Domain	Relay To								Delete Row
	DNS Name or IP Address	IP Address	Port	Transport	Priority	Weight	Auth	Modify RURI	
+ sip.company_1.con	10.0.1.149	10.0.1.149	5060	UDP ▾			No ▾	Yes ▾	☐
+ sip.company_2.con	10.0.1.150	10.0.1.150	5060	UDP ▾			No ▾	Yes ▾	☐
+ sip.company_3.con	10.0.1.151	10.0.1.151	5060	UDP ▾			No ▾	Yes ▾	☐
+ sip.company_4.con	10.0.1.220	10.0.1.220	5060	UDP ▾			No ▾	Yes ▾	☐

Add new rows 1 groups with 1 rows per group.

Also, forward destinations can be managed as SRV records with weights and priorities:



DNS Override For SIP Requests (Help)

Domain	Relay To								Delete Row
	DNS Name or IP Address	IP Address	Port	Transport	Priority	Weight	Auth	Modify RURI	
+ sip.company_1.con	10.0.1.149	10.0.1.149	5060	UDP ▾	1	50	No ▾	Yes ▾	☐
	10.0.2.149	10.0.2.149	5060	UDP ▾	1	50	No ▾	Yes ▾	☐
+ sip.company_2.con	10.0.1.150	10.0.1.150	5060	UDP ▾	1	100	No ▾	Yes ▾	☐
	10.0.2.150	10.0.2.150	5060	UDP ▾	2	100	No ▾	Yes ▾	☐
+ sip.company_3.con	10.0.1.151	10.0.1.151	5060	UDP ▾			No ▾	Yes ▾	☐
+ sip.company_4.con	10.0.1.220	10.0.1.220	5060	UDP ▾			No ▾	Yes ▾	☐

Add new rows 1 groups with 1 rows per group.

Here company_1 will load balance between 10.0.1.149 and 10.0.2.149, while company_2 will send all traffic to 10.0.1.150 and failover 10.0.2.150.

5 More Advanced solution using GHM (Generic Header Manipulation) and Dial Plan.

5.1 What is Generic Header Manipulation

The purpose of this feature is to enhance the interoperability between different vendor equipment, as many IP-PBX, Service Providers, and overall SIP devices require different usage of various SIP Headers. Different vendors interpret the SIP standard in a non-conforming way. Using GHM can resolve SIP protocol implementation discrepancies.

Rules are configured in the Dial Plan and SIP Trunk Page GUIs. The rules are configured in the same fields as regular expressions are written. With Regular Expressions it is possible to match substrings and variables from the SIP messages and when forwarding the SIP messages, they can be rewritten according to your needs. By variable substitutions it is also possible to take information from one header and put it into another header.

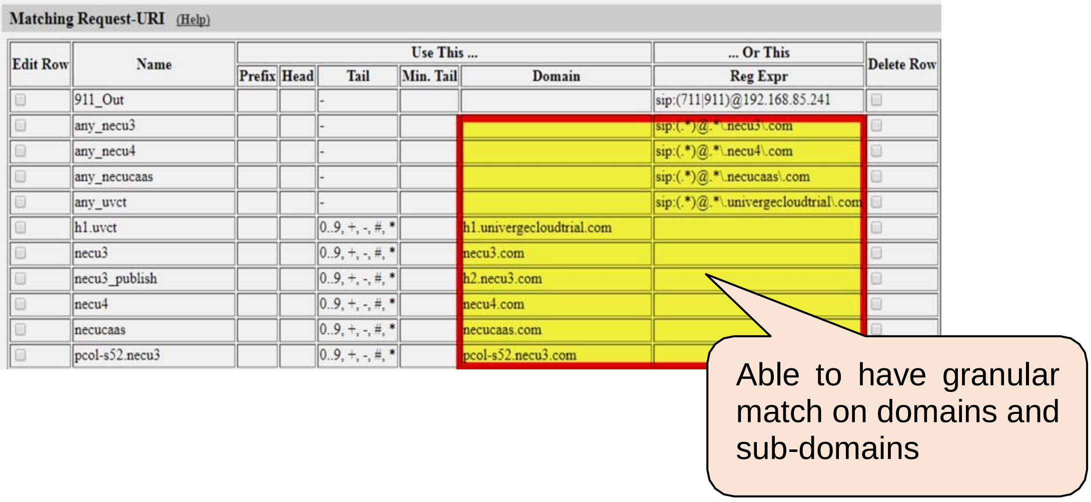
For detailed information and how to visit How to use Generic Header Manipulation

5.2 How GHM was used in our case?

Some additional requirements in terms of interoperability appeared during the implementation of the basic approach, and this is where extensive flexibility and unique capabilities make the SIParator the right solution which is ahead of any other SBC vendor.

In this case, as an example, an alteration of SIP headers was needed before forwarding SIP requests to the 3C Platform. In this case P-Asserted Identity Header must be added since it was not included in the request header received from the remote user.

In the dial plan, match on the Request **URI** will take care of identifying the domain (Tenant) or subdomains any request is associated to.

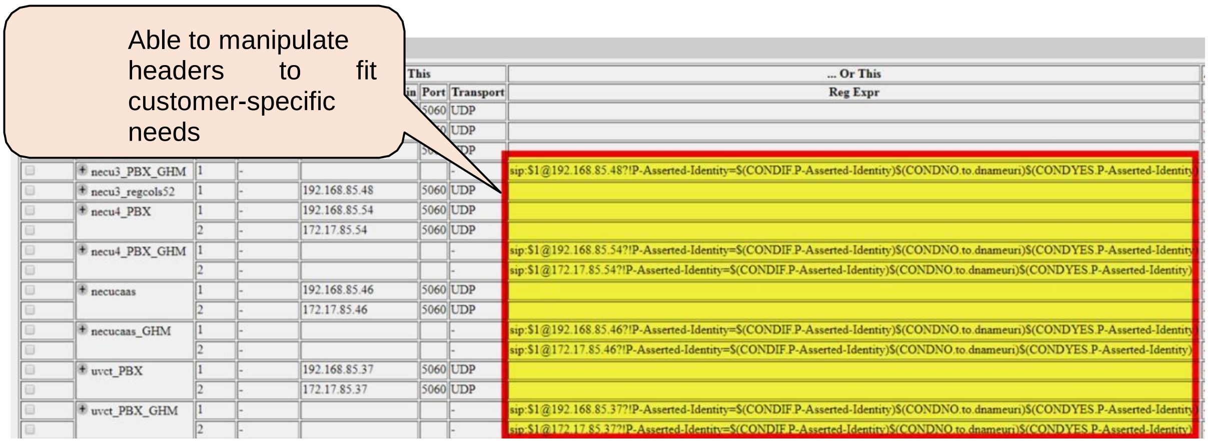


Matching Request-URI (Help)

Edit Row	Name	Use This ...					... Or This	Delete Row
		Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
□	911_Out			-			sip:(711|911)@192.168.85.241	□
□	any_necu3			-			sip:(.*)@.*\.necu3\.com	□
□	any_necu4			-			sip:(.*)@.*\.necu4\.com	□
□	any_necucaas			-			sip:(.*)@.*\.necucaas\.com	□
□	any_uvct			-			sip:(.*)@.*\.univergecloudtrial\.com	□
□	h1.uvct			0..9, +, -, #, *		h1.univergecloudtrial.com		□
□	necu3			0..9, +, -, #, *		necu3.com		□
□	necu3_publish			0..9, +, -, #, *		h2.necu3.com		□
□	necu4			0..9, +, -, #, *		necu4.com		□
□	necucaas			0..9, +, -, #, *		necucaas.com		□
□	pcol-s52.necu3			0..9, +, -, #, *		pcol-s52.necu3.com		

Able to have granular match on domains and sub-domains

Based on the matching criteria, we used header manipulation while defining forward destinations as shown here:



Able to manipulate headers to fit customer-specific needs

				This			... Or This
				in	Port	Transport	Reg Expr
					5060	UDP	
					0	UDP	
					50	DP	
□	+ necu3_PBX_GHM	1	-			-	sip:$1@192.168.85.48?!P-Asserted-Identity=$(CONDIF.P-Asserted-Identity)$(CONDNO.to.dnameuri)$(CONDYES.P-Asserted-Identity
□	+ necu3_regcols52	1	-	192.168.85.48	5060	UDP	
□	+ necu4_PBX	1	-	192.168.85.54	5060	UDP	
□		2	-	172.17.85.54	5060	UDP	
□	+ necu4_PBX_GHM	1	-			-	sip:$1@192.168.85.54?!P-Asserted-Identity=$(CONDIF.P-Asserted-Identity)$(CONDNO.to.dnameuri)$(CONDYES.P-Asserted-Identity
□		2	-			-	sip:$1@172.17.85.54?!P-Asserted-Identity=$(CONDIF.P-Asserted-Identity)$(CONDNO.to.dnameuri)$(CONDYES.P-Asserted-Identity)
□	+ necucaas	1	-	192.168.85.46	5060	UDP	
□		2	-	172.17.85.46	5060	UDP	
□	+ necucaas_GHM	1	-			-	sip:$1@192.168.85.46?!P-Asserted-Identity=$(CONDIF.P-Asserted-Identity)$(CONDNO.to.dnameuri)$(CONDYES.P-Asserted-Identity
□		2	-			-	sip:$1@172.17.85.46?!P-Asserted-Identity=$(CONDIF.P-Asserted-Identity)$(CONDNO.to.dnameuri)$(CONDYES.P-Asserted-Identity)
□	+ uvct_PBX	1	-	192.168.85.37	5060	UDP	
□		2	-	172.17.85.37	5060	UDP	
□	+ uvct_PBX_GHM	1	-			-	sip:$1@192.168.85.37?!P-Asserted-Identity=$(CONDIF.P-Asserted-Identity)$(CONDNO.to.dnameuri)$(CONDYES.P-Asserted-Identity
□		2	-			-	sip:$1@172.17.85.37?!P-Asserted-Identity=$(CONDIF.P-Asserted-Identity)$(CONDNO.to.dnameuri)$(CONDYES.P-Asserted-Identity)

In this case for example a forward destination was defined as "necu4_PBX_GHM", and in that case the destination will be 192.168.85.54 with fail over 172.17.85.54, and also IP-Asserted-Identity in case it is not present, will be added taking the information on the URI domain name coming on the To header inbound request.

To do so we are using a conditional header manipulation. For instance:

SIP:$1@192.168.85.54?P-Asserted-Identity=$(CONDIF.P-Asserted-Identity)$(CONDNO.to.dnamuri)$(CONDYES.P-Asserted-Identity)

For more detailed information on how to use Generic Header Manipulation you can review the Manual How to use generic Header Manipulation. In Section 7 you will see how to use conditional header manipulation.

6 Summary

This application note shows a multitenant hosted PBX (NEC UNIVERGE 3C) scenario, sharing a single SBC (Ingate SIParator) to manage remote access of users and extensions.

We present two solutions for this deployment, the first being one what we called the Initial Approach, which is very straight forward and easy to implement and an advanced solution taking advantage of dial plan and header manipulation features to enhance interoperability between end points and UNIVERGE 3C.

If you need additional information or want to discuss more detail or potential variants in similar situations, feel free to contact us at sales@ingate.com