Information Note
Vega Resilience Proxy

From Release 8.2 Vega gateways are available with an optional Resilience Proxy built in.

Although Vega gateways have been able to support resilient operation themselves by re-presenting calls to alternative VoIP or telephony destinations through use of call re-presentation (configured in dial plans and call presentation groups) the Resilience Proxy extends the Vega's functionality to providing resilient operation for SIP phones on a local site.

The principle concern in moving to an ITSP served VoIP solution, or in fact any VoIP solution where the Registrar / Proxy is off site, is that if the broadband link to the ITSP / Registrar / Proxy fails, then not only are inbound and outbound calls lost, but so are internal calls.

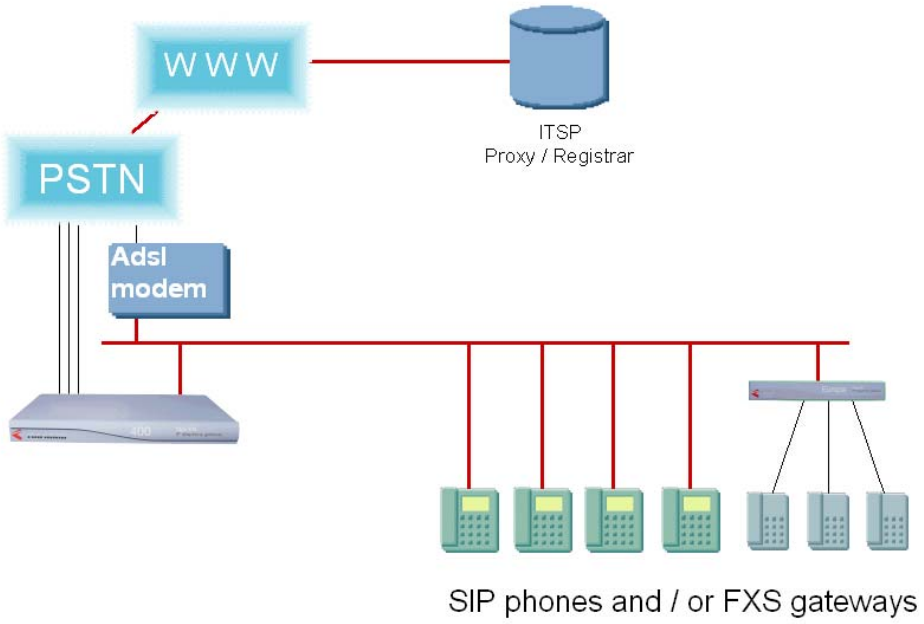
The Vega Resilience Proxy changes all this. Under broadband failure conditions the Vega Resilience Proxy allows local calls to continue to be made, also inbound and outbound calls can be made via the Vega telephony interfaces.

Typical configuration

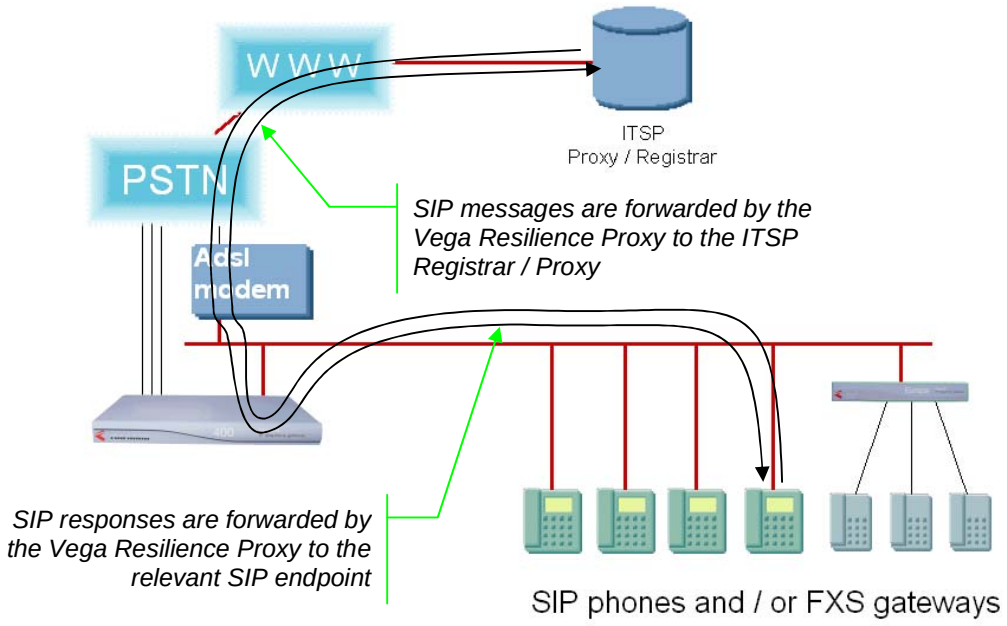
Although the Resilience Proxy functionality is available as an option on all Vega gateways, typically it is used on trunking gateways connected to the PSTN.

The Vega telephone interfaces will be connected to the PSTN to send and receive calls to / from the outside world.

The SIP handsets / local FXS gateways will be configured to register with and send calls to the ITSP's Registrar / Proxy. But, in order that the Vega Resilience Proxy sees and can handle VoIP messaging when the ITSP Registrar / Proxy is down, the SIP handsets and local FXS gateways must be configured with the Vega Resilience Proxy as their outbound proxy.



Normal operation (link to ITSP is good)



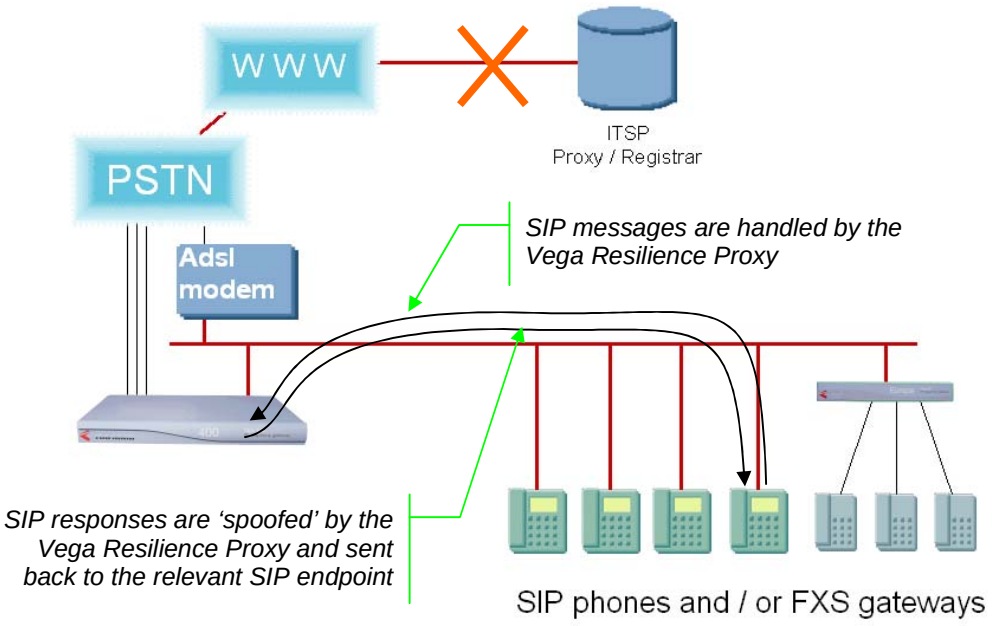
When the Vega Resilience proxy deems that the ITSP Registrar / Proxy is accessible it will forward Registration and all other SIP messages to the ITSP Registrar / Proxy. All responses and SIP messages originating at the ITSP will be forwarded to the relevant SIP endpoint.

Registration requests and responses will be monitored. If registrations are accepted by the ITSP Registrar / Proxy then the Resilience proxy will cache the result so that it can use it if the connection to the ITSP Registrar / Proxy is lost.

Calls arriving on the telephony interfaces of the gateway which are forwarded to the Resilience Proxy using the Vega dial plans will be handled like other endpoints – the SIP messages will be forwarded to the ITSP Registrar / Proxy for it to route the calls.

From \ To	To registered endpoint	To unregistered endpoint
From trusted or authenticated SIP endpoint or gateway	Routed to endpoint via Resilience Proxy via ITSP	Routed to endpoint via Resilience Proxy via ITSP
From SIP endpoint or gateway that is not trusted or authenticated	Routed to endpoint via Resilience Proxy via ITSP	Routed to endpoint via Resilience Proxy via ITSP

Failure operation (link to ITSP is down)



When the Vega Resilience proxy determines that the ITSP Registrar / Proxy is not accessible it will respond itself so that VoIP endpoints remain registered and SIP endpoints can make phone calls between themselves.

A call received by the Vega Resilience proxy (from a trusted or authenticated endpoint) that is destined for:

- a SIP endpoint registered on the Resilience Proxy
  - is forwarded to that SIP endpoint.

- a non registered endpoint
  - is forwarded to the gateway so that dial plans in the gateway can route calls to the PSTN; so that calls can be completed even though they cannot be routed via the ITSP.

A call arriving on a telephony interface of the gateway that is forwarded to the Resilience Proxy and is destined for:

- a SIP endpoint registered on the Resilience Proxy
  - is forwarded to that SIP endpoint.

- a non registered endpoint
  - will be rejected with 404-Not found. (Calls from the gateway will not be looped back to the gateway in order to avoid call forwarding fraud). If additional fallback handling is required Vega call re-presentation may be used to provide alternate routing.

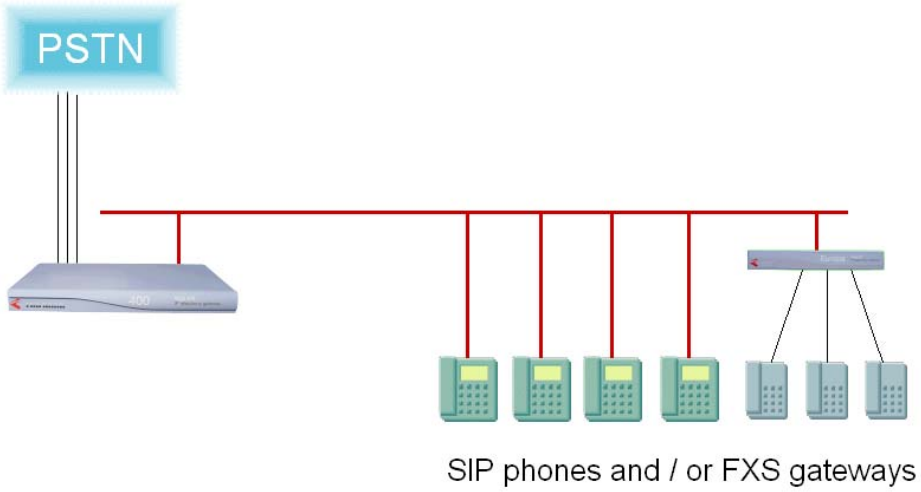
From \ To	To registered endpoint	To unregistered endpoint
From trusted or authenticated SIP endpoint or gateway	Routed to endpoint via Resilience Proxy	Routed to gateway via Resilience Proxy
From SIP endpoint or gateway that is not trusted or authenticated	Routed to endpoint via Resilience Proxy	Responded to with 404 – Not Found

Standalone registrar & proxy

Although not strictly designed to be a standalone registrar and proxy, the Vega Resilience proxy can be used for simple operations where a Registrar / Proxy is required to allow local devices to call one another and to allow local devices be able to make calls to the PSTN and to receive calls from the PSTN.

The Resilience Proxy acting in standalone mode will support up to 120 attached (registered) endpoints. It will support the SIP endpoints performing call transfers (using refer / replaces) but will ***not*** itself provide more advanced PBX style features like

- Voice Mail
- Conferencing[1]



To operate in standalone proxy mode configure the SIP endpoints to register with the Vega resilience Proxy.

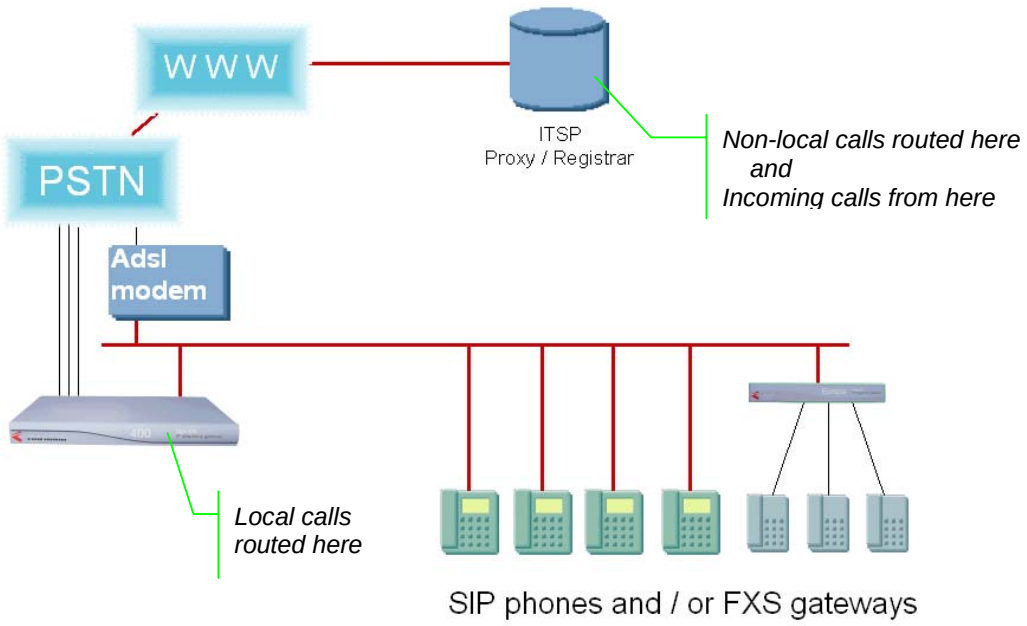
Devices that wish to register must either be in the trusted IPs table, or must be able to authenticate with the Resilience proxy.

From \ To	To registered endpoint	To unregistered endpoint
From trusted or authenticated SIP endpoint or gateway	Routed to endpoint via resilience Proxy	Routed to gateway via Resilience Proxy
From SIP endpoint or gateway that is not trusted or authenticated	Routed to endpoint via Resilience Proxy	Responded to with 404 – Not Found

[1] Any on-phone or on-SIP endpoint conferencing will continue to work, it will not be affected by the Resilience Proxy functionality

Local proxy for use with SIP trunk

With SIP trunking to an ITSP becoming more popular many users would like a system where the resilience proxy will provide the routing for local calls without the need to send the call to the ITSP. In this case the Resilience proxy routes the call directly if the SIP endpoint is registered with it, and only forwards the call to the ITSP if the call is not for a locally registered endpoint.



This method of operation may be selected by setting the Resilience Proxy parameter sipproxy.mode=sip_trunk

Sip phones and other SIP endpoints will still register with the ITSP so that the ITSP and the Resilience proxy know which SIP device to route incoming SIP calls to.

From \ To	To registered endpoint	To unregistered endpoint
From trusted or authenticated SIP endpoint or gateway	Routed to endpoint via Resilience Proxy	Routed to ITSP via Resilience Proxy
From SIP endpoint or gateway that is not trusted or authenticated	Routed to endpoint via resilience Proxy	Routed to ITSP via Resilience Proxy

SIP over TCP

The Vega Resilience proxy supports connections made over UDP and made over TCP.

The resilience proxy does not clear TCP connections made to it – this allows registrations and following calls to be made through the same socket connection.

In order to assist with keeping TCP connections to SIP endpoints open, the Vega has an optional TCP keep-alive function. Although turned off by default the Vega Resilience Proxy can be configured with a timeout that will trigger it to send out CRLF characters to SIP endpoints registered over a TCP socket.

The Vega Resilience proxy can accept and handle some SIP endpoints using UDP connections and others using TCP simultaneously.

The use of TCP or UDP connectivity between the Resilience Proxy and the ITSP Registrar / Proxy follows the TCP / UDP usage used in the message sent to the Resilience proxy triggering the message to be sent to the ITSP Registrar / Proxy.

Other features

Using the Vega Resilience proxy as an outbound proxy provides the added benefit that all SIP messaging to / from the ITSP (and hence to / from the raw internet) now pass through the single IP address / port of the Vega Resilience Proxy. This makes setting up NAT and firewall traversal much simpler as there is only a single IP / port to worry about for SIP signalling messages.

Also to help with NAT traversal the outside IP address of the Network can be configured in the Resilience proxy. For communications with the ITSP the Resilience Proxy will use this address as the address to send SIP messages and responses to (Media addresses are not affected). A single static route in the firewall forwards data arriving at this port to the Resilience Proxy.

How does the Resilience Proxy work?

When the Resilience Proxy receives any message, firstly it checks the IP address of the originator of the message:

- If the IP address matches an entry in the 'IPs to Ignore' table, then the message is ignored.
- If the IP address matches an entry in the 'IPs to reject' table, then the message is rejected with a 403 – Forbidden SIP response.

If not ignored or rejected, processing of the SIP messages is then dependent upon the accessibility of the ITSP Registrar / Proxy.

The Vega Resilience Proxy determines that the Registrar / Proxy is accessible when it responds to SIP OPTIONS messages. If it fails to respond to a SIP OPTIONS message, the Resilience proxy will use standard SIP timeouts to retry the OPTIONS. If it is still not responded to then the Vega will deem the Registrar / Proxy to be in-accessible. The Vega will periodically send (and retry sending) SIP OPTIONS messages to the Registrar / Proxy and will deem the Registrar / Proxy accessible again when it receives an OK response.

When the Registrar / Proxy is deemed to be accessible:

- All registration and SIP signalling messages from SIP endpoints will be forwarded to the Registrar / Proxy[2] (the resilience proxy only acts as an outbound proxy; it does not try and

[2] Except when configured as a local proxy for use with a SIP trunk, when call requests to devices registered locally will be handled directly by the resilience proxy

route calls even though it may know about registrations, because call forwarding or other advanced call handling services configured on the Registrar / Proxy may mean that even though a local number was dialled, the call is required to be routed elsewhere – e.g. to a mobile phone as the person is out of the office)
- Registration requests are monitored by the Resilience Proxy and positive outcome registrations are cached so that the Resilience Proxy can maintain this routing if connection to the ITSP Registrar / Proxy is lost.
- If a Registration response exceeds the Resilience Proxy registration response timeout the resilience proxy will remove the registration status from its internal cache. (If a response is received late, it will be forwarded to the SIP endpoint but will not be noted in the resilience proxy registration cache).
- In order that the Registrar / Proxy returns SIP messages via the Vega Resilience proxy the resilience proxy adds a record route header to messages it sends to the Registrar / Proxy

When the Registrar / Proxy is deemed to be in-accessible:
- Registration intervals are reduced (by default to 30 seconds) so that as soon as the Registrar / Proxy becomes available again communications are re-established with it as soon as possible.
- Cached registrations are not expired in the Vega Resilience Proxy so that internal calls that could be made before the Registrar / Proxy was lost can still be made.
- New registrations are accepted by the Resilience Proxy if the IP address of the registering device is a trusted IP address, or the device verifies itself by authentication.

In all cases the Resilience Proxy handles SIP signalling messages only. It is not designed to receive and forward media.

Simultaneous registrations of the same phone number

In some circumstances users may register multiple SIP devices with the same SIP User ID (e.g. a SIP desk phone and a SIP soft phone). If a call arrives for that SIP user, some Proxies will generate a forked call so that both devices ring simultaneously. Although the Resilience proxy will pass through registrations and forked calls, in 'Failure Operation' mode the Resilience proxy will not generate forked calls, it will only send the call to the last device that registered with that relevant SIP user ID.

Resilience Proxy Ignore / reject / trust / authenticate

The Resilience proxy has a number of tables that may be configured to define how to initially handle incoming messages:

IPs to ignore (up to 100 entries):
- Explicit blacklist of specific IP addresses and IP address ranges.
- Any SIP message from any of these addresses will be dropped and not responded to. This can help deter devices from retrying requests or attempting Denial of Service attacks.

IPs to reject (up to 100 entries):
- Explicit blacklist of specific IP addresses and IP address ranges.
- Any SIP message from any of these addresses will be actively rejected with a 403 – Forbidden

IPs to trust (up to 100 entries):

- Explicit whitelist of specific IP addresses and IP address ranges.
- If ITSP Registrar / Proxy is in-accessible this list specifies whether endpoint devices should be treated as trustworthy devices for registering and making calls.

SIP Auth table (up to 120 entries):

- If the ITSP Registrar / Proxy is in-accessible and a SIP message comes from a device that is not in the 'IPs to trust' list, the Vega will ask for authentication before handling the message
- The SIP Auth table contains:
  - Authentication User name
  - Authentication password
  - Authentication realm (to be same as Registrar / Proxy domain)
- Failure to authenticate will result in a response 407 – Proxy Authentication Required

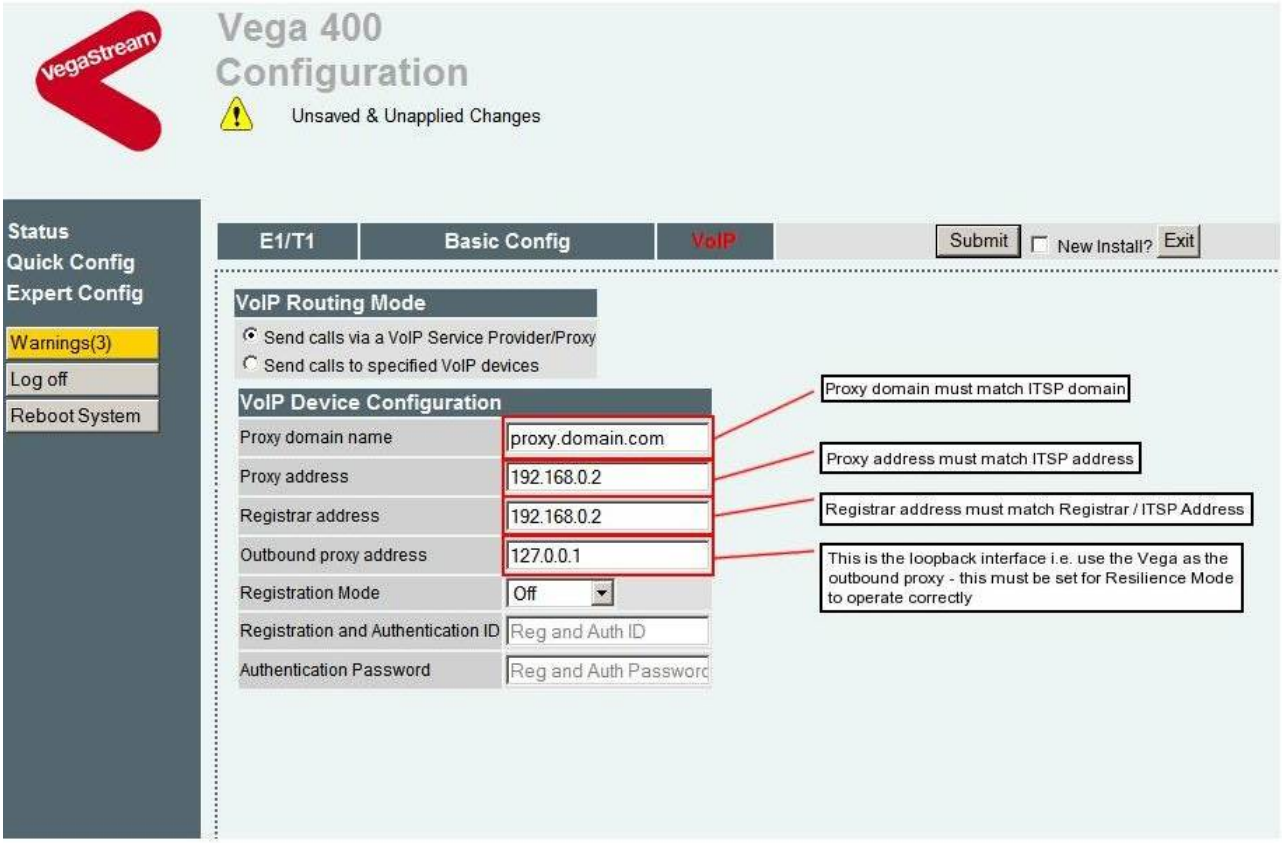
Access to the Vega gateway

The IP port number of the gateway is a different value to the IP port number of the resilience proxy, so even if the resilience proxy is enabled, if calls are to be routed directly out of the gateway without need to handle them using the resilience proxy, the call may be sent directly to the IP Port of the gateway.

Configuring Vega and Resilience proxy from the web browser.

Quick Config Parameters for Vega operation with the on-board Resilience Proxy

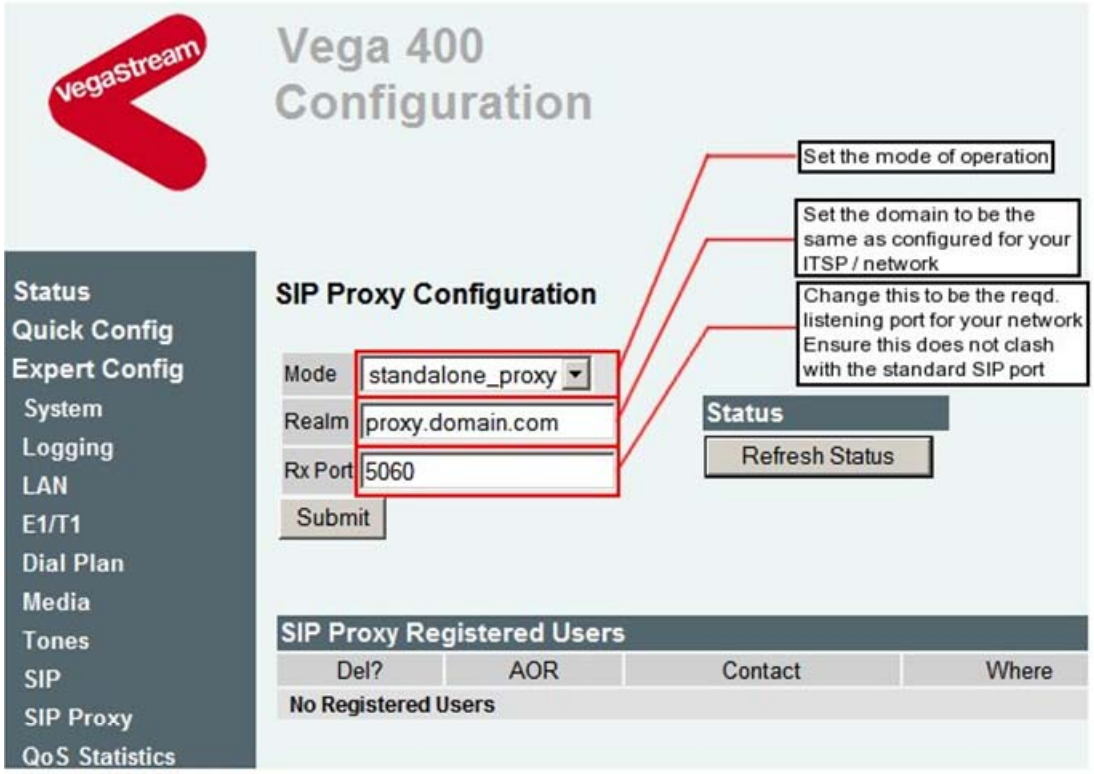
In order for the Vega telephony interfaces to make and receive calls and connect to the Resilience proxy the Vega proxy parameters must be configured as indicated below:



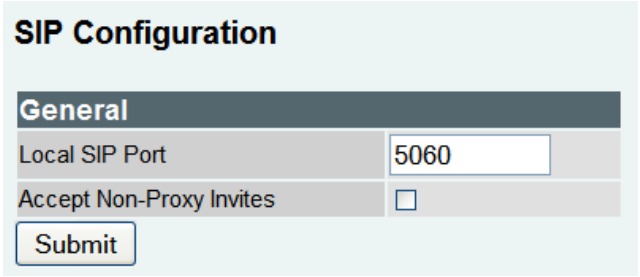
Resilience Proxy Configuration

Under Expert mode, select 'SIP Proxy', then follow setup details shown below:

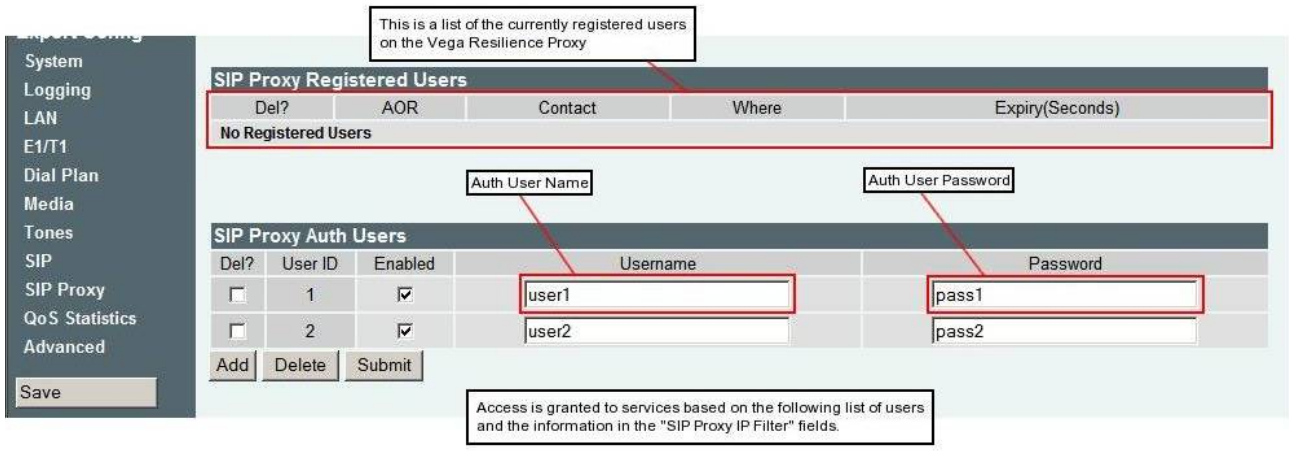
… set up Proxy mode, ITSP domain and Resilience proxy RXPort (listening port).



N.B. RxPort must be a different value to that set up for the Local SIP Port (the gateway's listening port) configured on the SIP page:



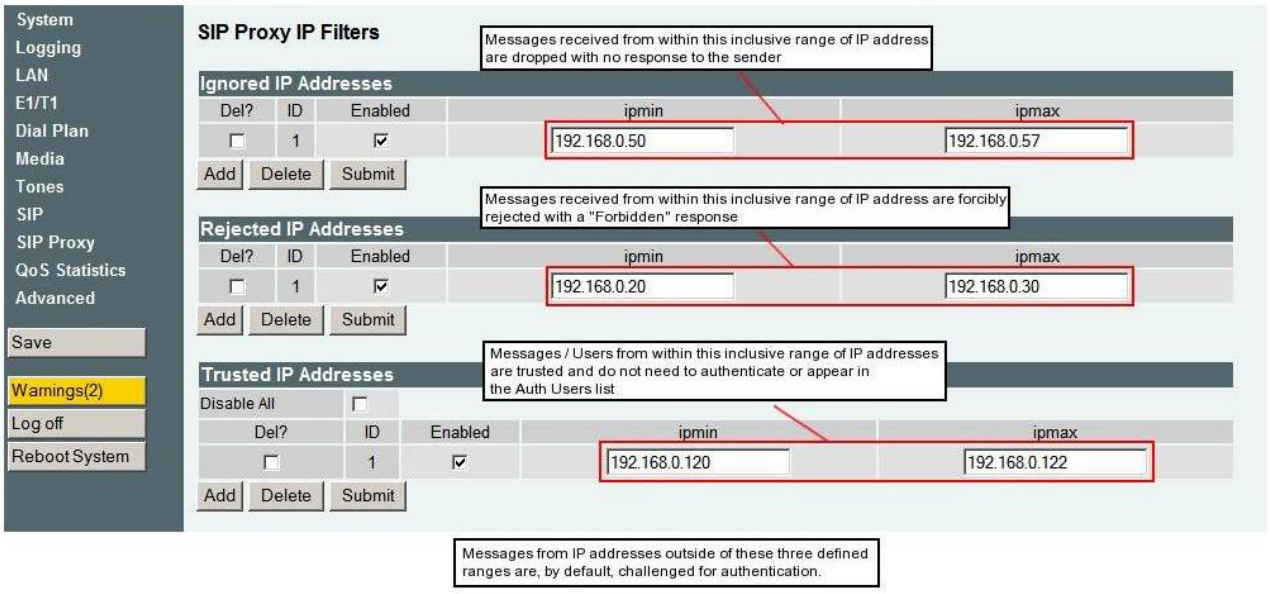
If required, set up any authentication details; note Auth user name must match the registration id of the relevant phone. (This is needed for the endpoints to continue registering with the Resilience Proxy under network failure conditions, if the endpoint does not have an IP address in the trusted IP address range – defined below)



Set up resilience proxy IP filters

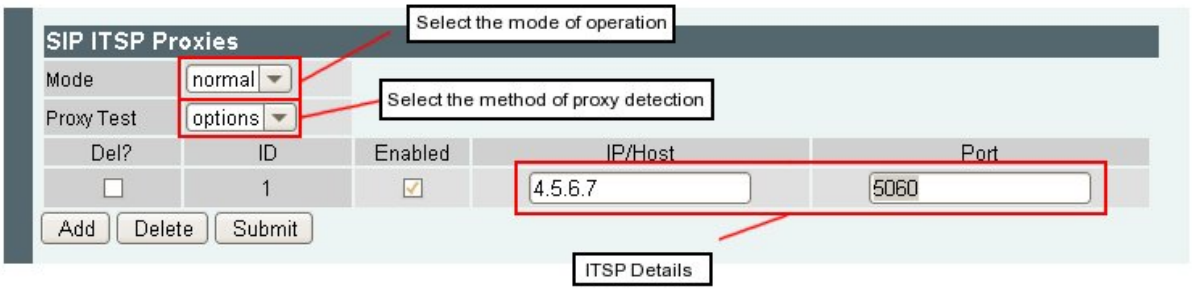
- define any IP address ranges from which registrations and calls should not be accepted (Ignored IP addresses) … no response will be sent by the Vega – this may be useful to stop spamming where bots home in on devices that respond to them.
- define any IP address ranges from which registrations and calls should be actively rejected (with a 403 – Forbidden response)
- define any IP address ranges from which registrations should be accepted without need for that endpoint to authenticate itself (usually used to define local subnet IP addresses – so that resilience proxy does not need to be configured with authentication details for local phones).

(Don't try and set up internal gateway here, it has its own configuration below)

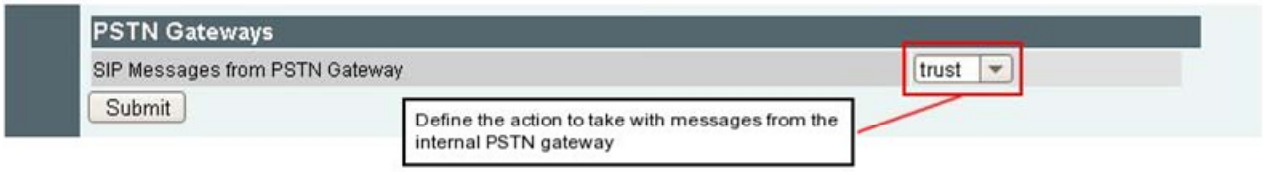


If the Resilience proxy is not in standalone mode, then the ITSP proxy / proxies details must be configured.

- **Mode of operation defines when to use which proxy if multiple proxies are specified**
- **Proxy test defines how to test for the ITSP proxy. (Selecting 'off' makes the Vega assume that the proxy is down.)**



Typically calls from the gateway that exists in the same chassis will be allowed and should be trusted, the opportunity to select authenticate, reject or ignore is however possible.



Resilience Proxy Command Line Interface Parameters

```
[sipproxy]
  rx_port=5060
  realm=abcdefghijwhatever.com
  mode=off                  ; can be standalone_proxy, forward_to_ITSP,
                            sip_trunk or off

[sipproxy.pstn_gw]
  from_action=trust         ; can be trust, auth, reject, ignore
  from_routing=itsp         ; can be itsp, regd_ua

[sipproxy.itsp_proxy]
  accessibility_check=options ; can be off or options
  options_tansport=udp      ; can be udp, tcp, default
  mode=normal               ; can be normal, cyclic, dnssrv

[sipproxy.itsp_proxy.x]
  enable=0
  ipname=0.0.0.0
  port=5060

[sipproxy.auth.user.x]
  enable=0
  username=user
  password=pass

[siproxy.ignore.x]
  enable=0
  pmin=0.0.0.0
  ipmax=0.0.0.0

[siproxy.reject.x]
  enable=0
  pmin=0.0.0.0
  ipmax=0.0.0.0

 [siproxy.trust.x]
  enable=0
  pmin=0.0.0.0
  ipmax=0.0.0.0

 [_advanced.siproxy]
  numsockets=120
  crlf_keepalive=0          ; specify time in seconds 0 to 180
  reg_forwarding_timeout=10 ; specify time in seconds 2 to 60
  itsp_down_reg_expires=60  ; specify time in seconds 30 to 60,000
```

Command line interface commands

Sipproxy show reg - shows cached registration information held in the Resilience Proxy
Sipproxy kill reg n - kills the cached registration entry n

Gottcha's

1. Registered number and PSTN number differ

Initial releases of resilience proxy support routing based on the registered number only. Some ITSPs register a different number from the PSTN telephone number assigned to that phone. In this case … under failure conditions the user will need to dial the registered number to contact another phone in the local office.

Future builds are expected to support an Alias Table … where the PSTN phone number can be associated with the registered number.

2. DNS is internet based

If the office does not have a local DNS server then on loss of internet the DNS server will also be lost. In these cases ensure that Vega configuration uses static IP addresses rather than DNS names, or alternatively the DNS name to IP address are statically defined in the Vega Lan Hosts table.

Contact Details
Email: support@vegastream.com
Web: www.vegastream.com
www.vegaassist.com

EMEA Office
VegaStream
The Western Centre
Western Road
Bracknell
Berks RG12 1RW
UK

+44 (0) 1344 784900

USA Office
VegaStream Inc.
6200 Stoneridge Mall Road
3rd Floor
Pleasanton
California 94588
USA

+1 925 399 6428