MiCollab Client for Mobile Resiliency Guide

RELEASE 7.0

Mitel®

NOTICE

Trademarks

MiCollab Client for Mobile Resiliency Guide
Release 7.0
September, 2015

PURPOSE OF THIS GUIDE

In MiCollab Release 7.0 and later, MiCollab Client for Mobile softphones support Domain Name System (DNS)-based SIP resiliency with MiVoice Border Gateways (MBGs). This guide provides the DNS configuration required to support SIP resiliency for MiCollab Client for Mobile softphones in an Enterprise or Cloud environment.

OVERVIEW

The MiCollab Client for Mobile softphone supports Session Initiation Protocol (SIP) for audio and video communication. It uses SIP for all call-related signaling, Transport Layer Security (TLS), Secure Real-time Transport Protocol (SRTP) and resiliency support.

MiCollab Client for Mobile softphones support SIP resiliency with an MBG, such that if the call signaling path is disrupted or the MBG is taken out of service, the softphone registers with an alternate MBG to regain service.

SIP softphone resiliency ensures that users experience a minimum disruption in service during an MBG upgrade or during the removal of an MBG from the network.

How it works

In an Enterprise or Cloud environment, the softphones are connected to the network through an MBG cluster. You use DNS to map the Fully Qualified Domain Name (FQDN) of the MBG cluster to the hostnames of the member MBGs. This mapping is contained in the configuration file on the DNS server. If the MBG that supports the softphones goes out of service, the softphones use the configuration data that they received from the DNS server to register with an alternate MBG. This allows the softphone to obtain service.

About DNS SRV Records

DNS Service (SRV) records are used to provide FQDN-to-hostname mapping and to specify priorities, weights, port configuration and Time to Live (TTL). The record name is made up of the service and protocol in use.

There are only three valid DNS SRV transport protocol for SIP:

- _sip._tcp
- _sips._tcp
- _sip._udp (not supported by MiCollab)

Figure 1 shows two examples of supported DNS SRV records:

DNS SRV_sip._tcp.mbgfw.company.com

priority 1,weight 10 port 5060 host mbg101.company.com TTL 60min
priority 1,weight 30 port 5060 host mbg102.company.com TTL 60min
priority 2,weight 50 port 5060 host mbg103.company.com TTL 60min

DNS SRV _sips._tcp.mbgfw.company.com

priority 1,weight 10 port 5061 host mbg101.company.com TTL 60min
priority 1,weight 30 port 5061 host mbg102.company.com TTL 60min
priority 2,weight 50 port 5061 host mbg103.company.com TTL 60min

Figure 1: Examples of DNS SRV Records

In the above example,

- FQDN of the MBG cluster is "mbgfw.company.com’
- Primary registrar/proxy = mbgfw.company.com
- "mbgfw.company.com" maps to the following MBG nodes:
  - mbg101.company.com
  - mbg102.company.com
  - mbg103.company.com
- priority: determines the order in which the MBGs are used. In the example above, mbg101 and mbg102 (priority 1) would be utilized before mbg103 (priority 2).
- weight: determines the workload handled by the MBGs and the higher the weighting the greater the workload. The workload for an MBG is equal to its weighting divided by the total weighting for the assigned priority. For example, mbg102 would handle 3/4 the workload for the priority 1 MBGs.
- port: identifies the SIP port used (5060 is default for TCP; 5061 is default for TLS)
- TTL: identifies the length of time that the data lives in the network. In this example, after 60 minutes the timer expires and the softphone will update its Registrar/Proxy file with the latest version from the DNS server.

TYPICAL DEPLOYMENT

In a typical Cloud deployment, the softphones use DNS SRV records to receive service through a preferred cluster of two or more MBGs with access to a backup MBG cluster. The MBGs in the cluster provide access to a communications platform (MiVoice Business, MiVoice 5000 or MiVoice MX-ONE). The communications platforms can also provide varying degrees of resiliency.

Figure 2 shows a deployment in which DNS resiliency for the MiCollab Client for Mobile softphones is supported by two MBG clusters.

On Startup, or after the TTL expires, the softphone queries the DNS server and the DNS server returns the list of configured MBGs. The softphone starts with the highest priority entries and selects an MBG based on the weightings. If the MBG is unavailable, the softphone attempts to connect to other members at the same priority level; otherwise, it moves a member at the next priority level down. This distributes the load according to weights across the available MBGs.

You can also create a lower priority list on the DNS server that directs the softphone service to another MBG cluster to provide reasonable (possibly more expensive) service in the event that the MBG cluster associated with higher priority list goes out of service.

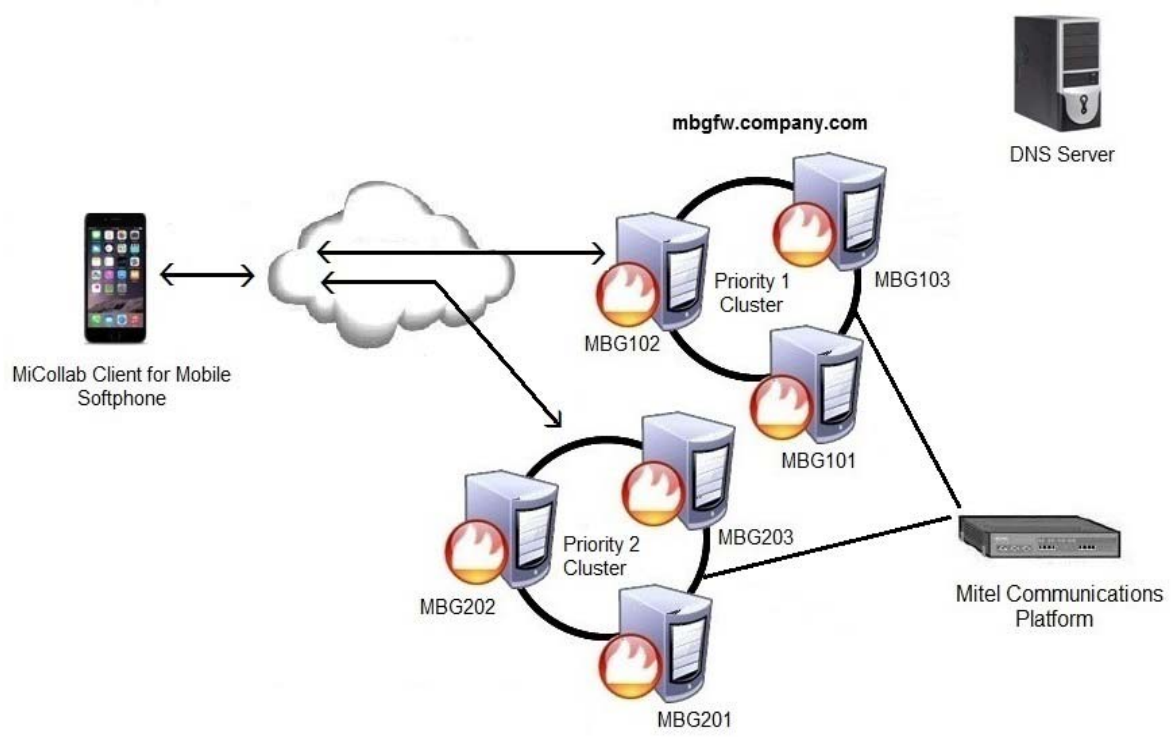

Figure 2: Softphone Resiliency in Cloud Deployment

The softphones periodically poll the MBGs in the higher priority list so that once service is restored, the user's softphone returns to the preferred MBG cluster.

MiCollab Client for Mobile softphones use SRV records. Other SIP phones can use other DNS queries, such as A-records or NAPTR. Figure 3 shows an example of DNS SRV entries for resilient softphones (assuming equal weighting):

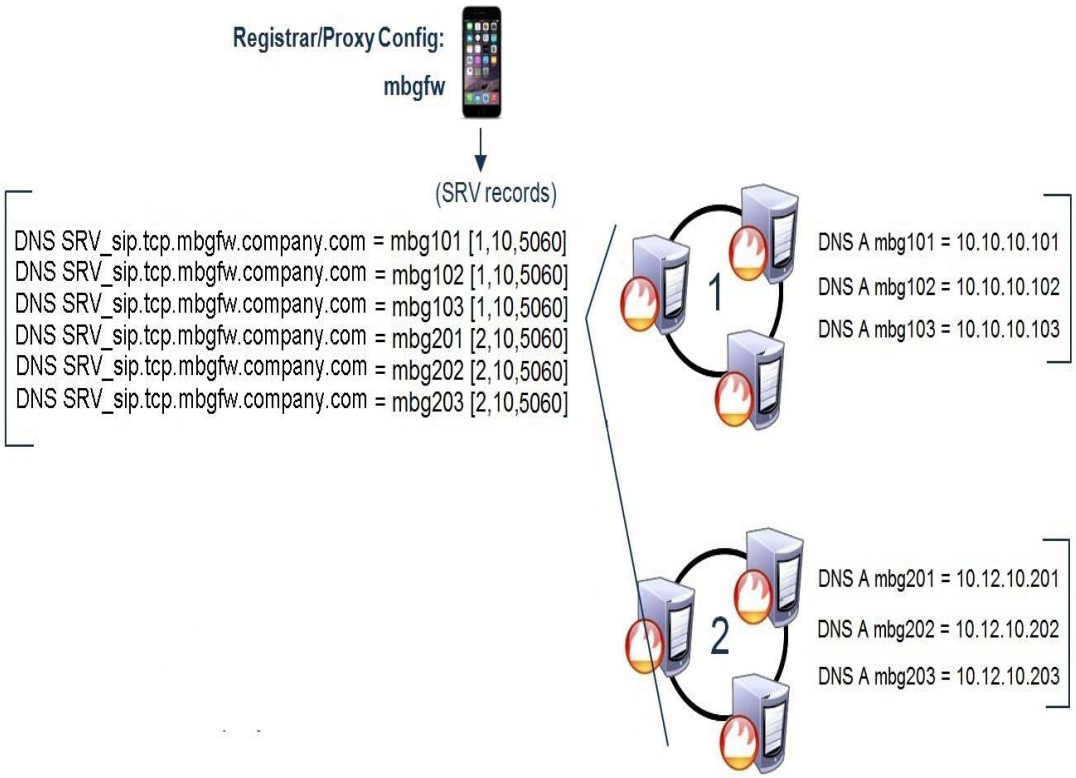

Figure 3: DNS SRV Entries for Resilient Softphones

CLIENT SOFTPHONE RESILIENCY

The Registrar/Proxy file in the MiCollab Client for Mobile softphone lists the hostnames of multiple MBGs. The softphone can register with any of the MBGs in the list subject to the priority and weighting settings. The softphones register on client start-up or after the Registration interval time expires.

If the MBG is taken out of service

1. If the MBG to which a softphone is registered is taken out of service, or if the connection to that MBG is lost, the user's call is dropped.
2. Calls that are in setup state when the MBG outage occurs are also dropped. The user is notified of the failure.
3. When the service outage occurs, the softphone initiates registration with another MBG in the list.
4. Incoming calls from other parties cannot connect with the softphone until it registers with the alternate MBG. During this registration period, incoming calls are routed to voicemail if the user has a mailbox on a Mitel communications platform.
5. After the softphone registers, it receives full service from the alternate MBG.
6. After the original MBG returns to service, the softphone remains on the alternate MBG unless it is redirected back to the original MBG based on priority or weight settings.

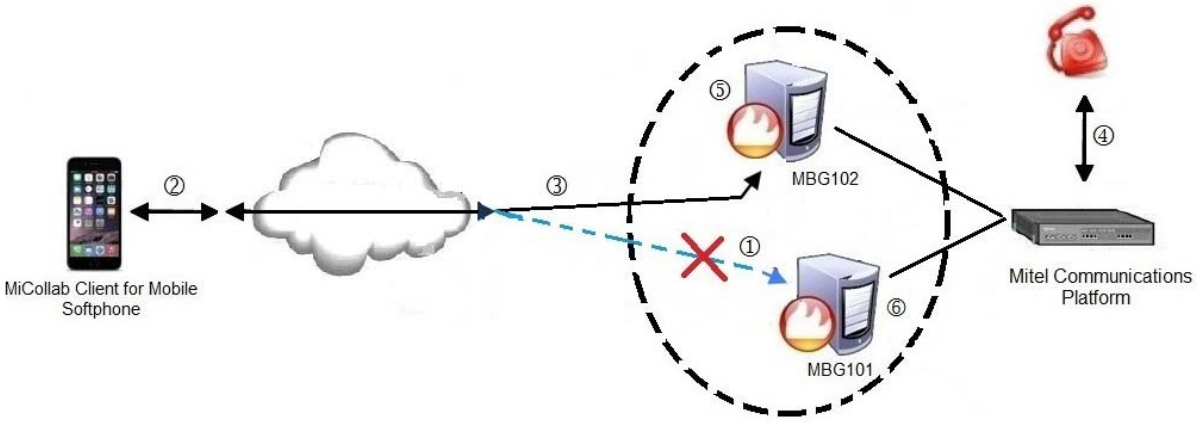

Figure 4: Client Softphone Resiliency

TLS and SRTP support

The softphones support TLS and SRTP for audio when they are connected to the following communication platforms:

- MiVoice Border Gateway
- MiVoice Business
- MiVoice 5000, and
- MiVoice MX-ONE

TLS versions 1.0, 1.1 and 1.2 are supported for SIP traffic encryption as well as SRTP (using SDES) to encrypt audio media streams.

The video stream is not encrypted or decrypted in MiCollab Release 7.0.

All SIP related security measures (SDES parameter negotiation in the Session Description Protocol (SDP) in the softphone are handled by the M5t SIP stack while all of the low-level certificate and key management is handled by OpenSSL 1.0.1 or higher.

Supported RFCs

The MiCollab Client for Mobile softphone supports the following Request for Comments (RFCs):

- RFC 1321 The MD5 Message-Digest Algorithm For authentication
- RFC 2246 The TLS Protocol Version 1.0
- RFC 2782 A DNS RR for specifying the location of services (DNS SRV)
- RFC 2976 The SIP INFO Method
- RFC 3261 SIP v2.0: Session Initiation Protocol
- RFC 3263 Session Initiation Protocol (SIP): Locating SIP Servers (NAPTR)
- RFC 3264 An Offer/Answer Model with SDP
- RFC 3265 SIP-Specific Event Notification (Subscribe/Notify)
- RFC 3311 The Session Initiation Protocol UPDATE Method
- RFC 3323 Privacy Mechanism
- RFC 3325 Private Extensions to the SIP for Asserted Identity within Trusted Networks
- RFC 3326 The Reason Header Field for the Session Initiation Protocol (SIP)
- RFC 3515 The Session Initiation Protocol (SIP) Refer Method
- RFC 3550 RTP: A Transport Protocol for Real-Time Applications
- RFC 3551 RTP Profile for Audio and Video Conferences with Minimal Control
- RFC 3725 Best Current Practices for Third Party Call Control
- RFC 3842 A Message Summary and Message Waiting Indication Event Package
- RFC 3891 The Session Initiation Protocol (SIP) 'Replaces' Header
- RFC 3892 The SIP Referred-By Mechanism
- RFC 3960 Early Media and Ringing Tone Generation
- RFC 4028 Session Timers
- RFC 4566 SDP: Session Description Protocol
- RFC 5923 Connection Reuse in the Session Initiation Protocol (SIP)

CONFIGURATION

Prerequisites

- MiCollab installed with Release 7.0 or later software
- MBGs installed, configured, and clustered
- DNS server and available domain name.

Configure MiCollab Client Softphones

1. Log into the MiCollab server manager.
2. Under **Applications**, click **MiCollab Client Deployment**.
3. Configure the MiCollab Client for Mobile softphones using the MiCollab Client Deployment blade. Refer to the help for instructions. During configuration, create client profiles with the FQDN of the MBG Cluster.

Specify FQDN of MBG Cluster

Specify the Fully Qualified Domain Name of the MBG cluster in the MiCollab Client Deployment Profiles.

1. Log into the MiCollab server manager.
2. Under **Applications**, click **MiCollab Client Deployment**.
3. On the **Deployment Profiles** tab, create client profiles with the FQDN of the MBG cluster.
   - Under **General Settings**, ensure that the **User Teleworker** option is checked.
   - Set the MBG SIP host field to "Custom DNS SRV".
   - Enter the FQDN of the MGB cluster (for example: mbgfw.company.com).

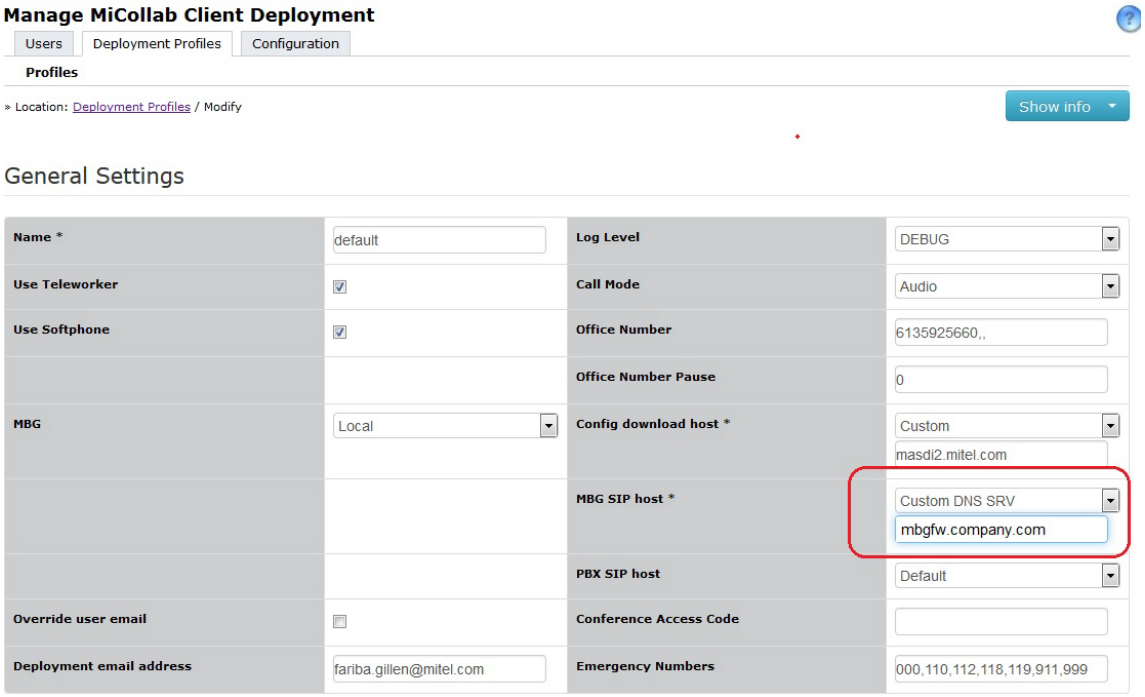

Figure 5: MBG Cluster FQDN

Configure the MBGs

Configure each MBG with the hostnames of the other MBGs in the cluster. Figure 6 shows an example of a cluster with their hostnames:

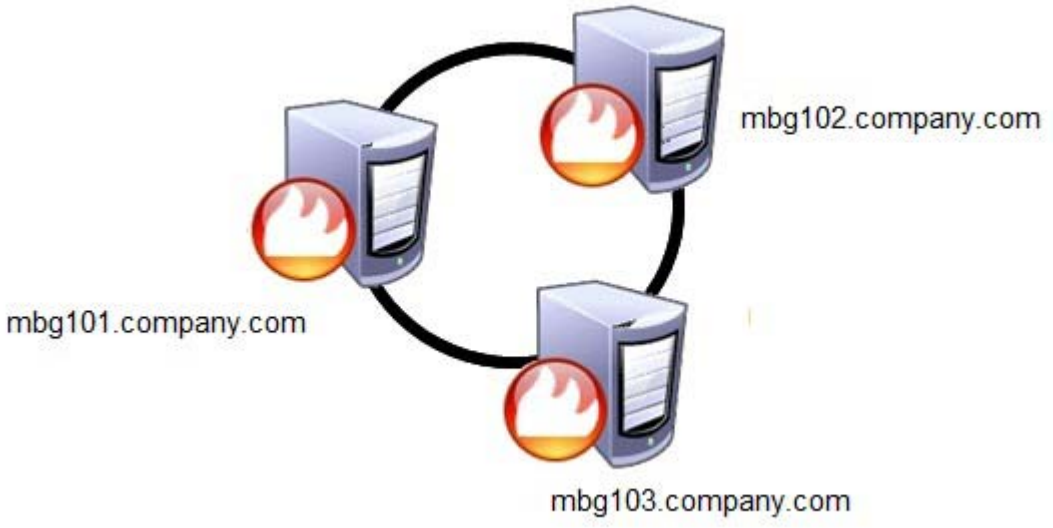

Figure 6: MBG Cluster with Hostnames (example)

Complete the following steps on *each MBG in the cluster*:

1. Log into the MBG server manager (for example: mbg201.company.com).
2. Click **System Configuration > Settings**.

3. Under **SIP Options**, ensure that the TCP/TLS box is checked.
4. Under **Allowed URI names** (see Figure 7):
   - Click **Add another** to add fields for the other MBGs
   - Enter the hostnames of the other MBGs in the cluster (see Figure 6 for an example of an MBG cluster with their hostnames).
5. Click **Save**.

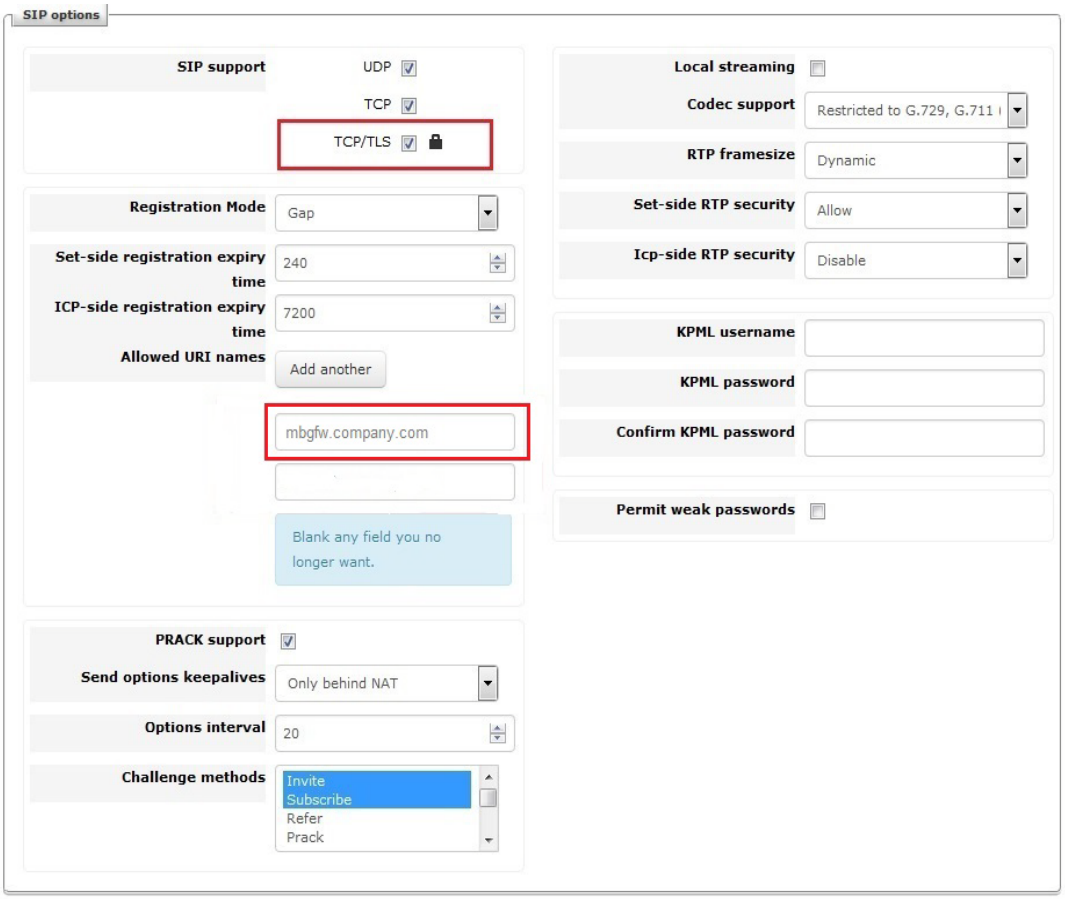

Figure 7: MBG SIP Options

6. Add the following configuration override to each MBG:

FILENAME	SECTION	PARAMETER	CONTENT
tug.ini	proxy::sip_tcp	idle_timeout	1200
tug.ini	proxy::sip_tls	idle_timeout	1200

This configuration override will prolong the life of the mobile phone batteries.

Configure DNS Server

Configure the DNS SRV records on the DNS server to provide the MBG FQDN to MBG cluster member hostname mapping, and to specify priorities, weights, port configuration and Time to Live (TTL). Figure 3 on page 4 provides a mapping example.

Figure 8 below shows an example of the DNS server configuration settings.

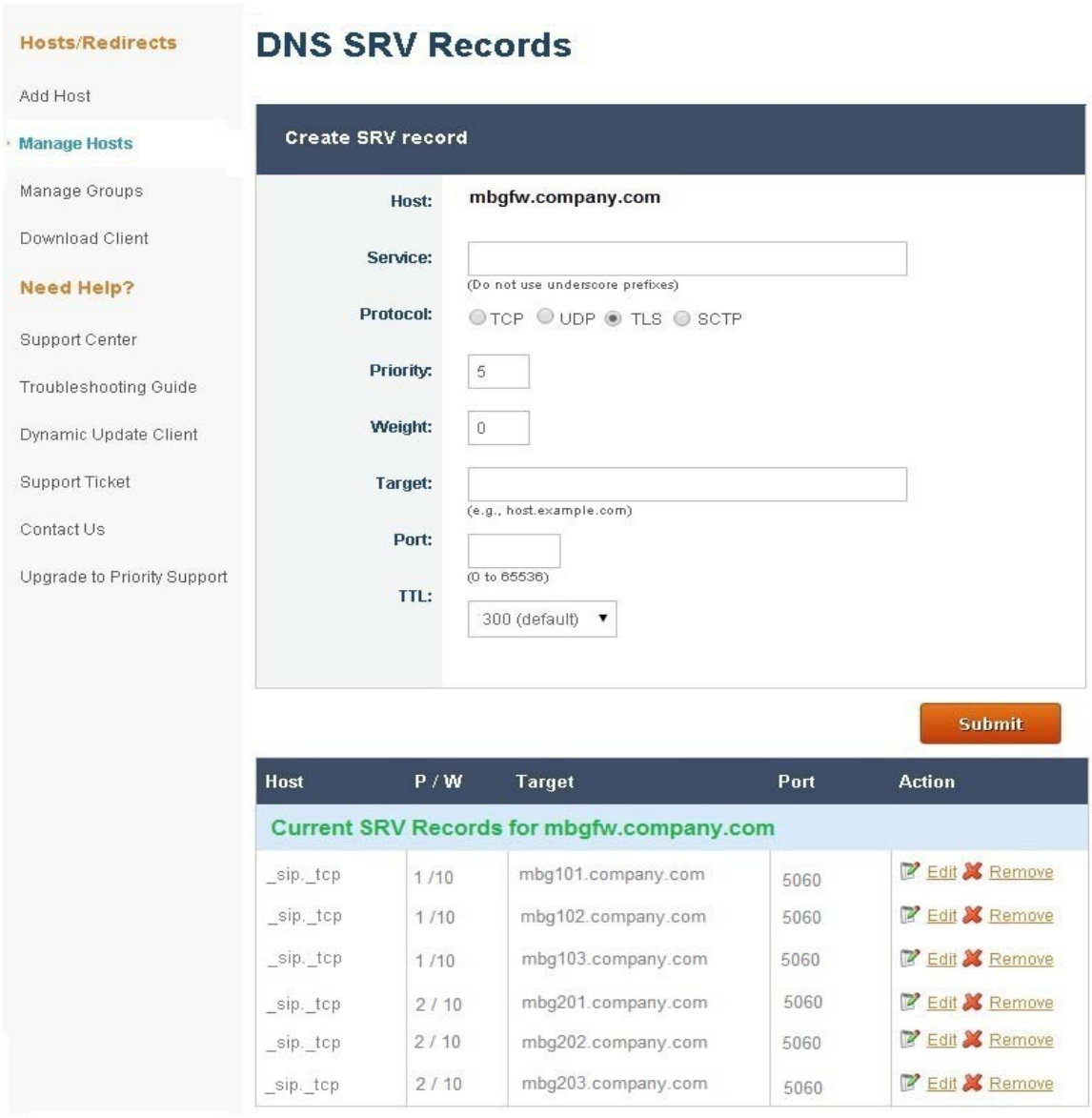

Figure 8: Configuration on DNS Server