Servizi VoIP

Guide

PBX

Asterisk

Guida per la configurazione

Istruzioni per l'interfacciamento con i servizi VoIP Unidata

UNIDATA SPA
Via Portuense, 1555
00148 Roma – Italia
Commercity M26

Tel +39 06 404041
Fax +39 06 40404002
www.unidata.it
info@unidata.it

C.F. - P.IVA 06187081002

Introduzione

Unidata permette di eseguire l'autenticazione verso Asterisk in due modalità: per account e per IP.

In genere, a meno di necessità particolari, Unidata preferisce l'autenticazione per account in quanto si adatta meglio alle più diverse situazioni.

Le istruzioni che seguono prevedono la configurazione nativa (da file di configurazione Asterisk) oppure tramite l'interfaccia web FreePBX e suoi derivati (Elastix, Trixbox, ecc).

L'account è rappresentato dal numero telefonico assegnato al cliente, sia esso un numero completo oppure un GNR (Gruppo Numerazione Ridotta).

> ⚠ Il numero deve sempre contenere anche il prefisso italiano 39
>
> *Esempio: 3906404041*

E' fondamentale per la vostra sicurezza configurare un firewall per proteggere il PBX da attacchi esterni come descritto al capitolo *Configurazione Firewall*.

Autenticazione per account

Interfaccia FreePBX/Elastix

1. Da Elastix: **PBX > Trunks > Add Trunk > Add SIP Trunk** e popolare

    a) **General Settings/Trunk Name**: nometrunk
    b) **Outgoing Settings/Trunk Name**: nometrunk
    c) **Outgoing Settings/Peer Details**:
    canredirect=no
    canreinvite=no
    host=217.72.100.4
    insecure=invite,port
    type=peer
    username=numero
    secret=password

2. **Incoming Settings/User Details**: <cancellare tutto>
3. **Registration/Register String**:numero:password@217.72.100.4/numero

Configurazione Asterisk

Eseguire le aggiunte seguenti ai file di configurazione di Asterisk sostituendo le parti colorate con i valori opportuni.

Aggiungere al file sip.conf di Asterisk un nuovo trunk:

```
[nometrunk]
canredirect=no
canreinvite=no
host=217.72.100.4
insecure=invite,port
type=peer
username=numero
secret=password
```

e alla sezione [general] una nuova registrazione:

```
[general]
register=numero:password@217.72.100.4/numero
```

Autenticazione per IP

Configurazione Asterisk

Eseguire le aggiunte seguenti ai file di configurazione di Asterisk sostituendo le parti colorate con i valori opportuni.

Aggiungere al file sip.conf di Asterisk un nuovo trunk:

```
[nometrunk]
canredirect=no
canreinvite=no
host=217.72.100.4
insecure=invite,port
type=peer
username=ip_pbx
secret=cisco
```

sostituendo **ip_pbx** con l'indirizzo IP di Asterisk, ovvero dall'IP da cui provengono le chiamate.

> ⚠ L'IP inserito nella configurazione deve essere STATICO e PUBBLICO.
>
> Se l'IP del PBX non è stato assegnato da Unidata oppure ancora non è stato comunicato alla divisione VoIP, è necessario fornirlo inviandolo all'indirizzo voip@unidata.it

Interfaccia FreePBX/Elastix

1. Da Elastix: **PBX > Trunks > Add Trunk > Add SIP Trunk** e popolare

   a) **General Settings/Trunk Name**: nometrunk
   b) **Outgoing Settings/Trunk Name**: nometrunk
   c) **Outgoing Settings/Peer Details**:
   canredirect=no
   canreinvite=no
   host=217.72.100.4
   insecure=invite,port
   type=peer
   username=ip_pbx
   secret=cisco

2. **Incoming Settings/User Details**: <cancellare tutto>

Configurazione Firewall

Se il PBX è attestato su una rete protetta da firewall, per il corretto funzionamento dei servizi VoIP Unidata è sufficiente eseguire le aperture:

Direzione	Protocollo	Porta sorgente	Porta destinazione	Host
Ingresso	UDP	Any	Any*	217.72.100.4 (SIP)
Ingresso	UDP	Any	Any	217.72.100.8 (RTP)
Uscita	UDP	Any	Any*	217.72.100.4 (SIP)
Uscita	UDP	Any	Any	217.72.100.8 (RTP)

* è possibile restringere il range di porte utilizzate, ma al momento tale pratica è sconsigliata perché l'evoluzione futura dei servizi VoIP potrebbe richiedere ulteriori porte da aprire con conseguenti modifiche alla configurazione.

Consigliamo vivamente di limitare il più possibile l'accesso al PBX e consentire connessioni solo da reti conosciute. Vengono continuamente scoperte vulnerabilità che potrebbero mettere in pericolo la sicurezza del PBX. L'errata o mancata configurazione di un firewall espone al rischio di frodi telefoniche, truffe, e altri comportamenti dannosi.