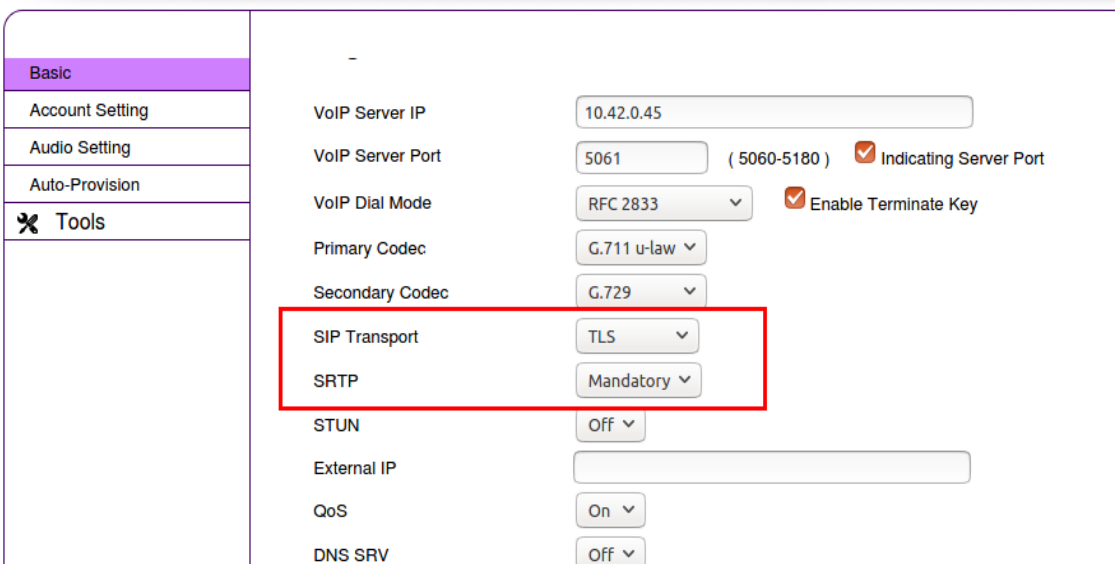
Release Note for TLS configuration in DuraFon-SIP

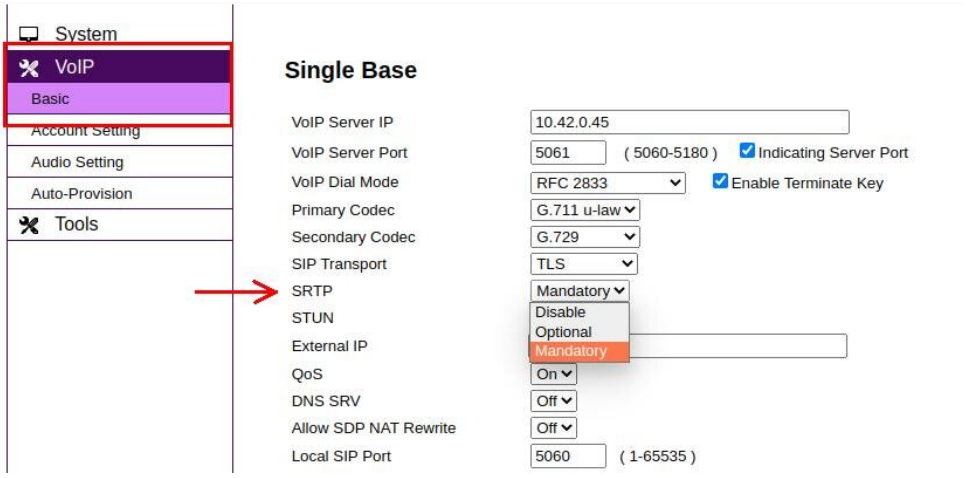
1. Overview

DuraFon-SIP supports TLS1.0, TLS 1.1 and TLS 1.2 for website GUI and SIP messaging. For website GUI, as a TLS client role in DuraFon-SIP, it follows the TLS web server to specify the version of TLS.

For SIP messaging, you need to select “Basic->SIP Transport” with TLS item as the photo in red mark.



Select “Baic->SRTP” with “Mandatory” item to force using SRTP directly without negotiate with the SIP server.



Once TLS is selected the phone will always negotiate the highest possible TLS version in the handshaking process. TLS 1.2, 1.1 and 1.0 are supported.

Note that there are no other Certificates setting required.

2. Test Scan

Use Tenable Nessus to do Vulnerabilities by Host. According to the below item 25 in test cases, DuraFon-SIP supports TLS 1.2.

Item	Severity	CVSS v2.0	Plugin	Name
1	MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
2	MEDIUM	6.4	57582	SSL Self-Signed Certificate
3	LOW	2.6	26194	Web Server Transmits Cleartext Credentials
4	INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
5	INFO	N/A	45590	Common Platform Enumeration (CPE)
6	INFO	N/A	54615	Device Type
7	INFO	N/A	35716	Ethernet Card Manufacturer Detection
8	INFO	N/A	86420	Ethernet MAC Addresses
9	INFO	N/A	84502	HSTS Missing From HTTPS Server
10	INFO	N/A	11219	Nessus SYN scanner
11	INFO	N/A	19506	Nessus Scan Information
12	INFO	N/A	11936	OS Identification
13	INFO	N/A	10919	Open Port Re-check
14	INFO	N/A	56984	SSL / TLS Versions Supported
15	INFO	N/A	10863	SSL Certificate Information
16	INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
17	INFO	N/A	21643	SSL Cipher Suites Supported
18	INFO	N/A	94761	SSL Root Certification Authority Certificate Information
19	INFO	N/A	22964	Service Detection
20	INFO	N/A	21642	Session Initiation Protocol Detection
21	INFO	N/A	25220	TCP/IP Timestamps Supported
22	INFO	N/A	136318	TLS Version 1.2 Protocol Detection
23	INFO	N/A	10287	Traceroute Information
24	INFO	N/A	11032	Web Server Directory Enumeration
25	INFO	N/A	10386	Web Server No 404 Error Code Check

Plugins / Nessus / 136318

TLS Version 1.2 Protocol Detection

Language: English

INFO Nessus Plugin ID 136318

Information | Dependencies | Dependents | Changelog

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Plugin Details

Severity: Info

ID: 136318

File Name: tls12_detection.nasl

Version: 1.1

Type: remote

Family: Service detection

Published: 5/4/2020

Updated: 5/4/2020

Vulnerability Information

Required KB Items:
SSL/Supported

The detail information is referred to

Test_Scan_SP935
_v0.13.6.html

~End of Documentation