Linksys by Cisco

APPLICATION NOTE

Security in IP Telephony: Activating SIP over TLS on Cisco SPA Products

This document overviews the implementation of IP Telephony Signaling Security mechanisms on Cisco SPA products. In particular, this document reviews the use of Transport Layer Security (TLS) for Session Initiation Protocol (SIP) sessions from Cisco Analog Terminal Adaptor (ATA) and IP phone devices.

This document assumes that the reader has reviewed the *Cisco SPA9000/Linksys Voice System Administration Guide* and the *Cisco/Linksys SPA Provisioning Guide*. Cisco SPA devices, both IP phones and ATAs, are referred to as SPA in this document.

Why is Standards-Based IP Telephony Security Important?

Security for VoIP calls is important because unauthorized third parties may try to intercept and/or insert packets into VoIP telephone calls. Security via other methods, such as VPNs, may cause performance issues, such as excessive delay or jitter, which diminish voice quality. Standards-based authentication and encryption methods deliver effective VoIP call security and prevent call snooping or voice path substitution by unauthorized third parties.

In addition, another potential benefit of migrating to a secure signaling method is the change from UDP to TCP for transport of the signaling messages. Although secure TCP sessions can require more call set-up processing, the frequency of on-going SPA SIP registration messages can be reduced. This reduction in signaling messages can reduce the load on service provider networks.

What is IP Telephony Security?

IP telephony security requires securing both the control channel and the voice path. Session security is based on authenticating the parties in the call and then encrypting the communication between the parties. Standards-based security methods for authentication and encryption ensure that the communication is not compromised.

cisco

Security on the control channel, or SIP signaling plane, requires authentication and encryption of IP telephony signaling protocols. Cisco SPA uses SIP as the VoIP signaling protocol. Typical signaling security risks include privacy of user account information.

Security on the voice path, or media plane, requires authentication and encryption of the media protocols. Cisco SPA uses RTP as the VoIP media protocol. Typical media security risk includes privacy of the voice communication.

Which IETF RFCs Have Been Implemented?

Selected Cisco SPA devices use standards-based security for IP telephony signaling:

- Control channel: The TLS Protocol Version 1.0, which is defined in RFC 2246
- Voice path: Secure Real-Time Protocol

This document reviews the SPA's TLS implementation.

Which SPA Devices Support TLS?

The following SPA devices will support TLS in firmware release 5.0 or later:

- ATA: SPA2102, SPA3102, WRP400
- Phones: SPA922, SPA942, SPA962

Detailed Explanation of TLS on SPA Devices

This section covers TLS components and their basic configuration. Each Service Provider network will be implemented differently but many similarities exist and are covered below.

Service Provider TLS Network Components

The TLS features require functionality on the SPA and in a Service Provider network element. The solution will also typically require a Session Border Controller (SBC) that supports TLS. This document assumes that an SBC will be used.

SPA TLS Call Signaling with an SBC

The signaling between the SPA (client) and the SBC (server) is secured by using the mechanisms defined in RFC 2246, The TLS Protocol Version 1.0. The SPA TLS implementation requires the SIP signaling to use TCP rather than UDP for transport on the IP networks. As a result, the endpoints can utilize TCP redundancy and security functionality.

When the TLS feature is enabled, the SPA initiates a TLS session to the SBC. The SBC returns a public certificate to the SPA. The SPA uses this information to create a shared secret key and performs the key exchange with the SBC. The SPA then initiates a session by using the shared secret to encrypt the signaling path to the SBC. As an additional security measure, the SBC can authenticate the SPA provided that the SBC has the correct client root certificate. The client root certificate is available from the Cisco sales team.

When the TLS session is set up, all SPA calls use this TLS session. If the TLS session drops, the SPA re-initiates the TLS session. The failure and retry mechanisms are per RFC2246.

NOTE: If the SBC is performing client authentication, then a TLS session can take approximately 12 seconds to initiate. The session time-out timers on the SBC must be set to 15 seconds or more. If two lines are used on the SPA, then the second line will only initiate the TLS session after the first line's session is stable.

NOTE: Service providers may be able to reduce SIP registration traffic by using TLS. TLS can utilize TCP error checking and retry mechanisms. When a TCP session is established, the service provider may find that SIP registration requests and acknowledgements, which can be used as UDP keep-alives, can be reduced. The SPA SIP registration timers are configurable, and the Service Provider can adjust these timers on the ATA as needed.

Activating TLS by Using the SPA User Interface

This section includes procedures for activating TLS by using the user interface.

For SPA2102,SPA3102, and WRP400

To activate TLS on the ATA, complete the following steps:

1. Start Internet Explorer and enter the IP address of the SPA to connect to the administration web server.

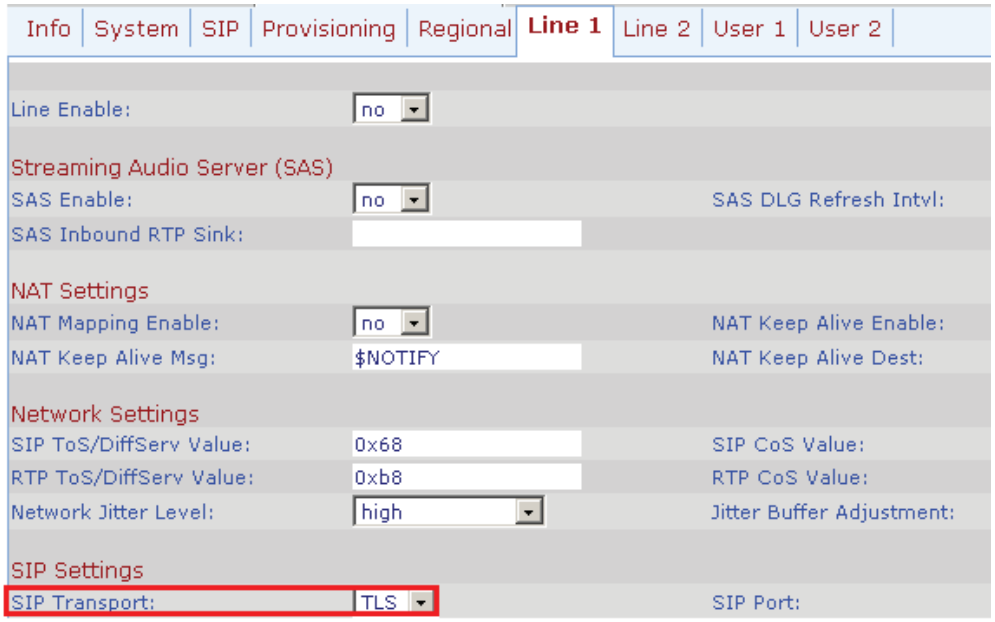
   NOTE: To learn the IP address of the SPA2102 or the SPA3102, connect an analog phone to the Phone 1 port. Lift the receiver, dial ********, then dial **110#**, and listen as the IP address is announced. Also, if the device does not allow for remote web access, dial ********, then dial **7932#**. Listening to the prompts, enter **1#** to enable WAN access and then enter **1** to save the settings.

2. Choose **Admin Login** and **Advanced** settings.

3. Click **Voice tab > Line 1** or **Line 2**. (SPA3102 has Line 1 only. SPA2102 and WRP400 have Line 1 and Line 2.)

4. Scroll down to the *SIP Settings* section.

5. In the *SIP Transport* field, choose **TLS**.



6. On SPA2102 and WRP400, repeat these steps to activate TLS on Line 2.

7. Click **Submit All Changes**.

For SPA9x2 Phones

To activate TLS on a SPA9x2 phone, complete the following steps:

1. Start Internet Explorer and enter the IP address of the SPA phone to connect to the administration web server.

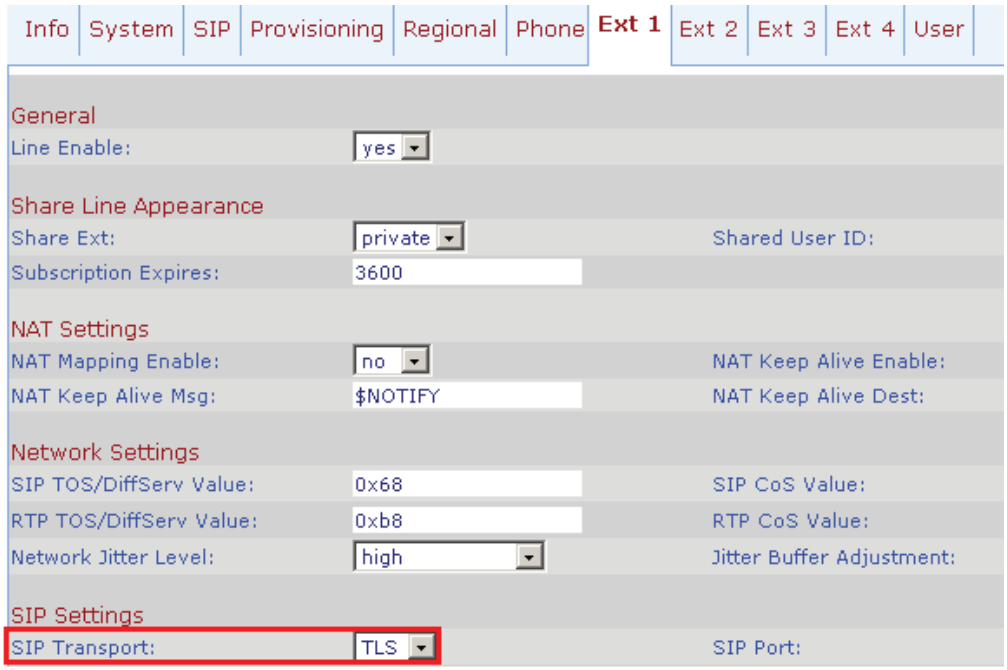
   NOTE: To learn the IP address of a SPA9x2 phone, press the menu key on the phone. Choose **9 – Network**, and then make note of the address in the *Current IP* field.

2. Choose **Admin Login** and **Advanced** settings.

3. Click the tab for the extension that you want to configure (*Ext 1*, *Ext2*,…).

4. Scroll down to the *SIP Settings* section.

5. In the *SIP Transport* field, choose **TLS**.



6. Click **Submit All Changes**.

7. Repeat these steps for each extension and each phone that you need to configure.

Activating TLS via Configuration Profile Parameter Settings

To activate TLS in the configuration profile, use the following parameter setting in the configuration template. To learn more about remote provisioning, please ask your Cisco account representative for the confidential *Cisco/Linksys SPA Provisioning Guide*.

Parameter Name	Description	Length	Default	To Enable TLS
SIP Transport	Instructs SPA to use a specific transport type (UDP, TCP or TLS)	Str03	No	**Set to TLS.** **SIP Transport{1} "TLS";**

Sample TLS Testing Checklist and Milestones

The following list outlines the potential steps required by a Service Provider to support TLS.

Step	Action Item
1	The Service Provider configures the SBC for TLS encryption of SIP signaling path. Optional for client authentication: The Service Provider obtains the client root certificate from Cisco and configures this root certificate on the SBC, per the SBC manufacturer's instructions.
2a	The Service Provider loads TLS-enabled firmware onto the SPA via the windows utility or via provisioning.*
2b	The Service Provider activates the TLS option in the SPA configuration profile via the Web GUI or via provisioning.
2c	The Service Provider activates the SPA debug server functionality on the SPA via the web GUI or via provisioning. The Service Provider activates the syslog server.
3a	The subscriber resets the SPA.
3b	Optional: The Service Provider should see the SSL session setup in Debug Log.
3c	The Service Provider confirms registration on Softswitch and makes call.

* Provisioning means updating the SPA configuration profile and then storing it on the Service Provider's provisioning server. The SPA then needs to fetch the configuration profile, which may also require the unit to fetch its firmware as well. More information is available in the *Linksys SPA Provisioning Guide*.

Troubleshooting

The following provides a list of Frequently Asked Questions (FAQ) regarding Cisco/Linksys SPA TLS implementation.

Issue: SPA will not set up TLS session

If the SPA will not set up a TLS session, check the time-out timers on the SBC. These timers should be at least 15 seconds. If the timers are correct, activate TLS and then run the SPA debug log and/or network traces. When these logs are captured, open a trouble ticket report and provide the logs to the support team.

Issue: SPA will not register

Try to register without TLS. When registration without TLS is verified, activate TLS and then run the SPA debug log and/or network traces to verify that the TLS session is being set up. If the SPA still does not register, contact Cisco/Linksys support.

Issue: SPA will not make calls

Confirm that the SPA is registered in Softswitch. Try to make calls without TLS. When call completion is verified without TLS, check the time-out timers on the SBC. These timers should be at least 15 seconds. Please enable the debug logs and confirm that the TLS session is set up. If the SPA still does not make or receive calls, please contact Cisco/Linksys support.

Issue: SPA has one-way audio

Confirm that the SPA is registered. Try to make calls without TLS enabled. When call completion is verified without TLS, enable the network traces. Confirm that the media packets are being sent in both directions and verify that the packets contain audio. If the SPA still has one-way audio, contact Cisco/Linksys support.

How do I debug my SPA? Is there a syslog / debug log?

A: The SPA sends out debug information via syslog to a syslog server. The ports can be configured (the default is 514), and do the following:

- Make sure you don't have a firewall running on your PC that potentially would block port 514.
- On the *System* page, set the Debug Server field to the IP address and port of your syslog server. Note that this IP address has to be reachable from the SPA. Also, set the *Debug Level* field to **3**.
- To capture SIP signaling messages, click the **Line** tab, and then set the *SIP Debug Option* field to **Full**. The output will be in a file named syslog.514.log.

Trouble Ticket Reporting

US/Canada Contacts

24-Hour Technical Support

US/Canada: 866-606-1866

Mexico: 800-314-0939

Support Web Site

http://www.linksys.com/support

Global Contacts

http://www.linksys.com/international

Related Documents

- RFC 2246, The TLS Protocol Version 1.0
- RFC 3711, Secure Real-Time Transport Protocol
- *Cisco/Linksys SPA9000 Voice System Administration Guide*
- *Cisco/Linksys SPA Provisioning Guide*
- *Cisco/Linksys SPA9x2 Phone Admin Guide*