

STIR/SHAKE using ClearIP

Contents

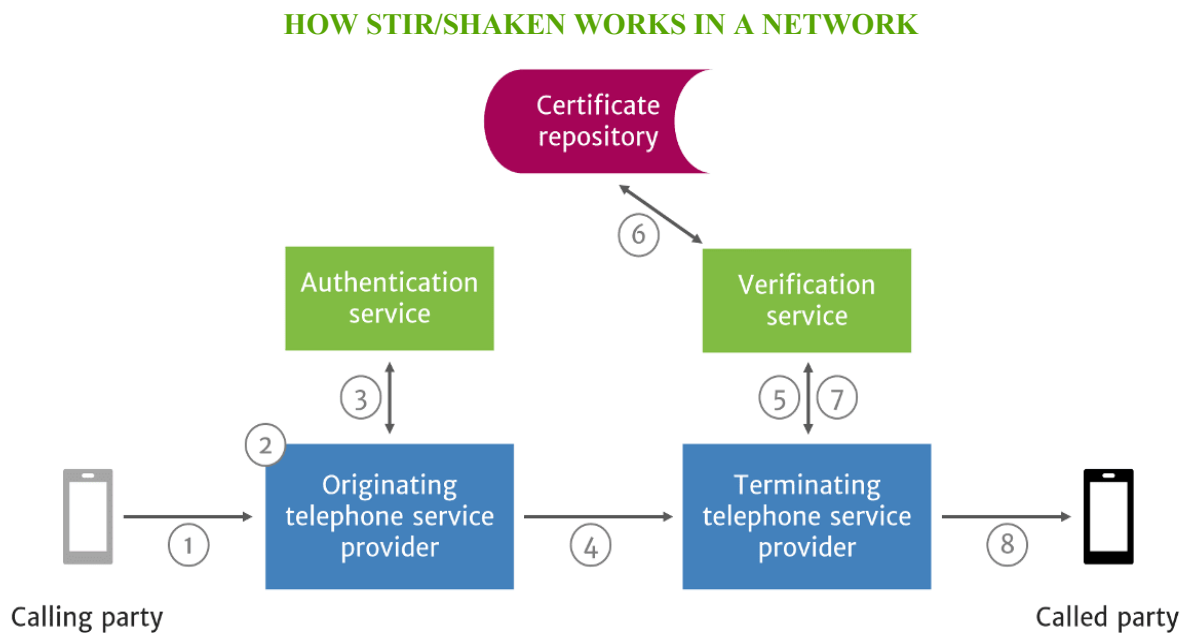
Contents	1
Overview	2
Configuring ClearIP	3
Organization.....	3
SBC	3
Service Provider	5
Groups.....	5
Users	5
STI.....	6
Certificates	6
Authentication Policies	6
Verification Policies.....	7
Cirrus Configuration	7
cirrussca.cfg	7
clearip.cfg.....	8
Adding CirrusSCA to Pacemaker	10
Adding CirrusSCA to Keepalived	10
Example CirrusSCA Configuration Files.....	11
cirrussca.cfg	11
clearip.cfg.....	11

Overview

This document details how to enable STIR/SHAKEN in Cirrus using ClearIP.

STIR/SHAKEN uses digital certificates, based on common public key cryptography techniques, to ensure the calling number of a telephone call is secure. In simple terms, each telephone service provider obtains their digital certificate from a certificate authority that is trusted by other telephone service providers. The certificate technology enables the called party to verify that the calling number is accurate and has not been spoofed. The details of how SHAKEN uses public key infrastructure is explained in our whitepaper on [Certificate Management for STIR/SHAKEN](#).

The following call flow diagram illustrates how STIR/SHAKEN works:



1. A SIP INVITE is received by the originating telephone service provider.
2. The originating telephone service provider checks the call source and calling number to determine how to attest for the validity of the calling number.
 - **Full Attestation (A)** — The service provider has authenticated the calling party and they are authorized to use the calling number. An example of this case is a subscriber registered with the originating telephone service provider's softswitch.
 - **Partial Attestation (B)** — The service provider has authenticated the call origination, but cannot verify the call source is authorized to use the calling number. An example of this use case is a telephone number behind an enterprise PBX.
 - **Gateway Attestation (C)** — The service provider has authenticated from where it received the call, but cannot authenticate the call source. An example of this case would be a call received from an international gateway.
3. The originating telephone service provider uses the authentication service to create a SIP Identity header. The authentication service could be a third-party service hosted in the cloud a software application integrated with the telephone service provider's softswitch or Session Border Controller (SBC). The SIP Identity header contains the following data:

- Calling number
 - Called number(s)
 - Current timestamp
 - Attestation level
 - Origination identifier
4. The SIP INVITE with the SIP Identity header is sent to the terminating telephone service provider. In addition, the Identity token may be sent across the internet, [out-of-band, to the terminating provider's Call Placement Service](#)
 5. The SIP INVITE with Identity header is passed to the verification service.
 6. The verification service obtains the digital certificate of the originating telephone service provider from the public certificate repository and begins a multi-step verification process. If all verification steps are successful, then the calling number has not been spoofed.
 - The SIP Identity header is base64 URL decoded and the details are compared to the SIP INVITE message.
 - The public key of the certificate is used to verify the SIP Identity header signature.
 - The certificate chain of trust is verified.
 7. The verification service returns the results to the terminating service provider's softswitch or SBC.

The call is completed to the called party.

Phoenixsoft's STIR/SHAKEN is divided into two components. These are ClearIP and CirrusSCA. ClearIP is provided by TransNexus and CirrusSCA is provided by Phoenixsoft.

Prior to configuring STIR/SHAKEN you will need to get an account with TransNexus. Use the following link to contact TransNexus. <https://transnexus.com/contact-us/>

Configuring ClearIP

Before starting you will need to have an account on clearip.com and log into the site. You will need to configure your organization and STI.

Organization

The first step is to configure your organization under the Organization drop-down. There is four parts to the organization. These are, SBCs, Service Providers, Groups, and Users.

SBC

Under SBC you will add the public IP address used by Cirrus. This will either be the IP address used by SILB or can be another IP address. It is recommended you use a different IP address so the CirrusSCA can run separate from SILB.

You will need to create a validation and authentication SBC with the same public IP address.

The tables below will list all fields that need to be set. All other fields can be left to the default value. Adding a Comment is option.

Validation

Field	Description	Example Value
Name	A unique name for this SBC. We would recommend naming it something like verification.XXX where XXX is the last 3 digits of the IP address.	verification.233
IP Address	The IP address that CirrusSCA will use.	216.160.198.233
Partition	A unique partition that will be used when sending verification request. I.e., any verification request will be sent to verification.sip.clearip.com	verification
Status	Whether this SBC is active, inactive, or blocked.	Active
Identity Header	The name of the SIP header the identity response will be sent in.	X-Identity

Authentication

Field	Description	Example Value
Name	A unique name for this SBC. We would recommend naming it something like authentication.XXX where XXX is the last 3 digits of the IP address.	authentication.233
IP Address	The IP address that CirrusSCA will use.	216.160.198.233
Partition	A unique partition that will be used when sending validation request. I.e., any validation request will be sent to validation.sip.clearip.com	authentication
Status	Whether this SBC is active, inactive, or blocked.	Active
Identity Header	The name of the SIP header the identity response will be sent in.	X-Identity

Service Provider

Create a service provider. We would recommend naming this the same as your company name.

Field	Description	Example Value
Name	A unique name for this service provider.	Phoenixsoft
Status	Status of the service provider. This can be either Active, Inactive, or Blocked.	Active

Groups

Create a new group under the service provide created above.

Field	Description	Example Value
Service Provider	The service provider this group will be under. Using the drop down select the service provide created above	Phoenixsoft
Name	A unique name for this group.	Phoenixsoft
Status	Status of the service provider. This can be either Active, Inactive, or Blocked.	Active

Users

Create three users named Attest-A, Attest-B, and Attest-C. The user will be used to determine the Attestation level when a call is authenticated.

Field	Description	Example Value
Service Provider	The service provider this group will be under. Using the drop down select the service provide created above	Phoenixsoft
Group	The group created above.	Phoenixsoft
Name	A unique name for this user. This will either be Attest-A, Attest-B, or Attest-C.	Attest-A

Status	Status of the service provider. This can be either Active, Inactive, or Blocked.	Active
--------	--	--------

STI

There are three parts that need to be configured under STI. These are Certificates, Authentication Policies, and Verification Policies.

Certificates

If you have a certificate add it under the certificate page.

Authentication Policies

You will need to create three policies. These are, Attest-A, Attest-B, Attest-C, and default.

Field	Description	Example Value
Service Provider	The service provider this group will be under. Using the drop down select the service provide created above	Phoenixsoft
Group	The group created above.	Phoenixsoft
User	The appropriate user for this policy. This will either be Attest-A, Attest-B, Attest-C, or blank (for the default case).	Attest-A
Status	Status of the service provider. This can be either Active, Inactive, or Blocked.	Active
Method	This can be set to either In-Band, Out-of-Band, or In-Band and Out-of-Band	In-Band
Action	The action used to create the Identity header. This will be set to the Attest level associated with the user. E.g., if the user is Attest-A then select action Attest A. If the user is blank set the action to Attest C.	Attest A
Certificate	The certificate used to sign the Identity header. Select the certificate created in the Certification section. If you do	Phoenixsoft

	not have a certificate leave this blank and TransNexus' certificate will be used, and the Attest level will be forced to C.	
--	---	--

Verification Policies

Field	Description	Example Value
SBC	The validation SBC that was created above.	validation.233
Status	Status of the service provider. This can be either Active, Inactive, or Blocked.	Active
Indication Method	The indication method to use to display the verification results.	Verstat
No Identity Header Action	How to handle calls where no STI header is present.	Report Only
Invalid Identity Header Action	How to handle calls when an error occurs validating the STI.	Indicate

Cirrus Configuration

CirrusSCA is designed to run on a single server under either pacemaker or keepalived. First, however, you will need to build the configuration files and make sure these files are saved on both servers.

cirrussca.cfg

This is the main configuration file used by CirrusSCA. Below are the parameters that need to be configured.

Parameter	Description	Example Value
ID	A unique ID for this application.	1000
Log_Path	The path where the log files will be saved. This directory must exist prior to running CirrusSCA	/usr/local/cirrus/logs/CirrusSCA/
Log_Mode	Where log message will be written to. This can be, FILE, COUT, FILE_COUT.	FILE
Log_Level	The maximum log level log message will be written.	DEBUG

MB_Interface	Define the MB interface. This parameter takes two values. These are IP address and port. You will need to define a MB interface for each instance of CirrusMB that is running on the system.	10.2.8.83 8654
Peer_Details	Define a peer connection. In this case it will be CLEARIP. You need to define a unique ID for this peer, the type (CLEARIP), and the configuration file used for this peer.	1 CLEARIP clearip.cfg
Default_SSID	Used to define the default SSID (STIR/SHAKEN ID).	PHOENIXSOFT
Request_Map	Map a request type, either AUTHENTICATE or VALIDATE to a peer. This parameter takes three values. These are, SSID, Type (AUTHENTICATE or VALIDATE), and a peer ID. The peer ID must match an ID of a peer defined under Peer_Details.	PHOENIXSOFT VALIDATE 1 PHOENIXSOFT AUTHENTICATE 1

clearip.cfg

Used to define the SIP connection to ClearIP.

Parameter	Description	Example Value
RAD_Log_Level	The log level used by the Radvision SIP stack. The log level is a bit mask with the following values: DEBUG 0x01 INFO = 0x02 WARN = 0x04 ERROR = 0x08 EXCEP = 0x10 LOCKDBG = 0x20 ENTER = 0x40 LEAVE = 0x80	0x1c

	It is recommended setting this to 0x1c which will log EXCEP, ERROR, and WARN.	
RAD_Log_Default_Filters	The default log filter level used by the Radvision SIP stack. It is recommended setting this to 0x1f.	0x1f
Run_Audit	Set to TRUE if we need to run an audit against the Radvision transactions.	FALSE
Number_Of_Simultaneous_Requests	The number of simultaneous requests.	2000
Msg_Size	The maximum size of a SIP messages. Because the INVITE or 302 response will include an Identity header this needs to be at least 2048.	3072
Peer	Define the peer connection to ClearIP. There are six parameters that need to be set. These are defined below.	See below for an example.

Peer Parameter

Parameter	Description	Example Value
SSID	The SSID this peer is associated with. This will be the same SSID used in the cirrussca.cfg file when defining a Reqeust_Map.	PHOENIXSOFT
Type	The type of request. This will be either AUTHENTICATION or VERIFICATION. Note: you will need to define a Peer for all combinations of an SSID and Type.	AUTHENTICATION
Own IP	The IP address CirrusSCA will bind to. This must match the IP address used when creating the SBC on ClearIP.	216.160.198.233
Own Port	The port this peer will use when creating the TCP connection to	5061

	ClearIP. Note: this port must be unique on the system and connect be the same port used by either SILB, SIRAD, or SupServer.	
Peer Host	The DNS used to connect to ClearIP. This will be a combination of the Partition used when creating the SBC and sip.clearip.com. E.g., for the Authentication SBC the partition was authenticate so the value would be authenticate.sip.clearip.com	authenticate.sip.clearip.com
Peer Port	The port used to connect to ClearIP.	5060
Transport	This must be set to TCP.	TCP

Adding CirrusSCA to Pacemaker

To run CirrusSCA under pacemaker you will need to create a new resource group and add the IP and SCA resource to this group.

Step	Description
1	Create link to the SCA heartbeat script. <pre>cd /usr/lib/ocf/resource.d/heartbeat ln -s /usr/local/cirrus/bin/sca.heartbeat.ocf sca</pre>
2	Create the SCA resource. <pre>pcs resource create SCA_IP ocf:heartbeat:IPaddr2 ip=216.160.198.233 cidr_netmask=28 op monitor interval=15s --group SCA pcs resource create SCAD ocf:heartbeat:sca op monitor interval=15s --group SCA</pre>

Adding CirrusSCA to Keepalived

Yet to be define. Under development.

Example CirrusSCA Configuration Files

cirrussca.cfg

```
//-----
// (C) Copyright 2001, PhoenixSoft, Inc.
//
// History
// Date      Person      Description
// -----
// 07/18/01  Stephen N    First Created
//
//-----

// Instance ID
ID = 1000

// Logging Parameters
Log_Path = /usr/local/cirrus/logs/CirrusSCA/
Log_Mode = FILE
Log_Level = DEBUG

// MB Parameters
//          IP
//          |          Port
//          |          |
MB_Interface = 10.2.8.83  8654
MB_Interface = 10.2.8.84  8654

// Peer Details
// ID
// | Type (CLEARIP, ...)
// | | Config File
// | | |
Peer_Details = 1  CLEARIP  clearip.cfg

// Default SSID. Used if no SSID in the request
Default_SSID = PHOENIXSOFT

// Request Map
// SSID
// |
// | Type (AUTHENTICATION, VALIDATION, ...)
// | | Peer Id (Must match a Peer_Detail ID above)
// | | |
Request_Map = PHOENIXSOFT  AUTHENTICATE  1
Request_Map = PHOENIXSOFT  VALIDATE      1
```

clearip.cfg

```
//-----
// (C) Copyright 2001, PhoenixSoft, Inc.
//
// History
// Date      Person      Description
// -----
// 07/18/01  Stephen N    First Created
//
//-----

// Logging Parameters
RAD_Log_Level = 0x1f
RAD_Log_Default_Filters = 0x1f

// Audit Parameters
Run_Audit = FALSE

// SIP Parameters
Number_Of_Simultaneous_Requests = 2000
Msg_Size = 3072
```

```

// Peer Details
//      SSID
//      |
//      |      Type (AUTHENTICATE or VALIDATE)
//      |      |
//      |      |      Own IP
//      |      |      |
//      |      |      |      Own Port
//      |      |      |      |
//      |      |      |      |      Peer Host
//      |      |      |      |      |
//      |      |      |      |      |      Peer Port
//      |      |      |      |      |      |
//      |      |      |      |      |      |      TCP
Peer = PHOENIXSOFT AUTHENTICATE 216.160.198.233 5061 authenticate.sip.clearip.com 5060 TCP
Peer = PHOENIXSOFT VALIDATE      216.160.198.233 5061 validate.sip.clearip.com 5060 TCP

```