

# **BCP – SRTP Configuration and Troubleshooting Guidelines for Oracle Enterprise SBC**

## **Revision History**

<i>Version</i>	<i>Author</i>	<i>Description of Changes</i>	<i>Date Revision Completed</i>
520-0043-00	Antonio Merenciano	Initial Release	Oct 21 <sup>st</sup> ,2010
520-0043-01	Anima Khindari	Added ETC NIU support information	July 27th, 2011
520-0043-02	Bhaskar Reddy Gaddam	Rebranded with latest release information	July 12th , 2018
520-0043-02	Priyesh Mehrotra	Rebranded with latest release information.IPsec configuraton removed.	July 16 <sup>th</sup> 2020

*Copyright © 2013, 2020, Oracle and/or its affiliates. All rights reserved..*

## **Status of this memo**

Oracle SBC Best Current Practices are working documents of the Professional Services department of Oracle Corporation. Note that other groups may also distribute working documents as Best Current Practices.

Best Current Practices are working documents valid until explicitly obsoleted, and may be updated, replaced or obsoleted by other documents at any time. It is recommended to use Best Current Practices as reference material as well as to cite them in other works in progress.

## **Abstract**

The use of the RFC 2119 keywords is an attempt to assign the correct requirement levels ("MUST", "SHOULD", "MAY", etc.).

This document defines a series of recommendations for Secure Real-time Transport Protocol (SRTP) configuration and troubleshooting on the Oracle SBC in a customer's production network. They should be used when either (a) deploying a new SBC, or (b) updating an existing configuration made before Best Current Practices were in place. When in conflict with Customer requirements or desires, the Customer's preference SHOULD take precedence.

## **Applicability**

This document is applicable to Oracle Enterprise Session Border Controller Release S-Cz8.4.0

## Table of Contents

<b>1</b>	<b>Introduction</b> .....	<b>3</b>
<b>2</b>	<b>Intended Audience</b> .....	<b>4</b>
<b>3</b>	<b>SRTP Topologies</b> .....	<b>5</b>
<b>4</b>	<b>Requirements</b> .....	<b>7</b>
4.1	HARDWARE REQUIREMENTS .....	7
4.2	SOFTWARE REQUIREMENTS .....	7
4.3	LICENSES REQUIREMENTS.....	7
4.4	BOOTLOADER REQUIREMENTS .....	8
<b>5</b>	<b>Design Aspects</b> .....	<b>9</b>
5.1	CONFIGURATION ELEMENTS .....	9
5.2	DESIGN CONSIDERATIONS.....	10
5.2.1	<i>Secured/Unsecured Network</i> .....	11
5.2.2	<i>Media traffic</i> .....	11
<b>6</b>	<b>Notes on the Reference Configurations</b> .....	<b>16</b>
6.1	SINGLE-ENDED SRTP TERMINATION ON SECURED NETWORKS .....	16
6.2	RTP AND SINGLE-ENDED SRTP TERMINATION ON UNSECURED NETWORKS.....	16
6.3	BACK-TO-BACK SRTP TERMINATION .....	17
<b>7</b>	<b>Troubleshooting</b> .....	<b>18</b>
7.1	DEBUGGING INFO.....	19
<b>8</b>	<b>References</b> .....	<b>27</b>
<b>9</b>	<b>Author’s Address</b> .....	<b>28</b>
<b>10</b>	<b>Disclaimer</b> .....	<b>29</b>
<b>11</b>	<b>Full Copyright Statement</b> .....	<b>30</b>
	<b>APPENDIX A. Reference Configuration: Single-Ended SRTP Termination on secured networks</b> .....	<b>31</b>
	<b>APPENDIX B. Reference Configuration: RTP and Single-Ended SRTP Termination on unsecured networks</b> .....	<b>43</b>
	<b>APPENDIX C. Reference Configuration: Back-to-Back SRTP Termination</b> .....	<b>55</b>

## 1 Introduction

The Secure Real-time Transport Protocol (**SRTP**) provides encryption and authentication for the call content and call signaling streams. Authentication provides assurance that packets are from the purported source, and that the packets have not been tampered with during transmission. Encryption provides assurance that the call content and associated signaling has remained private during transmission. SRTP/SDES is supported on the Oracle Session Border Controller.

RTP and RTCP traffic are encrypted as described in RFC 3711: The Secure Real-time Transport Protocol (SRTP). The negotiation and establishment of keys and other cryptographic materials that support SRTP is described in RFC 4568: Session Description Protocol (SDP) Security Description for Media Streams. Cryptographic parameters are established with only a single message or in single round-trip exchange using the offer/answer model defined in RFC 3264: An Offer/Answer Model with the Session Description Protocol.

This document should be used as a base reference only, outlining procedures to configure SRTP on the SBC node from its base configuration. An Oracle Systems Engineer should be consulted with regards to specific concerns as they apply to customer specific SBC configurations.

This document is based on features available in Oracle Enterprise Session Border Controller Release Notes, Release S-Cz8.4.0 software release, unless noted otherwise, and refers to other Oracle documentation for configuration detail.

Configuration guides are available for download from (<https://docs.oracle.com/>). Please contact your Oracle Systems Engineer for Best Current Practice (BCP) documentation.

**2 Intended Audience**

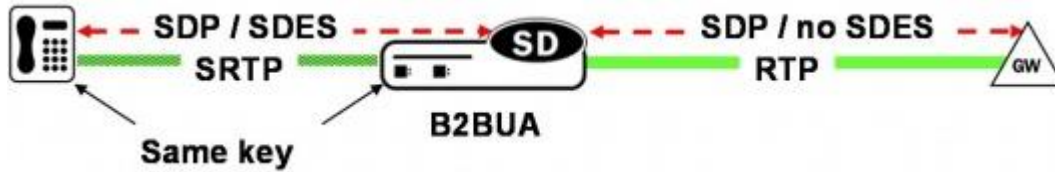
This document is intended for use by Oracle Systems Engineers, third party Systems Integrators, and end users of the Session Border Controller. It assumes that the reader is familiar with basic operations of the Session Border Controller, and has attended the following training course(s) (or has equivalent experience):

- [https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/8.4.0/releasenotes/esbc\\_scz840\\_releasenotes.pdf](https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/8.4.0/releasenotes/esbc_scz840_releasenotes.pdf)
- [https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/8.4.0/configuration/esbc\\_scz840\\_configuration.pdf](https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/8.4.0/configuration/esbc_scz840_configuration.pdf)
- [https://docs.oracle.com/en/industries/communications/session-border-controller/8.4.0/security/sbc\\_scz840\\_security.pdf](https://docs.oracle.com/en/industries/communications/session-border-controller/8.4.0/security/sbc_scz840_security.pdf)

3 SRTP Topologies

SRTP topologies can be categorised to three basic topologies:

- **Single Ended SRTP Termination**  
SRTP enabled on inbound interface, disabled on outbound interface (or vice versa)

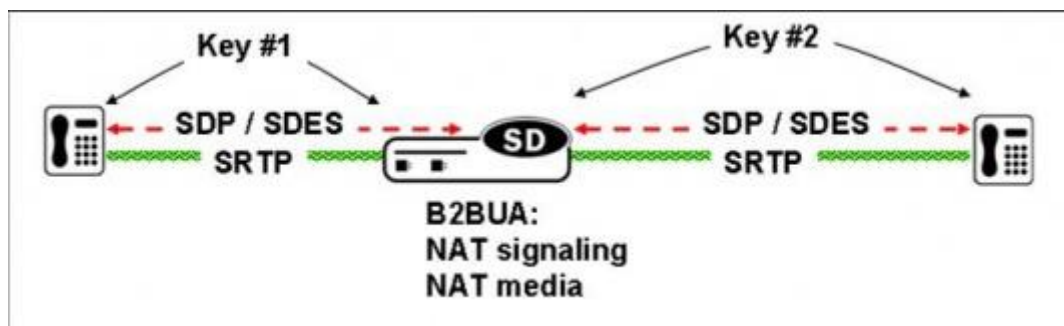


If SRTP is enabled for the inbound realm/interface, the SBC will handle the request according to the capabilities defined in the SRTP configuration. If there is a crypto attribute in the offer, the SBC will attempt to parse the crypto attributes and parameters in the SDP. It accepts exactly one of the offered crypto attributes for a given media stream, if this is configured as a valid crypto-suite on the SBC. If there is no crypto-suite configured on the SBC in the list of crypto-suites received, the SBC will reject the call with a “488 Not Acceptable Here” response.

Before the request is forwarded to the callee, the SBC allocates resources, updates the SDP with proper media addresses and ports, and the original crypto attribute is removed from the SDP.

Once the reply from the callee is received, SBC inserts the appropriate crypto attribute to form a new SDP, and forwards the response back to the caller. At this point, SRTP traffic is allowed between the caller and the SBC.

- **Back-to-back SRTP Termination**  
SRTP enabled on inbound interface, enabled on outbound interface. Separate crypto keys on either side..



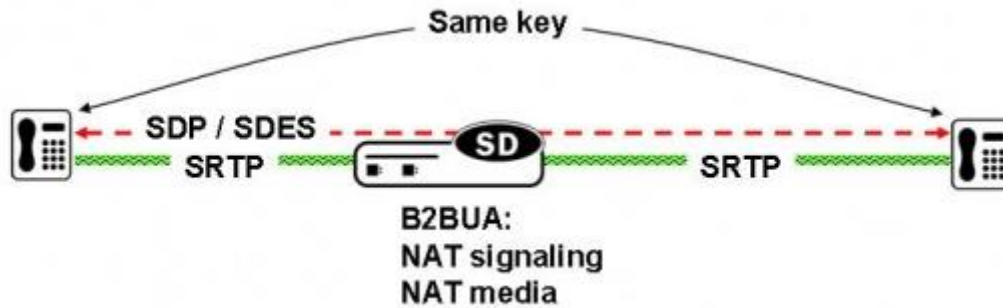
Similarly to the “Single End SRTP Termination” case above, before the request is forwarded to the callee, the SBC allocates resources and updates the SDP with proper media addresses and ports, however, at this point, the original crypto attribute is replaced with one generated by the SBC.

The construction of the crypto attribute in the SDP will be based on the configuration for the outbound realm/interface. Once the reply from the callee is received, the SBC could also accept or reject the “answer”

from the callee according to the configuration and the list of crypto-suites supported. If accepted, the SBC will replace the original crypto attribute from the callee with its own to form a new SDP. The new SDP is forwarded back to the caller. At this point, SRTP media sessions are established on both sides.

- **Pass-through SRTP**

Crypto attribute is not intercepted, just forwarded, and the key negotiation is done end-to-end.



If the configuration specifies “pass-through” mode, the SBC will not intercept the crypto attribute exchange between the caller and the callee. The crypto attribute will be forwarded as it is from the caller to the callee and vice versa. The SBC simply modifies media IP addresses and ports to enable media anchoring (if configured), hence SRTP flows pass transparently through the SBC

## 4 Requirements

### 4.1 Hardware Requirements

On Oracle 4600/6100/6300/6350 platforms standard network interfaces (NIU) is required which allows the use of the encryption needed for SRTP. The Oracle 1100 and 3900 and VME SBCs use the software datapath (DPDK) and support software-based SRTP.

```
Contents of PHY0 IDPROM
  Assy, 2 Port 10GigE SFP and 4 Port GigE SFP
  Oracle Part Number:      7089186
  Oracle Rev:              07
  Oracle FRU Part Number:  0000000
  Acme Packet Part Number: 002-0813-58-02
  Serial Number:          181536000256
  Acme Packet FunctionalRev: 1.02
  BoardRev:               02.00
  PCB Family Type:        Dual Port 10GigE and 4 Port 1GigE PHY
  ID:                     2 Port 10GigE SFP w/Encryption, ETC, TRANS & MGT and 4 Port GigE SFP
  Options:                0
  Manufacturer:           MITAC China - MSL
  Week/Year:              36/2015
  Sequence Number:        000256
```

SSM module is NOT a requirement for SRTP, although typically SRTP is deployed in conjunction with TLS for SIP. Therefore, TLS is used for encrypting signaling and SRTP is used for encrypting media. In this case, then the SSM module is also required to run TLS.

```
# show security ssm
SSM (Security Service Module) V2 present.
```

If UDP/TCP is used for SIP, then SSM module is not a requirement.

### 4.2 Software Requirements

S-CX6.2.0 software image or higher is required to support SRTP termination on the SBC. It is always recommended to use the latest image available on the Oracle customer support portal ([https:// support.us.oracle.com/](https://support.us.oracle.com/)).

### 4.3 Licenses Requirements

No additional licenses are required for the Oracle 6300/6350/6100/3900/4600/1100 to use SRTP. Oracle VME requires License for Software TLS and Software SRTP.

You can request license keys via the License Codes website at –

<http://www.oracle.com/us/support/licensecodes/acme-packet/index.html>

## 4.4 Bootloader requirements

Boot loader software loads the application to run on a platform. As such, boot loader software must be correct before system startup. Oracle Communications Session Delivery product distributions include and install the correct boot loader during application installation, meaning you need not consider boot loader version during first installation procedures.

Application software upgrades do not update boot loaders. For this reason, you need to verify this compatibility manually. The following topics provide information about identifying the need and performing the updates.

### Stage3 Boot Loader

Every new software release includes a system software image and a Stage3 boot loader. Oracle recommends you update this boot loader with every software upgrade, as described in the Software Upgrade section. Be sure to perform this update before booting the new system image.

The Stage3 boot loader is generally backward compatible with previous releases, but Oracle recommends that the Stage3 boot loader be installed from the same Major/Minor version as the system image. It is not normally necessary to update the boot loader when installing a maintenance or patch release when the Major.Minor release is the same. For example, the same nnCZ830.boot can be used with nnECZ820, nnECZ810m1, and so forth system software. But it should be upgraded when installing nnCZ830 system software to match that Major.Minor release.

The boot loader file name corresponds to the software image filename. For example, if the software image filename is nnCZ830.64.bz, the corresponding Stage3 boot loader filename is nnCZ830.boot.

The Stage3 boot loader is compatible with previous releases.

Stage 3 boot loader upgrade procedure can be found in the Update the Stage 3 Bootloader section of this guide.

Note:

The SBC does not support uploading the boot loader by way of the Web GUI.



## 5 Design Aspects

Due to the flexibility in the configuration for different SRTP modes, it is needed to consider different aspects of the desired design for proper configuration. Here is a brief explanation on the elements needed for SRTP configuration. This is just a basic reference, the configuration of each element will depend on the desired design and will be described in the following sections.

### 5.1 Configuration Elements

Here is a brief explanation on the elements needed for SRTP configuration. This is just a basic reference, the configuration of each element will depend on the desired design and will be described in the following sections.

- Security → media-security → **sdes-profile**

- 

This is the first element to configure, where the algorithm and the cryptos to be used are configured.

For sdes-profile, it is required to define the crypto-suites accepted, and also whether or not authentication and/or encryption are used for SRTP and if encryption is used for SRTCP. The “use-ingress-session-params” attribute is used to override previous parameters, specifying that the SBC will accept encryption/no-encryption, authentication/no-authentication in SRTP/SRTCP, using in the egress SDP the same session parameter that was received in the ingress SDP.

Finally “egress-offer-format” is used to instruct the SBC on how to build the egress SDP in the case of both RTP and SRTP are supported at the same time. This is further explained in the next section.

```
# show running-config sdes-profile
sdes-profile
  name sdes1
  crypto-list AES_CM_128_HMAC_SHA1_80
AES_CM_128_HMAC_SHA1_32
  srtp-auth enabled
  srtp-encrypt enabled
  srtcp-encrypt enabled
  egress-offer-format same-as-ingress
  use-ingress-session-params srtcp-encrypt
  srtp-auth
  srtp-encrypt
  mki disabled
  key
  salt
```

- Security → media-security → **media-sec-policy**

Media-sec-policy instructs the SBC how to handle the SDP received/sent under a realm (RTP, SRTP or any of them) and, if SRTP needs to be used, the sdes-profile that needs to be used.

The media-sec-policy should be assigned to a realm under the realm-config configuration.

```
(media-sec-policy)# show
media-sec-policy
  name                msp1
  pass-through        disabled
  inbound
    profile            sdes1
    mode               srtp
    protocol           sdes
  outbound
    profile            sdes1
    mode               srtp
    protocol           sdes
(media-sec-policy)#
```

## 5.2 Design Considerations

The intents of the design considerations explained here are to:

- Minimize interoperability issues by standardizing field configurations
- Provide guidelines for new users to the Session Border Controller
- Document when and why configuration elements should be changed from their default values
- Facilitate transition of customers from Systems Engineering to Technical Support by making configurations consistent (yielding predictable behavior)

Further, each design considers the following aspects:

- Flexibility: how resilient the configuration is, and how adaptable the configuration is (i.e. when turning up new connected networks)
- Scalability: minimizing redundant configuration objects and setting a templated foundation to allow overlay configuration with minimal disruption
- Compatibility: working with other popular devices in carriers' VoIP networks

The main aspects treated here focused on which traffic is desired under a realm, so each design needs to consider the following, previous to any configuration:

1. SIP Traffic: SIP over UDP/TCP (unsecured transport) or over TLS (secured transport protocol).
2. Media Traffic: media over RTP, media over SRTP or media over both RTP and SRTP allowed at the same time. This would differentiate the IP design, since:
  - a. For media over RTP only or SRTP only, just one IP address will be used for them
  - b. For media over both RTP/SRTP allowed at the same time, then the recommendation is to use two different IPs on the same network-interface. One will send RTP traffic and the other IP will be used for SRTP traffic. This should be considered for correct IP plan under the network.

### 5.2.1 Secured/Unsecured Network

By default, the SBC considers that SIP traffic, when SRTP is configured, should run over secured transport protocol, TLS. If this is not the case, the SBC needs to be instructed to allow SIP traffic over non-secured transport protocol (UDP/TCP).

```
sip-interface
  state                enabled
  realm-id             access1
  description
  sip-port
    address            11.0.0.11
    port               5060
    transport-protocol UDP
    tls-profile
    allow-anonymous   all
    ims-aka-profile
  carriers
...
  secured-network     enabled
```

When `secured-network` is set to `DISABLED` under a `sip-interface` where SRTP is configured, the `sip-interface` will only allow SIP over TLS. If SIP is received over UDP/TCP, the SBC will reject the call with “488 Not Acceptable Here”.

When `secured-network` is set to `ENABLED`, the SBC understands the network is secured and it accepts SIP traffic on UDP/TCP.

### 5.2.2 Media traffic

Every realm under the configuration should be instructed to the type of media that should handle whether that be RTP only, SRTP only or both RTP and SRTP. For each realm, it can be differentiated between the inbound and outbound media type, giving the flexibility of having different protocols for inbound or for outbound.

The “mode” parameter under the `media-sec-policy` controls the media protocol defined for each inbound/outbound flow under a realm.

#### 5.2.2.1 RTP Only

The “mode” parameter under the inbound/outbound section of the `media-sec-policy` should be set to `RTP`. In this case, no profile should be defined, and the protocol should be set to “None”.

```
(media-sec-policy)# show
media-sec-policy
  name          removeCrypto
  pass-through  disabled
  inbound
    profile
    mode          rtp
    protocol      none
  outbound
    profile
    mode          rtp
    protocol      none
(media-sec-policy)#
```

This is mostly used in single ended SRTP termination configurations, where this media-sec-policy removes the SRTP component part from the SDP to offer/accept only SRTP. This media-sec-policy should be applied under the realm where only RTP is desired.

```
realm-config
  identifier      backbone
  description
  addr-prefix    0.0.0.0
  network-interfaces
                  M10:0
...
  media-sec-policy removeCrypto
...
```

In the case of RTP only, no sdes-profile is needed.

#### 5.2.2.2 SRTP Only

The “mode” parameter under the media-sec-policy should be set to SRTP. The “profile” parameter should be set to the configured sdes-profile, and the protocol should be set to SDES.

In this case, only SRTP is accepted in the realm. An INVITE arriving to the realm without SRTP capabilities is rejected by the SBC with a “488 Not Acceptable Here”.

```
(media-sec-policy)# show
media-sec-policy
  name                               SRTP1
  pass-through                        disabled
  inbound
    profile                           sdes1
    mode                               srtp
    protocol                           SDES
  outbound
    profile                           sdes1
    mode                               srtp
    protocol                           SDES
(media-sec-policy)#
```

Where “sdes1” is the configured sdes-profile used for this implementation. Here are the default sdes-profile is suggested, to be superseded only by specific customer requirements.

```
# show running-config sdes-profile
sdes-profile
  name                               sdes1
  crypto-list                         AES_CM_128_HMAC_SHA1_80
AES_CM_128_HMAC_SHA1_32
  srtp-auth                           enabled
  srtp-encrypt                         enabled
  srtcp-encrypt                       enabled
  egress-offer-format                 same-as-ingress
  use-ingress-session-params         srtcp-encrypt
                                      srtp-auth
                                      srtp-encrypt
  mki                                  disabled
  key
  salt
```

The media-sec-profile configured for SRTP should be applied under the desired realm.

```
realm-config
  identifier                           access1
  description
  addr-prefix                           0.0.0.0
  network-interfaces                    M00:0
...
  media-sec-policy                       SRTP1
...
```

### 5.2.2.3 Both RTP/SRTP support

The “mode” under the media-sec-policy should be set to ANY. Also, the profile should be configured with the sdes-profile that would be used in case of SRTP and the protocol should be set to SDES.

When inbound mode=any, the SBC will accept SDP with only RTP description, SDP with only SRTP description and SDP with 2 m lines having both RTP and SRTP description.

When outbound mode=any, the SBC will insert an SDP with only RTP, only SRTP or with 2 m lines, supporting both RTP and SRTP, this is controlled under the sdes-profile:

```
(sdes-profile)# egress-offer-format
```

```
<enumeration> format of offer SDP in 'any' mode  
    {same-as-ingress | simultaneous-best-effort}
```

- Same-as-ingress: The SBC will use to build the egress SDP offer the mode received in the ingress realm. So if the SBC received only RTP in the ingress realm, it will insert only RTP in the egress SDP, and if it received only SRTP in the ingress SDP, it will set the egress SDP to only SRTP.
- Simultaneous-best-effort: The SBC will insert additional SRTP description in the SDP if the ingress SDP contained only RTP and vice-versa, so the resultant SDP should contain both RTP and SRTP media profiles contained in 2 different media lines in the SDP.

```
# show running-config sdes-profile  
sdes-profile  
  name                sdes1  
  crypto-list         AES_CM_128_HMAC_SHA1_80  
AES_CM_128_HMAC_SHA1_32  
  srtp-auth           enabled  
  srtp-encrypt        enabled  
  srtp-encrypt        enabled  
  egress-offer-format same-as-ingress  
  use-ingress-session-params srtp-encrypt  
  key                 srtp-auth  
  salt                srtp-encrypt  
  mki                 disabled
```

```
(media-sec-policy)# show
media-sec-policy
  name                               SRTP1
  pass-through                        disabled
  inbound
    profile                           sdes1
    mode                               any
    protocol                           SDES
  outbound
    profile                           sdes1
    mode                               any
    protocol                           SDES
(media-sec-policy)#
```

And this media-sec-policy should be applied under the realm where RTP+SRTP are desired:

```
realm-config
  identifier                           access1
  description
  addr-prefix                           0.0.0.0
  network-interfaces
                                         M00:0
...
  media-sec-policy                       SRTP1
...
```

## 6 Notes on the Reference Configurations

The intention of this document is not to provide a full set of configurations, as the flexibility of the SRTP configuration makes valid a high number of different possible configurations. The objective is to present some common and valid configurations that have been tested and verified in Oracle labs.

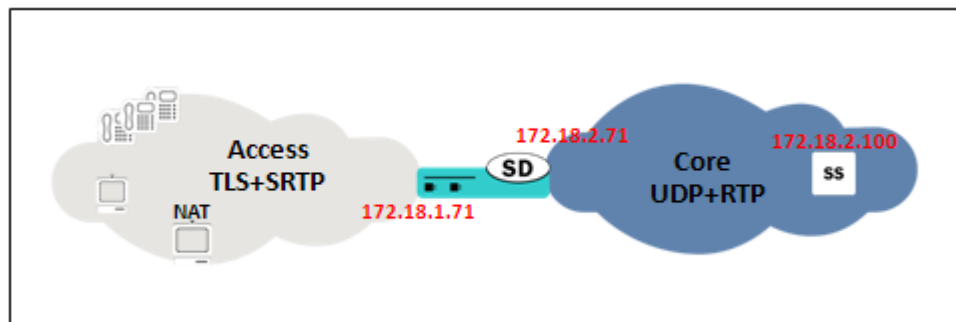
In the cases considered here, there is a considered “access” or “peer1A” network, in the 172.18.1.0/24 network, and a considered “core” or “peer1B” in the 172.18.2.0/24 network. In all cases SIP and media traffic runs on the same subnets.

To simplify the use of this BCP, no other elements are configured in this case, so no redundancy or DDoS prevention are configured in the configurations exposed. The configurations follow the guides of BCP for access (using policy based realm bridging) and peering scenarios. For TLS, it is assumed single-side authentication in all cases.

The configurations presented use SDES mechanism for SRTP encryption. No SRTP pass-through cases are presented here, as there is nothing required for the SBC to be transparent to the SRTP negotiation end-to-end.

### 6.1 Single-Ended SRTP Termination on secured networks.

This is the typical access scenario where SRTP is deployed completely in the access network, allowing the users to use TLS for SIP and SRTP for media. In the core network, UDP is used for SIP and RTP is used for media.



The IP used for SIP and SRTP in the SBC in the access network is 172.18.1.71, and the IP used for SIP and RTP in the core network is 172.18.2.71. The SIP Registrar/Proxy in the core network is in 172.18.2.100.

In this case, secured-network is set to DISABLED under the access sip-interface and ENABLED on the core sip-interface. Two media-sec-policies are created, one in the access network with mode=SRTP and one in the core with mode=RTP.

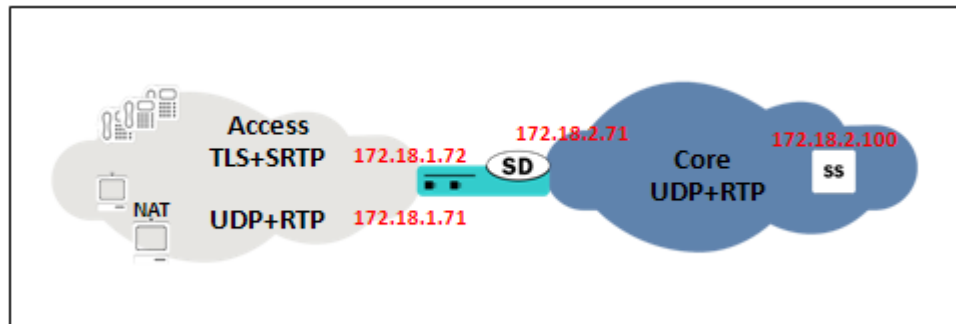
The sample configuration can be found in Appendix A

### 6.2 RTP and Single-Ended SRTP Termination on unsecured networks.

This is a very common architecture, where both RTP and SRTP endpoints reside in the access network, especially while in transition from RTP to SRTP. This means that both UDP/RTP and TLS/SRTP can be present in the access network. In the core network, UDP for SIP and RTP for media will be used.



In this case, in the access network we will use 172.18.1.71 for SIP traffic (UDP and TLS) and also for RTP traffic. 172.18.1.72 will be used for SRTP traffic. In the core network, 172.18.2.71 will be used for SIP and RTP. The SIP Proxy/Registrar uses 172.18.2.100.

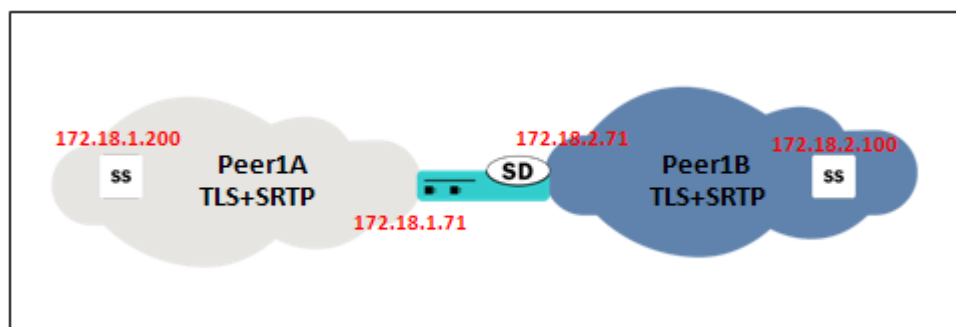


Secured-network parameter is set to ENABLED under the access sip-interface and ENABLED on the core sip-interface. Two media-sec-policies are created, one in the access network with mode=any and one in the core with mode=RTP. As in the access network both RTP and SRTP endpoints could be present, the egress-offer-format is set to simultaneous-best-effort.

The sample configuration can be found in Appendix B

### 6.3 Back-to-back SRTP Termination

Normally deployed in peering scenarios where SRTP is needed in both networks that the SBC is interconnecting. In that case, the Session Border Controller is doing SRTP termination so the SRTP key exchange is different in the two connected networks.



In the SBC, 172.18.1.71 will be used for SIP (TLS) and SRTP in the peer1A network, while 172.18.2.71 will be used in the 172.18.2.71.

The peer element sending traffic in the peer1A network will be in 172.18.1.200, while the peer element in the peer1B will be 172.18.2.100.

Secured-network is set to DISABLED under both sip-interfaces. Two media-sec-policies are created, one in the peer1A network with mode=SRTP and one in the peer1B with mode=SRTP, where each one is linked with a different SDES profile, to allow different cryptos between networks. Note that this is not required, and the same SDES profile could be used for both networks, the key exchange would keep different as the SBC would terminate the SRTP anyway, so configuring different SDES profiles would be only needed in the case where the crypto-suites supported in each network are different or have different characteristics.

## 7 Troubleshooting

A network capture taken on both access and core network should show RTP packets with the same sequence number, however, if SRTP termination is done in the SBC, the payload contained in RTP packets with the same sequence number will be different because of the encryption/unencryption done by the SBC.

To troubleshoot SRTP on the Session Border Controller, following commands can be used:

- “Show security srtp” commands show the security association created for SRTP encryption and its detailed information.
  - show security srtp <network\_interface> debug/brief/detail/raw
    - Note there is a warning when these commands want to be run, as it should be done carefully in production systems:  
WARNING: This action might affect system performance and take a long time to finish.  
Are you sure [y/n]?:
  - Show security srtp status <network\_interface>
  - Show security spd <network\_interface>

### # show security srtp sad M00 debug

WARNING: This action might affect system performance and take a long time to finish.

Are you sure [y/n]?: y

SRTP security-association-database for interface 'M00':

Displaying SA's that match the following criteria -

```

direction          : both
src-addr-prefix    : any
src-port           : any
dst-addr-prefix    : any
dst-port           : any
trans-proto        : ALL
Inbound:
destination-address : 62.2.139.213
destination-port    : 10012
vlan-id            : 0
sal-index           : 2
sad-index           : 10
ssrc                : 1514612894
encr-algo           : aes-128-ctr
auth-algo           : hmac-sha1
auth-tag-length     : 80
flags -
ms: 5489040, ls:    8
mtu                  : 1500
mki                  : 0
mki length           : 0
lifetime byte count -
ms: 0x 0, ls: 0x 0
packet count -
ms: 0x 0, ls: 0x 12F
roll over count      : 0
anti replay highest seq num : 11814
highest seq num      : 0
auth error count     : 0
anti replay count     : 0
mki mismatch count   : 0

```

```
ssrc mismatch count      : 1
```

```
# show security srtp sad M00 raw
```

```
WARNING: This action might affect system performance and take a long time to finish.
```

```
Are you sure [y/n]?: y
```

```
SRTP security-association-database for interface 'M00':
```

```
Displaying SA's that match the following criteria -
```

```
direction      : both
src-addr-prefix : any
src-port       : any
dst-addr-prefix : any
dst-port       : any
trans-proto    : ALL
```

```
Inbound:
```

```
Index I          VLN P <-- Masks --> SAD Next
TP Dest. IP Address SPI Pr ID TS P V Pr VLN TS P V Index Link
0000a 0 01 00000000 00000000 00000000 11 000 00 0 0 ff 000 00 0 0 0000a 00000
00000000 d58b023e
Index Flags MS Flags LS EX Flg MTU SSRC MKI MKI Len ROC
0000a 05489040 00000008 00202a 05dc 5a47289e 00000000 00000000 00000000
Master key: f6 8e c5 af 6c af 96 72 64 78 04 97 14 44 c1 a9
Master salt: 59 da 31 4d c2 3d 15 ca b6 3b 39 e1 27 2d
E-IV: 59 da 31 4d 98 7a 3d 54 b6 3b 39 e1 27 2d 00 00
HMAC ipad: 7a cc 93 f9 72 44 2d df ee df cc 89 3d a2 35 74 18 32 bb 25
HMAC opad: 2b 6d cc 43 49 fa 65 8e 4a d2 03 50 90 00 9f 10 16 6d 1a 90
Sequence Number Anti-replay window (128 bits wide)
00002f68 ffffffff ffffffff ffffffff ffffffff
Life Byte Count Packet Count Auth Err Anti-replay Err
0000000000000000 0000000000000271 00000000 00000000
ICV Len HSN MKI Mismatch SSRC Mismatch
04 00000000 00000000 00000001
```

## 7.1 Debugging Info

Following is the list of commands to be used in order to get SRTP and ETC specific information.

### 1. show nat flow-info srtp statistics

This command will show the global statistics for all SRTP flows.

```
# show nat flow-info srtp statistics
```

```
PPM_ID_SRTP_E:
PPX Global Statistics
```

```
-----
alloc_count      : 50
dealloc_count    : 16
input-packets    : 0
output-packets   : 0
sessions-count   : 2
init-requests    : 4
init-success     : 4
init-fail        : 0
modify-requests  : 0
modify-success   : 0
modify-fail      : 0
delete-requests  : 2
```

```

delete-success      : 2
delete-fail        : 0
query-requests     : 0
query-success      : 0
query-fail         : 0
resources-error    : 0
protect-fail       : 0
unprotect-fail     : 0
status-err         : 0
bad-param          : 0
alloc-fail         : 0
dealloc-fail       : 0
terminus           : 0
auth-fail          : 0
cipher-fail        : 0
replay-fail        : 0
replay-old         : 0
algo-fail          : 0
no-such-op         : 0
no-ctx             : 0
cant-check         : 0
key-expired        : 0
nonce-bad          : 0
read-failed        : 0
write-failed       : 0
parse-err          : 0
encode-err         : 0
pfkey-err          : 0
mki-changed        : 0
srtp-pkt-too-small : 0
srtp-pkt-too-small : 0

```

PPM\_ID\_SRTP\_D:  
PPX Global Statistics

```

-----
alloc_count        : 50
dealloc_count      : 16
input-packets      : 0
output-packets     : 0
sessions-count     : 3
init-requests      : 2
init-success       : 2
init-fail          : 0
modify-requests    : 1
modify-success     : 1
modify-fail        : 0
delete-requests    : 0
delete-success     : 0
delete-fail        : 0
query-requests     : 0
query-success      : 0
query-fail         : 0
resources-error    : 0
protect-fail       : 0
unprotect-fail     : 0
status-err         : 0
bad-param          : 0
alloc-fail         : 0
dealloc-fail       : 0
terminus           : 0
auth-fail          : 0
cipher-fail        : 0

```

```

replay-fail      : 0
replay-old       : 0
algo-fail        : 0
no-such-op       : 0
no-ctx           : 0
cant-check       : 0
key-expired      : 0
nonce-bad        : 0
read-failed      : 0
write-failed     : 0
parse-err        : 0
encode-err       : 0
pfkey-err        : 0
mki-changed     : 0
srtp-pkt-too-small : 0
srtp-pkt-too-small : 0

```

## 2. **show nat flow-info srtp by-addr 3.0.0.2 all**

This command will show the crypto information details for a flow with the given source address. If “all” is used, the details for all the SRTP flows will be displayed. However, “all” does not display the statistics from the octeon srtp code.

### # **show nat flow-info srtp by-addr 3.0.0.2 all**

Crypto Parameters 3.0.0.2:7001 -> 7.0.0.2:6058

```

=====
Collapsed        : false
SRTCP Only       : false
Crypto In
-----
destination-address : 208.54.47.80
destination-port   : 40000
vlan-id             : 632
encr-algo           : aes-128-ctr
auth-algo           : hmac-sha1
auth-tag-length  : 32
  key index      : 0
  mki            : none
  roll-over-count : 0

```

---No Crypto Out---

PPM\_ID\_SRTP\_D

PPX Statistics

-----

Stream #1

```

ssrc          : 3879260980
rtp-cipher-id : AES-128-ICM
rtp-auth-id   : HMAC-SHA1
rtp-security-level : Crypto + Auth
rtp-total-packets : 5423
rtp-total-bytes : 954448
rtp-cipher-bytes : 867680
rtp-auth-bytes : 932756
rtcp-cipher-id : AES-128-ICM
rtcp-auth-id   : HMAC-SHA1
rtcp-security-level : Crypto + Auth
rtcp-total-packets : 0
rtcp-total-bytes : 0
rtcp-cipher-bytes : 0

```

```

rtcp-auth-bytes      : 0
key-lifetime         : 42949672954294961871
direction            : Receiver

```

#### Crypto Parameters 3.0.0.2:7001 -> 7.0.0.2:6058

```

Collapsed           : false
SRTCP Only         : true
Crypto In

```

```

destination-address : 208.54.47.80
destination-port    : 40000
vlan-id             : 632
encr-algo           : aes-128-ctr
auth-algo           : hmac-sha1
auth-tag-length     : 32
key index           : 0
mki                 : none
roll-over-count     : 0

```

---No Crypto Out---

PPM\_ID\_SRTP\_D  
PPX Statistics

Stream #1

```

ssrc                : 0
rtp-cipher-id       : NULL
rtp-auth-id         : NULL
rtp-security-level  : None
rtp-total-packets   : 0
rtp-total-bytes     : 0
rtp-cipher-bytes    : 0
rtp-auth-bytes      : 0
rtcp-cipher-id      : NULL
rtcp-auth-id        : NULL
rtcp-security-level : None
rtcp-total-packets  : 0
rtcp-total-bytes    : 0
rtcp-cipher-bytes   : 0
rtcp-auth-bytes     : 0
key-lifetime        : 0
direction           : Unknown

```

### 3. show nat flow-info all

This command will show the crypto information for the SRTP flows. This command should not be executed in a production environment, since it dumps information of all the flows.

```
# show nat flow-info all
```

**Output curtailed due to size.**

..... continued

```

-----
SA_flow_key   : 7.0.0.2          SA_prefix : 32
DA_flow_key   : 10.176.28.218   DA_prefix : 32
SP_flow_key   : 6058            SP_prefix : 16
DP_flow_key   : 40000           DP_prefix : 16
VLAN_flow_key : 980
Protocol_flow_key : 17
Ingress_flow_key : 1

```

```

Ingress Slot   : 1
Ingress Port   : 0
NAT IP Flow Type : IPv4 to IPv4
XSA_data_entry : 208.54.47.80
XDA_data_entry : 3.0.0.2
XSP_data_entry : 40000
XDP_data_entry : 7001
Egress_data_entry : 0
Egress Slot    : 0
Egress Port    : 0
flow_action    : 0X1
optional_data  : 0
FPGA_handle    : 0x000000c1
assoc_FPGA_handle : 0x00000000
VLAN_data_entry : 632
host_table_index : 6
Switch ID     : 0x00000005
average-rate   : 0
weight        : 0x0
init_flow_guard : 300
inact_flow_guard : 300
max_flow_guard : 86400
payload_type_2833 : 0
index_2833     : 0
pt_2833_egress : 0
qos_vq_enabled : 0
codec_type     : 0
HMU_handle     : 0
SRTP Crypto In  : NONE
SRTP Crypto Out : AES_CM_128_HMAC_SHA1_32

```

-----

Input Link Parameters - IFD Index: 0x5

-----

```

IFD Byte Enable: false
EPD Mode Enable: true
Retain: false
ABJ Mode: true
Disable Empty: false
Ignore On Empty: false
TGID: 0x6
WRGID: 0x0
TG Enable: true
WRG Enable: false

```

Output Link Parameters - OFD Index: 0x5

-----

```

shaped_flow: false
latency_sensitive: false
pkt_mode: Packet Mode
zero_min_credit_flow: false
parent_pipe_num: 0x1
delta: 0x1
flow_credit_min_exp: 0x0
flow_credit_min_man: 0x0

```

IFD 0x00000005: dropCount = 0x00000000

IFD 0x00000005: acceptCount = 0x00001f35

-----

**4. show mbc errors**

This command will show counters for SRTP errors, including SRTP Flow Add Failed, SRTP Flow Delete Failed, and SRTP Flow Update Failed.

```
# show mbc errors
22:29:33-160
MBC Errors/Events      ---- Lifetime ----
      Recent   Total PerMax
Client Errors          0     0     0
Client IPC Errors      0     0     0
Open Streams Failed    0     0     0
Drop Streams Failed    0     0     0
Exp Flow Events        1     1     1
Exp Flow Not Found     0     0     0
Transaction Timeouts   0     0     0

Server Errors          0     0     0
Server IPC Errors      0     0     0
Flow Add Failed         0     2     2
Flow Delete Failed     0     0     0
Flow Update Failed     0     0     0
Flow Latch Failed      0     0     0
Pending Flow Expired   0     0     0
ARP Wait Errors        0     0     0
Exp CAM Not Found      0     0     0
Drop Unknown Exp Flow  0     0     0
Drop/Exp Flow Missing  0     0     0
Exp Notify Failed      0     0     0
Unacknowledged Notify  0     0     0
Invalid Realm          0     0     0
No Ports Available     0     0     0
Insufficient Bandwidth 0     0     0
Stale Ports Reclaimed  0     0     0
Stale Flows Replaced   0     0     0
Telephone Events Gen   0     0     0
Pipe Alloc Errors      0     0     0
Pipe Write Errors      0     0     0
Not Found In Flows     0     0     0
SRTP Flow Add Failed    0     0     0
SRTP Flow Delete Faile 0     0     0
SRTP Flow Update Faile 0     0     0
SRTP Capacity Exceeded 0     0     0
```

**5. show mbc statistics**

This command will show counters for number of active SRTP/SRTCP flows, as well as the number of SRTP Sessions maintained.

```
# show mbc statistics
22:29:40-168
MBCD Status      -- Period -- ----- Lifetime -----
      Active High Total   Total PerMax High
Client Sessions  1   1   1     1   1   1
Client Trans     0   1   3     3   3   1
Contexts         3   3   2     3   2   3
Flows            14  14   3    14  11  14
Flow-Port        2   2   2     2   2   2
Flow-NAT         13  13   5    16  11  13
Flow-RTCP        2   2   4     4   4   2
Flow-Hairpin     0   0   0     0   0   0
Flow-Released    0   0   0     0   0   0
MSM-Release      0   0   0     0   0   0
```



Rel-Port	0	0	0	0	0	0
Rel-Hairpin	0	0	0	0	0	0
NAT Entries	15	15	9	20	11	15
Free Ports	80000	80004	0	80004	80004	80004
Used Ports	4	4	4	4	4	4
Port Sorts	-	-	0	0	0	
Queued Notify	0	0	0	0	0	0
MBC Trans	0	3	3	3	3	3
MBC Ignored	-	-	0	0	0	
ARP Trans	0	0	0	0	0	0
Relatch NAT	0	0	0	0	0	0
Relatch RTCP	0	0	0	0	0	0
<b>SRTP Only Flows</b>	<b>1</b>	<b>1</b>	<b>3</b>	<b>3</b>	<b>3</b>	<b>1</b>
<b>SRTCP Only Flow</b>	<b>3</b>	<b>3</b>	<b>3</b>	<b>3</b>	<b>3</b>	<b>3</b>
<b>SRTP Collapsed</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>
<b>SRTP Sessions</b>	<b>1</b>	<b>1</b>	<b>3</b>	<b>3</b>	<b>3</b>	<b>1</b>

Flow Rate = 0.0

Load Rate = 0.0

**6. show mbc all**

This command will show counters for number of active SRTP/SRTCP flows, as well as the number of SRTP Sessions maintained.

**7. show sipd errors**

This command will show the counter for number of SIP sessions that failed to setup due to problems related to SRTP signaling.

```
# show sipd errors
22:29:50-178
SIP Errors/Events      ---- Lifetime ----
      Recent      Total PerMax
SDP Offer Errors      0      0      0
SDP Answer Errors     0      0      0
Drop Media Errors     0      0      0
Transaction Errors    0      0      0
Application Errors    0      0      0
Media Exp Events      0      0      0
Early Media Exps     0      0      0
Exp Media Drops       0      0      0
Expired Sessions      0      0      0
Multiple OK Drops     0      0      0
Multiple OK Terms     0      0      0
Media Failure Drops   0      0      0
Non-ACK 2xx Drops    0      0      0
Invalid Requests      0      0      0
Invalid Responses     0      0      0
Invalid Messages      0      0      0
CAC Session Drop      0      0      0
Nsep User Exceeded    0      0      0
Nsep SA Exceeded      0      0      0
CAC BW Drop           0      0      0
SRTP Errors         0    0    0
```

**8. show security srtp sessions**

This command will show the active srtp/srtcp sessions and the total allowed capacity of 10,000 sessions.

```
# show security srtp sessions
Capacity=10000
SRTP Sessions  -- Period -- ---- Lifetime ----
Active  High Total Recent  Total PerMax
  1    1    3    3    3    1
```

## 9. **dump-etc-help**

This command lists all the ETC related dump commands available on the system.

### # **dump-etc-help**

ETC Utility Help

```
dump-etc-crash           - Dumps Octeon crash logs
dump-etc-wqe-err        - Dumps Octeon WQE error logs
dump-etc-mem-stats      - Dumps Octeon memory stats
dump-etc-port-stats <file> OR <reset> - Dumps Octeon port statistics
dump-etc-cmd-stats <file> OR <reset> - Dumps Octeon command statistics
dump-etc-core-stats <file> OR <reset> - Dumps Octeon core statistics
dump-etc-host-stats <file> OR <reset> - Dumps Octeon host statistics
dump-etc-debug-stats <file> OR <reset> - Dumps Octeon debug statistics
dump-etc-ppm-stats <file> - Dumps Octeon ppm statistics
dump-etc-core-regs <file> - Dumps Octeon core registers
dump-etc-fpga <file> - Dumps Bender PHY FPGA statistics
dump-etc-stats          - Dumps all of the Octeon stats
dump-etc-all          - Dumps all of the above to file only
```

NOTE: If the file switch is chosen the utility will output to a file under /code  
The file name will be of the form 'command name.xz'. For example, a file  
dump-etc-cmd-stats.xz would be created if the command 'dump-etc-cmd-stats file' were  
to be entered.task done

## 10. **dump-etc-all**

This command dumps all of the octeon statistics to a file /ramdrv/dump-etc-all

## 11. **show support-info**

This command contains the following useful ETC related commands:

- show media host-stats
- show media host-stats
- show media classify
- dump-etc-stats
- ipt show all
- show ip connection
- show mbcid all

**8 References**

- [1] Oracle Enterprise Session Border Controller ACLI Configuration Guide, Release S-Cz8.4.0 , June 2020
- [2] Oracle Enterprise Session Border Controller Release Notes, Release S-Cz8.4.0 , June 2020..
- [3] "RFC 3711, The Secure Real-time Transport Protocol (SRTP)"
- [4] "RFC 4568, Session Description Protocol (SDP, Security Descriptions for Media Streams"
- [5] "RFC 3264, An Offer/Answer Model with the Session Description Protocol (SDP)"

**9 Author's Address**

Oracle, Corporation.  
100 Crosby Dr.  
Bedford, MA 01730  
USA

Priyesh Mehrotra  
email: [Priyesh.mehrotra@oracle.com](mailto:Priyesh.mehrotra@oracle.com)

**10 Disclaimer**

The content in this document is for informational purposes only and is subject to change by Oracle Corporation without notice. While reasonable efforts have been made in the preparation of this publication to assure its accuracy, Oracle Corporation assumes no liability resulting from technical or editorial errors or omissions, or for any damages resulting from the use of this information. Unless specifically included in a written agreement with Oracle Corporation, Oracle Corporation has no obligation to develop or deliver any future release or upgrade or any feature, enhancement or function.

**11 Full Copyright Statement**

Copyright © Oracle Corporation (2020). All rights reserved. Oracle Corporation, Session-Aware Networking, Net-Net and related marks are trademarks of Oracle Corporation. All other brand names are trademarks or registered trademarks of their respective companies.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implantation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice, disclaimer, and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to Oracle Corporation or other referenced organizations, except as needed for the purpose of developing open standards.

The limited permission granted above are perpetual and will not be revoked by Oracle Corporation or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and ORACLE CORPORATION DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

**APPENDIX A. Reference Configuration: Single-Ended SRTP Termination on secured networks**

```

certificate-record
  name          SDCert
  country       US
  state         MA
  locality      Burlington
  organization   Engineering
  unit
  common-name   172.18.1.71
  key-size      1024
  alternate-name
  trusted       enabled
  key-usage-list
                digitalSignature
                keyEncipherment
  extended-key-usage-list
                serverAuth

  options
  last-modified-by    admin@172.16.1.240
  last-modified-date  2010-09-07 12:14:20
local-policy
  from-address
                *

  to-address
                *

  source-realm
                access

  description
  activate-time    N/A
  deactivate-time  N/A
  state           enabled
  policy-priority  none
  last-modified-by    admin@172.16.1.240
  last-modified-date  2010-09-25 08:01:58
  policy-attribute
    next-hop      172.18.2.100
    realm         core
    action        none
    terminate-recursion  disabled
    carrier
    start-time    0000
    end-time      2400
    days-of-week  U-S
    cost          0
    app-protocol  SIP
    state         enabled
    methods
    media-profiles
    lookup        single
    next-key
    eloc-str-lkup    disabled
    eloc-str-match

media-manager
  state          enabled

```

```
latching                enabled
flow-time-limit         86400
initial-guard-timer     300
subsq-guard-timer       300
tcp-flow-time-limit     86400
tcp-initial-guard-timer 300
tcp-subsq-guard-timer   300
tcp-number-of-ports-per-flow 2
hnt-rtcp                disabled
algd-log-level          NOTICE
mbcd-log-level          NOTICE
red-flow-port           1985
red-mgcp-port           1986
red-max-trans           10000
red-sync-start-time     5000
red-sync-comp-time      1000
media-policing          enabled
max-signaling-bandwidth 10000000
max-untrusted-signaling 100
min-untrusted-signaling 30
app-signaling-bandwidth 0
tolerance-window        30
rtcp-rate-limit         0
trap-on-demote-to-deny  enabled
min-media-allocation    32000
min-trusted-allocation  60000
deny-allocation         32000
anonymous-sdp           disabled
arp-msg-bandwidth       32000
fragment-msg-bandwidth  0
rfc2833-timestamp       disabled
default-2833-duration   100
rfc2833-end-pkts-only-for-non-sig enabled
translate-non-rfc2833-event disabled
media-supervision-traps disabled
dnalg-server-failover   disabled
last-modified-by        admin@172.16.1.240
last-modified-date      2010-08-03 11:50:27
network-interface
name                    M00
sub-port-id             0
description
hostname
ip-address              172.18.1.71
pri-utility-addr
sec-utility-addr
netmask                 255.255.255.0
gateway                 172.18.1.1
sec-gateway
gw-heartbeat
state                   disabled
heartbeat               0
retry-count             0
retry-timeout           1
health-score            0
dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout             11
hip-ip-list             172.18.1.71
ftp-address
```



```

icmp-address          172.18.1.71
snmp-address
telnet-address
ssh-address
last-modified-by     admin@172.16.1.240
last-modified-date   2010-09-29 06:32:29
network-interface
name                 M01
sub-port-id         0
description
hostname
ip-address           172.18.2.71
pri-utility-addr
sec-utility-addr
netmask              255.255.255.0
gateway              172.18.2.1
sec-gateway
gw-heartbeat
state                disabled
heartbeat            0
retry-count          0
retry-timeout        1
health-score         0
dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout          11
hip-ip-list          172.18.2.71
ftp-address
icmp-address          172.18.2.71
snmp-address
telnet-address
ssh-address
last-modified-by     admin@172.16.1.240
last-modified-date   2010-09-29 06:33:52
phy-interface
name                 M00
operation-type       Media
port                 0
slot                 0
virtual-mac
admin-state          enabled
auto-negotiation     enabled
duplex-mode          FULL
speed                100
overload-protection  disabled
last-modified-by     admin@172.16.1.240
last-modified-date   2010-08-03 11:00:33
phy-interface
name                 M01
operation-type       Media
port                 0
slot                 1
virtual-mac
admin-state          enabled
auto-negotiation     enabled
duplex-mode          FULL
speed                100
overload-protection  disabled
last-modified-by     admin@172.16.1.240
last-modified-date   2010-09-29 06:32:01

```

```

realm-config
  identifier          access
  description
  addr-prefix        0.0.0.0
  network-interfaces
    M00:0
  mm-in-realm        enabled
  mm-in-network      enabled
  mm-same-ip         enabled
  mm-in-system       enabled
  bw-cac-non-mm      disabled
  msm-release        disabled
  qos-enable         disabled
  generate-UDP-checksum  disabled
  max-bandwidth      0
  fallback-bandwidth 0
  max-priority-bandwidth 0
  max-latency        0
  max-jitter         0
  max-packet-loss    0
  observ-window-size 0
  parent-realm
  dns-realm
  media-policy
  media-sec-policy    SRTP
  in-translationid
  out-translationid
  in-manipulationid
  out-manipulationid
  manipulation-string
  manipulation-pattern
  class-profile
  average-rate-limit 0
  access-control-trust-level none
  invalid-signal-threshold 0
  maximum-signal-threshold 0
  untrusted-signal-threshold 0
  nat-trust-threshold 0
  deny-period        30
  ext-policy-svr
  symmetric-latching disabled
  pai-strip          disabled
  trunk-context
  early-media-allow
  enforcement-profile
  additional-prefixes
  restricted-latching none
  restriction-mask    32
  accounting-enable   enabled
  user-cac-mode       none
  user-cac-bandwidth  0
  user-cac-sessions   0
  icmp-detect-multiplier 0
  icmp-advertisement-interval 0
  icmp-target-ip
  monthly-minutes    0
  net-management-control disabled
  delay-media-update disabled
  refer-call-transfer disabled
  dyn-refer-term     disabled
  codec-policy
  codec-manip-in-realm disabled

```

```

constraint-name
call-recording-server-id
xnq-state          xnq-unknown
hairpin-id         0
stun-enable        disabled
stun-server-ip     0.0.0.0
stun-server-port   3478
stun-changed-ip    0.0.0.0
stun-changed-port  3479
match-media-profiles
qos-constraint
sip-profile
sip-isup-profile
block-rtcp         disabled
hide-egress-media-update  disabled
last-modified-by   admin@172.16.1.240
last-modified-date 2010-09-08 11:20:12
realm-config
identifier         core
description
addr-prefix       0.0.0.0
network-interfaces
                  M01:0
mm-in-realm       disabled
mm-in-network     enabled
mm-same-ip        enabled
mm-in-system      enabled
bw-cac-non-mm     disabled
msm-release       disabled
qos-enable        disabled
generate-UDP-checksum  disabled
max-bandwidth     0
fallback-bandwidth 0
max-priority-bandwidth 0
max-latency       0
max-jitter        0
max-packet-loss   0
observ-window-size 0
parent-realm
dns-realm
media-policy
media-sec-policy      removeCrypto
in-translationid
out-translationid
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
class-profile
average-rate-limit 0
access-control-trust-level none
invalid-signal-threshold 0
maximum-signal-threshold 0
untrusted-signal-threshold 0
nat-trust-threshold 0
deny-period        30
ext-policy-svr
symmetric-latching disabled
pai-strip          disabled
trunk-context
early-media-allow
enforcement-profile

```

```

additional-prefixes
restricted-latching      none
restriction-mask         32
accounting-enable        enabled
user-cac-mode            none
user-cac-bandwidth       0
user-cac-sessions        0
icmp-detect-multiplier   0
icmp-advertisement-interval 0
icmp-target-ip
monthly-minutes          0
net-management-control   disabled
delay-media-update       disabled
refer-call-transfer      disabled
dyn-refer-term           disabled
codec-policy
codec-manip-in-realm     disabled
constraint-name
call-recording-server-id
xnq-state                xnq-unknown
hairpin-id               0
stun-enable              disabled
stun-server-ip           0.0.0.0
stun-server-port         3478
stun-changed-ip          0.0.0.0
stun-changed-port        3479
match-media-profiles
qos-constraint
sip-profile
sip-isup-profile
block-rtcp               disabled
hide-egress-media-update disabled
last-modified-by         admin@172.16.1.240
last-modified-date       2010-09-08 11:57:07
session-agent
hostname                  172.18.2.100
ip-address                 172.18.2.100
port                       5070
state                      enabled
app-protocol               SIP
app-type
transport-method           UDP
realm-id                   core
egress-realm-id
description
carriers
allow-next-hop-lp         enabled
constraints                disabled
max-sessions               0
max-inbound-sessions       0
max-outbound-sessions      0
max-burst-rate             0
max-inbound-burst-rate     0
max-outbound-burst-rate    0
max-sustain-rate           0
max-inbound-sustain-rate   0
max-outbound-sustain-rate  0
min-seizures               5
min-asr                    0
time-to-resume             0
ttr-no-response            0
in-service-period          0

```

burst-rate-window	0
sustain-rate-window	0
req-uri-carrier-mode	None
proxy-mode	
redirect-action	
loose-routing	enabled
send-media-session	enabled
response-map	
ping-method	
ping-interval	0
ping-send-mode	keep-alive
ping-all-addresses	disabled
ping-in-service-response-codes	
out-service-response-codes	
media-profiles	
in-translationid	
out-translationid	
trust-me	disabled
request-uri-headers	
stop-recurse	
local-response-map	
ping-to-user-part	
ping-from-user-part	
li-trust-me	disabled
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
p-asserted-id	
trunk-group	
max-register-sustain-rate	0
early-media-allow	
invalidate-registrations	disabled
rfc2833-mode	none
rfc2833-payload	0
codec-policy	
enforcement-profile	
refer-call-transfer	disabled
reuse-connections	NONE
tcp-keepalive	none
tcp-reconn-interval	0
max-register-burst-rate	0
register-burst-window	0
sip-profile	
sip-isup-profile	
last-modified-by	admin@172.16.1.240
last-modified-date	2010-09-25 08:01:12
sip-config	
state	enabled
operation-mode	dialog
dialog-transparency	disabled
home-realm-id	core
egress-realm-id	
nat-mode	None
registrar-domain	*
registrar-host	*
registrar-port	5060
register-service-route	always
init-timer	500
max-timer	4000
trans-expire	32
invite-expire	180

```

inactive-dynamic-conn      32
enforcement-profile
pac-method
pac-interval              10
pac-strategy              PropDist
pac-load-weight           1
pac-session-weight        1
pac-route-weight          1
pac-callid-lifetime       600
pac-user-lifetime         3600
red-sip-port              1988
red-max-trans             10000
red-sync-start-time       5000
red-sync-comp-time        1000
add-reason-header         disabled
sip-message-len           4096
enum-sag-match            disabled
extra-method-stats        disabled
rph-feature               disabled
nsep-user-sessions-rate   0
nsep-sa-sessions-rate     0
registration-cache-limit  0
register-use-to-for-lp     disabled
options
refer-src-routing         disabled
add-ucid-header           disabled
pass-gruu-contact         disabled
sag-lookup-on-redirect    disabled
last-modified-by          admin@172.16.1.240
last-modified-date        2010-09-25 10:16:17
sip-interface
state                     enabled
realm-id                   access
description
sip-port
  address                  172.18.1.71
  port                     5061
  transport-protocol       TLS
  tls-profile               SDCert
  allow-anonymous          registered
  ims-aka-profile
carriers
trans-expire               0
invite-expire              0
max-redirect-contacts     0
proxy-mode
redirect-action
contact-mode               none
nat-traversal              always
nat-interval               30
tcp-nat-interval          90
registration-caching       enabled
min-reg-expire             300
registration-interval      3600
route-to-registrar         enabled
secured-network          disabled
teluri-scheme              disabled
uri-fqdn-domain
trust-mode                 all
max-nat-interval           3600
nat-int-increment          10
nat-test-increment         30

```

```

sip-dynamic-hnt      disabled
stop-recurse        401,407
port-map-start      0
port-map-end        0
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
sip-ims-feature      disabled
operator-identifier
anonymous-priority  none
max-incoming-conns  0
per-src-ip-max-incoming-conns 0
inactive-conn-timeout  0
untrusted-conn-timeout  0
network-id
ext-policy-server
default-location-string
charging-vector-mode  pass
charging-function-address-mode pass
ccf-address
ecf-address
term-tgrp-mode      none
implicit-service-route  disabled
rfc2833-payload     101
rfc2833-mode        preferred
constraint-name
response-map
local-response-map
ims-aka-feature      disabled
enforcement-profile
route-unauthorized-calls
tcp-keepalive       none
add-sdp-invite      disabled
add-sdp-profiles
sip-profile
sip-isup-profile
last-modified-by    admin@172.16.1.240
last-modified-date  2010-09-25 12:07:23
sip-interface
state               enabled
realm-id            core
description
sip-port
  address            172.18.2.71
  port               5060
  transport-protocol  UDP
  tls-profile
  allow-anonymous    agents-only
  ims-aka-profile
carriers
trans-expire        0
invite-expire       0
max-redirect-contacts  0
proxy-mode
redirect-action
contact-mode        none
nat-traversal       none
nat-interval        30
tcp-nat-interval    90
registration-caching  disabled
min-reg-expire      300
```

registration-interval	3600
route-to-registrar	disabled
<b>secured-network</b>	<b>enabled</b>
teluri-scheme	disabled
uri-fqdn-domain	
trust-mode	all
max-nat-interval	3600
nat-int-increment	10
nat-test-increment	30
sip-dynamic-hnt	disabled
stop-recurse	401,407
port-map-start	0
port-map-end	0
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
sip-ims-feature	disabled
operator-identifier	
anonymous-priority	none
max-incoming-conns	0
per-src-ip-max-incoming-conns	0
inactive-conn-timeout	0
untrusted-conn-timeout	0
network-id	
ext-policy-server	
default-location-string	
charging-vector-mode	pass
charging-function-address-mode	pass
ccf-address	
ecf-address	
term-tgrp-mode	none
implicit-service-route	disabled
rfc2833-payload	101
rfc2833-mode	transparent
constraint-name	
response-map	
local-response-map	
ims-aka-feature	disabled
enforcement-profile	
route-unauthorized-calls	
tcp-keepalive	none
add-sdp-invite	disabled
add-sdp-profiles	
sip-profile	
sip-isup-profile	
last-modified-by	admin@172.16.1.240
last-modified-date	2010-09-19 14:33:05
steering-pool	
ip-address	172.18.1.71
start-port	20000
end-port	49999
realm-id	access
network-interface	
last-modified-by	admin@172.16.1.240
last-modified-date	2010-08-03 11:44:49
steering-pool	
ip-address	172.18.2.71
start-port	20000
end-port	49999
realm-id	core
network-interface	



```
last-modified-by      admin@172.16.1.240
last-modified-date    2010-09-29 06:35:12
system-config
hostname
description
location
mib-system-contact
mib-system-name
mib-system-location
snmp-enabled          enabled
enable-snmp-auth-traps disabled
enable-snmp-syslog-notify disabled
enable-snmp-monitor-traps disabled
enable-env-monitor-traps disabled
snmp-syslog-his-table-length 1
snmp-syslog-level     WARNING
system-log-level      WARNING
process-log-level     NOTICE
process-log-ip-address 0.0.0.0
process-log-port      0
collect
  sample-interval     5
  push-interval       15
  boot-state          disabled
  start-time          now
  end-time            never
  red-collect-state   disabled
  red-max-trans       1000
  red-sync-start-time 5000
  red-sync-comp-time  1000
  push-success-trap-state disabled
call-trace            disabled
internal-trace        disabled
log-filter            all
default-gateway       172.18.1.1
restart               enabled
exceptions
telnet-timeout        0
console-timeout       0
remote-control        enabled
cli-audit-trail       enabled
link-redundancy-state disabled
source-routing        disabled
cli-more              disabled
terminal-height       24
debug-timeout         0
trap-event-lifetime   0
default-v6-gateway    ::
ipv6-support          disabled
last-modified-by      admin@172.16.1.240
last-modified-date    2010-09-10 12:25:16
tls-profile
name                  SDCert
end-entity-certificate SDCert
trusted-ca-certificates
cipher-list
  ALL
verify-depth          10
mutual-authenticate   disabled
tls-version           compatibility
cert-status-check     disabled
cert-status-profile-list
```

```
last-modified-by      admin@172.16.1.240
last-modified-date    2010-09-07 12:18:56
media-sec-policy
  name                 SRTP
  pass-through         disabled
  inbound
    profile            sdes1
    mode               srtp
    protocol           sdes
  outbound
    profile            sdes1
    mode               srtp
    protocol           sdes
  last-modified-by    admin@172.16.1.240
  last-modified-date  2010-09-08 11:17:33
media-sec-policy
  name                 removeCrypto
  pass-through         disabled
  inbound
    profile
    mode               rtp
    protocol           none
  outbound
    profile
    mode               rtp
    protocol           none
  last-modified-by    admin@172.16.1.240
  last-modified-date  2010-09-08 11:56:09
sdes-profile
  name                 sdes1
  crypto-list          AES_CM_128_HMAC_SHA1_80
  srtp-auth            enabled
  srtp-encrypt         enabled
  srtpc-encrypt        enabled
  egress-offer-format  same-as-ingress
  use-ingress-session-params srtpc-encrypt
                        srtp-auth
  mki                  srtp-encrypt
                        disabled
  key
  salt
  last-modified-by    admin@172.16.1.240
  last-modified-date  2010-09-25 08:18:51
```

**APPENDIX B. Reference Configuration: RTP and Single-Ended SRTP Termination on unsecured networks**

```

certificate-record
  name          SDCert
  country       US
  state         MA
  locality      Burlington
  organization   Engineering
  unit
  common-name   172.18.1.71
  key-size      1024
  alternate-name
  trusted       enabled
  key-usage-list
                digitalSignature
                keyEncipherment
  extended-key-usage-list
                serverAuth

  options
  last-modified-by   admin@172.16.1.240
  last-modified-date 2010-09-07 12:14:20
local-policy
  from-address
                *

  to-address
                *

  source-realm
                access

  description
  activate-time   N/A
  deactivate-time N/A
  state          enabled
  policy-priority none
  last-modified-by   admin@172.16.1.240
  last-modified-date 2010-09-25 08:01:58
  policy-attribute
    next-hop      172.18.2.100
    realm         core
    action        none
    terminate-recursion disabled
    carrier
    start-time    0000
    end-time      2400
    days-of-week  U-S
    cost          0
    app-protocol  SIP
    state         enabled
    methods
    media-profiles
    lookup        single
    next-key
    eloc-str-lkup disabled
    eloc-str-match

media-manager
  state          enabled

```

```
latching                enabled
flow-time-limit         86400
initial-guard-timer     300
subsq-guard-timer       300
tcp-flow-time-limit     86400
tcp-initial-guard-timer 300
tcp-subsq-guard-timer   300
tcp-number-of-ports-per-flow 2
hnt-rtcp                disabled
algd-log-level          NOTICE
mbcd-log-level          NOTICE
red-flow-port           1985
red-mgcp-port           1986
red-max-trans           10000
red-sync-start-time     5000
red-sync-comp-time      1000
media-policing          enabled
max-signaling-bandwidth 10000000
max-untrusted-signaling 100
min-untrusted-signaling 30
app-signaling-bandwidth 0
tolerance-window        30
rtcp-rate-limit         0
trap-on-demote-to-deny  enabled
min-media-allocation    32000
min-trusted-allocation  60000
deny-allocation         32000
anonymous-sdp           disabled
arp-msg-bandwidth       32000
fragment-msg-bandwidth  0
rfc2833-timestamp       disabled
default-2833-duration   100
rfc2833-end-pkts-only-for-non-sig enabled
translate-non-rfc2833-event disabled
media-supervision-traps disabled
dnalg-server-failover   disabled
last-modified-by        admin@172.16.1.240
last-modified-date      2010-08-03 11:50:27
network-interface
name                    M00
sub-port-id             0
description
hostname
ip-address              172.18.1.71
pri-utility-addr
sec-utility-addr
netmask                 255.255.255.0
gateway                 172.18.1.1
sec-gateway
gw-heartbeat
state                   disabled
heartbeat               0
retry-count             0
retry-timeout           1
health-score            0
dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout             11
hip-ip-list             172.18.1.71
ftp-address
```

```

icmp-address          172.18.1.71
snmp-address
telnet-address
ssh-address
last-modified-by     admin@172.16.1.240
last-modified-date   2010-09-29 06:32:29
network-interface
name                 M01
sub-port-id         0
description
hostname
ip-address           172.18.2.71
pri-utility-addr
sec-utility-addr
netmask              255.255.255.0
gateway              172.18.2.1
sec-gateway
gw-heartbeat
state                disabled
heartbeat            0
retry-count          0
retry-timeout        1
health-score         0
dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout          11
hip-ip-list          172.18.2.71
ftp-address
icmp-address          172.18.2.71
snmp-address
telnet-address
ssh-address
last-modified-by     admin@172.16.1.240
last-modified-date   2010-09-29 06:33:52
phy-interface
name                 M00
operation-type       Media
port                 0
slot                 0
virtual-mac
admin-state          enabled
auto-negotiation     enabled
duplex-mode          FULL
speed                100
overload-protection disabled
last-modified-by     admin@172.16.1.240
last-modified-date   2010-08-03 11:00:33
phy-interface
name                 M01
operation-type       Media
port                 0
slot                 1
virtual-mac
admin-state          enabled
auto-negotiation     enabled
duplex-mode          FULL
speed                100
overload-protection disabled
last-modified-by     admin@172.16.1.240
last-modified-date   2010-09-29 06:32:01

```

```

realm-config
  identifier          access
  description
  addr-prefix        0.0.0.0
  network-interfaces
    M00:0
  mm-in-realm        enabled
  mm-in-network      enabled
  mm-same-ip         enabled
  mm-in-system       enabled
  bw-cac-non-mm      disabled
  msm-release        disabled
  qos-enable         disabled
  generate-UDP-checksum  disabled
  max-bandwidth      0
  fallback-bandwidth 0
  max-priority-bandwidth 0
  max-latency        0
  max-jitter         0
  max-packet-loss    0
  observ-window-size 0
  parent-realm
  dns-realm
  media-policy
  media-sec-policy    SRTP
  in-translationid
  out-translationid
  in-manipulationid
  out-manipulationid
  manipulation-string
  manipulation-pattern
  class-profile
  average-rate-limit 0
  access-control-trust-level none
  invalid-signal-threshold 0
  maximum-signal-threshold 0
  untrusted-signal-threshold 0
  nat-trust-threshold 0
  deny-period        30
  ext-policy-svr
  symmetric-latching disabled
  pai-strip          disabled
  trunk-context
  early-media-allow
  enforcement-profile
  additional-prefixes
  restricted-latching none
  restriction-mask    32
  accounting-enable   enabled
  user-cac-mode       none
  user-cac-bandwidth 0
  user-cac-sessions   0
  icmp-detect-multiplier 0
  icmp-advertisement-interval 0
  icmp-target-ip
  monthly-minutes     0
  net-management-control disabled
  delay-media-update  disabled
  refer-call-transfer disabled
  dyn-refer-term      disabled
  codec-policy
  codec-manip-in-realm disabled

```

```

constraint-name
call-recording-server-id
xnq-state          xnq-unknown
hairpin-id         0
stun-enable        disabled
stun-server-ip     0.0.0.0
stun-server-port   3478
stun-changed-ip    0.0.0.0
stun-changed-port  3479
match-media-profiles
qos-constraint
sip-profile
sip-isup-profile
block-rtcp         disabled
hide-egress-media-update  disabled
last-modified-by   admin@172.16.1.240
last-modified-date 2010-09-08 11:20:12
realm-config
identifier          core
description
addr-prefix         0.0.0.0
network-interfaces  M01:0
mm-in-realm         disabled
mm-in-network       enabled
mm-same-ip          enabled
mm-in-system        enabled
bw-cac-non-mm       disabled
msm-release         disabled
qos-enable          disabled
generate-UDP-checksum  disabled
max-bandwidth       0
fallback-bandwidth  0
max-priority-bandwidth  0
max-latency         0
max-jitter          0
max-packet-loss     0
observ-window-size  0
parent-realm
dns-realm
media-policy
media-sec-policy   removeCrypto
in-translationid
out-translationid
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
class-profile
average-rate-limit  0
access-control-trust-level  none
invalid-signal-threshold  0
maximum-signal-threshold  0
untrusted-signal-threshold  0
nat-trust-threshold  0
deny-period         30
ext-policy-svr
symmetric-latching  disabled
pai-strip           disabled
trunk-context
early-media-allow
enforcement-profile

```

```

additional-prefixes
restricted-latching      none
restriction-mask         32
accounting-enable        enabled
user-cac-mode            none
user-cac-bandwidth       0
user-cac-sessions        0
icmp-detect-multiplier   0
icmp-advertisement-interval 0
icmp-target-ip
monthly-minutes          0
net-management-control   disabled
delay-media-update       disabled
refer-call-transfer      disabled
dyn-refer-term           disabled
codec-policy
codec-manip-in-realm     disabled
constraint-name
call-recording-server-id
xnq-state                xnq-unknown
hairpin-id               0
stun-enable              disabled
stun-server-ip           0.0.0.0
stun-server-port         3478
stun-changed-ip          0.0.0.0
stun-changed-port        3479
match-media-profiles
qos-constraint
sip-profile
sip-isup-profile
block-rtcp              disabled
hide-egress-media-update disabled
last-modified-by         admin@172.16.1.240
last-modified-date       2010-09-08 11:57:07
session-agent
hostname                 172.18.2.100
ip-address               172.18.2.100
port                    5070
state                   enabled
app-protocol             SIP
app-type
transport-method        UDP
realm-id                 core
egress-realm-id
description
carriers
allow-next-hop-lp        enabled
constraints              disabled
max-sessions             0
max-inbound-sessions     0
max-outbound-sessions    0
max-burst-rate           0
max-inbound-burst-rate   0
max-outbound-burst-rate  0
max-sustain-rate         0
max-inbound-sustain-rate 0
max-outbound-sustain-rate 0
min-seizures             5
min-asr                  0
time-to-resume           0
ttr-no-response          0
in-service-period        0

```



burst-rate-window	0
sustain-rate-window	0
req-uri-carrier-mode	None
proxy-mode	
redirect-action	
loose-routing	enabled
send-media-session	enabled
response-map	
ping-method	
ping-interval	0
ping-send-mode	keep-alive
ping-all-addresses	disabled
ping-in-service-response-codes	
out-service-response-codes	
media-profiles	
in-translationid	
out-translationid	
trust-me	disabled
request-uri-headers	
stop-recurse	
local-response-map	
ping-to-user-part	
ping-from-user-part	
li-trust-me	disabled
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
p-asserted-id	
trunk-group	
max-register-sustain-rate	0
early-media-allow	
invalidate-registrations	disabled
rfc2833-mode	none
rfc2833-payload	0
codec-policy	
enforcement-profile	
refer-call-transfer	disabled
reuse-connections	NONE
tcp-keepalive	none
tcp-reconn-interval	0
max-register-burst-rate	0
register-burst-window	0
sip-profile	
sip-isup-profile	
last-modified-by	admin@172.16.1.240
last-modified-date	2010-09-25 08:01:12
sip-config	
state	enabled
operation-mode	dialog
dialog-transparency	disabled
home-realm-id	core
egress-realm-id	
nat-mode	None
registrar-domain	*
registrar-host	*
registrar-port	5060
register-service-route	always
init-timer	500
max-timer	4000
trans-expire	32
invite-expire	180

```

inactive-dynamic-conn      32
enforcement-profile
pac-method
pac-interval              10
pac-strategy              PropDist
pac-load-weight           1
pac-session-weight        1
pac-route-weight          1
pac-callid-lifetime       600
pac-user-lifetime         3600
red-sip-port              1988
red-max-trans             10000
red-sync-start-time       5000
red-sync-comp-time        1000
add-reason-header         disabled
sip-message-len           4096
enum-sag-match            disabled
extra-method-stats        disabled
rph-feature               disabled
nsep-user-sessions-rate   0
nsep-sa-sessions-rate     0
registration-cache-limit  0
register-use-to-for-lp     disabled
options
refer-src-routing         disabled
add-ucid-header           disabled
pass-gruu-contact         disabled
sag-lookup-on-redirect    disabled
last-modified-by         admin@172.16.1.240
last-modified-date        2010-09-25 10:16:17
sip-interface
state                     enabled
realm-id                  access
description
sip-port
  address                  172.18.1.71
  port                     5061
  transport-protocol       TLS
  tls-profile              SDCert
  allow-anonymous          registered
  ims-aka-profile
sip-port
  address                  172.18.1.71
  port                     5060
  transport-protocol       UDP
  tls-profile
  allow-anonymous          registered
  ims-aka-profile

carriers
trans-expire              0
invite-expire             0
max-redirect-contacts     0
proxy-mode
redirect-action
contact-mode              none
nat-traversal             always
nat-interval              30
tcp-nat-interval          90
registration-caching      enabled
min-reg-expire            300
registration-interval     3600

```

```

route-to-registrar      enabled
secured-network      enabled
teluri-scheme          disabled
uri-fqdn-domain
trust-mode             all
max-nat-interval       3600
nat-int-increment      10
nat-test-increment     30
sip-dynamic-hnt        disabled
stop-recurse           401,407
port-map-start         0
port-map-end           0
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
sip-ims-feature        disabled
operator-identifier
anonymous-priority     none
max-incoming-conns    0
per-src-ip-max-incoming-conns 0
inactive-conn-timeout  0
untrusted-conn-timeout 0
network-id
ext-policy-server
default-location-string
charging-vector-mode   pass
charging-function-address-mode pass
ccf-address
ecf-address
term-tgrp-mode         none
implicit-service-route disabled
rfc2833-payload        101
rfc2833-mode           preferred
constraint-name
response-map
local-response-map
ims-aka-feature        disabled
enforcement-profile
route-unauthorized-calls
tcp-keepalive          none
add-sdp-invite         disabled
add-sdp-profiles
sip-profile
sip-isup-profile
last-modified-by      admin@172.16.1.240
last-modified-date    2010-09-25 12:07:23
sip-interface
state                  enabled
realm-id               core
description
sip-port
  address              172.18.2.71
  port                 5060
  transport-protocol   UDP
  tls-profile
  allow-anonymous      agents-only
  ims-aka-profile
carriers
trans-expire           0
invite-expire          0
max-redirect-contacts 0

```

```

proxy-mode
redirect-action
contact-mode          none
nat-traversal         none
nat-interval          30
tcp-nat-interval      90
registration-caching  disabled
min-reg-expire        300
registration-interval 3600
route-to-registrar    disabled
secured-network      enabled
teluri-scheme         disabled
uri-fqdn-domain
trust-mode            all
max-nat-interval      3600
nat-int-increment     10
nat-test-increment    30
sip-dynamic-hnt       disabled
stop-recurse          401,407
port-map-start        0
port-map-end          0
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
sip-ims-feature       disabled
operator-identifier
anonymous-priority    none
max-incoming-conns    0
per-src-ip-max-incoming-conns 0
inactive-conn-timeout 0
untrusted-conn-timeout 0
network-id
ext-policy-server
default-location-string
charging-vector-mode  pass
charging-function-address-mode pass
ccf-address
ecf-address
term-tgrp-mode        none
implicit-service-route disabled
rfc2833-payload       101
rfc2833-mode          transparent
constraint-name
response-map
local-response-map
ims-aka-feature       disabled
enforcement-profile
route-unauthorized-calls
tcp-keepalive         none
add-sdp-invite        disabled
add-sdp-profiles
sip-profile
sip-isup-profile
last-modified-by      admin@172.16.1.240
last-modified-date    2010-09-19 14:33:05
steering-pool
ip-address          172.18.1.71
start-port            20000
end-port              49999
realm-id              access
network-interface

```

```

last-modified-by      admin@172.16.1.240
last-modified-date    2010-08-03 11:44:49
steering-pool
  ip-address           172.18.2.71
  start-port           20000
  end-port             49999
  realm-id             core
  network-interface
  last-modified-by    admin@172.16.1.240
  last-modified-date  2010-09-29 06:35:12
system-config
  hostname
  description
  location
  mib-system-contact
  mib-system-name
  mib-system-location
  snmp-enabled         enabled
  enable-snmp-auth-traps  disabled
  enable-snmp-syslog-notify disabled
  enable-snmp-monitor-traps disabled
  enable-env-monitor-traps disabled
  snmp-syslog-his-table-length 1
  snmp-syslog-level    WARNING
  system-log-level     WARNING
  process-log-level    NOTICE
  process-log-ip-address 0.0.0.0
  process-log-port     0
collect
  sample-interval     5
  push-interval       15
  boot-state          disabled
  start-time          now
  end-time            never
  red-collect-state   disabled
  red-max-trans       1000
  red-sync-start-time 5000
  red-sync-comp-time  1000
  push-success-trap-state disabled
call-trace            disabled
internal-trace        disabled
log-filter            all
default-gateway       172.18.1.1
restart               enabled
exceptions
telnet-timeout        0
console-timeout       0
remote-control        enabled
cli-audit-trail       enabled
link-redundancy-state disabled
source-routing        disabled
cli-more              disabled
terminal-height       24
debug-timeout         0
trap-event-lifetime   0
default-v6-gateway    ::
ipv6-support          disabled
last-modified-by      admin@172.16.1.240
last-modified-date    2010-09-10 12:25:16
tls-profile
  name                SDCert
  end-entity-certificate SDCert

```

```

trusted-ca-certificates
cipher-list
    ALL
verify-depth      10
mutual-authenticate disabled
tls-version       compatibility
cert-status-check disabled
cert-status-profile-list
last-modified-by  admin@172.16.1.240
last-modified-date 2010-09-07 12:18:56

```

**media-sec-policy**

```

name          SRTP
pass-through  disabled
inbound
  profile     sdes1
  mode        any
  protocol    sdes
outbound
  profile     sdes1
  mode        any
  protocol    sdes
last-modified-by  admin@172.16.1.240
last-modified-date 2010-09-08 11:17:33

```

**media-sec-policy**

```

name          removeCrypto
pass-through  disabled
inbound
  profile
  mode        rtp
  protocol    none
outbound
  profile
  mode        rtp
  protocol    none
last-modified-by  admin@172.16.1.240
last-modified-date 2010-09-08 11:56:09

```

**sdes-profile**

```

name          sdes1
crypto-list   AES_CM_128_HMAC_SHA1_80
srtp-auth     enabled
srtp-encrypt  enabled
srtpc-encrypt enabled
egress-offer-format simultaneous-best-effort
use-ingress-session-params srtpc-encrypt
                                srtp-auth
mki           srtp-encrypt
                                disabled
key
salt
last-modified-by  admin@172.16.1.240
last-modified-date 2010-09-25 08:18:51

```

**APPENDIX C. Reference Configuration: Back-to-Back SRTP Termination**

```
certificate-record
  name          SDCert
  country       US
  state         MA
  locality      Burlington
  organization   Engineering
  unit
  common-name   172.18.1.71
  key-size      1024
  alternate-name
  trusted       enabled
  key-usage-list
                digitalSignature
                keyEncipherment
  extended-key-usage-list
                serverAuth

  options
  last-modified-by    admin@172.16.1.240
  last-modified-date  2010-09-07 12:14:20
certificate-record
  name          SDCertII
  country       US
  state         MA
  locality      Burlington
  organization   Engineering
  unit
  common-name   172.18.2.71
  key-size      1024
  alternate-name
  trusted       enabled
  key-usage-list
                digitalSignature
                keyEncipherment
  extended-key-usage-list
                serverAuth

  options
  last-modified-by    admin@172.16.1.240
  last-modified-date  2010-09-07 12:14:20
local-policy
  from-address    *
  to-address      *
  source-realm    peer1A
  description
  activate-time   N/A
  deactivate-time N/A
  state           enabled
  policy-priority none
  last-modified-by    admin@172.16.1.240
  last-modified-date  2010-09-25 08:01:58
  policy-attribute
    next-hop      172.18.2.100
```

```

realm                peer1B
action               none
terminate-recursion  disabled
carrier
start-time           0000
end-time             2400
days-of-week        U-S
cost                 0
app-protocol         SIP
state                enabled
methods
media-profiles
lookup               single
next-key
eloc-str-lkup        disabled
eloc-str-match

local-policy
from-address         *
to-address           *
source-realm         peer1B
description
activate-time        N/A
deactivate-time      N/A
state                enabled
policy-priority      none
last-modified-by    admin@172.16.1.240
last-modified-date   2010-09-25 08:01:58
policy-attribute
next-hop             172.18.1.200
realm                peer1A
action               none
terminate-recursion  disabled
carrier
start-time           0000
end-time             2400
days-of-week        U-S
cost                 0
app-protocol         SIP
state                enabled
methods
media-profiles
lookup               single
next-key
eloc-str-lkup        disabled
eloc-str-match

media-manager
state                enabled
latching             enabled
flow-time-limit      86400
initial-guard-timer  300
subsq-guard-timer    300
tcp-flow-time-limit  86400
tcp-initial-guard-timer 300
tcp-subsq-guard-timer 300
tcp-number-of-ports-per-flow 2
hnt-rtcp             disabled
algd-log-level       NOTICE
mabcd-log-level      NOTICE
red-flow-port        1985

```



```

red-mgcp-port      1986
red-max-trans     10000
red-sync-start-time 5000
red-sync-comp-time 1000
media-policing    enabled
max-signaling-bandwidth 10000000
max-untrusted-signaling 100
min-untrusted-signaling 30
app-signaling-bandwidth 0
tolerance-window 30
rtcp-rate-limit  0
trap-on-demote-to-deny enabled
min-media-allocation 32000
min-trusted-allocation 60000
deny-allocation 32000
anonymous-sdp      disabled
arp-msg-bandwidth  32000
fragment-msg-bandwidth 0
rfc2833-timestamp  disabled
default-2833-duration 100
rfc2833-end-pkts-only-for-non-sig enabled
translate-non-rfc2833-event disabled
media-supervision-traps disabled
dnalg-server-failover disabled
last-modified-by  admin@172.16.1.240
last-modified-date 2010-08-03 11:50:27
network-interface
name                M00
sub-port-id         0
description
hostname
ip-address          172.18.1.71
pri-utility-addr
sec-utility-addr
netmask             255.255.255.0
gateway             172.18.1.1
sec-gateway
gw-heartbeat
state               disabled
heartbeat           0
retry-count         0
retry-timeout       1
health-score        0
dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout         11
hip-ip-list         172.18.1.71
ftp-address
icmp-address        172.18.1.71
snmp-address
telnet-address
ssh-address
last-modified-by  admin@172.16.1.240
last-modified-date 2010-09-29 06:32:29
network-interface
name                M01
sub-port-id         0
description
hostname
ip-address          172.18.2.71

```

```

pri-utility-addr
sec-utility-addr
netmask          255.255.255.0
gateway          172.18.2.1
sec-gateway
gw-heartbeat
  state          disabled
  heartbeat      0
  retry-count    0
  retry-timeout  1
  health-score   0
dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout      11
hip-ip-list      172.18.2.71
ftp-address
icmp-address     172.18.2.71
snmp-address
telnet-address
ssh-address
last-modified-by admin@172.16.1.240
last-modified-date 2010-09-29 06:33:52
phy-interface
  name           M00
  operation-type Media
  port           0
  slot           0
  virtual-mac
  admin-state    enabled
  auto-negotiation enabled
  duplex-mode    FULL
  speed          100
  overload-protection disabled
  last-modified-by admin@172.16.1.240
  last-modified-date 2010-08-03 11:00:33
phy-interface
  name           M01
  operation-type Media
  port           0
  slot           1
  virtual-mac
  admin-state    enabled
  auto-negotiation enabled
  duplex-mode    FULL
  speed          100
  overload-protection disabled
  last-modified-by admin@172.16.1.240
  last-modified-date 2010-09-29 06:32:01
realm-config
  identifier     peer1A
  description
  addr-prefix    0.0.0.0
  network-interfaces
                M00:0
  mm-in-realm   enabled
  mm-in-network enabled
  mm-same-ip    enabled
  mm-in-system  enabled
  bw-cac-non-mm disabled
  msm-release   disabled

```

qos-enable	disabled
generate-UDP-checksum	disabled
max-bandwidth	0
fallback-bandwidth	0
max-priority-bandwidth	0
max-latency	0
max-jitter	0
max-packet-loss	0
observ-window-size	0
parent-realm	
dns-realm	
media-policy	
<b>media-sec-policy</b>	<b>SRTPA</b>
in-translationid	
out-translationid	
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
class-profile	
average-rate-limit	0
access-control-trust-level	none
invalid-signal-threshold	0
maximum-signal-threshold	0
untrusted-signal-threshold	0
nat-trust-threshold	0
deny-period	30
ext-policy-svr	
symmetric-latching	disabled
pai-strip	disabled
trunk-context	
early-media-allow	
enforcement-profile	
additional-prefixes	
restricted-latching	none
restriction-mask	32
accounting-enable	enabled
user-cac-mode	none
user-cac-bandwidth	0
user-cac-sessions	0
icmp-detect-multiplier	0
icmp-advertisement-interval	0
icmp-target-ip	
monthly-minutes	0
net-management-control	disabled
delay-media-update	disabled
refer-call-transfer	disabled
dyn-refer-term	disabled
codec-policy	
codec-manip-in-realm	disabled
constraint-name	
call-recording-server-id	
xnq-state	xnq-unknown
hairpin-id	0
stun-enable	disabled
stun-server-ip	0.0.0.0
stun-server-port	3478
stun-changed-ip	0.0.0.0
stun-changed-port	3479
match-media-profiles	
qos-constraint	
sip-profile	

```

sip-isup-profile
block-rtcp          disabled
hide-egress-media-update  disabled
last-modified-by    admin@172.16.1.240
last-modified-date  2010-09-08 11:20:12
realm-config
  identifier         peer1B
  description
  addr-prefix        0.0.0.0
  network-interfaces
                    M01:0
  mm-in-realm        disabled
  mm-in-network      enabled
  mm-same-ip         enabled
  mm-in-system       enabled
  bw-cac-non-mm      disabled
  msm-release        disabled
  qos-enable         disabled
  generate-UDP-checksum  disabled
  max-bandwidth      0
  fallback-bandwidth 0
  max-priority-bandwidth 0
  max-latency        0
  max-jitter         0
  max-packet-loss    0
  observ-window-size 0
  parent-realm
  dns-realm
  media-policy
  media-sec-policy  SRTPB
  in-translationid
  out-translationid
  in-manipulationid
  out-manipulationid
  manipulation-string
  manipulation-pattern
  class-profile
  average-rate-limit 0
  access-control-trust-level none
  invalid-signal-threshold 0
  maximum-signal-threshold 0
  untrusted-signal-threshold 0
  nat-trust-threshold 0
  deny-period        30
  ext-policy-svr
  symmetric-latching disabled
  pai-strip          disabled
  trunk-context
  early-media-allow
  enforcement-profile
  additional-prefixes
  restricted-latching none
  restriction-mask    32
  accounting-enable   enabled
  user-cac-mode       none
  user-cac-bandwidth 0
  user-cac-sessions   0
  icmp-detect-multiplier 0
  icmp-advertisement-interval 0
  icmp-target-ip
  monthly-minutes    0
  net-management-control  disabled

```

```

delay-media-update      disabled
refer-call-transfer     disabled
dyn-refer-term          disabled
codec-policy
codec-manip-in-realm    disabled
constraint-name
call-recording-server-id
xnq-state               xnq-unknown
hairpin-id              0
stun-enable             disabled
stun-server-ip          0.0.0.0
stun-server-port        3478
stun-changed-ip         0.0.0.0
stun-changed-port       3479
match-media-profiles
qos-constraint
sip-profile
sip-isup-profile
block-rtcp              disabled
hide-egress-media-update disabled
last-modified-by        admin@172.16.1.240
last-modified-date      2010-09-08 11:57:07
session-agent
hostname                172.18.2.100
ip-address              172.18.2.100
port                    5060
state                   enabled
app-protocol            SIP
app-type
transport-method        TLS
realm-id                peer1B
egress-realm-id
description
carriers
allow-next-hop-lp       enabled
constraints              disabled
max-sessions            0
max-inbound-sessions    0
max-outbound-sessions   0
max-burst-rate          0
max-inbound-burst-rate  0
max-outbound-burst-rate 0
max-sustain-rate        0
max-inbound-sustain-rate 0
max-outbound-sustain-rate 0
min-seizures            5
min-asr                 0
time-to-resume          0
ttr-no-response         0
in-service-period       0
burst-rate-window       0
sustain-rate-window     0
req-uri-carrier-mode    None
proxy-mode
redirect-action
loose-routing           enabled
send-media-session      enabled
response-map
ping-method
ping-interval           0
ping-send-mode          keep-alive
ping-all-addresses     disabled

```

```

ping-in-service-response-codes
out-service-response-codes
media-profiles
in-translationid
out-translationid
trust-me          disabled
request-uri-headers
stop-recurse
local-response-map
ping-to-user-part
ping-from-user-part
li-trust-me       disabled
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
p-asserted-id
trunk-group
max-register-sustain-rate  0
early-media-allow
invalidate-registrations  disabled
rfc2833-mode              none
rfc2833-payload           0
codec-policy
enforcement-profile
refer-call-transfer       disabled
reuse-connections        NONE
tcp-keepalive             none
tcp-reconn-interval       0
max-register-burst-rate   0
register-burst-window     0
sip-profile
sip-isup-profile
last-modified-by         admin@172.16.1.240
last-modified-date       2010-09-25 08:01:12
session-agent
hostname                  172.18.1.200
ip-address                 172.18.1.200
port                       5060
state                      enabled
app-protocol               SIP
app-type
transport-method          TLS
realm-id                   peer1A
egress-realm-id
description
carriers
allow-next-hop-lp         enabled
constraints                disabled
max-sessions               0
max-inbound-sessions       0
max-outbound-sessions      0
max-burst-rate             0
max-inbound-burst-rate     0
max-outbound-burst-rate    0
max-sustain-rate          0
max-inbound-sustain-rate   0
max-outbound-sustain-rate  0
min-seizures               5
min-asr                     0
time-to-resume             0
ttr-no-response            0

```

in-service-period	0
burst-rate-window	0
sustain-rate-window	0
req-uri-carrier-mode	None
proxy-mode	
redirect-action	
loose-routing	enabled
send-media-session	enabled
response-map	
ping-method	
ping-interval	0
ping-send-mode	keep-alive
ping-all-addresses	disabled
ping-in-service-response-codes	
out-service-response-codes	
media-profiles	
in-translationid	
out-translationid	
trust-me	disabled
request-uri-headers	
stop-recurse	
local-response-map	
ping-to-user-part	
ping-from-user-part	
li-trust-me	disabled
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
p-asserted-id	
trunk-group	
max-register-sustain-rate	0
early-media-allow	
invalidate-registrations	disabled
rfc2833-mode	none
rfc2833-payload	0
codec-policy	
enforcement-profile	
refer-call-transfer	disabled
reuse-connections	NONE
tcp-keepalive	none
tcp-reconn-interval	0
max-register-burst-rate	0
register-burst-window	0
sip-profile	
sip-isup-profile	
last-modified-by	admin@172.16.1.240
last-modified-date	2010-09-25 08:01:12
sip-config	
state	enabled
operation-mode	dialog
dialog-transparency	disabled
home-realm-id	peer1B
egress-realm-id	
nat-mode	None
registrar-domain	*
registrar-host	*
registrar-port	5060
register-service-route	always
init-timer	500
max-timer	4000
trans-expire	32

```

invite-expire          180
inactive-dynamic-conn  32
enforcement-profile
pac-method
pac-interval          10
pac-strategy          PropDist
pac-load-weight       1
pac-session-weight    1
pac-route-weight      1
pac-callid-lifetime   600
pac-user-lifetime     3600
red-sip-port          1988
red-max-trans         10000
red-sync-start-time   5000
red-sync-comp-time    1000
add-reason-header     disabled
sip-message-len       4096
enum-sag-match        disabled
extra-method-stats    disabled
rph-feature           disabled
nsep-user-sessions-rate 0
nsep-sa-sessions-rate 0
registration-cache-limit 0
register-use-to-for-lp disabled
options
refer-src-routing     disabled
add-ucid-header       disabled
pass-gruu-contact     disabled
sag-lookup-on-redirect disabled
last-modified-by      admin@172.16.1.240
last-modified-date    2010-09-25 10:16:17
sip-interface
state                 enabled
realm-id              peer1A
description
sip-port
  address              172.18.1.71
  port                 5061
  transport-protocol   TLS
  tls-profile          SDCert
  allow-anonymous      agents-only
  ims-aka-profile
carriers
trans-expire          0
invite-expire         0
max-redirect-contacts 0
proxy-mode
redirect-action
contact-mode          none
nat-traversal         none
nat-interval          30
tcp-nat-interval      90
registration-caching  disabled
min-reg-expire        300
registration-interval 3600
route-to-registrar    disabled
secured-network      disabled
teluri-scheme         disabled
uri-fqdn-domain
trust-mode            all
max-nat-interval      3600
nat-int-increment     10

```



```

nat-test-increment      30
sip-dynamic-hnt         disabled
stop-recurse           401,407
port-map-start          0
port-map-end            0
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
sip-ims-feature         disabled
operator-identifier
anonymous-priority      none
max-incoming-conns     0
per-src-ip-max-incoming-conns 0
inactive-conn-timeout  0
untrusted-conn-timeout 0
network-id
ext-policy-server
default-location-string
charging-vector-mode    pass
charging-function-address-mode pass
ccf-address
ecf-address
term-tgrp-mode          none
implicit-service-route  disabled
rfc2833-payload        101
rfc2833-mode            preferred
constraint-name
response-map
local-response-map
ims-aka-feature         disabled
enforcement-profile
route-unauthorized-calls
tcp-keepalive           none
add-sdp-invite          disabled
add-sdp-profiles
sip-profile
sip-isup-profile
last-modified-by       admin@172.16.1.240
last-modified-date     2010-09-25 12:07:23
sip-interface
state                   enabled
realm-id                peer1B
description
sip-port
  address                172.18.2.71
  port                   5061
  transport-protocol     TLS
  tls-profile            SDCertII
  allow-anonymous        agents-only
  ims-aka-profile
carriers
trans-expire            0
invite-expire           0
max-redirect-contacts  0
proxy-mode
redirect-action
contact-mode            none
nat-traversal           none
nat-interval            30
tcp-nat-interval        90
registration-caching    disabled

```

min-reg-expire	300
registration-interval	3600
route-to-registrar	disabled
<b>secured-network</b>	<b>disabled</b>
teluri-scheme	disabled
uri-fqdn-domain	
trust-mode	all
max-nat-interval	3600
nat-int-increment	10
nat-test-increment	30
sip-dynamic-hnt	disabled
stop-recurse	401,407
port-map-start	0
port-map-end	0
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
sip-ims-feature	disabled
operator-identifier	
anonymous-priority	none
max-incoming-conns	0
per-src-ip-max-incoming-conns	0
inactive-conn-timeout	0
untrusted-conn-timeout	0
network-id	
ext-policy-server	
default-location-string	
charging-vector-mode	pass
charging-function-address-mode	pass
ccf-address	
ecf-address	
term-tgrp-mode	none
implicit-service-route	disabled
rfc2833-payload	101
rfc2833-mode	transparent
constraint-name	
response-map	
local-response-map	
ims-aka-feature	disabled
enforcement-profile	
route-unauthorized-calls	
tcp-keepalive	none
add-sdp-invite	disabled
add-sdp-profiles	
sip-profile	
sip-isup-profile	
last-modified-by	admin@172.16.1.240
last-modified-date	2010-09-19 14:33:05
steering-pool	
ip-address	172.18.1.71
start-port	20000
end-port	49999
realm-id	peer1A
network-interface	
last-modified-by	admin@172.16.1.240
last-modified-date	2010-08-03 11:44:49
steering-pool	
ip-address	172.18.2.71
start-port	20000
end-port	49999
realm-id	peer1B

```
network-interface
last-modified-by      admin@172.16.1.240
last-modified-date    2010-09-29 06:35:12
system-config
hostname
description
location
mib-system-contact
mib-system-name
mib-system-location
snmp-enabled          enabled
enable-snmp-auth-traps  disabled
enable-snmp-syslog-notify  disabled
enable-snmp-monitor-traps  disabled
enable-env-monitor-traps  disabled
snmp-syslog-his-table-length  1
snmp-syslog-level      WARNING
system-log-level       WARNING
process-log-level      NOTICE
process-log-ip-address  0.0.0.0
process-log-port       0
collect
  sample-interval      5
  push-interval        15
  boot-state           disabled
  start-time           now
  end-time             never
  red-collect-state    disabled
  red-max-trans        1000
  red-sync-start-time  5000
  red-sync-comp-time   1000
  push-success-trap-state  disabled
call-trace             disabled
internal-trace         disabled
log-filter             all
default-gateway        172.18.1.1
restart                enabled
exceptions
telnet-timeout         0
console-timeout        0
remote-control         enabled
cli-audit-trail        enabled
link-redundancy-state  disabled
source-routing         disabled
cli-more               disabled
terminal-height        24
debug-timeout          0
trap-event-lifetime    0
default-v6-gateway     ::
ipv6-support           disabled
last-modified-by      admin@172.16.1.240
last-modified-date    2010-09-10 12:25:16
tls-profile
name                   SDCert
end-entity-certificate SDCert
trusted-ca-certificates
cipher-list            ALL
verify-depth           10
mutual-authenticate    disabled
tls-version            compatibility
cert-status-check      disabled
```

```

cert-status-profile-list
last-modified-by      admin@172.16.1.240
last-modified-date    2010-09-07 12:18:56
tls-profile
name                  SDCertII
end-entity-certificate SDCertII
trusted-ca-certificates
cipher-list
                      ALL
verify-depth          10
mutual-authenticate   disabled
tls-version            compatibility
cert-status-check     disabled
cert-status-profile-list
last-modified-by      admin@172.16.1.240
last-modified-date    2010-09-07 12:18:56

```

**media-sec-policy**

```

name                  SRTPA
pass-through          disabled
inbound
  profile             sdes1
  mode                srtp
  protocol             sdes
outbound
  profile             sdes1
  mode                srtp
  protocol             sdes
last-modified-by      admin@172.16.1.240
last-modified-date    2010-09-08 11:17:33

```

**media-sec-policy**

```

name                  SRTPB
pass-through          disabled
inbound
  profile             sdes2
  mode                srtp
  protocol             sdes
outbound
  profile             sdes2
  mode                srtp
  protocol             sdes
last-modified-by      admin@172.16.1.240
last-modified-date    2010-09-08 11:17:33

```

**sdes-profile**

```

name                  sdes1
crypto-list           AES_CM_128_HMAC_SHA1_80
srtp-auth             enabled
srtp-encrypt          enabled
srtpc-encrypt         enabled
egress-offer-format   same-as-ingress
use-ingress-session-params srtpc-encrypt
                      srtp-auth
mki                   srtp-encrypt
                      disabled

```

```

key
salt
last-modified-by      admin@172.16.1.240
last-modified-date    2010-09-25 08:18:51

```

**sdes-profile**

```

name                  sdes2
crypto-list           AES_CM_128_HMAC_SHA1_32
srtp-auth             enabled
srtp-encrypt          enabled

```

```
srtp-encrypt          enabled
egress-offer-format  same-as-ingress
use-ingress-session-params srtp-encrypt
                    srtp-auth
mki                  srtp-encrypt
                    disabled
key
salt
last-modified-by     admin@172.16.1.240
last-modified-date   2010-09-25 08:18:51
```