



ORACLE

DDOS Prevention Configuration for SIP Peering environments

Technical Application Note

ORACLE

COMMUNICATIONS



Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

1	Table of Contents	
2	INTENDED AUDIENCE	4
3	DOCUMENT OVERVIEW	4
4	GENERAL APPROACH	5
4.1	SUPPORTED PLATFORMS	5
4.2	TRAFFIC TERMINOLOGIES USED IN SBC	5
4.3	ENDPOINTS PROMOTION AND DEMOTION	5
4.3.1	Statistics	6
5	DDOS PREVENTION FOR PEERING ENVIRONMENTS	7
5.1	TEST ENVIRONMENT	7
5.2	TEST METHODOLOGY	7
5.2.1	Maximum Signaling Bandwidth (max-signaling-bandwidth)	7
5.2.2	Max and Min Untrusted Signaling Percentages (max-untrusted-signaling & min-untrusted-signaling)	8
5.2.3	DDoS Attacks	8
5.3	SBC CONFIGURATION FOR DDOS PREVENTION IN PEERING ENVIRONMENT	8
5.3.1	Realm Configuration	8
5.3.2	SIP Interface	9
5.3.3	Session Agent and Access-Control	10
5.4	DDOS CONFIGURATION SETTINGS PER PLATFORM IN PEERING ENVIRONMENTS	11
5.4.1	Acme Packet 4600 1000000 Flow Table 16G memory - copper single GigE	11
5.4.2	Acme Packet 6100 1000000 Flow Table 16G memory - copper single GigE	12
5.4.3	Acme Packet 6350 2000000 Flow Table 48G memory - copper single GigE	12
5.4.4	Acme Packet 6300 1000000 Flow Table 16G memory - copper single GigE	13
6	APPENDIX A	14
7	APPENDIX B	17
7.1	DDOS-2 SHOW COMMANDS	17



2 Intended Audience

This document is intended for use by Oracle Systems Engineers, third party Systems Integrators, Oracle Enterprise customers and partners and end users of the Oracle Enterprise Session Border Controller (SBC). It is assumed that the reader is familiar with basic operations of the Oracle Enterprise Session Border Controller.

3 Document Overview

This document is designed to provide a basic framework for DDoS configuration in SIP Peering environments across all hardware. The scope of this document is limited to providing a minimum set of configuration settings to enable basic protection. The contents herein cannot be considered advanced or customer specific in any way. Where appropriate, limitations of this protection will be addressed throughout the course of this document. This document will not go into any detail pertaining to the underlying SIP configuration.

All base configurations used during testing were created according to Best Current Practices

4 General Approach

This document is designed to provide minimal DDoS settings for SIP peering SBC environments across all hardware.

The software release used for the testing is R SCZ8.4.0. The SBC model used here is Policy Based Realm Bridging Model(PBRB).

4.1 Supported Platforms

Here is the list of supported platforms for DDoS configuration.

Platform	Flow Table Size	Memory
AP 6350	2000000	48G
AP6300	1000000	16G
AP4600	1000000	16G
AP6100	1000000	16G
VME720	720	4G
AP1100	720	4G
AP3900	16000	16G

4.2 Traffic Terminologies Used in SBC

1. Flow- An individual conversation between two endpoints (may or may not be policed) –finest layer
2. Queue - A bundle of flows coming from the same IP/port
3. Pipe -A bundle of queues that represent a class of traffic (Untrusted, trusted...)
4. Port - Port is located between the wire-speed fabric and the path to the CPU. The coarsest layer of the framework

4.3 Endpoints Promotion and Demotion

Endpoints, irrespective of whether or not they are defined as session-agents are promoted/demoted between hardware-enforced trusted and denied Access Control List traffic queues based on trust level configuration. Static ACLs are also configurable to further classify signaling traffic as being permanently assigned to the appropriate trust queue. Trust is assigned through several mechanisms including the access-control-trust-level parameter of the realm the session-agent or end point is a member of, trust-level of provisioned ACLs, and the allow-anonymous setting on the applicable sip-interface. The SBC will demote an endpoint if:

- It receives too many signaling messages within the configured time window (maximum-signal-threshold in the realm or static ACL)
- It receives too many invalid signaling messages within the configured time window (invalid-signal-threshold in the realm or static ACL)
- It receives too many signaling messages from an untrusted source within the configured time window (untrusted-signal-threshold in the realm or static ACL)

- A trusted endpoint exceeds the call admission controls and the cac-failurethreshold defined in an ACL (the call admission control limits are defined in media profiles)
- An untrusted endpoint exceeds call admission controls and the untrust-cac-failurethreshold defined in an ACL.

The SBC will promote an endpoint if:

- It received a 200 OK response to a registration
- The registration overload protection (reg-overload-protect) option has been set globally in the sip-config element (this is temporary, and only if a 401 or 407 response is received)
- The deny-period has expired.

4.3.1 Statistics

Each promotion and demotion event, between trusted, untrusted, and deny queues is counted and kept as an ACL statistic. These counts are maintained separately for signaling applications. Statistics for ACL status and operations can be seen using the ACLI commands show sipd acs.

```
OraceSBC-# show sipd acs
```

```
22:20:15-102
```

```
SIP ACL Status
```

	Active	-- Period --		Lifetime		
		High	Total	Total	PerMax	High
Total Entries	1	1	0	2	1	2
Trusted	1	1	0	2	1	2
Blocked	0	0	0	0	0	0
Blocked NATs	0	0	0	0	0	0

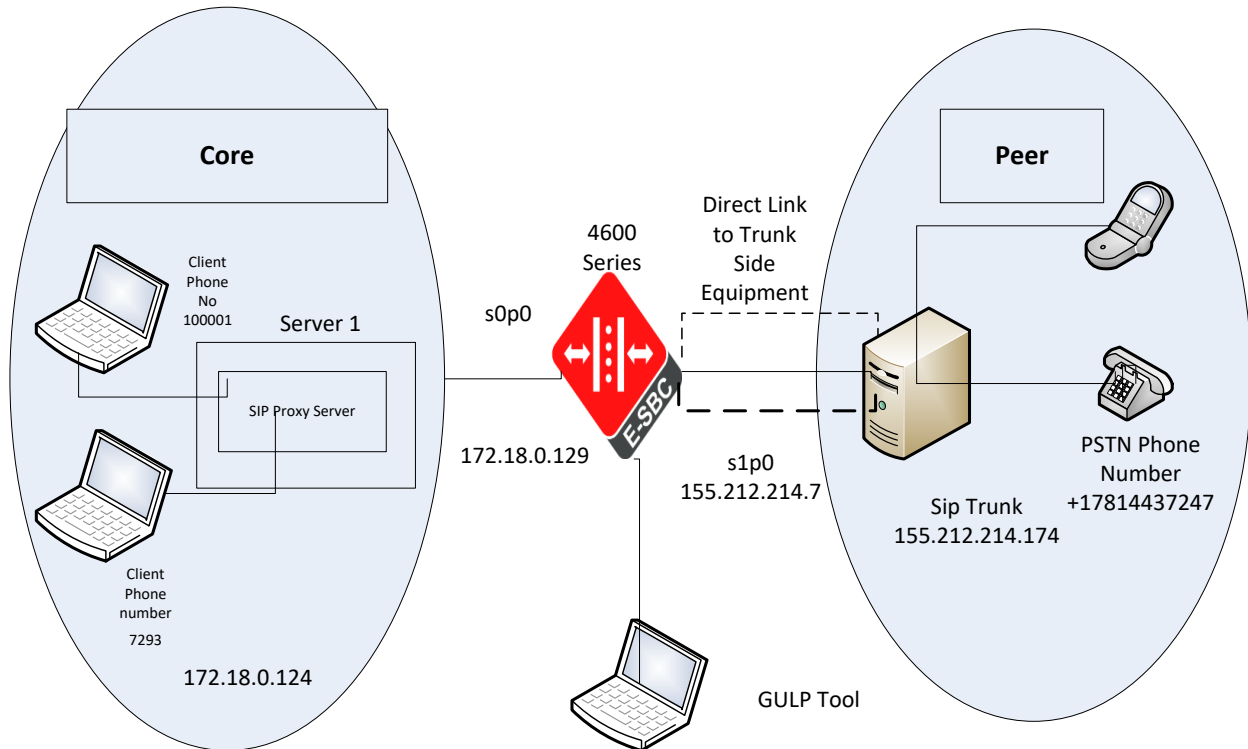
```
ACL Operations
```

	---- Lifetime ----		
	Recent	Total	PerMax
ACL Requests	0	174	2
Bad Messages	0	0	0
Promotions	0	174	2
Demotions	0	1	1
Trust->Untrust	0	1	1
Untrust->Deny	0	0	0

5 DDoS Prevention for Peering Environments

5.1 Test Environment

The test network used for SIP Peering with basic DDoS configuration is shown below.



5.2 Test Methodology

The chosen test methodology aims to determine the maximum signaling bandwidth required per platform to keep the CPU usage below 90%. Throughout the testing, parameters from the media-manager configuration object are modified to limit the amount of traffic entering the SD to a point where no more than 89% of CPU resources are consumed.

5.2.1 Maximum Signaling Bandwidth (max-signaling-bandwidth)

The maximum signaling bandwidth (max-signaling-bandwidth) is calculated per platform by sending SIP OPTIONS packets with the max-forwards header set to 0. The SD will process this packet and response with a 483 "Too Many Hops".

$$\text{max-signaling-bandwidth} = \text{OPTIONS/sec} * \text{Bytes/OPTIONS}$$

Hardware platforms utilize bytes per second and VNF platforms utilize packets per second. VNF platforms (COTS, VM, 1100) derive max-signaling from number of signaling cores. A value of 0 represents dynamic max-signaling applied which can be overwritten by customer.

Hardware platforms have a max signaling rate typically 40M for 6xxx and 10M for 4600.

5.2.2 Max and Min Untrusted Signaling Percentages (max-untrusted-signaling & min-untrusted-signaling)

In a SIP Peering environment, all of the network elements external to the Net-Net SD are known and trusted. Both “max-untrusted-signaling” and “min-untrusted-signaling” parameters are set to the smallest value allowed, which is “1”, to ensure optimal detection. These values are calculated as a percentage of max-signaling-bandwidth.

5.2.3 DDoS Attacks

DDoS attacks were generated from a PC running the Acme Packet tool GULP. GULP can be located on any untrusted IP routable to the SIP interface of the peer realm. The DDoS attack applied for this testing is a SIP INVITE flood which creates a barrage of SIP signaling to the Net-Net SD’s sip-interface IP address.

Without the application of DDoS prevention configuration, the host CPU would quickly spike to 100% in an attempt to process and respond to these rogue INVITE methods with a 403 Forbidden response.

With DDoS prevention configuration, the SD silently drops packet from these attacks at the hardware level (protecting the host CPU from overload

The following are Media Manager parameters that have platform specific defaults (not configurable).

- min-media-allocation
- min-trusted-allocation
- Deny-allocation (used only at the application level)

For this test environment ,these defaults will be used and are indicated in the platform results later by system model.

5.3 SBC Configuration for DDoS Prevention in Peering Environment

The following parameters are configured in the SBC for DDOS Prevention in peering environment

- Realm Configuration
- Sip Interface
- Session Agent and Access-Control

5.3.1 Realm Configuration

To configure DDOS settings in SBC for a particular realm ,Go to configure terminal->media-manager->realm-config and select the realm.

```
OraceSBC# con t
OraceSBC(configure)# media-manager
```



```

OraceSBC(media-manager)# realm-config
OraceSBC(realm-config)# select
identifier:
 1: Peer   s0p3:0 0.0.0.0
 2: Core   s0p0:0 0.0.0.0
 3: Genesys s0p0:0 0.0.0.0
 4: Nice   s0p3:0.4 0.0.0.0
 5: public slp0:0.4 0.0.0.0

selection: 1

OraceSBC(realm-config)# access-control-trust-level high
OraceSBC(realm-config)# done

```

The following realm-config parameters are used in the basic DDoS configuration.

Parameter	Peer Realm	Core Realm
access-control-trust-level	high	high
invalid-signal-threshold	0	0
average-rate-limit	0	0
maximum-signal-threshold	0	0
untrusted-signal-threshold	0	0

5.3.2 SIP Interface

To configure DDOS settings in SBC for a particular sip-interface ,go to configure terminal ->session-router->sip-interface and select the SIP interface.

```

OraceSBC# con t
OraceSBC (configure)# session-router
OraceSBC(session-router)# sip-interface
OraceSBC(sip-interface)# select
<RealmID>:
 1: Peer   192.168.1.94:5060
 2: Core   172.18.0.129:5060
 3: Genesys 172.18.0.255:5060
 4: Nice   192.168.1.25:5060
 5: public 141.146.36.72:5080

selection: 1
OraceSBC(sip-interface)# sip-ports
OraceSBC(sip-port)# select
<address>:
 1: 192.168.1.94:5060/UDP
 2: 192.168.1.94:5060/TCP

selection: 1

OraceSBC(sip-port)# allow-anonymous agents-only
OraceSBC(sip-port)# done

```

sip-ports parameter SHOULD be used for Peering environments. Setting "allow-anonymous" to agents-only will allow the SBC to reject requests sent by any IP which has not yet been defined as a "Session-Agent" in the SBC configuration. In Peering configurations, the customer SHOULD define each IP of a peer's device as a "session-agent" for optimal purpose.

Parameter	Peer Realm	Core Realm
allow-anonymous	agents-only	all

Although it is not recommended, but it is still possible to allow packets from an IP that has not yet defined as a Session-Agent, by setting "allow-anonymous" to "all". In this setup, the SBC will simply allow the request under DDoS threshold opposed to rejecting it with a 403 Forbidden response.

5.3.3 Session Agent and Access-Control

Any peering signaling device SHOULD be defined as a Session-Agent in SBC configuration. Further, for proper DDoS prevention, it requires explicitly configuring one access control per address of each Session-Agent address or other address (that has not yet been defined as a session-agent).

Following parameters highlighted are configured in the session agent for DDoS settings.

realm-id	peer
constraints	enabled
max-sessions	X
max-burst-rate	Y
max-sustain-rate	Z
time-to-resume	60 sec
burst-rate-window	1 sec
sustain-rate-window	30 sec

To configure DDoS setting per session agent , Go to configure terminal->session-router>session-agent

```
OraceSBC(configure)# session-router
OraceSBC(session-router)# session-agent
OraceSBC(session-agent)# select
<hostname>:
 1: 10.232.50.11 realm=Peer
 2: 10.232.50.50 realm=Peer
 3: 172.18.0.124 realm=Core
 4: 172.18.0.133 realm=Core
 5: 155.212.214.174 realm=Peer

selection: 5

OraceSBC(session-agent)# max-sessions 10
```

There is no demotion event when access-control-trust-level in the realm-config is set "high" as packets from the trusted peer endpoint are always allocated in the trusted queue for processing. It becomes a concern when there is excessive amount of SIP traffic sent by a customer which is beyond the SLA. Session constraints under session-agent can be deployed to further mitigate this problem. Listed above are a small set of constraints to provide basic level of call admission control in order to ensure that a session-agent's capacity is not exceeded, or the Net-Net SD will reject the service with 503 Exceed Constraints. Please be advised that these settings are only optional. Customers may consider them when deploying their service in a Peering environment with or without DDoS configuration.

max-sessions –X Define a maximum number of sessions (inbound and outbound) allowed by the session agent. Once the session limit is reached, the Net-Net SD will start rejecting new service with 503 Exceed Constraints until the number of seconds in time-to-resume has elapsed.

max-burst-rate –Y Define a number to set the maximum rate of call (per second) this session agent will allow. Once the rate limit is reached, the Net-Net SD will start rejecting new service with 503 Exceed Constraints until the number of seconds in time-to-resume has elapsed.

max-sustain-rate - Z In general, set this to the average call rate (per second) which that SA can sustain. Once the average rate limit calculated in (Calls made in current + previous window) / Delta (current second – start of previous window), exceeds the limit Z , the Net-Net SD will be start rejecting new service with 503 Exceed Constraints until the number of seconds in time-to-resume has elapsed.

For access control configuration, go to configure terminal->session-router->access-control

Parameter	Realm	Realm
realm-id	peer	core
source-address	n.n.n.n/[mask bit is optional] (peer SA IP, or non-SA IP)	[m.m.m.m]/ [mask bit is optional] (core SA IP or non-SA IP)
application-protocol	SIP	SIP
trust-level	high	high

In core realm, it is recommended to configure an access-control on per session-agent basis instead of putting it into a single source-subnet/mask. That will give the core session-agent its own flow versus sharing one flow for multiple devices or the entire subnet.

5.4 DDoS Configuration Settings per Platform in Peering Environments

Below are the recommended parameters settings that are derived from the above test results for each platform in a SIP Peering model. Changes under media-manager require system reboot to take effect. Be sure to follow precautions to reboot SBC(s) to unnecessary service outage during this execution.

5.4.1 Acme Packet 4600 1000000 Flow Table 16G memory - copper single GigE

Platform	AP4600
Flow Table	1000000
Memory	16GB
Software Release	SCZ 8.3.0 AND NEWER

The following table lists the five parameters germane to DDoS Configuration Settings in Peering Environments for the Acme Packet 4600 and their settings on the core and peer realms.

Parameter	Core realm-config	Peer-realm-config
access-control-trust-level	high	high
average-rate-limit	0	0
invalid-signal-threshold	0	0
maximum-signal-threshold	0	0
untrusted-signal-threshold	0	0

The media-manager configuration should be set as suggested in the following table for the Acme Packet 4600 in PBRB Model.

Parameter	PBRB Model
max-signalingbandwidth	2651610
max-untrustedsignaling	1
min-untrustedsignaling	1
tolerance-window	30

5.4.2 Acme Packet 6100 1000000 Flow Table 16G memory - copper single GigE

Platform	AP6100
Flow Table	1000000
Memory	16GB
Software Release	SCZ 8.3.0 AND NEWER

The following table lists the five parameters germane to DDoS Configuration Settings in Peering Environments for the Acme Packet 6100 and their settings on the core and peer realms.

Parameter	Core realm-config	Peer-realm-config
access-control-trust-level	high	high
average-rate-limit	0	0
invalid-signal-threshold	0	0
maximum-signal-threshold	0	0
untrusted-signal-threshold	0	0

The media-manager configuration should be set as suggested in the following table for the Acme Packet 6100 in the PBRB model.

Parameter	PBRB Model
max-signalingbandwidth	7070960
max-untrustedsignaling	1
min-untrustedsignaling	1
tolerance-window	30

5.4.3 Acme Packet 6350 2000000 Flow Table 48G memory - copper single GigE

Platform	AP6350
Flow Table	2000000
Memory	48GB
Software Release	SCZ 8.3.0 AND NEWER

The following table lists the five parameters germane to DDoS Configuration Settings in Peering Environments for the Acme Packet 6350 and their settings on the core and peer realms

Parameter	Core realm-config	Peer-realm-config
access-control-trust-level	high	high
average-rate-limit	0	0
invalid-signal-threshold	0	0
maximum-signal-threshold	0	0
untrusted-signal-threshold	0	0

The media-manager configuration should be set as suggested in the following table for the Acme Packet 6350 in the PBRB model.

Parameter	PBRB Model
max-signalingbandwidth	7070960
max-untrustedsignaling	15
min-untrustedsignaling	14
tolerance-window	30

5.4.4 Acme Packet 6300 1000000 Flow Table 16G memory - copper single GigE

Platform	AP6300
Flow Table	1000000
Memory	16GB
Software Release	SCZ 8.3.0 AND NEWER

The following table lists the five parameters germane to DDoS Configuration Settings in Peering Environments for the Acme Packet 6300 and their settings on the core and peer realms.

Parameter	Core realm-config	Peer-realm-config
access-control-trust-level	high	high
average-rate-limit	0	0
invalid-signal-threshold	0	0
maximum-signal-threshold	0	0
untrusted-signal-threshold	0	0

The media-manager configuration should be set as suggested in the following table for the Acme Packet 6100 in the PBRB model.

Parameter	PBRB Model
max-signalingbandwidth	7070960
max-untrustedsignaling	1
min-untrustedsignaling	1
tolerance-window	30

6 Appendix A

The following is a sample configuration from the lab environment in PBRB model.

```
OraceSBC# sh con sh

capture-receiver
  state          enabled
  address        172.18.0.125
  network-interface s0p0:0
access-control
  realm-id       Peer
  source-address 155.212.214.0/16
  application-protocol SIP
  trust-level    high

local-policy
  from-address   *
  to-address     *
  source-realm   Peer
  policy-attribute
    next-hop     172.18.0.124
    realm        Core
local-policy
  from-address   *
  to-address     *
  source-realm   Core
  policy-attribute
    next-hop     155.212.214.7
    realm        Peer
media-manager
  latching       disabled
  max-signaling-bandwidth 2651610
  max-untrusted-signaling 1
  min-untrusted-signaling 1
  tolerance-window 30
network-interface
  name           s0p0
  ip-address     172.18.0.129
  netmask        255.255.0.0
  gateway        172.18.0.1
  hip-ip-list    172.18.0.129
  icmp-address   172.18.0.129

network-interface
  name           s1p0
  ip-address     155.212.214.7
  netmask        255.255.255.0
  gateway        155.212.214.1
  hip-ip-list    155.212.214.7
  icmp-address   155.212.214.7
phy-interface
  name           s0p0
  operation-type Media
phy-interface
  name           s1p0
  operation-type Media
```

```

slot 1

realm-config
  identifier Core
  network-interfaces s0p0:0
  mm-in-realm enabled
  out-translationid changel
  access-control-trust-level high
  refer-call-transfer enabled
  session-recording-server NiceAir2

realm-config
  identifier Peer
  network-interfaces slp0:0.4
  access-control-trust-level low

session-agent
  hostname 172.18.0.124
  ip-address 172.18.0.124
  port 4080
  realm-id Core
  description Genesys Agent
  options refer-reinvite
  refer-call-transfer enabled
  refer-notify-provisional all

session-agent
  hostname 172.18.0.133
  ip-address 172.18.0.133
  port 8080
  realm-id Core

session-agent
  hostname 155.212.214.174
  ip-address 155.212.214.174
  port 5060
  realm-id Peer
  description Peer Agent
  options refer-reinvite
  refer-call-transfer enabled
  refer-notify-provisional all
  max-sessions [X vakuue in 5.3.3]
  max-burst-rate [Y value in 5.3.3]
  max-sustain-rate [Z value in 5.3.3]
  time-to-resume 50
  burst-rate-window 1
  sustain-rate-window 1

sip-config
  home-realm-id Core

  options max-udp-length=0
  refer-src-routing enabled

sip-interface
  realm-id Core
  sip-port
    address 172.18.0.129
    allow-anonymous all
  sip-port
    address 172.18.0.129
    transport-protocol TCP
    allow-anonymous all
  out-manipulationid ACME_NAT_TO_FROM_IP

```

```

sip-interface
  realm-id Peer
  sip-port
    address 155.212.214.7
    port 5080
    allow-anonymous agents-only

steering-pool
  ip-address 155.212.214.7
  start-port 20000
  end-port 29999
  realm-id Peer

steering-pool
  ip-address 172.18.0.129
  start-port 10000
  end-port 10999
  realm-id Core

system-config
  comm-monitor
    state enabled
    monitor-collector
      address 10.232.50.200
  default-gateway 10.138.194.129

```


7 Appendix B

7.1 DDoS-2 show commands

DDoS-2 is supported for platforms: Acme Packet 4600, Acme Packet 6100, Acme Packet 6300, Acme Packet 6350, and Acme Packet VNF platforms.

DDoS-2 increases the number of trusted endpoints to a maximum of 500K for Acme Packet 4600/6100/6300 and 750K for Acme Packet 6350. It also increases the number of denied endpoints to a maximum 96K for Acme Packet 6350 and 64K for Acme Packet 4600/6100/6300

The command show acl info provides information about present usage of the HASH table.

Static ALC's are stored in both TCAM and HASH table. The fully qualified flows are stored in HASH table and the non-fully qualified flows are stored in the TCAM table.

```
OraceSBC# show acl info
```

```
Access Control List Statistics:
```

	# of entries	% utilization	Reserved Entry Count
Denied	0	0.0%	32768
Trusted	5	0.1%	8192
Media	0	0.0%	64000
Untrusted	7	0.2%	4096
Dynamic Trusted	0	0.0%	250000

```
Total table space used = 12 of 359056 (99.99% free)
```

```
Media Entries not allocated due to ACL constraints: 0
Trusted Entries not allocated due to ACL constraints: 0
Untrusted Entries not allocated due to ACL constraints: 0
Denied Entries not allocated due to ACL constraints: 0
```

```
OraceSBC# show acl all
```

```
TRUSTED entries:
```

```
intf:vlan Source-IP/mask port/mask Destination-ask
IP/m      port/mask  prot type  index  recv  drop
0/0:0     0.0.0.0
          icmp static 105257 0      0
0/3:0     0.0.0.0
          icmp static 105258 0      0
0/2:0     0.0.0.0
          icmp static 105259 9195  0
0/0:0     0.0.0.0
          tcp  static 105261 0      0
0/0:0     0.0.0.0
          5060  udp  static 105262 219  0
```

```
UNTRUSTED entries:
```

```

intf:vlan Source-IP/mask port/mask Destination-ask
IP/m
port/mask prot type index recv drop
0/3:0 0.0.0.0 192.168.1.94
tcp static 101162 0 0
0/3:0 0.0.0.0 192.168.1.94
5060
0/0:0 0.0.0.0 172.18.0.255
udp static 101163 0 0
tcp static 101165 3158 0
0/0:0 0.0.0.0 172.18.0.255
5060
0/3:0 0.0.0.0 192.168.1.25
udp static 101166 135 0
tcp static 101168 0 0
0/3:0 0.0.0.0 192.168.1.25
5060
0/2:0 0.0.0.0 141.146.36.72
udp static 101170 0 0
Total deny entries: 0 (0 dropped)
Total media entries: 0
Total trusted entries: 5 (0 dropped)
Total untrusted entries: 7 (0 dropped)
Media Entries not allocated due to ACL constraints: 0
Trusted Entries not allocated due to ACL constraints: 0
Untrusted Entries not allocated due to ACL constraints: 0
Denied Entries not allocated due to ACL constraints: 0
Trusted Endpoints not allocated due to ACL constraints: 0

```



CONNECT WITH US

-  blogs.oracle.com/oracle
-  facebook.com/Oracle/
-  twitter.com/Oracle
-  oracle.com

Oracle Corporation, World Headquarters

500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries

Phone: +1.650.506.7000
Fax: +1.650.506.7200

Integrated Cloud Applications & Platform Services

Copyright © 2020, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0615