



ORACLE

DDOS Prevention Configuration for SIP Access 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 ACCESS 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	Maximum Signaling Threshold (max-signaling-threshold)	8
5.2.4	DDoS Attacks	8
5.3	OBSERVATIONS/LIMITATIONS	9
5.4	SBC CONFIGURATION FOR ACCESS ENVIRONMENT	10
5.4.1	Realm Configuration	10
5.4.2	SIP Interface	10
5.5	DDOS CONFIGURATION SETTINGS PER PLATFORM IN ACCESS ENVIRONMENTS	11
5.5.1	Acme Packet 4600 1000000 Flow Table 16G memory - copper single GigE	11
5.5.2	Acme Packet 6100 1000000 Flow Table 16G memory - copper single GigE	12
5.5.3	Acme Packet 6350 2000000 Flow Table 48G memory - copper single GigE	12
5.5.4	Acme Packet 6300 1000000 Flow Table 16G memory - copper single GigE	13
5.5.5	Acme Packet 3900 1600000 Flow Table 16G memory - copper single GigE	14
5.5.6	Acme Packet 1100 720 Flow Table 4G memory - copper single GigE	14
5.5.7	Acme Packet VME 720 Flow Table 4G memory - copper single GigE	15
6	APPENDIX A	16
7	APPENDIX B	19
7.1	DDOS-2 SHOW COMMANDS	19



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 Access 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 access 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, untrusted, 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 acls.

```
OraceSBC-# show sipd acls
```

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

```
SIP ACL Status
```

	-- Period --			Lifetime		
	Active	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

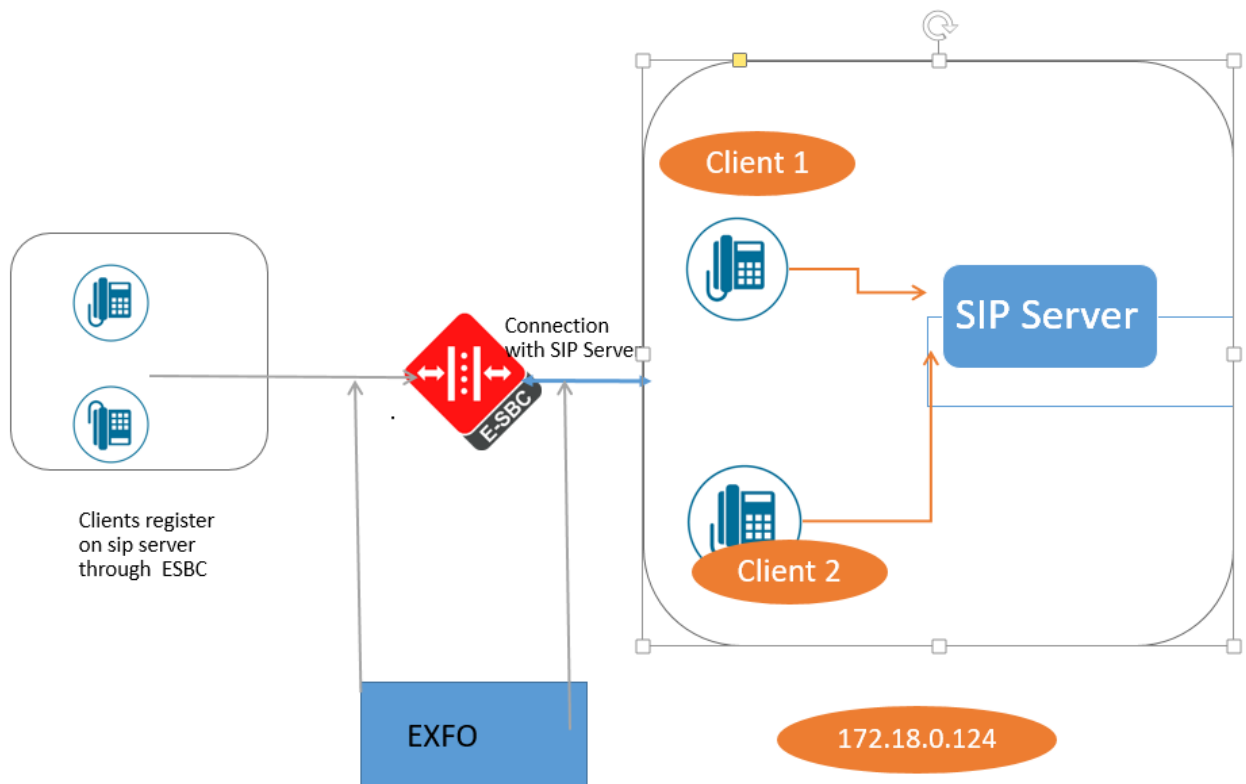
```
ACL Operations
```

	---- 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 Access Environments

5.1 Test Environment

The test network used for SIP Access with basic DDoS configuration is shown below. A third party SIP server operates as the registrar in the core network and requires authentication on all SIP Registrations.



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".

max-signaling-bandwidth = OPTIONS/sec * 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)

With the max-signaling-bandwidth parameter set to the calculated value, the max-untrusted-signaling and min-untrusted-signaling parameters in the media-manager configuration are modified until the defined background traffic and applied DDoS attack consume approximately 89% of CPU resources. For purposes of this document CPU consumption under the threshold of 89% is considered to be within an acceptable range. The max-untrusted-signaling parameter is determined first by trial and error to find the maximum setting acceptable. Following this, various min-untrusted-signaling parameter settings are exercised to verify the CPU resources consumed remain under 89%.

5.2.3 Maximum Signaling Threshold (max-signaling-threshold)

The maximum-signaling-threshold value is defined as part of the realm-configuration object and governs the number of SIP signaling messages which can be received from a given source during the period of time defined in the tolerance-window (30 second default window). Once a trusted source exceeds this threshold it will be demoted to the untrusted queue. Provisioning this provides further protection to the Session Director by allowing it to remove a violating endpoint from the trusted queue, effectively preserving the integrity of that queue for non-violating trusted sources.

Due to the nature of this setting, it is recommended each network administrator define a value based on network usage. In absence of customized network analysis, it is recommended a value no less than 4000 be used along with a defined tolerance-window of 30 seconds. As defined, a value of 4,000 was chosen with the intention that it not affect those trusted users who are behaving properly or otherwise as expected under normal circumstances. In the event of either endpoint malfunction or malicious attack, this value will easily be exceeded resulting in demotion to the offending source

5.2.4 DDoS Attacks

The baseline of trusted traffic consists of SIP Registrations and calls and produces a total SD CPU Utilization of 55% for all tests. To create this traffic, the EXFO protocol simulation tool registers a group of access endpoints with unique IP addresses to the SD and another group of core endpoints directly to the Registrar in the core network. Calls are then initiated from the access endpoints to the core endpoints

DDoS attacks were generated from a PC running the Acme Packet tool GULP. GULP is located on the direct subnet of the SIP interface of the access realm. The DDoS attack applied for this testing is a SIP Register flood which creates a flood from approximately 1000 untrusted endpoints at line rate.

5.3 Observations/Limitations

The settings outlined in this appendix are beneficial when facing malicious or nonmalicious flood attacks, such as a REGISTER avalanche following a network outage. By limiting the amount of untrusted traffic to the SBC, the registration rate allowed will be throttled and the SBC will not be overrun by the high rate of registrations. However, there is an opportunity cost between the level of protection against a DDoS flood attack and the convergence time for this type of avalanche condition. For example, raising the percentage of untrusted bandwidth allowed will inevitably allow more untrusted traffic to traverse the SBC, and minimize the convergence time. The opportunity cost here is higher CPU usage during the flood, a result of higher demand on the processor due to the increased level of registrations it's required to process. Additionally, when set as an option in the sip-configuration, reg-overload-protect requires the SBC temporarily promote a registering endpoint upon receipt of a 401/407 response from the "real" registrar. This temporary promotion is in advance of the real and final promotion, which takes place following the 200 OK response to a REGISTER request containing authentication credentials. During a registration avalanche from untrusted sources, temporary promotion based on the initial REGISTER request sent from a specific source helps minimize the amount of time it will take to promote the collective untrusted sources, to trusted sources, effectively restoring service in the event of an outage as quickly as possible. This is also referred to as: minimizing the convergence time. The addition of any SIP option relevant to DDoS, including reg-overload-protect, would require additional testing. For customers with specific convergence requirements, additional research must be conducted to arrive at an appropriate DDoS configuration for deployment.

A limitation of the configuration parameters described in this appendix is the handling of SIP message spoofing. When a trusted user is "spoofed" by another user or a defective trusted user sends many SIP messages, the CPU utilization of the SBC may spike to 100%. One safe-guard implemented as part of this appendix is the establishment of a setting for maximum-signaling-threshold, defined in the realmconfiguration object. When set, this provides an entry level amount of protection by removing a violating source from the trusted queue once the defined threshold is exceeded. To further handle this scenario, there are additional advanced DDoS configurations that can be set. For example: if the desired outcome is to deny violating sources from the hardware level, the access-control-trust-level should be set to low in the realm-configuration object. This also requires the configuration of the untrustedsignal-threshold to properly demote offending untrusted users to the deny list. If one wishes to move an endpoint back into the untrusted queue the access-control-trustlevel of "medium" should be used. The DDoS configuration recommendations in this appendix are meant as a general baseline to help protect the SBC from DDoS. For more complete protection, DDoS configurations should be determined by the examining the applicable environment and customizing based on the environment driven traffic flows and load levels.

5.4 SBC configuration for Access Environment

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

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

5.4.1 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: Access 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: 3

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

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

Parameter	Access Realm	Core Realm
access-control-trust-level	low	high
invalid-signal-threshold	1	0
average-rate-limit	0	0
maximum-signal-threshold	4000	0
untrusted-signal-threshold	1	0

The maximum-signal-threshold of 4000 is very high so as not to impact service. It should be reduced to a number close to the maximum number of signaling messages from one client within the tolerance-window on the realm, which by default is 30 seconds. Base the threshold on an actual trace to account for the extraneous messages that are normally not considered, and make sure to account for network loss and/or renegotiations.

5.4.2 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: Access 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: 172.18.0.255:5060/UDP
2: 172.18.0.255:5060/TCP

selection: 1

OraceSBC(sip-port)# registered
OraceSBC(sip-port)# done

```

Parameter	Access Realm	Core Realm
allow-anonymous	registered	all

5.5 DDoS Configuration Settings per Platform in Access Environments

Below are the recommended parameters settings that are derived from the above test results for each platform in a SIP Access 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.

5.5.1 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 Access Environments for the Acme Packet 4600 and their settings on the access realm based on whether endpoints can be denied or not.

Parameter	No Denied	Denied
access-control-trust-level	medium	low
invalid-signal-threshold	2	1
maximum-signal-threshold	25	25
untrusted-signal-threshold	10	2
Nat-trust-threshold	0	0
Deny-period	30	1800

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-signaling-bandwidth	2651610
max-untrustedsignaling	15
min-untrustedsignaling	12
app-signaling-bandwidth	0
tolerance-window	30

5.5.2 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 Access Environments for the Acme Packet 6100 and their settings on the core and access realms.

Parameter	Core realm-config	Access-realm-config
access-control-trust-level	high	low
average-rate-limit	0	0
invalid-signal-threshold	0	1
maximum-signal-threshold	0	4000
untrusted-signal-threshold	0	1

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-signaling-bandwidth	7070960
max-untrustedsignaling	1
min-untrustedsignaling	1
tolerance-window	30

5.5.3 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 Access Environments for the Acme Packet 6100 and their settings on the core and access realms.

Parameter	Core realm-config	Access-realm-config
access-control-trust-level	high	low
average-rate-limit	0	0
invalid-signal-threshold	0	1
maximum-signal-threshold	0	4000
untrusted-signal-threshold	0	2

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-signaling-bandwidth	7070960
max-untrustedsignaling	15
min-untrustedsignaling	14
tolerance-window	30

5.5.4 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 Access Environments for the Acme Packet 6300 and their settings on the core and access realms.

Parameter	Core realm-config	Access-realm-config
access-control-trust-level	high	low
average-rate-limit	0	0
invalid-signal-threshold	0	1
maximum-signal-threshold	0	4000
untrusted-signal-threshold	0	1

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-signaling-bandwidth	7070960
max-untrustedsignaling	1
min-untrustedsignaling	1
tolerance-window	30

5.5.5 Acme Packet 3900 160000 Flow Table 16G memory - copper single GigE

Platform	AP3900
Flow Table	160000
Memory	16GB
Software Release	SCZ 8.3.0 AND NEWER

The following table lists the five parameters germane to DDoS Configuration Settings in Access Environments for the Acme Packet 3900 and their settings on the access realm based on whether endpoints can be denied or not.

Parameter	No Denied	Denied
access-control-trust-level	medium	low
invalid-signal-threshold	2	1
maximum-signal-threshold	25	25
untrusted-signal-threshold	10	1
Nat-trust-threshold	0	0
Deny-period	30	1800

The media-manager configuration should be set as suggested in the following table for the Acme Packet 3900 in PBRB Model.

Parameter	PBRB Model
max-signaling-packets	40000
max-untrusted-signaling	7
min-untrusted-signaling	7
tolerance-window	30

5.5.6 Acme Packet 1100 720 Flow Table 4G memory - copper single GigE

Platform	AP3900
Flow Table	720
Memory	4GB
Software Release	SCZ 8.3.0 and newer

The following table lists the five parameters germane to DDoS Configuration Settings in Access Environments for the Acme Packet 1100 and their settings on the access realm based on whether endpoints can be denied or not.

Parameter	No Denied	Denied
access-control-trust-level	medium	low
invalid-signal-threshold	2	1
maximum-signal-threshold	25	25
untrusted-signal-threshold	10	1
Nat-trust-threshold	0	0
Deny-period	30	1800

The media-manager configuration should be set as suggested in the following table for the Acme Packet 1100 in PBRB Model.

Parameter	PBRB Model
max-signaling-packets	10000
max-untrustedsignaling	7
min-untrustedsignaling	4
tolerance-window	30

5.5.7 Acme Packet VME 720 Flow Table 4G memory - copper single GigE

Platform	VME
Flow Table	720
Memory	4GB
Software Release	SCZ 8.3.0 and newer

The following table lists the five parameters germane to DDoS Configuration Settings in Access Environments for the Acme Packet VME and their settings on the access realm based on whether endpoints can be denied or not.

Parameter	No Denied	Denied
access-control-trust-level	medium	low
invalid-signal-threshold	2	1
maximum-signal-threshold	25	25
untrusted-signal-threshold	10	1
Nat-trust-threshold	0	0
Deny-period	30	1800

The media-manager configuration should be set as suggested in the following table for the Acme Packet 1100 in PBRB Model.

Parameter	PBRB Model
max-signaling-packets	100000
max-untrustedsignaling	7
min-untrustedsignaling	4
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

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 15
  min-untrusted-signaling 12
  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                          Access
  network-interfaces                  s0p0:1
  mm-in-realm                         enabled
  out-translationid                   changel
  access-control-trust-level          medium
  refer-call-transfer                 enabled
  session-recording-server            NiceAir

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

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                            Access
  sip-port
    address                           172.18.0.255
    allow-anonymous                    registered
  sip-port
    address                           172.18.0.255
    transport-protocol                 TCP
    allow-anonymous                    registered
  out-manipulationid                  ACME_NAT_TO_FROM_IP

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	4	0.0%	32768
Trusted	5	0.1%	8192
Media	0	0.0%	64000
Untrusted	7	0.2%	4096
Dynamic Trusted	2	0.0%	250000

```
-----  
Total table space used = 18 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
```

```
DENIED 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          172.18.0.255  
      1-1023      tcp  static  113451  
0/3:0      0.0.0.0          192.168.1.25  
      1-1023      tcp  static  113452  
0/3:0      0.0.0.0          192.168.1.94  
      1-1023      tcp  static  113455  
0/0:0      0.0.0.0          172.18.0.129
```

```
      1-1023      tcp  static  113456  
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                                     172.18.0.129
          icmp static 105257 0      0
0/3:0      0.0.0.0                                     192.168.1.94
          icmp static 105258 0      0
0/2:0      0.0.0.0                                     141.146.36.106
          icmp static 105259 9195   0
0/0:0      0.0.0.0                                     172.18.0.129
          tcp  static 105261 0      0
0/0:0      0.0.0.0                                     172.18.0.129
          5060      udp  static 105262 219   0
UNTRUSTED entries:
intf:vlan Source-IP/mask                    port/mask Destination-
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      udp  static 101163 0      0
0/0:0      0.0.0.0                                     172.18.0.255
          tcp  static 101165 3158  0
0/0:0      0.0.0.0                                     172.18.0.255
          5060      udp  static 101166 135   0
0/3:0      0.0.0.0                                     192.168.1.25
          tcp  static 101168 0      0
0/3:0      0.0.0.0                                     192.168.1.25
          5060      udp  static 101169 0      0
0/2:0      0.0.0.0                                     141.146.36.72
          5080      udp  static 101170 0      0
Total deny entries:      4 (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