ORACLE DATA SHEET

DDOS PREVENTION CONFIGURATION SERVICE

ORACLE
COMMUNICATIONS CONSULTING

Evaluating the customer's vulnerability to denial of service (DoS) and distributed denial of service (DDoS) attacks, Oracle offers advanced security features that provide unparalleled protection against DDoS attacks.

SERVICE FEATURES

- Receive a consultative evaluation of vulnerability to DoS and DDoS attacks
- Develop a security strategy
- Develop implementation plans
- Develop active monitoring procedures
- Fully defend IP borders with Oracle's security framework

AREAS OF RECOMMENDATION

- Best current practices adherence
- Errata
- Performance
- Scalability
- Manageability
- Security

Overview

The DDoS Prevention Configuration Service is an evaluation of the customer's vulnerability to denial of service (DoS) and distributed denial of service (DDoS) attacks. Oracle offers advanced security features that provide unparalleled protection against DDoS attacks. Using the Oracle security framework to the fullest capacity will enable customers to fully defend their IP borders. The DDoS Prevention Configuration Service will help customers develop a security strategy, implementation plans and active monitoring procedures using session-aware filtering and enforcement capabilities.

Prerequisites

A customer or reseller that owns an Oracle Communications Session Border Controller (SBC) that was purchased directly from Oracle or from an authorized reseller, and is under warranty or a current maintenance service agreement. A customer that purchases the DDoS Prevention Configuration Service will provide the requested configuration information.

Features and Key Deliverables

Oracle's security framework is highly flexible and is most efficient when engineered to meet the exact demands and requirements of a specific deployment. The DDoS Prevention Configuration Service will perform the necessary analysis and modeling of an SBC deployment, taking into consideration the various threats a deployment faces today, and will provide a set of configurations that have been tested and proven to combat these threats.

ORACLE

- **Requirements and Data Gathering Phase.** To design a highly tuned set of DDoS prevention configurations for a specific customer deployment, Oracle will conduct a comprehensive requirements gathering effort to determine all the inputs necessary for the DDoS prevention design.

  In addition, requirements gathered will also be used as inputs for a test environment built at Oracle facilities for simulation and testing. In addition to the hardware and software configuration information gathered, Oracle will also obtain operational data such as signaling and media flows from log files, external network traces, CPU utilization rates, packet processing rates, busy hour call attempts, call hold times and third-party device behavior/capabilities.

- **Design Phase.** The DDoS Prevention Configuration Service design varies dependent on the current mode of operation of the SBC. At the core of the security architecture is a concept of queues. In this architecture, signaling traffic from a unique endpoint, until proven to be trustworthy via application-layer VoIP protocol criteria (e.g. successful SIP registration), is treated as untrusted and placed in a bandwidth-restricted "untrusted" queue for processing. Once promoted to "trusted", the endpoint's signaling traffic is processed in the trusted queue with guaranteed bandwidth. Additionally, there is an optional deny list where misbehaving endpoints are placed for a period of time such that all signaling from this endpoint is silently discarded.

  The configured size of the untrusted and trusted queues is highly dependent on the customer's network requirements. A sizable untrusted queue can allow a timely recovery from an event such as a complete softswitch outage by allowing larger numbers of endpoints to re-register. However, a large untrusted queue can also strain the host CPU under a malicious attack. Oracle will recommend the proper queue sizes that will achieve a balance between the recovery needs and bandwidth protection. The level of trust is configurable on the SBC on a per-realm basis. As part of this service, Oracle will provide queue design recommendations, and recommends the use of the three queues listed below.

  - **Low** – Endpoints are treated as untrusted initially, can be promoted to trusted and demoted to the deny list. This is useful for second-line residential VoIP offerings where the access networks cannot be secured. Convert the Microsoft Word document to Adobe PDF.
  - **Medium** – Endpoints are treated as untrusted initially, can be promoted to trusted and demoted back to untrusted, but never demoted to the deny list. This is useful for enterprise access VoIP offerings where service should never be denied.
  - **High** – Endpoints are always treated as trusted. This is useful for service provider core devices e.g. softswitches.

  For example, in the case of a SIP trunking/peering/interconnect model where third-party devices are known, trusted and statically configured, a series of Access Control Lists (ACLs) is sufficient to permit known third-party devices and block all traffic from unknown sources. This will address most malicious attacks in a SIP trunking model.

  Addressing IP-address spoofing attacks, which appear to be sourced from trusted resources, dynamic ACLs triggered by application-layer thresholds and session constraints (limits on signaling behaviors e.g. burst rate) should be used. The constraints and triggers are highly tuned to the behavior and capabilities of the PBXs/SBCs that interwork with the SBC.

The endpoints in the untrusted access networks (e.g. residential VoIP) are not known to the SBC in advance via configuration, but rather dynamically register for service at initial boot up, (and then in advance of the registration expiration period). Typically these endpoints can number in the thousands. This creates a much more dynamic environment to which the SBC must react in overload or attack situations. The queues and promotion/ demotion/deny trigger criteria must be highly tuned to the behavior of the endpoints and the capabilities of the trusted network devices.

Using the data gathered in the data collection phase, Oracle will design a suite of configuration settings to protect both the SBC and the service as a whole using the capabilities described above. The initial design will be presented to the customer and approved by the customer prior to proceeding to the test phase.

Oracle reserves the right to recommend software versions of a newer vintage than the customer currently has in production should newer functionality or software corrections provide a more optimal solution. It is outside of the scope of this activity to design and implement any configuration changes that do not pertain to DDoS prevention.

- **Test Phase.** Oracle will conduct a thorough test effort on the proposed design. Using inputs from the data-gathering phase, Oracle will simulate the customer's SBC deployment and will run through a suite of test cases that best match the customer's application. The testing will simulate the volume of traffic the customer typically experiences, then layer on a number of overload conditions, both malicious and non-malicious. The output of this phase is a test report showing the behavior of key performance indicators (KPIs), such as CPU and memory utilization, during each attack. If the testing reveals inadequacies in the proposed design, Oracle will return to the design stage and alter the configuration settings as necessary.
- **Delivery Phase**. Oracle will present the final design and test results to the customer via conference call. All deliverable documents will be made available to the customer five business days before the conference call for customer review.
- **Acceptance Phase.** Upon successful delivery phase, it is the customer's responsibility to return the signed Acceptance Form as forwarded by Oracle.

If testing reveals an issue that requires a software correction, Oracle will take responsibility for raising an issue on behalf of the customer and ensure that the issue is driven to completion. Upon availability of corrected software, Oracle will re-run the test phase. If preferred, and the necessary DDoS tools and call generators are available, the testing phase can take place at either customer or partner test facilities.

Customer Responsibilities

- The customer will provide all necessary configurations and interconnect information to Oracle.
- The customer will identify a technical contact that will participate in the information gathering call, will be the point of contact for all information requests or technical questions and will provide signoff for completed work.

Ordering

This service must be ordered by the customer or a reseller directly from Oracle.

Assumptions

- Service cannot begin prior to receipt of a valid order from the customer and before acceptance of the order by Oracle
- Customer will be able and willing to provide requested information
- Customer will make Oracle aware if a government security clearance is required by the Oracle Communications Consulting team prior to sending any information to Oracle
- Service start and completion date will be mutually agreed upon by Oracle and the customer

CONTACT US

For more information about the DDoS Prevention Configuration Service, visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

CONNECT WITH US

B blogs.oracle.com/oracle

f facebook.com/oracle

twitter.com/oracle

oracle.com

Integrated Cloud Applications & Platform Services

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.