OX Dovecot Anti-Abuse Shield

DATASHEET

Protect your business: Dovecot Anti-Abuse Shield

Abuse protection meets Webmail
Most ISPs and Mail Providers have protection in place for SMTP abuse, but very few have the same protection for WebMail, POP and IMAP. Dovecot Anti-Abuse Shield solves this problem by providing a single system for handling abuse. It integrates with both OX App Suite and Dovecot Pro to protect against login and authentication abuse, brute force attacks and also to enforce common authentication and authorization policies across the platform.

Customization is the key
The anti-abuse daemon ships with default policies to protect against brute force attacks. For even more sophisticated protection, Open-Xchange can provide customized Lua scripts that handle a wide variety of abuse scenarios as well as implementing customer-specific features and policies.

Comprehensive feature set
Anti-Abuse Shield features include DNS lookup, native GeoIP support, ratelimiting and tarpitting, a flexible in-memory statistics database to provide abuse statistics and integration with customer authentication/authorization systems using the open HTTP REST API.

Security is embedded in all OX Products

OX App Suite

- Integration with Dovecot Anti-Abuse Shield
- OX Guard for secure end-to-end email encryption
- Defensive programming against OWASP Top Ten and other vulnerabilities

Dovecot Pro

- Anti-Abuse Shield to detect brute-force, account compromise and enforce policies
- Optional at-rest encryption of end-user mailbox data

PowerDNS Pro

- Powerful Anti-DDoS Protection
- Parental Controls
- RPZ integration for DNS Firewall functionality
- DNSSEC Hosting and Validation

Regular static Code Analysis to improve code quality and security

16116-2

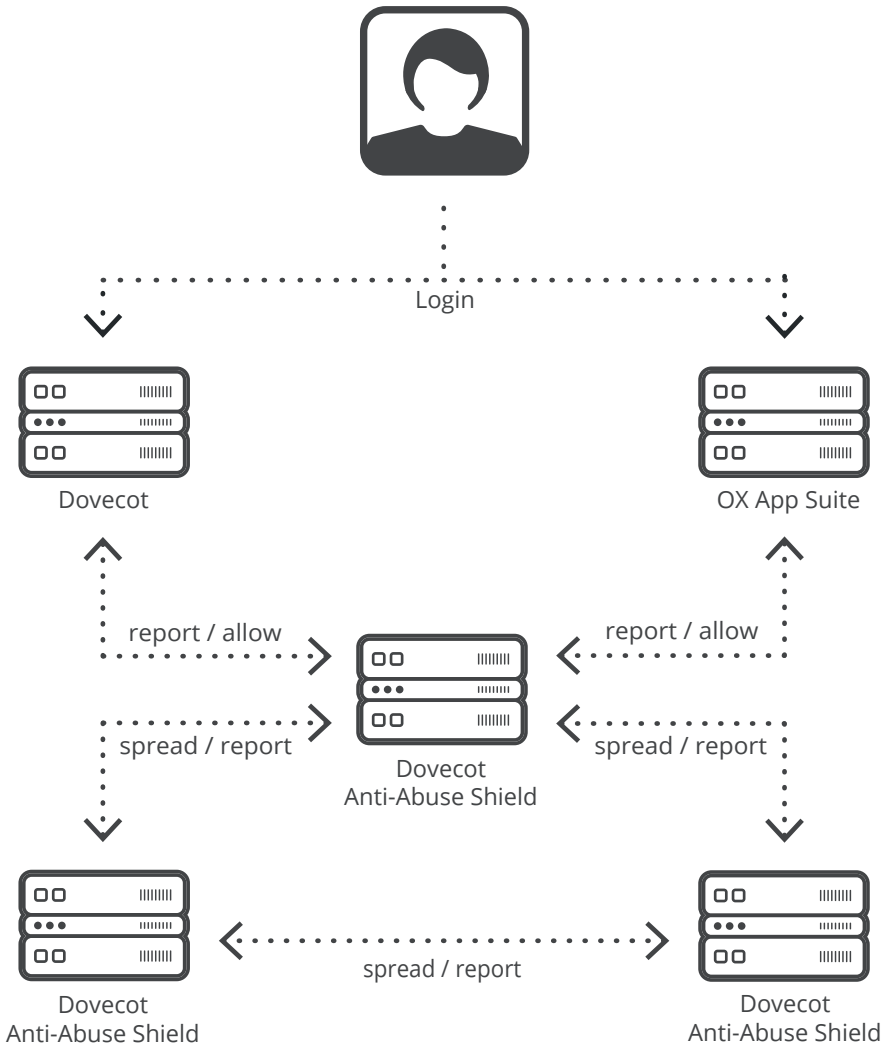
The Magic behind the Security

Clustering
Dovecot Anti-Abuse Shield can be configured to run in a clustered environment, with multiple servers sharing data to achieve an unified view of abusive behavior. Clustering uses the UDP protocol and all information is encrypted over the wire using symmetric encryption and a shared secret between all servers.

Clustering is achieved by configuring each Anti-Abuse Shield server to replicate the in-memory DB to a configured set of servers. Typically, those other servers would be configured to also replicate their DB to the same set of servers, thus creating a "mesh". In this way, Dovecot Anti-Abuse Shield can be configured to create a highly available cluster, where all servers in the cluster have all the information about abuse, and can thus be accessed in the same way by clients (the diagram below visualizes this approach).

Alternative clustering arrangements can be configured, for example creating a set of "report-only" servers, which receive reports from clients and "spread" those reports to a set of "allow-only" servers, which contain all the abuse statistics and are queried by clients to decide whether to allow or refuse logins.

How Dovecot Anti-Abuse Shield works



Anti-Abuse Shield at a glance:

Replicated/Clustered Architecture
Login reports are shared between all the servers in the cluster so there is a single view of abuse.

Scriptable Policy Language
Using the Lua language, the functionality of the daemon can be extended to record and protect against a large variety of abusive behavior.

DNS Lookup
For looking up IP addresses and domains in blacklists.

GeoIP Lookup
GeoIP lookups can be made and incorporated into policy decisions.

Ratelimiting and Tarpitting
Both can be enabled and enforced based on IP address, login name, GeoIP location, time windows, etc.

Flexible In-Memory Statistics Database
A versatile and extensible in-memory database is used to store statistic information about abuse over time periods from a few minutes to many hours.

Integration with Customer Authentication/Authorization Systems
Customers can use the open HTTP REST API to benefit from the protection of the anti-abuse daemon in their own authentication and authorization systems.

Admin Console
The admin console can be used for introspection, debugging and retrieving statistical information.

Persistent Replicated Blacklist
Configurable via a REST API or the Lua policy engine, supports auto-expiry of entries, replication between all cluster nodes, and optionally uses a Redis DB for persistence.

Webhooks
Integrate Anti-Abuse Shield with other systems using webhooks to send events.

www.open-xchange.com | info@open-xchange.com

Stay Open. OX®