How to Set Up a Training Environment

https://campus.barracuda.com/doc/48202812/

Create a separate mail account for testing. If you use a real mail account, it will be classified as one that sends spam. The training mailboxes must be configured on the mail server and not on the Barracuda NextGen Firewall F-Series. The training mail server must be capable of IMAP.

On an external mail server, set up a training environment where misclassified mail can be filed. You must also configure a script to collect the mail from this training environment.

There must be connectivity between the IMAP server and the Barracuda NextGen Firewall F-Series. To test connectivity, enter the following at the command line:

- `telnet IMAPServer imap2` (tests the connection itself)
- `A001 CAPABILITY`
- `A002 LOGIN` *username pwd* (verifies the user and password)

Setting up the Environment

The training environment consists of an IMAP mail server and email clients, which can directly access the mail server's folder structure (like Microsoft Outlook, Mozilla, Evolution, etc). On the mail server, create the following mailboxes:

- SPAM – Contains spam that was delivered and not tagged.
- HAM – Contains mail that was incorrectly tagged as spam.
- FORGET – Contains mail that should not be tagged as spam or ham.

Users of the training mail server can sort misclassified into these mailboxes. SpamAssassin regularly collects and processes the mail from these mailboxes to improve its filter mechanisms. Depending on how accurately users can sort misclassified mail, you can set up these mailboxes either for all mail server users or for each mail user separately.

Environment for UNRELIABLE Users

For unreliable users, set up an environment where all users file misclassified mail into a shared HAM-SPAM-FORGET folder structure, which is detached from the training environment. The mail server administrator verifies that emails have been correctly sorted before moving them to the training environment. This approach may be provide additional work for the administrator but can help prevent the spam filter from learning incorrect mail classification.

Environment for RELIABLE Users

For reliable users, set up an environment where all users have access to the training environment on the mail server and file misclassified mail into the corresponding mailboxes.

> To maintain privacy on this "public" file structure, you may configure user access rights so that users can only see their own emails.

Each user has the HAM-SPAM-FORGET folder structure and sorts misclassified mail into these folders.

Configuring a Script for Email Collection

You must configure a script to collect emails from the training environment.

Example Script

For example, you can use a script that is similar to the following:

```
#!/bin/bash # assumptions: # HAM and SPAM live under /home/$USER/mail/ # TARGETDIR should not be /tmp/, but a more secure location # no filelocking, etc # 2003-12-18 j.radinger@barracudanetworks.com TARGETDIR=/tmp/ SPAM=`find /home/*/mail/ -type f -name SPAM` HAM=`find /home/*/mail/ -type f -name HAM` for a in SPAM HAM; do if [ -f $TARGETDIR/$a ]; then rm -f $TARGETDIR/$a fi done for a in $SPAM; do cat $a >> $TARGETDIR/SPAM done for a in $HAM; do cat $a >> $TARGETDIR/HAM done
```

Configuring a Training Environment on a German MS Exchange Server

If your training environment is configured on a German Microsoft Exchange Server, specify the paths to the mailboxes as follows:

- Mailbox **SPAM**:&ANY-ffentliche Ordner/spamassassin/SPAM
- Mailbox **HAM**:&ANY-ffentliche Ordner/spamassassin/HAM
- Mailbox **FORGET**:&ANY-ffentliche Ordner/spamassassin/FORGET

After setting up the training environment, configure the training settings on the Barracuda NextGen Firewall F-Series. Continue with How to Improve Spam Filtering.

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.