VIPRE Email Security
Server Edition

Best Practices Guide

Document Version: VESS-BPG-10.3.1

Last updated: Last updated: Friday, September 3, 2021

Contents

1 Introduction

The guide that follows is a collection of the best installation and configuration practices compiled by VIPRE Security for use with the VIPRE Email Security - Server Edition software. This guide is in no way meant to be all-inclusive to every installation environment, but is meant to serve as a general overview of our best suggestions for deployment, configuration and use of VIPRE within the scope of our customers' unique and diverse IT environments.

1.1 What does this guide cover?

The purpose of this document is to aid you in the use and installation of VIPRE, and help you understand the best practices recommended by VIPRE's Support and Development groups. Throughout this guide, you will find generalized best practices to improve the security of your enterprise, the level of impact our software places on your system, and the way to get the maximum output from your purchase.

This guide is divided into five sections:

- Environmental Setup
- Installation
- Configuration
- Antispam/Antivirus Setup
- General Usage

It will begin by recommending changes you can make to your environment to aid in the installation of VIPRE. Then, we'll dive into the installation and setup of the software, and conclude with some strongly recommended operating practices. By the end of this document, you should be very familiar with VIPRE and feel comfortable using it in your infrastructure.

> We assume that you're familiar with administrative concepts, such as port forwarding, Exchange Administration, Windows Administration, and application-level firewall configuration.

2 Environmental Setup

The method in which you install and utilize VIPRE is highly dependent on two factors:

- The version of Exchange in use
- The number of servers in the environment

Thus, in this area of our guide, we're going to discuss how to tailor your VIPRE installation based around your messaging platform and the amount of computers associated with it.

2.1 Exchange roles

Within Exchange, there are five roles, two of which VIPRE installs upon. These roles are the:

- **Edge Transport – (VIPRE)**
- **Hub Transport – (VIPRE)**
- Mailbox Server
- Client Access Server
- Unified Messaging Server

For the sake of completeness, we'll briefly explain the roles VIPRE installs upon and how this will affect your messaging infrastructure.

Edge Transport: This is a separate box that sits on the edge of the network (between the internet and any other servers in the network) and does pre-filtering. VIPRE performs connection filtering on this role.

Transport Hub: This role handles the flow of messages and routes them to the right mailbox. Connection filtering will be performed on this role only if an Edge server is not in use. Antispam, Antivirus, Attachment filtering, and Disclaimers work on this role.

The reason this is important to know is because Exchange does not necessarily contain "clusters," but it certainly supports multiple servers to distribute load. What this means for you as an administrator is that the installation of VIPRE will depend on whether or not you have a single server or multiple server installation.

Single Server Instructions

With a single server installation, all Exchange roles are consolidated into one area, making the installation of Exchange much easier. In this case, you can install VIPRE normally, without any special considerations.

Multiple Server Installation

The installation of VIPRE with multiple servers is a fairly straight forward process, but it does require you to understand the Exchange roles and to know which portions of VIPRE you should install upon your servers, depending on which role they're functioning as within your environment. The instructions for each depend upon whether the server is running the Edge or Hub roles.

Edge Transport instructions

On the edge transport, VIPRE performs connection filtering and anti-spoofing. When you install VIPRE on your edge transport, you need to make sure these are enabled.

Hub Transport instructions

On the hub transport, VIPRE performs attachment filtering, anti-spam, antivirus, and disclaimers. Connection filtering is also performed if there is no edge role. To make sure these are all setup correctly, you need to make sure these are enabled.

3 Installation

This area of the best practices guide will familiarize you with the best practices involved with installing VIPRE. Keep in mind, this is not a substitute for the full version of the VIPRE Email Security - Server Edition User Guide.

> VIPRE must be installed on an Exchange server. A member server or workstation will only allow the quarantine and report viewers to install.

You may begin the installation by following the User's Guide and ensuring you follow the general guidelines we discuss below.

3.1 Databases and backup scripts

VIPRE installs an Access Database and it is *strongly recommended* that you implement an SQL Server 2005 or above database. Similarly, you should also follow the backup scripts and 3rd party installation recommendations (if applicable). Failure to this can result in unexpected behavior and possible server crashes.

Additionally, we need to do a few special checks:

Test Outlook Web Services

In order to install VIPRE in an Exchange environment and have these roles work properly with VIPRE, you should complete the following steps:

a) On the Exchange Hub Transport server, run the following command from the Exchange Management Shell:

```
Test-OutlookWebServices | FL
```

> **If there are ANY errors or warnings, run the command again**. If there are still errors or warnings, fix them before proceeding. VIPRE will not filter spam if this test fails.

Create a Service Account

You will need to create a new user account for the VIPRE Plug-in Manager service to use. It must only be a member of the Domain Users built in group and nothing else! It does not need a mailbox or any additional rights. All rights will be assigned by the install utility. However, be sure to set the password to never expire.

Test Impersonation

On Exchange, we need to make sure that the PIMsvc account can impersonate. To do this, you can follow these instructions:

1. In the address bar, type in the path to your server's outlook web access site. It will normally look like this:

   `localhost/owa/user@domain.com`

2. This will bring you to the OWA login page. Here you will log in with the PIM Service account credentials you created, which should look like this:

   User Name: domain\PIMSVCACCOUNT
   Password: *******

3. Once in, if you can access and modify another user's account with the same credentials, then impersonation will work and your server will function properly. If you cannot, then you should contact VIPRE Security Support:

◆ Open a case online - https://businesssupport.vipre.com/support/tickets/new
   or
◆ Call +877-757-4094

4 VIPRE Configuration

This area of the best practices guide will familiarize you with the VIPRE Security configuration recommendations for VIPRE.

4.1 Domain Settings

VIPRE integrates directly with the active directory domain to retrieve information from your Exchange server. Accordingly, in the "Domains" tab, you can place your active directory domain information. Note that this should not be your email domain. VIPRE will retrieve your recipient email domains from Exchange.

4.2 Setup Antispoofing

VIPRE anti-spoofing prevents spoofed messages from being marked as internal and then bypassing the Antispam plug-in. The fact that an "X-Ninja-Antispam:" header is present tells us that either the message was external and was flagged as spoofed. A reason a spoofed message would make it to the inbox is because this email address is either in the users allowed senders or contact list. One way to prevent this would be to remove that email address from the offending list. The second way is to enable anti-spoofing. This section concentrates on this method.

> VIPRE does not consider all email addresses from your email domain as internal. Only addresses that belong to an exchange mailbox or are a contact in active directory are considered internal. If you have a printer or similar device that send notification emails from a non AD address, a Global allowed senders rule should be configured for this address to prevent the following rule from catching emails from it.

Enable Antispoofing:

1. Open the VIPRE Management Console.
2. Navigate to **Settings**>**Domains**>**Antispoofing**.
3. Check **Enable Antispoofing**.
4. Add the IP address of all mail sending devices to this list.

> If you have an Edge Role Server, do not add its IP to the list.

Enable Antispoofing on the Antispam Policy:

1. Expand **Policies & Recipients**.
2. Expand **Antispam**.
3. Select **Default Antispam Policy**.
4. Choose the **Policy Settings** tab.
5. Ensure that the **Spoofing** area on the bottom of the policy settings is set to **Quarantine them**.

4.3 Register Agents

When you've first installed VIPRE, you will want to make sure that the transport agents have been registered. Agent Registration will appear in the VIPRE console like what you see below.
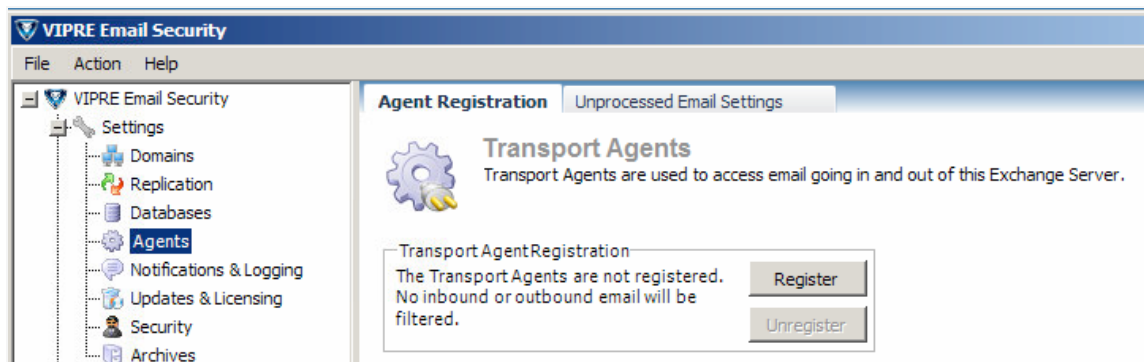
4.4 Ensure product is registering

You should make sure that your product is properly registering. You should follow these steps to ensure your license is registered and properly functioning.

1. Open the VIPRE Console.
2. Select the **Settings** area.
3. Click **Updates & Licensing**.
4. Enter your registration key into the box and click **Register**.
5. Depending on which products you've licensed, you should see various modules display. If you have a full license, you will see:

   - Antispam
   - Antivirus
   - Attachment Filtering
   - Disclaimers

6. If these do not show up, retype your key and press register again. This will request a new authentication from VIPRE.

4.5 Setup Email Notifications

In the event that your system experiences errors or critical stop points, you need to be notified and prepared to react. Accordingly, the experienced administrator should setup email notifications to alert them of any critical alerts or errors. To do so, you can follow these steps:

1. Navigate to **Settings**
2. Select the **Notifications & Logging** dropdown
3. Under Email Notifications, select **Add**
4. In the dialog box, enter your administrator's email address.
5. Click the **Apply** button.

6. Check the **Enable email notifications** check box
7. Click the **Apply** button again.

4.6 Network Configuration

Because VIPRE takes advantage of many networking capabilities, including the ability to retrieve multiple updates from various servers throughout the internet, we have drafted a set of recommended best network configuration practices that should allow VIPRE to operate unhampered in your environment.

SOAP requirements

In order for your system to properly retrieve updates, you must configure any hardware or software protocols to allow the SOAP protocol to be transmitted across the internet. If this is not done, updates will not complete properly.

Port 80 Exclusions

To retrieve updates from our update servers, you will need to ensure that port 80 is open for outbound connections to:

◆ licensing.sunbeltsoftware.com (Port: 80)

◆ updates.sunbeltsoftware.com/spursspurs.aspx (Port: 80)

◆ ec.sunbeltsoftware.com (Port: 80)

Unless properly accounted for, Proxy servers can be the bane of your updates existence with VIPRE. To ensure that you're properly retrieving updates, make certain that you enter your proxy server information on the **Proxy** tab of the **Updates and Licensing** submenu within settings. The exact configuration will depend on the type of proxy you're operating.

5 Antispam

Antispam consists of connection filtering technology, as well as the Antispam Engine with custom rules, Real-time Blocked Lists, and DNS/reverse DNS authentication (SPF). Below are our recommended settings for these features.

5.1 RBL settings

RBL stands for Real-time blocked lists; we recommend ensuring that both of our RBL lists are applied. Pressing the **RBL Settings** button will enable the two default engines:

- zen.spamhaus.org
- bl.spamcop.net

These should both be checked and operating. Additionally, you will need to make sure the **Enable RBL Check** box is selected. If it's not (like in the figure below) *it will not work*!
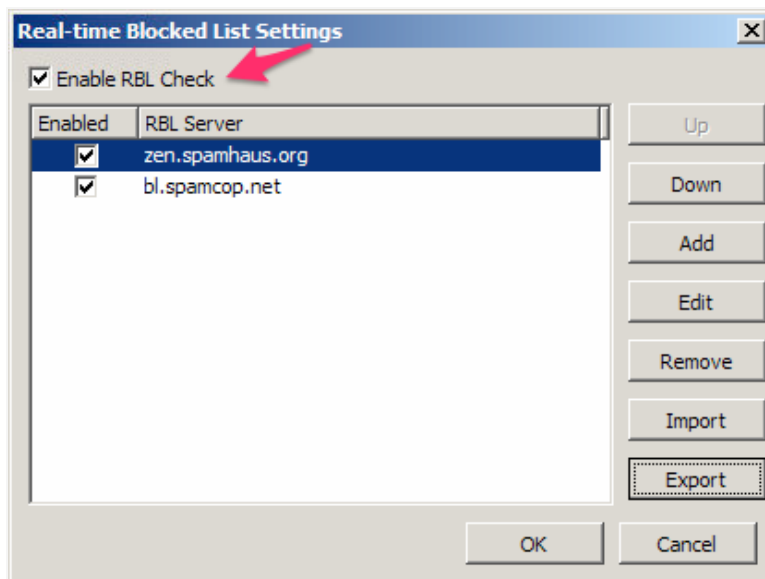
If you have to enable the **Enable RBL Check** checkbox, make sure you hit the apply button when you are finished.

5.2 SPF Settings

SPF stands for *Sender Policy Framework*; it is a DNS and Reverse DNS framework designed to authenticate mail senders and prevent spoofing and spam practices. VIPRE uses SPF to enhance its security and aid users in preventing unwanted email.

If "Enable Sender Policy Framework" is checked, there will be an "X-Ninja-Spf" header added to every received message. This header will contain the result of the SPF check.

Possible results are: Pass, None, SoftFail, Fail, TempError, PermError, Neutral. (Fail is the same thing as HardFail)

SPF should be turned on with the **Enable Sender Policy Framework** checkbox. You then need to select either **Block soft fail** (allow) or **Block hard fail** (hard rejection).

> SPF does not need to be setup on a server that does not perform antispam, antivirus, or attachment (such as a mail store server or a backend server).

> We do not recommend enabling **Block hard fail** because a hard failed message is virtually guaranteed to be spam. A hard fail indicates that the address does not reside on the SPF record and should not be sending email.

5.3 Enable Default policy

To allow administrators the ability to configure VIPRE before deployment, VIPRE comes with the Default Antispam Policy set to disabled. To guard against spam, you should enable this policy by right-clicking on the policy and selecting enable, like you see in the screenshot below.
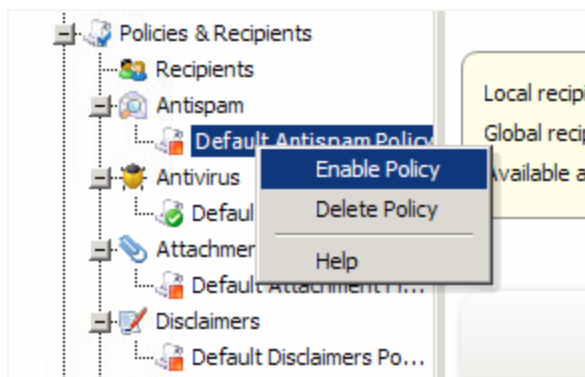
5.4 Scores and email headers explanation

To help you further refine your rules and monitor mailflow within your organization, we'd like to show you how VIPRE x-headers operate. Thus, here is the anatomy of the header from the Antispam plug-in:

1. The name of the plug-in
2. The Antispam policy the recipients were on (The number is the policy ID)
3. The action that was taken (This can be "Allowed," "Quarantined," or "Deleted")
4. The reason that action was taken. The possible entries here can be any of those listed in the dialog at Policies & Recipients -> Antispam-> [Policy] -> Rules -> Set Order...
5. The score given to a message:
   a. Score from Antispam custom rules that modify points
   b. Score from Antispam policy custom rules that modify points
   c. Score from the Antispam Engine
   d. The total of a, b, and c. This is what gets checked against the thresholds

If Part 4 of the header says anything other than "Final Score," the score will almost always be 0. This is because in this case it matched a rule that had an action other than modify score. In this case, we

already know what to do with the message, so the engine is never run against it and no modify weight rules are run against it.

An example of one of the "almosts" would be if a message is going to several recipients on the same policy and one recipient has the sender in their personal Allowed Senders folder and none of the other recipients do.

That one recipient may see something like:

```
X-Ninja-Antispam: Policy 4 - Allowed - Allowed Senders (Personal) - 0,-50,25 (-
25)
```

5.5 Attachment Filtering

We highly recommend the use of VIPRE "SMART rules," that can block all email attachments other than those specifically defined by you. For example, if you wanted to block all attachments other than **pdf** files, you could define two rules, one that allows **pdf**, and one that quarantines all attachments. This will allow the rule that's defined first (allow pdf) to be applied, and then for the other rule to disallow all other attachments.

Rule	Action	Scan Inside...	Inbound Internal	Inbound External	Outbound Internal	Outbound External
PDF document files (*.p...	Allow Attachment	☑	☑	☑	☑	☑
.	Quarantine Email	☑	☑	☑	☑	☑

You could, of course, repeat this procedure and allow common file types, such as .jpg, .gif, etc. In the wizard to add a filter, VIPRE includes many common file types, and allows you to define your own safe types.

Also, to ensure that your email attachments are properly being delivered to your recipients, you should make sure that you are filtering in the proper direction. Briefly summarized, filtering directions work like this:

- ◆ **Inbound Internal**: Messages from internal user to internal recipient
- ◆ **Inbound External**: Messages sent to an internal recipient from an external source
- ◆ **Outbound Internal**: An outgoing message from an internal user to an internal recipient
- ◆ **Outbound External**: An outgoing message from an internal user to an external recipient (any email sent outside of the internal network)

6 General Usage

This area of the best practices guide will show you some general usage best practices and how to make the most out of your purchase.

6.1 Disclaimers

When adding disclaimers to your VIPRE console, you should ensure that you first copy the text of the HTML template and paste it into the Plain Text template editor area as well. If you do not do this, the template will not display properly in both HTML and plain text format.

6.2 Conserving Licenses

Because VIPRE is a licensed per mailbox product, there will probably be occasions where you will want to conserve the number of licenses you have in use. By default, VIPRE will consider a mailbox as active so long as that mailbox has a policy applied to it. However, as routine business operations (such as turnover and restructuring) occur, mailbox licenses will still be occupied as long as there is a policy applied to that mailbox, whether or not it's sending or receiving mail.

To correct this and conserve your licenses, you can navigate to the recipients area and perform a global search for the mailbox you'd like to exclude. Once you've found the mailbox, you can open it up and select "no policy" for the Antispam, Attachment Filtering, and Disclaimers policies. This will deactivate the mailbox from use, and also stop VIPRE from applying any sort of filtering. For the sake of clarity, we've included a screenshot.

AV protection is policy based; you can therefore remove users from individual AV policies.
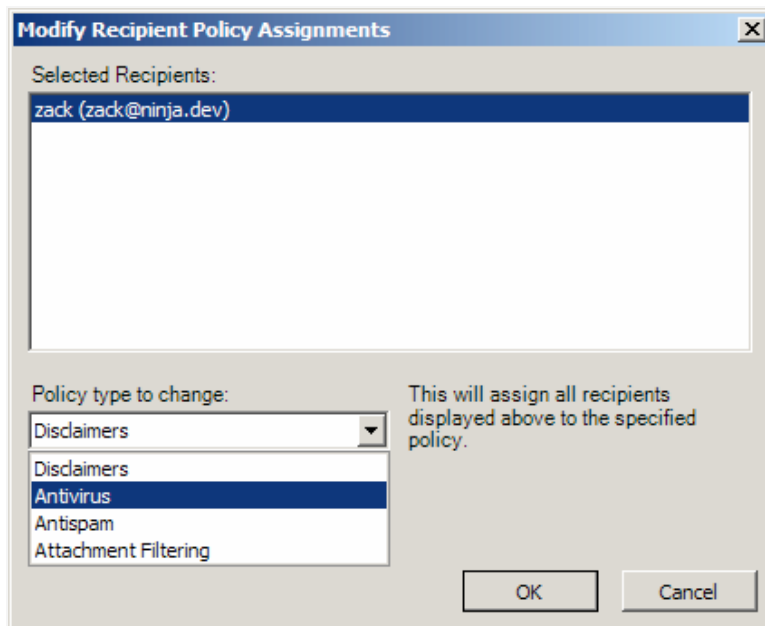
6.3 Disable "Junk Email Folder"

To provide a centralized method for SPAM management, you should disable the junk email folder from outlook for your users. Otherwise, you may experience conflicts between the Junk Email Folder and the

VIPRE Spam folder that causes SPAM to be caught in both areas. To disable the Junk Email Folder, you can disable it through the Exchange Management Console.

> ℹ️ Group Policy is not supported.

6.4 Allowed Senders folder Usage

As a best practice, the Allowed Senders folder in VIPRE should only be used for a very rare false positive email. Outlook contacts do not need to be added to this folder, as they are added by default.

6.5 Blocked Senders folder Usage

The Blocked Senders folder is best used as a folder for email that is not from a SPAM provider, but email you still wish to consider email. For example, if you have a former employee who is constantly sending you irritating email, you could add this employee to the "Blocked Senders" folder. This will count all the employee's email as SPAM.

6.6 Auto-Delete is NOT Recommended

When configuring custom SPAM handling rules and exceptions, you should do your best to avoid setting emails to delete upon being flagged. If this is done, the email will be removed as soon as it is sent. This means that in the case of a rare false positive, the email will be unrecoverable.

Contacting VIPRE Support or Sales

VIPRE Business and Enterprise Support

311 Park Place Blvd, Suite 300, Clearwater, FL, 33759, USA

Telephone: +1 (877) 757-4094

https://businesssupport.vipre.com

VIPRE Sales

311 Park Place Blvd, Suite 300, Clearwater, FL, 33759, USA

Telephone: +1 (855) 885-5566 (+1 727-324-0001)

Email: vipresales@vipre.com