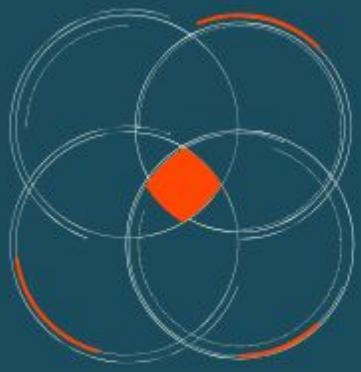
VMRacks
Managed Security Services

WHITE PAPER

CUSTOM IP REPUTATION



Ryan Cowell

Stephen Trout

Abstract

Healthcare organizations, businesses, and governments that handle sensitive information rely upon advanced threat monitoring tools and mitigation platforms to protect against crippling cybercrime attacks. Yet commercial cloud-based security services that secure internet protocol (IP) addresses and provide for endpoint security by effectively blocking inbound bots, Trojans, viruses, and other forms of malware, as well as filtering for spam and unsolicited bulk email (UBE), can be cost-prohibitive, especially for smaller businesses.

This White Paper describes an effective alternative to expensive anti-malware and filtering solutions; a custom IP Reputation tool that effectively delivers block lists of spam and criminal malware directly to firewalls, routers, and DNS Servers, and helps prevent unauthorized data exfiltration from servers. Accurate white listing of acceptable IPs, Subnets, and FQDNs is also achieved, and coordinated with automated lists.

VM Racks Custom IP Reputation uses near-real time intelligence to protect critical network and data assets - crucial for environments with sensitive data such as protected health information (PHI). Our multi-tiered approach to security continues to provide the superior data integrity and protection our customers count on to maintain an excellent business reputation and customer satisfaction.

Table of Contents

01 Introduction

IP Reputation tools are invaluable for assessing and mitigating security risks; they distinguish malicious activity and histories associated with IP addresses that should be blocked (also called “blacklists”) from good senders, or “whitelists.” While a number of these blocklists are freely available, the advanced threat protection needed for sensitive data tends to come from expensive, highly curated, automated feeds offered in commercial blocklist subscriptions. Customizable for each unique computing environment, these tools provide excellent protections, yet tend to cost hundreds, even thousands per month - a cost prohibitive solution, particularly for small businesses.

VM Racks understands the need to prioritize blocking of unwanted and potentially dangerous traffic. An experienced managed security service provider with HIPAA expertise for thousands of small businesses and enterprise-level clients, our mission for over twenty years has been to safeguard the integrity, privacy, and availability of sensitive data. This White Paper examines the fruit of our labors in one critical area: Custom IP Reputation. Offered as an integral part of our managed security services, this practical expertise demonstrates how your data security can be strengthened while keeping business costs under control.

02 Determining Your Blocklists

IP addresses and domains controlled by hackers, bots, and spammers all represent a potential liability to your vital data. Unfortunately, the financial burden of dealing with malicious or unwanted traffic can be exorbitant. To cite just one example, a small ISP in Utah, USA, with 37 employees, recently testified that it spends more than $280,000 a year to deal with spam and related harm.

To date, a multitude of public blocklists have been published, used in coordination with server rules designed to protect networks from malicious attacks. ISPs and corporate entities will often create their own internal blocklists from known

offenders, while most server administrators will include anti-spam filters on their mail servers.

To maintain costs and pass this savings on to our customers, VM Racks' system administrators have utilized highly accurate threat intelligence, such as the freely available blocklists published at Danami: https://docs.danami.com/juggernaut/user-guide/ip-block-lists.

These blocklists may then be supplemented with country codes in order to provide comprehensive geo-blocking. In cases where clients do not expect any traffic from outside of their primary region, geo-blocking the "rest of the World" further minimizes their exposure to potential attacks. These decisions must be determined by each client's particular business needs and level of acceptable risk.

Because VM Racks uses these externally generated blocklists in addition to our own internal honeypot lists (detected hacking attempts on our servers not yet in any lists), the total number of entries blocked can actually fluctuate during periods of global attacks. If our servers pick up the activity, they will add these bad actors to our internal list. Otherwise, it's very likely they will eventually end up on the blocklists we use.

03 The VM Racks Solution

For VM Racks, a layered security approach is key. System administrators will appreciate that our operating system of choice is VyOS, a heavily customized Linux distribution based on Debian that has been stripped down to minimal components for use as a router and/or networking device OS. Being a Linux distribution - and therefore free and open source - it also provides some standard Linux tools for server management. All of the code used to setup the devices, such as downloading and processing the blacklists, is written in perl.

For our perimeter defense system, we use a server with specialized network connections that are set up in pairs on the motherboard. These connections are set to “fail closed,” meaning that if the server is powered off, or in the event of a catastrophic server failure, the network traffic will simply pass through the system to avoid service disruption. In a remote data center environment, a connection that can survive a system failure is desirable. In an office environment, it would be convenient, but there is also likely to be someone who can physically move a cable to bypass the device upon failure

A perimeter device blocks the known bad IP addresses before they can even get into our secured environment. On a client server, we will block IPs that are associated with the primary service the server provides - web attacks for web servers, ssh brute force attacks on SFTP servers, mail attacks on mail servers, and so on. This should help to minimize false positives, and with a properly secured firewall, the ports for other services are not going to be available, Limiting client level blocks to the "service type" also decreases the overhead on the client system by limiting the number of blocklists to be maintained and contributes to a multi-tiered solution.

Utilizing this second line of defense for our clients provides more granularity. The perimeter device will block the bulk of the known bad IPs, but sometimes we may want to block, for example, all connections *except* those from North America. This is where we can customize the blocking on a per client basis on the WAFs (Web Application Firewall). The WAFs have several layers of security for examining web traffic, but CSF (ConfigServer Security & Firewall) is a freely available software firewall system that is easily configured via text files. (https://www.configserver.com/cp/csf.html).

VM Racks also manages the firewall settings using CFEngine for configuration management. CSF was part of the inspiration for the blocklist setup on the VyOS devices - in fact, the blocklist format used for the VyOS is copied from CSF - so that any lists can be used directly with either system, without extra processing for

compatibility. Finally, we also run a custom setup script for our environment, which installs necessary system packages, perl modules, sets up configurations for Nagios monitoring, and sets cron jobs to control the list retrieval process, and more.

Curating the Lists

The frequency component for curating our lists is determined by a combination of CSF and additional blocklist feeds. CSF uses a format in the blocklist entry that specifies how frequently to check for updates. Since we desired all of our systems to be compatible, we used the same format for setting up the VyOS blocklist settings. The the update frequency and settings within the configuration files is based on the settings for each particular list. The perimeter devices check every 2 hours to see if any of the lists have "expired," and should be retrieved again prior to processing the blocklists. Some lists are updated more frequently; it depends on the lists used and the needs of the users. Though infrequent, country codes can actually change from time to time so they are updated on the system once per day to ensure they are as accurate as possible.

04 Advantages over Commercial Products

As mentioned, VM Racks multi-layered approach to security offers distinct advantages over comparable, commercial service providers. These are primarily seen in cost, but also in blocklist intelligence and flexibility.

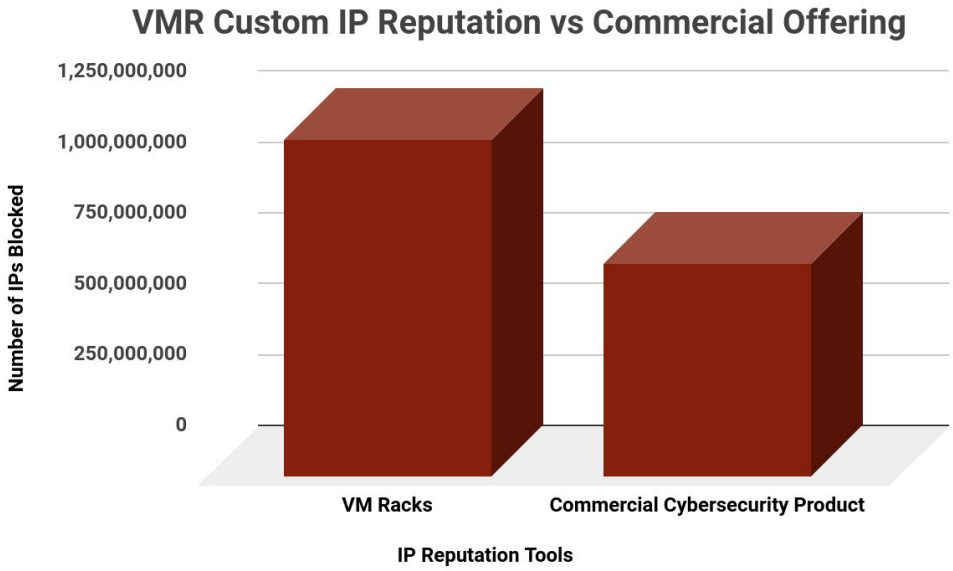
Cost

We've described how to use freely available blocklists, and where to find them. Using a software firewall such as CSF is also entirely free, and can provide flexibility for blocklists including country-code blocking. An experienced sysadmin should have no problem setting this up. While there is some initial configuration required to get it running, there is zero out of pocket expense for use. As mentioned, comparable tools with this level of advanced protection can be in the thousands per month, depending on the environment.

Blocklist intelligence and Flexibility

CSF is one of a number of superior resources available for firewall blocklist feeds and server protection. These lists have proven to provide excellent protection with a minimum of false positives. VM Racks also has the flexibility of customized blocking, on a per client basis. This allows for greater efficiency and capacity savings, as well as improved network performance and reduced bandwidth utilization.

Still, we wondered if we were able to meet or exceed the sheer quantity of IPs blocked, as compared to a commercial provider. To test this, we examined how one of our enterprise-level clients fared with the commercial product, as opposed to our approved, curated lists and equivalent country codes:



Key takeaway: VM Racks exceeded a comparable commercial offering by over 400 million IPs blocked.

05 Summary

VM Racks Custom IP Reputation has consistently mitigated malicious traffic and eliminated the threat of data exfiltration for our small and enterprise - level clients. These companies depend on VM Racks every day to help secure their environments and maintain the integrity and availability of sensitive data necessary to serve their customers. As we've seen, a layered or multi-tiered approach that utilizes open-source tools can actually achieve an equivalent or greater level of security compared to commercial service products, while keeping costs at a minimum. This can be a welcome solution for those companies unable to acquire expensive cybersecurity solutions.