Enhanced Geo-Target Based Network Defense

Proactive Network Defense for the Global Market in the Zettabyte IP Traffic Era

A PacketViper White Paper
Revised: August, 2018

INTRODUCTION

Despite advances by commercial firewall providers, cyber security breaches are an increasingly prevalent, dangerous and costly problem for companies. Furthermore, liability and legal ramifications for such breaches are an emerging problem for businesses of all sizes, and statistics indicate that many companies remain ill-prepared for such attacks. One approach to network security with great potential to reduce the threat of cyber-attacks, but which is currently underutilized for a number of reasons, is the implementation of a precise geo-targeted defense. Innovative advances in Geo-IP filtering have enabled heretofore unseen levels of precision, agility and user-friendliness, and this new and enhanced Geo-IP filtering should make the technology a viable and essential part of any comprehensive, layered approach to network security.

This paper underscores some of the problems with the current security paradigm, describes how targeted Geo-IP filtering addresses those limitations, and provides a description of how this approach can be integrated into a typical security system within the context of different business practices and needs of individual companies.

GEO-TARGETED CYBERSECURITY AND NETWORK DEFENSE

Cyber-attacks are a global phenomenon. It's now possible for anyone with a computer or a smart phone and an Internet connection to launch an attack on a target victim anywhere in the world. Rented botnets can be used to distribute spam and phishing emails in addition to aiming DDoS attacks at victim organizations.

Geo-IP filtering is a network security tool that allows or denies network traffic, at the port level, based on geographical location, combined with a variety of other factors such as company, source/destination network, time and/or rate. Sometimes referred to as country filtering or blocking, Geo-IP filtering allows your network to choose places in the world from which it will accept or to which it will send network traffic. More importantly, innovative designs in Geo-IP Filtering enable new and unparalleled levels of precision that allow businesses to prevent access to and from high risk geographical areas without excluding potentially valuable customers or business.

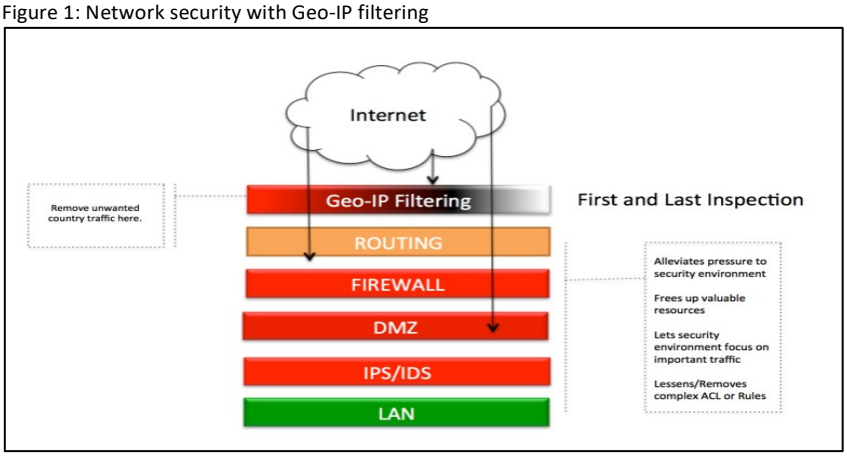
These days, effective Geo-IP filtering is about much more than simply blocking a country. An effective Geo-IP filter must filter both inbound and outbound traffic as a first and last line of defense.

AN ADDITIONAL LAYER

Geo-IP filtering dramatically reduces that risk by improving the security of both the internal network and the DMZ, creating a synergistic and fundamental improvement in overall network safety. Furthermore, when placed at the start of your security chain, enhanced Geo-IP filtering eliminates unnecessary traffic and threats while simultaneously reducing the need for security inspections—all of which ultimately result in improved performance throughout the most exposed area of your security chain.

To illustrate, Figure 1 below suggests how a Geo-IP filter should be the first and last inspection for traffic entering or exiting your network. With the Geo-IP filter sitting inline as an undetectable bridge, this layer quickly eliminates unwanted traffic for the remaining layers on your security chain while preventing unwanted outbound traffic to suspect locations.

Figure 1: Network security with Geo-IP filtering



LIMITATIONS OF THE TYPICAL NETWORK SECURITY APPROACH

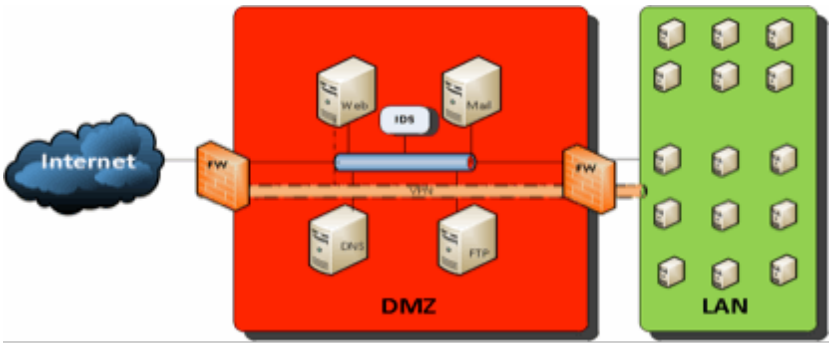
Unfortunately, despite proven advantages of Geo-IP filtering there remains common misunderstandings of the fundamental concepts underlying its usage. For example, many popular firewalls claim to have Geo-IP filtering. However, these firewalls generally offer either a geographical tool that is too rudimentary to be effective or too complex to be useful. The simpler tools resort to overly simplified methods that require entire nations to be excluded, costing a company potentially valuable markets or clientele. Other firewalls offer overly complex geographical systems that are unwieldy and difficult to implement. Companies who have attempted to use these features experienced numerous problems once enabled. Stoppages, delays and slow speeds for browsing, email, web services, and remote access from users abroad were among the most common problems cited.

With these types of serious limitations and problems with geographic screening tools, or with the occurrence of the first handful of legitimate connection requests from a particular country, many users simply disabled the country blocking features in their firewalls and returned to their initial approach. Analysis of these problems showed that current geographic filters failed because the firewalls lacked the ability to filter on a more precise basis than just the location of the computer or network. Currently available solutions cost-effectively address these limitations and offer the flexibility to filter geographical location and their ports, yet not restrict customer or vendor access.

Consider a fairly typical example of a company's Internet presence. Most businesses find it necessary to make certain services such as Web, Mail, DNS, and FTP accessible to the public. This part of the network is also more accessible to hackers, and therefore is typically housed in a DMZ to protect the core of the network and its vital data. The DMZ is protected from the Internet to some extent by a firewall, and a second, more intensive firewall protects the internal network from any breaches of the DMZ. To be fair, this is a straightforward design that usually provides good protection while providing essential services to your employees, customers and vendors.

On the other hand, this model has several underlying weaknesses that could cause significant to catastrophic damage to your company.

Figure 2: A typical network security model



First, note that the public portions of your network – Web, DNS, FTP and Mail – are necessarily housed in the more vulnerable DMZ. Of course, some parts of the network must be made accessible to the outside Internet by including them in the DMZ, but that means they are also more likely to be compromised. Is it acceptable for your business to lose the use of its website, email, VPN, DNS, spam filter, or proxy for any amount of time, let alone potentially extended periods of time?

PROXIES & GEOGRAPHY

A critical component in the arsenal of cyber attackers – but one that can suggest a solution – is the crucial role of proxies and geography. Essential to the success of the attack is the use of Web proxies. By routing traffic through open proxies, the attackers attempt to bypass IP blocks. Attackers use tools that provide lists of open proxies and cycle through them after a fixed number of attempts. This allows cyber attackers to multiply their threats and to attack networks with virtual impunity. With multiple sources observing attack traffic originating from almost 200 unique countries/regions at the end of 2016, this global presence creates a world of opportunities for hackers and can overwhelm the ability of network firewalls and other security devices to keep up.
As long as hackers have unlimited space in which to operate, and security systems are forced to spread their attention in all directions, cyber attackers will have the upper hand. To maintain network security in an increasingly threatening future, it is therefore absolutely essential to implement systems that shrink attackers' options and prevent criminals from having unlimited

attempts to penetrate vulnerable networks. Unfortunately, traditional network security systems are designed with an entirely defensive philosophy, and are not capable of reducing hackers' capacity to attack. Instead, security professionals should recognize that enhanced Geo-IP filtering is the best available solution for effectively reducing cyber-attacker options. Geo-IP filtering reduces attacker options by denying them use or direct network paths to or from networks, and enhanced Geo-IP filtering is particularly effective relative to typical security systems when hackers resort to the use of proxies.

THE SILENT KILLER OF NETWORK SECURITY: MASSIVE GROWTH IN GLOBAL IP TRAFFIC

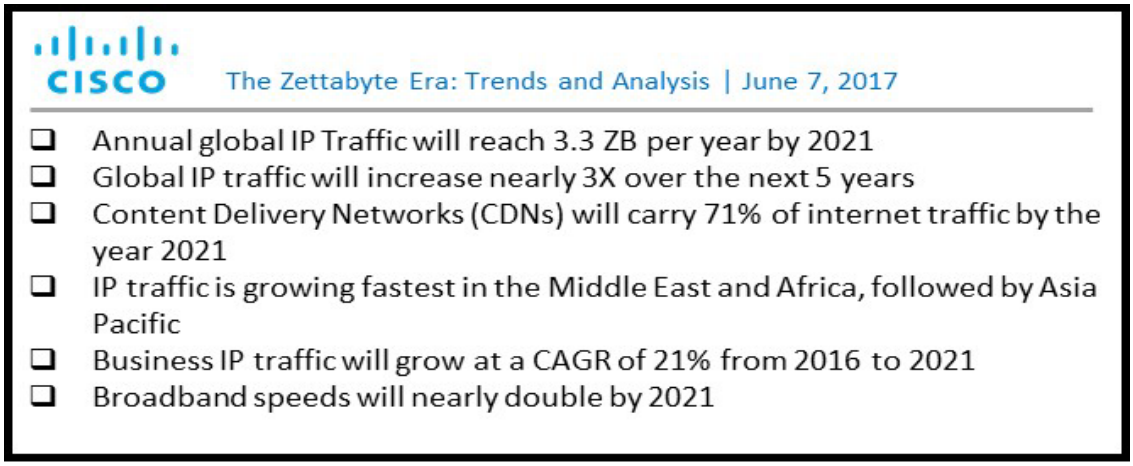
While firewalls were evolving to provide much needed comprehensive filtering across the entire OSI stack, a new problem was brewing on the attacker front. Cyber-attacks have become a global phenomenon. Today anyone with a computer or a smart phone and an internet connection can launch an attack on a target victim anywhere in the world. Due to the ease with which attackers can cultivate a botnet and illicit services that rent the use of botnets, the cost to attack is cheap, getting cheaper, and more readily available. Rented and/or newly built botnets can be used to distribute spam and phishing emails, steal money, steal identities and propagate new malware. Cost is no longer a consideration as villains seek to aim high volume attacks at organizations.

This is all exacerbated by the cultural need to be 'constantly connected'. People's desire to maintain real-time, constant connection to the internet results in a proliferation of devices which provide countless amounts of bot configuration options. The fluid nature of this expanding and contracting attacker landscape is impossible to address with firewalls and logging systems. Attackers leverage this advantage to distract network managers and constantly keep security teams on their heels in a reactive state. These attackers have countless resources and methods at their disposal and start with a simple reconnaissance scan, probe or some other simple test of service limits. They hide these within everyday traffic patterns to distract administrators and gain intelligence to penetrate, incapacitate and/or extract data from a network.

A ROOT CAUSE PROBLEM

All of these increasing global IP traffic trends represent a root cause problem for network security managers, as evidenced in these excerpts from a recent CISCO report on IP traffic trends:

Figure 3



INCREASINGLY UNMANAGEABLE TRAFFIC, LOG AND ALERT VOLUMES

These global IP traffic volumes that encounter the corporate border are resulting in a problematic amount of logging and alerting, which quickly becomes overwhelming for organizations of all size. ESG Research cites the volume of security alerts as the #1 operational challenge in security operations today. This is equally true of MSP, MSSP and SOC teams as it is for in-house network security teams. While larger enterprises are increasingly investing in security information and event manager (SIEM) applications, the value of these solutions is compromised by the traffic volume problem. The increases in traffic correspondingly drives up the number of alerts, time required to check and time it takes to remediate. Also, some popular SIEM solutions have volume-based pricing schemes, so the illegitimate traffic can increase SIEM fees and security costs.

SPAM AND BUSINESS EMAIL COMPROMISES – A RELATED PROBLEM

As demonstrated earlier, hacking and cyber security are truly global problems. Spammers set up shop in co-locations, unregulated network space and vulnerable systems around the world. They are continually in motion and almost impossible to track, but Geo-IP filtering can help address this problem. The following use cases from customers who have implemented the PacketViper Geo-IP filter illustrate the dramatic improvements gained by eliminating unwanted traffic coming into their mail systems. These cases show that Geo-IP filtering eliminated thousands of purely nuisance messages as well as messages laden with phishing links and malicious attachments, while at the same time restoring the bandwidth associated with this unwanted mail traffic.

Figures 4 and 5 show that the PacketViper customer ***eliminated about 100,000 spam messages each day and about 70% of the spam messages each hour***. This decreased the load on the spam filter and made administration of these systems much simpler and less time consuming while reducing loads throughout the security chain.

Figure 4: Reduction in daily messages when Geo-IP filtering is added

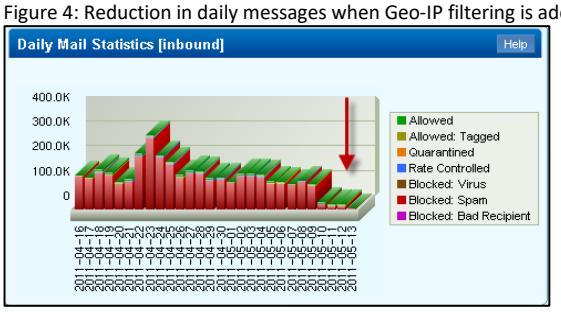
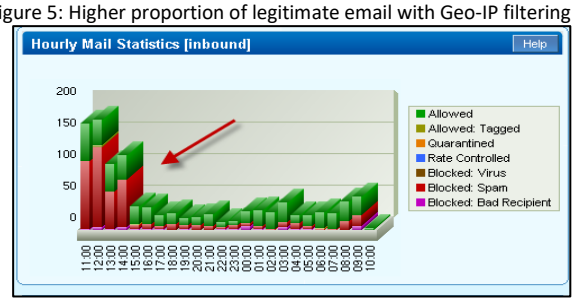


Figure 5: Higher proportion of legitimate email with Geo-IP filtering



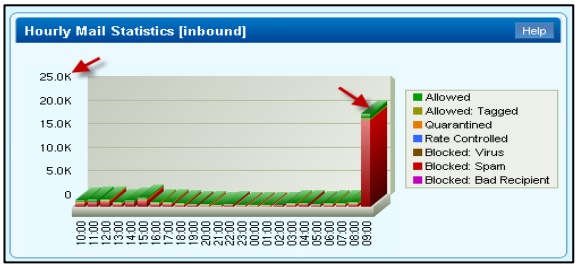
Source for both images: Actual PacketViper customer

Figures 6 and 7 show the immediate spike in spam traffic that occurs when the Geo-IP filter is turned off for two different PacketViper customers.

With the Geo-IP filter on, threatening mail numbered fewer than 1000 messages per hour, but ***increased by 2000% without Geo-IP filtering.*** Although the rest of the security chain is still doing its job when the Geo-IP filter is off, the chances of something harmful getting through are clearly worsened.

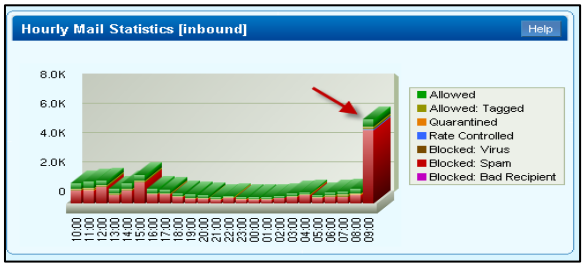
The increased load also slows the process of messages, and increases bandwidth usage because of the additional message packets traversing the security environment.

Figure 6: "Customer X" spam spike when Geo-IP filtering is turned off



Source: Redacted PacketViper Customer Data

Figure 7: "Customer Y" spam spike when Geo-IP filtering is turned off



Source: Redacted PacketViper Customer Data

ENHANCED GEO-IP FILTERING --- GRANULARITY AND PRECISION

Geo-IP filters can reduce threats of any sort of cyber-attack, including botnets, zombie systems, malware infected web servers, and email viruses. Outbound geo-location filtering helps combat these types of breakouts by limiting their ability to operate freely around the world. In other words, Geo-IP filtering not only stops threats from penetrating your network, it also addresses the possibility that one of your employee's laptops, cell phones, or other local device could carry a threat and transmit it to the Internet via your network. Both inbound and outbound filtering are important benefits of Geo-IP filtering, and they can dramatically reduce your exposure to security risks and the costs and liabilities that go along with them.

It is important to remember that in a typical security system, ***a port opened through your firewall allows equal access to anyone in the world***. Given the statistics on the volume of attacks that a computer network is likely to face, is that a wise or necessary

gamble? Instead, a reasonable person might ask, how much business do we conduct in a certain nation? How many clients do we have in another? How likely is it that we should want to market our business across the world? What if we have three important B2B clients in one problem country? What if those three clients grow to thirty which require connectivity from dozens of problem geographies? One can see the exponential growth in rule and exception complexity that challenge even the most tightly run perimeter security teams and toolsets.

Additionally, one might reasonably decide to balance the results of those responses with the volume of cyber-attacks originating in any of those countries and provide access to your network according to the dictates of your business needs, not on an arbitrary all-or-nothing basis. In fact, this sort of controlled and measured access to your network is exactly what Geo-IP filtering allows.

Geo-IP filtering enables a security system to decide whether to allow access to your network's service port for any nation in the world. Geo-IP Filtering also limits which geographical locations have access to specific ports and services, thereby alleviating pressure on those services and reducing their exposure.

The diagrams in Figures 8 and 9 below illustrate how this might look in practice. Figure 15 illustrates Internet traffic entering a network from various countries without challenge until it reaches the company's outermost firewall. Traffic is allowed to proceed to a designated port, regardless of where the traffic originates.

Figure 8: Inbound network traffic without Geo-IP filtering

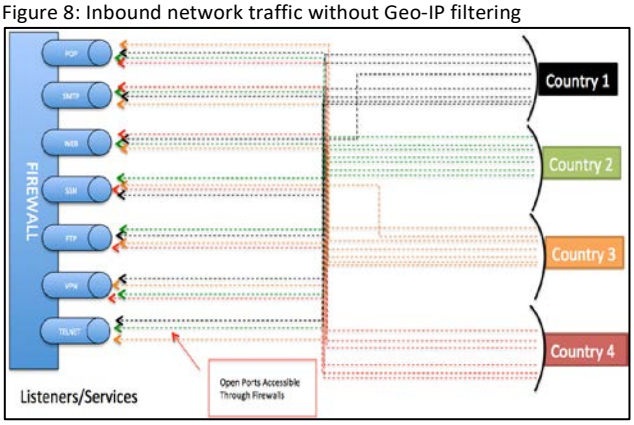
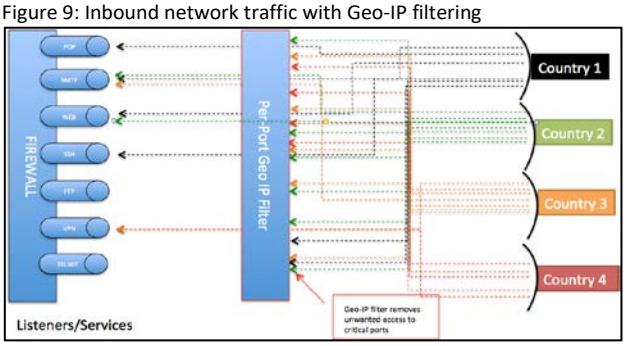


Figure 9 illustrates Internet traffic encountering the Geo-IP filter before it gets to the outermost firewall. The Geo-IP filter drops packets based on specific country/region policies, eliminating a high portion of unwanted traffic.

Figure 9: Inbound network traffic with Geo-IP filtering



When a Geo-IP filter is implemented correctly, you will find your security environment is less stressed and more secure.

THE SIGNIFICANCE OF COMPANY WITHIN COUNTRY GEO-TARGET BASED APPROACH TO NETWORK SECURITY

An easy to use Geo-IP filtering system must have great flexibility, customization and precision. Geo-IP filtering must be flexible in order to be modified to meet the customer's constantly changing needs and markets. And Geo-IP filtering must be precise enough to target extremely specific geographic areas while avoiding blacking out entire countries or being forced to exclude valuable markets or existing clients, prospects and partners. Extensive research proved that the key to solving this problem would involve

the ability to filter by country at the network port level. This method allows customers to specify which countries are permitted to access specific network ports, instead of completely blocking them. In this way, it is possible to eliminate unwanted network traffic and focus on traffic that is important to the environment. Additionally, although filtering at the network port level allows for greatly increased customizability, the global business environment creates a chance that a well-known global business like Microsoft may reside within any given country at any given time.

Therefore, it was also necessary to have the ***ability to intelligently override simplistic all-or-none country filtering using constantly updated intelligence lists of global businesses, existing supply and demand chain relationships, and high-risk networks***. These lists provide the capability for users of enhanced Geo-IP filtering to override country filters by quickly selecting a company from the global network lists, and adding the important network ports specific to that company.

Finally, based on the lessons learned from older Geo-IP filters, ***enhanced Geo-IP filtering must allow users a seamless, efficient and straightforward experience.*** *Real time clickable logs* with an individualized NetCheck™ allow customers to quickly view in real time which countries are entering and receiving traffic, click on any log entry and quickly see additional details such as associated networks, source country, region, city, ISP, and RDNS, along with quick block.

In summary, enhanced Geo-IP filtering is:

- PRECISE – Filtering at the network port level, by country and company both inbound and outbound
- CUSTOMIZABLE – Easily apply updated intelligence lists of global businesses and high-risk networks
- FLEXIBLE – A quick and simple point and click method with all the necessary information at your fingertips

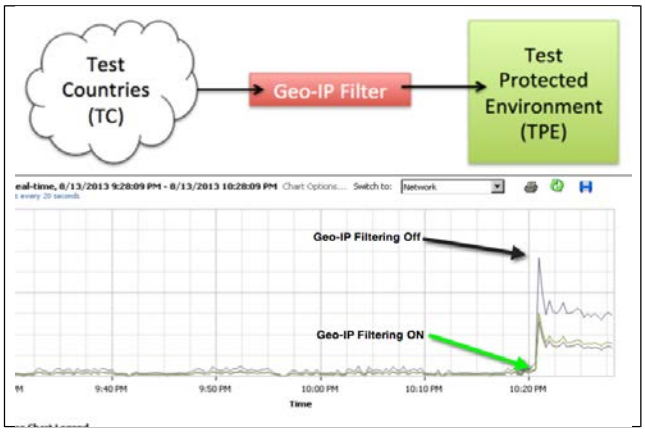
DATA, RESULTS AND BENEFITS OF ENHANCED GEO-IP FILTERING

The following proof points show how the PacketViper Geo-IP filtering solution eliminates malicious and other unwanted traffic from a network environment. One use case comes from our own test lab, and the second comes from an actual customer environment.

Test Case 1: Performance and Network Load From PacketViper Test Lab Environment for small / mid-size location

Our Test Lab Environment includes three ESX hosts, two of which contain 24 VMs configured to simulate 12 separate countries, and one set up to simulate protected systems and services. The test environment generates high connections and simulates the actual threats to a network by automated scripted port scans, ICMP, DNS, telnet, web, SSH, and FTP requests per test country VM to test protected VMs. We then placed our PacketViper Enhanced Geo-IP Filter inline to determine its impact. We found that without Geo-IP filtering, the average CPU load was 75% of capacity, and the network usage averaged 1.2 MB per sec. Once the filter was inline, CPU load dropped to 9% of capacity and the network usage dropped to an average of 324KB per second, as shown in Figure 10. These are reductions in load on the network of approximately 90% and 75% respectively.

Figure 10: Connections per hour from TC to TPE: 13 million connections on average per hour, sustained.



Without Geo-IP Filtering:
Loads to TPE: ***CPU Load Average 75%*** (Average taken over 1-hour period)
Network Usage: 1.2 MB per sec

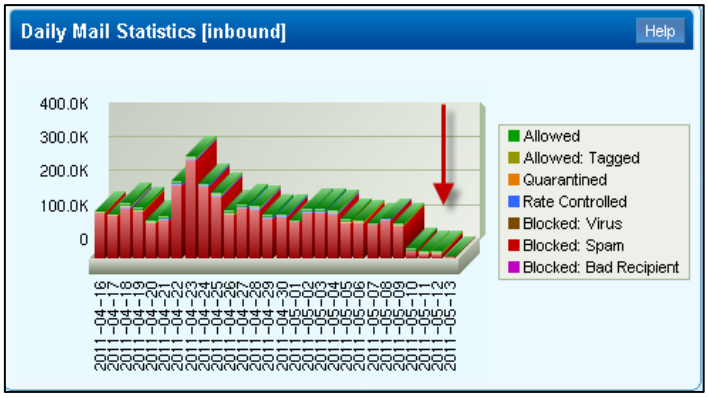
With Geo-IP Filtering:
Loads to TPE: ***CPU Load Average 9%*** (Average taken over 1-hour period)
Network Usage: 324KB per sec

Source: PacketViper Test Lab Environment

Test Case 2: Observed Real World Effects on Bandwidth/Spam/Administration

One of our customers who was receiving an average of several hundred thousand email messages per day discovered that substantial bandwidth was being consumed for just email services. This company noticed its email servers being inundated by many unnecessary spam messages. Although messages were being filtered through their spam-filtering appliance, this mail load was consuming bandwidth, straining the spam filter, and requiring constant management. Once Geo-IP filtering was implemented, the customer reduced its load from an average of 110,000 messages per day to fewer than 20,000 messages per day—a reduction of over 80% of unwanted mail. The results are shown in Figure 11.

Figure 11: Daily mail statistics with and without Geo-IP filtering



Source: PacketViper customer

Based on average email size of 10KB, or an 80-word plain text email message, and administration hourly rate of average of $75.00:

Without Geo-IP Filtering: One Small to Mid-size location
Email per Day; 110,000 average
Est. Daily Bandwidth Use: 10.7MB

- Mid to Large Spam Filter annual license costs (est.): $4,900.00
- Administration/Management: 5 hr / week, 260 hr / year @ $75 /hr FTE cost ($19,500)
- Est. Yearly Costs: $24,400.00 (Not including Bandwidth usage)

With Geo-IP Filtering: One Small to Mid-size location
Email per Day: less than 20,000
Est. Daily Bandwidth Use: 1.9MB

- Small Spam Filter annual license costs (est.): $900.00
- Administration/Management: 2/hr week, 104 hr/year @ $75 / hr FTE cost ($7,800)
- Est. Yearly Costs: $8,700 (Not inc. Bandwidth usage)

Annual savings of $15,700 / year per small-to-mid sized location based on spam reduction alone at the perimeter, without accounting for enhancements in overall security, reduction in load on border Firewalls / NGX Firewalls, and cascading costs of events in the interior network fabric, SIEM and SOC environments.

CONCLUSION

Advances in Geo-IP filtering have created crucial improvements in the technology's utility as an important network security tool. These developments allow companies to maintain a global presence while filtering out undesirable or unnecessary geographical areas. With improvements in precision, flexibility, and customization, enhanced Geo-IP filtering can dramatically increase network security and should be included in every company's security designs.

ABOUT PACKETVIPER

PacketViper is a leading provider of integrated cybersecurity deception, defense and intelligence solutions. Our threat defense platform & integrated approach to deception, defense and intelligence helps customers do more with existing resources while reducing cybersecurity related risks and costs. PacketViper customers are in both the public and private sector and cover multiple industries.

For more please visit www.packetviper.com.

Satisfaction Guaranteed