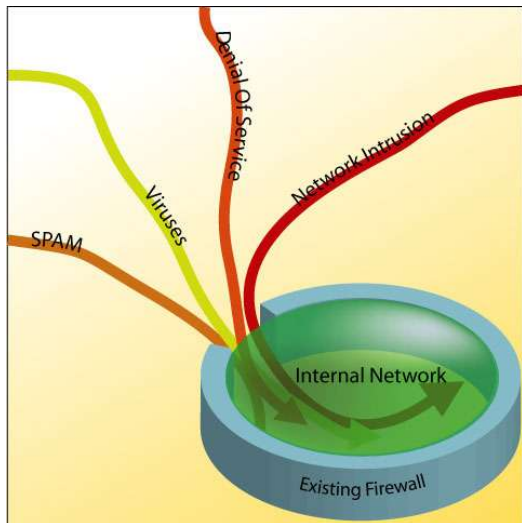


v.Protect Overview

(More than just spam and virus scanning)

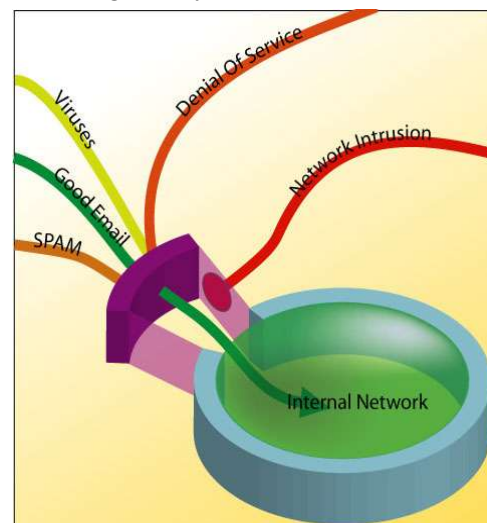
Hosting your own corporate email server provides many advantages. The ability to share contact lists, calendars, files and more is indispensable for many organizations, as is the ability to have direct control over the entire system. A large concern of most email administrators, however, is protecting their valuable corporate network. Most corporate email servers are ill equipped to handle the challenges presented by direct connectivity to the Internet, and therefore open up security concerns for the network.



In order to deliver mail from the Internet directly to users in the corporate network, the corporate server must accept mail from outside. The traditional way of handling this has been to open up a 'hole' in the corporate firewall to allow outside mail connections in. While this approach works for receiving email, the problems with opening up such a 'hole' are obvious. The mail server becomes exposed to a vast array of Internet based attacks from all over the world.

v.Protect eliminates this problem. By providing a 'shield' between the corporate email server and the Internet, v.Protect guards against almost any kind of attack. And since this 'shield' is outside of the corporate network, that means the network is protected, too. v.Protect guards your email server from all of the following:

- Spam
- Viruses
- Network Intrusion
- Denial of Service Attacks
- Email Address Scanning
- Server exploits
- Phishing
- Banking Scams
- and Much More.





v.Protect Details

No single method of protection offers sufficient threat detection capability or flexibility to truly guard a corporate email server from the dangers of the Internet. This is why v.Protect uses multiple layers of analysis on all data before passing it on to your network. Each layer performs its own unique set of functions.

Trust Layer:

The v.Protect service is designed not to allow unauthorized locations to connect directly to your corporate email server. This part of the protection plan allows malicious connections from the Internet to be recognized and dropped immediately. When someone tries to directly connect to the corporate mail server and exploit any vulnerability, or simply directly inject their spam, they are immediately recognized and rejected.

Connection Layer:

When a computer on the Internet attempts to connect to the v.Protect server, they must meet requirements which legitimate mail servers are able to handle, but many malicious programs are not. This is the point at such questions are asked as: "Is this computer trying to send email to a legitimate email address?", "How many times has this computer tried to send to illegitimate addresses?", and "Is this computer obviously running a spam/virus related program?" If certain requirements are not met, the v.Protect service ceases communications with the remote computer instantly; saving the user and the administrator from having to deal with blatant attacks such as these at all.

Malware/Virus Scanning:

After v.Protect decides to accept a connection from the sending server, the email is moved into the scanning process. v.Protect's malware scanner not only performs virus scanning with signatures updated about every 20 minutes, it also scans for potential spyware, trojans, and other types of malware not typically detected by other virus scanners. If malware is found at this stage, the email is quarantined on the v.Protect server, and a notification is sent to the intended recipient. Unlike some other services, v.Protect does not send a message back to the claimed sender of the email. This is because modern viruses tend to fake the "From" address in the emails they send, making such return messages serve no other purpose than to cause panic in someone who very likely did not send the virus in the first place.

**Allowed/Blocked list:**

If the email is determined not to contain dangerous files, it is passed on to the spam scanning process. The first thing checked is whether the particular sender of this email is explicitly blocked or allowed. If one or the other is true, v.Protect acts accordingly.

Distributed Anomaly Scanning:

Beginning the deeper spam scanning process, the anomaly scanner checks distributed databases which statistically track hundreds of millions of emails being received every day. While some other scanning services use distributed scanning such as this, most rely on only one data source for this information. v.Protect uses several, ranging from fully automated systems to systems which rely entirely on human reporting of spam. Each service assigns a confidence level that the email v.Protect is scanning is undesirable. Then v.Protect assigns its own confidence level based on these scores.

Hyperlink Analysis:

v.Protect next looks at each link in the message and compares them to a constantly updated database of links that have been observed to be sent in spam. Using this data, v.Protect modifies its confidence that the message is spam.

Network Tests:

Many virus writers are now using the computers they have infected to send spam, making a profit from the damage they have done. By examining the source of the message, and every computer that has passed it along, v.Protect can determine whether the mail was sent using one of these exploited machines. It is also possible to see whether the mail was sent by a known spammer, whether it originated in a country that the recipient does not wish to receive mail from, and much more useful data. Once again, v.Protect uses this information to modify the confidence that the message is spam.

Heuristic Testing:

v.Protect uses several thousand rules to test every part of the message, looking for such things as words that have been obscured, or words commonly used in spam. These tests also look for patterns used in scams and phishing attacks. This test list is modified both automatically and manually on a constant basis, helping v.Protect to stay one step ahead of the spammers and scammers. None of these tests alone are sufficient to mark a message as suspicious, but together they can have a powerful influence on the message confidence level.

**Learning Engine:**

As the spammers and scammers modify their tactics, we have to modify ours as well. This is why v.Protect learns from every message that passes through, and from the few cases in which it is wrong. This allows v.Protect to spot trends in mail; sometimes before they are noticed by humans.

Custom Rules:

Finally, v.Protect passes the message on to any custom written rules for the recipient. This is a much different and more powerful method than the simple blocked/allowed list mentioned above and used by most other scanning services. In the event that v.Protect doesn't match a company's needs exactly, this layer allows v.Protect to be customized and extended for each company or each recipient within a company.

Based on the levels of confidence assigned above, v.Protect's configureable delivery engine makes the decision what to do with the email. Depending on the malware confidence level assigned to the message, v.Protect may reject the message outright, quarantine it on the server, deliver it to an administrator, deliver it to the user marked as spam, or simply deliver the message as clean.

v.Protect's scanning and detection engine is one of the most accurate and powerful available. It was developed to be flexible and configureable, while giving users the ability to trust their inbox again.