



ANS Spam Plus **Frequently Asked Questions**

Spam Services

Q - How well does your spam filtering service work?

A - Our focus is to block the most spam while never blocking legitimate business email. Our customers tell us we block 90 to 95 percent of their unwanted email without blocking legitimate messages. Customers who participate in our spam filtering process and submit spam messages to us typically see a higher percentage of blocked spam.

Q - How can ANS maintain greater than 90% spam filtering effectiveness without requiring end users to maintain white lists of senders?

A - White listing is simply a workaround for ineffective filtering. ANS has an extremely granular methodology for detecting spam that blocks a high percentage of spam without resorting to white listing. Because our filters do not incorrectly block legitimate messages, users are not required to create and maintain white lists of senders. Our technology advantage results in less work for our customers.

Q - When using ANS' spam blocking service, how do I know if I have spam?

A - Most customers rely on our off-network quarantine service to house their spam. This service allows customers to use a Web browser to review blocked messages and restore messages from quarantine, if desired. Customers get periodic notifications if their quarantine mailbox contains messages that have not been reviewed.

As an alternative to quarantining spam, ANS can tag spam messages and forward them for internal processing.

Q - Will any of my regular business email get filtered?

A - No. We understand the importance of business email, and we strive to not block legitimate business email. However, in some instances, certain types of email newsletters, especially HTML-based newsletters, may get filtered, depending on a number of factors.

Q - Why is the ANS service more cost effective than simply installing another server to filter my mail?

A - ANS' services and network were built from the ground up to provide the best message management solution for enterprises. It would be cost prohibitive for most companies to match ANS' functionality, network architecture, and level of service and support. Further, ANS' strategy of providing message management services outside our clients' corporate networks gives us advantages that desktop and premised-based solutions cannot offer.

ANS' redundant network guarantees server availability, providing uncompromised reliability and continuity of service. ANS' network completely shields vulnerable corporate email servers from the Internet, protecting against attacks and providing transparent filtering of malicious and nuisance email.

Our services are more cost-effective than installing and administering such services internally, and help free valuable IT resources for more strategic initiatives. Our spam blocking services are tuned to not block legitimate business email, and we enable corporate IT groups to set filtering and policy options appropriate for their business environment.



ANS Spam Plus **Frequently Asked Questions**

Anti-Virus Services

Q - How does ANS' virus protection work?

A - All email messages with file attachments must clear four levels of inspection before being forwarded. These levels include:

1. Filename and Filetype blocking: Specific filenames can be blocked from our network. If our virus engines do not have an updated definition to block a new virus, filename blocking can be used to prevent the virus from reaching customers. Customers can also add and remove filenames to be blocked for their domains.
2. Policy enforcement: Customers can add and remove content types to be blocked for their domains. By default, ANS blocks all files with the Visual Basic (vbs) and executable (exe) content types.
3. Anti-virus engine 1
4. Anti-virus engine 2

If a virus is detected that cannot be cleaned, the email is bounced back to the sender with a message indicating the email contains a virus. The infected document is not included in the bounced message to the sender, to avoid reinfecting the sender's system.

If a virus is detected and can be cleaned, the virus is removed from the attachment and the email is sent to the intended recipient. Text is added to the message indicating the email contained a virus that was removed. The sender of the infected message is also notified that they sent an infected email.

Q - How often does ANS' anti-virus software get updated?

A - Our network looks for library updates from our partners every 10 minutes.

As a development partner with our three anti-virus providers - Sophos, Symantec and Trend Micro - ANS receives alerts of new viruses as soon as they are discovered. When we receive an alert, we take immediate action to block any suspicious email until our anti-virus engines have been updated to detect the new virus.

Q - Is my network protected with my current anti-virus software?

A - There are varying levels of protection provided by anti-virus software. The differing levels of protection depend on a number of factors, including:

1. Desktop anti-virus software can protect systems, but desktop software is subject to significant delays in updating. Virtually all recent virus outbreaks have been email-based and spread extremely fast throughout an enterprise. Organizations simply cannot update all their desktop anti-virus software quickly enough to rely on this protection exclusively.

ANS' system provides the perfect enhancement to desktop anti-virus protection because we update our virus definitions often and quickly. Further, our update blankets your entire email system. In a world where more than 30 new viruses are released every day, using only desktop protection leaves your systems highly vulnerable to virus infection.



ANS Spam Plus **Frequently Asked Questions**

2. If you are using email server anti-virus solutions in combination with desktop anti-virus software, your system has better protection than with desktop software only. However, there are some items to note:
First, the ANS anti-virus system is updated to block new viruses faster than server-based anti-virus solutions. In the best case scenario, both systems might learn about a new virus at the same time (assuming the server solution has the earliest alerts for new viruses). However, ANS can move to deploy interim and final solutions faster since ANS has the staff, tools, and the ability to test and deploy updates quickly. Once a patch is available, ANS implements it across our network in as little as 10 minutes.

Second, ANS' multiple anti-virus engines greatly increase the likelihood a virus will be detected and blocked. Most organizations do not have the resources to deploy and support multiple gateway-based anti-virus solutions.

Q - How does ANS handle viruses in ZIP and other archive files?

A - Like most gateway-based anti-virus solutions, ANS recursively unpacks every archive to scan its contents.

Q - What are TNEF files and why can they be a problem?

A - TNEF is a Microsoft encoding method used by Microsoft Exchange in transmitting messages between Exchange servers. TNEF is also used in Microsoft Outlook when messages are sent in RTF format. Some anti-virus engines have difficulty scanning TNEF encoded files. When an engine has trouble scanning these files, it may forward the incompletely scanned file, which carries the risk of virus infection. ANS decodes TNEF files before passing them through our anti-virus engines, ensuring proper scanning and virus identification.

TNEF encoding is quite common since Microsoft Outlook is among the most used email clients, creating a significant security risk if your anti-virus solution does not process TNEF files.

Security

Q - How does your service protect my email infrastructure?

A - As your email enters our network, we clean and filter it before delivering it to your email server. If your server is unavailable for any reason, we will not bounce your messages. Rather, ANS queues messages until they can be delivered, protecting you from email loss.

Q - How does your service protect my servers?

A - Because your servers are shielded behind our network, your servers are completely invisible to the Internet and cannot be attacked. Regardless of your OS, your patch level, or any vulnerability that may be exploited, your servers and your data are protected. Even when a corporation installs a local hardware solution to protect its email servers, the risk of suffering a disabling denial of service attack is still high. A local solution simply cannot protect as well as the ANS network. To successfully strike our network, an attacker would have to simultaneously disable dozens of servers across seven data centers across three different Tier 1 Internet backbone providers.



ANS Spam Plus **Frequently Asked Questions**

Q - How secure is ANS' network?

A - ANS' data centers are compliant with the American Institute of Certified Public Accountants' SAS 70 standards. SAS 70 standards require a data center's network infrastructure and processes to pass rigorous, third-party testing and demonstrate an environment with the processes and controls to effectively host and exchange corporate data and financial information for enterprise customers. Many companies, especially financial services companies, require credible proof that a service provider has processes and controls in place to provide a stable and secure network that can safely exchange private customer data; meeting SAS 70 standards helps provide that proof. Because of the standards we've adopted, ANS customers are assured greater levels of reliability, availability, and security.

ANS leverages the advantages of our distributed architecture and software to protect our customers from denial of service and hacker attacks. Because our customer's servers sit behind our secure network, they are protected from such threats.

Q - How secure is my email?

A - ANS does not read, copy, distribute, tamper with, change, or otherwise interfere or observe your email beyond our filtering for unwanted content.

Without the ANS service, email is no safer than a postcard once it leaves an email server en route to its destination. Email sent over the Internet is inherently public, and it can travel through servers that do not have the safeguards and security measures provided by the ANS network.

Reporting

Q - What type of reports does ANS offer?

A - ANS offers a variety of reports, based on the services for which you are contracted.

Daily statistics are available in the following formats:

- Master Report with a summation of all domain email traffic
- Delivery Report with information about messages delivered to your domains
- Outgoing Mail Report with information about messages sent from your domains
- Spam Report with information about spam messages blocked
- Rejection Report with data about messages rejected by the various filters
- Virus Report with information about the number and volume of files scanned and the number of viruses detected and cleaned
- Deferral Report with data about the number and volume of messages deferred for delivery when a customer has a mail server outage
- Top Report with information about the top email senders and receivers, spam recipients, and rejected virus recipients.

Q - How often are these reports updated?

A - ANS reports are updated every four to six hours.



ANS Spam Plus **Frequently Asked Questions**

Q - How can I access these reports?

A - Authorized users at your organization can access the ANS Administration Center through a Web browser to view reports at any time.

Disaster Recovery

Q - How reliable is my mail service with ANS managing my email traffic?

A - The ANS solution has built-in redundancy; we guarantee our network will be available to accept, process, and deliver your email 99.999 percent of the time. In fact, since our service inception more than two years ago, our customers have never experienced a service outage.

Q - What happens if one of the ANS data centers goes down?

A - With our advanced network management structure, we can accommodate an offline data center by dynamically spreading network traffic among the remainder of our network. Unlike basic redundant architectures, which only have primary and backup data centers, each ANS data center is independent and interlinked to the entire network, to ensure maximum system availability.

Q - What happens to my email if our network or servers fail?

A - ANS automatically queues all mail for a company's domain for as many as five days. Although unlikely, if your servers are not operational within this time period, ANS can forward mail to another location, or we can create Web-based mailboxes for your users so they can continue to send and receive email even during your outage.

Q - Does ANS store my email permanently?

A - No, ANS does not maintain permanent storage of our customers' email data. Email that is queued temporarily for disaster recovery purposes is never stored permanently.

Q - How does your system know when our mail server is available again?

A - Our data centers scan every 10 minutes to determine if your server or connection is available. Once an unavailable server is restored, we start forwarding stored email immediately in a "flow controlled" fashion.



ANS Spam Plus **Frequently Asked Questions**

Getting Started

Q - What must I do to start using ANS Spam Plus services?

A - Upon signing a service agreement, an ANS Client Service representative will walk you through the set-up procedures. During your orientation, the representative will provide information about changing your MX record to point to our mail network. After that step, there is no hardware to install and no software to configure. Beyond certain site-specific options that you will want to set, we take care of everything.

Q - How many users must I have to use ANS' Spam Plus services?

A - While there is no minimum number of users required, our services are designed as a corporate solution. We do not offer a consumer version of our service.

Q - Do email aliases count toward my total number of users?

A - No. Your total number of users is the number of "unique" users with a specific email address attached to a computer. We refer to these unique users as "seats."

Q - Is there a minimum amount of monthly email traffic required?

A - There is no monthly minimum amount of email traffic to use our services.

Q - Do you scan and filter my internal traffic (i.e., within my organization/LAN/WAN/VPN)?

A - No. ANS only scans email to and from the Internet (i.e., external email domains)

Q - Can I try the ANS Spam Plus services on an evaluation basis?

A - Yes. Your ANS account manager has details about evaluation programs.

Q - How am I billed?

A - ANS bills customers monthly for service usage.

Q - What level of technical support is included in the service agreement?

A - The service comes with 24/7 technical support.

Q - What sort of lag time (latency) can I expect to see after configuring my domain's email delivery for ANS?

A - Virtually none. Our network of distributed servers processes millions of messages daily so any delay from sender to recipient is imperceptible.