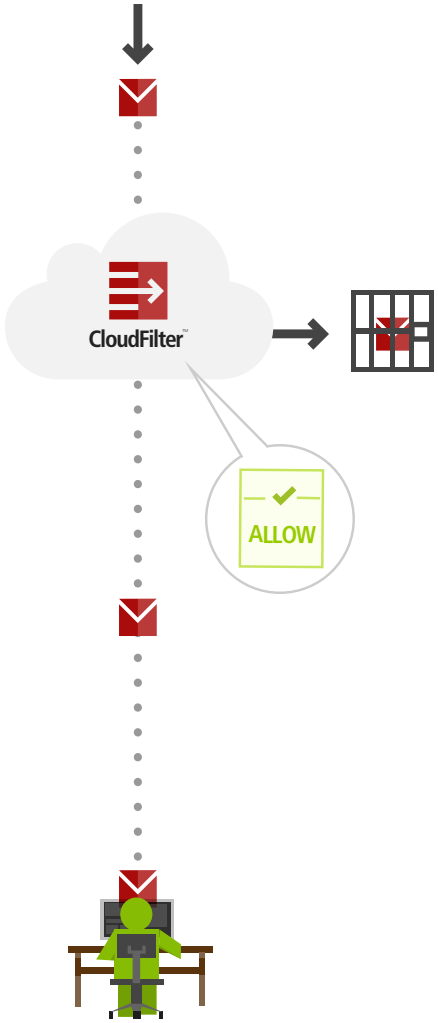
Why allow rules can cause spam leakage (and how to prevent it)



Spammers love to send from major email providers such as @hotmail.com, @yahoo.com, @gmail.com, and even your own domain. This makes their emails seem legitimate. So, let's say someone sends you some spam from @gmail.com when you have a rule to "allow all email from @gmail.com".

Normally when your email is routed through CloudFilter, a battery of tests and scans are performed which show whether or not a message is spam. If it is spam, CloudFilter quarantines the message.

Unless

If a bad allow rule has been added for a domain, user or user group, then CloudFilter is forced to obey the rule rather than the scan results. It will let all email from that domain pass through without being flagged as spam. It's a bit like a "get out of jail free" card for spam.

When allow rules let through all messages from major email providers and your own domain your users will probably get spam, and it may even appear to users that CloudFilter isn't working. However, the real problem is that bad allow rules are keeping CloudFilter from scanning those emails at all.

How to create good allow rules

Every allow rule you create is an additional 'hole' in your email security, so be sure to add them carefully. Here are some examples of rules which will deliver either good or bad results:

Bad

allow @gmail.com to @yourdomain.com - or - **allow @yourdomain to @yourdomain**

Spam sent from anything@gmail.com or anything@yourdomain.com will get through to all your users regardless of the spam score.

Good

allow bob.smith@gmail.com to userabc@yourdomain.com

This is much safer. By limiting the rule to sending and receiving users, the likelyhood that you'll receive spam is cut drastically.