Alt-N SecurityGateway for Email Servers - Universal Email Security Gateway
Manufacturer: Alt-N Technologies| Model: Standard | Origin: Texas, USA | Website: www.altn.com | Price: £204 for up to 25 users

Simplicity	Value	Documentation
3.5/5	5/5	4.5/5
Functionality	Performance	Overall
4/5	4.5/5	86%

The Good
Alt-N SecurityGateway is competitively priced and simple to set up*. It will ensure efficient and hassle free message spooling once up and running.

The Bad
* Though the set-up is simple, full configuration has a lot of options, which is good for granularity, but not for a novice. Currently extension filtering does not check within archives, though antivirus does.

Testing
Real-time: during a seven-day trial period SecurityGateway detected and stopped everything it claimed it would; spam, malware, relaying and SPF errors.

Attachment filtering: the service works using the last extension, so bill.pdf.exe and bill.exe will both be caught. At the moment it does not check archives, but this is on the roadmap. Archives are currently scanned by antivirus.

Manual malware: all exe's and scr's thrown at the program were detected and caught with a signature and outbreak protection seems to have stop all unknown exe's and scr's. During testing it missed one out of two DOCM files – Barracuda missed both and still does. It is good practice to block these outright. No email security gateway can really claim 100% catch rate.

Conclusion
I stumbled upon Alt-N while looking for a Microsoft Exchange alterative and then noticed they did an email security gateway. On another project I was hunting around for email security gateways and was struggling to find one that was not a piece of hardware or needed virtualisation to install. There are quite a lot which install within Windows, but few are vendor agnostic.

Before reviewing and testing version 3.0 I tested out the previous version, which by default was just Clam AV with Kaspersky and Cyren Outbreak protection as an add-on. Version 3.0 only has one option. The previous version caught everything from 'the wild' and stopped everything I threw at it manually.

Version 3.0 has ClamAV, which pretty much every single gateway uses, as it is free and open source. Cyren AV has replaced the Kaspersky engine. From leaving it running for a few days it has caught everything spam and virus wise. On manual testing it missed one file (DOCM), though it is good practice to block common file extensions (EXE, SCR and Macro Office files etc).

SecurityGateway is under half the cost of Barracuda Virtual Firewall and has a higher catch rate. Barracuda in real time and manual testing has let in twice as much as SecurityGateway did. One big

attraction for me is that, SecurityGateway is installed straight onto the server, no virtual machine to set up, or additional hardware required.

Vendor Statement
SecurityGateway for Email Servers combines nearly two decades of email security expertise with proven security technologies to protect message traffic from malicious attacks, message tampering and email address identity theft. Using multiple security methods, SecurityGateway assures the accurate delivery of legitimate email while minimizing the potential of false positives.

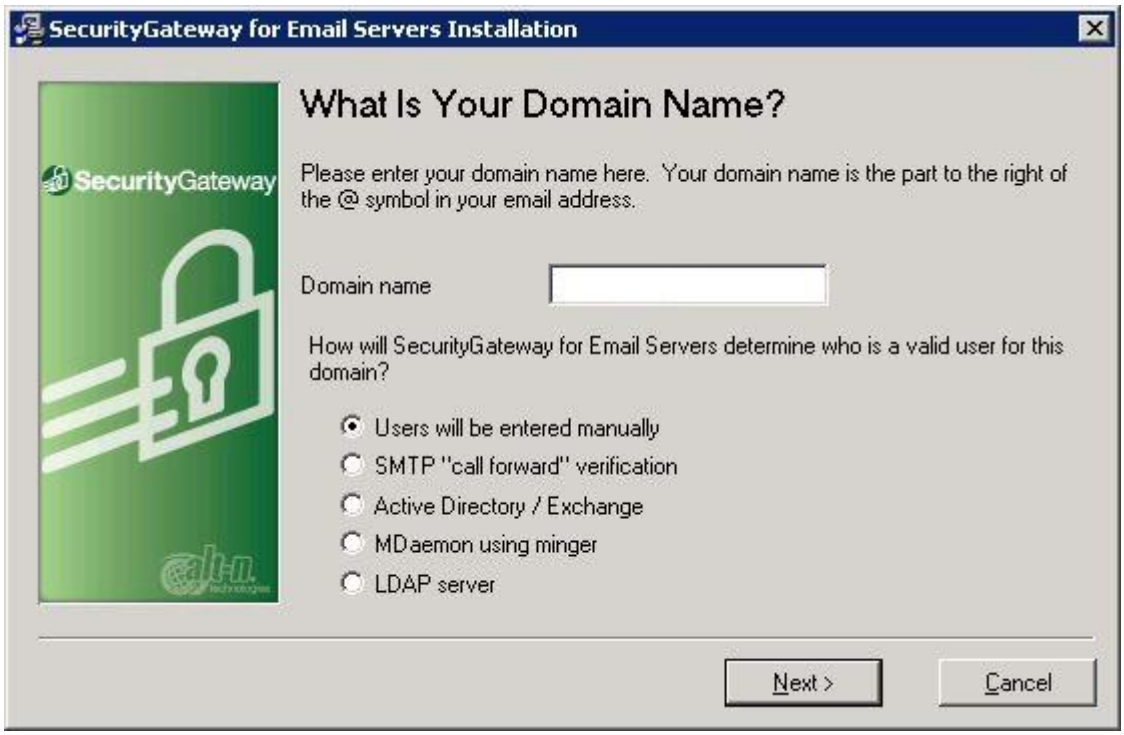
SecurityGateway incorporates multiple AV engines and proactive Outbreak Protection technology, combined with additional signature recognition and heuristic analysis, to detect viruses, spam, phishing, spyware and other types of unwanted and harmful email…

What Does This Solve?
Simple! Unwanted emails: scams, spam, infected emails, phishing emails and basic data leakage. Email servers get shedloads of virus, spam and SMTP relay attempts daily.

What Can SecurityGateway Do?
SecurityGateway scans all emails with two antivirus engines (plus an outbreak engine for new viruses and spam waves) as well as basic data leakage prevention rules.

Installation
Installing the product is of course the first step and is fairly quick. Just install and open the ports.

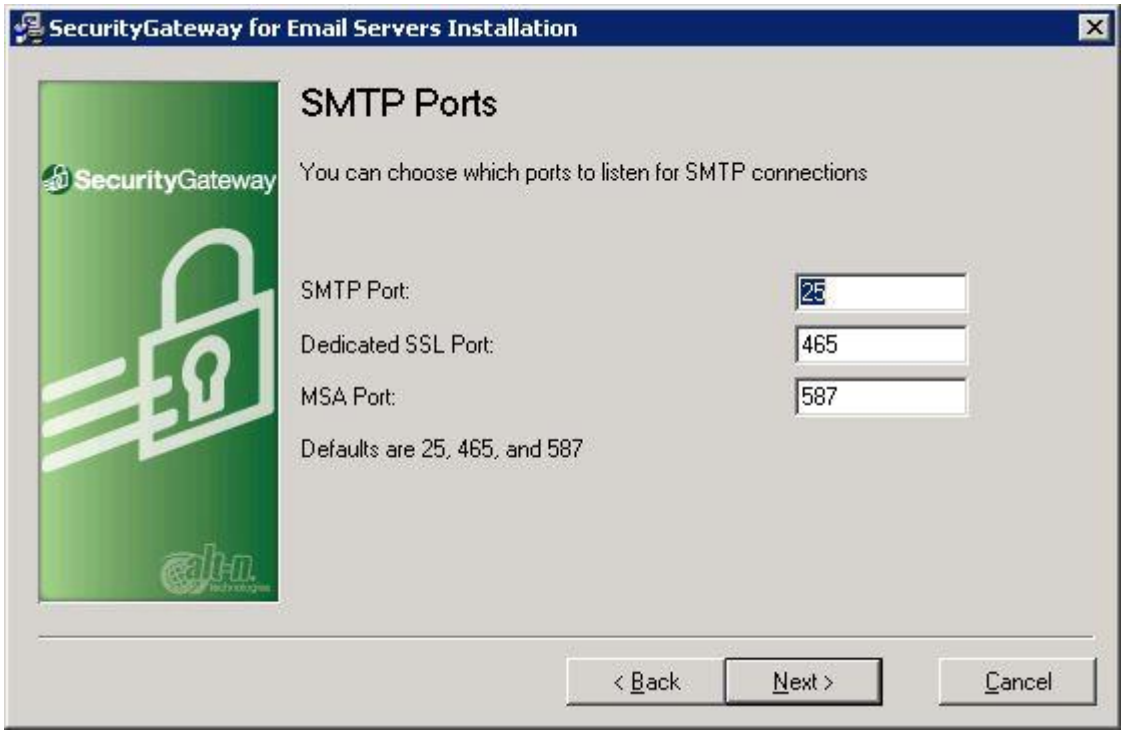
Customer information, which is probably for licensing.



Enter the email domain and specify how users should be added. If you select the top one, the gateway will reject non listed addresses.

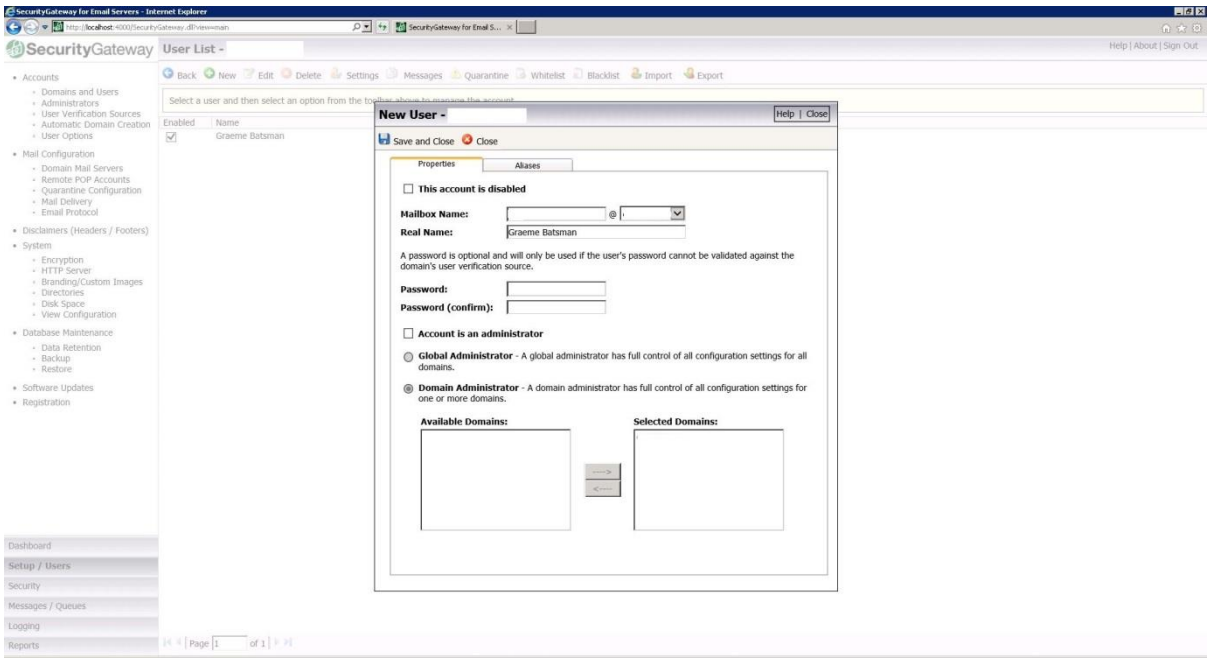
Enter the IP or domain of the actual email server. The gateway receives the email and forwards it on.

Setup administrator account and password.

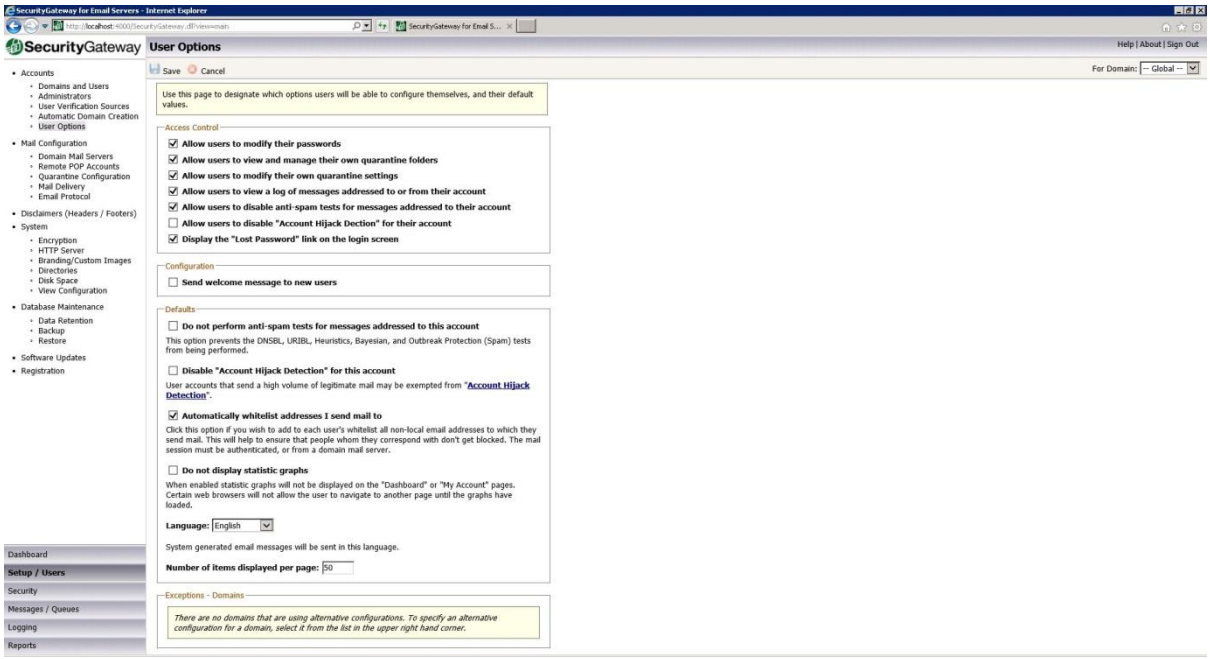


Default ports are typically fine.

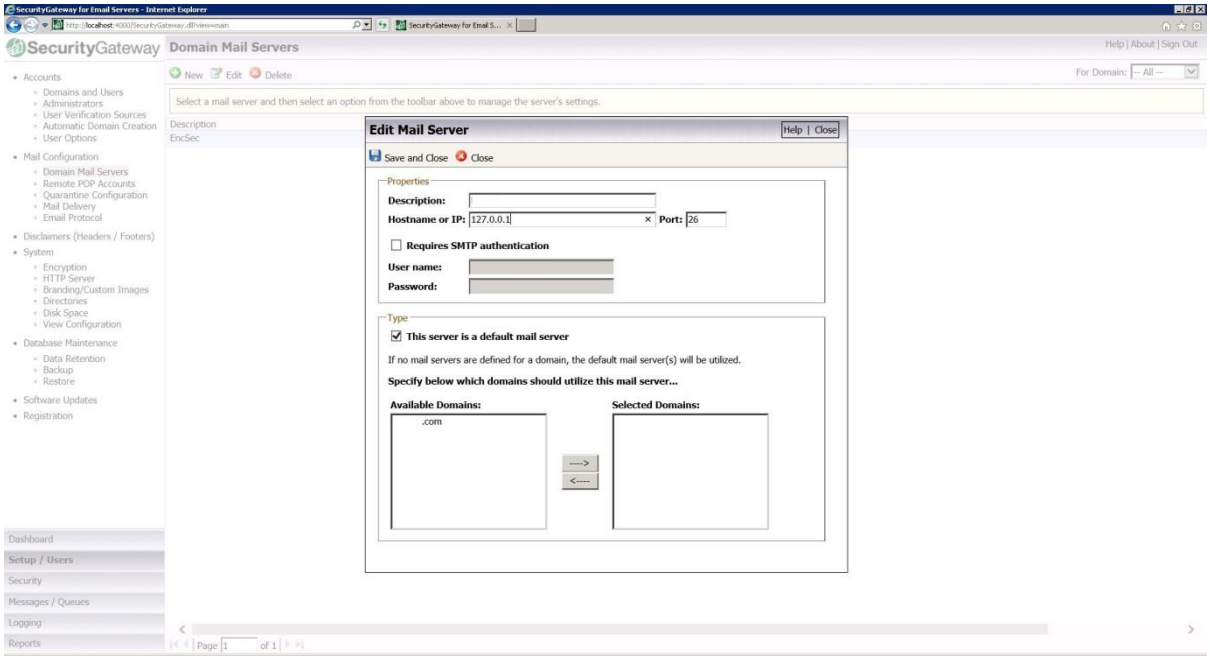
Enter a required URL for admin and quarantine access. 4443 is handy if webmail is running on 443.



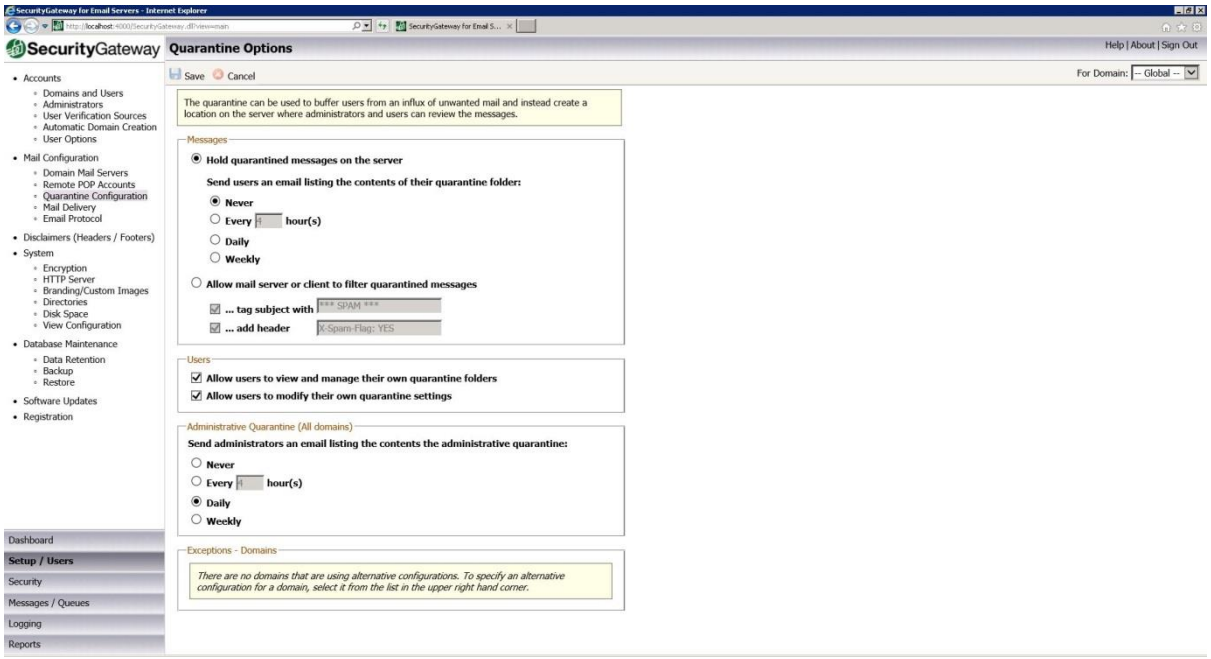
Adding a new user is simple, just add the mailbox and person's name and click save and close.



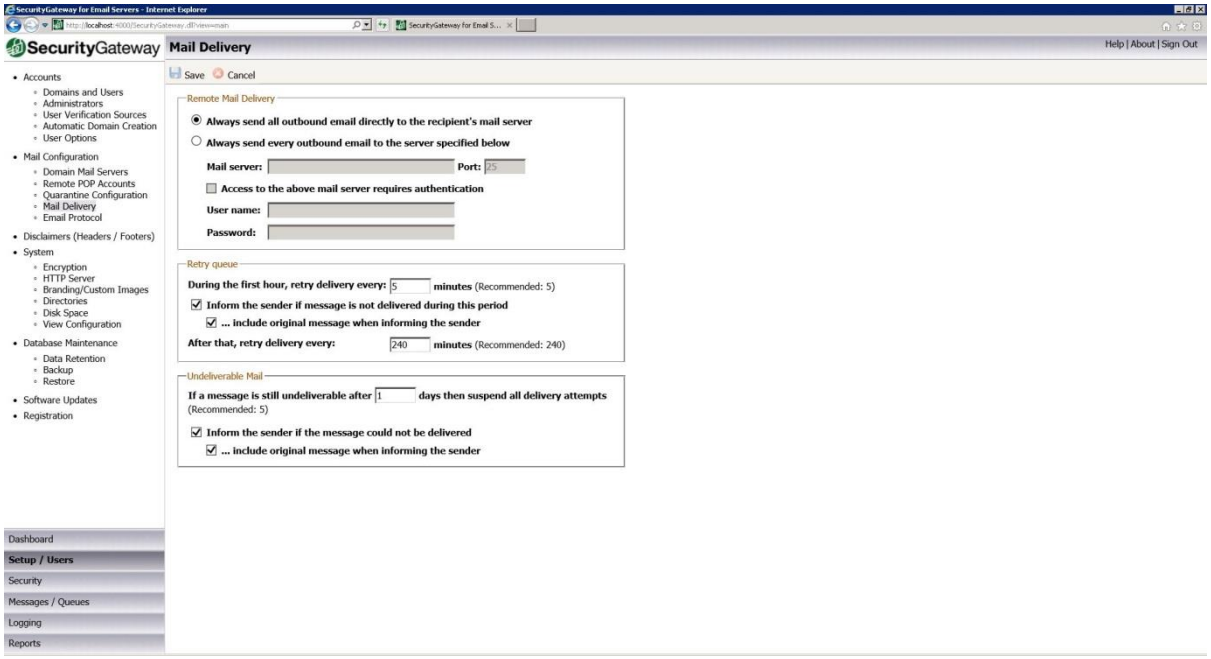
Settings that control what users can do when viewing their quarantine account.



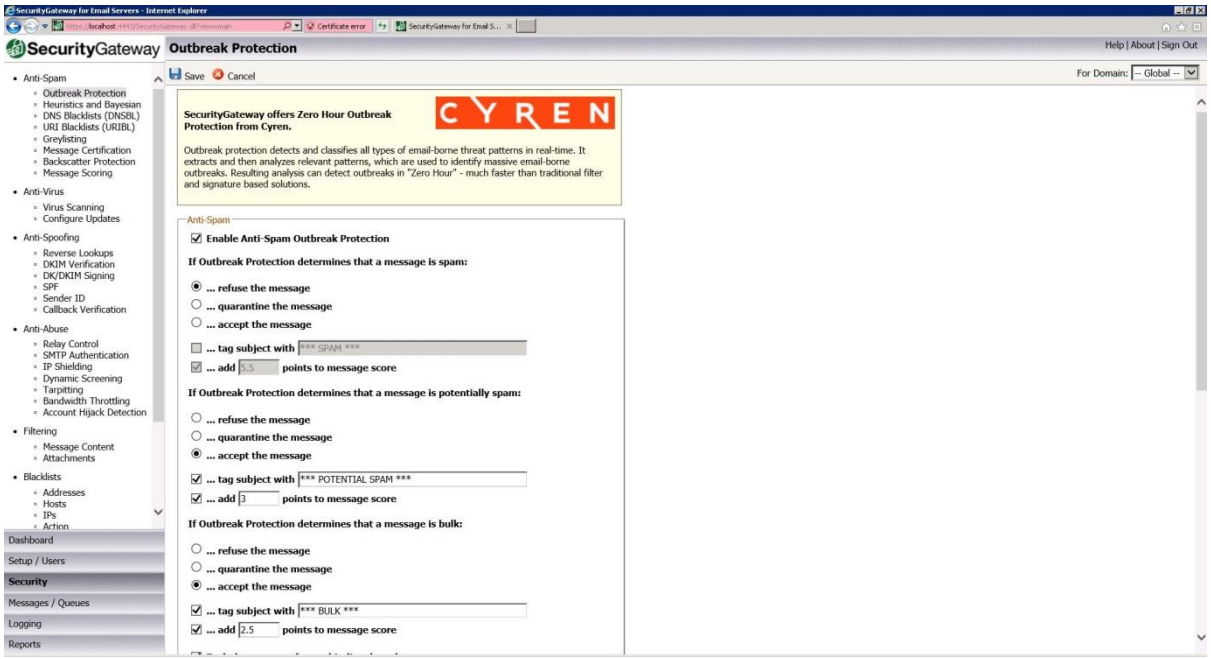
Where you specify the end mail servers IP or domain name.



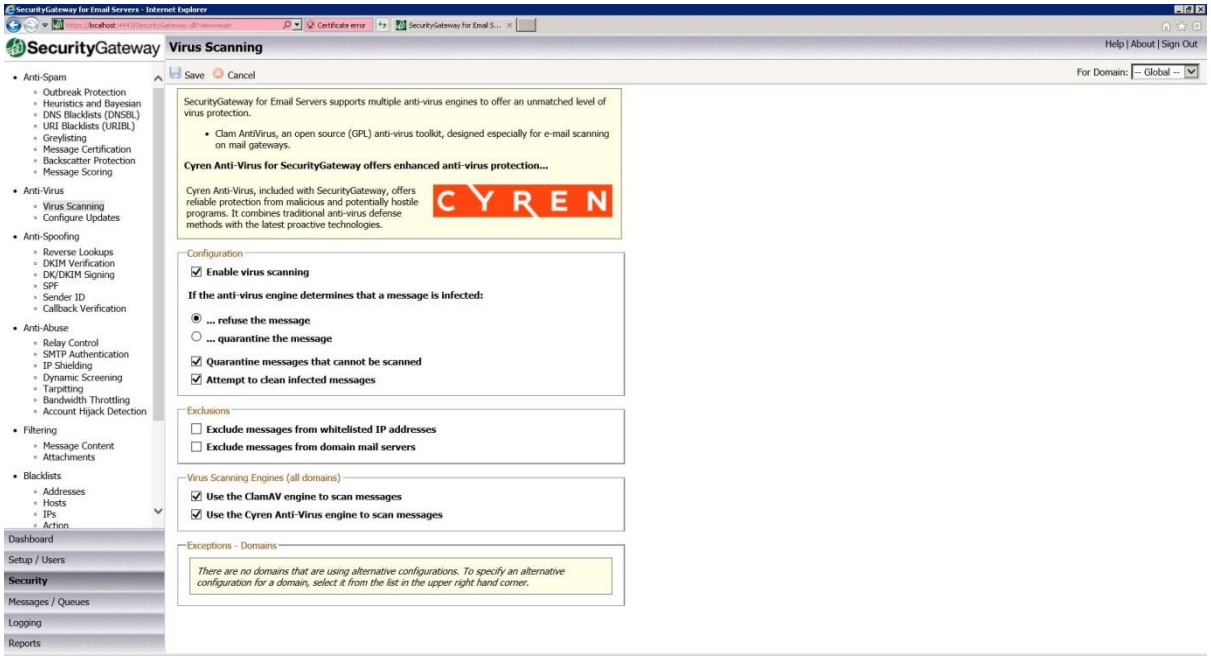
Quarantine settings.



Outbound SMTP settings.



Outbreak protection settings.

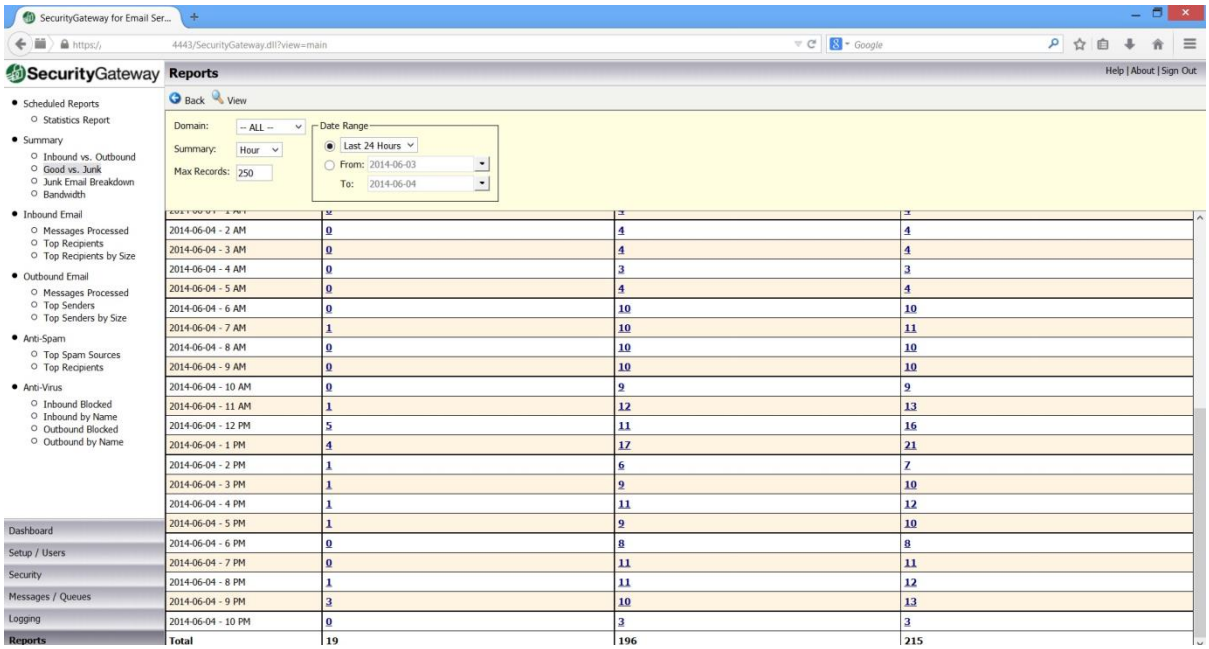


Antivirus settings - very simple.

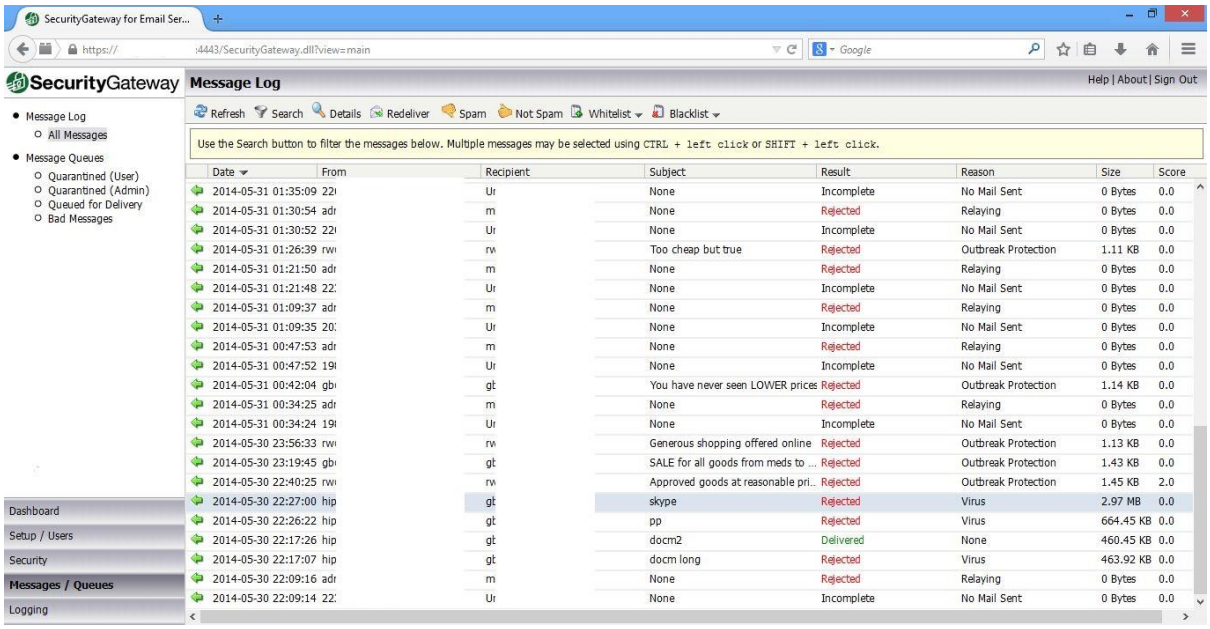
E: graeme@datasecurityexpert.co.uk | A: Graeme Batsman, 78 York Street, London, W1H 1DP
T: 020 3371 0495 | M: 07909 474479 | Follow Me On Twitter: @graemebatsman

Reporting

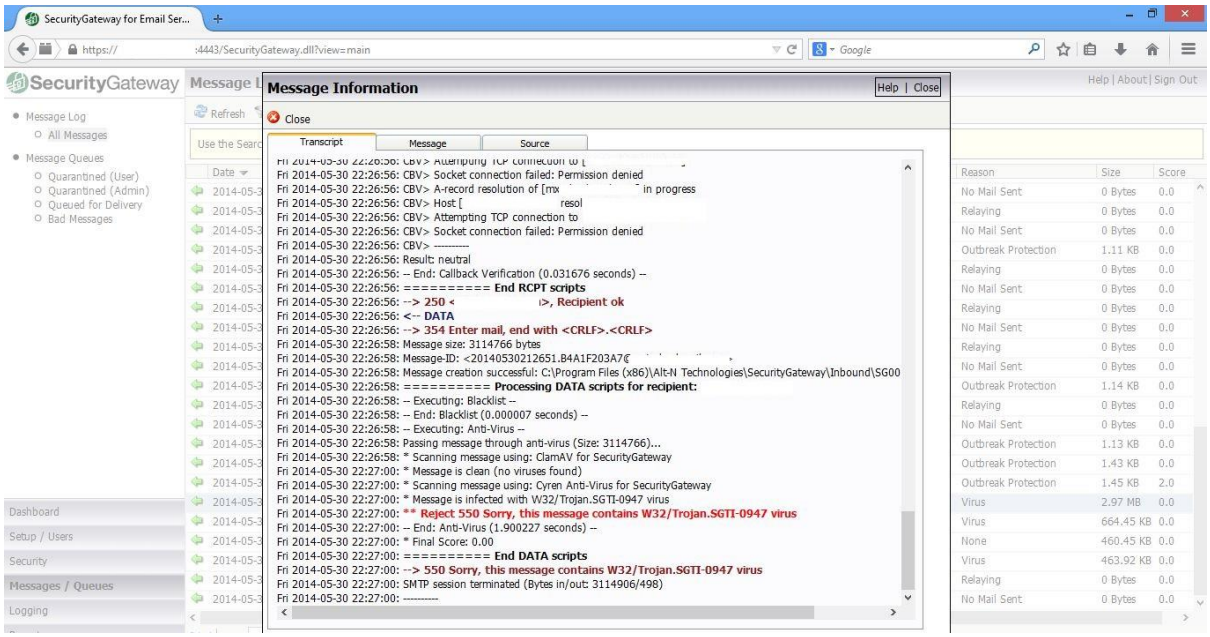
SecurityGateway offers various charts and reports. Some are shown below.



One of the reports - good vs junk emails.



Message log which shows: viruses, spam and clean messages.



Detailed analysis of an email.