



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 alternative 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.

The screenshot shows a Windows-style installation window titled "SecurityGateway for Email Servers Installation". On the left is a green vertical banner with the SecurityGateway logo and a large padlock icon. The main area is titled "Customer Information" and contains the text "Please enter the following information." Below this are three input fields: "Name" with the text "Graeme Batsman", "Company" (empty), and "Country" with a dropdown menu showing "United Kingdom [GB]". At the bottom of the main area is a disclaimer: "The information you provide will not be sold to third parties. It will only be used for technical support purposes and for product related communications to assist, should you require." At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

Customer information, which is probably for licensing.



SecurityGateway for Email Servers Installation

What Is Your Domain Name?

Please enter your domain name here. Your domain name is the part to the right of the @ symbol in your email address.

Domain name:

How will SecurityGateway for Email Servers determine who is a valid user for this domain?

- ☒ Users will be entered manually
- ☐ SMTP "call forward" verification
- ☐ Active Directory / Exchange
- ☐ MDAemon using minger
- ☐ LDAP server

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

SecurityGateway for Email Servers Installation

Email Server

SecurityGateway for Email Servers will send all email for domain encsec.com to this email server:

Description:

Host Name or IP: Port:

☐ Requires SMTP authentication

User name:

Password:

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



SecurityGateway for Email Servers Installation

Set Up Administrator Account

The created account will be a global administrator. You can set up more accounts from within SecurityGateway later.

☒ Local User - member of local domain (encsec.com)
☐ External - not a member of local domain (encsec.com)

Full name:

Mailbox (don't include a domain name):

Password:

Verify Password:

< Back Next > Cancel

Setup administrator account and password.

SecurityGateway for Email Servers Installation

SMTP Ports

You can choose which ports to listen for SMTP connections

SMTP Port:

Dedicated SSL Port:

MSA Port:

Defaults are 25, 465, and 587

< Back Next > Cancel

Default ports are typically fine.



SecurityGateway for Email Servers Installation

HTTP User Interface

The HTTP Host Name will be used to construct login links for the quarantine summary report and other system generated email messages.

HTTP Host Name: (ex: sg.company.mail)

You can choose which ports to listen on for HTTP connections

HTTP Port: Default: 4000

HTTPS Port: Default: 4443

< Back Next > Cancel

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

SecurityGateway for Email Servers - Internet Explorer

http://localhost:4000/SecurityGateway.dll?view=main

SecurityGateway User List

Back New Edit Delete Settings Messages Quarantine Whitelist Blacklist Import Export

Select a user and then select an option from the toolbar above to manage the account.

Enabled	Name
<input checked="" type="checkbox"/>	Graeme Batsman

New User Help | Close

Save and Close Close

☐ This account is disabled

Mailbox Name: @

Real Name:

A password is optional and will only be used if the user's password cannot be validated against the domain's user verification source.

Password:

Password (confirm):

☐ Account is an administrator

☐ Global Administrator - A global administrator has full control of all configuration settings for all domains.

☒ Domain Administrator - A domain administrator has full control of all configuration settings for one or more domains.

Available Domains:

Selected Domains:

Dashboard
Setup / Users
Security
Messages / Quines
Logging
Reports

Page 1 of 1

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



The screenshot shows the 'User Options' configuration page in the SecurityGateway web interface. The left sidebar contains a navigation menu with categories like Accounts, Mail Configuration, Disclaimers, System, Database Maintenance, Software Updates, and Registration. The main content area is titled 'User Options' and includes a 'Save' button. It contains several sections: 'Access Control' with checkboxes for allowing users to modify passwords, view and manage quarantine folders, modify quarantine settings, view message logs, disable anti-spam tests, and disable 'Account Hijack Detection'. There is also a checkbox for displaying a 'Lost Password' link. The 'Configuration' section has a checkbox for sending a welcome message to new users. The 'Defaults' section includes checkboxes for not performing anti-spam tests, disabling 'Account Hijack Detection', automatically whitelisting addresses, and not displaying statistic graphs. A language dropdown is set to 'English', and the 'Number of items displayed per page' is set to 50. An 'Exceptions - Domains' section at the bottom states that there are no domains using alternative configurations.

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

The screenshot shows the 'Domain Mail Servers' configuration page. An 'Edit Mail Server' dialog box is open, allowing configuration of a mail server. The dialog has 'Save and Close' and 'Close' buttons. It includes a 'Description' field, a 'Hostname or IP' field (containing '127.0.0.1'), and a 'Port' field (containing '26'). There is a checkbox for 'Requires SMTP authentication'. Below these are fields for 'User name' and 'Password'. The 'Type' section has a checked checkbox for 'This server is a default mail server'. At the bottom, there are two lists: 'Available Domains' (containing '.com') and 'Selected Domains' (empty), with arrows indicating the ability to move domains between them.

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

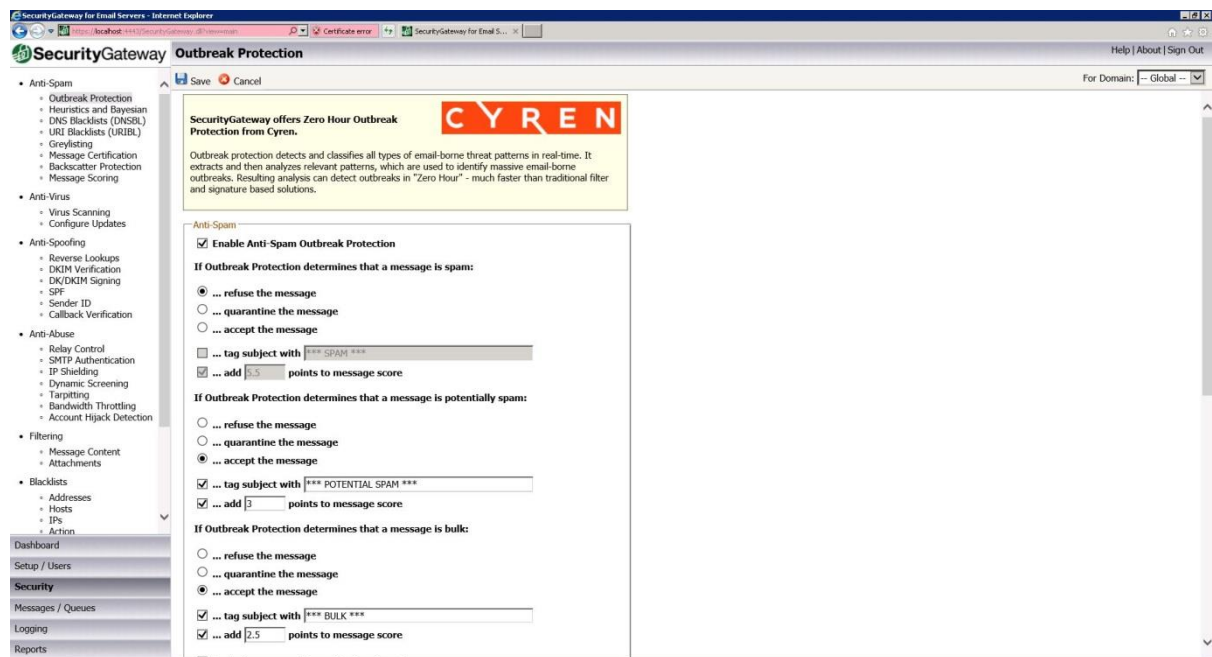


The screenshot shows the 'Quarantine Options' configuration page in the SecurityGateway web interface. The left sidebar contains a navigation menu with categories like Accounts, Mail Configuration, Disclaimers, System, Database Maintenance, Software Updates, and Registration. The main content area is titled 'Quarantine Options' and includes a 'Save' button and a 'Cancel' button. The page is divided into several sections: 'Messages' (with options for 'Hold quarantined messages on the server' and 'Allow mail server or client to filter quarantined messages'), 'Users' (with checkboxes for 'Allow users to view and manage their own quarantine folders' and 'Allow users to modify their own quarantine settings'), 'Administrative Quarantine (All domains)' (with options for 'Send administrators an email listing the contents of the administrative quarantine'), and 'Exceptions - Domains' (with a note about alternative configurations). The 'For Domain' dropdown is set to 'Global'.

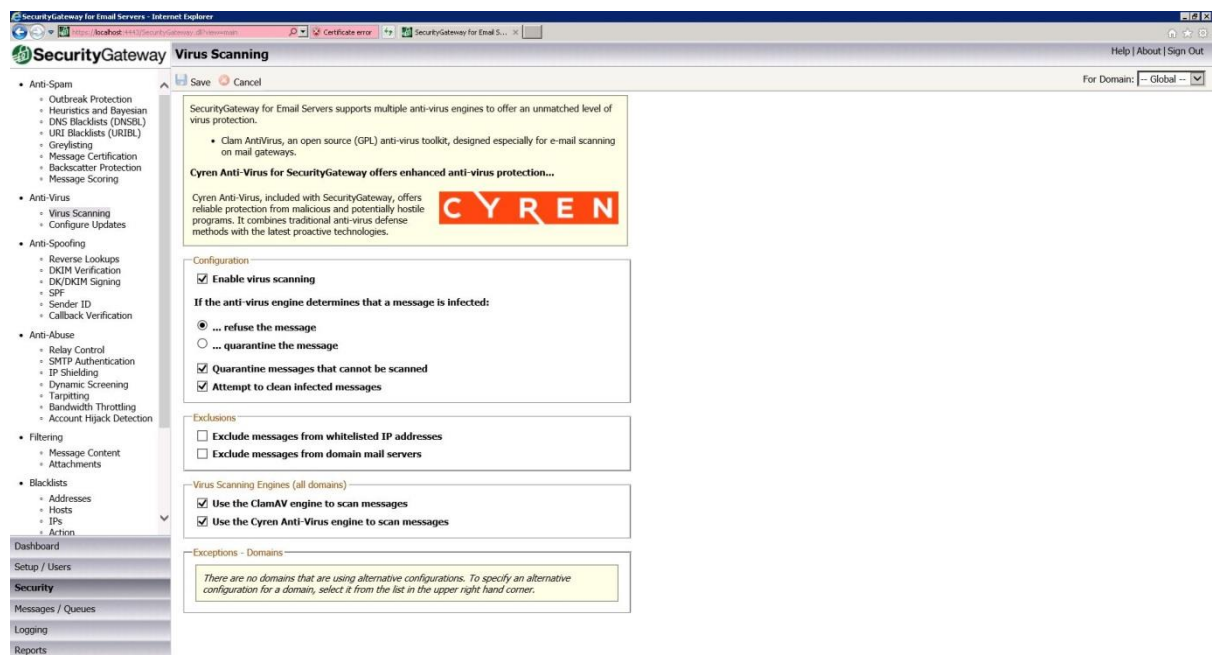
Quarantine settings.

The screenshot shows the 'Mail Delivery' configuration page in the SecurityGateway web interface. The left sidebar is the same as the previous screenshot. The main content area is titled 'Mail Delivery' and includes a 'Save' button and a 'Cancel' button. The page is divided into several sections: 'Remote Mail Delivery' (with options for 'Always send all outbound email directly to the recipient's mail server' and 'Always send every outbound email to the server specified below'), 'Retry queue' (with options for 'During the first hour, retry delivery every' and 'After that, retry delivery every'), and 'Undeliverable Mail' (with options for 'If a message is still undeliverable after' and 'Inform the sender if the message could not be delivered'). The 'Mail server' field is set to 'smtp.gmail.com' and the 'Port' is set to '25'. The 'User name' field is set to 'smtp.gmail.com' and the 'Password' field is empty.

Outbound SMTP settings.



Outbreak protection settings.



Antivirus settings - very simple.



Reporting

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

The screenshot shows the 'Reports' section of the SecurityGateway interface. It includes a sidebar with navigation links and a main table displaying email statistics for the date 2014-06-04. The table has columns for time intervals, and counts for various categories. A 'Total' row at the bottom summarizes the data.

Time Interval	Messages Processed	Top Recipients	Top Senders
2014-06-04 - 2 AM	0	4	4
2014-06-04 - 3 AM	0	4	4
2014-06-04 - 4 AM	0	3	3
2014-06-04 - 5 AM	0	4	4
2014-06-04 - 6 AM	0	10	10
2014-06-04 - 7 AM	1	10	11
2014-06-04 - 8 AM	0	10	10
2014-06-04 - 9 AM	0	10	10
2014-06-04 - 10 AM	0	9	9
2014-06-04 - 11 AM	1	12	13
2014-06-04 - 12 PM	5	11	16
2014-06-04 - 1 PM	4	12	21
2014-06-04 - 2 PM	1	6	7
2014-06-04 - 3 PM	1	9	10
2014-06-04 - 4 PM	1	11	12
2014-06-04 - 5 PM	1	9	10
2014-06-04 - 6 PM	0	8	8
2014-06-04 - 7 PM	0	11	11
2014-06-04 - 8 PM	1	11	12
2014-06-04 - 9 PM	3	10	13
2014-06-04 - 10 PM	0	3	3
Total	19	196	215

One of the reports - good vs junk emails.

The screenshot shows the 'Message Log' section of the SecurityGateway interface. It displays a table of email messages with columns for Date, From, Recipient, Subject, Result, Reason, Size, and Score. The messages are sorted by date, showing a mix of clean, spam, and virus-infected emails.

Date	From	Recipient	Subject	Result	Reason	Size	Score
2014-05-31 01:35:09	22i	Ur	None	Incomplete	No Mail Sent	0 Bytes	0.0
2014-05-31 01:30:54	adr	m	None	Rejected	Relaying	0 Bytes	0.0
2014-05-31 01:30:52	22i	Ur	None	Incomplete	No Mail Sent	0 Bytes	0.0
2014-05-31 01:26:39	rw	rw	Too cheap but true	Rejected	Outbreak Protection	1.11 KB	0.0
2014-05-31 01:21:50	adr	m	None	Rejected	Relaying	0 Bytes	0.0
2014-05-31 01:21:48	22i	Ur	None	Incomplete	No Mail Sent	0 Bytes	0.0
2014-05-31 01:09:37	adr	m	None	Rejected	Relaying	0 Bytes	0.0
2014-05-31 01:09:35	20i	Ur	None	Incomplete	No Mail Sent	0 Bytes	0.0
2014-05-31 00:47:53	adr	m	None	Rejected	Relaying	0 Bytes	0.0
2014-05-31 00:47:52	19i	Ur	None	Incomplete	No Mail Sent	0 Bytes	0.0
2014-05-31 00:42:04	gb	gt	You have never seen LOWER prices	Rejected	Outbreak Protection	1.14 KB	0.0
2014-05-31 00:34:25	adr	m	None	Rejected	Relaying	0 Bytes	0.0
2014-05-31 00:34:24	19i	Ur	None	Incomplete	No Mail Sent	0 Bytes	0.0
2014-05-30 23:56:33	rw	rw	Generous shopping offered online	Rejected	Outbreak Protection	1.13 KB	0.0
2014-05-30 23:19:45	gb	gt	SALE for all goods from meds to ...	Rejected	Outbreak Protection	1.43 KB	0.0
2014-05-30 22:40:25	rw	rw	Approved goods at reasonable pri...	Rejected	Outbreak Protection	1.45 KB	2.0
2014-05-30 22:27:00	hip	gt	skype	Rejected	Virus	2.97 MB	0.0
2014-05-30 22:17:26	hip	gt	docm2	Delivered	None	460.45 KB	0.0
2014-05-30 22:17:07	hip	gt	docm long	Rejected	Virus	463.92 KB	0.0
2014-05-30 22:09:16	adr	m	None	Rejected	Relaying	0 Bytes	0.0
2014-05-30 22:09:14	22i	Ur	None	Incomplete	No Mail Sent	0 Bytes	0.0

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



Message Information

Transcript

2014-05-30 22:26:56: CBV> Attempting TCP connection to [redacted]
2014-05-30 22:26:56: CBV> Socket connection failed: Permission denied
2014-05-30 22:26:56: CBV> A-record resolution of [redacted] in progress
2014-05-30 22:26:56: CBV> Host [redacted] resolved
2014-05-30 22:26:56: CBV> Attempting TCP connection to [redacted]
2014-05-30 22:26:56: CBV> Socket connection failed: Permission denied
2014-05-30 22:26:56: CBV> -----
2014-05-30 22:26:56: Result: neutral
2014-05-30 22:26:56: -- End: Callback Verification (0.031676 seconds) --
2014-05-30 22:26:56: ===== End RCPT scripts
2014-05-30 22:26:56: --> 250 4
2014-05-30 22:26:56: <- DATA
2014-05-30 22:26:56: <-> 354 Enter mail, end with <CRLF>,<CRLF>
2014-05-30 22:26:58: Message size: 3114766 bytes
2014-05-30 22:26:58: Message-ID: <20140530212651.B4A1F203A7@redacted>
2014-05-30 22:26:58: Message creation successful: C:\Program Files (x86)\Alt-N Technologies\SecurityGateway\Inbound\SG00
2014-05-30 22:26:58: ===== Processing DATA scripts for recipient:
2014-05-30 22:26:58: -- Executing: Blacklist --
2014-05-30 22:26:58: -- End: Blacklist (0.000007 seconds) --
2014-05-30 22:26:58: -- Executing: Anti-Virus --
2014-05-30 22:26:58: Passing message through anti-virus (Size: 3114766)...
2014-05-30 22:26:58: * Scanning message using: ClamAV for SecurityGateway
2014-05-30 22:27:00: * Message is clean (no viruses found)
2014-05-30 22:27:00: * Scanning message using: Cyren Anti-Virus for SecurityGateway
2014-05-30 22:27:00: * Message is infected with W32/Trojan.SGTI-0947 virus
2014-05-30 22:27:00: ** Reject 550 Sorry, this message contains W32/Trojan.SGTI-0947 virus
2014-05-30 22:27:00: -- End: Anti-Virus (1.900227 seconds) --
2014-05-30 22:27:00: * Final Score: 0.00
2014-05-30 22:27:00: ===== End DATA scripts
2014-05-30 22:27:00: --> 550 Sorry, this message contains W32/Trojan.SGTI-0947 virus
2014-05-30 22:27:00: SMTP session terminated (Bytes in/out: 3114906/498)
2014-05-30 22:27:00: -----

Reason	Size	Score
No Mail Sent	0 Bytes	0.0
Relaying	0 Bytes	0.0
No Mail Sent	0 Bytes	0.0
Outbreak Protection	1.11 KB	0.0
Relaying	0 Bytes	0.0
No Mail Sent	0 Bytes	0.0
Relaying	0 Bytes	0.0
No Mail Sent	0 Bytes	0.0
Relaying	0 Bytes	0.0
No Mail Sent	0 Bytes	0.0
Outbreak Protection	1.14 KB	0.0
Relaying	0 Bytes	0.0
No Mail Sent	0 Bytes	0.0
Outbreak Protection	1.13 KB	0.0
Outbreak Protection	1.43 KB	0.0
Outbreak Protection	1.45 KB	2.0
Virus	2.97 MB	0.0
Virus	664.45 KB	0.0
None	460.45 KB	0.0
Virus	463.92 KB	0.0
Relaying	0 Bytes	0.0
No Mail Sent	0 Bytes	0.0

Detailed analysis of an email.