noSpamproxy®

Version 14.0

Net at Work
Building IT-Excellence.

Alle Funktionen auf einen Blick

The three NoSpamProxy® modules Protection, Encryption and Large Files offer reliable protection against spam and malware, secure email encryption and simple and easy sending of large files.

In addition to these security-focused modules, the Disclaimer and Additional server options provide functionalities for managing email disclaimers as well as for implementing high-availability solutions.

NoSpamProxy Suite includes the modules Protection, Encryption and Large Files as well as the Disclaimer option.

Inhalt

Anti-Spam Features

Feature NoSpamProxy	Protection	Encryption	Large Files	Suite
Level of Trust (acquiring information on e-mail communication, creation of address pairings)	X			X
Realtime Blocklists (RBLs)	X			X
Email Attachment Filtering				
• Based on file name, content type and size; optional allowlisting	X	X[4]	X	X
• Email blocking	X		X	X
• Attachment removal	X		X	X
Attachment upload to the Web Portal; optional quarantine	X[4]	X[4]	X	X[4]
Content filter for files in archives	X		X	X
Different content filters for files transferred via the Web Portal	X		X	X
Blocking of suspicious emails	X			X
Filtering of emails based on specific characters	X			X
Core Antispam Engine	X			X
Integrated Malware Scanner	X			X
Sandbox-based attachement inspection	X[5]			X
Scanning of emails for viruses using On-access virus scanners	X			X
DLP – Keyword-based filtering of emails	X			X
DLP – Notification about keyword matches	X			X
Support for Certified Senders Alliance (ECO)	X			X
Greylisting	X			X
Filtering of emails containing suspicious links (SUR-BL, Spamhaus Domain Blocklist, UriBL, 32Guards)	X			X
SpamAssassin support (via SpamD)	X			X
Advanced header checking for corporate domains in sender addresses	X			X
Extensive checking of Header-FROM and Header-TO	X			X
Defining a threshold of outbound e-mails per hour/ per day (Flow Guard)	X			X

Feature NoSpamProxy	Protection	Encryption	Large Files	Suite
Content Disarm and Reconstruction/Office file preview as PDF file	X			X
Content Disarm and Reconstruction/Removal of active and unknown content in PDF files	X			X
Verification of reverse-DNS entries for delivering IP addresses (RDNS check)	X			X
Verification of RDNS entry resolving to the delivering IP address	X			X
Verification of A record availability for the Envelope-Sender Domain	X			X
Verification of sender domain consistency between email envelope and email header	X			X
Check of whether the display name contains a corporate domain (or one of its subdomains)	X			X
Check of whether the display name contains an obfuscated corporate domain (or one of its subdomains)	X			X
Check of whether a domain contained in the display name differs from the domain contained in the email address	X			X
Check of whether the Header-FROM contains more than one email address	X			X
Verification of SPF, DKIM, DMARC and ARC	X			X
Verification through 32Guards, a meta data system that evaluates the hash values of an e-mail	X			X
Check of whether emails were transferred via a TLS-secured connection	X			X
ICAP Client support	X			X
URL Safeguard – Prevention of access to malicious content by rewriting links	X			X
URL Safeguard – Deactivation of links contained in emails	X			X
CxO Fraud Detection – Protection against attacks by matching names with corporate users	X			X

1) Requires a locally installed on-access virus scanner.
2) Requires the digiSeal server from secrypt.
3) High availability with multiple servers requires an additional server license..
4) Requires an appropriate Large Files license.
5) Requires an appropriate Sandbox Service license.

Signature and Encryption Features

Feature NoSpamProxy	Protection	Encryption	Large Files	Suite
SSL/TLS- based encryption of SMTP connections				
• Opportunistic encryption	X	X	X	X
• Forced encryption for specific domains	X	X	X	X
Automatic "Best Practices configuration" for TLS 1.2/1.3 and perfect forward secrecy and deactivation of weak ciphers	X	X	X	X
DANE support	X	X	X	X
Signing of emails using S/MIME or PGP		X		X
Supports S/MIME 4.0		X		X
Encryption of emails using S/MIME or PGP		X		X
Verification of signatures for incoming, signed emails (S/MIME and PGP)		X		X
Decryption of incoming, encrypted messages (S/MIME and PGP)		X		X
RSASSA PSS Signature support (e.g. for EDI@ Energy policy)		X		X
Automatic collection of certificates from incoming emails (S/MIME only)		X		X
PDF Mail (the email including all attachments is converted into a password-encrypted PDF)		X		X
With PDF Mail, attachments can be optionally sent via the Web Portal		X		X
Email queue and key material requests (S/MIME or password for PDF Mail) via email to communication partners		X		X
Encryption of attached PDF documents with password		X		X
• Sending PDF passwords by text message		X		X
Web Portal • Reply function for PDF Mail • Storage of passwords for PDF Mail • Notification if password not yet set		X		X
Management of PDF encryption via tags in the subject line		X		X
Custom designs for all emails generated by NoSpamProxy	X	X	X	X
Custom designs for PDF mails based on sender's address		X		X
Management of encryption options via Microsoft Outlook Add-In		X		X

Feature NoSpamProxy	Protection	Encryption	Large Files	Suite
Permanent decryption of PDF attachments via Microsoft Outlook Add-In		X		X
Application of qualified signatures to attached documents[2]		X		X
Checking of qualified signatures for attachments to incoming emails[2]		X		X
Verification report on incoming emails provides information on encryption and signature status		X		X
Requesting and managing certificates from D-Trust, German National Research and Education Network (DFN), GlobalSign, SSL Plus, Digicert and SwissSign (request, renew, revoke)		X		X
Requesting and managing certificates from a Microsoft CA (Windows 2008 Server R2 or later)		X		X
Generation and management of PGP key pairs via the management console		X		X
Centralised management of all public and private certificates		X		X
Import/export of S/MIME certificates		X		X
Import/export of PGP keys		X		X
Automatic encryption of emails using S/MIME/PGP, including fallback to PDF encryption		X		X
Quarantine for unknown root and SubCA certificates and PGP keys		X		X
Support for gateway certificates and PGP keys		X		X
Support for Chiasmus-encrypted files	X	X	X	X
Public key querying via LDAP		X		X
Public key querying via Open Keys		X		X
Automatic upload of public keys to Open Keys		X		X

1) Requires a locally installed on-access virus scanner.
2) Requires the digiSeal server from secrypt.
3) High availability with multiple servers requires an additional server license..
4) Requires an appropriate Large Files license.
5) Requires an appropriate Sandbox Service license.

Large FileTransfer

Feature NoSpamProxy	Protection	Encryption	Large Files	Suite
Sending of large files by email via Microsoft Outlook Add-In			X	X
Encrypted connection to files on Web Portal (SSL)			X	X
Setting of file size limits	X		X	X
Reply option for external recipients			X	X
Reply option for external recipients without invitation link			X	X
Malware check of uploaded files by the Integrated Malware Scanner			X	X
Overview of all stored files via user interface			X	X
Files are stored in encrypted form on the Web Portal			X	X
Data between two Web Portal installations is synchronized and tunneled			X	X
Password protection for files stored on the Web Portal			X	X
File approval by administrators			X	X
Automatic approval of files after selectable time frames			X	X
Konfiguration von internen und externen Download-URLs			X	X
Senders are informed when attachments are downloaded			X	X

1) Requires a locally installed on-access virus scanner.
2) Requires the digiSeal server from secrypt.
3) High availability with multiple servers requires an additional server license..
4) Requires an appropriate Large Files license.
5) Requires an appropriate Sandbox Service license.

Advanced Email Routing

Feature NoSpamProxy	Protection	Encryption	Large Files	Suite
Sender domain-based routing of emails	X	X	X	X
Recipient domain-based routing of emails	X	X	X	X
Unlimited number of send and receive connectors (SMTP)	X	X	X	X
Connectors for				
• De-Mail via Telekom Deutschland	X	X	X	X
• De-Mail via Mentana Claimsoft	X	X	X	X
• POP3 connector		X	X	
• AS/2 Business to Business	X	X	X	X
• Deutschland-Online Infrastruktur (NdB-VN)	X	X	X	X
De-Mail rights management at user level	X	X	X	X
Microsoft 365	X	X	X	X

1) Requires a locally installed on-access virus scanner.
2) Requires the digiSeal server from secrypt.
3) High availability with multiple servers requires an additional server license..
4) Requires an appropriate Large Files license.
5) Requires an appropriate Sandbox Service license.

Allgemeine Features

Feature NoSpamProxy	Protection	Encryption	Large Files	Suite
Easy setup via configuration wizard	X	X	X	X
NoSpamProxy provides a multi-tenancy in the following areas: rules, message tracking, e-mails on hold, DKIM keys, user fields, e-mail server, in- and outbound connectors, domains, corporate user, partner menu, Web Portal URL and branding	X	X	X	X
Detailed configuration options for filtering and signature/encryption options based on rules; similar to firewall rules (filtering for gateway, sender, recipient)	X	X	X	X
Central management of local users	X	X	X	X
Import of users via Active Directory via encrypted connections (LDAPS/SGC)	X	X	X	X
Import of users via Azure Active Directory (no restrictions)	X	X	X	X
Restriction of the objects to be imported from the Active Directory based on organisational units (OUs)	X	X	X	X
Restriction of the objects to be imported from Active Directory with the help of LDAP filters	X	X	X	X
Import of users from generic LDAP directories (e.g. Lotus Domino)	X	X	X	X
Archive interface				
• d.velop d3 Konnektor	X	X	X	X
• File system storage	X	X	X	X
• Archive mailbox (SMTP)	X	X	X	X
Rewriting of internal email addresses (also group based)	X	X	X	X
Central message tracking	X	X	X	X
Access message tracking by using the ODATA API.	X	X	X	X
Configuration of De-Mail sending options via Microsoft Outlook Add-In	X	X	X	X
Hiding of internal email server topology	X	X	X	X
TNEF support	X	X	X	X
Rights management for the management console (Configuration, People and Identities, Reporting)	X	X	X	X
Size limit for incoming emails	X	X	X	X
High availability: Synchronisation of the entire configuration between all roles[3]	X	X	X	X
Management using PowerShell Cmdlets	X	X	X	X

Feature NoSpamProxy	Protection	Encryption	Large Files	Suite
BATV support for incoming emails	X	X	X	X
Audit Log	X	X	X	X

Reporting

Feature NoSpamProxy	Protection	Encryption	Large Files	Suite
Overview of processed De-Mails		X	X	X
Report on email (entire)	X	X	X	X
Report on email addresses with the highest spam percentage	X	X	X	X

Disclaimer

Feature NoSpamProxy	Protection	Encryption	Large Files	Suite
Central management of unlimited number of templates	X[1]	X[1]	X[1]	X
Templates possible for HTML and text emails	X[1]	X[1]	X[1]	X
Simple integration of images	X[1]	X[1]	X[1]	X
Dynamic content from Active Directory fields	X[1]	X[1]	X[1]	X
Free selection and configuration of the Active Directory fields	X[1]	X[1]	X[1]	X
Extensive HTML editor	X[1]	X[1]	X[1]	X
Allocation of administrator rights specifically for Disclaimer	X[1]	X[1]	X[1]	X
Extensive set of rules	X[1]	X[1]	X[1]	X
Disclaimer rules based on: • AD group memberships • Keywords in the body text • Keywords in the subject field • Keywords in recipient address • Keywords in sender address • Keywords in the email header • Date range • Inbound mails	X[1]	X[1]	X[1]	X
Unlimited number of conditions and exceptions possible in rules	X[1]	X[1]	X[1]	X

1) Requires a locally installed on-access virus scanner.
2) Requires the digiSeal server from secrypt.
3) High availability with multiple servers requires an additional server license..
4) Requires an appropriate Large Files license.
5) Requires an appropriate Sandbox Service license.

noSpam proxy®
CLOUD

www.nospamproxy.de

Net at Work
Building IT-Excellence.

www.netatwork.de