

SurGATE™ Messaging Gateway

Enterprise Solutions



Spam Signature

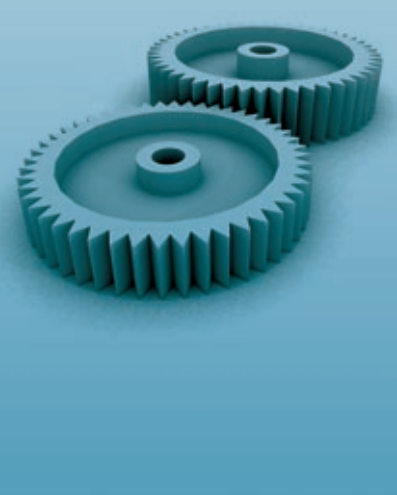
SurGATE Messaging Gateway allows to define spam signatures in your local language. Surgate appliances at the customer site update their own databases periodically. In addition to local signatures Surgate has millions of English spam signatures

Performance

Surgate is a high-performance and scalable solution for enterprises. With its pure C-coded and multi-thread scanning engine, it meets needs from SMBs to telco. It can handle two millions mail per appliance. These are the numbers in production environment not test numbers with 3 Kb e-mail. Surgate has about 20 spam catching methods. With its layered structure Surgate drops e-mail at the IP layer. Thanks to built-in firewall, SMTP IPS and LDAP integration, Surgate rejects most of e-mail without any content filtering. With %99 spam catching rate Surgate saves resources of your e-mail server and provides more mail processing capabilities for mail servers.

SRN Reputation Network

Surgate Reputation Network (SRN) is the name of a central IP reputation scoring system developed by Surgate Labs. It includes traditional features such as RBLs' but it also has "white list" and "greylisting ignore" features. By white listing feature it disables spam filters for the e-mail come from trusted sources. By this way SRN reduces false-positive rate.



How SRN Works?

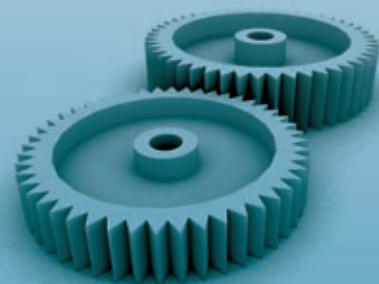
Surgate appliances send sender IP addresses and spam scores to the SRN center instantly. A sample record is as follows.

```
03/04/09 03:24:48: [qid: 31162-1238718288-118595] avspam_scan: ret [1]
[spam signature detected []
03/04/09 03:24:48: created /opt/surgate/quarantine/2009/04/03/03/
03/04/09 03:24:48: [qid: 31162-1238718288-118595] mid: 9320b064d431
792d495e438a001178f8@gmail.com from: XXXX@gmail.com to: YYYY@
surgatelabs.com [ip: 91.102.160.158, sub: =?windows-1254?Q?KOLTUKLA]
ret: 20, score: 120.00, [q/b:] 1/0, errbuf: spam signature detected
03/04/09 03:24:48: srncli_send: data (ip=91.102.160.158, rv=20, sc=120)
send successfully.
03/04/09 03:24:48: [23410] sql_insertmaillog: exec time: 0.0037s
```

These scores are assessed by mail processors at SRN center. IP address has a score above the threshold will be added to blacklist database. When a Surgate appliance receives an e-mail it makes query to SRN servers for source IP. This behaviour works like RBLs. If the source IP has a bad reputation the appliance rejects e-mail from this source.

SurGATE SMTP-AUTH Connector

Thanks to Surgate SMTP AUTH Connector, users can use Surgate as sender server (client-side "Server Requires Authentication" must be enabled) even if accounts are not on Surgate. In this way, users can send out e-mail in the office without any problem.



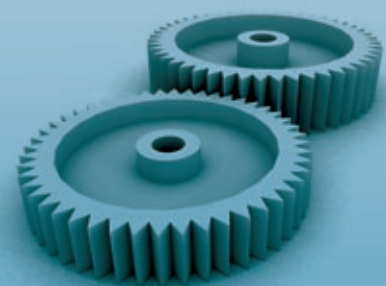
Disabling RBL by SMTP-AUTH Connector

Most companies' employees use DSL connection out of the office. DSL IP addresses can be in blacklists. In this case if the user tries to send e-mail to anybody behind a mail security gateway, the e-mail will not be received because the IP address is in black list. Since they do RBL controls at IP layer without opening SMTP session, they will never know it is not spammer. Surgate waits for the authentication to reject the e-mail even if the IP is in the black list. If the user successfully authenticated, Surgate disables RBL, reverse DNS and Greylisting controls for this session.

Surgate always wait for sender and recipient address. By this way, system admin can see the connection information even if it is in RBL.

Fake Sender Check

Surgate provides enterprise-class features such as user control from directory services (LDAP). E-mail is checked at the SMTP level before entering queue and connects directory server to check if the receiver exists. In this way if the e-mail comes to user not in the directory server, the e-mail is rejected without filtering. The mail server does not have to respond to the sender for unknown users. By this way non-existing users will not consume mail server resources. Additionally if the domain of the sender is local, Surgate also checks LDAP for sender address. As a result, Surgate prevents mail boxes against to fake senders. This makes Surgate unique.

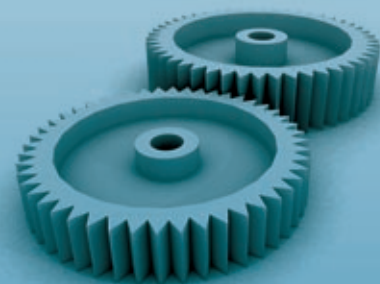


POP3 Proxy

Surgate POP3 Proxy module works transparently between the user and the real POP3 server. This module sends the requests from users to real server and from servers to users without making any changes. If this feature and SMTP-Auth Connector are used together, Surgate can be easily integrated to your existing network without making any changes at end-user side.

Greylisting

Greylisting is a name of the method we define as "Wait and Pass" that controls source IP address, sender and receiver e-mail addresses. If the hash of these three information is not in Surgate database then Surgate temporarily behaves as out of service and reject the e-mail. If the sender is a real MTA then it will send the same message after a while. Since spammers intend to send some millions mails in a short time, they never try again to send a failed mail. If the sender is Bot-Net client or a software used by spammers then the message will not be resent. In this way spams are blocked quickly without using any content filtering algorithms. If the sender is a real MTA then it will send the same message in a short time and message will be received by the recipient. If the same source send an e-mail again then the email will by-pass grey-listing feature. In this way, the only real e-mail will be held for the first time. You have option to enable or disable this option.

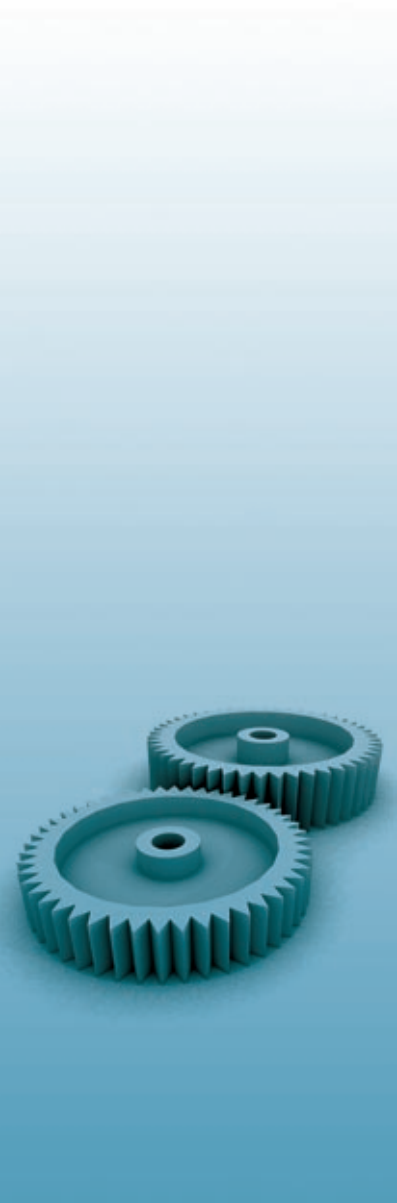


Profile Support

Surgate allows to create policies for IP addresses, e-mail addresses and domain names with its profile management feature. Thanks to this feature, system administrator can assign super-users for each domain and each super-user can manage domain individually without requesting help from system administrator. This reduces operating costs. The superusers can customize following features:

- Bayesian database
- SMTP settings
- Antivirus settings
- Antispam settings
- Header filtering

SurGATE Messaging Gateway supports submission port 587.



SurGATE™ Messaging Gateway

Enterprise Solutions

