

Managed Proxy

To ensure that your employees surf securely at all times.

The Proxy Service protects clients against attacks from the Internet. A proxy solution is recommended as an enhancement to a firewall solution. A firewall controls the traffic between internal networks (LAN, DMZ) and the Internet.

Web Traffic Analysis

The proxy service interrupts encrypted and unencrypted web traffic (http, https) between the internal client and the Internet. In this way, the internal client has no direct contact to content from the Internet because it sends its enquires to the proxy, which then evaluates the enquiries and, if permitted, loads the content for the client from the Internet. With it, it is possible to create a detailed policy for access to content in the Internet or also an internal network.

Web Antivirus/Anti Malware

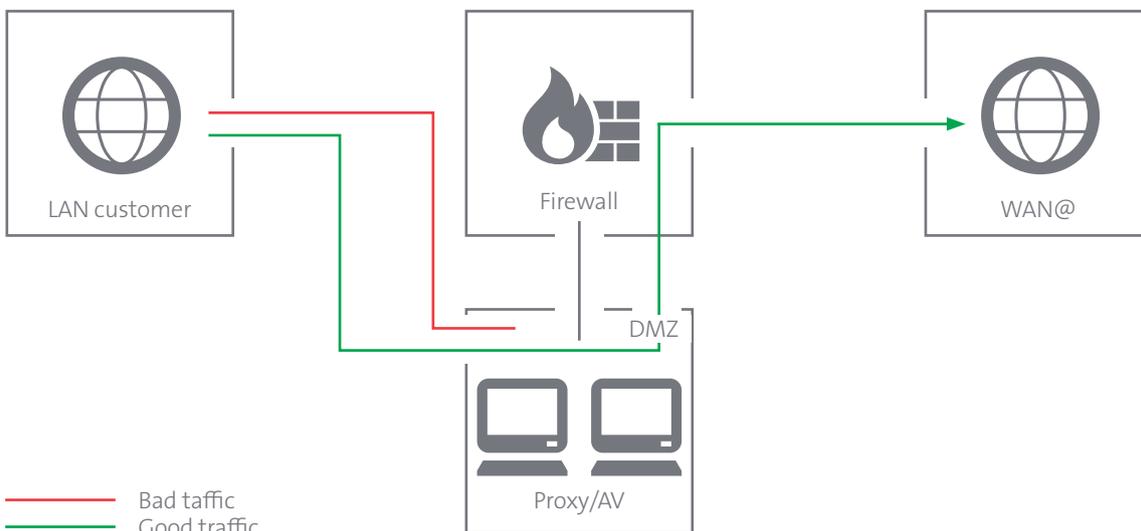
A policy decides which content must be examined for viruses or malware. Content which has been examined and found to be harmless can then be delivered to the client more quickly based on an entry in the cache without a second test. Updating the signature data-

base is done automatically, and it is constantly monitored to make sure it is up to date. An investigation of data traffic is possible in both directions (download/upload). This virus/malware scanning is no replacement for security software on the client systems but is rather an additional barrier to prevent malicious software from gaining entry into the network.

Web Filtering

All well-known web sites on the Internet (e.g. <http://www.nzz.ch>; <http://www.sex.com>) are placed into categories by the proxy service. The customer can request the blocking of web sites by category so that users no longer have access to these categories. There is the ability to override the predefined categories and allow or block specific URLs (called white lists and black lists, respectively). Unknown websites can be classified by the customer. A web filter (called a "policy") can be defined for an entire company, for specific groups (e.g. only HR, only Accounting, etc.) or for specific users.

Managed Proxy



Managed Proxy

Application Control (option)

In certain cases, you do not wish to totally block access to websites (using a web filter) but would like to deactivate certain functions. With an application control you can limit the use of specific functions for applications such as streaming media (YouTube, etc.), social networks, web mail, instant messaging (Facebook chat, etc.). In particular, the streaming of audio and video, chatting, publishing blogs or file up/down-

loading can be disabled. (This presumes an interruption in the SSL encrypted communication!)

Bandwidth Management (option)

On average, more than 50% of available bandwidth of a company's Internet connection is used for non-productive traffic (in particular, streaming). Thanks to this function, various Internet applications can be pre-assigned with minimum and maximum bandwidths.

Recurring services

Security Incident Monitoring and Management

A security incident is a potential attack on a customer system. The security incidents which are automatically detected and recognised are classified and displayed in the Security Dashboard.

Each change to an incident is time-stamped and is visible in the Security Dashboard. If a security incident is classified as harmful, it is assessed by a security analyst. Security incidents classified as harmless and false positive are logged

Client Protection

Users (clients) – no matter whether mobile or fixed users – which work via the proxy are protected according to the contractually established services.

Proxy, Web Antivirus and Web Filter Management

This service ensures regular updates and enables the maintenance of categories. Among them are: manufacturer feeds, updates which you have ordered as a change plus the daily updating of antivirus patterns and the tuning of policies according to best practices.

Reporting

The following reports are made available in the Security Dashboard as regards Proxy Services:

- | | |
|---------------------------|---|
| Web filtering | > Most violations by User |
| > Top active users | > Most violations by Category |
| > Most popular categories | > Most-popular URLs |
| > Most-blocked URLs | > Content type usage |
| > Web antivirus | > Most frequent and/or malware |
| > Most virus-active URLs | > Amount of malware blocked for web antivirus |
| > Most-blocked URLs | |

Advanced Proxy Reporter (option):

- In addition to the standard reports, the following reports can be obtained:
- > Day page view: Which data volumes are processed per day by the proxy
 - > Malware per month: Which malware was found during the month
 - > Site by request: Which top 25 websites were requested most frequently during the month
 - > Site total bytes: Which top 25 websites generated the highest data volume per month
 - > Top talker: Which top 25 source IP addresses generated the highest load per month
 - > Top categories: Which top 25 categories were used

How you benefit

- > Access to the Internet can be successfully controlled.
- > The service unburdens your firewall and Internet connection.
- > You analyse encrypted and unencrypted web traffic.
- > Your corporate network is even better protected against viruses and malware.