univention
be open.

Univention Corporate Server

Extended IP and network management documentation

univention
be open.

Table of Contents

1. Advanced proxy configuration 4
1.1. Cascading of proxies 4
1.2. Operation as a transparent proxy 4
1.3. Integration of a virus scanner in the proxy 5

Chapter 1. Advanced proxy configuration

1.1. Cascading of proxies

Feedback

In some scenarios, cascading of proxy servers may be required. In such a setup, individual proxy servers access logically superordinate proxy servers when web sites are opened, which then fetch the requested data from the Internet. This allows creation of a hierarchical structure of proxy servers and, for example, the operation of a central cache in a company's headquarters that the proxy servers at the individual company sites can access.

The superordinate proxy server is referred to as a *parent proxy* The parent proxy can be specified via the Univention Configuration Registry variables `squid/parent/host` (IP address or hostname) and `squid/parent/port` (port number).

Proxy requests from computers in the proxy server's local network are answered directly and not forwarded to the parent proxy. If additional networks should be excluded from forwarding to the parent proxy, these can be specified via the Univention Configuration Registry variable `squid/parent/directnetworks`. When doing so, the CIDR notation must be used (e.g. 192.168.2.0/24); several networks should be separated by blank spaces.

1.2. Operation as a transparent proxy

Feedback

It is possible to configure Squid as a transparent proxy. This can help avoid configuring the proxy server in all application programs. When using a transparent proxy, all unencrypted web queries are automatically rerouted through the proxy server.

Note

This only works for unencrypted web traffic, not for `https`.

Note

LDAP authentication on the proxy server must not be enabled.

The following configuration steps need to be made:

- The proxy server must be configured as the default gateway on all clients.
- The proxy server must be configured to use IP forwarding.

```
echo "net.ipv4.ip_forward = 1" >> /etc/sysctl.conf
sysctl -p
```

- The Univention Configuration Registry variable `squid/transparentproxy` must be set to *yes* on the proxy server. After that Univention Firewall and Squid need to be restarted:

```
/etc/init.d/univention-firewall restart
/etc/init.d/squid3 restart
```

This enables packet filter rules which redirect all queries for the web ports to the proxy server.

1.3. Integration of a virus scanner in the proxy

Feedback

Following the installation of ***univention-dansguardian***, the virus scanner and the filter for web contents are activated. ClamAV is used as the virus scan engine

The filtering of web content and the virus scanner can be activated separately. In order to deactivate the content filter, the Univention Configuration Registry variable `squid/contentscan` must be set to *no* and Squid restarted. To disable the virus scanner, the Univention Configuration Registry variable `squid/virusscan` must be set to *no*. If neither of the two variables is set to *yes*, DansGuardian is not used. After changes to the variables Squid and DansGuardian must be restarted.

The following variables can be used to configure the virus scan:

Table 1.1. UCR variables for filter rules

UCR variable	Description
`dansguardian/virus/notifyemail`	If this value is set to a valid e-mail address, a notification is sent via e-mail as soon as a user attempts to download a file infected with a virus.
`dansguardian/virus/exception/extension`	Files which have a suffix specified in this variable are not scanned for viruses. This option should be employed with caution as file suffixes do not provide definitive information on the actual contents of a file.
`dansguardian/virus/exception/mimetypes`	MIME types specified in this variable are not scanned for viruses. This option should also be employed with caution.
`dansguardian/virus/exception/sites`	This can be used to exclude complete web sites from virus scans, e.g. by excluding the company's intranet.
`dansguardian/virus/exception/urls`	In contrast to the previous variable, this can be used to exempts only individual URLs from the virus scan.