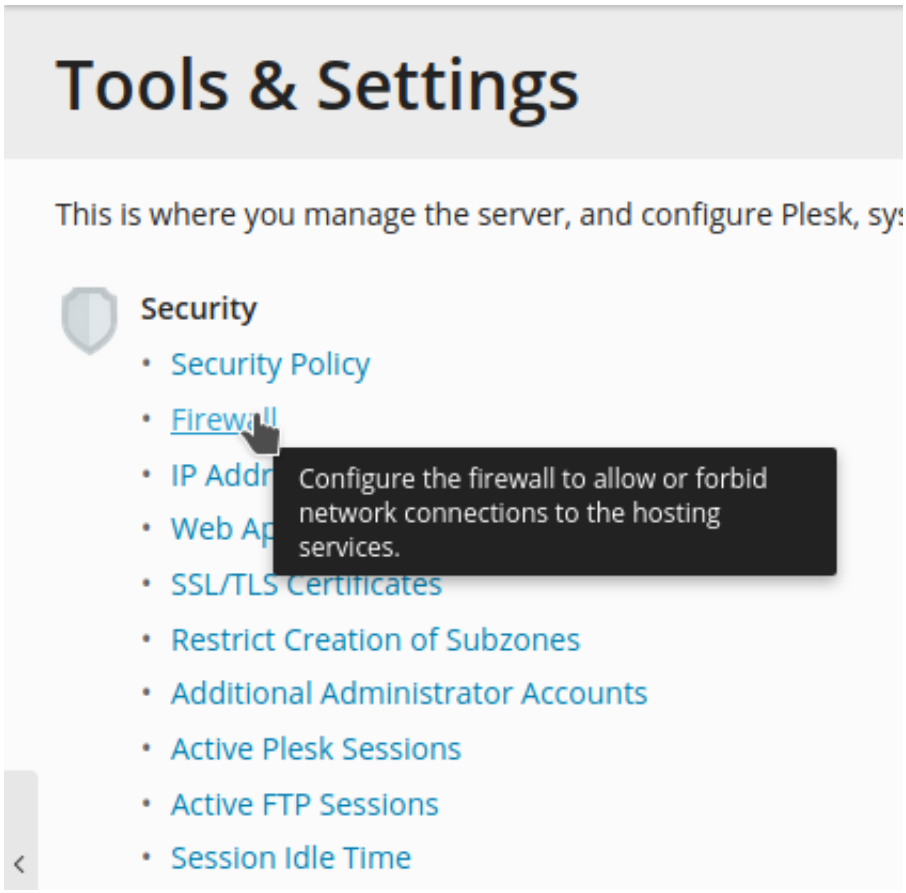
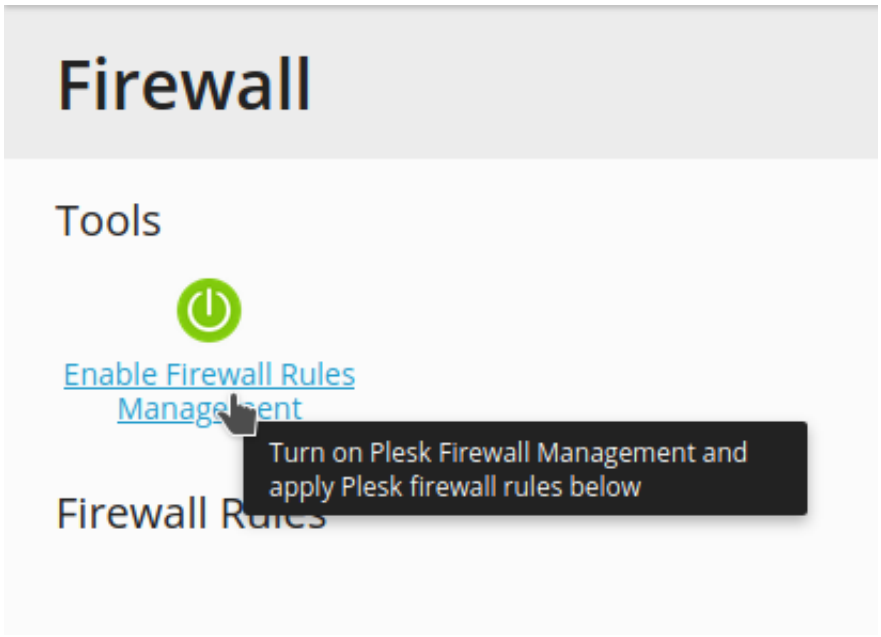
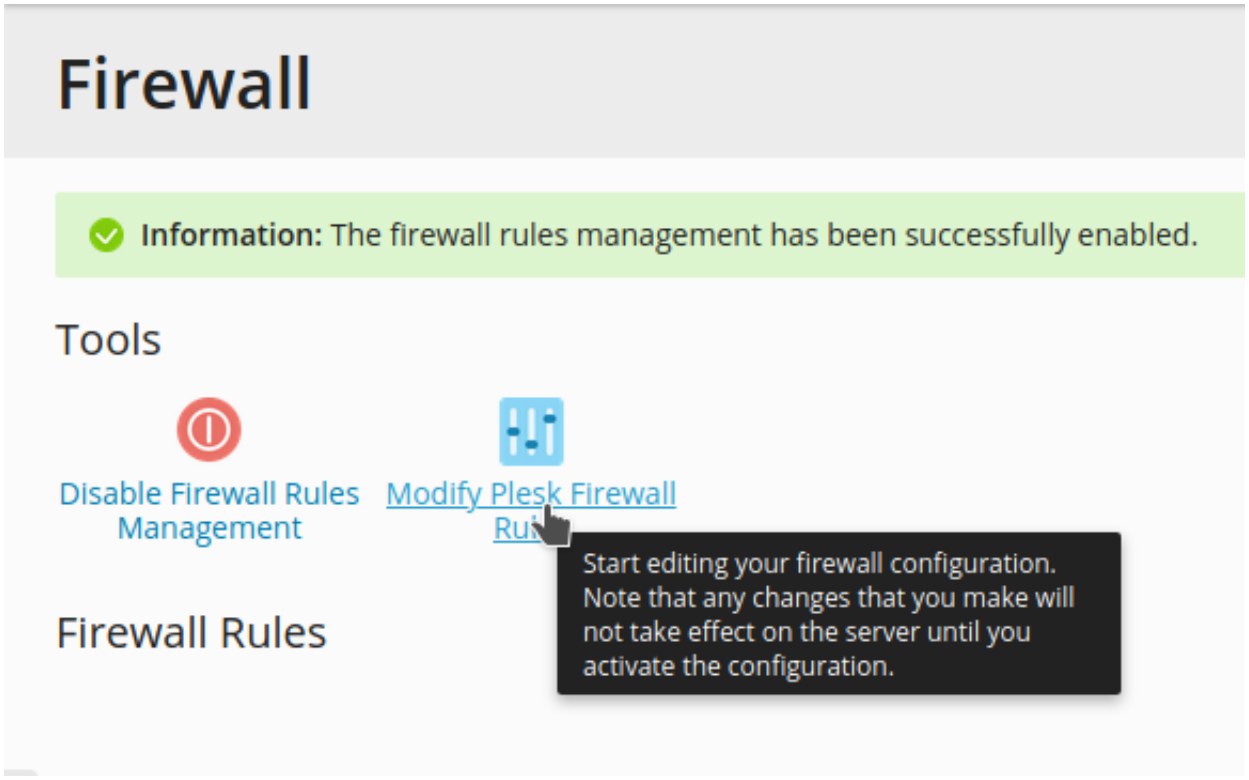
# Sicherheitseinstellungen in Plesk

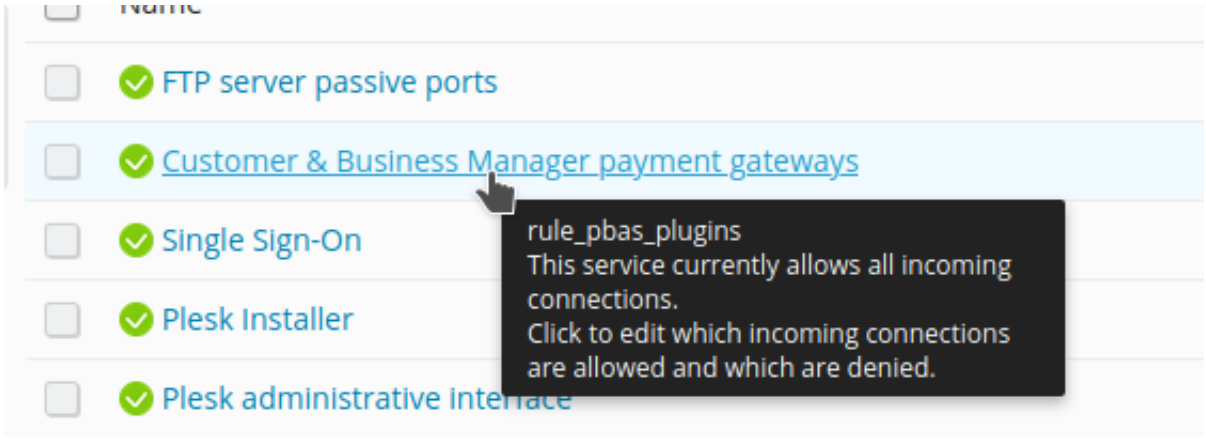
https://nissel.it/index.php/2020/03/10/sicherheitseinstellungen-in-plesk/

## Firewall

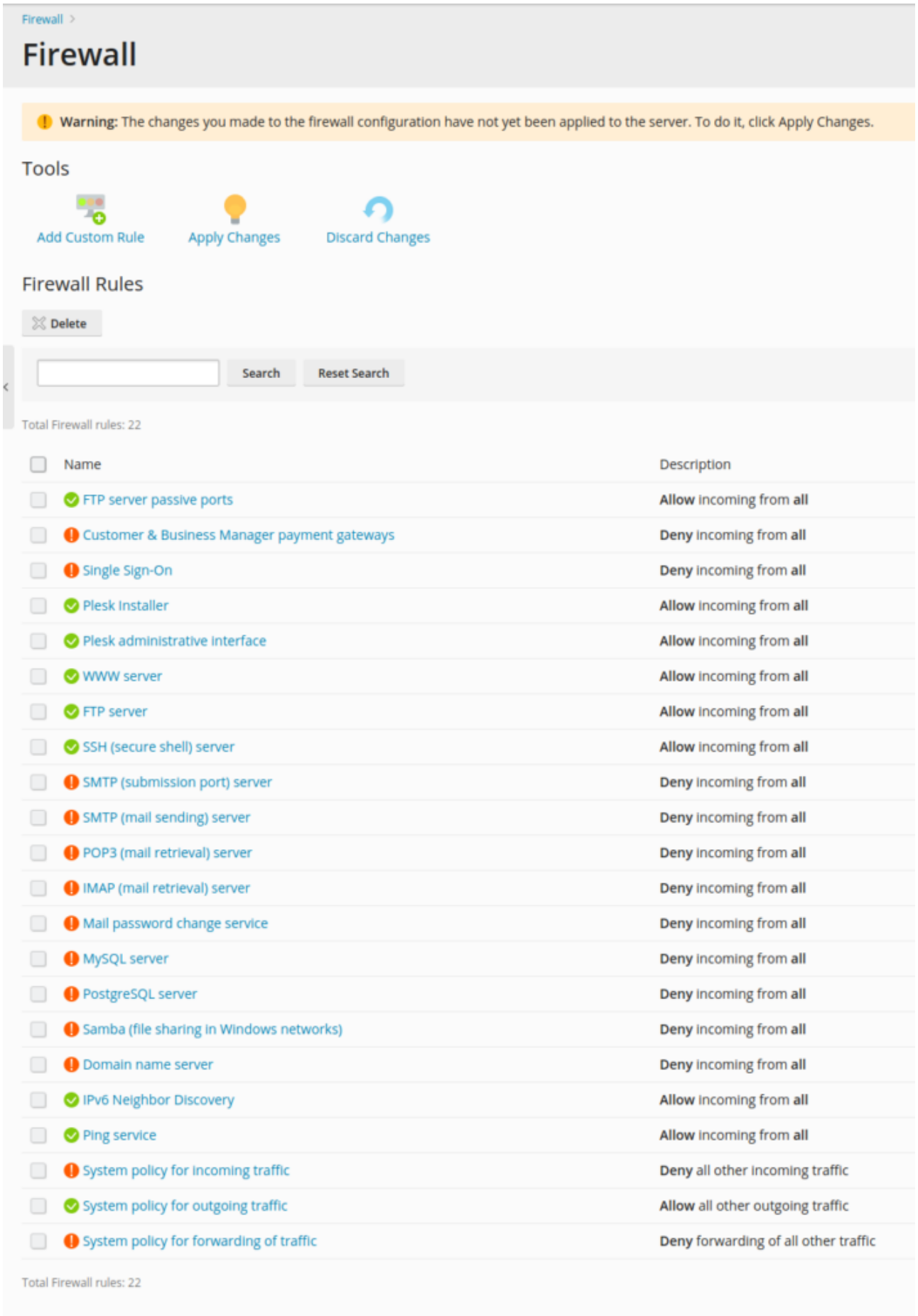


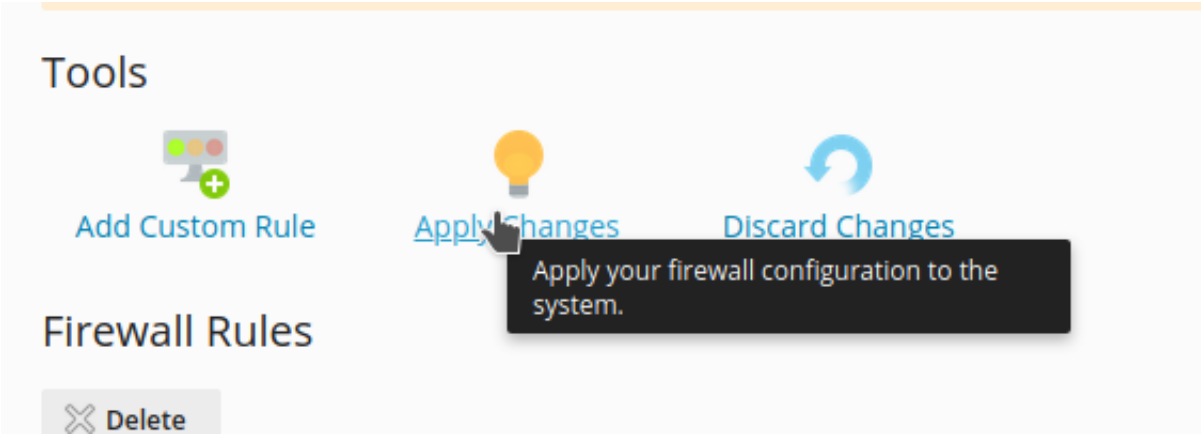

Firewall
Tools
Enable Firewall Rules Management
Turn on Plesk Firewall Management and apply Plesk firewall rules below
Firewall Rules


Firewall
Information: The firewall rules management has been successfully enabled.
Tools
Disable Firewall Rules Management
Modify Plesk Firewall Rules
Start editing your firewall configuration. Note that any changes that you make will not take effect on the server until you activate the configuration.
Firewall Rules




Die Regeln können gelöscht oder geändert werden. Ich würde empfehlen die Regeln einzeln auf "Deny" umzustellen. Wenn man hier über das Ziel geschossen ist, kann man einzelne Regeln wieder aktivieren.

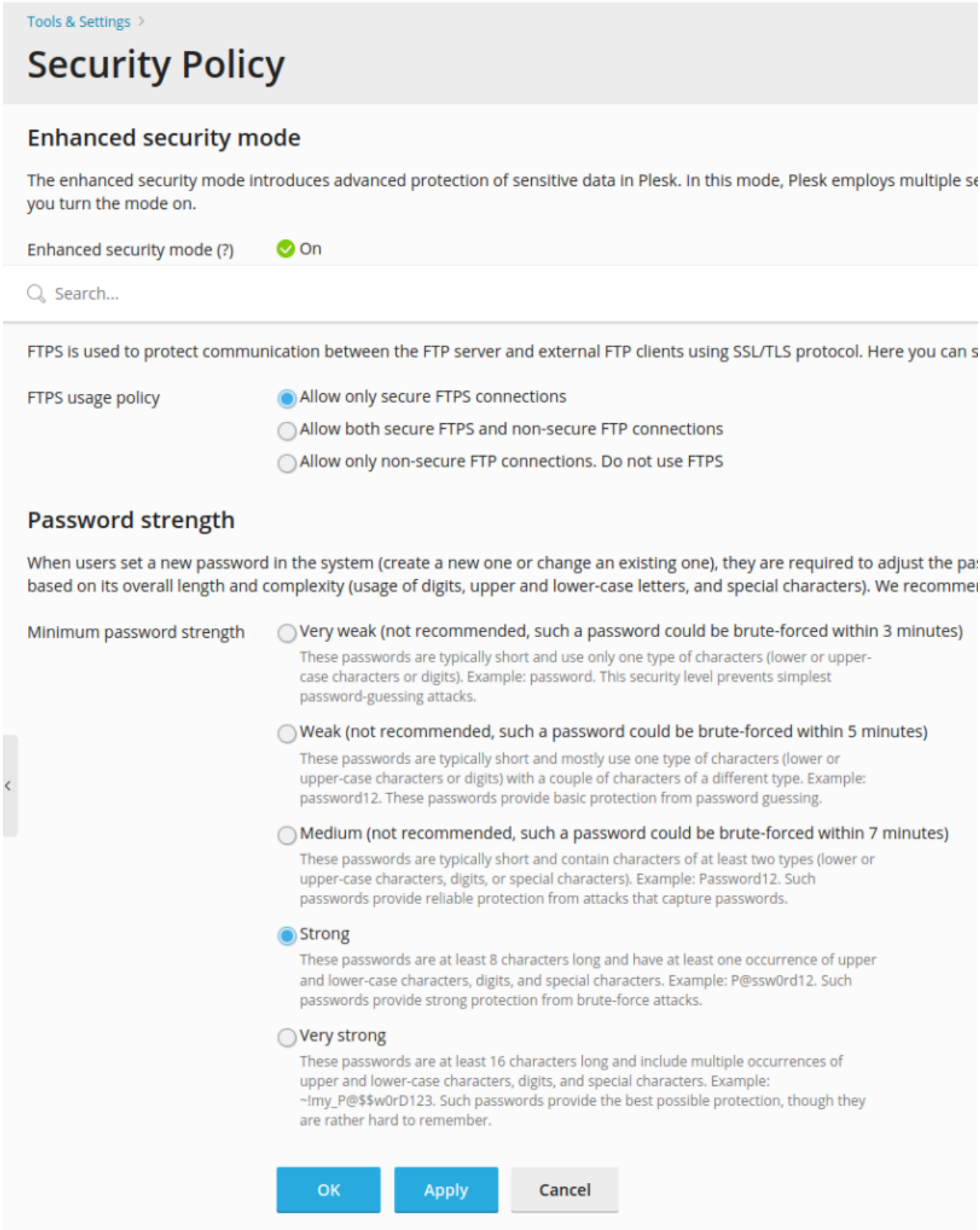

Firewall >
Firewall
Warning: The changes you made to the firewall configuration have not yet been applied to the server. To do it, click Apply Changes.
Tools
Add Custom Rule
Apply Changes
Discard Changes
Firewall Rules
Delete
Search
Reset Search
Total Firewall rules: 22
Name
Description
FTP server passive ports
Allow incoming from all
Customer & Business Manager payment gateways
Deny incoming from all
Single Sign-On
Deny incoming from all
Plesk Installer
Allow incoming from all
Plesk administrative interface
Allow incoming from all
WWW server
Allow incoming from all
FTP server
Allow incoming from all
SSH (secure shell) server
Allow incoming from all
SMTP (submission port) server
Deny incoming from all
SMTP (mail sending) server
Deny incoming from all
POP3 (mail retrieval) server
Deny incoming from all
IMAP (mail retrieval) server
Deny incoming from all
Mail password change service
Deny incoming from all
MySQL server
Deny incoming from all
PostgreSQL server
Deny incoming from all
Samba (file sharing in Windows networks)
Deny incoming from all
Domain name server
Deny incoming from all
IPv6 Neighbor Discovery
Allow incoming from all
Ping service
Allow incoming from all
System policy for incoming traffic
Deny all other incoming traffic
System policy for outgoing traffic
Allow all other outgoing traffic
System policy for forwarding of traffic
Deny forwarding of all other traffic
Total Firewall rules: 22




## Fail2Ban

TODO

## Passwort und FTP Policy


Tools & Settings
Security Policy
Enhanced security mode
The enhanced security mode introduces advanced protection of sensitive data in Plesk. In this mode, Plesk employs multiple se
you turn the mode on.
Enhanced security mode (?)
On
Search...
FTPS is used to protect communication between the FTP server and external FTP clients using SSL/TLS protocol. Here you can s
FTPS usage policy
Allow only secure FTPS connections
Allow both secure FTPS and non-secure FTP connections
Allow only non-secure FTP connections. Do not use FTPS
Password strength
When users set a new password in the system (create a new one or change an existing one), they are required to adjust the pa
based on its overall length and complexity (usage of digits, upper and lower-case letters, and special characters). We recomme
Minimum password strength
Very weak (not recommended, such a password could be brute-forced within 3 minutes)
These passwords are typically short and use only one type of characters (lower or upper-case characters or digits). Example: password. This security level prevents simplest password-guessing attacks.
Weak (not recommended, such a password could be brute-forced within 5 minutes)
These passwords are typically short and mostly use one type of characters (lower or upper-case characters or digits) with a couple of characters of a different type. Example: password12. These passwords provide basic protection from password guessing.
Medium (not recommended, such a password could be brute-forced within 7 minutes)
These passwords are typically short and contain characters of at least two types (lower or upper-case characters, digits, or special characters). Example: Password12. Such passwords provide reliable protection from attacks that capture passwords.
Strong
These passwords are at least 8 characters long and have at least one occurrence of upper and lower-case characters, digits, and special characters. Example: P@ssw0rd12. Such passwords provide strong protection from brute-force attacks.
Very strong
These passwords are at least 16 characters long and include multiple occurrences of upper and lower-case characters, digits, and special characters. Example: ~!my_P@$$w0rD123. Such passwords provide the best possible protection, though they are rather hard to remember.
OK
Apply
Cancel

# SSH root Login nur mit Zertifikat

Zuerst muss ein Zertifikat auf seinem Rechner erstellt und der Puplic key nach /root/.ssh/authorized_keys kopiert werden.
Anleitung Linux Clients
Anleitung Windows Clients

In der SSH Server Konfiguration muss dann der Login mit Passwort für den Root unterbunden sein
/etc/ssh/sshd_config

```
PermitRootLogin without-password
```

Linux: Ubuntu 18.04.4
Plesk: Obsidian 18.0.24

Quellen: https://www.fene-blog.de/linux-ssh-zugriff-ohne-passwort-per-ssh-key-konfigurieren/
https://devops.ionos.com/tutorials/use-ssh-keys-with-putty-on-windows/