McAfee® UTM Firewall version 4.0.3

Release Notes

This document provides information about McAfee UTM Firewall (*formerly SnapGear®*) version 4.0.3 and instructions for upgrading your UTM Firewall device to this latest firmware version.

You can find additional information at the following locations:

- **Help** – Help is built into your UTM Firewall. Click the Help icon in the upper right corner of the Management Console.
- **Support** – Visit mysupport.mcafee.com to find product documentation, announcements, and support.
- **Product Updates** – Visit my.securecomputing.com for the latest firmware versions.

In this document...

About this release

UTM Firewall firmware version 4.0.3 is compatible with the following UTM Firewall hardware models:

- SG310
- SG560
- SG560U
- SG565
- SG580
- SG640
- SG720

New features

This release incorporates the following new features:

General

- Customizable SMTP banner for use in answering incoming connections
- Improved GUI tab visibility
- squid enabled on SG560U
- OSPF available on the SG560U
- Default status graph hide-able with graph.attr.hide_default_graph=1
- **Enable debug** checkbox added to the PPTP server page
- Specific WPA2 setting for WiFi
- Custom error or reject html page for Access Control can be set by defining `/etc/config/proxy.html`
- ifmond 'parentof' connection attribute makes custom ifmond rules easier
- iptables layer7 match updated to the latest revision, and works properly
- /proc/.../nf_conntrack displays a replied count similar to the 3.x ip_conntrack_stat
- forward connlimit custom-rule match added

3G USB Modems

- Mode-switch modems (for example, ZTE and Onda) support added
- Sierra Wireless USB 306/307 support added

Antivirus

- ClamAV back by popular demand
- ClamAV updated to version 0.95.2

Authentication

Users are prevented from disabling users or groups that would result in administrative lockout

IPSec

- Ipsec can be run on an alias
- **Hide TOS** checkbox added to the IPSec General Settings page
- Dead Peer Detection can be set on the server side of a road warrior tunnel

Technical Support Report (TSR)

- Statistics moved to end of the TSR and compressed
- Kernel boot loader version included in TSR for USB based devices (SG560U)

Major fixes

This release resolves the following major issues.

General

- UPnP and UPnP rule deletion works properly
- 4.0 default forward rules taken into account by auto-forward rules for NAT
- *crontab* file that manages pw aging created when upgrading from 3.x
- SG310 serial port works correctly with dialup modems
- Excessive CPU use of auth/proxy80 corrected
- Re-installing same firmware revision on a 560U works properly
- ifmond passes link-check on PPPoE connections when the connection is up
- PPTP back to 3.x speeds
- Security policy applies even when "lock changes" is not in use
- Non-HTTP proxy requests directed at the UTM Firewall consume fewer resources

3G USB Modems

Disabling diald connection always ends connection

DNS

resolv.dnsmasq permissions forced to be correct

IPSec

- Fixed misbehaving IPSec after "scheduling while atomic" syslog error
- Ipsec now also works on non-default route interfaces
- Ipsec ASN.1 vulnerability CVE-2009-2185 fixed
- Routed IPSec tunnels (road-warrior server end) are no longer trapped by some phase 2 negotiations
- Dead Peer Detection on non-initiator aggressive tunnels (server -side road warrior) now works properly

PPTP

PPTP with RADIUS no longer interacts poorly with MPPE modes

Proxy

Changed http proxy to work around some websites' peculiarities

Minor fixes

This release resolves the following minor issues.

General

- Sender: header over-ridable using Device-Config when sending mail
- Connection status page reports correct MACs for A2-A4
- ifmond works properly when using builtin-log
- Web Protection Service server phasing over to new DNS/IP
- Web proxy automatically turned on or off when enabling or disabling Web Protection Service
- Configuration backups support directories
- POP email identification set to UTM Firewall
- Default-deny removed from Access Control
- Failover page html format corrected

DNS

dnsmasq trace removed

IPSec

- IPSec failover and IPSec GRE-based failover Administration Guide examples updated for 4.0 conditions
- IPSec pfkey debug handles IP addresses correctly
- Editing *ipsec.conf* followed by an "ipsec setup restart" syncs all cached configurations properly

PPTP

Warning generated if PPTP is used without a resolvable host name

Statistics

Serial dial-out connections show up on connection status page

Time zone

- Removed Daylight Savings Time for Western Australia
- Updated time zones for Egypt and Bangladesh

Upgrading your McAfee UTM Firewall device

To update your McAfee UTM Firewall to firmware version 4.0.3:

1. Log into my.securecomputing.com.
2. Click **Current Downloads**. The Downloads page is displayed.
3. Click the link that corresponds to your UTM Firewall model, and save the .sgu file to a convenient location.
4. In the McAfee UTM Firewall Management Console, navigate to **SYSTEM > Advanced > Flash Upgrade**. The Upgrade via HTTP page is displayed.
5. Click **Browse** and locate the .sgu file you saved in Step 3.
6. Click **Upgrade**. The Flash Upgrade (HTTP) page is displayed.

The firmware upgrade will take several minutes. At the end of the upgrade, the UTM Firewall device automatically reboots.

Note: Due to feature changes, configurations from previous firmware versions may not work as expected in 4.0.3. Please update your configuration to assure major services (such as SMTP or POP3) are operating as desired.

For more information on upgrading your firmware, including additional upgrade options, refer to the *McAfee UTM Firewall 4.0.3 Administration Guide*.

License attributions

Some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar Free Software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires that for any software covered under the GPL which is distributed to someone in an executable binary format, that the source code also be made available to those users. For any such software covered under the GPL, the source code is available from the my.securecomputing.com website. If any Free Software licenses require that McAfee provide rights to use, copy or modify a software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein.

McAfee®

For support information, visit mysupport.mcafee.com.

700-2226A00