



Astaro Security Gateway **Vers**

Release Notes

Version: RvD7.100

Author: RvD Rev. B

2 / 11 D3. December 2007

CONTENTS

WHAT'S NEW IN ASTARO SECURITY GATEWAY V7.1 3

- WEB FILTERING..... 3
- OTHER NEW FEATURES 4
- MANAGEMENT AND ADMINISTRATION 5
- PERFORMANCE IMPROVEMENTS 5

CHANGES 6

- FEATURE AND BEHAVIOR CHANGES..... 6
- DROPPED FEATURES 6

SYSTEM REQUIREMENTS 7

- HW REQUIREMENTS 7
- SUPPORTED WEB BROWSER 7

INSTALLATION AND UPGRADE INFORMATION 8

- UPGRADING ASG V7.0 TO V7.1 8
- UPGRADING ASG V6 HARDWARE APPLIANCES TO V7.1 8
- UPGRADING ASG V6 SOFTWARE INSTALLATIONS TO V7.1 9
- BACKUP CONVERTER LIMITATIONS..... 9
- SOFTWARE DOWNLOAD 10

SUPPORTING MANAGEMENT APPLICATIONS 11

- ASTARO COMMAND CENTER SUPPORT 11
- ASTARO REPORT MANAGER SUPPORT 11

KNOWN ISSUES..... 11

' w/1An vi c :v un1/oR W yGo:17 . /1i c /7 Vers

The new version provides a completely re-designed HTTP proxy, replacing the squid proxy which has been used up until now. The new proxy significantly improves Web Filtering functionality & performance.

The new version also offers many usability enhancements as well as bug fixes.

' i b F:11i o:vg

The new HTTP proxy provides the following major enhancements:

uy1:t i 2:oi y1Ro7 v/1:t i mRdi (E SLMt COKi obi oRn)

NTLMv2 and Kerberos authentication has been added to the Active Directory Single-Sign-On (SSO) capabilities during complete rewrite of the SSO facility. Support of these protocols is required in order to authenticate against a Windows Domain Controller running in Native Mode. Kerberos is supported by Internet Explorer 7 and Firefox browsers (IE6 only support NTLMv2). Kerberos is used as default if available. SSO Support for pure Broadcast/NetBIOS domains running with NT4 as Domain Controller is not supported any longer.

Clients running Windows Vista joined to a domain using Windows 2003 R2 server as domain controllers can only use Kerberos Authentication (so they need to put the firewall hostname in the browser proxy settings).

NRvyGo: v1 Gn/gi Rf bl/yk /vd c w:1i l:n1n pi o pRf:li

Within HTTP profiles you can now define filter actions that block and allow access to dedicated URLs/sites at the same time.

W:oi /m:vg mi d:/ b7p/nn

Scanning of video and audio streams can be selectively disabled in order to avoid delays caused by downloading and scanning the entire stream through the HTTP proxy prior to playing.

BIRyk yRv 1i v1 bi fRai dRc vIR/d

File extension filter rules are now applied before downloading a file. This avoids unnecessary waste of bandwidth.

27v/m:y yRvf:gGo/1:Rv yw/vgi n c :1wRG1 oi n1/o1

Configuration changes of the HTTP proxy no longer require a restart, which has often lead to a termination of existing connections.

PoRf:li OF:11i o /y1:Rv IRgg:vg

To help troubleshooting wrong profile/filter assignment matching, the used profile and filter action is now logged in the http logfile.

HSSP PoRx7 ny/vn PT W5 oi qGi n1 bRd:i n

The proxy now employs virus scanning for bodies sent with POST requests to foreign servers as well. If the body contains a Virus, the content is blocked with '403 Forbidden'

T 1w i o v i c f i / 1G o i n

Besides HTTP proxy enhancements the new release also includes the following new features:

P / y k i 1 f : l i o b / n i d R v : v l i o f / y i

Packet filter rules can now be based on network definitions that are bound to specific network interfaces. This significantly improves the flexibility of packet filter rules in many environments.

u G 1 R - P / y k i 1 f : l i o o G l i g i v i o / 1 R v f R o E u S 1 o / f f : y

Packet filter rules can now be generated automatically from DNAT/SNAT configurations by selecting the new checkbox within the NAT-rule.

W P u M W / v v i o c : 1 w X - W P u M F l / g

If the spam score of an email exceeds the configured SPAM warn threshold (but doesn't exceed the quarantine threshold) the SMTP SPAM engine now adds an 'X-SPAM-Flag: Yes' header to the forwarded email. This allows the user to configure a filter rule within his email client for moving suspected SPAM mails into a dedicated folder.

E i 1 c R o k u y y R G v 1 v g O U n / g i

Additional pre-defined reports have been added offering information similar to the Web Security reporting. Data displayed can be selected by timeframe, sorted by various orders or drilled down by clients, servers and service.

N R v 1 i v 1 f : l i o d R G b l i b 7 l i n G p p R o 1

The download manager now supports file names using double byte characters. The double byte default character set can be selected via WebAdmin.

V : o 1 G / l H u M u N - u d d o i n n i n (M u N / d d o i n n 1 / k i R t i o)

When activating active/active HA (cluster) or active/passive HA (stand-by) configurations, MAC addresses of all interfaces (except for the HA interface) are changed to virtual MAC addresses taken from the range 00-1A-8C-F0-XX-XX, which is part of the official MAC address range owned by Astaro.

M G l : p l i - I P - N w i y k U p l : v k F / : l R t i o

In order to avoid occurrences of unnecessary fail-over you can now define multiple IP addresses (*Check IPs*) – in a comma-separated list – when configuring the primary network interface for uplink fail-over. Fail-Over will only be initiated if all of the specified IPs fail to reply to a *ping* message. The same (set of) IPs can be specified multiple times. The default *Check IP* 0.0.0.0 is a symbolic IP address that represents the interface's default gateway.

2 7 v 2 E W i v w / v y i m i v 1 n

DynDNS can now be used on more than one interface and also on static interfaces like "Ethernet Standard"

u G 1 R m / 1 y G n i o y o i / 1 R v f R o i 2 : o i y 1 R o 7 W v g l i - W g v - T v

You can now trigger the automatic creation of user objects for users authenticated via Novell eDirectory in Single-Sign-On mode.

M/v/gi mi v1 /vd udm:v:n1o/ 1Rv

The V7 WebAdmin interface contains the following usability improvements:

2:n/bl:vg Rf poRx7 /vd IPWi xyi p1Rvn

You can now (temporarily) disable exception rules within proxies and IPS without deleting them.

2:n/bl:vg Rf /l:/ni n Rv vi 1c Rdk :v1i of/yi n

You can now (temporarily) disable additional addresses (aliases) for network interfaces without deleting them.

. IRb/I EuS So/ti on/I Rp1Rv

NAT-Traversal can now be deactivated/activated via a global option under Site-to-Site VPN >> Advanced.

Pi ofRom/vyi ImpoRt i mi v 1n

The performance of the HTTP proxy has been significantly improved through the following enhancements:

Iv1i ll:gi v1y/ywvg

All content cached within the HTTP proxy cache will only be scanned once. Re-scanning will only be done if the Virus scanner configuration changes. This helps increasing throughput of the HTTP Proxy.

Ei c IT mRdi l

The new proxy uses an IO model that allows for increased network performance of up to 80% depending on hardware and content scanning configuration.

FGll nGppRo1 fRo HSSP srs yRvvi y1Rv ki i p/l:t i

The new proxy fully supports HTTP 1.1 keepalive on client and server connections, improving network performance.

Nw/vgi n

Fi /1Goi /vd bi w/t :Ro yw/vgi n

V:o1G/I MuN uddoi nni n fRo Hu yRvf:gGo/1:Rvn

As interface MAC addresses are now dynamically changed to virtual MAC addresses when activating a high availability configuration, it might happen that client PCs and other network components can't communicate with the ASG as they still use the old MAC addresses they might have in their ARP cache.

2Rm/:v jR:v:vg fRo uy1ti 2:oi y1Ro7 (' :vdRc n) dRm/:vn

In order to join the AD domain, the firewall must find a DC (Domain Controller) machine. In previous versions, this was done with a NetBIOS broadcast. Starting with ASG 7.100, pure AD (native) mode is used, which in turn requires finding the DC with a DNS lookup. There are also more strict requirements on DNS resolution and time differences. The following conditions must be met:

- The time zone on the firewall and the DC must be the same.
- There MUST NOT be a time difference of more than five minutes between the firewall clock and the DC clock.
- The ASG hostname must exist in the AD DNS system.
- The ASG must use the AD DNS as forwarder, or must have a DNS request route for the AD domain which points to the AD DNS server.

2Rm/:v oi -jR:v vi i di d Rv Gpgo/di

Customers upgrading from versions prior to 7.100 MUST re-join the Firewall to the AD domain if they use SSO. See above for more information.

Ki obi oRn nGppRo1oi qG:oi n poRpi o vi 1c Rok ni 1Gp

In order for opportunistic SSO Kerberos support to work, the clients MUST use the FQDN hostname of the ASG in their proxy settings - using the IP address will not work. NTLMv2 mode is not affected by this requirement, and will automatically be used if it is not met, or if the browser does not support Kerberos authentication.

Nw/vgi d bi w/t :RGo c :1w 1o/vnp/oi v1 poRx7 poRf:li n 1w/1 w/t i Gni onOgoRGpn /nn:gvi d

When transparent mode is enabled in a proxy profile, user authentication is not supported. Consequently, having users or groups in a filter assignment does not make sense. Up to 7.011, the proxy would silently match the assignment based on time events only. In 7.100, the proxy will completely ignore filter assignments with users/groups in transparent mode.

2Rc vIR/d m/v/gi oc :vdRc /ppi /on RvI7 Rv nIRc dRc vIR/dn

When a download is triggered in 7.100, the proxy will start to retrieve the content without initially displaying the download manager. It will only start to show the download manager if it was not able to transfer half of the advertised content size within five seconds.

2 oRppi d fi /1Goi n

WWT nGppRo1 fRo ES4 dRm/:vn

SSO Support for pure Broadcast/NetBIOS domains running with NT4 as Domain Controller is not supported any longer.

Windows minimum requirements

Hardware minimum requirements

Astaro minimum recommendation for V7.1 installations:

Intel Pentium III 667 MHz, 256MB RAM, 10 GB hard disk drive and above.

Best performance results running on:

Dual Xeon or Athlon, 2GB RAM, 36 GB SCSI 15krpm hard disk drive and above.

For proved hardware components please check our Hardware Compatibility List (HCL) at:

<http://www.astaro.com/lists/HCL-ASG-V7.txt>

ASG V7.1 might also be installed within VMWare virtual environments, such as VMWare Server, VMWare ESX Server, VMWare Workstation or VMWare Player, by using a pre-configured/pre-installed ASG ISO called VMWare Virtual Appliance. This ISO provides the same functionality as the standard ASG.

WebAdmin supported browser combinations

Astaro Security Gateway V7 WebAdmin will support the following browser/platform combinations:

MS Windows 2000/XP/Vista

- IE6 or higher (including IE7)
note: parallel installations of IE6 and IE7 are not supported!
- Mozilla Firefox 1.5 or higher
- Safari 3.0 or higher

Linux:

- Mozilla Firefox 1.5 or higher

Mac OSX:

- Safari 2.0.3 or higher
- Mozilla Firefox 1.5 or higher

ER11 : the iPhone Safari browser has certain limitations – hence it is not supported

Other browsers could also work, but might be subject to rendering or JavaScript issues. They are unsupported. Java or Flash support is not needed.

As with the new GUI technology much of the GUI processing has been moved from the appliance to the management workstation we recommend using [Firefox](#) on a system with at least 512 MB RAM and a CPU with 1,5 GHz. More system performance will increase GUI processing speed significantly.

Ivn1/II/1Rv /vd Upgo/di IvfRom/1Rv

Upgo/d:vg uW Verz 1R Vers

Please note: please contact support for installations with less than 512MB RAM if *automatic firmware download* (Management>>Up2Date>>Configuration) can not be used.

When upgrading from version 7.0x to V7.1 please carefully read the following notes if AD SSO is used:

2Rm/:vn oi -jR:v fRo uy1:t i 2:oi y1Ro7 WW

Customers upgrading from versions prior to 7.100 MUST re-join the Firewall to the AD domain if they use SSO. In order to join the AD domain, the firewall must find a DC (Domain Controller) machine. In previous versions, this was done with a NetBIOS broadcast. Starting with ASG 7.100, pure AD (native) mode is used, which in turn requires finding the DC with a DNS lookup. There are also more strict requirements on DNS resolution and time differences. The following conditions must be met:

- The time zone on the firewall and the DC must be the same.
- There MUST NOT be a time difference of more than five minutes between the firewall clock and the DC clock.
- The ASG hostname must exist in the AD DNS system.
- The ASG must use the AD DNS as forwarder, or must have a DNS request route for the AD domain which points to the AD DNS server.

Upgo/d:vg uW V6 w/odc /oi /ppl:/vyi n 1R Vers

ASG V7.1 runs on all currently sold Astaro Security Gateway (ASG) appliance models.

For upgrading ASG V6 appliances to ASG V7.1 Astaro offers the following three alternatives:

sr Ivn1/II c :1wvi c yRvf:gGo/1Rv

- Ask your certified Astaro partner to install ASG V7.1 firmware on your appliance
- Use the Setup Wizard (recommended) to create your configuration for ASG V7.1
- import your existing V6 license

Cr Ivn1/II c :1w:mpRo1 Rf V6 yRvf:gGo/1Rv

- Ask your certified Astaro partner to install ASG V7.1 software on your appliance and convert existing V6 configuration into new release.

hr uG1Rm/1y V6 1R Vers Gpgo/di

- Beginning with ASG V6.310 you are able to automatically upgrade V6 firmware and configuration files to V7.0 (suggested for remote installations)
- You can then upgrade 7.0 to 7.1 in a second step

Upgrading existing ASG V6 software installations to ASG V7.1

For upgrading existing ASG V6 software installations to ASG V7.1 Astaro offers the following two alternatives:

Alternative 1: New ISO image

- Download and install new ASG V7.1 ISO image on gateway
- Use the Setup Wizard (recommended) to create your configuration for ASG V7.1
- import your existing V6 license

Alternative 2: Backup and Restore

- Store the V6 system configuration into a backup file
- Download and install new ASG V7.1 ISO image on gateway
- Click on "Restore existing backup File" on the Setup Wizard screen

Important

- All log files and reports of your V6 installation will be deleted during migration (make a backup first)
- V6 license files can also be used within V7.1

Limitations

Due to the different system architectures an exhaustive conversion of V6 into V7.1 configuration files is not possible.

Thus the conversion covers all settings, aside from the following:

- HA configuration
- Remote syslog
- IPS
- Site to site/remote access IPSec VPN (conversion for PPTP only)
- Certificates (will not be carried over)
- QoS rules
- dynamic (DHCP) IP-Addresses on Eth-VLAN Interfaces (will not be supported in V7.1)
- DHCP Relay
- Eth-alias instances with status=0 (status fields will not be supported in V7.1)
- Email address fields (e.g. settings -> adminmail)
- eDirectory user authentication (conversion for SSO mode only)
- Active Directory/NTLM
- WebAdmin authentication via external sources
- HTTP proxy
- SMTP proxy
- Group definitions (network and service groups), which contain further groups will be expanded.

It should be noted however, that with the simplification of the administration interface, as well as new self configuring features (such as HA), all of the settings listed above can be adjusted with minimal effort.

WRf1c /oi 2 Rc v1R/d

The new version is available at Astaro's official download servers:

ftp://ftp.astaro.de/pub/ASL/v7.0/iso_i386/

http://download.astaro.de/ASL/v7.0/iso_i386/

WGppRo1:vg m/v/gi mi v1 /ppl:y/ 1:Rvn

un1/oR NRmm/vd Ni v1i o nGppRo1

Astaro Security Gateway V7.1 will be supported by Astaro Command Center (ACC) V1.4.

un1/oR ai pRo1 M/v/gi o nGppRo1

Astaro Security Gateway V7.1 will be supported by Astaro Report Manager (ARM) V4.6.

KvRc v InnGi n

The actual ASG V7 Known Issues List (KIL) can be found at
http://www.astaro.com/lists/Known_Issues-ASG-V7.txt