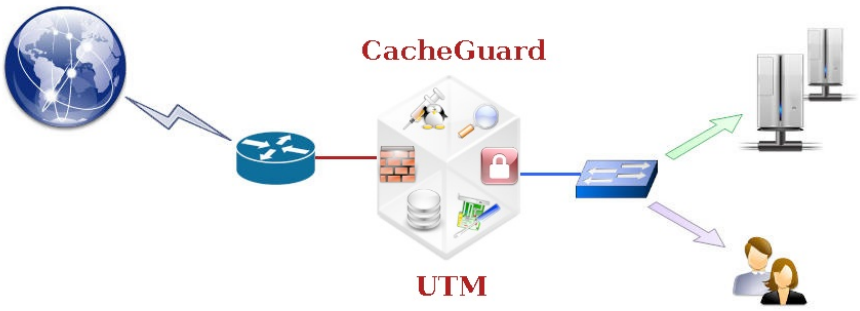
Table of Contents

CacheGuard Overview

The User's Guide allows you to quickly and briefly learn how to configure and administrate a CacheGuard appliance. To get a detailed description of each used command in this guide, you are invited to refer to the Commands Manual. The Web administration GUI that comes with CacheGuard-OS is a front end to the CLI, and hence is not separately documented.

CacheGuard Gateway allows you to connect your networks to the internet with security and peace of mind and protects your IT infrastructures against harmful traffic. In addition, with CacheGuard Gateway you can offer the QoS (Quality of Service) required by your most critical network traffic such as VoIP . What makes CacheGuard Gateway a unique solution is that it works in 2 senses: in forwarding mode it protects your connected users to the internet while in reverse mode it protects your Web applications. To get a CacheGuard Gateway you can simply install CacheGuard-OS on the machine of your choice. The only limitation is that you will need 2 NIC (Network Interface Cards) on that machine. To get help on CacheGuard-OS installation, please refer to the Getting Started section.



CacheGuard-OS embeds a variety of network security and traffic optimisation features such as, but not limited to, firewall, VPN, Web antivirus, filtering proxy, reverse proxy, WAF, traffic shaping and Web caching. All those features can be securely and efficiently activated at the same time on the same machine to take maximum advantage of the machine on which it runs.

Using CacheGuard-OS

Implementing and configuring CacheGuard-OS is easy and quick even if you are not a network and security expert. With CacheGuard-OS all the complexity of integrated open source software is put under the hood to allow you to just have to turn on the key and benefit from an extraordinary engine.

CacheGuard Gateway Functions:

CacheGuard-OS Network Optimization

- Network Appliance
- Internet Gateway
- Web Load Balancer
- 802.1q VLANs
- Support of NTP
- Traffic Shaping
- DHCP Server
- Caching DNS

CacheGuard-OS IP security

- Internal/External/Auxiliary zoning
- Forwarding and Reverse Web Proxy
- Transparent HTTP Proxy
- Proxy chaining and parallel implementation
- Access lists
- IP Firewall with NAT and PAT
- IPsec VPN in Site to Site or Remote Access modes
- Blocking Synflood, Port Scan, Spoofing...

CacheGuard-OS Web Security

- URL Guarding based on URL blacklists and white lists and regular expressions
- URL Guarding Policies based on access time, IP and LDAP requests
- Automatic blacklists updating
- Web Application Firewall (XSS, SQL Injection...)
- Access Logging
- LDAP & Kerberos AD© authenticating
- SSL Terminator
- SSL Mediator/Inspector

CacheGuard-OS High Availability

- RAID capabilities
- Backup & Restore on spare machine
- Ethernet link bonding
- VRRP Redundancy
- Multi WAN support

- Antivirus at the Web Gateway
- Antivirus as a service (for emails)

CacheGuard-OS Web Optimization

- Persistent Web caching
- HTTP Compression
- Web Cache sharing
- Traffic Shaping

CacheGuard-OS Administration

- CLI (Command Line Interface) configuration
- Console port administration
- Remote administration with Web GUI and SSH
- Logging to remote SysLog servers
- SNMP agent and trap generation

Change logs

Version UF-2.3.2 (25 March 2025)

- The **cache report** command has been fixed to display the correct Web cache report.
- The installation program has been fixed to exclude USB disks from the list of available disks when installing the OS from a USB stick.
- The software defined network has been modified to always activate the path checker even in a single gateway mode.
- The configuration file upload via the Web GUI has been improved to support large files and all kinds of Web browsers.
- Some minor bugs have been fixed.

Version UF-2.3.1 (13 March 2025)

- The OS has been upgraded to support the 255.255.255.254 network mask (prefix 31).
- The guard filter deletion has been fixed to properly remove the deleted filter from guarding policies.
- A new usage form has been added to the **vpnipsec** command to generate IPsec VPN profile (or script) file to use on remote client systems when the IPsec VPN is configured in access mode.
- The system can now send some information (such as IPsec VPN client configurations) by email. To this end, the **email** command has been enhanced to configure the email server and credentials to use to send emails.
- The keyword **wait** has been added to commands that normally run in background to specify that the command should be executed in blocking mode (e.g. **apply** command).
- The **file** command has been enriched to allow to delete a file on a remote file server.
- Some minor bugs have been fixed.

Version UF-2.2.2 (31 July 2024)

- OpenSSH has been upgraded to its latest stable version (9.8p1).
- Apache Web Server has been upgraded to its latest stable version (2.4.62).
- Squid has been upgraded to its latest version (6.10).
- StrongSwan has been upgraded to its latest version (5.9.14).
- Duplicated lease end time errors and records in the DHCP report have been fixed.
- The IPsec VPN report has been fixed to properly display certificate based authenticated connections.
- The Kerberos initialisation issue has been fixed.
- Some minor bugs have been fixed.

Version UF-2.2.1 (6 April 2024)

- The Linux kernel has been upgraded to the version 6.6.14 and all drivers have been upgraded to support the latest hardware in the market.
- The installation program has been fixed to allow an installation from a USB memory stick.
- The firewall has been improved to support the SIP protocol.
- The bug which prevented the restore operation since the UF-2.0.1 OS version has been fixed.
- The reverse Web mode has been enhanced to allow configurations in which backend Web servers (real hosts) are accessed via the external network interface or via site to site IPsec VPN tunnels established with the system. In addition, the reverse Web proxy can now communicates with real hosts. As a consequence, the syntax of the **rweb** command has been changed (see the **rweb host** usage form). In case where the appliance is upgraded using a patch, the **rweb** interface and the **http** protocol are used for existing configurations.
- The installation program has been enhanced to support an installation on a machine with only 512 MB of RAM.
- The size of the installation CDROM image has been reduced.
- The PXE installation program has been enhanced to support UEFI based machines (64 bits only).
- Some minor bugs have been fixed.

Version UF-2.1.3 (25 January 2024)

- The Web access module has been fixed to allow clients that are connected via the 802.1q pseudo interfaces (in VLAN mode) to use the embedded Web proxy.
- The **firewall** command has been improved to allow the modification of default limits for DoS (Denial of Service) attack. See the **firewall dos** command for further information.
- The default maximum number of TCP new connections (SYN) per source IP address has been raised. New default values can be obtained using the **firewall dos** command.
- The access command has been improved to allow the specification of 802.1q pseudo interfaces in Web access rules (see the **access web** command).
- In absence of any other specifications, a blank manager template is now initialised with a default system CA certificate and a default server certificate.

- Some minor bugs have been fixed.

Version UF-2.1.2 (11 December 2023)

- The proxy, the name server and the antivirus have been upgraded to their latest stable versions.
- The IPsec VPN server has been enhanced to allow remote VPN servers having a non fixed IP address to establish a site to site IPsec VPN tunnel.
- Some minor bugs have been fixed.

Version UF-2.1.1 (1 December 2023)

- The OS has been adapted to suit Microsoft Azure (TM) and Amazon AWS (TM) clouds requirements.
- The installation program has been improved to detect NVMe and virtual block based disks.
- Default associations between physical and logical network interfaces have been changed on a gateway system. Now by default, the external interface is associated to eth0 and the internal interface is associated to eth1.
- The generated system CA certificate during the first appliance start-up, is now properly installed.
- Admin access management has been fixed to properly allow newly added IPs.
- The **password** command has been enhanced with the possibility to modify both the console and Web administration passwords in a single operation.
- The CDROM installation program has been enhanced to support UEFI based machines (64 bits only).
- The Linux kernel has been upgraded to the version 4.19.288.
- The ssh password authentication can now be disabled (see the **admin ssh password** command).
- The bug that blocking explicit log rotations in case where the **web** (or **tweb**) mode is deactivated, has been fixed.
  .
- Some minor bugs have been fixed.

Version UF-2.0.2 (11 April 2023)

- The **waf** command has been fixed to do not erase the bypass application set for a website in case where the bypass rule list is erased for that website.
- The WAF Auditing module has been fixed to properly decode HTML encoded data in POST requests.
- The **system report service** command has been fixed to display the DNS server state.
- Now the DNS server can be queried even if the **web** and **tweb** are both disabled.
- The appliance access manager has been fixed to take into consideration override names setup with the **ip name** command. In addition, in case of any modification in override names, the Firewall and QoS are restarted.
- The **rweb site del**... command has been fixed to do not remove back end Web servers associated to a website in case where the deleted website name will remain present for another protocol (http or https). The fix has been also applied to other configuration related to reverse websites (**rweb via**..., **waf rweb**...).
- The Web GUI automatic logout has been fixed.
- Now the **apply check** command displays possible warnings.
- The routing issue via the auxiliary network interface has been fixed.
- The firewall rules management module has been fixed to do not apply the default policy to new connections incoming from the internal zone in case where the VLAN mode is deactivated and rule sets other than the **web** rule set are not empty.
- The firewall has been fixed to allow fragmented IP packets in IPsec traffic.
- The SSL mediation mode has been fixed to automatically download intermediate certificates even in case where the Web access has been restricted by the **access web**command.
- The **tls** command has been enhanced to allow for setting the size of generated RSA private keys.
- The bug that was preventing to install the OS without the Web caching feature has been fixed.
- Some minor bugs have been fixed.

Version UF-2.0.1 (3 February 2023)

- A new command called **manager** have been added to the system to manage remote gateways. To use this command, the OS should be installed as a *manager* system (as opposed to a system installed as a *gateway* system).
- The Linux kernel has been upgraded to the version 4.19.231.
- All open source packages have been upgraded to their latest versions and have been rebuild from scratch using latest GNU C library (glibc-2.35) and GNU C compiler (gcc-11.2.0).
- The new usage form **system report connection** has been added to the **system** command to display the number of active connections with the appliance.
- The new usage form **system report antivirus** has been added to the **system** command to display the status of the last automatic antivirus signatures update.
- The apply reporting has been fixed to report 100% (instead of 99%) when the antivirus update is fully completed.
- Trusted CA certificates have been updated from Mozilla as of: Thu Sep 30 21:39:27 2021 GMT. The OS has been enhanced to automatically update trusted CA certificates once a month.
- The system has been upgraded to support TLS 1.3.
- The maximum period for log retentions has been modified from 365 to 366 days (available during installation only).
- Some basic open source software have been upgrade to their latest stable versions.
- The **tls** command has been enhanced to allow the generation of certificates that do not use OCSP.
- The **tls server** and **tls ca** command usage forms of the **tls** command have been changed to be uniform with the **tls client** usage form.

- The syntax of **tls** command has been changed. Now to manage server certificate the **server** keyword should be systematically used as the first argument. To manage the system CA components (certificate and key) the **system** keyword should be specified after the **ca** keyword. To manage third party CA certificate the **third** keyword should be specified after the **ca** keyword. To import third party CA certificate, the **load** keyword replaces the **import** keyword.
- The **apply** command has been modified to automatically generate new TLS objects in case where explicit TLS generations or loadings are note invoked.
- Restricted administrator users can now be deleted properly without generating an error during the apply operation.
- The syntax of the **admin** command has been changed for SSH key management. Now an identifier should be associated to an SSH key first. Then, its content can be loaded from a trusted file server.
- Now, the first time a new restricted administrator is logged in, she/he is invited to modify her/his password.
- The **cancel** command can now be invoked by restricted administrator users without generating any errors.
- OWASP Core Rule Set (CRS) has been upgraded to its latest version (3.3.2). This involves the renaming and renumbering of generic filters.
- CAUTION: the syntax of the **waf** has been modified as follows: "waf rweb bypass" becomes "waf rweb bypass **rule**". Also generic WAF filters has been renamed and renumbered. If your configuration includes the bypass of some generic rules in order to avoid false positive matches, you are invited to review your configuartion. Please refer to the documentation for further details.
- Now the blocking of Web requests/responses by the WAF is based on an anomaly scoring principal. Please refer to the documentation for further details.
- The WAF module has been enhanced to offer the following functionality: blocking of DoS (Denial of Service) attacks, blocking of requests based on IP reputation, blocking of requests coming from a particular country, bypass of generic filters based on the type of the application (WordPress, Drupal...). Please refer to the documentation for further details.
- The logging has been enhanced to allow the activation or deactivation of logging on remote syslog servers as per the type of traffic (see the command **log**).
- The syntax of the **authenticate**... command has been slightly changed. Please refer to the documentation for details.
- The **ip**, **access** and **vpnipsec** commands have been improved to accept IP addresses in CIDR notation (in the form *<ip/prefix>* instead of *<ip> <netmask>*).
- The limitation associated to the IPsec VPN usage in a multi WAN configuration has been removed. Now it is possible to route IPsec traffic via a master gateway and automatically switch the routing via a backup gateway in case of a failure on the master gateway. See the **vpnipsec** command manual for further information.
- A new command called **file** has been added to the system to load or save all files related to the configuration in a single operation.
- The rights of restricted administrator users have been changed. Now restricted administrator users can only read (consult) the system configuration. Restricted administrator users are now called unprivileged administrator users (refer to the **admin** command for further information).
- The **traceroute** command has been added to the system.
- The association of multiple client SSL certificates to the SVMP-v3 user name has been removed from the system (now only one client SSL certificate can be associated to the SVMP-v3 user name). See the **admin** command for further information.
- The management of TLS chain certificates has been modified. Now when defining an HTTPS reverse website, you have the possibility to specify an intermediate CA certificates. Please refer to the **tls** and **rweb** commands for further information.
- The system integrity checking has been modified to allow the deactivation of **web**, **tweb** and **rweb** modes at the same time.
- The CacheGuard-OS License Agreement has been upgraded to version 2.5 to include OS installation as a *manager* system.
- Lots of minor bugs have been fixed.

Version EH-1.5.5 (20 April 2021)

- The QoS controller has been fixed to properly shape the traffic on the external and auxiliary interfaces when the VLAN mode is activated.
- The system has been improved to avoid any latency in web browsing during the antivirus update process. This requires about 1280 KB of additional RAM so a RAM upgrade may be needed on the target machine.
- Some minor bugs have been fixed.

Version EH-1.5.4 (16 March 2021)

- The issue that was slowing down the AV signatures downloads has been fixed.
- TCP communications have been tuned to get better performances.
- The proxy, the VPN and the antivirus have been upgraded to their latest stable versions.
- Some minor bugs have been fixed.

Version EH-1.5.3 (11 February 2021)

- The installation program has been fixed to include all required SCSI drivers in the boot loader initial RAM disk.
- The access control module has been fixed to properly allow administration accesses when the VLAN mode is activated.
- The installation module has been fixed to detect VirtIO devices.
- In order to comply with the RFC 5280, the "OCSP Signing" Extended Key Usage has been removed from

generated X509v3 certificates (only the "TLS Web Server Authentication" Extended Key Usage is kept).
- Some minor bugs have been fixed.

Version EH-1.5.2 (2 December 2020)

- The network name resolution module has been enhanced to resolve the embedded OCSP responder host name to the system's external IP address (external VRRP IP in HA mode). This helps to avoid asymmetric routing when the **ocsp** mode is activated.
- Some minor bugs have been fixed.

Version EH-1.5.1 (31 October 2020)

- The IPsec VPN support has been added to the system and a new command called **vpnipsec** has been added to manage IPsec VPNs. Both site to site (**site**) and remote **access** VPN configurations are supported. The embedded forwarding Web proxy and resources behind the embedded firewall can securely communicate via the IPsec VPN.
- The Linux kernel has been upgraded to the version 4.9.230 and all drivers have been upgraded to support the latest hardware in the market.
- The reporting in the Web GUI dashboard has been fixed to properly refresh all reports (including reports on NICs and disks).
- The **system report cpu** usage form of the **system** command has been replaced by **system report load**.
- The **tls** command has been enhanced to allow the loading of a CSR file in order to generate signed certificate by the system's CA certificate. With this enhancement the system can now act as a mini PKI.
- When a CA certificate is added to the system it is automatically considered as a trusted CA for Web browsing. Now it is possible to do not trust a CA certificate for browsing by specifying the optional **off** argument when adding the CA certificate with the **tls** command. In this case the CA certificate can only be for other purposes (such as the VPN server).
- The **authenticate ldap certificate** usage form of the **authenticate** command has been removed. If an LDAPS server SSL certificate has to be verified against a CA certificate, the CA certificate should be imported first using the **tls** command and then the CA certificate verification can be activated using the **authenticate ldaps ca ...** command. In case where the system is upgraded using a patch, an existing LDAPS CA certificate is purged and then it should be configured again manually.
- The authentication type for SNMP-v3 user has been changed from SHA-1 to SHA-256.
- The **md5** and **sha** (for SHA-1) authentication hash functions are no longer allowed for SNMP-v3 traps. Allowed authentication hash functions are now: **sha256**, **sha384** and **sha512**.
- Access policies to (from) the appliance from (to) remote networks/hosts have been reinforced by the specification of the involved network interface. Therefore, the syntax of the **access** command has been changed. In case where the system is upgraded using a patch, an access entry for every interface is added to the system and access policies should probably be reviewed after having patched the system.
- When defining a transparent network with the **transparent** command, the network interface from which traffic are transparently caught should be specified now. In case where the system is upgraded using a patch, the same transparent network is added for every interface and transparent networks should probably be reviewed after having patched the system.
- Some minor bugs have been fixed.

Version EH-1.4.2 (29 June 2020)

- The ICAP service not restarted with the previous patch is restarted to properly handle the brotli compression format.
- The **tls** command has been enhanced to allow you to create client certificates signed by the system's CA certificate. Client certificates can be used to authenticate VPN clients (VPN features are coming soon).
- The **tls ca** command can now be used to add and import an intermediate CA as well as a root CA.
- Self signed SAN certificates generation has been fixed to properly generate a self signed certificate and not a CA certificate.
- Certificates can now be revoked with the **tls** command.
- An OCSP (Online Certificate Status Protocol) responder has been added to the system. You can use the **tls** and **port** commands to configure it. Use the **mode** command to activate it.
- Some minor bugs have been fixed.

Version EH-1.4.1 (11 June 2020)

- A new mode called **tnat** (for transparent NAT) has been added to the system. When the **tnat** mode is deactivated,Web traffic in transparent mode go to the internet with their real IP addresses (and are not source NAT with the appliance's external IP address).
- The transparent mode activation has been moved from the "[GENERAL]/[Main Settings]/[Main Features]" page to the "[NETWORK]/[Main Settings]/[Network Services]" page in the Web GUI.
- The transparent command has been enhanced to take into account the QoS for traffic exchanged via the auxiliary interface.
- The DNS has been fixed to properly listen on VRRP IP addresses.
- The proxy configuration has been fixed to add the X-Forwarded-For header to all HTTP(S) requests if at lease one next peer is configured.
- The maximum period for log retentions has been modified from 31 to 365 days (available during installation only).
- Internal access policies have been modified to allow the connect method to ports 1024-49151 (in addition to the port 443) from the forwarding proxy

- The CSR and signed certificate generation programs has been fixed to properly handle Certificate Signing Requests and CA signed certificates for SAN certificates.
- Failed login via the Web GUI are now logged and reported with SNMP traps and syslog alerts.
- Some additional ciphers has been added to the SSH server. This command prints a report on the current running operation in background. The Web GUI has also been enhanced with an animated icon to show the current running operation.
- A new command called **job** has been added to the system.
- Now the antivirus uses HTTPS instead of HTTP to download virus signatures.
- Reports displayed in the Web GUI dashboard are now automatically updated.
- The option **report** has been added to the **qos** to print a report on the traffic managed by the QoS controller.
- Some minor bugs have been fixed.

Version EH-1.3.7 (29 May 2018)

- The CacheGuard-OS License Agreement has been upgraded to version 2.4.
- The bug making the main proxy to crash while the web mode is deactivated has been fixed.
- The **system end** command has improved to display the *scheduled* state when the subscription renewal is scheduled for the next day.
- A new command named **keyboard** has been added to the system. This command allows you to set the console key map.
- The installation module has been improved to allow the creation of partitions larger than 2TB.
- The SNMP agent has been enhanced to give SSDs lifetime.
- The **ip** command has been fixed to do not allow names for pinged servers in static routes.
- Some minor bugs have been fixed.

Version EH-1.3.6 (9 March 2018)

- The Web proxy default access rights have been modified to allow the "PATCH" method in both forwarding and reverse modes.
- The **waf** command has been enhanced to offer the possibility to globally allow or deny the "PATCH" method as an insecure HTTP method.
- Custom WAF rules has been extended to support the "PATCH" HTTP method.
- The **apply** command has been fixed to properly check the integrity of destination NAT rules and do not erroneously produce the error 212.
- The internal firewall rules have been fixed to properly allow DHCP request broadcasts and lease renewals.
- The **dhcp report** command has been fixed to display DHCP lease end times in local time instead of UTC time.
- Some minor bugs have been fixed.

Version EH-1.3.5 (8 January 2018)

- The antivirus module has been enhanced to bypass a white list of domain names. Therefore the **antivirus whitelist** usage form of the **antivirus** command has been modified to allow you to define a white list of domain names as well as a white list of virus signatures.
- The Web proxy default access rights have been modified to allow the "PUT", "DELETE" and "TRACE" methods in both forwarding and reverse modes.
- The **setup** command has been enhanced to use dialogues boxes.
- The dialogue box version of the **setup** command has been enhanced to allow you to set the timezone in the virtual edition.
- The virtual edition has been enhanced to set the console keyboard layout during the first startup.
- The bug making the guarding module to crash with some malformed URLs has been fixed.
- The textual configuration view in the Web GUI has been improved to have a more user-friendly representation of the whole configuration.
- Some minor bugs have been fixed.

Version EH-1.3.4 (17 September 2017)

- Communication between the appliance and the patch download service has been switched from HTTP to HTTPS.
- Communication between the appliance and the subscription/registration service has been enhanced to support HTTPS.
- Custom WAF rules have been enhanced to allow the specification of more than one HTTP method separated by the pipe character.
- The **waf** command has been enhanced to offer the possibility to globally allow or deny insecure HTTP methods such as "PUT", "DELETE", "CONNECT" and "TRACE".
- Some minor bugs have been fixed.

Version EH-1.3.3 (4 September 2017)

- The bug that prevented caching big objects has been fixed.
- ICP (RFC 2187) has been replaced by HTCP (RFC 2756) for communications between cache peers.
- The **dns** command has been enhanced to allow the explicit resolution of all names to IPs.
- Custom WAF rules has been extended to support the "PUT", "DELETE", "CONNECT", "OPTIONS" and "TRACE" HTTP methods.
- Some minor bugs have been fixed.

Version EH-1.3.2 (20 July 2017)

- The Web cache is no longer cleared after the antivirus activation.
- The RAM vs HDD capacities tuning has been improved to have better performance for the caching.
- The memory consumption for the caching has been improved and the usage of the available persistent cache has been reviewed accordingly.
- Due to the instability of the compress mode while combined with the antivirus mode, the compress mode is automatically disabled for forwarding web traffic when the antivirus mode is activated. This fix should be considered as a workaround before the complete resolution of the issue in future releases.
- The bug that prevented saving logs has been fixed.
- The bug that prevented activating the DHCP server has been fixed.
- Due to a high number of InvalidState and IllegalSyn rejected TCP packets on networks, rejected InvalidState and IllegalSyn TCP packets are no longer logged.
- Some minor bugs have been fixed.

Version EH-1.3.1 (29 June 2017)

- The antivirus module can now be used as a service by external systems such as an MTA (Mail Transfer Agent).
- The antivirus module has been enhanced with the possibility to integrate a white list of virus names to eliminate false positive matches.
- The authentication mode has been upgraded to support the Kerberos protocol.
- The **system report** usage form of the **system** command has been enhanced to print the total number of blocked or allowed contents.
- The WAF has been enhanced to offer the possibility to expose original HTTP error messages generated by backend Web servers.
- The time format in all logs has been changed to be compliant with the RFC3339 (with the caveat that the time offset format may not be respected for some logs).
- The compression module has been fixed to properly compress javascript files.
- The embedded firewall has been enhanced to protect against UDP flood attacks.
- The CA certificate bundle has been updated to its latest version.
- The subscription system has been fixed so the renewal of an expired subscription takes into account the date of purchase as the start date. In this case, the renewal is done for the given period rounded to the nearest whole day.
- The subscription system has been fixed so the reactivation of a suspended appliance is completed without errors.
- The dashboard layout has been enhanced.
- A **Donate** button has been added to the Web GUI of the free edition in order help us to maintain CacheGuard-OS and and develop new features
- The trial period has been extended from 15 to 21 days.
- Some minor bugs have been fixed.

Version NG-1.2.6 (29 December 2016)

- The upgrade from v1.2.4 to v1.2.5 by applying a patch has the side effect that some processes swap on disk. This issue has been fixed by applying a patch to upgrade to the present version. Please note that for the v1.2.5, CacheGuard-OS requires a minimum of 1 GB of RAM to activate the antivirus mode. Therefore if the antivirus mode is activated on an appliance running under the v1.2.5, the applying of the patch may require upgrading the RAM on the target machine. Otherwise the appliance may stop working properly.

Version NG-1.2.5 (21 December 2016)

- A workaround has been added to the system to resolve the inability of some Microsoft (TM) OS's to download updates while the compress mode is activated.
- The upload of a local configuration file from the Web GUI has been fixed to support Web browsers other than Firefox.
- The Web GUI has been upgraded to support Microsoft (TM) IE11.
- The antivirus basic module has been upgraded to its latest version.
- Some minor bugs have been fixed.

Version NG-1.2.4 (20 October 2016)

- The firewall and access control modules have been fixed to support the active FTP protocol with a data port other than 20 (in EPRT and PORT mode).
- The forwarding proxy has been modified to allow the HTTP method OPTIONS. However the method OPTIONS remains denied for reverse websites.
- The CacheGuard logo has been slightly modified.
- The **conf** command has been fixed to properly save authentication modes.
- Network diagrams in the User's Guide have been enhanced.
- The dashboard in the Web GUI has been enhanced to display the available OS updates and the end of the system subscription.
- Some minor bugs have been fixed.

Version NG-1.2.3 (11 September 2016)

- The free edition has been limited to 5 users in forwarding mode and 3 users in reverse mode.
- The syntax of the **register** command has been modified according to the new licensing terms.
- The SSL mediation has been modified to allow the usage of 3DES algorithm to encrypt data between the system and target HTTPS servers.
- The **authenticate mode** usage form of the **authenticate**command has been changed.
- The automatic loading of a URL list has been improved so in the case where a URL list has never been loaded, it is entirely loaded from scratch.
- The bug in the Web GUI that prevented adding new SNMP traps has been fixed.
- The installation program has been fixed to properly generate the default and CA certificates.

Version NG-1.2.2 (2 June 2016)

- A critical bug fix related to the basic forwarding proxy module has been integrated into the system. The bug made the appliance totally unstable.
- The bug that prevented to start the integrated DHCP server has been fixed.
- Some minor bugs have been fixed.

Version NG-1.2.1 (2 May 2016)

- The **guard** command has been enhanced with the possibility to update an existing rule without changing its order in the guard list.
- The CLI has beed enhanced with the possibility to move an element in an ordered list. Commands in question are: **ip**, **guard**, **qos** and **firewall**.
- The Web GUI has been fixed to not change the order of a guard rule in the guard rule list when its associated URL lists are updated.
- The Web GUI has been fixed to not erase the list of URL lists associated to a guard rule when the order of that rule is modified in the guard rule list.
- The redirection to an error page has been fixed in the guarding module to work properly in conjunction with the SSL mediation module.
- Some minor bugs have been fixed.

Version NG-1.2.0 (6 April 2016)

- An SSL mediation (sometimes called inspection) mode has been added to the system. This mode allows you to cache HTTPS traffic and/or block unwanted contents in HTTPS traffic. The **mode** command has been updated to allow you to activate this new feature (**mode sslmediate on**) and the new command **sslmediate** has been added to the system in order to configure the SSL mediation module.
- A new command named **urllist** has been added to the system. This command replaces the **guard category** usage form of the **guard** command. URL lists can be used by the **guard** command but also the new command **sslmediate**.
- The IP routing has been enhanced to support the usage of multiple gateways to route the traffic to the same network.
- The Linux kernel has been upgraded to the latest stable version.
- Concurrent accesses to loaded files have been improved to avoid any file overwriting.
- The system patching has been improved to load patches directly from official CacheGuard servers.
- A download progress bar has been added to backup management and patching pages in the Web GUI.
- The installation program has been enhanced to detect USB Ethernet adapters.
- All major basic modules have been upgraded to their latest versions.
- The **access** command documentation has been fixed (removal of **rweb** access).
- Some network activity reporting has been added to the system.
- A dashboard has been added to the Web GUI.
- The udpeer and tcpeer ports have been respectively renamed to icppeer and httppeer.
- The SFTP is now supported to load/save files.
- Some default port numbers have been changed.
- Some minor errors have been fixed in the documentation.
- Some minor bugs have been fixed.

Version NG-1.1.5 (3 December 2015)

- The value of the "X-Forwarded-Proto" header which is added to requests sent to backend Web servers (in reverse mode) has been fixed as follows: the value "http" or "https" is set depending on whether the client used HTTP or HTTPS to connect to cloaked Web servers.
- The **system** command has been enhanced to display the CPU architecture (32 or 64 bits).
- The patching system has been fixed in order to avoid the applying of the same patch more than once.
- The patching system has been fixed in order to create new empty directories.
- The guard management module has been fixed to update guard rules when a guard policy is deleted.
- The bug in the HA module that blocks the AH protocol used to authenticate HA nodes has been fixed.
- The firewall module has been fixed to not block IGMP snooping when the HA mode is activated.
- The bug that makes erroneous ARP announcements in HA mode has been fixed.
- Internal firewall rules have been reinforced.
- The logging of denied IP packets has been enhanced to report information about the rejection reason.
- The antivirus basic module has been upgraded to its latest version.
- The firewall basic module has been upgraded to its latest version.
- Some minor enhancements have been done.

- Some minor bugs have been fixed.

Version NG-1.1.4 (10 October 2015)

- The bug introduced in version 1.1.3 that prevented to automatically update guard categories has been fixed.
- The security of the VRRP has been enhanced.

Version NG-1.1.3 (5 October 2015)

- The reverse Web mode has been enhanced to allow the specification of a port number and QoS for backend Web servers. After having applied a patch the default port and QoS will respectively be 80 and 100. Therefore the syntax of the **rweb** command has been modified for the usage form **rweb host**.
- The usage form **access rweb** of the **access** command has been suppressed.
- The reverse Web load balancing has has been enhanced to allow the specification of a session cookie generated by Web applications running on backend Web servers. Therefore the syntax of the **rweb** command has been modified for the usage form **rweb balancer**.
- The bug making the guarding policy inconsistent when one of its guard filters has been deleted has been fixed.
- The bug making the configuration of patched system inconsistent after a factory reset has been fixed.
- The HA basic module has been upgraded to its latest version.
- The authentication module has been expanded with a test option.
- Some minor bugs have been fixed.

Version NG-1.1.2 (2 September 2015)

- The CacheGuard OS License Agreement has been upgraded to version 2.1
- IPV6 has been disabled in the Linux kernel.
- The issue to access via the HTTPS proxy to the https://outlook.office365.com website (and similar websites that preferably use IPV6 IP addresses) has been resolved.
- The LDAP authentication module has been optimised so all communications with LDAP servers are forced to use IPV4 only.
- The authentication module has been enhanced to allow LDAP binding during the basic authentication phase instead of comparing the entered password to a predefined password attribute.
- The authentication module has been fixed to allow distinguished names containing white spaces. In the case where the OS is upgraded using a patch the authentication LDAP request should be redefined (see the **authenticate ldap request** command).
- Some minor bugs have been fixed.

Version NG-1.1.1 (1 August 2015)

- The firewall has been fixed to properly manage other protocols than TCP and UDP.
- The IPv6 has been added to the list of supported protocols by the firewall.
- The TLS component management module has been optimised in order to avoid restarting some services when it's useless.
- The bug making a custom WAF rule inconsistent when it contains a star has been fixed.
- Some minor bugs have been fixed in the Web GUI.

Version NG-1.1.0 (13 July 2015)

- **Note**: Please note that to upgrade from version NG-1.0.15 to version NG-1.1.0 you should first apply a patch to upgrade to the version NG-1.0.16. Therefore you would be able to upgrade from version NG-1.0.16 to version NG-1.1.0. Patche files are available at www.cacheguard.net/cacheguard-patch.html.
- The installation program has been fixed to report warnings in respect to setup configurations.
- The reverse mode has been enhanced for HTTPS websites to add an "X-Forwarded-Proto http" header to HTTP requests sent to backend Web servers (useful for some known applications)
- The **apply** command manual has been completed to give additional information in respect to errors reported during the process of checking the RAM capacity.
- A RAM upgrade is now automatically applied after a reboot.
- The **system** command has been enhanced to check for new updates.
- The bug in the **conf** command which caused the saving of wrong values for the QoS attached to "tweb internal" queue been fixed.
- All commands that use a network name parameter (such as access or rweb) have been enhanced to check if the given name is a FDN (Full Distinguished Name).
- The syntax of WAF rules defined in a flat file has been changed. The keyword **regexp** has been replaced by **uri** and **body**. A new feature has been added to WAF rules to allow filtering based on source IP addresses. The keyword **ip** holds this position.
- The DHCP server has been modified to configure DHCP clients with a Web proxy based on the proxy PAC file (ha.pac) delivered by the system.
- A new feature has been added to the WAF to allow you to bypass false positive matches.
- OWASP rule set for the WAF has been upgraded to its latest version.
- The CacheGuard logo has been modified.
- Some minor bugs have been fixed.

Version NG-1.0.16 (13 July 2015)

- **Note**: Please note that no OS has been released for this version but only patch files. Patch files are available at www.cacheguard.net/cacheguard-patch.html.
- The patching program has been fixed in order to properly patch the configuration DB.

Version NG-1.0.15 (9 May 2015)

- The SNI (Server Name indication) support has been added to generated SSL certificates. Therefore more of the same IP address can be shared by multiple HTTPS websites.
- The TLS/SSL support has been hardened to ensure a higher security level.
- Some minor bugs have been fixed.

Version NG-1.0.14 (28 January 2015)

- The bug that causes incorrect dimensioning of the antivirus capacity has been fixed. To fix this issue you should reinstall the appliance as there is no available patch to address this issue (unless you have a support contract).
- Some minor bugs have been fixed.

Version NG-1.0.13 (22 January 2015)

- The high availability management module has been enhanced to not change the state (**failover** or **active**) of a system in HA mode after an apply operation.
- The installation program has been enhanced to report paying configurations.
- The **conf** command has been fixed to properly manage the transparent port configuration (**port thttp**).
- Some minor bugs have been fixed.

Version NG-1.0.12 (29 December 2014)

- The bug making the guards auto update to crash in case of a communication problem with a file server has been fixed.
- The antivirus basic module has been upgraded to its latest version.
- The automatic logout problem in Web GUI has been fixed.
- Some minor bugs have been fixed.

Version NG-1.0.11 (24 November 2014)

- The bug introduced in version 1.0.10 that prevented having more than one reverse website associated to the same IP address has been fixed.
- The bug introduced in version 1.0.10 that prevented activation of the web server when the reverse website list contains HTTPS websites has been fixed.
- Generic WAF rules associated to a reverse website are reset when a reverse website is deleted.
- The **rweb** mode has been enhanced to redirect HTTP to HTTPS for HTTPS reverse websites (if the IP address associated to HTTPS website is used for an HTTP website).
- The bug that makes the reverse website list unsorted after deleting and adding a new website has been fixed.

Version NG-1.0.10 (17 November 2014)

- The reverse website module has been enhanced to deny attempts to access to website names that are not explicitly defined in the system.
- The configuration saving module has been fixed to properly save all generic WAF rules.
- The bug preventing the main proxy to start when the transparent mode is deactivated has been fixed.
- SSH keys management has been improved.
- Some minor display issues have been fixed in the Web GUI.

Version NG-1.0.9 (31 October 2014)

- The apply operation has been improved to ensure that in a High Availability configuration, master IP addresses are owned by an appliance once all functional services have been started on that appliance.
- The Web GUI has been fixed to properly insert, add and remove elements in lists in the same submitted operation (for firewall rules for instance).
- The Web GUI has been fixed to allow you to enter a six digit value for the maximum cached object size (*cache-maxobject.apl* page).
- The bug that prevents activation of the firewall in the following two conditions has been fixed: a non empty auxiliary firewall rule set and the auxiliary network interface not bound to a physical NIC.
- The bug producing an "illegal instruction" error in some virtualization systems has been fixed.
- The console port attached to a serial port is no longer activated if the target machine doesn't have a serial port during the installation.
- The Web proxy accessibility has been modified to allow web traffic incoming from all network interface devices but the external interface.
- The transparent feature has been changed to transparently catch Web traffic incoming from all network interface devices but the external interface. In previous versions, only Web traffic incoming from the internal interface (**web** interface in **vlan** mode) were caught.
- The configuration saving process has been fixed to properly save new guard auto update configurations.
- The traffic shaper module has been improved to allow Web traffic shaping exchanged with the auxiliary network

interface.
- Web GUI pages to save or load the configuration have been regrouped in the same page and improved to allow saving/uploading the configuration to/from the local machine.
- The bug in the *gui/transparent.apl* page that blocks post and reload content operations has been fixed.
- The Web GUI for the page *gui/qos-shape-gateway.apl* has been enhanced with tabs.
- In the Web GUI, font sizes have been reduced and all icons in the top bar have been grouped to the left.
- The caching system has been enhanced to allow the caching of objects greater than the configured max object size for a limited part of the persistent cache.
- The syntax of the **cache** command has been changed to configure a lower and upper size limit for cached objects.
- A new MIB definition has been released for the SNMP agent to include the size of the reserved area on the persistent cache for very big objects.
- The bug that prevents installation of the OS on a Microsoft (TM) Hyper-V VM has been fixed.
- The bug that drops default traffic in case of an empty shaping rule set for routed traffic has been fixed.
- The QoS rule compilation for reverse websites has been optimised.
- The bash shellshock vulnerability has been fixed.
- Some other minor bugs have been fixed.

Version NG-1.0.8 (24 September 2014)

- The Web Auditing GUI has been fixed to properly display post arguments without evaluating html tags.
- The cache size and memory usage tuning has been reviewed according to recent statistics.
- The installation program has been enhanced to allow the deactivation of some features that require lots of storage space on disk. This allows you to install the system on machines with low storage capacity.
- The bug related to the premature display of the termination message of some system operations has been fixed.

Version NG-1.0.7 (11 September 2014)

- The Web GUI has been improved to allow the displaying of long list in different pages.
- The bug that prevents applying custom WAF rules has been fixed.
- The configuration saving has been modified to save restricted administrator users. The saving is limited to login names only (passwords and configurations related to each restricted administrator are not saved).
- In order to ensure command syntax coherency the keyword **raz** has been replaced by **clear** in the **waf rweb custom** command usage form.
- Some other minor improvements have been added to the system to manage the configuration.
- Some other minor bugs have been fixed.

Version NG-1.0.6 (1 September 2014)

- The High Availability module has been improved to ensure that master IP addresses are owned by an appliance once all functional services have been started on that appliance.
- The email syntax checking has been fixed to allow the usage of dash in an email address.
- The reporting of the antivirus last update date has been fixed to display the actual date.
- The configuration settings present in the form of a list have been modified in two ways: lists are kept sorted if the order of elements in the list is not significant. TLS objects and guard categories are some examples of those lists. For ordered lists like firewall rules and shaping rules for routed traffic, the keyword **insert:** has been added to the related management commands to allow the insertion of and element before another one. This avoids to have to save, edit and load the configuration settings.
- The Web GUI has been improved to allow the insertion of elements in lists subject to insertion. The look and feel of pages managing those list has also been improved.
- The **firewall** command has been change to allow the definition of rules with **any** as the output network interface.
- In order to avoid a false positive rule matching by the configured WAF for the Web GUI, **tftp** has been renamed to **ftp_trivial** in the **firewall** command.

Version NG-1.0.5 (7 August 2014)

- A major bug preventing the main proxy to start in some circumstances has been fixed. These circumstances were as follows: transparent mode is off, the transparent list contains at list one network and at least one share or HA peer is configured.
- Backup and restore operations have been fixed to restore properly restricted administrators.
- The patching operation has been optimised but remains manual until a possible next version.
- A new command named **ha** (High Availability) has been added to the system. Combined with the argument **master**, this command allows you to make an attempt to reactivate a master appliance which has been marked faulty without needing to reboot the appliance.
- The Web GUI has been improved to log administrators logins.
- The panel board menu has been improved to allow access to menu items without sub menus.

Version NG-1.0.4 (29 July 2014)

- A critical bug regarding the activation of VLANs and bonding interfaces making the appliance inconsistent and out of service has been fixed (bug introduced in error in the precedent version).
- The timezone setting during the installation has been taken again into account (bug introduced in error in the precedent version).
- The firewall configuration has been modified to give higher priority to NAT rules than the SNAT (Source NAT)

mode.
- The IP routing configuration has been fixed so route to a single host can operate properly.
- The installation program has been enhanced to set a default value for the WAF limit files which is less than or equal to the maximum size for uploaded file given during the installation.
- The Web GUI bug that prevents activation of administration services has been fixed.
- IP routing has been fixed to allow routing via a gateway connected to the auxiliary interface.
- The bug that prevents having an IP route without having a default route has been fixed.
- The textual configuration displaying has been enhanced.
- The auto logout for the Web GUI has been fixed.

Version NG-1.0.3 (21 July 2014)

- The Web GUI bug that prevents changing the Web GUI password with a password containing the characters '$' or '!' has been fixed.
- The verification of input values for online commands and the Web GUI has been enhanced.
- The firewall module has been fixed to allow traffic with **any** as the protocol.
- The Web authentication module has been fixed to allow authentication for reverse websites.
- The Web GUI has been improved to avoid false positive matches by generic WAF rules.
- The FTP proxy over HTTP has been fixed to display properly directory contents.
- The bug that prevents having more than one HTTP reverse websites configured with the same IP address has been fixed.
- Some other minor bugs have been fixed.

Version NG-1.0.2 (14 July 2014)

- The bug that prevents HTTPS reverse websites deleting has been fixed.
- The apply operation integrity check has been fixed to prevent error messages when the VLAN mode is activated.
- When a reverse website present in several forms (HTTP, HTTPS, with multiple IP addresses) is deleted, all its configurations (backend Web servers, load balancing, standby mode...) are preserved until the deletion of its last occurrence.
- The total arguments length limit for the Web GUI has been fixed so the firewall can be configured properly using the Web GUI.

Version NG-1.0.1 (12 July 2014)

- A minor bug related to the synflood tuning has been fixed
- A minor bug related to the URL blacklist message page has been fixed.

Version NG-1.0.0 (CacheGuard OS Version 6) (30 June 2014)

- The QoS management has been enhanced and the syntax of the **qos** command has also been changed. Now the keyword **bandwidth** should be specified to define bandwidth limits and the borrowing of the excess bandwidth can be activated or deactivated using the keyword **borrow**. Also the traffic shaping could be specified as a percentage or as a fixed value in Kbps. Other traffic than the traffic destined to the appliance itself (the gateway) could also be shaped in this version.
- Keywords "intern" and "extern" have been respectively renamed to **internal** and **external**.
- The CacheGuard License Agreement has been upgraded to version 2.0. In this version all CacheGuard Software components are subject to the GNU General Public License v3 while the aggregation of those components and other Open Source Software (as OSI definition) forming the "CacheGuard OS" is licensed under the "CacheGuard OS License Agreement version 2.0".
- An SNMP agent and trap sender has been added to the system to monitor the appliance. Please use the **admin snmp** command to configure the SNMP monitoring.
- Keywords related to SSL/TLS have been changed in the **admin** and **authenticate** commands for coherency purposes.
- A new feature has been added to the system so the system can be backed up and restored (see the **system backup** command)
- A contact email address may be specified with the **register** command.
- The Linux kernel has been upgraded to a latest stable version.
- The access list management for file and monitoring servers has been improved to allow the adding of host names in addition to host IPs.
- The ntp server management has been improved to allow the adding of ntp server names in addition to ntp server IPs.
- The keyword **https** in the **admin** command has been renamed to **tls** as the generated certificate is used by both the Web GUI and the SNMP agent.
- A new logical network interface named **auxiliary** has been added to the system. You can use it for your specific needs (for instance to implement a DMZ or a Back Office zone).
- The syntax of the **firewall** command has been changed.
- Software RAID support has been added to the system.
- The OS is now available in two versions: 32 bits and 64 bits.
- New filter types based on time, authentication and IP ranges have been added to URL guarding module. Therefore the syntax of the command has been completely reviewed. Please refer to the **guard** command documentation for further information.
- In the **authenticate** command, the argument "attribute" has been renamed to **request**.
- Transparent traffic is clearly distinguished from forwarding traffic. A dedicated port is used for the transparent

mode and a new command named **transparent** can manage the transparency for selected networks. Also the QoS module manages forwarding and transparent traffic separately.
- The syntax of the **rweb** command has been changed so the management of SAN and wildcard certificates became easier.
- The load balancing policy may be configured for reverse websites. This new feature includes the possibility to have sticky connections.
- The installation program has been improved.
- In order to ensure command syntax coherency the "access" and "virus" logs have been renamed respectively to to **web** and the **antivirus**.
- The logging module has been enhanced to allow the logging of denied packets by the IP firewall.
- In logging mode (mode log is activated) each log type (firewall, web, rweb, guard, virus, waf) can selectively be activated or deactivated.
- Many minor bugs have been fixed.

Version 5.7.7 (4 July 2013)

- The **system** command has been improved to display the subscription end date.
- A new feature has been added to the health panel to report the status of the antivirus and URL guard updates.
- The Web GUI look and feel has been enhanced.
- Some minor bugs have been fixed.

Version 5.7.6 (28 February 2012)

- A new subscription verification module has been added to the system.

Version 5.7.5 (20 October 2011)

- Some minor bugs have been fixed in the Web GUI.
- The log rotation system has been fixed to properly rotate the WAF log.

Version 5.7.4 (12 October 2011)

- The OS has been improved to support a better crash recovery.

Version 5.7.3 (15 August 2011)

- Installation in test mode has been improved to allow choosing the OS to load at bootup.
- The mgt (for management) vlan has been renamed to mon (for monitoring).
- The keyword mgt (for management) in the **access** command has been renamed to mon (for monitoring).

Version 5.7.2 (11 July 2011)

- The command "factoryreset" has been removed and replaced by the argument **factoryreset** added to the **conf** command.
- Reporting capabilities has been added to the proxy cache module (see the **cache report** command).
- Reporting and health checking capabilities has been added to the system (see the **system report** command).

Version 5.7.1 (20 June 2011)

- The proxy cache module has been upgraded to its latest version.
- The bug that prevents downloading small video files while the cache and antivirus mode are both enabled has been fixed.
- The command "filter" was renamed to **waf** (for Web Application Firewall).
- In the **mode** command, the keyword "filter" was renamed to **waf**.
- In the command "log", the keyword "filter" was renamed to **waf**.
- In the **antivirus** command, the keyword "clear" was renamed to **create**.

Version 5.6.10 (27 May 2011)

- The antivirus no longer checks images and textual contents.

Version 5.6.9 (20 May 2011)

- The minor bug related to the PUA mode activation has been fixed in the Web GUI.
- All diagrams in the documentation has been enhanced with new icons.

Version 5.6.8 (16 May 2011)

- The persistent caching module has been enhanced for better disk caching performance.
- The antivirus module has been upgraded to its latest version to fix several internal bugs.
- The antivirus no longer checks video contents.
- The syntax of the **antivirus maxobject** command has been changed.
- Now files larger than the limit configured with the **antivirus maxobject** command won't be scanned by the

antivirus.
- A new command named **setup** has been added to the system. This command is automatically executed when you first connect to the system.

Version 5.6.7 (25 April 2011)

- The Web GUI look and feel has been enhanced.
- The Web auditing GUI has been fixed to display properly all virus and guard logs.
- Now the **antivirus update report** command also displays the last automatic AV update.

Version 5.6.6 (20 April 2011)

- The minor bug related to the trial version initial date has been fixed.

Version 5.6.5 (14 April 2011)

- Now the proxy is allowed to connect to ports between 1024 and 49151.
- The bug that prevents clients connecting to the internal DNS when the appliance doesn't use itself as a DNS has been fixed.

Version 5.6.4 (4 April 2011)

- The CacheGuard Logo has been changed.
- The licensing key system has been revised.
- The Web GUI look has been revised.

Version 5.6.3 (2 February 2011)

- The integrated AntiMalware software has been upgraded to its highest version.
- The Web Audit module has been improved to show denied URLs and attempts to access Malware.
- Accessing Web sites that use NTLM / SSPI authentication works now with latest IIS Web servers when the compress or filter mode are activated.

Version 5.6.2 (28 January 2011)

- Setting auto update for blacklists has been fixed in the Web GUI.
- The whole documentation has been reviewed.
- Some other minor bugs have been fixed.

Version 5.6.1 (17 June 2010)

- The installation program has been enhanced to allow the booting and installing of the OS from a USB memory stick.
- The Linux kernel has been upgraded to the version 2.6.34 and all required drivers have been integrated to support the latest hardware.
- Some minor bugs have been fixed in the Web GUI.
- The default serial speed has been changed to 115200.
- Some optimisation has been made to reduce the CDROM image size.

Version 5.6.0 (18 March 2010)

- An AntiMalware (Virus, Trojan, Worm) has been added to the appliance.

Version 5.5.5 (28 February 2010)

- The Web GUI has been enhanced to allow direct accesses to menu boards from the main bar menu.

Version 5.5.4 (16 February 2010)

- The tuner module has been enhanced to manage parallel Web requests more adequately.
- The guarding module has been enhanced to allow or deny the usage of direct IP addresses instead of domain names.
- The Web Audit module has been fixed to print messages properly.
- An anti-malware has been added to the appliance in beta test mode.
- The backup retention policy for logs has been changed so the system backs up logs for a period of 30 days.
- A new feature has been added to the system so unwanted Web access and rejected requests to protected Web servers are all logged in separated files.

Version 5.5.3 (15 December 2009)

- The Web GUI has been fixed to properly refresh logs when an explicit refresh is invoked.
- A new option has been added to the Web GUI to clear the persistent Web cache.

Version 5.5.2 (30 November 2009)

- The Web GUI has been fixed to properly display the top main menu in ie8.

Version 5.5.1 (16 November 2009)

- The guarding feature has been reinforced so that Web users are no longer allowed to directly use IP addresses instead of domain names to bypass URL filters.
- In the Web GUI, clear passwords has been removed from displayed reports.
- The Web GUI has been enhanced to support IE8.

Version 5.5.0 (13 October 2009)

- The **user** command has been removed and replaced by the argument **user** added to the **admin** command.
- A new command named **cache** has been added to the system. This command allows management of some cache parameters.
- The **forceloadurl** command has been removed and replaced by the argument **loadurl** added to the new **cache** command.
- The argument "denyurl" has been added to the **filter** command. This argument allows you to set a specific URL to redirect to when an HTTP request is blocked.
- The filter and compress modules have been improved to support accessing Web sites that use NTLM / SSPI authentication (even if NTLM/SSPI is not compliant with HTTP).
- The URL blacklist auto updating module has been enhanced to properly download all remaining files since the last update process.
- The file transfer module has been improved to manage errors during file transfer.
- The Web GUI has been modernized and improved.
- The User's Guide has been enhanced.
- USB keyboards are now supported.
- Some internal minor bugs have been fixed.

Version 5.4.2 (15 March 2009)

- An option to manage SSL CA chain has been added to the **rweb** command.

Version 5.4.1 (22 February 2009)

- The syntax of the **guard** command has been changed and new guard management features have been added to the appliance. An option allows you to update an existing blacklist category from a diff file. A second option allows you to automatically update a blacklist category since the last update/create date until today. It is also possible to program automatic blacklist category updates. Also the blacklist category save option has been removed.

Version 5.4.0 (2 January 2009)

- An LDAP authentication mode has been added to the appliance.
- The bug that prevented connection to internal NTP servers has been fixed.

Version 5.3.7 (25 Nov 2008)

- Now the multi CPU mode is activated during the installation if there is more than one installed CPU.
- A Huge Memory management mode (RAM > 4GB) is now available on the standard CDROM and can be chosen during the installation.

Version 5.3.6 (20 Nov 2008)

- The crash management module has been enhanced.
- The bug in the Health Checking module that inadvertently restarted services has been fixed.
- Now the **rweb** mode is turned off by default.
- An option to cancel the running **apply** operation has been added.
- The patching module has been completely reviewed.
- The Web auditing GUI has been enhanced.
- Generic content filtering rules have been updated.
- The reverse web auditing GUI properly displays all warning messages.
- The reverse web mode works properly even if there is only one declared HTTP Web site name.
- The reverse web mode works properly even if there is no DNS declared.

Version 5.3.5 (16 Sept 2008)

- Some internal minor bugs have been fixed.
- The CacheGuard License has been upgraded to the version 1.2. Now you can edit and modify the proprietary part of CacheGuard for your exclusive personal use. You still may not, except as permitted by applicable law, loan or create derivative works from the proprietary part of CacheGuard (see the new license).

Version 5.3.4 (28 Aug 2008)

- A CSS (Cascading Style Sheets) was added to the Web GUI.
- SSL v2 is no longer supported when the appliance acts as a reverse Web proxy (only SSL v3 and TLS v1.0 are supported now).

Version 5.3.3 (29 May 2008)

- In the Web GUI, the **logout** screen properly displays all images.

Version 5.3.2 (8 May 2008)

- The connection to the Web auditing GUI works properly when the Guarding mode is deactivated (concerns only appliances installed for less than 20 users).

Version 5.3.1 (20 March 2008)

- The HTTP Transparent and HTTP Compress combination mode problem that produces some inconsistent HTTP requests has been fixed.
- Synflood rules are less aggressive so overloaded Web browsing works properly without faulty rejects.
- Textual output has been formatted to comply vt100 terminals.
- The power-off button on SPC appliances works now and shuts down the system properly.
- The LCD display on SPC appliances works properly.
- The **conf diff** command has been optimised.
- A "Show Configuration" option has been added to the Web GUI.

Version 5.3.0 (14 March 2008)

- The furtive error while adding a list item in the Web GUI has been corrected.
- Connections to next peers work properly.
- Object sharing between cache peers has been optimised.
- All source codes are rebuilt using gcc v4.1.2.
- All basic packages have been upgraded.
- The **halt** command can power off the system even if the administrator is remotely logged in.
- The support of old Pentium Pro CPU has been added to the Linux kernel.

Version 5.2.8 (23 December 2007)

- The memory usage has been optimised.

Version 5.2.7 (1 December 2007)

- The number of parallel connections from peers is not restricted. Peers are considered as trusted parties that do not generate flooding traffic.
- The free trial version for more than 10 users has been limited to 15 days. When the trial period is about to end, the **apply** command no longer applies a new configuration unless a valid license key is installed.

Version 5.2.6 (24 November 2007)

- In Anonymous mode, the "WWW-Authenticate" header is no longer hidden.

Version 5.2.5 (5 November 2007)

- A Synflood guarding has been added for traffic labeled **other**.
- The number of parallel connections per client IP address has been restricted, which allows this release to stop flooding.
- Bug fix: The log rotation process has been fixed to save logs with the correct date and time.
- Bug fix: The IP address configuration has been fixed when the HA mode is deactivated.
- This is the first stable version.

Version 5.2.4b (1 November 2007)

- The Synflood guarding module has been enhanced for Web traffic.
- The Linux kernel has been upgraded to 2.6.23.1.

Version 5.2.3b (26 October 2007)

- Multiple reversed HTTP Web sites may be associated to the same public IP address.
- The brute force attack guarding module has been enhanced for Web traffic.

Version 5.2.2b (21 October 2007)

- The Web GUI audit module is activated even if the **filter** and **rweb** modes are not activated.
- In the **rweb** command, when adding a reversed Web site name, a mandatory IP address must be given for a HTTP Web site as well as for a HTTPS Web site.
- The QoS policy for a reversed Web site has been changed to be based on its public IP address.
- Some minor bugs have been fixed in the QoS module.

Version 5.2.1b (12 October 2007)

- The Web GUI has been optimised.
- Bug fix: The configuration loading works properly even if the file to load does not exist.
- The reverse Web auditing documentation has been enhanced.
- Passwords having a length of 9 or greater are supported.
- FTP and TFTP protocols are supported by the Firewall.
- In High Availability mode all services are activated properly after configuration changes.

Version 5.2.0b (5 October 2007)

- X-Forwarded-Host, X-Forwarded-Server are removed from HTTP headers requests - X-Forwarded-For is also removed if no Next Peer is declared when the anonymous mode is activated.
- Port numbers for Next Peers can range from 0 to 65535 (see the **peer** command).
- An audit mode is integrated with the content filtering module. Auditing allows the inspection of HTTP request content and facilitates the filtering rule design process (see **admin**, **filter** and **port** commands).
- A "Logout" link has been added to the Web GUI.
- Deleting an administrator user works properly.

Version 5.1.2b (1 October 2007)

- The Via header is removed from all requests even if the anonymous mode is not activated.
- In the command **port**, the keyword "webadmin" was renamed to **wadmin**.
- In the command **password**, the keyword "webadmin" was renamed to **wadmin**.
- In the **rweb** and **transaction** commands, the keyword "print" has been renamed to **show**.
- Bug fix: The ftp passive mode can now be activated properly.
- The administration access topology can now be configured with the **admin** command.

Version 5.1.1b (22 September 2007)

- Bug fix: the website deleting with the **rweb** command works properly and all related custom filters are removed.
- Bug fix: custom filter rules are properly applied to the running configuration and appropriate services restart.

Version 5.1.0b (20 September 2007)

- TRACK and TRACE methods are denied for the embedded Web server and all hosted Web servers even if the filtering mode is not activated.
- Content filtering is only applicable in reverse Web sites and does not affect the forwarding proxy.
- Custom content filtering based on regular expressions is operational.
- The syntax of the **guard** command has been changed.
- The **conf** command is optimised to run faster.

Version 5.0.0b (9 September 2007)

- The content filtering mode (**filter** mode) for reversed Web sites is operational. When the **filter** and **rweb** mode are activated, requests on protected Web sites are filtered for generic attacks (xss, sql injection...), protocol violations and other anomalies.
- The content filtering is hardened for the Web GUI.
- The configuration is properly saved for backend servers associated to a Web site.
- Guard categories are created even if the **guard** mode is deactivated.
- Guard black and white lists are loaded properly (the given file name must not include ".domains", nor ".expressions" nor ".urls" nor the ".gz" extensions).
- Setting VRRP in the Web GUI works correctly (a wrong content filtering rule was previously set in error).

Version 4.1.6b (2 September 2007)

- By default Route Tracing (traceroute) is allowed from the internal zone to the external zone.
- Bug fix: The Web GUI for the firewall configuration (Menu items "Security/External Firewall" and "Security/Internal Firewall") was fixed to work properly for long content.
- The content filtering for the Web GUI is more permissive for punctuation characters.
- Some other minor bugs were corrected.

Version 4.1.5b (28 August 2007)

- The licensing is also based on the number of Web Sites to reverse.
- The "Hard Factory Reset" procedure resets properly the "admin", "superadmin" and the root passwords.
- Images in the User's Guide available from the Web GUI are shown properly.

Version 4.1.4b (22 August 2007)

- The network installation and its documentation are improved (Mainly: the TFTP IP Address is guessed and if the installation fails, the installation environment is properly reset to give the ability to relaunch the installation).

Version 4.1.3b (17 August 2007)

- Bug fix: The port forwarding integrity is properly checked during the **apply** operation (Cannot NAT the destination IP to the appliance itself).
- Bug fix: When adding firewall rules using Web GUI, an empty entry does not add an "any to any" rule. To specify an "any to any" rule the keyword **any** must be specified for the Source IP, the Destination IP or the Ports field.
- Bug fix: The QoS/Incoming Flows menu item works properly in the Web GUI (Bug due to contenting filtering in the Web GUI).
- Bug fix: Web Site adding works properly in the Web GUI (Bug due to contenting filtering in the Web GUI).

Version 4.1.2b (13 August 2007)

- Bug fix: Network traffic other than Proxy traffic (HTTP, HTTPS and FTP) are shaped properly without abnormal slowdown.

Version 4.1.1b (10 July 2007)

- The Appliance could be installed properly using a PXE network device. The TFTP server IP address is configurable during installation.

Version 4.1.0b (9 July 2007)

- The Web GUI security has been improved.
- Bug fix: Native IP addresses could be setup properly in the Web GUI.
- The **rweb** VLAN is configurable using the Web GUI.
- The reverse mode is configurable using the Web GUI.
- The keyword "confcert" was renamed to **genssl** (related commands: **rweb** and **admin**).
- When an HTTPS reverse Web site is deleted, the associated host list is erased only if no other external IP address is associated with this HTTPS Web site.

Version 4.0.0b (24 June 2007)

- A **reverse** mode is at last available in this version. This mode allows you to implement the appliance as a reverse proxy in front of Web servers to secure, accelerate and shape Web traffic. (see the **mode** and **rweb** commands).
- SSH key loading works properly.
- SATA storage controller are supported again in this version (support was accidentally removed from the previous version).
- The keyword "gencert" is renamed **confcert** in the **admin** command.

Version 3.5.0b (4 June 2007)

- The QoS bandwidth shaping works properly for all types of traffic.
- The syntax of the **qos** command has changed.
- The QoS management can be deactivated using the **mode** command.
- The "fw" command has been renamed to **firewall**.
- This is an intermediate version before a main one supporting the **reverse** mode.
- The reverse mode is named **rweb** and some related commands are already integrated in the present version (but the **rweb** mode is not yet operational):
  - The reverse mode could be activated using the command: **mode rweb on**.
  - The forward mode could be deactivated using the command: **mode web off**.
  - A new vlan named **rweb** is available for Web servers.
  - A Filtering mode is integrated to inspect inside Web requests (see the **mode filter** command).
  - Allowed Web servers can be restricted to those declared with the **access rweb**... command.

Version 3.4.0b (2 May 2007)

- The certificate generation procedure for the Web GUI supports white spaces in entries.
- The alter image mode is no longer supported - The core proxy module has changed.
- Time & Date can be setup properly by using the Web GUI.
- The log rotation procedure properly deletes logs older than 10 days (or with a serial number greater than 10).

Version 3.3.2b (12 April 2007)

- The documentation of the **mode** command has been fixed (gateway has been renamed to router).
- The Web GUI is enhanced for the General Feature and Network related modes.
- The Web GUI can show the last apply report even if the configuration is locked.

Version 3.3.1b (10 April 2007)

- In the **mode** command, **gateway** has been renamed to **router**.
- The integrated DHCP server may be activated via the CLI or Web GUI.
- The integrated DHCP server supports a failover mode.
- Network PCMCIA cards are detected.

Version 3.3.0b (28 Mar 2007)

- System and access logs are rotated together even if the access log is empty.
- A VRRP IP address can be associated to the external network interface (Useful for incoming connections via the external network interface, crossing the embedded firewall and destined to internal networks).
- The access to the embedded DNS is allowed.
- In HA mode, the vrrp multicast is allowed for all IP in the local network (and not only for declared HA peers).
- In HA mode, if the health checker cannot properly restart all vital service, a fail over is forced. The forced fail over is logged in the daemon.log log file.
- When defining administrator access with the **access** command, an optional netmask could be specified.
- Bug fix: The configuration difference is correctly displayed in the Web GUI.
- The Web GUI is available via the embedded Proxy only when the VLAN mode is deactivated.

Version 3.2.7b (21 Mar 2007)

- Now, the Health Checker is correctly launched and checks all activated services.
- The Web GUI is available via the embedded Proxy.
- Minor enhancements and optimisation.

Version 3.2.6b (14 Mar 2007)

- Bug fix: Now, the tftp command is found during the installation phase.

Version 3.2.5b (10 Mar 2007)

- When loading/saving guard categories, the category type may be optionally specified.
- Security was fixed so that, in VLAN mode, the embedded Firewall allows or denies only traffic to or from the **web** VLAN.
- The syntax of the **access** and **fw** commands has been changed. The access type **other** in the **access** command has been replaced by the **fw** command followed by the keyword **intern**. In the **fw** command, the source IP address and optionally the network mask is specified.
- Other minor bug corrections.

Version 3.2.4b (21 February 2007)

- An optional port number may be defined when adding a Next Peer.
- Support has been added for the SCSI Message Fusion Driver (required for VMware certified version: LSI Logic).

Version 3.2.3b (13 February 2007)

- Support for TFTP to exchange Files with the appliance. To do that, the syntax of the following commands is changed: **access**, **vlan**, **conf**, **system**, **log**, **guard**.
- The completion for the **dns** command supports the keyword **localhost**.
- To respect the command syntax homogeneity, the keyword "snmp" is renamed to **mgt** for the following commands: **access**, **vlan**. The **mgt** keyword specifies "snmp" and other possible management protocols later (The snmp agent is still not integrated in this version).
- The configuration cannot be applied if the internal and external IP addresses belong to overlapped networks (The text of the error number 203 is also modified).
- The **ip** command checks if the given IP address is a valid host IP address (The network and broadcast IP address cannot be given now).
- Bug fix: Swapping between the VLAN mode and Native Mode (mode vlan on/off) restarts adequate services to bind to appropriate network interfaces.
- Bug fix: The system patching (Menu item "File/System Patches") works correctly in the Web GUI now (the "Do Operation" produce the awaited result).
- Other minor bug corrections.

Version 3.2.2b (2 February 2007)

- A shortcut "Apply" button was added to the Web GUI's main menu.
- The keyboard selection during installation was enhanced.
- The **access** command documentation was enhanced.
- The README.txt file in the VMware virtual machine version package was enhanced.

Version 3.2.1b (23 Jan 2007)

- The **apply** command can be applied after a "factoryreset" without adding a DNS server.

- The Web GUI is now compliant with IE7 and FireFox 2.0.

Version 3.2.0b (17 Jan 2007)

- Initial public announcement

Getting Started

CacheGuard-OS is an autonomous OS (Operating System) that transforms an x86/x64 based machine (virtual or bare metal) into a network Security & Optimization appliance. **Caution:** the installation of CacheGuard-OS on a machine, formats all disks on that machine so all persistent data on that machine would be lost.

CacheGuard-OS is based on a Linux kernel and multiple other well-known open source software built from scatch to ensure the maximum level of integrity and security. The mere aggregation of those software and specific software developed by CacheGuard Technologies Ltd forms CacheGuard-OS. Note that CacheGuard does not depend on a particular Linux distribution because it is by itself an appliance oriented Linux distribution.

Open source software used by CacheGuard-OS are mainly distributed under the GNU GPL. Open source programs developped by CacheGuard Technologies Ltd are distributed under the CacheGuard License which is a specific open source license. Please read the License Agreement carefully before any usage.

The installation program proposes to install CacheGuard-OS as a Gateway or a Manager system. A Gateway system is actually the system that provides network Security and Optimisation services. If you install several Gateways, you have the possibility to manage them separately one by one or manage them via a centralised Manager. In the latter case, you can install CacheGuard-OS as a Manager on a dedicated machine that you can use as a centralised Manager. Note that you should exclusively select one installation type on the same machine. In other words, the same machine can't act as a Gateway and as a Manager.

The installed Gateway can be used in forwarding mode to protect internel internet users while ins reverse mode, the Gateway secures and optimises network traffic exchanged with Web applications . Both modes can be activated at the same time on the same Gateway.

Machine Requirements

Gateway Machine Requirements

The required machine resource for a Gateway system mainly depends on the total number of users to protect (in forwarding mode) or the maximum number of **simultaneous** users of Web applications to protect (in reverse mode). What we mean by simultaneous users are active users that consume the appliance resources (mainly RAM and CPU). Simultaneous users are distinguished from concurrent users that may be all connected to protected Web applications without necessarily consuming any resources on CacheGuard appliance. On Web applications servers, concurrent users usually consume RAM and/or disk spaces while on CacheGuard, only simultaneous users consume RAM and CPU (number of simultaneous users <= number of concurrent users).

During the installation, the OS is fine-tuned according to the required number of users to support in order to provide the best balance between performances and resources consumption. To provided an optimised quality of service, the tuner program considers that all forward users are not connected at the same time but only 20 percent of them. For instance, an appliance installed for 100 users allows you to protect 100 users/clients and is tuned to run for 20 simultaneous users. In this case, a burst of 100 simultaneous users will be granted for a short period of time.

For 100 users (20 simultaneous users), a typical machine configuration would be:

- Architecture: x86/x64
- CPU: 4 Cores
- RAM: 8 GB
- Disk: 250 GB
- Network: 2 x Ethernet NIC

For more users, prefer a machine with more RAM, CPU cores and disk capacity. As a rule of thumb, add 1 CPU core and 1 GB RAM (+ 75 GB disk in forwarding mode) for every 10 additional simultaneous users. For instance, an appliance that needs to support 40 simultaneous users, requires 6 CPU cores, 10 GB of RAM (+ 400 GB of disk capacity in forwarding mode).

On a hardware machine, CacheGuard-OS is more efficient with several low capacity disks configured as a RAID compared to a single high capacity disk. CacheGuard-OS innately supports software RAID by using 3% of the CPU resources only. Supported RAID levels are as follows: RAID 0 (stripping), RAID 1 (mirroring), RAID 5 (stripping + checksum), RAID 6 (stripping + double checksum) and RAID 10 (stripping + mirroring).

With CacheGuard-OS you have the possibility to activate all integrated security and optimisation features at the same time on the same machine. Some functions like the HTTP real time compression and the antivirus are more CPU intensive than others and the activation of the antivirus requires about 2 GB of RAM. Configuration rules mentioned above can be applied if you plan to activate all available features at the same time. You probably need less resources in case where you don't need to activate all available features together. Please note that in all cases, CacheGuard-OS

requires at least **512 MB** of RAM during its installation.

CacheGuard-OS requires at least **2 NIC** (Network Interface Card). In case where your machine has only one NIC, you have the possibility to use an USB Ethernet adapter as the second NIC. To benefit from link bonding feature and/or to use the auxiliary network interface, you will need additional network interfaces (or USB Ethernet adapters).

Note that CacheGuard-OS can be installed for a minimal number of users on a mini computer. The minimum machine configuration to support 10 users in forwarding mode is as follows:

- Architecture: x64
- CPU: 2 Cores
- RAM: 4 GB RAM
- Disk: 40 GB
- Network: 2 x Ethernet NIC

This configuration allows you to activate all CacheGuard-OS features at the same time on a x64 (64 bits) machine. However, in case where big RAM consumer services such as the antivirus are not required, CacheGuard-OS can run on a machine with only 256 MB of RAM. With that amount of RAM, your CacheGuard-OS based machine would perfectly work as a firewall and VPN server. But as mentioned before, the OS installation would still require at least **512 MB** of RAM.

Manager Machine Requirements

The required machine resource for a Manager system mainly depends on the total number of Gateway systems to manage. To manage 10 Gateway systems, a typical machine configuration would be:

- Architecture: x86/x64
- CPU: 2 Cores
- RAM: 1 GB
- Disk: 25 GB
- Network: 1 x Ethernet NIC

To manage more gateways, prefer a machine with more disk capacity. As a rule of thumb, add 25 about GB of disk capacity for every 10 additional Gateway systems to manage.

Machine compatibility

CacheGuard-OS supports almost all popular x86/x64 based devices in the market. If your device is not detected during the installation, please contact us and we will do our best to integrate adequate drivers into the OS to support your device.

OS Installation

The same installation CDROM can be used to install the appliance as a Gateway system as well as a Manager system. Just follow given instructions during the installation to select the required system to install.

CDROM drive Installation

To install CacheGuard-OS from a CDROM drive, follow instructions below:

- Download the x64 or x86 ISO image file.
- Write the ISO image file to a CDROM using your favourite burner tool.
- Boot your target appliance from the CDROM and follow instructions to install CacheGuard-OS.

USB memory stick Installation

To install CacheGuard-OS from a USB memory stick, follow instructions below:

- Download the x64 or x86 ISO image file.
- Write the contents of the ISO image file to a USB stick and make it bootable. You can use UNetbootin to create your bootable USB stick. UNetbootin can be downloaded from https://unetbootin.github.io/. Alternatively you can use the following Linux command:

  sudo dd if=CacheGuard-OS.iso of=/dev/sdX conv=fdatasync status=progress

  in which you should replace *CacheGuard-OS.iso* by the required CacheGuard-OS ISO file and */dev/sdX* by the device path of your plugged USB stick. **CAUTION**: when using the *dd* Linux command, it is highly important to identify your USB stick device path with grate care. Otherwise you can completely erase your PC/Workstation disks.

- Boot your target appliance from the USB stick and follow instructions.
- Please note that to avoid conflicts with other USB storage devices connected to your machine, the installation USB stick should be plugged in last. This allows the installation program to distinguish the installation USB stick from other USB storage devices.

Network Installation

To install CacheGuard-OS from the network, your target machine should support PXE boot. You will also need an installation server that runs the following services:

- A DHCP server
- A TFTP server

To install CacheGuard-OS from the network, follow the instructions below:

- Recursively copy the cacheguard directory on the installation CDROM to the root directory of your TFTP server (usually /srv/tftp on a Linux server).
- Recursively copy the cacheguard-boot directory on the installation CDROM to the root directory of your TFTP server.
- Recursively copy the isolinux directory on the installation CDROM to the created cacheguard-boot directory on your TFTP server.
- As an example, on a Linux server, if the installation CDROM is mounted on the /mnt/cdrom and if the TFTP server root directory is /srv/tftp, you can use the following commands:
    - sudo cp -rf /mnt/cdrom/cacheguard /srv/tftp/
    - sudo cp -rf /mnt/cdrom/cacheguard-boot /srv/tftp/
    - sudo cp -rf /mnt/cdrom/isolinux /srv/tftp/cacheguard-boot/
    - Then the DHCP configuration file on the Linux installation server should include a section as follows:

```
...
allow booting;
allow bootp;
filename "/cacheguard-boot/isolinux/pxelinux.0";
subnet <network-ip-address> netmask <network-mask> {
    range <first-ip-address> <last-ip-address>;
    next-server <tftp-ip-address>;
}
...
```

    - Please note the **filename** statement above should refer the /cacheguard-boot/isolinux/pxelinux.0 file for an installation on a BIOS based machine. For an installation on an UEFI based machine, the **filename** statement should refer the /cacheguard-boot/pxeboot.efi file.
- Now you can boot the target machine on its network interface that supports PXE (preferably the first interface).

The OVA & VHD distribution forms

The Gateway OVA (Open Virtual Appliance) form uses 2 network interfaces that you should connect to appropriate networks according your requirements. The VHD (Virtual Hard Drive) is a disk image that you can connect to a VM having at least 2 network interfaces connected to appropriate networks. Normally, CacheGuard's external interface should be connected to an internet router or DMZ while it’s internal interface should be connected to the LAN. After having started the VM, login as "admin" (the password is "admin") and follow the setup operation.

VMware ® Notes

For security reasons, VMware tools are not installed and can't be installed on a CacheGuard appliance.

Oracle VirtualBox ® Note

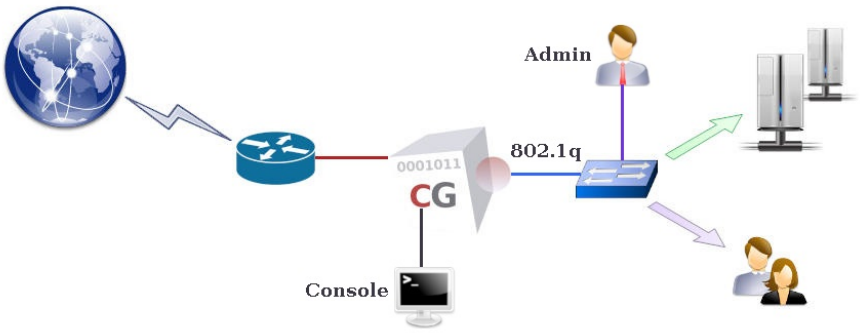
CacheGuard is fully compatible with Oracle VirtualBox ®.

Microsoft Hyper-V ® Note

Please note that if you plan to install CacheGuard on a Microsoft Hyper-V ® VM, think about disabling the MAC address spoofing on your VM.

Gateway Connection

In a basic configuration, CacheGuard Gateway divides your network into two separated areas: an external non trusted area connected to the internet and an internal trusted area connected to your LAN. CacheGuard uses two logical network interfaces. The first network interface is called **external** and the second network interface **internal**. Each logical network interface should be associated to at least one physical network interface.



The link command without any argument displays all detected physical network interfaces in your machine. The command link bond displays associations between logical and physical network interfaces. Use those commands to identify your network interfaces. By default the external network interface is associated to *eth0* and the internal network interface to *eth1*.

Connect the internal physical interface to your LAN and the external physical interface to your WAN (usually your internet router).

Gateway Configuration

First Configuration

To start, connect to CacheGuard console interface and login as the "admin" user. The console interface is one of the following:

- Monitor/Keyboard connected to your machine
- RS232 Serial port (The serial port configuration should be as follows: "115200 8N1")

When you first connect to the appliance the setup command is automatically executed to perform a basic network configuration. You have also the possibility to use the CLI (Command Line Interface) instead of the setup command to make a basic network configuration. To do so, you can use the following commands:

- *ip external 192.168.1.1 255.255.255.0*
- *ip internal 10.20.0.254 255.255.255.0*
- *ip route add default 192.168.1.254*
- *dns add 127.0.0.1*

At this stage, the new IP configuration is not yet active. To activate it, you must execute the apply command (in case where the setup command is used, the apply command is automatically executed).

Basic Configuration

The configuration procedure is straightforward: you run a set of commands to build a new configuration and then you apply that new configuration to activate it in a single transaction. The magical command that allows you activate a new configuration is called apply. This command replaces the running (current) configuration by the newly made configuration. It is important to note that during the phase of creating a new configuration, the running configuration is not affected. Therefore, you have the possibility to tune your new configuration before affecting the running configuration.

The apply command makes a series of verifications to ensure that the new configuration is consistent. If no integrity issues is detected, the apply operation begins and may approximately take between 5 and 180 seconds (depending on requested operations and your machine resources). Please note that the apply command runs in background. This means that after its invocation you can continue to execute some other commands but you can't modify any configurations before the termination of the last apply command. The apply report command displays a state report of its execution.

Many services in CacheGuard-OS depend on the appliance internal clock so setting the right time and date is crucial in running CacheGuard-OS. To setup the time and date of your system, use the following command:

- *clock <YYYY/MM/DD-hh:mm:ss>*
- *apply*

where YYYY/MM/DD-hh:mm:ss are respectively the year, month, day, hours, minutes and seconds. For instance you can use the following: 2024/03/20-03:06:26. You have also the possibility to use NTP servers to setup the time and date. Please refer to the Date & Time documentation for further information.

The rest of the configuration may be done using an SSH client or a Web browser. Only trusted administrators are allowed to remotely manage the appliance. To declare a remote administrator as trusted, add her/his network IP address and the logical network interface via which she/he is allowed to connect to the system to the list of trusted administrators. The access command allows you to manage the list of trusted remote administrators. For instance, to allow an administrator having an IP address in the network *10.20.0.0 255.255.255.0* to connect to the system via the internal network interface, use the following commands:

- *access admin add internal 10.20.0.0 255.255.255.0*
- *apply*

The SSH and Web administration GUI interfaces/services should be activated before usage. To activate both, use the following commands:

- *admin ssh on*
- *admin wadmin on*
- *apply*

To connect to a remote CacheGuard appliance from a Linux system, you can use the "*ssh admin@10.20.0.254*" command, where *10.20.0.254* is the internal IP address of your CacheGuard appliance. To configure a remote CacheGuard appliance using a Web browser, connect to the URL: "***https***://*10.20.0.254:8090*" where *10.20.0.254* is the internal IP address of your CacheGuard appliance. The default SSL certificate provided by the appliance is a self-signed certificate identified by the Id **default** in CacheGuard-OS. Before permanently accepting this certificate as a valid certificate, compare its fingerprint in your Web browser against the fingerprint obtained from your CacheGuard console port by invoking the tls server fingerprint default command. Mind that the protocol used is http**s** and not http. By default, credentials to use to login via the Web administration GUI are the same as those used to login via the console port or via SSH. Think about setting different passwords for the console/ssh interfaces and the Web administration GUI (use the command password login).

Supported features/functions are called modes and they can be activated or deactivated using the mode command. By default, the forwarding Web proxy (**web** mode) as well as the **transparent** mode are activated. The transparent mode allows the appliance to transparently intercept HTTP traffic (TCP port 80) without being obliged to configure your Web browsers (Firefox, Chrome, Edge, Safari...) to use CacheGuard as a Web proxy. With this mode, the routing configuration of your networks should route all HTTP traffic via your CacheGuard appliance. For a basic implementation, your appliance may be your default gateway to the internet (see the Transparent Implementation for further information). In a non-transparent mode (**web** mode), your Web browsers should be configured to explicitly use CacheGuard Web proxy. The CacheGuard Web proxy can be reached at "*10.20.0.254:8080*" where "*10.20.0.254*" is the internal IP address of your CacheGuard appliance.

One interesting mode is the Web caching mode. To activate it, you can use the following commands:

- *mode cache on*
- *apply*

There are plenty of modes in CacheGuard-OS that you can activate or deactivate as per your requirements. The General Modes section in this User's Guide gives you a brief description of each.

At this stage, you can use your appliance as a gateway to connect to the internet and browse the Web. If you need to protect your Web servers by your CacheGuard appliance, you must activate the reverse mode by invoking the mode rweb on and then configure the reverse mode using the rweb command. To get an optimised configuration, it is recommended to deactivate features that are not required. For instance, if you no longer need the forwarding Web proxy, you can deactivate it by using the mode web off command.

The command help gives a brief description of all available commands. To obtain the detail for a specific command, use the help command followed by a command (example: help ip). A completion facility is available when typing commands. To use the completion press the <TAB> key to complete a command or to obtain a list of available arguments.

General Modes

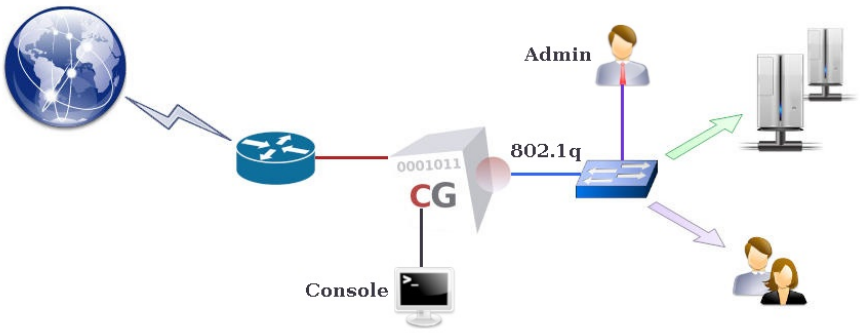
CacheGuard appliance is an integrated appliance that Secures and Optimises the internet traffic by providing a whole range of features. To get a perfectly optimised appliance configuration, it is recommended that you activate features that you actually need and deactivate all others. But if needed, it is possible to activate all available features at the same time on the same appliance and all activated features would work seamlessly and efficiently together.

The mode command allows you to activate or deactivate different features called modes. For almost all modes, there is a command with the same name that allows you to configure that mode. For instance, the embedded firewall can be activated by using the mode firewall on command and the firewall can be configured using the firewall command. We can distinguish two groups of modes: network modes and function modes. Sections below give you a brief description of all avaialble modes. Note that the apply command must be invoked after activating or deactivating a mode.

Network Modes

This section gives a brief description of all network modes. Available network modes operate at the (TCP/UDP) IP level and are as follows:

- DHCP server
- Caching DNS
- High Availability
- Passive FTP
- Quality of Service
- Network Router
- Source NAT
- Transparent Web
- Transparent Web SNAT
- Tagged VLANs



DHCP server

CacheGuard appliance can provide dynamic IP addresses to connected devices ;integrates a DHCP server to dynamically deliver IP . To activate the DHCP server use the mode dhcp on command. You can configure the DHCP server using the dhcp command. That commands allows you the define dynamic IP ranges and, if needed, reserve IP addresses for your devices.

Caching DNS

CacheGuard appliance integrates a caching only Domain Name Server that can be used by all other integrated services but also external clients. To activate the integrated DNS server and make it available to be used by external clients, use the following commands:

- *dns raz*
- *dns add localhost*
- *mode dns on*

High Availability

Two or more CacheGuard appliances can be implemented in a HA (High Availability) mode by using the VRRP protocol. In addition, network interfaces (**external**, **internal**...) of a CacheGuard appliance can be associated to more than a physical network interface to offer link resiliency. To activate the HA mode, use the mode ha on command. Once the HA mode is activated, you must use the vrrp command to associate one or more VRRP IP addresses to at least one

network interface. To associate more than a physical network interface to a network interface use the link command.

Passive FTP

By default, CacheGuard appliance uses the passive FTP protocol to initiate FTP sessions with external FTP servers. To use the active FTP mode, you must deactivate the passive FTP mode. To deactivate the passive FTP mode, use the mode ftppassive on command. Please note that switching between the passive and active FTP modes is done globally (you can't select the FTP mode for particular FTP session).

Quality of Service

CacheGuard appliance can shape and schedule the network traffic to offer QoS (Quality of Service) to your users an applications. Using the QoS manager in a CacheGuard appliance allows you to reserve the required network bandwidth for your most critical applications. To activate the QoS mode, use the mode qos on command. Then, you can use the qos command to configure the traffic shaping at your conveniences. All traffic destined to services (proxy, antivirus...) running on the appliance itself as well as the traffic that is only routed via the appliance are handled by the QoS manager.

Network Router

CacheGuard appliance can act as a network router supporting static routes and multi gateways configuration. Use the mode router on command to activate the router mode. To configure the routing, use the ip route command.

Source NAT

CacheGuard appliance can NAT (Network Address Translation) the source IP address of all outgoing traffic via its external network interface with its own external IP address. This mode is called snat (for source NAT) and you can activate it using the mode snat on command.

Transparent Web

CacheGuard appliance can be transparently implemented in a network to intercept Web traffic in order to be managed (cached, filtered...). In a transparent implementation, there is no need to configure Web browsers to use CacheGuard appliance as a Web proxy. The easiest way to transparently implement a CacheGuard appliance in a network is to use it as the default gateway to the internet. This mode is called tweb (or transparent) and can be activated by using the mode tweb on (or mode transparent on) command. The transparent (or tweb) command can then be used to selectively intercept Web traffic.

As HTTP is increasingly being replaced by HTTPS on the Web, the power of the transparent mode is considerably reduced. But fortunately CacheGuard appliance can also be configured to intercept HTTPS traffic. The transparent interception of HTTPS traffic is called the **sslmediate** mode and is described in the Function Modes section below. The **sslmediate** mode is considered as a function mode rather than a network mode as its implementation requires to deal with SSL CA certificates in addition to the network configuration.

Transparent Web SNAT

In transparent mode (**tweb** is activated), intercepted Web traffic can preserve their real IP addresses or be Source NATed with the CacheGuard appliance external IP address. The **tnat** (transparent NAT) mode allows you to activate (**on**) source IP address NATing of transparently intercepted Web traffic. The **tnat** mode is activated by default. To deactivate it, use the command mode tnat off. Please note that when the **tnat** is deactivated, routed Web traffic should not be asymmetric against CacheGuard appliance (ie. all incoming and outgoing Web traffic exchanged with Web clients should be routed from the same CacheGuard appliance network interface).

Tagged VLANs

CacheGuard appliance supports 802.1q VLAN (Virtual LAN) tagging on its internal network interface to secure and isolate predefined functional traffic (**admin**, **web**, **rweb**...). To activate the VLAN mode, use the mode vlan on command. Once the VLAN mode is activated, you must use the vlan and ip commands to define VLANs and affect IP addresses to them.

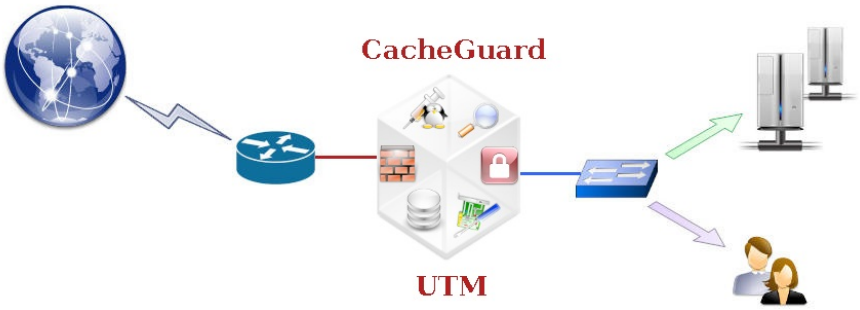
If you activate both the **web** and **rweb** modes at the same time on the same appliance and in your configuration your CacheGuard appliance SSL offloads HTTPS traffic destined to your Web applications (network traffic between CacheGuard and real Web servers are unencrypted), you would probably need to use a distinct VLAN for the **rweb** traffic type. Refer to the rweb command to know how to configure the **rweb** mode for SSL offloading.

Function Modes

This section gives a brief description of all function modes. Available function modes operate at the application level and are as follows:

- Anonymous Browsing
- Antivirus
- Web Authentication

- Statefull Firewall
- Forwarding Web Proxy
- HTTP Compression
- OCSP Responder
- Reverse Web Proxy
- SSL Mediation
- Traffic Logging
- URL Guarding
- IPsec VPN
- Web Application Firewall
- Web Caching



Anonymous Browsing

CacheGuard appliance can alter some HTTP headers to make anonymous Web requests. To activate the anonymous browsing mode, use the mode anonymous on command. Please note that activating this mode can result in being bannded by some websites and thus it is recommendend to let this mode deactivated.

Antivirus

CacheGuard appliance embeds an antivirus that blocks malware (viruses, trojans and worms) in Web traffic destined to Web clients (humans or machines) as well as to Web servers. The antivirus can also be used as service by external systems such as an MTA (Mail Transfer Agent). To activate the antivirus use the mode antivirus on command. The antivirus command can be used to configure the antivirus.

Web Authentication

The embedded Web proxy in CacheGuard appliance can be configured to request LDAP or Kerberos servers to authenticate Web clients before granting them access to the Web (or Web servers in reverse mode). To activate the authentication mode, use the mode authenticate on command. You must then use the authenticate command to configure the authentication.

Statefull Firewall

CacheGuard appliance integrates a stateful firewall that allows you to control the routed network traffic based on its source and/or destination IP addresses and used protocol. In addition, the firewall allows you to NAT the source and/or destination IP of a network traffic. To activate the firewall mode, use the mode firewall on command. The firewall can be configured using the firewall command.

Forwarding Web Proxy

CacheGuard appliance integrates a forwarding Web proxy that allows you to do not expose your users directly to the internet. To activate the forwarding Web proxy mode, use the mode web on command. The Web proxy combined with other modes such as, but not limited to, the firewall, antivirus, URL guarding and Web caching allows you to offer a high level of security and network traffic optimisation to your users.

HTTP Compression

CacheGuard appliance can compress in real time textual contents in Web traffic such as, but not limited to, HTML, CSS and JavaScript contents to save your network bandwidth usage. Use the mode compress on command to activate the HTTP compression.

OCSP Responder

CacheGuard appliance can act as an OCSP responder to check the revocation status of certificates that are signed by its own CA certificate. To activate the OCSP responder, use the mode ocsp on command. If your CacheGuard configuration uses certificates that are signed with its CA certificate, the activation of the embedded OCSP responder can be very useful. Signed certificates can be used by services such as the IPsec VPN server or the reverse Web proxy. You can use the tls command to configure the OCSP responder.

Reverse Web Proxy

CacheGuard appliance integrates a reverse Web proxy that allows you to do not expose your Web servers directly to the internet. To activate the reverse Web proxy mode, use the mode rweb on command. The reverse Web proxy combined with other modes such as, but not limited to, the firewall, antivirus, WAF and Web caching allows you to publish Web applications with a high level of security and network traffic optimisation. Use the rweb command to configure the reverse proxy.

SSL Mediation

CacheGuard appliance can act as an SSL mediator between Web clients (humans or machines) and HTTPS Web servers located on the internet (in the external zone). When the SSL mediation mode is activated, the HTTPS traffic destined to Web clients is decrypted and then re-encrypted before being sent to Web clients. The SSL mediation allows the appliance to inspect HTTPS traffic in order to block malware or cache clean contents. To activate the SSL mediation mode, use the mode sslmediate on command. The SSL mediation mode require that Web clients trust the CacheGuard appliance CA certificate. To manage the CacheGuard appliance CA certificate, use the tls command. To configure the SSL mediation, use the sslmediate command.

Traffic Logging

CacheGuard appliance can log allowed Web traffic as well as blocked (Web or non Web) traffic. The logging gives you visibility into traffic exchanged with or via the appliance. To activate the traffic logging, use the mode log on command. You have the possibility to select which type of traffic should be logged. Logs are stored locally and can also be send in real time to remote syslog servers. Use the log command to configure the traffic logging.

URL Guarding

CacheGuard appliance can act as a URL filter/guard that allows you to restrict the Web usage in your organisation. With the help of the URL guarding you can block the access to categories of websites such as, but not limited to, adult, gambling, hacking and advertisement. To activate the URL guarding mode use the mode guard on command. URL guarding is based on lists of URLS (blacklists or white lists) that you can manage using the urllist command. Use the guard command to configure the URL guarding.

IPsec VPN

CacheGuard appliance embeds an IPsec VPN server that can be configured in site to site (inter site) or remote access mode. The IPsec VPN server combined with the forwarding or reverse Web proxy allows you to implement configurations in which Web clients and/or Web servers communicate with the appliance using secure VPN tunnels. To activate the IPsec VPN server, use the mode vpnipsec on command. Use the vpnipsec command to configure the IPsec VPN server.

Web Application Firewall

CacheGuard appliance integrates a WAF (Web Application Firewall) to protect Web applications against content attacks such as, but not limited to, XSS (cross site scripting), SQL injection and remote code execution. In addition, the WAF can block unwanted Web requests based on IP or country reputation. To activate the WAF, use the mode waf on command in conjunction with the mode rweb on command (the WAF can only operate when the reverse Web proxy is activated). To configure the WAF, use the waf command.

Web Caching

CacheGuard appliance can cache the Web traffic to save your network bandwidth and in some environments accelerate the Web browsing. To activate the Web caching, use the mode cache on command. To configure the Web caching, use the cache command.

Date & Time

Many services in CacheGuard-OS such as, but not limited to, the Web caching, the antivirus and the URL guarding depend on the appliance internal clock. In addition, some periodic jobs should run during off-peak hours to do not penalize end users during business hours. That's whey setting the right date and time is essential to run CacheGuard-OS.

It is also important to note that the current real time on a CacheGuard appliance depends on the time zone in which you are. For instance, to setup the Berlin (in Germany) time zone, you can use the following command:

- *timezone Europe/Berlin*
- apply

You can use the timezonelist command to get the list of all available time zones. The internal clock can be manually configured using the clock command or be automatically setup and maintained with the help of remote NTP (Network Time Protocol) servers.

Manual Setting

To manually setup the date & time use the clock *<YYYY/MM/DD-hh:mm:ss>* command where *<YYYY/MM/DD-hh:mm:ss>* is as follows:

- YYYY is a 4 digits specifying the year
- MM is a 2 digits specifying the month
- DD is a 2 digits specifying the day
- hh is a 2 digits specifying hours
- mm is a 2 digits specifying minutes
- ss is a 2 digits specifying seconds

For instance, a valid date and time specifications can be: *2024/03/20-03:06:26*.

NTP Servers

To maintain an accurate clock on a CacheGuard appliance, it is highly recommended to use secure and reliable NTP servers. For security reasons, we suggest that you rely on 3 NTP servers at least and always rely on a odd number of NTP servers offered by distinct providers. The ntp command allows you to manage NTP servers. For instance, To add an NTP server having the *192.168.0.1* IP address, use the following commands:

- *ntp add 192.168.0.1*
- *apply*

Configuration Management

A CacheGuard appliance is configured and administrated using online commands or the Web administration GUI. There are mainly two types of commands: commands with an immediate action and configuration commands. A CacheGuard configuration is represented by a set of configuration commands invoked with adequate arguments.

Configuration commands can be invoked with or without arguments. Without any arguments, a configuration commands normally displays the related configuration to that command. Invoked with one or more arguments, a command normally modifies the configuration. For instance, the ip command invoked without any arguments, display all IP addresses associated to network interfaces while invoked with a network interface name, an IP address and a mask, it modifies the IP address associated to that network interface. For instance, the "*ip external 192.168.22.254 255.255.255.0*" command set the IP address associated to the "*external*" network interface to *192.168.22.254 255.255.255.0*.

Invoked without any arguments, the conf command allows you to display the list of all configuration commands and their associated arguments that form a configuration. With CacheGuard-OS, there is always a current (or running) configuration and a new configuration. The new configuration may be the same as or different than the current configuration. If a configuration command is invoked with arguments that modify the current configuration, the new and current configuration will differ. It is important to note that invoking configuration commands has no immediate impact on the running configuration.

To activate a new configuration, or in other words to replace the running configuration by a new configuration, the apply command should be invoked. You can use the **conf diff** command to compare the new configuration against the running configuration and display the difference between them.

Command Arguments

There are 4 types of command arguments:

- Scalar arguments like an IP address
- Keyword arguments like **external**
- Boolean parameters (allowed values are **on** and **off**)
- List arguments like a list of static IP routes

A boolean is normally used to activated (value **on**) or deactivate (value **off**) a sub configuration state. For instance, the mode cache on command allows you to activate the Web caching. A list argument is manipulated using the following keyword arguments:

- **add**: adds an element to the end of a list.
- **insert**: inserts an element at before a given element in a list.
- **del**: delete an element form a list.
- **raz**: erases (empties) the list.

For instance, the ip route add *10.0.10.0 255.255.255.0 192.168.60.254* command, adds a route to the *10.0.10.0 255.255.255.0* via the *192.168.60.254* gateway, to the list of static routes; the ip route del *10.0.10.0 255.255.255.0 192.168.60.254* command, removes that route, and the ip route raz removes all routes from the list of static routes.

Applying a Configuration

With CacheGuard-OS, there is always a current (or running) configuration and a new configuration. To activate the new configuration the apply command should be invoked. The apply operation is a background job that can take from seconds to minutes according to the nature of the new configuration to apply and the performances of the machine on which CacheGuard-OS is running. The apply report command allows you to get the state execution report of the latest **apply** operation. If after having made a new configuration, you decide to abandon it, you can use the cancel command. The cancel command can't be invoked when an **apply** operation is running. To cancel a running **apply** operation, you can use the apply cancel command.

The new configuration to apply is a set of commands that should form a consistent configuration. In other words, commands in a configuration should be compatible with each other. For instance you can’t activate (or apply) a configuration that specifies a static route via a gateway that is not in the broadcast domain of a connected network interface. The apply command is responsible of the integrity and consistency of configurations. If the new configuration to apply is inconsistent, the apply command reject that configuration and the apply operation would not start and instead, a list of integrity errors is displayed.

Load & Save a Configuration

The current or new configuration can be saved on a file server (FTP, TFTP...). Note that only trusted file servers are allowed to exchange files with a CacheGuard appliance. That's why it is necessary to trust a file server before being able to save a configuration on it. You must use the access command to add a file server to the list of trusted file servers. For instance, to trust the TFTP file server having the *172.18.2.1* IP address to exchange files via the **internal** network interface, use the following commands:

- *access file add internal 172.18.2.1*
- *apply*

Once the apply operation is finished, you can save the current configuration in a file named *cacheguard.conf* on that server by using the conf save tftp *172.18.2.1 cacheguard.conf* command. The saved file will contain a list of configuration commands. The saved configuration file can be loaded at any time into the system using the conf load tftp *172.18.2.1 cacheguard.conf* command. Please note that the apply command is not included in the saved file and should be manually invoked afterwards.

The configuration which is the object of this documentation section, is also called the logical configuration as the real operational configuration may contain additional data/files such as, but not limited to, SSL certificates, custom WAF rules and SSH public keys. To save all related data to a configuration in separated files on a file server, you must use the file command. For instance, to save all data related to a configuration in a folder named "*CGFiles*" on a TFTP file server having the *172.18.2.1* IP address, use the file save tftp*172.18.2.1 CGFiles* command. To reload those files back into the system, use the file load tftp *172.18.2.1 CGFiles* command.

The Network

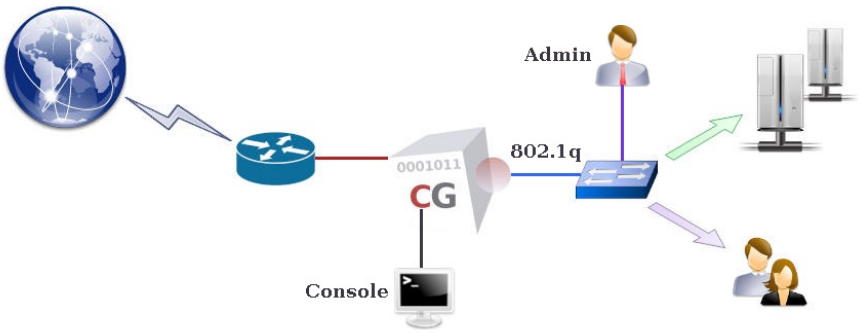
A freshly installed CacheGuard-OS has no IP configurations at all and before being able to connect to it as an administrator (**admin** user), you must set an IP address for at least one of its network interfaces. The only way to set an IP address for the first time on a CacheGuard appliance, is to use the CacheGuard appliance console port. At the first login (as the **admin** user) via the console port, a command named **setup** is automatically executed and allows you to set CacheGuard's **internal** and **external** IP addresses. As an alternative method, you can use the ip command.

Network Interfaces

With a CacheGuard appliance, the network is divided in at least 2 zones: the *internal zone* and the *external zone*. The *external zone* is considered as an untrusted zone (the internet) while protected users and servers should be placed in the *internal zone* (considered as trusted). A third optional zone called *auxiliary* can be created and used as per your convenience (for instance, as a DMZ or as a Back Office zone). The *internal zone* can be optionally divided into sub zones using tagged VLANs.

CacheGuard appliance connects each zone via a distinct logical network interface. Hence, a CacheGuard appliance can support up to 3 logical network interfaces: the **external**, the **internal** and the **auxiliary** logical network interfaces. In this network topology, internal users and servers are routed via the **internal** interface while CacheGuard appliance uses its **external** interface to connect to the internet.

A logical network interface should be associated to at least one physical network interface. The link command allows you to associate a logical network interface to a physical (*eth0*, (*eth1*...) network interface. A link configuration in which more than one physical network interface is associated to a logical network interface is called *link bonding*. The *link bonding* is an active/backup link configuration that allows service continuity in case of a failure on a link connectivity. You can refer to the Link Bonding section for further information on the *link bonding*.



Appliance IP addresses

To support the IP protocol, a logical network interface must be associated to a main IP address. The ip command allows you to set main IP addresses. Additional IP addresses can be implicitly associated to a logical network interface by other commands. For instance, the vrrp command allows you to create floating IP addresses in HA mode while the rweb command may create IP aliases associated to a main IP address. The example below set the **external** IP address to *192.168.1.1 255.255.255.0* and the **internal** IP address to *10.20.0.254 255.255.0.0*:

- *ip external 192.168.1.1 255.255.255.0*
- *ip internal 10.20.0.254 255.255.0.0*
- *apply*

Using 802.1q VLANs

CacheGuard appliance supports 802.1q VLAN (Virtual LAN) tagging on its internal network interface to secure and isolate predefined functional traffic (**admin**, **web**, **rweb**...). When using tagged VLANs, a pseudo network interface is implicitly created for each defined VLAN. To use VLANs, you have to activate the VLAN mode by using the mode vlan on command and then configure VLANs with the help of the vlan and ip commands. Note that in VLAN mode, the native IP address associated to the **internal** network interface is no longer active and you should configure a separated IP address for each pseudo network interface. For instance, the following commands define tagged VLANS 10, 20 and 30 respectively associated to the **web**, **rweb** and **admin** functional traffic and set a distinct IP address for each created VLAN (all other functional traffic will be let in the default VLAN 0).

- *vlan web 10*
- *vlan rweb 20*

- *vlan admin 30*
- *ip internal.0 10.0.0.254 255.255.255.0*
- *ip internal.10 10.0.10.254 255.255.255.0*
- *ip internal.20 10.0.20.254 255.255.255.0*
- *ip internal.30 10.0.30.254 255.255.255.0*
- *mode vlan on*
- *apply*

Network Routes

To route (or forward) IP traffic, you must create routing tables. CacheGuard-OS supports static routes only. However, you have the possibility to create multi gateways routes in order to balance the IP routing between multiple gateways. In a multi gateways configuration, gateway failures can be detected and the routing configuration is dynamically modified to no longer route the traffic via failed gateways. Please note that gateways in a route specification should be directly connected to a CacheGuard's network interface and have an IP address in the same network as the connected network interface IP address. As an example, the following commands allows you to create 2 default gateways via the *192.168.1.254* and *192.168.1.253* gateways and a static route to the *172.22.22.0 255.255.255.0* network via the *10.20.0.1* gateway.

- *ip route add default 192.168.1.254*
- *ip route add default 192.168.1.253*
- *ip route add 172.22.22.0 255.255.255.0 10.20.0.1*
- *apply*

Domain Name Servers

To connect to external name based services (for instance, websites), CacheGuard appliance needs a DNS (Domain Name Server) to translate domain names to IP addresses. CacheGuard appliance embeds a caching only DNS (Domain Name Server) that you can activate by adding the *localhost* (or the *127.0.0.1* loopback IP address) to the list of DNS servers. You have also the possibility to add external DNS to the system using the dns command. If you activate the internal DNS server, you will have the possibility to allow external clients to use it as a service. Please note that you have the possibility to restrict the DNS access to trusted networks only by using the access command. The example below, activate the internal DNS and allows IP clients to use it as a service.

- *dns add 127.0.0.1*
- *mode dns on*
- *apply*

DHCP Server

CacheGuard appliance integrates an easy to handle DHCP server that you can activate to deliver dynamic IP addresses to connected devices. The dhcp command allows you to define dynamic IP address ranges and/or fixed IP addresses for particular devices identified by their MAC addresses on an Ethernet network. Please note that dynamic IP addresses can only be delivered to devices that are connected to the **internal** network interface (or the **web** interface in VLAN mode). The example below, activate the DHCP server, configure it to deliver dynamic IP addresses between *10.20.0.11* and *10.20.0.15* and fixes the IP address *10.20.0.10* and the hostname *john* for a device having the 00:01:00:02:00:03 MAC address.

- *mode dhcp on*
- *dhcp range add 10.20.0.11 10.20.0.15*
- *dhcp fixed add john 00:01:00:02:00:03 10.20.0.10*
- *apply*

High Availability

CacheGuard appliance uses several technologies to assure the *High Availability* of services that it offers. The HA in a CacheGuard appliance is based on the redundancy and resiliency concepts. If you plan to implement CacheGuard solutions to secure and/or optimise critical services in your organisation, it is highly recommended to implement the HA offered in CacheGuard-OS.

The VRRP Protocol

By associating several CacheGuard appliances in HA mode, you can assure service continuity and HA (High Availability) in case of a (software or hardware) failure on one of them. To associate two (or more) CacheGuard appliances in HA mode, you must activate the HA mode on them by using the mode ha on command. In HA mode, up and running appliances automatically start to handle the network traffic that has been initially destined to a failed appliance. The HA mode is based on VRRP (Virtual Router Redundancy Protocol) and can be configured using the vrrp command.

When using the VRRP, two (or more) CacheGuard appliances share the same virtual IP (VRRP IP) address (in addition to their real IP addresses) on their same network interface. External services/clients should then address appliances configured in HA mode by using their VRRP IP addresses (and not their real IP addresses). A VRRP IP address can then be **master** (active) or **backup** on a network interface. The master VRRP IP is active on a network interface until a

failur on that network interface. Following that failure, the backup VRRP IP becomes active (on the backup appliance). Each CacheGuard appliance embeds a service called health checker that continuously verifies the health the services running on it. In case of a repetitive failure on a service, the health checker deactivates its network interfaces allowing other associated appliances in HA mode to fail over the failed appliance.

Link Bonding

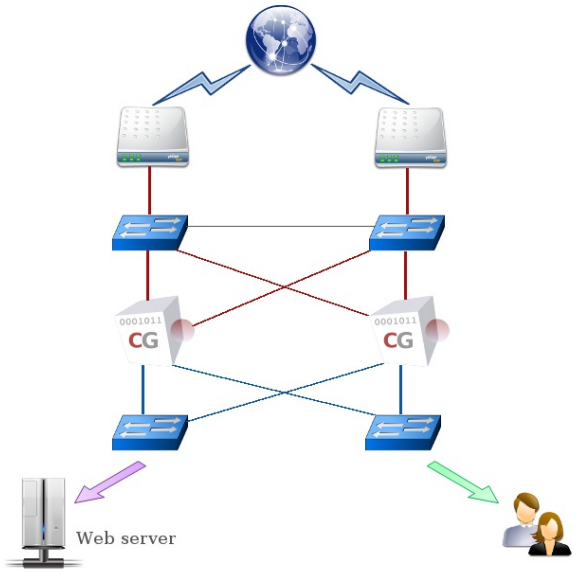
As seen before, logical network interfaces (**internal**, **external** and **auxiliary**) should be associated to at least one physical network interface. However, you have the possibility to a associate a logical network interface to more than one physical network interface. The association of a logical network interface to more than a physical network interface is called *link bonding*. The link bonding can be configured using the link command. In a link bonding configuration, there is always an active link while others are backup links. In this context, a link is composed of a NIC (Network Interface Card), a cable and a port on network switch. When a logical network interface is configured with link bonding, if the active link associated to that logical network interface fails, traffic are no longer exchanged via that failed link and a backup link is then activated to handle the network traffic for that logical network interface.

HA Network Example

The diagram below shows a highly available network architecture based on the redundancy and resiliency of all its components. In this network architecture, logical network interfaces of each CacheGuard appliance are connected to two distinct switches. To eliminate any SPoF (Single Point of Failure), the CacheGuard appliance as well as the internet router are doubled-up. The following commands configure the two CacheGuard appliances in HA mode to offer the best-ever level of availability.

First Appliance Configuration

- *hostname cacheguard1*
- *link bond external raz*
- *link bond external add eth0*
- *link bond external add eth2*
- *link bond internal raz*
- *link bond internal add eth1*
- *link bond internal add eth3*
- *ip internal 172.18.2.251 255.255.255.0*
- *vrrp internal raz*
- *vrrp internal add 172.18.2.254 master*
- *vrrp internal add 172.18.2.253 backup*
- *peer ha add 172.18.2.252*
- *ip external 192.168.2.1 255.255.255.0*
- *vrrp external raz*
- *vrrp external add 192.168.2.3 master*
- *vrrp external add 192.168.2.4 backup*
- ip route raz
- *ip route add default 192.168.2.254 50*
- *ip route add default 192.168.2.253 0*
- *mode web on*
- *mode cache on*
- *mode ha on*
- *apply*



Second Appliance Configuration

- *hostname cacheguard2*
- *link bond external raz*
- *link bond external add eth0*
- *link bond external add eth2*
- *link bond internal raz*
- *link bond internal add eth1*
- *link bond internal add eth3*
- *ip internal 172.18.2.252 255.255.255.0*
- *vrrp internal raz*
- *vrrp internal 172.18.2.253 master*
- *vrrp internal 172.18.2.254 backup*
- *peer ha add 172.18.2.251*
- *ip external 192.168.2.2 255.255.255.0*
- *vrrp external raz*
- *vrrp external add 192.168.2.4 master*
- *vrrp external add 192.168.2.3 backup*
- ip route raz
- *ip route add default 192.168.2.253 50*
- *ip route add default 192.168.2.254 0*
- *mode web on*
- *mode cache on*
- *mode ha on*

- *apply*

In this example, the first CacheGuard appliance (*cacheguard1*) has its active default gateway set to *192.168.2.254* (which is the LAN IP address of the internet router on the left). This CacheGuard appliance is then configured to use the *192.168.2.253* IP address (which is the LAN IP address of the internet router on the right) as its default gateway in case of a failure on the *192.168.2.254* gateway (internet router on the left). The same VRRP IP addresses are used on both appliances but with inverted states (the **master** and **backup** VRRP IP addresses are inverted). In this way, both CacheGuard appliances can be solicited by clients in an active/active mode.

In addition, each CacheGuard appliance operates in a link bonding configuration in which its **external** logical network interface is associated to its *eth0* and *eth2* Ethernet cards while its **internal** logical network interface is associated to its *eth1* and *eth3* Ethernet cards. Finally, the Web caching is activated on on both appliances and each is configured to request the other's HA Web cache using the peer ha... command for an even better bandwidth saving.

The two CacheGuard appliances configured in this way, can then be used in an active/active mode with the help of a WPAD (Web Proxy Auto Discovery) script set on Web browsers. Note that CacheGuard appliance in HA mode, provides a WPAD script via the *http://<cacheguard-internal-ip-address>/ha.pac* URL where *<cacheguard-internal-ip-address>* is an **internal** master VRRP IP address. The provided WPAD script supports sticky connectivity in order to reach a give target URL requested by a given Web client, always via the same Web proxy (in normal circumstances when both CacheGuard appliances are up and running).

You can also use your own WPAD script to share the total Web traffic on both CacheGuard appliances according to your needs. To use a WPAD script, save it in a file having the "*.pac*" extension and put it on Web server availabe from your Web browsers. Be sure that the "*application/x-ns-proxy-autoconfig dat*" mime-definition is set for WPAD script files on that Web server. A WPAD script can be as follows:

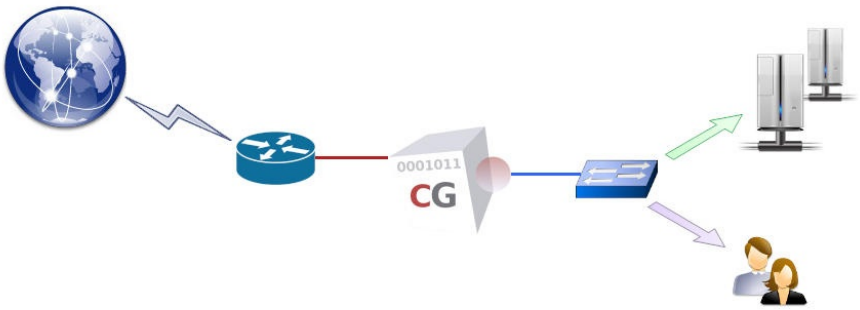
```
function FindProxyForURL( url, host )
{
  if (url.substring(0, 5) == "http:"   ||
  url.substring(0, 6) == "https:") {

  if ( (Math.floor( Math.random() * 2)) == 0 ) {
  return "PROXY 172.18.2.254:8080 ; DIRECT";
  }
  else {
  return "PROXY 172.18.2.253:8080 ; DIRECT";
  }
  }
  return DIRECT;
}
```

The network architecture above and its' associated CacheGuard appliance configurations allow you to support various failure sceneries such as, but not limited to, one or more physical network card failures, one or more cable failures, one or more switch failures, one CacheGuard appliance failure, one internet router failure.

Transparent Mode

CacheGuard appliance integrates a Web proxy that can be explicitly used by Web clients (humans or machines). In an explicit implementation, Web users must configure their Web browsers to use CacheGuard appliance as an HTTP/HTTPS proxy by using its **internal** IP address (**web** address in VLAN mode) and proxy port (8080 by default). If modifying Web browsers configurations would not be an option in your networks, you have the possibility to implement CacheGuard in a transparent mode. In transparent mode, HTTP traffic (and optionally HTTPS traffic) are transparently intercepted by the appliance and then can be handled by the many integrated services that a CacheGuard appliance offers (URL filtering, antivirus, Web caching...).

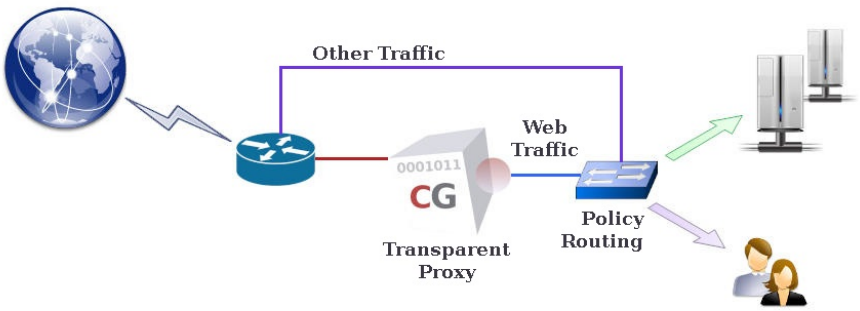
To be able to act as a transparent Web gateway (proxy), CacheGuard appliance must be placed on the Web traffic route (ie. Web traffic should traverse the CacheGuard appliance). The easiest way to achieve that, is to use CacheGuard appliance as the default gateway on your LAN. If using CacheGuard as the default gateway for all internet traffic is not wanted, you can use a switch L4 (Layer 4) and implement a policy-based routing that would route only Web traffic via the CacheGuard appliance. You must use the mode tweb on (or mode transparent on) command to activate the transparent mode.



Please note that the transparent interception of HTTPS traffic requires that you activate the SSL mediation on your CacheGuard appliance. Implementing the SSL mediation requires that you deploy the CacheGuard appliance CA certificate on all Web client devices. Please refer to the SSL Mediation section to get help on how to implement it.

Using a Switch L4

A switch L4 allows you to route the IP traffic according to the TCP/UDP headers in addition to and IP address. To route Web traffic only via the CacheGuard appliance and other traffic via another gateway, your policy-based routes on your switch L4 should route all traffic destined to the TCP port 80 (HTTP) and optionally the TCP port 443 (HTTPS) via the CacheGuard appliance and other traffic via your usual internet traffic.



If you are familiar with Linux, you can perfectly use a Linux box to implement this policy-based routing. There are plenty of examples on the Web to learn how to implement policy-based routing with a Linux box. As an introduction to such a configuration, you can use the following commands on a Linux box to implement this policy-based routing:

- iptables -t mangle -A PREROUTING -p tcp --dport 80 -j MARK --set-mark 5
- echo "100 transparent-proxy" >> /etc/iproute2/rt_tables
- ip route add default via <cacheguard-internal-ip> table transparent-proxy
- ip rule add fwmark 5 table transparent-proxy

where <cacheguard-internal-ip> would be your CacheGuard appliance internal IP address. Please refer to the ip and iptables man pages on a Linux machine to get further information Linux commands used in that configuration.

Selective Transparency

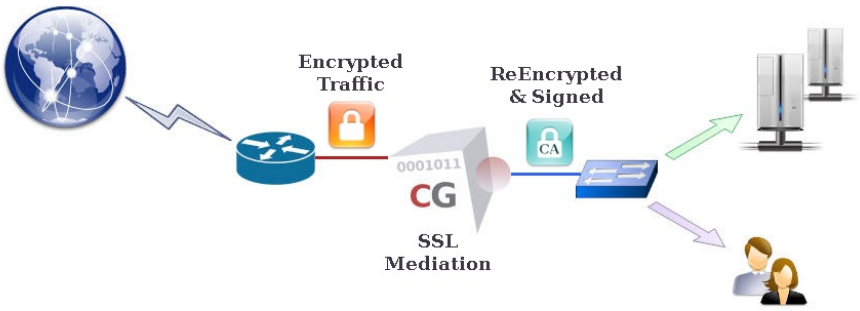
Once the transparent mode is activated on a CacheGuard appliance, all routed Web traffic via that appliance are intercepted by it regardless of the their IP addresses. This behaviour may have some limitations for users who want to have more control over their Web traffic (e.g. administrators). To remedy this behaviour, Web traffic interception may be limited to some networks only by using the transparent (or tweb) command. For instance, to limit the transparent mode to Web clients that belong to the *172.18.2.0 255.255.255.0* or *10.26.0.0 255.255.0.0* networks and routed via the **internal** network interface, you can use the following commands:

- *mode transparent on*
- *transparent raz*
- *transparent add internal 172.18.2.0 255.255.255.0*
- transparent add internal 10.26.0.0 255.255.0.0
- *apply*

SSL Mediation

CacheGuard appliance can decrypt HTTPS (encrypted) traffic in order to be able to inspect its content. After being inspected, the encrypted Web traffic can be cached or be blocked in case where a malware is detected in it. In this way, bandwidth consuming contents such as video chunks can be cached and malware blocked even in an encrypted format. Without the SSL mediation, such traffic handling would simply not be possible (as caching or inspecting encrypted traffic is simply not possible). The purified and/or cached traffic is then re-encrypted by CacheGuard-OS before being sent to Web clients. This feature is called SSL mediation on a CacheGuard appliance.

Please note that as decrypting an re-encrypting HTTPS traffic can be considered as a MITM (Man in the Middle) attack, you should ensure that activating the SSL mediation complies with laws in your country and/or organisation. Also be aware that activating the SSL mediation is fully under your responsibility. You are invited to read the CacheGuard-OS License Agreement for further information.



When the SSL mediation is activated, decrypted traffic is re-encrypted again before being sent to Web clients. To transmit re-encrypted traffic to Web clients, the Web proxy uses dynamically generated SSL certificates that are signed by a private CA (Certificate Authority) certificate. As Web clients would have to deal with HTTPS traffic that uses a private CA certificate (called system CA certificate), they must have confidence in that CA certificate. That's why prior to activating the SSL mediation, you must import CacheGuard CA certificate into your browsers. Otherwise the HTTPS communications will fail. You can decide to transparently intercept HTTPS traffic or not using the sslmediate command. To activate the SSL mediation and configure it to transparently intercept HTTPS traffic, use the following command:

- *mode transparent on*
- *mode sslmediate on*
- *sslmediate transparent on*
- *apply*

The System CA

The CacheGuard CA certificate is called the system CA certificate and it's available at *http://<cacheguard-internal-ip>/* where *<cacheguard-internal-ip>* is the internal IP address of your CacheGuard appliance. A default system CA certificate is generated the first time you turn on your CacheGuard appliance. It is recommended that you regenerate that CA certificate or import your own CA certificate into your CacheGuard appliance and set it as the system CA. You can use the following commands to generate the system CA certificate and its associated private RSA key:

- *tls ca system generate*
- *apply*

To import a CA certificate and its associated private RSA key into your CacheGuard appliance and set it as the system CA certificate, you must first put them on a trusted file server in a first step. A trusted file server is a file server allowed to exchange files with CacheGuard appliance (refer to the access command to get help on how to declare a file server as trusted). The next step will then be to load them into your CacheGuard appliance from that trusted file server. Assuming that your CA certificate and its associated private key are respectively named *cg-ca.certificate* and *cg-ca.key* and are placed on a trusted SFTP file server having the *172.18.2.1* IP address, you can use the following commands to import them into your CacheGuard appliance:

- *password file add sftp 172.18.2.1 john*
- *tls ca system load certificate sftp 172.18.2.1 cg-ca.certificate*
- *tls ca system load key sftp 172.18.2.1 cg-ca.key*
- *apply*

Exception Lists

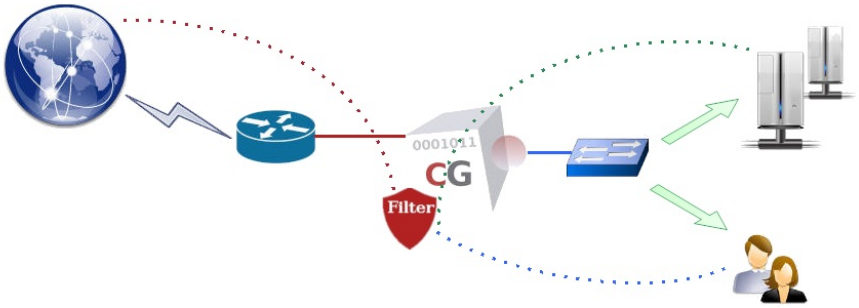
To remedy MITM attacks, some HTTPS websites use a technique called SSL pinning. The SSL pinning consists of hard coding the HTTPS certificate into the Web traffic content making any MITM attacks, and at the same time the SSL mediation, impossible.

Fortunately CacheGuard appliance can be configured to exceptionally bypass the SSL mediation for some predefined domain names (**deny** policy) or only operate on a predefined list of domain names (**allow** policy). You can create exceptions by directly specifying domain names (quick method) or by using URL lists. To manage URL lists, you can refer to the urllist command. As an example, to activate the SSL mediation for the *example.com* domain name only, you can use the following commands:

- *sslmediate policy allow*
- *sslmediate exception urllist raz*
- *sslmediate exception domainname raz*
- *sslmediate exception domainname add example.com*
- *apply*

URL Guarding

The URL guarding (or filtering) allows you to have control over the Web browsing in your organisation. You can activate the URL guarding by using the mode guard on command. This feature is based on blacklists (denied) or white lists (allowed) of domain names and URLs that you can manage using the urllist command. You have also the possibility to use regular expressions in addition to URL lists. In this way, you have the possibility to give access to only allowed websites in your white lists or block access attempts to URLs appearing in your blacklists. The guard command allows you to configure the URL guarding by creating filters, policies and rules.



A URL guard rule denies access to a set of blacklists or allows access to a set of white lists according to filters associated to a policy. Each rule is associated to one and one policy identified by a unique name. A policy can be associated to one or more filters. Finally a filter can specify a source IP address, an LDAP request or a time specification. A policy named **default** allows you to define a default rule to apply to all Web clients for which no other policies are matched. In the example below, a default rule is created to block access to Advertising and Malware websites for all Web clients:

- *mode guard on*
- *urllist add Advertising*
- *urllist add Malware*
- *urllist load create Advertising tftp 172.18.2.1 Advertising domains urls*
- *urllist load create Malware tftp 172.18.2.1 Malware domains urls*
- *guard rule add default deny Advertising Malware*
- *apply*

In the example above, two URL list categories named *Advertising* and *Malware* are created first and then populated with list of domain names and URLs in files located on a remote TFTP file server having the 172.18.2.1 IP address. Please note that prior to be able to exchange files with a (TFTP, FTP or SFTP) file server, the file server should be declared as trusted. You can refer to the access file command to learn how to add a file server to the list of trusted file servers. The sixth argument in the *urllist load...* command usage form specify the base name (*Advertising* or *Malware*) of files that should be located on the specified file server and the urllist command expects to find files with the *.domains.gz* and *.urls.gz* extensions. As you can guess, URL list files should be in gzip compressed format (loading uncompressed URL list files is not supported).

Domain name files (*.domains.gz*) should contain a list of domain base names (one per line). A domain base name is a domain name without any prefix. For instance *example.com* is considered as domain base name while *www.example.com* is not. To specify a domain name with a prefix, you should put in a URL file (*.urls.gz*). URL files (*.urls.gz*) should contain a list of content specification (one per line) similar to a URL without the protocol part in the form <domain-name>/<path> where the <domain-name> is a fully qualified domain name and the <path> is a path specification. For instance, *www.example.com/foo/bar/zoo.html* is a valid URL in this context while *http://www.example.com:81/foo/bar/zoo.html?id=1* is not.

URL Lists

The URL guarding is mainly based on URL lists that you should keep updated (as every day, thousands of new websites are published on the Web). Daily updated URL lists are offered as an optional service by CacheGuard Technologies Ltd that you can easily subscribe to. However, you have the possibility to use your own URL lists and keep them automatically updated on your CacheGuard appliance. To update a URL list, you have the possibility to create it from scratch by loading its full content from URL list file or just load a difference file (preferred method). For instance, to automatically update the URL list named *WebMail* from *ftp://172.18.2.1/DF/WebMail* on a daily basis, you can use the following command:

- *password file add ftp 172.18.2.1 john*
- *urllist auto WebMail on load update daily ftp 172.18.2.1 DF/WebMail*
- *apply*

Difference URL list files should respect a syntax explained in the urllist command manual. Please refer that manual for further information.

Policies & Filters

Guard policies allow you to apply the URL guarding to a specific group of Web clients matching certain criteria. For instance, you may want to block Advertising websites for users in the *10.0.10.0 255.255.255.0* network that belong to the *cn=support,ou=groups,dc=example,dc=com*LDAP group between 12:30 and 13:30 (1:30 PM) hours. To that end, you should first create 3 guard filters and then associate them to a policy and finally create a guard rule based on that guard policy. The following commands allow you to define such a guarding policy:

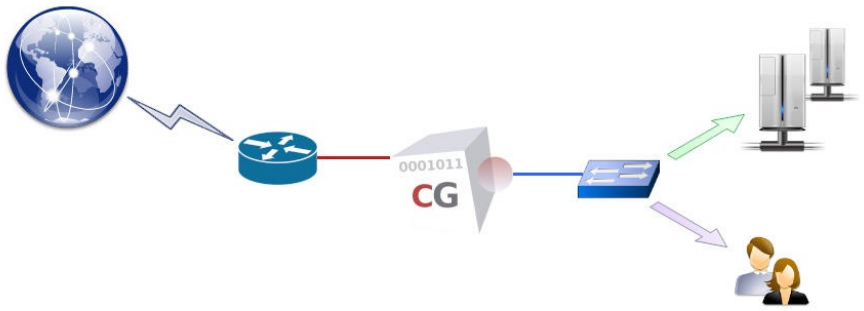
- *guard filter ip add london network 10.0.10.0 255.255.255.0*
- *guard filter time add lunchHours slot 12:30-13:30*
- *guard filter ldap add supportTeam 'cn=support,ou=groups,dc=example,dc=com' memberUid 'objectclass=posixGroup'*
- *guard policy add londonSupport ip london time lunchHours ldap supportTeam*
- *guard rule add londonSupport deny Advertising*
- *apply*

Please note that LDAP filters can only be used when the Web authentication mode is activated. Please refer to the Web Authentication section and the authenticate command manual for further information on LDAP authentication. **LDAP filter Note**: in the example above, the *memberUid* specifies the LDAP attribute used to store the login name provided by users during the authentication. The *objectclass=posixGroup* is the request to retrieve the user on the LDAP server.

Web Server Cloaking

CacheGuard appliance can be implemented as a reverse Web proxy in front of a group of Web servers to protect them against (unwanted) direct accesses on the one hand, and to optimise the Web traffic exchanged with them on the other. This implementation is called the *reverse mode* (or **rweb** mode) and protected Web application *reverse websites*. All security and optimisation features available in CacheGuard-OS can join together to offer the best-ever security and network optimisation solution to protect Web application. You can find below all the advantages of this mode combined with others:

- **Firewall**: blocks unwanted network accesses to Web servers.
- **Reverse Proxy**: allows to do note expose Web servers directly to the internet.
- **SSL Offloading**: terminates SSL connections on the CacheGuard appliance in order to offload Web servers.
- **WAF**: the Web Application Firewall (WAF) blocks content attacks such as SQL injections.
- **Load Balancing**: allows to balance a website load on a group of Web servers.
- **High Availability**: allows service continuity in case of a failure on a CacheGuard appliance or a Web server.
- **Caching**: caches satic Web objects such as images to offload Web servers.
- **HTTP Compression**: saves the WAN bandwidth.
- **Antivirus**: blocks malware injections on Web pages.
- **QoS**: allows to shape the Web traffic and offer QoS to critical applications.



To activate the reverse mode, you can use the mode rweb on command. Then you must use the rweb command to configure this mode. For instance, the following commands allow you to activate the reverse mode and protect the Web server having the *10.0.10.11* IP address and hosting the *www.example.com* website name:

- *mode rweb on*
- *ip external 192.168.1.1 255.255.255.0*
- *rweb site add www.example.com http*
- *rweb host www.example.com add rweb http 10.0.10.11*
- *apply*

Anti Spoofing Note: a host is always specified alongside a network interface via which it is allowed to communicate in order to block any IP address spoofing. The **rweb** keyword in the "*rweb host www.example.com add **rweb** http 10.0.10.11*" command above, specifies that network interface. It represents the pseudo network interface named **rweb** in VLAN mode or the native **internal** network interface (in case where the VLAN mode is deactivated). Please refer to the rweb command manual for detailed information on this topic.

In reverse mode, CacheGuard appliance acts as a virtual Web server cloaking real Web servers (called hosts). Cloaked Web servers should then be publicly exposed with the CacheGuard appliance external IP address. For instance, in the example above, the *www.example.com* name should be publicly resolved to 192.168.1.1.

Load Balancing

If more than one host is associated to a website, the total load on that website is balanced over all its associated hosts. In addition, CacheGuard appliance continuously checks the availability of hosts and in case of a failure (unavailability) on a host, it no longer sends to it Web requests (ie. it removes it from the pool of load balanced hosts), hence providing websites high availability.

The default load balancing method consists of sending the same number of requests to each host. This method is called robin (for round-robin). When adding (associating) a host to a website name, an optional weight can be specified to configure the load balancing in order to solicit more or less that host. In addition, if the underlying Web application (running on hosts) of a website requires that a given Web client be always managed by the same host (to preserve any application context), you must activate the sticky load balancing for that website. Sticky connections are based on an inserted (by CacheGuard appliance) or on existing HTTP cookie that you must configure using the rweb command.

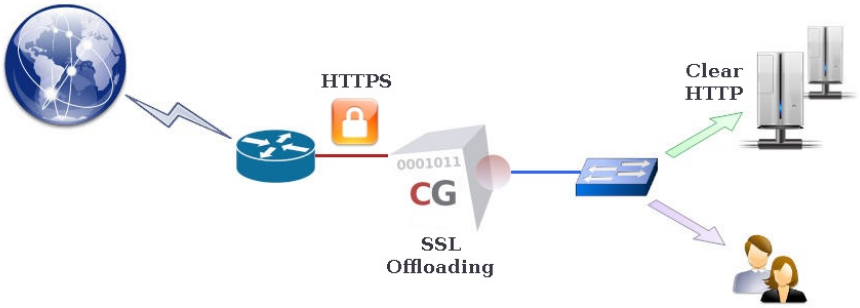
For instance, to complete the previous example, we can add the host having the *10.0.10.12* IP address to the pool of load balanced hosts and configure a round-robin sticky load balancing for the *www.example.com* website. The following command allows you to have such a configuration:

- *rweb host www.example.com add rweb http 10.0.10.12*
- *rweb balancer www.example.com robin sticky*
- *apply*

SSL Offloading

In order to allow a CacheGuard appliance to handle (inspect, cache...) Web contents in HTTPS (encrypted) traffic, it should be capable to decrypt it first to have an unencrypted access to its content. To this end, CacheGuard appliance acts as an SSL terminator for HTTPS websites that it manages. While communications between Web clients and HTTPS websites that are managed by a CacheGuard appliance are always encrypted, communications between the appliance and hosts can be encrypted (using HTTPS) as well as unencrypted (using HTTP).

When the HTTP protocol is used to communicate with hosts, CacheGuard appliance acts as an SSL off-loader for those hosts. It is important to note that in an SSL offloading configuration, every care should be taken to isolate unencrypted Web traffic between CacheGuard appliance and hosts in order to do not allow unauthorised access to that unencrypted traffic. The **http** keyword in the "*rweb host www.example.com add rweb* ***http*** *10.0.10.12*" command above, specifies to use the SSL offloading for that host. To do not perform an SSL offloading for a host, you can use the **https** keyword instead of **http**. Refer to the rweb command manual for further information on this topic.



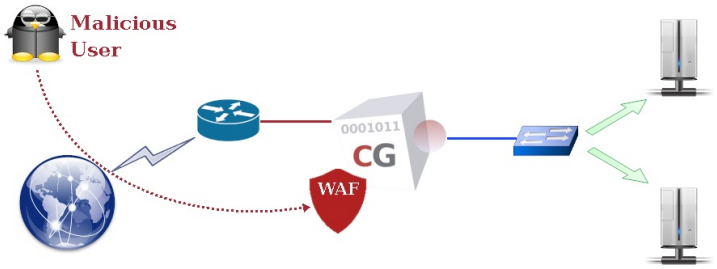
As an SSL off-loader, CacheGuard appliance must naturally have access to public SSL certificates and private keys associated to HTTPS websites that it manages. You can use the tls command to manage SSL certificates and private keys used by the appliance. The same website name can exist in HTTP and HTTPS versions. In this case, all requests on the HTTP version are forwarded to the HTTPS version by default (you can modify this behaviour if needed). In the previous example, to add the SSL encryption capability to the *www.example.com* website (publicly reachable at *https://www.example.com/*), you can use the following commands:

- *tls server add myTLSObject*
- *tls server generate myTLSObject*
- *rweb site add www.example.com https myTLSObject*
- *apply*

TLS Note: once the apply operation is completed, an RSA private key, a self signed X.509 SSL certificate and a CSR (Certificate Signed Request) are generated. You can save the CSR on a trusted file server and then submit it to your CA authority to be signed. The new official signed certificate can then be loaded into the CacheGuard appliance. You can refer to the access file and tls server command manuals to get help on how to load and save SSL certificates.

The WAF

WAF stands for Web Application Firewall and allows you to protect Web applications against malicious Web requests destined to violate or damage Web applications and/or servers. CacheGuard appliance integrates a WAF that works jointly with the Web Server Cloaking to provide an even higher level of security for Web servers. The WAF can protect against content attacks such as, but not limited to, XSS (Cross Site Scripting), SQL injection and command injection. Malicious requests are then blocked even before reaching real Web servers (hosts).



To enable the WAF, both **rweb** and **waf** modes must be activated using the mode rweb on and mode waf on commands. You can refer to the Web Server Cloaking section to learn how to configure the **rweb** mode. Then you can use the waf command to configure the content filtering for protected Web applications. The CacheGuard WAF provides two types of content filtering that can be activated on the same appliance at the same time. The two content filtering types are as follows:

- **Generic Filtering**: rejects all known content attacks and can be globally activated (for all websites) or be activated per protected website.
- **Customised Filtering**: allows or denies Web requests that you can design by yourself per website.

Generic Filters

Generic WAF rules are classified by groups called filters (a filter is composed of WAF rules). Each blocking rule in a generic filter has a score point (an integer) and whenever a rule is matched in a Web traffic, its score point is added to a global score. Once a threshold score is reached for a given Web traffic, the Web traffic is blocked by the WAF. Generic filters are provided by OWASP and are classified as follows:

- **dliis**: rules to prevent from IIS applications Data Leakage.
- **dljava**: rules to prevent from Java applications Data Leakage
- **dlphp**: rules to prevent from PHP applications Data Leakage.
- **dlsql**: rules to prevent from SQL requests Data Leakage.
- **java**: rules to protect Java Applications.
- **lfi**: rules to protect against Local File Inclusion attacks.
- **nodejs**: rules to protect Node.js Applications.
- **php**: rules to protect PHP Applications.
- **rce**: rules to protect against Remote Code Execution attacks.
- **rfi**: rules to protect against Remote File Inclusion attacks.
- **sf**: rules to protect against Session Fixation attacks.
- **sqli**: rules to protect against SQL Injection attacks.
- **xss**: rules to protect against Cross-site Scripting attacks.

Generic filters can be globally activated or deactivated. For instance, to activate the WAF and protect all websites (cloacked by the reverse Web proxy in **rweb** mode) against SQL injection attacks, you can use the following commands:

- *mode rweb on*
- *mode waf on*
- *waf generic sqli on*
- *apply*

In absence of any generic WAF filter specifications for a website, that website would be protected by globally activated generic WAF filters. If a particular website needs specific protections, you have the possibility to activate or deactivate generic WAF filters for that website. For instance, to deactivate the **sqli** generic filter for the *www.example.com* website, you can use the following commands:

- *waf rweb generic www.example.com sqli off*
- *apply*

Custom Filters

Custom WAF filters allow you to have accurate control over Web requests on a website in particular. A custom WAF filter is composed of custom WAF rules defined in a textual file that you can load into a CacheGuard appliance. A custom WAF rule allows you to allow or deny a Web request according to its HTTP method and content. A rule is defined in 1, 2 or 3 lines according to the specified HTTP method.

The definition of a custom WAF rule should always begin with the **rule** keyword and be followed by an identifier, an action (**allow** or **deny**) and an HTTP method (in lowercase). Supported HTTP methods are *GET*, *HEAD* and *POST*. For the *GET* and *POST* methods, a second optional line can specify allowed contents (the path and arguments part) in the Web request. The second line should always begin with the **uri** keyword and be followed by a (PCRE: Perl Compatible Regular Expression) regular expression specifying allowed contents. For the *POST* method, a third optional line can specify allowed contents in the *POST* request. The third line should always begin with the **body** keyword and be followed by a regular expression specifying allowed data in the body part of the *POST* request.

As an example, the following custom WAF filter includes 6 rules: the first and second rules allow *GET* requests on respectively "/" and "*index.html*" locations. The third rule, allows *POST* requests on "*/cgi-bin/set-phone.cgi*" with a body in the form of "*name=<string>&phone=<numbers>*". The last 3 rules block (deny) any other Web requests.

```
rule r1 allow get
uri "^/$"

rule r2 allow get
uri "^/index\.html$"

rule r3 allow post
uri "^/cgi-bin/set-phone.cgi$"
body "^name=[[:print:]]*\&phone=[[:digit:]]*$"
```

```
rule r4 deny get
rule r5 deny head
rule r6 deny post
```

To apply this custom WAF filter to the *www.example.com* website, save it first in a file located on a trusted file server. Then you will be able to load it into your CacheGuard appliance and associate it to the *www.example.com* website. Please refer to access file command manual to learn how to declare a trusted file server. The following commands load a custom WAF filter described in a file named *www.example.com.rules* from a TFTP file server having the *172.18.2.1* IP address and apply it to the *www.example.com* website:

- *waf rweb custom www.example.com load tftp 172.18.2.1 www.example.com.rules*
- *apply*

When a custom WAF filter is loaded into the appliance, the custom WAF rule compiler examines its content and in case where an error is detected, the loading is rejected. Note that when generic WAF filters are combined with a custom WAF filter, generic WAF filters are applied first. In this way, malicious Web requests are rejected by generic WAF filters before reaching the custom WAF filter.

Reputation Filters

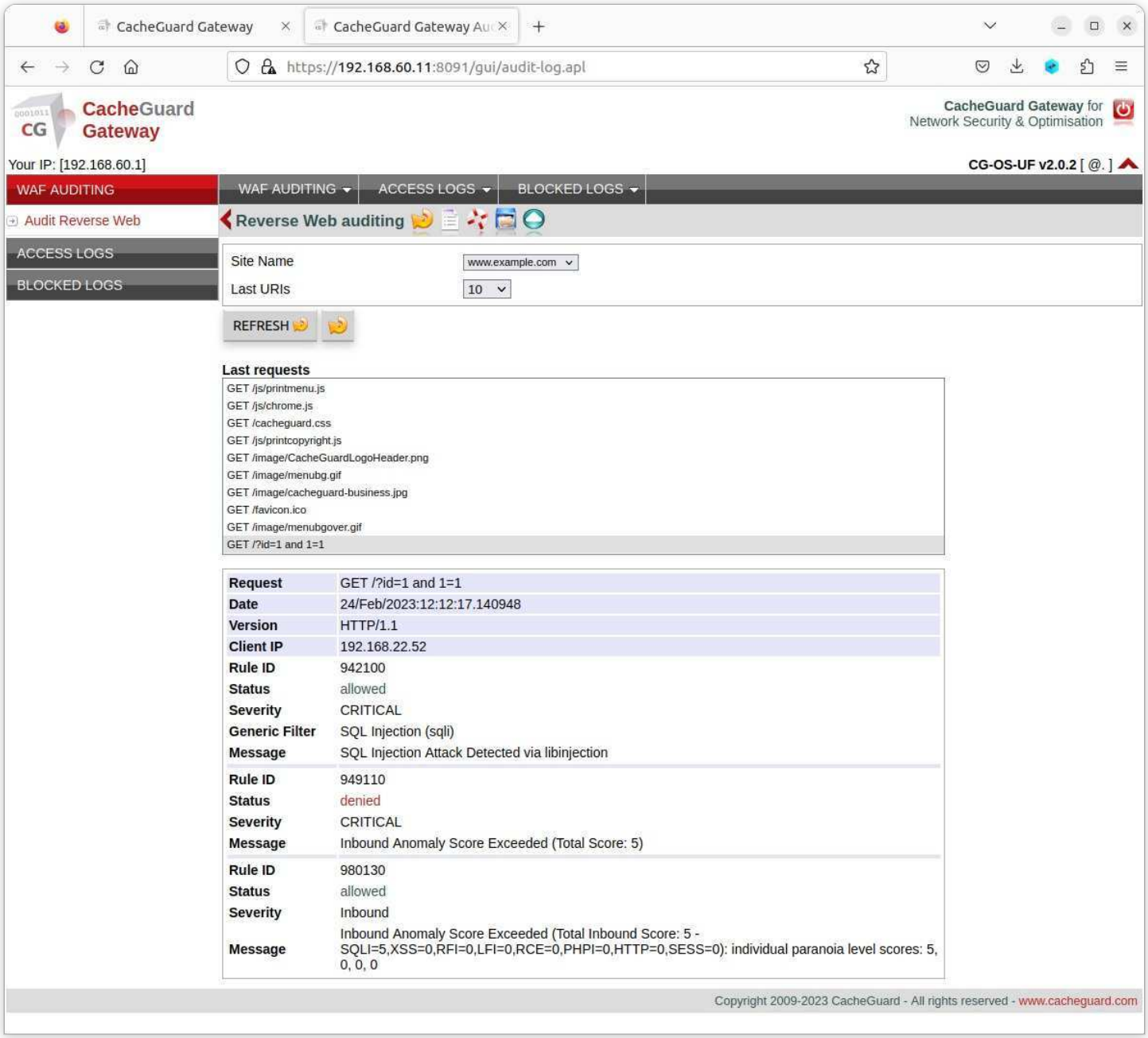
CacheGuard appliance can block Web requests incoming from IP addresses that have a bad reputation. This is called reputation based filtering. The reputation based filtering in CacheGuard appliance, can be configured to block all Web requests sent from IP addresses belonging to a country in particular or to an RBL (Real Time Blacklist). You can find more information on the reputation based filtering in the waf command manual.

Website Auditing

A Web request auditing Web GUI is integrated into the CacheGuard appliance and allows you to inspect all HTTP requests on a given website. With the help of the Web auditing, you can know why a Web request is blocked and what is the WAF rule (generic or custom) that blocks it. To activate the Web auditing for the *www.example.com* website, use the following commands:

- *admin waudit on*
- *waf rweb audit www.example.com on*
- *apply*

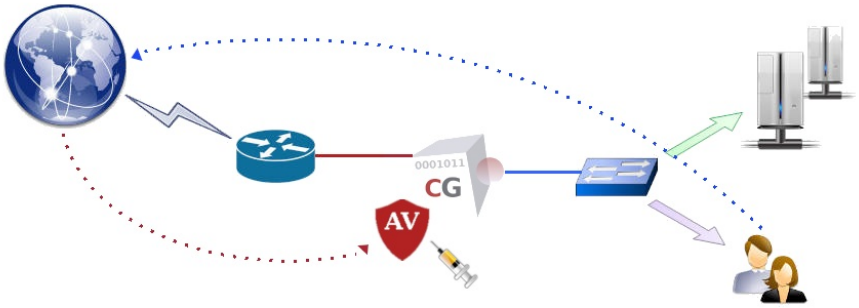
The Web auditing Web GUI is accessible via the *https://<cacheguard-ip-address>:8091* URL where *<cacheguard-ip-address>* is the CacheGuard appliance IP address. The IP address to use depends on the administration access policy and administration topology configured on the appliance. Please refer to the access admin and admin topology command manuals for further information. The screenshot below shows the Web auditing GUI.



Sometime a WAF rule is matched by mistake for a regular Web request. We call that a false positive match. The Web request auditing can help to detect false positive matches in order to remedy by modifying the Web application (when it's possible) or by bypassing rules that cause false positive matches. You can refer to the waf command manual to learn more about WAF rule bypassing.

The Antivirus

The antivirus detects malware (virus, trojans, worms) in Web traffic incoming from the **external** zone and blocks them at the gateway even before they can enter into your networks. The antivirus can operate in forwarding/browsing (**web**) mode as well as in reverse (**rweb**) mode. In forwarding mode, it rejects all attempts to access malware in Web traffic while in reverse mode, all attempts to upload a malware on protected Web servers are blocked (in **rweb** mode, CacheGuard appliance is implemented in front of Web servers). To activate the antivirus, you can use the mode antivirus on command followed by the apply command.



The antivirus detects MS Office macro viruses, mobile malware, and other threats. It supports 32/64-bit Portable Executable files and 32-bit ELF files. It scans not only simple files but also inspects inside archive and compression files such as, but not limited to, zip (+ sfx), rar (+ sfx), tar, gzip, bzip2, MS OLE2, MS cabinet files (+ sfx), MS CHM (Compiled HTML), MS szdd compression format, BinHex, SIS (SymbianOS packages), AutoIt, NSIS. In addition, the following file types are inspected:

- PE files compressed or obfuscated with the following tools: Aspack (2.12), UPX (all versions), FSG (1.3, 1.31, 1.33, 2.0), Petite (2.x), PeSpin (1.1), NsPack, wwpack32 (1.20), MEW, Upack, Y0da Cryptor (1.3).
- Almost every mail file format including TNEF (winmail.dat) attachments.
- The most popular file formats like: MS Office and MacOffice files, RTF, PDF, HTML.
- Various obfuscators, encoders, files vulnerable to security risks such as: JPEG (exploit detection), RIFF (exploit detection), uuencode, ScrEnc obfuscation.

Automatic Updating

CacheGuard appliance periodically checks the malware signature database and if necessary, downloads updates. Updates are downloaded from a public service named *database.clamav.net* on the internet. It is important to note that any download abuse can be blocked by that service for a given period of time which is not on the CacheGuard appliance control. In order to not be banned by that service, it is recommended to let CacheGuard appliance to automatically update the signature database and avoid any explicit updates (unless it is absolutely necessary).

To complete the standard malware signature database offered by *database.clamav.net*, additional malware signatures are proposed as an optional service by CacheGuard Technologies Ltd that you can easily subscribe to. After having subscribed to that optional service, you can simply activate it on your CacheGuard appliance by setting the provided password and file server name on your CacheGuard appliance (commands to use would be access file and password file).

Antivirus & WAF

When CacheGuard appliance is implemented as a WAF in front of your Web servers (the **rweb** and **waf** modes are both activated) the antivirus scans all attempts to upload files onto your protected/cloaked real Web servers. In case where a malware is detected in an uploaded file, CacheGuard appliance instantly blocks that upload even before the uploaded file can reach Web servers. Note that the only supported method to upload a file by the antivirus is the *POST* method with an encryption type of *multipart/form-data*. The following commands activate and configure the antivirus to scan any attempt to upload a file on the Web server having the IP address 10.20.0.100 and protected/cloaked by CacheGuard appliance:

- *rweb site add www.example.com http*
- *rweb host www.example.com add rweb http 10.20.0.100*
- *mode rweb on*
- *mode waf on*
- *mode antivirus on*
- *apply*

Antivirus & MTA

The antivirus is natively used by the integrated Web proxy to block malware in Web traffic. However, it can also be used as a service offered to external clients/services such an MTA (Mail Transfer Agent). For instance, to give access to a a remote exim4 MTA having the *10.20.0.200* IP address and communicating with CacheGuard appliance via its internal network interface, you can use the following commands:

- *ip internal 10.20.0.254 255.255.0.0*
- *port antivirus 8083*
- *access antivirus add internal 10.0.20.200 255.255.255.255*
- *apply*

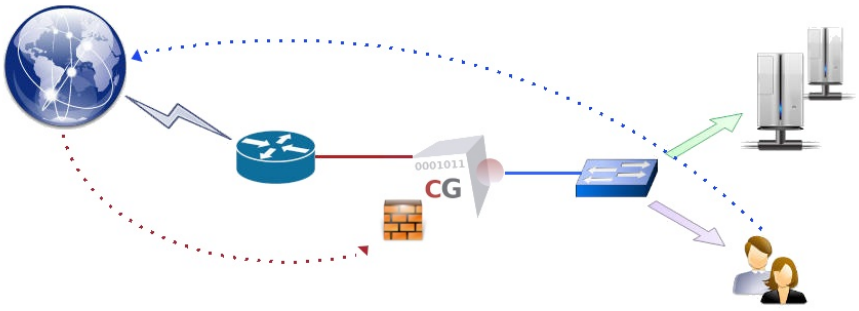
In this example, the exim4 MTA should then be configured to use CacheGuard appliance as an antivirus service by adding the *av_scanner = clamd: 10.20.0.254 8083* line to its configuration file.

Testing the Antivirus

The European Expert Group for IT Security provides some virus file for testing purpose. You can find those files on the https://www.eicar.org/ website. To test the antivirus with the help of those testing virus files, you must download and put them on a an HTTP (not HTTPS) Web server and then try to download them via your CacheGuard appliance Web proxy. If your CacheGuard antivirus is properly configured, the download attempt should be blocked by your CacheGuard appliance. To directly test from the https://www.eicar.org/ website which use HTTP**S** (and not HTTP), you must activate the SSL mediation on your CacheGuard appliance. Please refer to the SSL Mediation section to learn how to activate the SSL mediation.

Network Security

CacheGuard appliance distinguishes between two types of network traffic: traffic exchanged with the appliance itself and traffic that are only routed via the appliance (for which the source or destination are not the appliance itself). To control the traffic exchanged with the appliance itself, you can use the access command while the firewall command can be used to control routed traffic. Both types of traffic are managed by a stateful firewall integrated into the appliance.



Administration Access

For security reasons, the administration access (via SSH or the Web GUI) to a CacheGuard appliance is only granted to users (or machines) being in trusted networks. The same rule is applied to file servers and monitoring systems that need to access the appliance. File servers are used to exchange files (via TFTP, FTP or SSH) with the appliance for configuration or administration purposes (for instance, to load/save SSL certificates or make a system backup). Monitoring managers can be used to monitor the appliance using SNMP.

In the example below, the appliance is configured to give SSH and Web administration GUI accesses via its **internal** network interface to remote users (or machines) in the *172.18.2.0 255.255.255.0* network. In addition, the SNMP manager having the *172.18.2.202* IP address is allowed to send SNMP requests to the appliance via its **internal** network interface and the file server *ftp.cacheguard.net* is allowed to exchange files with the appliance via its **external** network interface.

- *access admin add internal 172.18.2.0 255.255.255.0*
- *access file add external ftp.cacheguard.net*
- *access mon add internal 172.18.2.202*
- *apply*

Note that to exchange files, CacheGuard appliance can use TFTP, FTP or STFP. As FTP and SFTP servers often require authentication (with login/password), you have the possibility to store authentication credentials (login/password) to access those file servers in CacheGuard appliance in order to do not have to interactively provide them whenever your appliance needs to exchange files with them. To set and store credentials to access a file server, you have the possibility to specify them with the access command or use the password command. The following commands set credentials to have an FTP access to the *ftp.cacheguard.net* file server and an SFTP access to the file server having the *172.18.2.203* IP address.

- *password file add ftp ftp.cacheguard.net john*
- *access file add internal 172.18.2.203 sftp john*
- *apply*

Web Browsing Access

By default, the Web proxy is accessible to all devices except those located in the external zone (routed via the **external** network interface). This default access policy can be modified by using the access web command usage form in order to limit the Web proxy access to a list of predefined networks only. To activate the Web proxy access limitation, you must define at least one Web access. Note that when at least one previous peer or one transparent network is defiend, the Web proxy access limitation is implicitly activated and you must explicitly define allowed networks to access the Web proxy. Please refer to the peer and transparent commands manual for more information about peers and transparent networks.

To restrict the Web proxy access to devices located on the *172.18.2.0 255.255.255.0* or *10.26.0.0 255.255.0.0* networks via CacheGuard's **internal** network interface, you can use the following commands:

- *access web raz*
- *access web add internal 172.18.2.0 255.255.255.0*

- *access web add internal 10.26.0.0 255.255.0.0*
- *apply*

The Firewall

CacheGuard appliance can act as a stateful firewall with NAT capabilities to filter routed network traffic according to the source and destination IP addresses and used protocols. To filter the network traffic, you must define firewall rules. A firewall rule is attached to a network interface and controls incoming traffic via that interface. Rules attached to a network interface form a rule set and you have as many rule set as network interfaces. To use the firewall, you must activate it first by using the mode firewall on command and then you can define rules by using the firewall command. In absence of any rules, the following default rules are applied:

- New connections incoming from the **external** zone and destined to the **internal**, **auxiliary** and **vpnipsec** zones are denied.
- New connections incoming from the **internal** zone (the **web** zone only in VLAN mode) and destined to other zones are allowed.
- New connections incoming from the auxiliary zone are denied by default (to allow traffic you should explicitly specify rules).
- In VLAN mode (mode vlan on), new connections incoming from the **rweb**, **antivirus**, **admin**, **mon**, **file** and **peer** zones are denied by default. In non VLAN mode (mode vlan off), they are all considered as being the **internal** zone and therefore follow the principals applied to the **internal** zone.
- New connections incoming from the **vpnipsec** zone and destined to the **internal** zone (the **web** zone only in VLAN mode) are allowed. Incoming connections from the **vpnipsec** zone and destined to other zones are denied by default.

If at least one firewall rule is present in a rule set, default rules are no longer applied and only network traffic that are explicitly defined by firewall rules would be allowed (or denied). Each firewall rule set, implicitly includes a **deny any** rule at its end (and you do not need to add it yourself). As an example, the following commands allow all TCP traffic incoming form the **web** interface that have a source IP address in the 172.18.2.0/24 network and outgo to the **external** zone (via the **external** network interface).

- *mode firewall on*
- *mode router on*
- *firewall web add allTCPToInternet allow tcp 172.18.2.0/24 external*
- *apply*

In the example above, if the VLAN mode is activated, the defined rule is exclusively applied to the **web** pseudo network interface (tagged VLAN). Otherwise, it would be applied to the **internal** native network interface.

When defining a firewall rule, you have the possibility to apply a NAT (Network Address Translation) to the source and/or destination IP address of the traffic. As an example, the following commands allow the *192.168.44.55* IP address to establish TCP connections via the **external** network interface to the *192.168.22.11:80* destination and NAT that destination to *10.0.10.11:81*:

- *mode firewall on*
- *mode router on*
- *firewall external add allWeb allow tcp 192.168.44.55 admin 192.168.22.11 80 nil 10.0.10.11 81*
- *apply*

It is **IMPORTANT** to note that in firewall rules, destination and source **NAT** are always applied **AFTER** the filtering.

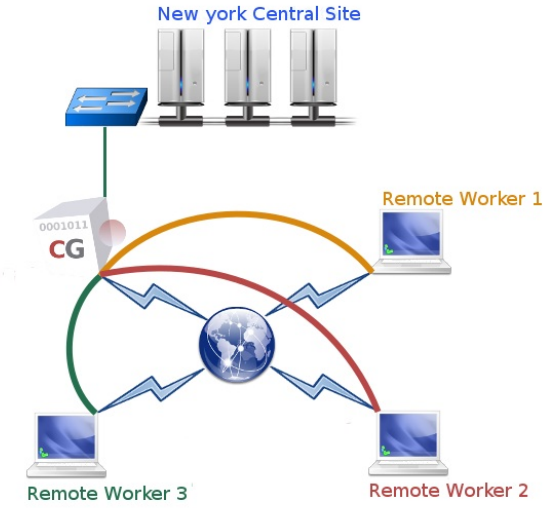
IPsec VPN

VPN stands for Virtual Private Network and IPsec for Internet Protocol Security. An IPsec VPN allows you to authenticate and encrypt data packets between private networks over a public IP network (ie internet) to provide secure encrypted communications. You can build persistent IPsec VPNs between sites or allow remote workers to access your internal infrastructures via an IPsec VPN. CacheGuard appliance integrates an IPsec VPN server that you can activate by using the mode vpnipsec on command. Then the vpnipsec command can be used to configure the IPsec VPN server.

We distinguish two types of IPsec VPNs: site to site VPNs and remote access VPNs. A site to site (or inter site) VPN allows you to build a permanent secure tunnel between two sites. With such a tunnel, computers in both sites can communicate with each other in a secure way as they were on the same location whereas in reality they can be separated by several thousands of kilo meters. To build a site to site IPsec VPN tunnel, you need two VPN servers: a local VPN server and the remote (or peer) VPN server.

A remote access VPN is a central VPN server to which remote workers can connect via secure tunnels built on top of the internet. With such tunnels remote workers can access computers protected by the VPN server in a secure way as they were on the same location.

Please note that on a CacheGuard appliance, you have to choose between the site to site mode or the remote access mode (both modes can't be activated at the same time). The vpnipsec access on and vpnipsec access off commands allow you to switch between the two modes.



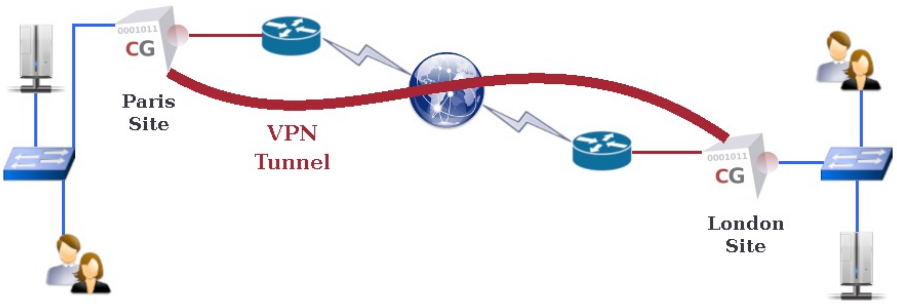
Remote Access VPN

To build a remote access IPsec VPN, you need a central IPsec VPN server while each remote worker connect the central VPN server using an IPsec VPN client. CacheGuard appliance supports almost all native IPsec VPN clients provided by devices and OS in the market (such as MS Windows™ 11, Apple™ Mac & iPhone...). In case where native VPN clients would not work, alternative third party IPsec VPN clients such as strongSwan can be used. The following commands allow you to activate the IPsec VPN in remote access mode and let CacheGuard appliance to be used as the default gateway for remote users:

- *mode vpnipsec on*
- *vpnipsec access on*
- *vpnipsec network access add local default*
- *apply*

Site to Site VPN

This section allows you to learn how to build an IPsec VPN tunnel between 2 sites through a simple example. In our example we consider that we want to establish a IPsec VPN tunnel between a site called London (*172.22.11.254 255.255.255.0* **internal** netwrok) and a site called Paris (*172.22.10.0 255.255.255.0* **internal** netwrok).



To implement that VPN, the configuration on the Paris site would be:

- *ip external 192.168.155.1 255.255.255.0*
- *ip internal 172.22.10.254 255.255.255.0*
- *mode vpnipsec on*
- *vpnipsec access off*
- *vpnipsec authenticate psk very-strong-and-long-psk-2connect-2paris*

- *vpnipsec site add London 192.168.155.2 psk very-strong-and-long-psk-2connect-2london*
- *vpnipsec network site London raz*
- *vpnipsec network site London add remote 172.22.11.0 255.255.255.0*
- *apply*

while the configuration on the London site is:

- *ip external 192.168.155.2 255.255.255.0*
- *ip internal 172.22.11.254 255.255.255.0*
- *mode vpnipsec on*
- *vpnipsec access off*
- *vpnipsec authenticate psk very-strong-and-long-psk-2connect-2london*
- *vpnipsec site add Paris 192.168.155.1 psk very-strong-and-long-psk-2connect-2paris*
- *vpnipsec network site Paris raz*
- *vpnipsec network site Paris add remote 172.22.10.0 255.255.255.0*
- *apply*

In the example above, to simplify the configuration we used the same network (*192.168.155.0*) to connect both CacheGuard's **external** network intefaces. In reality, the **external** network interface of each appliance is connected to a distinct internet router that source NAT all outgoing traffic with its public IP address. Let’s consider that the internet router in Paris has the *10.0.10.1* public IP address (with the *192.168.155.254* private IP address) and the internet router in London the *10.0.11.1* public IP address (with the *192.168.155.254* private IP address). In this case, the configuration on the Paris site would be:

- *ip external 192.168.155.1 255.255.255.0*
- *ip internal 172.22.10.254 255.255.255.0*
- *ip route add default 192.168.155.254*
- *mode vpnipsec on*
- *vpnipsec access off*
- *vpnipsec authenticate psk very-strong-and-long-psk-2connect-2paris*
- *vpnipsec site add London 10.0.11.1 psk very-strong-and-long-psk-2connect-2london*
- *vpnipsec network site London raz*
- *vpnipsec network site London add remote 172.22.11.0 255.255.255.0*
- *vpnipsec nat role London active*
- *vpnipsec nat public add 10.0.10.1*
- *apply*

while the configuration on the London site is:

- *ip external 192.168.155.1 255.255.255.0*
- *ip internal 172.22.11.254 255.255.255.0*
- *ip route add default 192.168.155.254*
- *mode vpnipsec on*
- *vpnipsec access off*
- *vpnipsec authenticate psk very-strong-and-long-psk-2connect-2london*
- *vpnipsec site add Paris 10.0.10.1 psk very-strong-and-long-psk-2connect-2paris*
- *vpnipsec network site Paris raz*
- *vpnipsec network site Paris add remote 172.22.10.0 255.255.255.0*
- *vpnipsec nat role Paris passive*
- *apply*

UDP encapsulation and NATT: it is **IMPORTANT** to note that UDP encapsulation is systematically used by CacheGuard appliance to allow IPSec traffic to successfully traverse NAT devices.

In our example, as both CacheGuard appliances are behind NAT (their external IP addresses are translated into a public IP address), the VPN tunnel can't be established without some additional settings. In such a situation, one site should take an active role (to initiate the VPN establishment) while the other should act as passive (wait an incoming VPN establishment request). In our example we choose to set the London site as an active site and the Paris site as a passive site. In addition, as the used authentication method is PSK, the passive appliance (in Paris) should know it's public IP address to know which PSK in its PSK base should be used. Hence, the vpnipsec nat public add 10.0.10.1 command used on the Paris site.

Client error 404	Object not found
Message	The requested URL was not found on this Web Gateway. The request for this URL could not be served at this moment.

Client error 404	Object not found
Message	The requested URL was not found on this Web Gateway. The request for this URL could not be served at this moment.

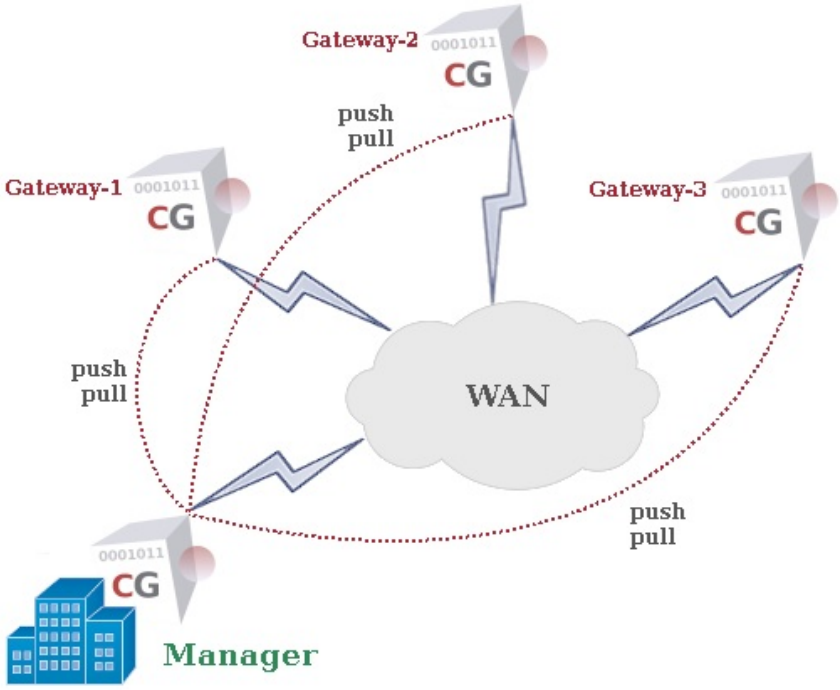
Client error 404	Object not found
Message	The requested URL was not found on this Web Gateway. The request for this URL could not be served at this moment.

Client error 404	Object not found
Message	The requested URL was not found on this Web Gateway. The request for this URL could not be served at this moment.

Client error 404	Object not found
Message	The requested URL was not found on this Web Gateway. The request for this URL could not be served at this moment.

Using a Manager

If you deploy several CacheGuard Gateways in your organisation, you have the possibility to configure them separately one by one. But most of the time deployed Gateways in the same organisation have similar configurations and you are required to repeat the same configuration process as many times as you have deployed Gateways. A CacheGuard Manager system gives you the possibility to centrally configure and manage several remote Gateways from a single point. With a manager you have the possibility to create a configuration template and build Gateway configurations based on that template. Built configurations on a Manager system can then be pushed in parallel to several gateways with just a couple of clicks or commands.



Also if you need to automatically update data like URL lists, the Manager allows you to download them only once and push them in parallel to all managed Gateways. The Manager allows you to manage your Gateways in a uniform and optimised way.

Gateway Access

Before being able to manage Gateways from a Manager, Gateways should allow the Manager to have a management access to them. The Manager uses the SSH protocol and SSH keys to connect to Gateways. That's why Gateways should allow the Manager's IP address to have an SSH access to them and authorise the Manager's SSH public key (to do not have to enter a password for each SSH access). A Gateway can be managed by one master Manager and optionally a backup Manager. The backup manager has always a hot copy of all Gateway configurations on the master Manager and can be activated in case of a failure on the master Manager.

Note that a Manager system has only one logical network interface called **internal**. To get the Manager's IP address and its SSH public key, you can use the following commands on the Manager:

- *ip internal*
- *manager ssh show*

To allow a master Manager that has the IP address 192.168.1.22 and the SSH public key 'ssh-rsa AAAAB3Nza...' to have a management access on a Gateway system via its external NIC, use the following commands on the Gateway:

- *manager add master external 192.168.1.22 'ssh-rsa AAAAB3Nza...'*
- *apply*

Gateway Enrolment

Once a Manager is allowed to access a Gateway, the first step is to enrol Gateways on the Manager and optionally pull Gateways current configurations and save them on the Manager. Gateway configurations on the Manager are identified by a unique identifier that you have to set during the enrolment. In addition, Gateways on the Manager are organised by groups called domains and a Gateway should belong to one and only one domain. In this way, you can

push or pull configurations in parallel on all Gateways belonging to a domain.

To enrol and pull the configuration of a Gateway having the IP address 10.0.10.254 use the following commands on the Manager:

- *manager gateway add my-company gateway-1 10.0.10.254*
- *manager gateway pull my-company gateway-1*

Note that in this example, *my-company* and *gateway-1* are respectively the identifier and domain name selected for the enrolled Gateway. The pull operation is performed in background. To get a report on the latest pull operation, use the following command:

- *manager gateway report pull*

Gateway Configuration

Gateway configurations can be modified on the Manager and then be pushed to remote Gateways by the Manager. To begin editing a Gateway configuration on the Manager, use the following command:

- *manager gateway begin conf gateway-1*

This command takes you inside the Gateway configuration context where you can use commands that you normally use on a Gateway system. Once you finished configuring the Gateway, you can use the **apply** command to verify and validate its integrity and then use the **end** command go back to the Manager configuration level. At this stage you have the possibility to push the new Gateway configuration to the remote Gateway by using the following command:

- *manager gateway push my-company gateway-1*

The push operation is performed in background. To get a report on the latest push operation you can use the following command:

- *manager gateway report push*

Working with Templates

The Manager's strength is its ability to work with templates. A template is a particular Gateway configuration that you can apply to Gateways. In this way, you can quickly configure multiple Gateway systems that have almost the same configuration. You will just need to customise what should be different on a Gateway compared to another (its IP addresses for instance). To create a template called *my-template* on a Manager system and then begin to configure it use the following commands:

- *manager template add my-template*
- manager template begin conf my-template

Once you finished configuring the template, you can use the **apply** command to verify and validate its integrity and then use the **end** command go back to the Manager configuration level. Now that you have a template, you can apply it to a Gateway configuration. To achieve that, you must be inside a Gateway configuration context. To configure a managed Gateway using a template called *my-template* use the following command:

- *conf manager template my-template*

Master & Slave Managers

In order to offer recovery and availability, a slave Manage can be configured to have a hot copy of all data on the master Manager. In this way, in case of a failure on a master Manager, the slave Manager can be activated in order to offer service continuity in handling managed Gateways. To allow the master and slave Managers to communicate with each other, both Managers should know the IP address of the other. In addition, the slave Manager should be know the SSH public key of the master Manger to allow it to connect using SSH. Assuming that the master Manager has the 192.168.1.22 IP address and the slave Manager the 192.168.1.33 IP address, use the following commands on the master Manager:

- *manager sync role master*
- *manager sync peer 192.168.1.33*
- *apply*

And the following commands on the slave Manager:

- *manager sync role slave*
- *manager sync peer 192.168.1.22 'ssh-rsa AAAAB3Nza...'*
- *apply*

Where '*ssh-rsa AAAAB3Nza...*' is the SSH public key of the master Manager.

Administration Interfaces

This section describes how to connect to a CacheGuard appliance in order to configure and administrate it. Three configuration/administration interfaces are available in a CacheGuard appliance:

- The console port
- The HTTPS interface (Web administration GUI)
- Secure Shell (SSH)

Each interface is detailed below.

The Console port

The console port is the main interface of a CacheGuard appliance. It is either a serial port (male DB9 RS232) or simply a Screen/Keyboard connected to the appliance. To use the serial port, link up your CacheGuard appliance serial port and your workstation serial port using a crossed serial cable. Then you can use your favourite terminal emulator (putty, minicom, screen...) to connect to your CacheGuard appliance. Serial communications with a CacheGuard appliance should use the following configurations: 115200 8N1 (115200 baud rate, 8 data bits, None parity, 1 stop bit).

The console port is the most secure and available administration interface in a CacheGuard appliance. Note that after the installation, the only available administration interface is the console port. To give remote administration access to an administrator for the first, you must use the console port (*access admin* command).

An administrator must be authenticated before connecting to the system. The "*admin*" user is the main administrator with the highest administration level. Other administrator users with less privileges can be added to the system using the command admin user. You must login as the "*admin*" user for the first to connect to the appliance. The password to use is the password that you setup during the installation (the default password for pre installed CacheGuard appliances is "*admin*"). Please refer to the Administrator Users section of this documentation for further information on administrator users.

The administration/configuration process via a character interface (console port or SSH) is made using the CLI (Command Line Interface). To see the list of all available commands, use the help command without any arguments. To get help on how to use a command, use the help command followed by that command name. If you forget the syntax of a command, a completion facility can help you to find its right syntax to use. The completion is available by using the <TAB> keyboard key.

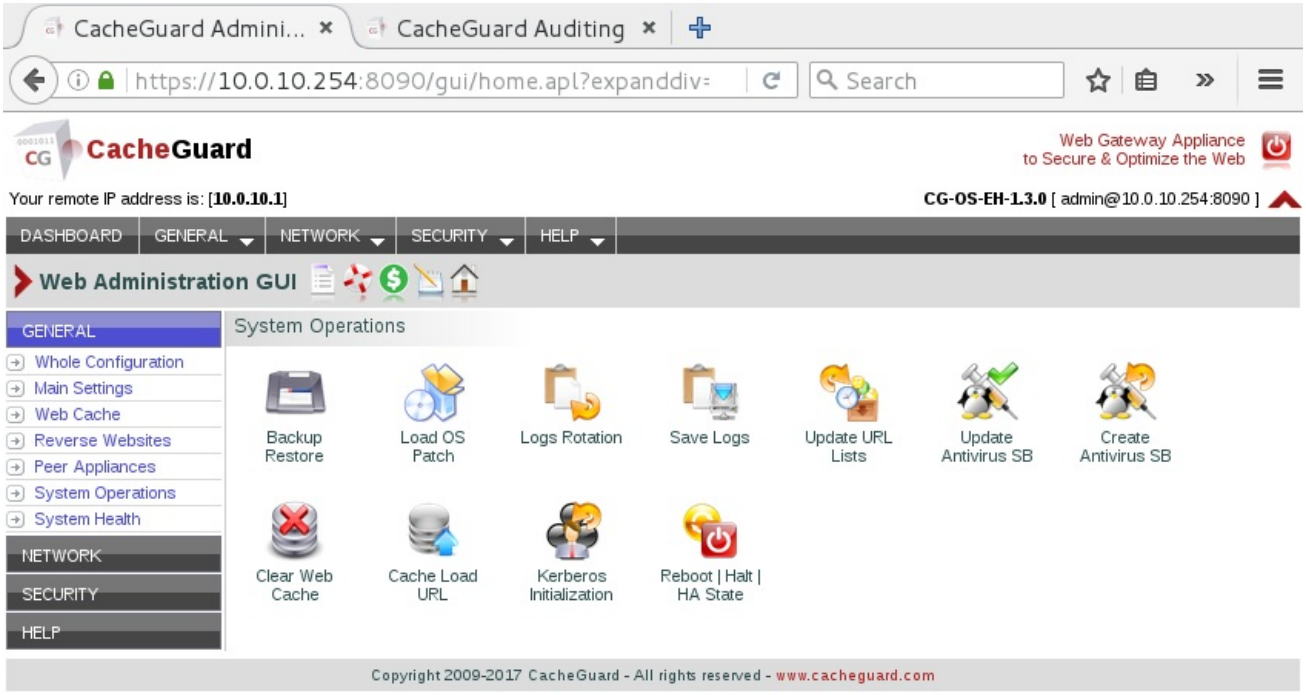
When using a character interface, the administrator has the ability to create mini-programs using a light-weight "*bash*" (an open source scripting language). Finally, you can use the history command to get an history of previously typed commands. To disconnect from the console port, use the exit command. The connection is also automatically closed if no command is typed for a certain period of time.

Web Administration GUI

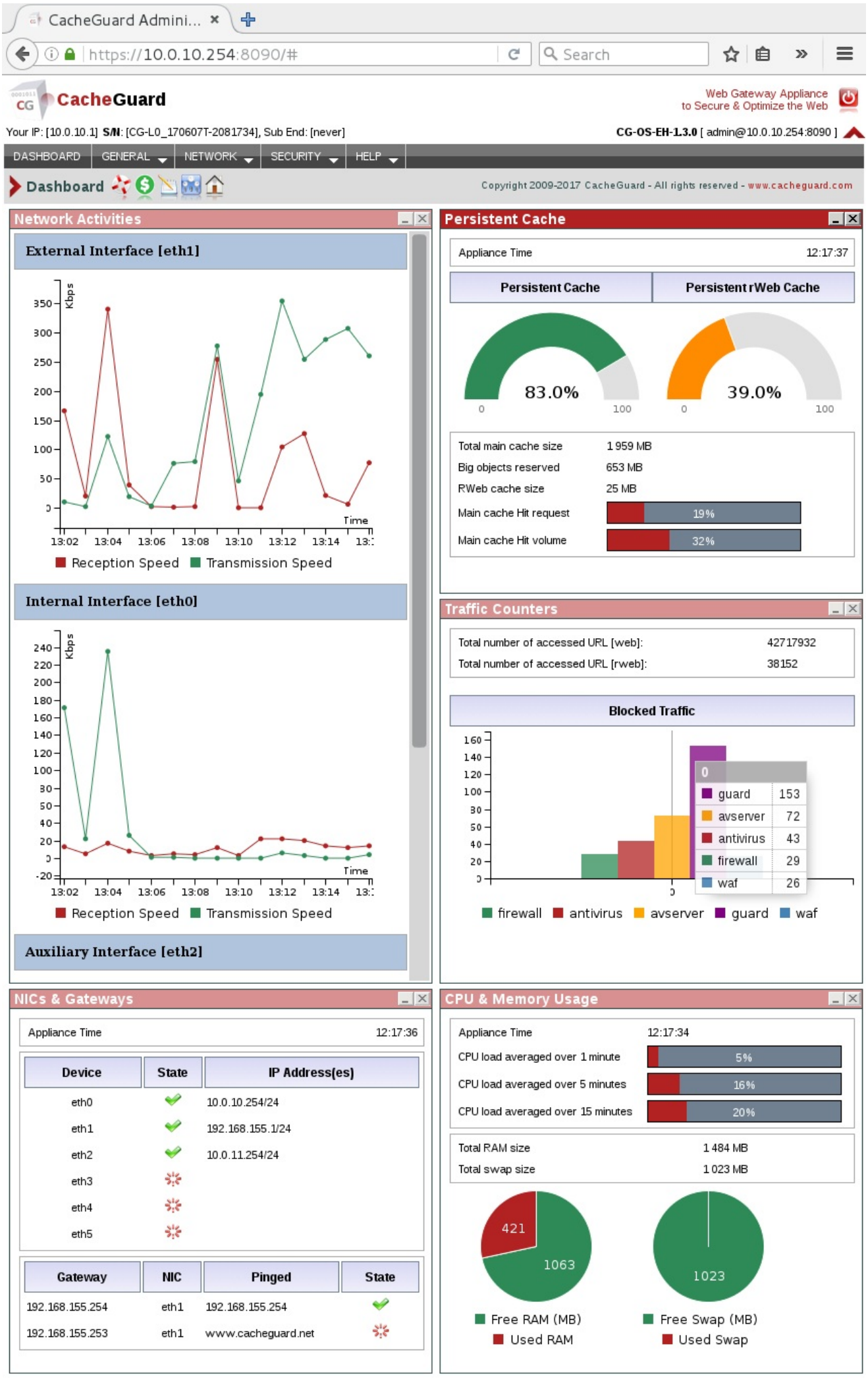
For those who are not familiar with a CLI (Command Line Interface) or simply prefer a GUI (Graphical User Interface), a Web administration GUI is available. To connect to the Web administration GUI you need a Web browser. CacheGuard supports almost all modern Wen browsers in the market such as, but not limited to, Firefox, Chrome, Safari, Opera and Edge. Before being able to connect to a CacheGuard appliance via a Web browser, the Web administration GUI should be activated on the appliance and the remote administrator IP must be allowed to connect.

To activate the Web administration GUI on the appliance and allow remote administrators in the network "*10.20.0.0 255.255.255.0*" to connect to the appliance via its internal network interface, use the following commands:

- *admin wadmin on*
- *access admin add internal 10.20.0.0 255.255.255.0*
- *apply*



Once the apply operation is finished, the appliance can be administrated using a Web browser. To connect to the Web administration GUI, use the following URL: "***https***://10.20.0.254:8090" where 10.20.0.254 is the internal IP address of the appliance. Note that the used protocol is HTTP**S** (and not HTTP). The default Web administration GUI port number is 8090. To modify this value you can use the **port wadmin** command. By default, the password for the Web administration GUI is the same as the password used to login via the console port. It is recommended that you create a separate password for the Web administration GUI as opposed to the password used for character interfaces (using the **password wadmin** command).



The Web administration GUI is a graphical front end to the CLI and can replace the CLI or be used in parallel with it. Using the Web administration GUI is very straightforward: in a first step you build a configuration using different Web pages available via menus and then you activate it by performing an apply operation (as this is the case with the CLI).

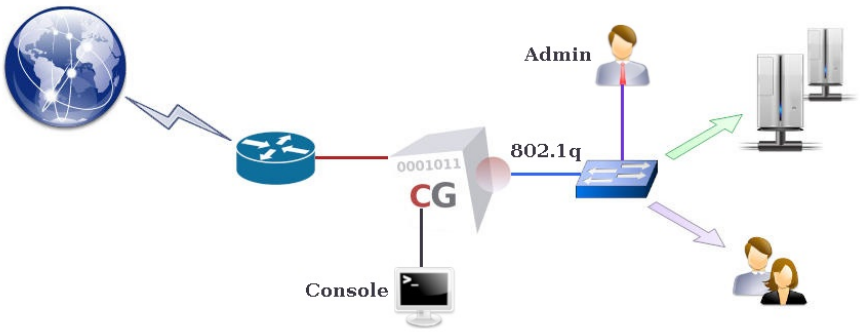
When the running (active) configuration is different from a newly built configuration, a blinking down arrow button appears in the title bar inviting you to press on it. Pressing on that icon forwards you to the Apply New Configuration page where you can proceed with the apply operation by pressing the SUBMIT button (or on the green check icon in the title bar) ; it's that simple. The Web administration GUI is not detailed in the User's Guide as we hope that its usage is as friendly as straightforward to do not require a detailed documentation.

Secure Shell (SSH)

The appliance can also be remotely administrated using an SSH client. When logged in via an SSH client, the administrator can use the CLI to administrate and configure the appliance. To use the SSH administration interface you should use an SSH client installed on your workstation (Linux *ssh* command or the *Putty* application).

To use the SSH administration interface, remote administrators should be allowed to access the appliance and the SSH service should be activated on the appliance. To activate the SSH service on the appliance and allow remote administrators in the network *10.20.0.0 255.255.255.0* to connect to the appliance via its internal network interface, use the following commands:

- *admin ssh on*
- *access admin add internal 10.20.0.0 255.255.255.0*
- *apply*



Once the apply operation is finished, the appliance can be administrated via an SSH client. To connect to a remote CacheGuard appliance from a Linux system, use the "*ssh admin@10.20.0.254*" command where 10.20.0.254 is the internal IP address of the remote CacheGuard appliance. The SSH password to use is the same as the password used to login via the console port. It is also possible to import a public SSH key into a CacheGuard appliance to be able to connect to it without having to enter the administrator password. Among other things, using an SSH key allows you to automate periodic tasks such as a system backup (see the **system backup** command).

The process of generating SSH keys depends on the used remote workstation. For instance, to generate an SSH key pair (public and private) on a Linux system you can use the "*ssh-keygen*" command. To import a public SSH key into a CacheGuard appliance, you should first copy it on a file server supporting TFTP, FTP or SFTP protocols and then load it into your CacheGuard appliance from that file server (you can also run that file server on your workstation). Only trusted file servers are allowed to exchange files with a CacheGuard appliance. To add the file server having the *10.20.0.1* IP address to the list of trusted file servers and allow it to exchange files via the internal network interface of a CacheGuard appliance, use the following commands:

- *access file add internal 10.20.0.1*
- *apply*

Each SSH key must be identified with a unique identifier that you should specify prior to import it into a CacheGuard appliance. To add an SSH key identified by the *john* identifier and import it into your CacheGuard appliance from a trusted TFTP file server, use the following commands:

- admin ssh key add john
- admin ssh key load john tftp 10.20.0.1 id_rsa.pub

where *10.20.0.1* and *id_rsa.pub* are respectively the file server IP address and the SSH key filename on that trusted file server. After having imported a public SSH key into a CacheGuard appliance, an allowed remote administrator having the private SSH key associated to that imported public SSH key can login without having to enter a password.

To disconnect an SSH session use the exit command. The SSH session is also automatically closed if no command is typed for a certain period of time.

Administrator Users

Only authenticated users are allowed to administrate and configure a CacheGuard appliance. The main administrator user is named "*admin*". This user exists by default in the system and has the highest privilege.

Secondary administrator users with fewer privileges can be added to the system. Secondary administrators have the right to build configurations but cannot apply them (only the "*admin*" user has this privilege). Some secondary administrative operations such as cache loadurl can be executed by secondary administrators. The admin user command allows you to manage secondary administrator users.

To create a new administrator user called "*john*", login as the "*admin*" user first and then use the following commands:

- *admin user add john*
- *apply*

By invoking the "*admin user add john*" command, the "*admin*" user is asked to choose a temporary password for "*john*". Once the apply operation is finished, the administrator user called "*john*" can login. The first time a secondary administrator login to a CacheGuard appliance, she/he is invited to modify her/his password by entering an allowed password (see the command password to learn more about allowed passwords).

CacheGuard Monitoring

CacheGuard services and the machine on which CacheGuard-OS is operarting can be monitored at any time to have a quick look on the status of a CacheGuard appliance. The monitoring allows you to detect failures and dysfunctions soon enough so you can undertake actions to repair them and provide the required service continuity to your users. To monitor the system you can use SNMP (Simple Network Management Protocol) or directly connect to the system and use online commands or equivalent Web administration GUI pages.

Note that essential services are internally monitored by a third service called the "*Health Checker*". In case of a failure on an essential service, the "*Health Checker*" tries to restart the failed service. This operation is logged internally and if configured, an SNMP manager can receive a trap on the status of that restart operation.

Direct access

You can use some commands combined with the **report** keyword to get a report on the underlying command function. As an example, you can use the following commands:

- *system report*
- *urllist report*
- *antivirus report*

You can refer to the Commands Manual to learn more about commands that support reporting.

Using SNMP

A CacheGuard appliance integrates an SNMP agent that can be polled by an SNMP manager. It is also possible to configure the appliance to send SNMP traps to an SNMP receiver. Please note that a CacheGuard appliance uses TCP SNMP traps called SNMP notifications. To allow an SNMP manager having the *172.18.2.1* IP address to poll your CacheGuard appliance and send SNMP notifications version 1 to a receiver having the *172.18.2.2* IP address use the following command:

- *admin snmp on*
- *access mon add internal 172.18.2.1*
- *admin snmp trap add v1 172.18.2.2*
- *apply*

By invoking the "*admin snmp trap add v1 172.18.2.2*" command, the administrator is asked to enter a password (SNMP community string) to connect to the SNMP receiver. SNMP v1, v2c and v3 are supported by CacheGuard-OS and the SNMP agent can be configure to work with UDP, TCP and TCP tunnelled over TLS. Well-known MIBs commonly used to monitor Linux systems are supported and a dedicated MIB called CacheGuard-MIB can also be used. You can find the ASN.1 MIB description of CacheGuard-MIB via the Web administration GUI (menu option *[NETWORK] > [Monitoring Configuration] > [SNMP Agent Settings]*), on the original installation CDROM or the official CacheGuard website.

Traffic Logging

The logging gives you visibility into allowed or denied traffic exchanged with or via a CacheGuard appliance. As an administrator, you have the possibility to select which type of traffic should be logged. You can refer to the log command description in the Commands Manual to learn more about available log types. Logs are stored locally on a CacheGuard appliance and can be saved on trusted remote file servers for inspection. You have also the possibility to send them in real time to remote log servers using the "*syslog*" protocol (based on UDP or TCP).

Managing Logs

An daily automatic log rotation during off-peak hours (between 04:00 AM and 06:59) backups logs for a period of *n* days where *n* is a value between 1 and 365 configured during the CacheGuard-OS installation. Each rotated log is identified by an integer between 1 and *n* called the log serial number. The most recent log (yesterday log) has the number 1 and oldest one has the number *n*. Note that in case where the appliance is overloaded, logs rotation occurs hourly in order to avoid to fill the provisioned log space on disks.

To save the current (today's) log, an explicit log rotation should be forced. The explicit log rotate allows you to do not have to wait for the daily automatic logs rotation. To rotate logs and have a report on the status of the log rotation, use the following commands:

- *log rotate*
- *log rotate report*

Once the log rotation operation is finished, you can save the desired log types on a trusted file server. Note that saved logs are in a gzip compressed format. To save the most recent Web access log in a file named "*web-access-log.gz*" located on the TFTP server having the IP address *172.18.2.1*, use the following command:

- *log save web 1 tftp 172.18.2.1 web-access-log.gz*

Note that logs can be saved on trusted file servers only. To declare a file server as trusted use the access file command. The logging can also be completely disabled. To completely disable the logging, use the following commands:

- *mode log off*
- *apply*

Logging Web Accesses

All Web accesses in forwarding and reverse modes can be logged. The Web access logging allows you to observe all Web access in detail and know which machine accesses which URL at which time. To activate the Web access logging in forwarding and reverse modes, use the following commands:

- *mode log on*
- *log type web on*
- *log type rweb on*
- *apply*

Logging Denied Traffic

Allowed access logging concerns Web traffic only (in **web** or **rweb** modes). However, all rejected traffic (Web or non Web) by services running on a CacheGuard appliance can be logged. For instance, you have the possibility to configure the appliance to log all attempts to access forbidden URLs (denied by the URL guarding) and all rejected network traffic at the IP level (denied by the firewall). To this end, you must use the following commands:

- *mode log on*
- *log type guard on*
- *log type antivirus on*
- *log type waf on*
- *log type firewall on*
- *apply*

Syslog Servers

You can optionally send all locally saved logs to remote log servers that support the *syslog* protocol (UDP or TCP). Prior to activate the logging of a traffic type on a remote syslog server, the remote syslog server must be allowed on a

CacheGuard appliance. To configure the appliance to send in real time its URL guarding logs to the syslog server having the IP address *172.20.2.1* and configured to use UDP, use the following commands:

- *mode log on*
- *log syslog add udp 172.20.2.1*
- *log type guard on on*
- *apply*

More than a syslog server can be specified on a CacheGuard appliance. In this case, logs are send to all specified syslog servers in parallel.

Operating System

Registration & Subscription

The registration process allows you to get a free S/N (Serial Number) that uniquely identifies your CacheGuard appliance. For commercial installations, the S/N is then used to purchase a subscription that allows you to use your appliance for a given period of time. A subscription is effected by a license key, which is sent to you the first time you purchase a subscription. Following the initial subscription period, a subscription renewal is required to continue to use your appliance.

The registration process is normally a manual process that should be initiated form an already installed appliance. Note that a CacheGuard appliance on a public cloud is automatically registered during its deployment. To begin the registration process it is more convenient to use the Web administration GUI as you will be asked to connect to the CacheGuard appliance registration Web portal to get an OTP (One Time Password).

To begin the registration process, go to the menu option *[GENERAL] > [Main Settings] > [Registration & Subscription]* of the Web administration GUI and follow given instructions. Please refer to the register command in the Commands Manual for further information.

Backup & Restore

To allow you to quickly recover a crashed machine due to a hardware or software issue, the configuration of a CacheGuard appliance and its essential data (antivirus signatures, URL lists, SSL certificates...) can be saved on a file server and then be restored on a freshly installed CacheGuard appliance (by reinstalling CacheGuard-OS on a new machine). To backup a CacheGuard appliance, you should A system first create a backup file on your appliance and then save that backup file on a trusted file server. The backup creation is a process that runs in background and you have to wait for its termination before being able to save the created backup file.

To create and save a system backup named "*cacheguard.backup*" on the trusted TFTP server having the IP address *172.18.2.1* use the following commands:

- *system backup create*
- *system backup create report*
- *# Wait for the backup process termination...*
- *system backup save tftp 172.18.2.1 cacheguard.backup*

Backup files can only be saved on trusted file servers. To declare a file server as trusted, use the access file command. To restore a previousely saved backup named "*cacheguard.backup*" from the trusted TFTP server having the IP address *172.18.2.1* use the following commands:

- *system backup load tftp 172.18.2.1 cacheguard.backup*
- *apply*

It is important to note that this backup and restore method works only if the freshly installed CacheGuard appliance and the failed CacheGuard appliance are on the same CacheGuard-OS version. In case where the freshly installed CacheGuard appliance and the failed CacheGuard appliance would not be on the same CacheGuard-OS version, you will have the possibility to make a logical restore. The logical restore is described in the Reinstalling the OS below and would require that you have to have a copy of your CacheGuard appliance logical configuration. See the Reinstalling the OS below for further information.

Patching the OS

CacheGuard Technologies Ltd regularly releases new CacheGuard-OS versions and provides OS patches to upgrade already installed CacheGuard appliances to the latest CacheGuard-OS version. It goes without saying that it is highly recommended to keep your CacheGuard appliance up to date by installing the latest available patches.

Patching the OS is always subject to risk. That's why it is highly recommended that you save your logical configuration and all its related data/files (SSL certificates, custom WAF rules, antivirus whitelist...) on a trusted file server before proceeding with an OS patch. In this way, you will be able to reinstall your CacheGuard appliance from scratch by installing the latest CacheGuard-OS version on it and then restore your configuration. The section Reinstalling the OS below describes how to easily recover a CacheGuard appliance configuration.

OS patches can be loaded on a CacheGuard appliance from a trusted file server and then be applied to the appliance (refer to the access file command to declare a file server as trusted). To load a patch file named *CacheGuard-UF-64-2.1.3-patch.cgp* from the trusted TFTP server having the IP address *172.18.2.1*, use the following commands:

- *system patch tftp 172.18.2.1 CacheGuard-UF-64-2.1.3-patch.cgp*
- *apply*

You can get CacheGuard-OS patches from official CacheGuard servers on the internet. CacheGuard-OS patches can also be directly downloaded on a CacheGuard appliance from an official CacheGuard patch server on the internet. Please refer the system command in the Commands Manual for further information.

Caution: during the patching operation, it is highly recommended to take all precautions to avoid any power shortage on your CacheGuard appliance. If during the patching operation your machine is accidentally turned off or if, for an unforeseeable reason, the patching operation fails, the appliance may fall into an inconsistent state and then, the only recovery solution would be to reinstall CacheGuard-OS on your machine and then manually restore your configuration.

Reinstalling the OS

Some major CacheGuard-OS versions may be released without providing an OS patch. Those releases require that you reinstall CacheGuard-OS from scratch on your machine. In order to avoid having to manually reconfigure your newly installed CacheGuard appliance, you can save its logical configuration and all data/files related to that logical configuration (SSL certificates, custom WAF rules, antivirus whitelist...) on a trusted file server. In this way, you will be able to restore them on your newly installed CacheGuard appliance.

To save the logical configuration of a CacheGuard appliance in a file named "*CG.conf*" and all its related data in separated files in a folder named "*CGFiles*" located on a TFTP server having the IP address *172.18.2.1*, use the following commands:

- *conf save tftp 172.18.2.1 CG.conf*
- *file save tftp 172.18.2.1 CGFiles*

To restore a CacheGuard appliance logical configuration from a file named "*CG.conf*" and all its related data/files from a folder named "*CGFiles*" located on a TFTP server having the IP address *172.18.2.1*, use the following commands:

- *conf load tftp 172.18.2.1 CG.conf*
- *file load tftp 172.18.2.1 CGFiles*
- *apply*

Please be aware that there is some limitations to this logical backup and restore method. With this method, the following data/files are not saved and then can't be restored:

- Administrator passwords
- Antivirus Signatures
- URL lists

But no worries, antivirus signatures and URL lists are automatically downloaded from trusted file servers during the apply operation. However, if you have secondary administrator users, you will have recreate them manually.

Rebooting the Appliance

In some circumstances you may be asked to reboot your CacheGuard appliance. To reboot your appliance, use the command reboot.

Client error 404	Object not found
Message	The requested URL was not found on this Web Gateway. The request for this URL could not be served at this moment.