A high-availability, next-generation-firewall for distributed networks

Dr. Götz Güttich

With the devices in the Eagle and Wolf Series, Clavister is supplying next-generation firewalls which are particularly suitable for environments where multiple firewalls are in use, for example, in distributed networks. Their central management tools ensure that the relevant staff always have a clear overview of the situation. The devices are available as part of various hardware configurations which means that companies can use the device that best suits the performance requirements in that branch's particular environment. Since the hardware solutions only differ in their performance (in terms of functionality, all of the products are identical), this test, which was carried out using two Clavister W30s, is also applicable to the other next-generation firewalls from the same manufacturer.

The Clavister W30, which was designed for use in branch offices, remote offices and small data centres includes VPNs (IPsec, L2TP, PPTP and SSL), advanced routing (also as part of a policy) and anti-spam features alongside the actual firewall functionality with deep packet inspection, as is the case with modern next-generation firewalls (NGFs). In addition to this, there are Kaspersky anti-virus functions, an IPS, load balancing, bandwidth management, link aggregation, a web filter and application control functions. The device has six GBit ethernet interfaces and an expansion slot and supports high availability to enhance the failsafe characteristics of the NGF installation.

The test

In the test, we firstly set up one of the W30 solutions on our network as an internet gateway. To do this, we connected the product to the network switch and DSL modem and booted it. We then accessed the web-based management interface of the device using a browser and ran the initial configuration. Alternatively, there is a command line which can run batch files, for example. This makes sense when many new devices need to be configured automatically.

Once the initial setup was completed, we looked at the configuration tool in detail via a browser (which, according to the manufacturer, is best for managing individual devices) and learned about the functional scope of the solution. In addition, we adapted the configuration specifically to our needs.

Next, we set up various VPN connections to external networks and devices. Once this had been done, we installed the central management tool "Clavister InControl" on a Windows 7 work station, which, according to the manufacturers, can manage several thousand gateways and included our gateway in the InControl configuration. We then took InControl in hand and analysed the scope of the solution.

When this process was completed, we analysed the internal and external interfaces of the device with various security tools such as Nessus, Nmap and Metasploit. We had assigned the external interface with a fixed IP address for this purpose. Our goal was to find out if there were security flaws or if the solution revealed

unnecessary information that could help hackers to attack the system. Furthermore, we also used several attack tools to perform DoS attacks on the device, for example, and to test how it responded to them.

Finally, we modified our test installation so that we could look at the high-availability function of the products (HA) in detail. Since the HA feature can not cope with dynamically assigned external IP addresses and PPPoE connections, for this purpose, we connected both devices as a cluster behind a router which took on the role of providing internet access.

In doing so, we maintained the configuration of the fixed external IP address. In the cluster, the system which was originally configured by us took on the role of the master. The second device, which we hadn't yet touched, had joined as a slave of the configuration from the master.

Commissioning

The commissioning process of the W30 is relatively simple. All you have to do is unpack the product and work through the enclosed quick-start guide. This suggests using the first interface as the LAN interface and the second for the WAN connection. Once all cables are connected, the relevant staff can boot the device and then connect to the product's web interface via the default IP address https://192.168.1.1.

After that, you will find yourself on the overview screen of the management tool. This allows you to start the "Setup Wizard", which will assist you during the initial configuration of the solution.

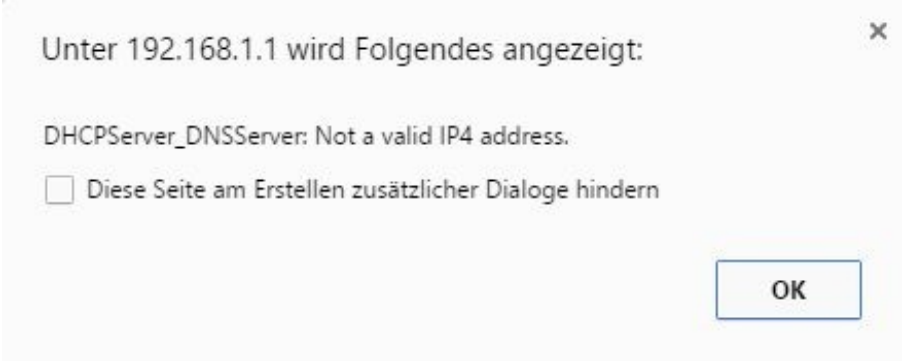
After we had completed this step, the system displayed a welcome screen which told us which steps the assistant would carry out. First of all, we had to set a new password for the administrator account, which makes sense, as it ensures that Clavister devices are not able to function on the network with standard passwords.

The next step was to set the correct time and to configure the time zone. Then we had to configure the WAN interface. As mentioned previously, we initially used the device as an internet gateway on a "Telekom" (company: German Telecommunications) DSL connection.

That is why we chose the option "PPPoE" for the WAN configuration. Alternatively, the solution can work with fixed IP addresses and those assigned via DHCP or via PPTP. For the PPPoE configuration, it sufficed to enter the user name and password and to assign the service a name. After that, the WAN interface was set up.

The next step was to set up a DHCP server for the LAN. In doing so, we mistyped something and discovered as a result that the wizard makes you aware of faulty configuration details and requests they be corrected. Therefore, you can assume that the initial configuration will generally run smoothly.

Finally, the assistant wants to know which time servers will keep the system time up to date and which syslog server should be used to receive data from the device. This brings the initial configuration to a close and the changes are adopted. Usually the licensing of the product is part of the functionality of the wizard, but we did not perform this step because our test devices already came with an installed licence.



The setup wizard alerts users to errors in the configuration

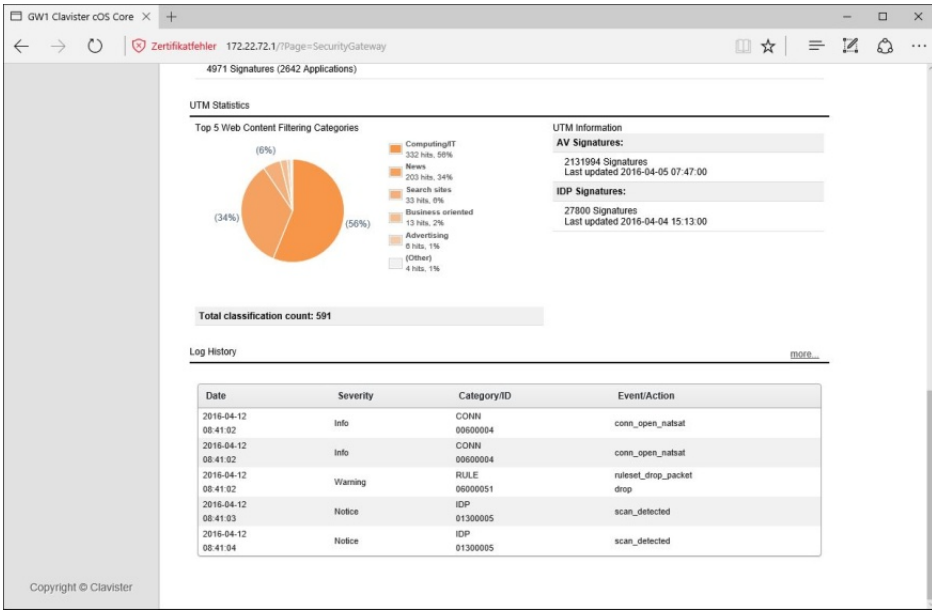
The web-based configuration tool is used to manually adjust the LAN address. In fact, this step is described in the "Getting Started Guide" available on the Clavister website so that there are no problems during the test. In our opinion, this step is also part of the initial configuration and should therefore be processed within the wizard. The same goes for the definition of rules for internet access.

By default, Clavister allows the services DNS and HTTP for access to the external network following the initial configuration. This can, of course, be changed at any time via the management

tool. However, it would be nice if the wizard could, at least, help in creating a rudimentary internet access policy which is more suited to the company's requirements.

The web-based configuration tool

After we had completed the initial configuration, we logged into the NGF using our new LAN address and started by setting up a guest LAN on the third interface of the device. We established a WLAN access point there so that visitors were able to browse the internet using our internet connection, without seeing our LAN components.



The status screen provides content filter statistics, as well as other information

To do this, we basically copied our LAN configuration with an additional DHCP server and another subnet on the third interface. The guest WLAN then worked as expected.

When we had ensured in this manner that all the users on our network had access to the internet via the Clavister device, we started to deal with the configuration tool itself and, as a result, the functional scope of the solution, thus adapting our setting specifically to our requirements. To do this, we firstly updated the device's firmware to cOS Core 11.02.01.03, the version that was up-to-date at the time of the test, to ensure that we were working with the latest version.

After logging into the web interface, the administrator will find himself back on a status screen which will inform him about the current status of the NGF. A menu bar appears at the top of the window and on the left-hand side there is a tree structure which contains the items which belong to the menu that is open.

The status screen mentioned above contains a system overview with performance, connections, CPU load, memory usage, system time, the top five applications, the top five web content filter categories and the like. You can view and search through various log files directly below this. These include the system log, the anti-virus log, the log for application control, the intrusion detection log and the content filter log.

Under "Sub Systems", the administrators can view the current blacklist and have the option to revoke existing lock-outs. In addition, it is possible to look at the existing connections in detail in list form.

From here, the DHCP server can also be configured, the hardware can be monitored (for example, the CPU temperature) and the interface activity can be displayed. The interface overview also includes graphical information relating to the send and receive rate. Furthermore, under Sub Systems, the system even displays the routing table, data regarding server load balancing and similar information.

The sub menu "Maintenance" gives users the opportunity to safeguard and restore the configuration and the core binaries. In addition to this, they can upload a new licence, perform a reset or reset the device to its factory default settings.

You can also activate notifications which will inform the relevant staff members about new firmware releases and set up automatic updates to the anti-virus and the intrusion protection system. This section was logically structured and should not pose administrators any issues.

Options for loading new firmware files and a support area which provides you with a diagnostic console with system messages and the option to download a support file that provides system information, together with a tools menu, make up the overview of

the system status. The tools menu includes functions such as Ping, an SSH key generator and a packet capture tool.

With the latter, data transmitted over individual interfaces can be captured and downloaded onto the PC in a CAB file for further analysis – for example with a sniffer. Overviews of IDP signatures are also included in the tools, as is an application library, which includes a large number of applications (such as AOL, Sophos AV, Google Play and many more) and informs the user about what each application does and what each application's associated hazard level is. Since the application library is used later to define the rules for application monitoring, it makes sense to familiarise yourself with it in advance.

The system settings

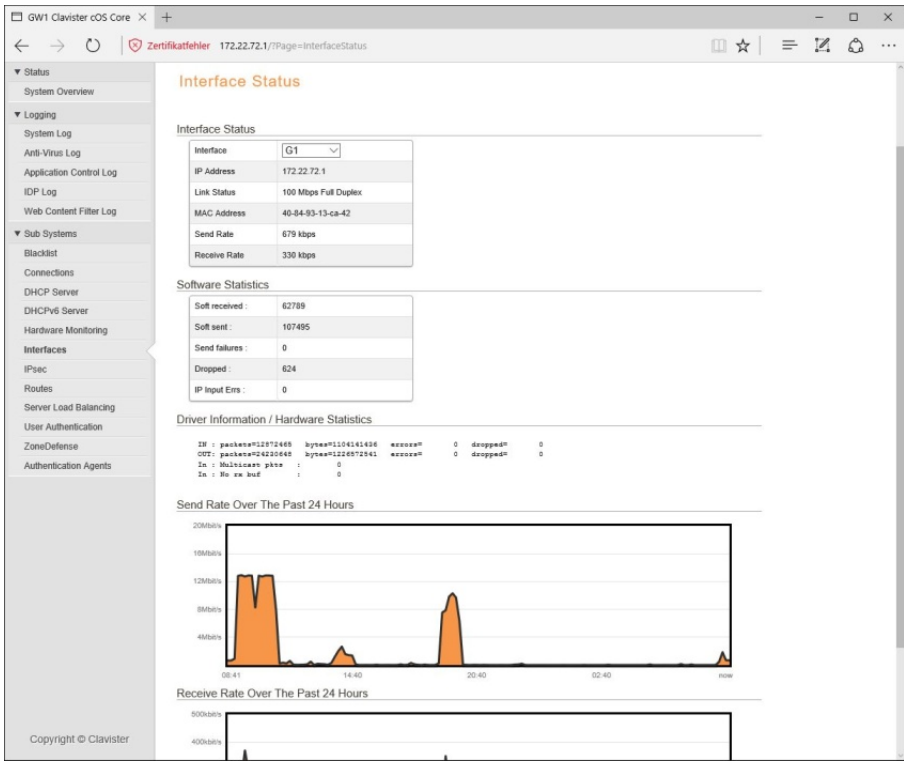
The main menu "System" contains all the settings to configure the device itself. First of all, these include the settings for the system time, time zone, time server and the DNS client. The persons responsible can also determine which users can access the device's management interface via which networks, which systems in the network can receive logs and events from the NGF (via services like syslog and SNMP) and what the high availability configuration looks like, which we will look at in more detail at a later date.

Monitoring is an important part of system management. First of all, monitoring of hardware plays a role in this respect. By default, Clavister has a sensor for the CPU temperature in place for this purpose. However, it is also possible to use other sensors which keep an eye on the voltage, the fan and similar components. Nevertheless, the availability of the sensors always depends on the hardware which is currently in use.

On the contrary, the purpose of the "link monitor" is to monitor items such as hosts or networks. If these are not available for any reason, the device is able to perform predefined actions such as failovers and reconfigurations.

not blocked by IDP and similar rules and the definition of HTTP banner files which define the appearance of the authentication and application level gateway restriction pages.

Various device settings round off the system menu. These include IP settings such as the default TTL, logging of checksum errors and many more, as well as TCP settings such as sequence number validation. If the administrators hover over an item with their



The interface status also includes graphical representations of the transmitted data traffic

Finally, the "real time monitor alerts" monitor certain values such as the CPU load, performance, the number of spam messages or even the number of dropped packages. The relevant employees can set limits for these and the NGF generates log entries if these thresholds are exceeded. The system settings also include user management for the local user database, a white list which contains entries that are

mouse (hover function), the W30 will display a brief explanation of every configuration option, which is very useful because there are settings here which not even IT employees who are well-versed in network protocols are necessarily familiar with. In addition to these protocols there are also settings relating to ICMP, PPP, connection time-outs, length limits and performing fragmentation and local reassembly. This

also applies to SSL settings, the state engine, the maximum number of pipe users and diagnosis. During operation, it occurred to us that the device is set up to send anonymous user statistics to Clavister automatically by default.

This can be prevented here, but in our opinion this configuration step should also be carried out as part of the initial setup wizard. Settings for application control such as the maximum number of unclassified packages and unclassified bytes round off the system configuration.

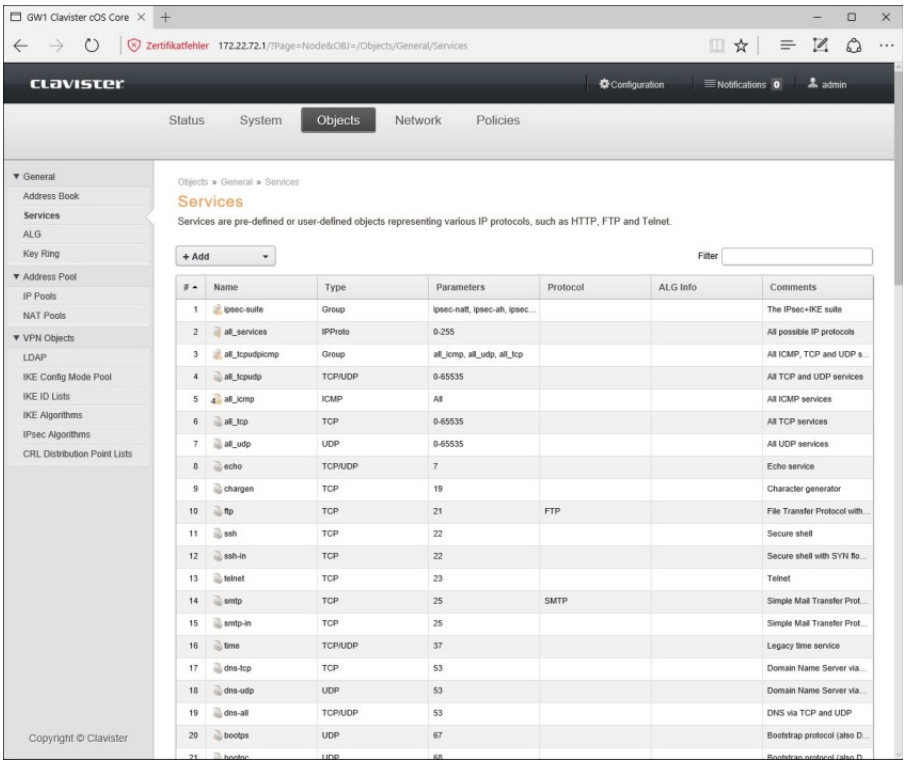
Objects

The objects are the basis for defining the policies. First of all, they include the address book, the IP, network and MAC addresses. If required, administrators also have the option to add new host and network addresses. In contrast to this, the services represent the protocols used on the network. Clavister has already predefined a large number of these, such as "all_icmp", "ssh", "ipsec_suite", "igmp" or "ping". Once again, it is also possible for the relevant staff to add their own items at any time.

Items relating to the application level gateways can be found under "ALG". ALGs for H.323 and SIP have been predefined, but you can also add your own where necessary, for example, for HTTP, POP3, PPTP and so on. In the same place, the relevant IT employees can view the key ring and create new keys, if necessary – such as for securing connections.

Another interesting point: the address pools. These are home to IP pools (dynamic items with IP leases) and NAT pools which can be used in NAT rules.

The VPN items are used to define virtual private networks. First of all, the VPN configuration



Clavister has already predefined all of the relevant services

enables LDAP servers to be defined. The NGF can download certificates and certificate revocation lists (CRLs) from these servers, if required.

The "IKE config fashion pool" then assigns IP addresses and DNS and WINS servers to the VPN clients during operation. Apart from that, the algorithms to be used and other items can be defined via the VPN settings.

Network settings

The purpose of the main point "Network" is essentially to configure the interfaces, VPNs and routes. Consequently, the settings for the ethernet adapter with address, network and virtual routing can be adjusted. The link aggregation can also be set here, along with the PPPoE interfaces, VLANs and similar items.

Another interesting point: the VPN configuration. The Clavister solution supports IPsec, SSL, GRE and 6in4 and can communicate not only with PPTP and L2TP servers and clients, but also with PPTP V3 and L2TP V3 components. During the test, we established IPSec connections to a Lancom router of the type 1781A and to the current NCP VPN client for Windows. These connections posed no difficulties.

That's not all, the network settings also support "interface groups" where multiple interfaces can be combined for easier policy management. In terms of routing, not only can the operator set static routes, but also implement routing tables on a policy basis.

Apart from that, it is also possible to achieve load balancing

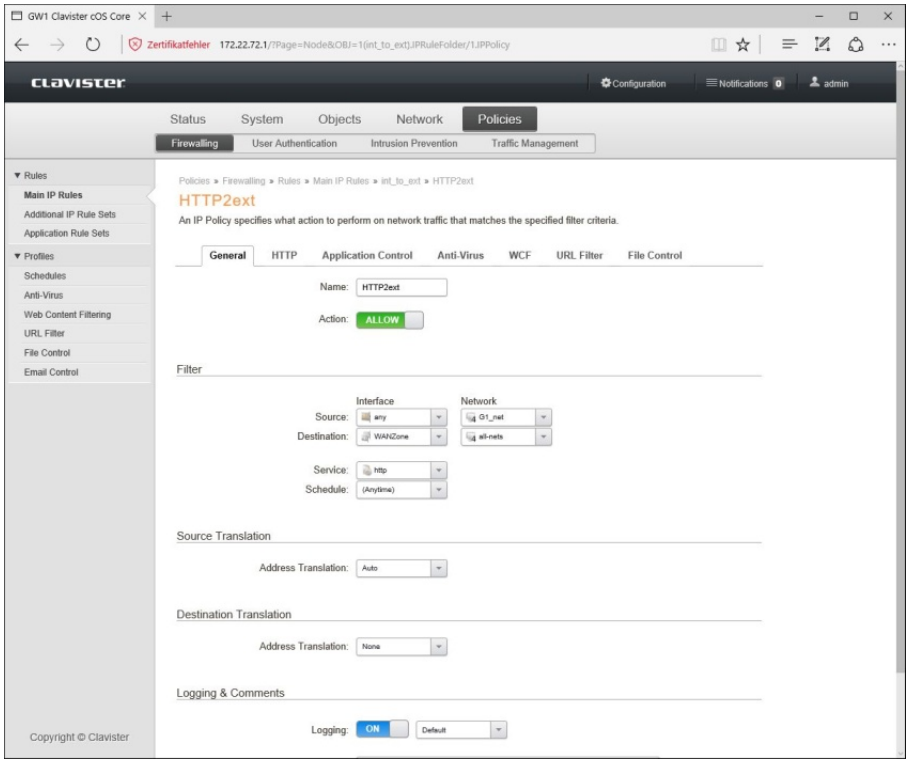
using the various routes. Dynamic routing with the help of OSPF, virtual routing and multicast routing are also supported. Finally, under "network services", the administrators configure DHCP servers and relays, radius relays, DynDNS and so on.

The policies

The area "policies" is at the heart of the NGF because the relevant staff set the rules that will be used to safeguard data transfers. In this regard, the "main IP rules" must be determined first of all. These can be compiled into groups to increase clarity and manageability.

For example, it is possible to disable all the rules in a group at once. The individual rules work – as is the case with most firewalls – with parameters such as source and destination of the data transfer (network, host and such like), the affected service (such as "FTP" or "all_ip"), the period (in which the rule is valid) and the action to be carried out (drop, allow, deny, reject). Furthermore, administrators also have the opportunity to add services such as application control, the web content filter, or even the anti-virus function to the policies, which will then become active for the relevant protocols. There were no absolutely no difficulties with this during the test.

At this point, let's say something about the application control mentioned above. This provides the appropriate staff with the option to create rules that only apply to the traffic generated by a specific application. It works with signatures that have been stored in a database. With the help of application control, very finely tiered policies can be created. For example, it is possible to assign a particular user group with a specific range for the use of Bittorrent. This allows the network data traffic to be adapted specifically to the requirements of the organization.



The definition of a firewall rule

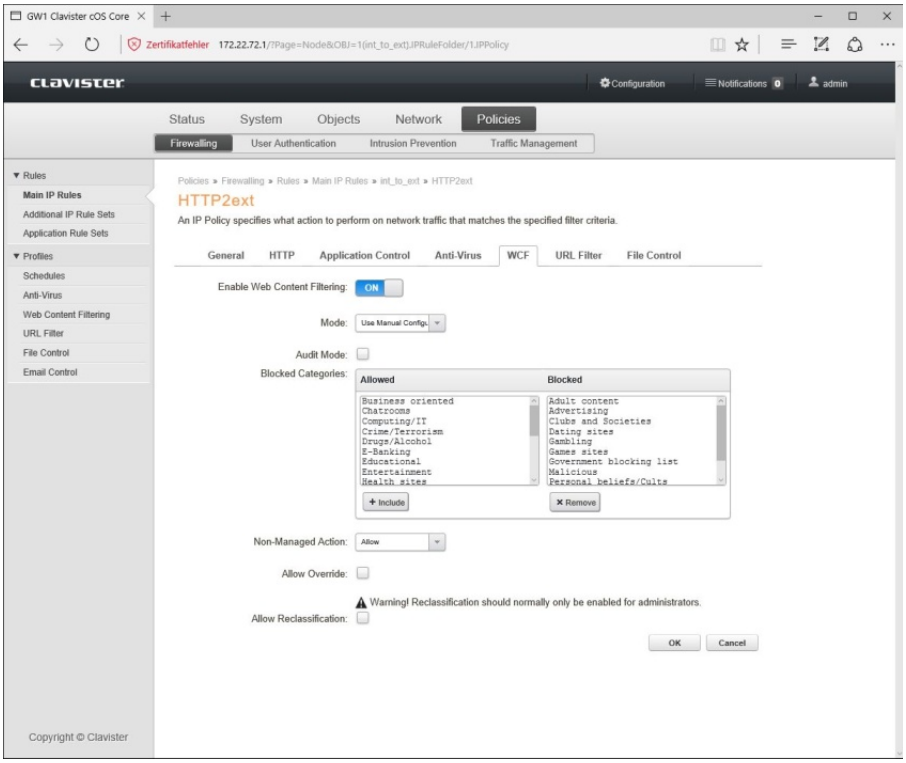
Under "Profiles", the relevant staff can specify schedules during which time certain rules apply. Framework conditions for services such as the anti-virus system (e.g. file types excluded by the scan or handling compromised files) and the web content filter (categories such as "advertising", "gambling", "swimsuit" etc. which are to be banned) can also be set, amongst other things. Email control with white and blacklist and anti-spam are also configured here.

In terms of user authentication, the system supports external LDAP and radius servers alongside the local database. Intrusion prevention works with signatures which can be used with the help of policies to monitor traffic for attacks. These policies consist of a name, the affected service, a schedule, the signatures in question and such like. On the other hand, the "zone defence" is used to block hosts and networks with the aid of switches in the event of IPS and threshold rule block infringements. Last but not least, the W30 also has extensive traffic-shaping functions.

Installation of InControl

After we had worked through the configuration tool and optimised our configuration, we installed the management software "InControl" on a test client on the LAN using Windows 7. As mentioned before, this is suitable for managing large installations with many NGFs. The software consists of a client/server combination. In this way, it is possible to distribute them on the network and access them via multiple cli-

ents. The installation runs via a wizard and should not pose administrators any issues. Immediately after setup had been completed (for the test we installed all the components on one system), we



The configuration of the web content filter

were able to call up the client and log on to the server with the default access data "admin" and "admin".

Next, we had to add our gateways to the InControl configuration. To do this, we had to generate a key to secure the connection on the individual gateways first of all and release it for management connections via the key ring. Then the IT staff can specify the IP addresses of the gateways in InControl and enter the applicable keys for the individual devices. After that, InControl registers with the NGFs and they appear in the software workspace. It sounds complicated but we worked through these steps quickly and since the whole procedure was described precisely in the documentation, there really shouldn't be any issues here.

Working with InControl

After logging in with the console, the user will find himself at "Home". At this point, the solution displays the "Global domain" first of all. The administrators either add their existing gateways to this as described above, or set up their own domains or HA clusters. We will come back to the clusters later. For performance reasons, Clavister recommends taking the global domain where possible. However, in large environments it can still make sense to create your own domains since the policy management can be based on domain, if necessary.

InControl provides various tabs at the top of the screen, including a ribbon bar containing icons which can be used to call up appropriate functions for each selected context. The solution's workspace is somewhat similar to Microsoft Office, which simplifies the integration into the tool significantly.

The first tab – "File" – is used to export and import data, define the SMTP server for email alerts and similar tasks. The "Home" tab is more interesting, which – as mentioned before – is displayed immediately after you have logged in. This contains the registered security gateways, lists with alarms and licence details and the library browser which gives users access to items such as the traffic summary, the top app usage, the top rule usage, the top talkers and such like. In addition to this, "home" also provides a log explorer (which can run queries), reporting functions (which can be automated with a schedule, if required, it is also possible to send reports by email) and a log analyser, which informs the administrators about application usage, the top talkers, the interface usage and so on. There is also the option here to configure monitoring dashboards which display parameters which are of interest to the relevant staff in the form of gauges, graphics and similar formats. Furthermore, you can manage users who may access InControl either as an administrator or as an auditor and manage groups and audit trails. The latter points include the configuration changes on the gateway and various other actions.

If an IT employee selects a gateway, the icon "Configure" becomes active. This is used to set up the devices. There is a tree structure on the left hand side which contains the gateway in question and the items "system", "objects", "network", "policies" and "update centre". This gives those respon-

sible access to the functionality of the NGFs. Since the functional scope of the solutions has already been presented, we won't go into the details once again. It's enough to say that the tree structure was very clearly designed and that the configuration work with InControl went smoothly. We liked the InControl interface in the test even more than the web interface and we would even recommend that users who only have one Clavister firewall in operation install InControl and carry out the configuration using this software. However, this is certainly a matter of preference.

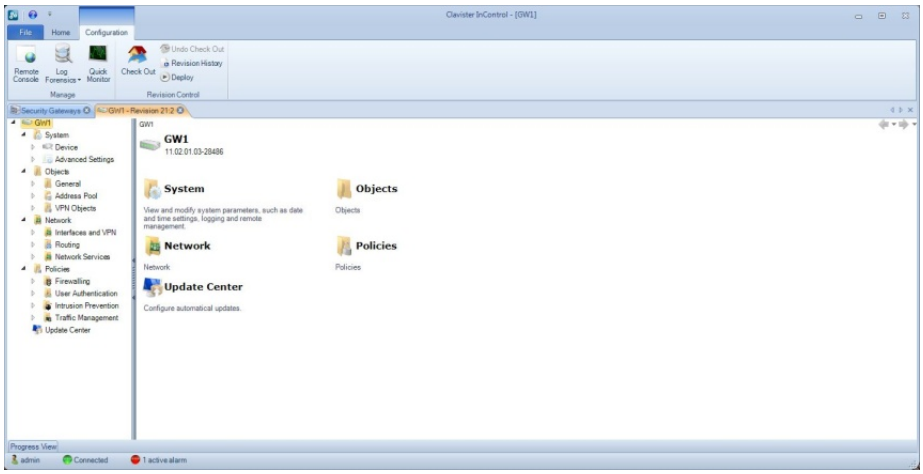
As mentioned above, the configuration can also take place on a domain basis. If an administrator selects a domain instead of a gateway, then they have the option to adapt items, services, NAT pools, profiles and much more to their requirements at domain level. By clicking the right mouse button on a gateway, several other functions are available. These are a remote console, a revision control for configuration, device maintenance functions (with upload firmware, download technical support file, restart, etc.) and such like. In this respect, the "Quick monitor" feature is worth mentioning. This can also be accessed by clicking the right mouse button. This is a predefined monitoring dashboard which provides information on throughput, CPU and buffer usage, the CPU temperature, connections and interface statistics. All of the functions which are accessible via the right mouse button are also available via icons in the ribbon bar.

The "Progress view" shows the current status, for example when distributing configurations. An overview of the accumulated error messages rounds off the scope of InControl.

Security

When we worked through the management tools, we set out to look at the device in detail with various hacking and security solutions in relation to security flaws. While doing this, we always scanned the external and internal interfaces (both had been assigned fixed IP addresses for this purpose). The specific result of this was that Nmap detected the open services for our configuration on the internal interface such as HTTP, SSH and such like, as we would expect. In addition to this, the tool suspected that the device was a D-link device, but also stated straight away that this statement was not reliable. All of the ports on the external interface were filtered, that is why Nmap could not acquire much information. Nevertheless, the scanner established that it was a Clavister solution with the aid of the MAC address. Nessus also detected the released services on the internal interface, even with the version of the server in use, and criticised the certificate installed on the device. That was only logical, since we had left the self-generated original Clavister certificate on the device and therefore this does not represent a security risk. Nessus also stated that it was a Clavister solution. Nessus did not find anything on the external interface.

Just like nmap, Metasploit also thought it was a D-Link device after the scan of the internal interface. The security solution also detected the released services, as expected. It didn't find anything at the external interface either. Not one of our attack tools could cause the Clavister solution any embarrassment, on either the internal or external interface. It was completely unmoved by the attacks and came through the security test unharmed.



The InControl configuration dialogue

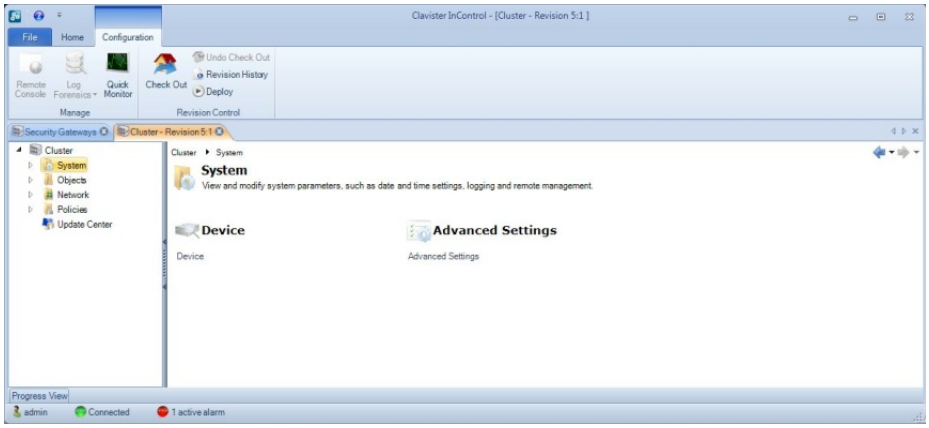
High availability

During the next step, we used InControl to set up a cluster with our two NGFs. To do this, fixed IP addresses were used again on the WAN interfaces.

Firstly, we added our two gateways to the InControl system and configured the later master gateway so that it met our requirements. To do this, we essentially

adopted our old configuration, but we also pointed various IP addresses at the interfaces. In order for the cluster configuration to work, all of the device interfaces must have both a shared IP address as well as a private IP address (in the case of unused interfaces, that can be loopback). Once this was done, it sufficed to define a cluster in InControl, combine two of the gateway interfaces as synchronisation interfaces and then add the master to the cluster first, followed by the slave. As soon as that had taken place, InControl asked for the mode which the cluster should be operated in. There are three different options to choose from in this case. Firstly, "Synced". In this case, the whole configuration of InControl is managed, it is uploaded to the first node and then after a break, it is uploaded to the second node. In this mode, it is no longer possible to manage the cluster simultaneously via the web interface, InControl must be used for management. In "Auto" mode, the tool only uploads the configuration to the first node and the cluster takes on the syncing process. Finally, the third option is called "Manual". In this case, everything is up to the administrator. If you have chosen a mode, we chose the second option in the test (because we wanted to continue to use the web interface at the same time), InControl asks what network interfaces should be used for the synchronisation. After we had answered this question, the tool uploaded the configuration to the first node, synchronisation took place and the cluster went into operation. In the test, there were no difficulties during failover. By the way, according to the manufacturer, failover takes less than 800 milliseconds. As mentioned before, clusters can also be created via the web interface. There is also a wizard for requesting the required parameters.

The "Quick monitor" in operation



Clusters can be managed in the same way as individual gateways while they are in operation

Conclusion

The Clavister W30 made an excellent impression during the test. The solution is equipped with all the safety functions that are required in the business environment. Examples of this high standard are the next-generation firewall, the IPS, the web filter, the application control and the anti-virus and anti-spam features, to name but a few. The central management tool is exemplary, the routing functions have been designed efficiently and with the web interface and CLI, administrators have a comprehensive set of alternative tools at their disposal for managing devices. These can also be used simultaneously, if required. For applications where high availability is required, Clavister also provides functions which are easy to operate and can be used to implement clusters quickly and efficiently. Therefore, the solutions come highly recommended.