

Securepoint Operation Center: Central Management of IT Security Systems



The control center for your security and network systems

- Configuration and administration of all Securepoint UTM/VPN gateways, WiFi/Network Access Controller and Mail Archiving solutions
- Easy integration of systems from different manufacturers into the SOC
- Simple password management
- Central remote-administration and configuration
- Central monitoring/logging/reporting, even according to the „four-eyes-principle“
- Automated, time-scheduled backups and tasks
- Real-time control and risk management with automated warning
- License and inventory administration of all machines and appliances
- Executable as local desktop or central server appliance
- Integrable into your IT backup structure

Securepoint Operation Center (SOC)

The control center for your IT security and networks.

The Securepoint Operation Center (SOC) is a central management solution for all Securepoint solutions such as VPN/UTM systems, the Network Access Controller (NAC) and the Unified Mail Archive (UMA). It also offers the simple integration of solutions from other manufacturers. The immediate available status and the possibility of system control from everywhere, both offer a time-saving and clearly-arranged process for configuration, monitoring, reporting and simple administration of all systems.

SOC adjusts to your demands

The new Securepoint Operation Center (SOC) is an all-round talent and adjusts to your demands. SOC simplifies:

- the overview of all Securepoint and other products.
- the system configuration and the easy system management of UTM and VPN systems, Network Access Controller and the Unified Mail Archive (UMA) of Securepoint.
- the integration of third-party systems, like Intel Server Control[®], by a certain interface. Link easily any kind of third-party system having a web interface to the SOC!
- automated system backups and system updates.
- the real-time control and the monitoring function, the logging, the error search and the reporting according to the „four-eyes-principle“
- the management and encoding of log-data.
- the user access management (authentication, user/password storage).
- central definition of global regulations.
- the license and device management,
- and it allows large VPN or UTM rollouts!

Fast overview of all systems



The dashboard shows a graphical overview of all UTM and VPN gateways. You have the possibility to get the most important monitoring data by the SOC dashboard.

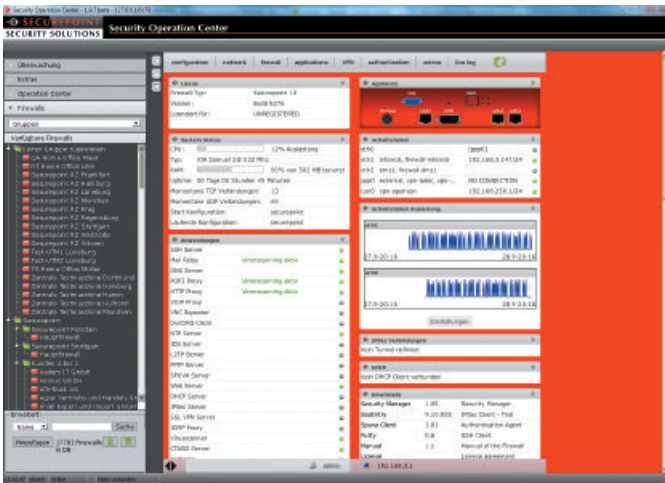
Main dashboard functions:

- The dashboard disposes a box and list view of all UTM and VPN systems.
- The CPU and memory operating grade (load), the Swap removal partition and license life time for every single UTM and VPN gateway will be displayed graphically.
- The amount of the TCP and UDP connections as well as the current Securepoint version will be indicated additionally.
- Searching, filtering, sorting and presentation of systems will be executed by the dashboard in order to receive a fast overview of thousands of systems.
- Multi-Tabbing allows a simultaneous remote connection to various systems.



Have an eye for everything and have it under control!

Central administration, backups and updates



All VPN and UTM systems can be managed by the Securepoint Operation Center. Even widely ramified networks can be managed securely. A clearly arranged illustration of all systems will be available for you. Numerous sorting and filtering functions will help the administrator to keep an overview of even large UTM and VPN infrastructures.

Administration and configuration:

The availability of a central remote configuration of your UTM/VPN gateways is the main function of the SOC.

Automated backup:

The SOC can activate automatically all UTM and VPN systems and realize central backups on time schedule. The backup period is freely adjustable. Backups can easily be restored by the system on the UTM/VPN systems.

Tasks:

You can create tasks and orders for your gateways and users that are supposed to be realized automatically at a certain point of time; such as backups, updates etc.



Tasklog:

You can check whether the generated tasks have been realized adequately and whether errors have aroused and must be corrected.

Groups:

In this menu the gateway groups can be administrated. These groups help to organise a great amount of UTM/VPN gateways that must be managed.

Versions:

Here you receive necessary information of the software versions available. New versions can be downloaded and software updates can be realized.

Protocol:

All processes realized by a user at the SOC will be recorded as well as every action like writing backups and monitoring operation of the system. It is possible to track which action has been executed by which user or system.

UTM/VPN gateways:

All gateways are listed here as a tree. The list contains the name, IP address, type, location and possessor of the particular system. All User and their rights are indicated and editable.

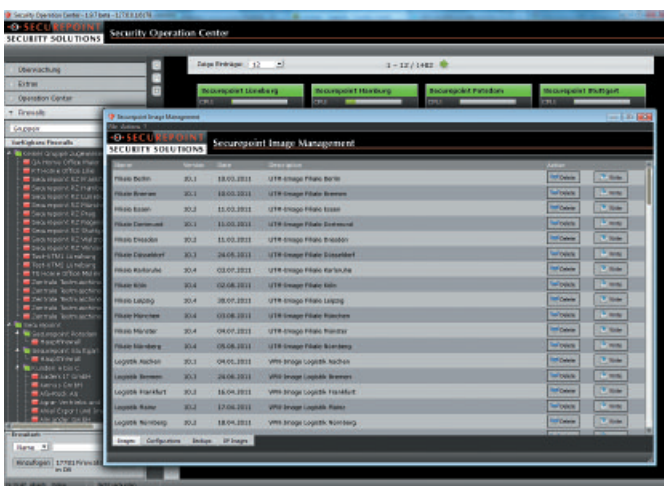
User administration:

You can set all users and categorize them into user-groups in the SOC. It is also possible to appoint restricted user rights and administrator rights.

Securepoint Operation Center (SOC)

The control center for your IT security and networks.

Automated setting of firmware images

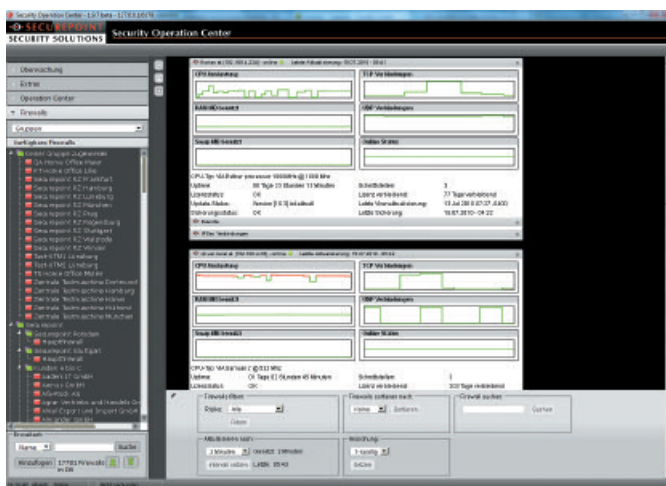


The firmware image management of the SOC provides a system for the setting/administration of installation images. It is possible to generate new configuration with the help of an automated assistant.

Central guided rollouts for big infrastructures:

Installation images can be generated by new configurations or existing backups. Both, the basic installation images and the generated installation images, will be managed centrally in the SOC. New basic images can be reloaded from the Securepoint website in order to create specific installation images for a lot of gateways. They can be stored e. g. on a USB stick. Every gateway can boot directly from this stick and will run with the designated configuration. This is an important function if gateways are installed by technically unversed staff or if external employees are not allowed to get access to those gateways. Fast and uncomplicated UTM-rollouts can be realized.

Central monitoring, logging and reporting



The SOC offers a wide variety of central auditing, monitoring, logging and reporting functions. You can have an eye on everything – any time.

Four-Eyes-Principle:

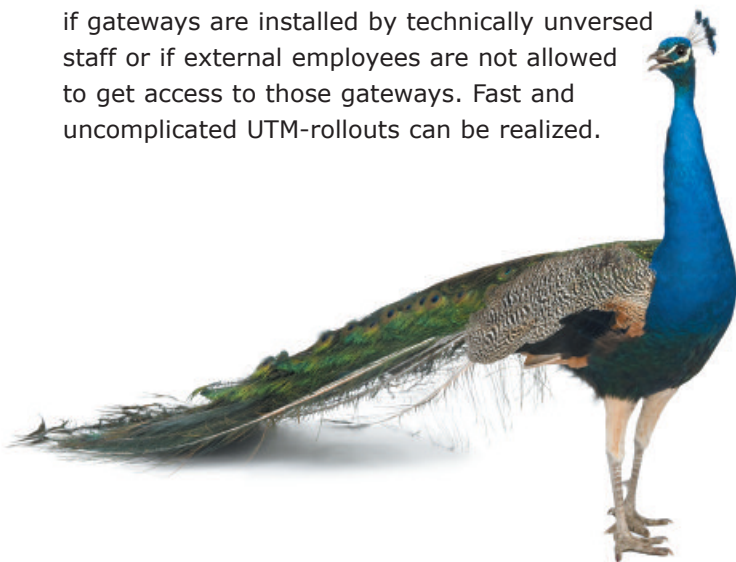
The SOC supports the „four-eyes-principle“ for logs and reports. It means that important decisions cannot be taken or risky actions cannot be realized by a single person. It is to reduce the risk of errors and abuse and to make it verifiably in case of relevant operations as required by employment law. Log-data can be anonymised and are encrypted.

Monitoring:

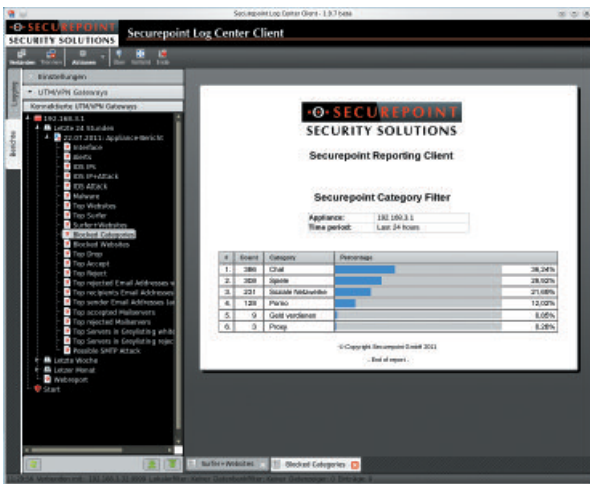
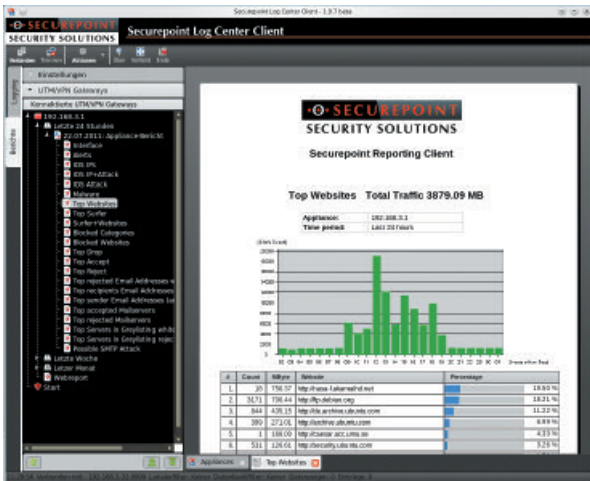
Via monitoring all administrators can get a general idea of the status and the processor load of all UTM/VPN systems. Various escalation levels provide the system administrators with information that is needed in order to take precise action on critical situations.

Auditing:

All procedures within the Securepoint Operation Center will be logged and can be verified. Traceability and complete control can be taken for granted any time.



SOC is your visual acuity:



Reports:

For analyzing the protocol data specifically, the implemented SOC filters are helpful tools in order to create a large variety of reports. The following reports can be generated by the SOC LogClient graphically and in tabularly form:

- Interface-Load: sent/received traffic
- Alerts: activated alarms
- IDS IPs Intrusion Detection system attacks
- IDS IP+attack: attackers IP and ways of attacking
- IDS attack: tabular of the detected attacks
- Malware: name, type and amount of malware
- Top websites: traffic of the websites visits
- Top surfer: all users, who cause traffic
- Webreport: traffic analysis for every user
- Surfer+Websites: visited websites according to user
- Blocked categories: blocked websites categories
- Blocked websites
- Top drop: declined packets
- Top accept: accepted packets
- Top Reject: rejected packets
- Top rejected email: rejected emails
- Top recipients email: received emails
- Top sender email: received/rejected emails
- Top accepted mail servers
- Top rejected mail servers
- Top server in grey-listing white-listed
- Top server in grey-listing rejected
- Possible SMTP attack: server IPs on SMTP attacks

Logging:

The SOC LogCenter records Syslog protocol data of the gateways and archives them in scheduled intervals. Real-time analysis can be realized by LiveLog. Archived data can be preserved in an eligible period of time and will be deleted afterwards. On demand the LogCenter sends daily report-, alarm- and incidence-emails regarding self-defined incidences.

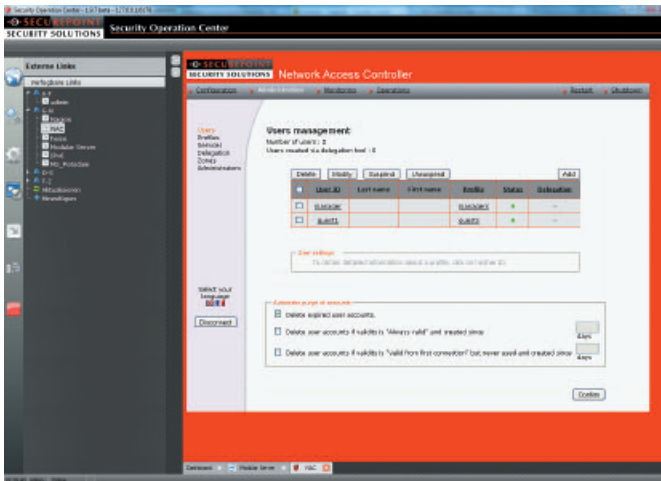
Reporting:

The SOC LogClient creates reports for every registered gateway by the protocol data. The reports can be illustrated graphically, tabularly or in a mixed way. Data of the previous 24 hours, week, month or year can be displayed.

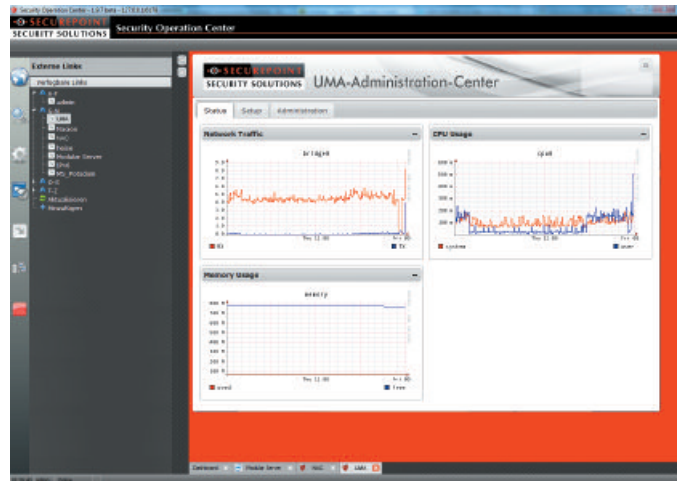
Securepoint Operation Center (SOC)

The control center for your IT security and networks.

Management of Network Access Controller



Management of Unified Mail Archive



The new Securepoint WiFi and Network Access Controller (NAC) can easily and comfortably administrated by the SOC. The NAC allows employees/guests to dial in to conference und training rooms, offices and public locations (such as hotels, clinics, governments, internet-cafes, restaurants etc.) via WiFi or LAN (free of configuration) and to get easy and secure access to internet, data-, voice- and video applications. The billing of guest-accounts is also possible and traceability and control is guaranteed at any time. Of course, any type of PC, notebook, mobile phones, iPhones and iPads are supported.

Internet access without any configuration:

All network accesses are available without the need for any configuration and hotel/clinic staff is able to provide clients, guests and employees with these services without any specific technical background knowledge. A simple instruction of the NAC system is sufficient and complies with all regulatory requirements (like protection against copyright infringement, provider responsibility etc.).

It is also possible to administrate the Securepoint Unified Mail Archive (UMA) by the SOC.

Functions of the Unified Mail Archive:

- Unloading of mail servers like MS Exchange etc.
- Legally compliant, audit compliant, automated archiving of the complete email traffic according to the German authority standard with Governikus LZA
- Preservative long-term storage according to the technical guideline 03125 due to BSI (TR-ESOR) and to DIN – in evaluation according to Protection Profile Archi-Safe and TR certification (Governikus LZA)
- Applicable with MS Exchange and other mail server
- Direct access via web interface, Microsoft Outlook® and other email clients (for example Thunderbird, AppIE-Mail etc.)
- Full text indicated search for emails
- Simple recovery of accidentally or intentionally deleted emails
- „Supervisor mode“ according to the “four-eyes-principle“ for auditors in order to comply with the legally required data protection
- Connection to Active Directory or LDAP services
- Automated, internal time stamp



SOC is available as desktop or server system!

Simple linking of third-party systems



The Securepoint Operation Center (SOC) is a multi talented and allows you to link and to administrate a variety of different third-party systems; even from various manufacturers such as:

- Securepoint and TERRA UTM solutions
- Securepoint and TERRA VPN solutions
- Securepoint Network Access Controller (NAC) for WiFi management
- Securepoint Unified Mail Archive (UMA) solutions for audit compliant email archiving

Link Center:

The following third-party products can be linked by the Link center:

- Intel Server Control® solutions are directly supported by the SOC.
- As well as any other solution from various manufacturers possessing a web interface.
- RDP and VNC links can be included as well into the Link Center.

SOC is available as desktop and server application



The Securepoint Operation Center can be configured and operated as a local desktop or as a client/server application. It can be installed on a server wherefrom all services are centrally available. Lots of SOC clients can get access to the central SOC server in order to administrate UTM and VPN systems or third-party servers or applications. It can be integrated into a central back-up concept including a save and encrypted access. The SOC is particularly suited for managed services, provider and data processing center implying a high level of safety.



Securepoint Operation Center (SOC)

Overview: advantages of SOC



- Save time on configuration, maintenance and update by the central management.
- Reduce your daily workload by SOC organization and arrange responsibilities.
- Assign installations/configurations to users and groups they should be responsible for.
- Realize tasks like updates etc. centrally and schedule recurring tasks at fixed points of time.
- Avoid a complex password administration and get a fast and easy access to all Securepoint gateways and third-party systems.
- Keep always track about what is happening in your network. Monitor all data like licenses, threats, versions and loads in real-time by the intelligent dashboard.
- React faster to threats and be always up-to-date.
- Monitor detailed statistics for performance, network activities, web use and traffic for single or various locations.
- Take care for security by automated backups and tasks.
- Save administration costs that incur automatically with a variety of systems!
- AND: SOC is free of charge!

Systemhaus/Partner:



SECUREPOINT
SECURITY SOLUTIONS

Securepoint GmbH
Salzstrasse 1
21335 Lueneburg
Germany

phone: ++49 41 31 / 24 01-0
fax: ++49 41 31 / 24 01-50

mail: info@securepoint.de
web: www.securepoint.cc