

### Comprehensive security shield

Mission Control Application Gateway, Mission Control Firewall, **Mission Control Internet Proxy**, Mission Control Security Gateway, Mission Control Passport, Mission Control Intrusion Detection, Mission Control Email Shield, Mission Control Virus Protection, Mission Control Client VPN, Mission Control Wireless Zone Protector



## Mission Control Internet Proxy Datasheet Description

The Mission Control Internet Proxy terminates the client's web connections and reopens new ones according to the company's security policy. Depending on the modules that are activated, it protects the clients from malware and restricts the URL categories where they are allowed to connect to.

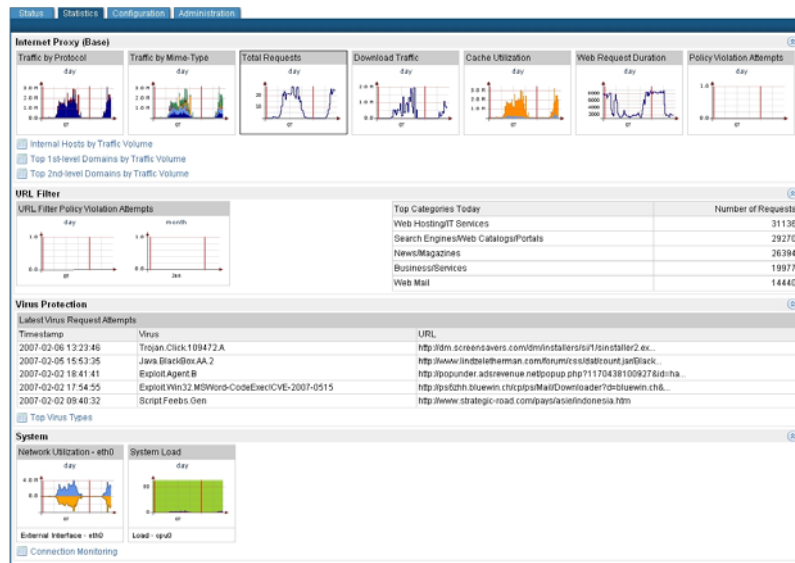
It is running on dedicated **industrial strength hardware** for reliable 7x24h operation. The **hardened operating system** assures that only essential tools and utilities are activated and therefore cannot lead to unexpected instability and compromised systems. Mission Control Security Engineers further ensure that all appropriate security related settings are up to date and configured correctly.

The Mission Control Internet Proxy provides a proxy for **SSL, HTTP and FTP over HTTP**. The FTP protocol is translated to HTTP on the client side. SSL connections are checked against the security policy and **tunneled** through if granted. The company wide distribution of the proxy configuration is supported with **Proxy Auto Configuration (PAC)**. It allocates a configuration file on the proxy that is fetched from the clients for dynamic configuration.

**Blacklist** entries based on IP addresses, domains, domain names or hostnames can be customized on the Mission Control Internet Proxy. The limited number of entries can be enhanced with the module URL Filter, extending this feature with category based and customizable black-, and whitelists.

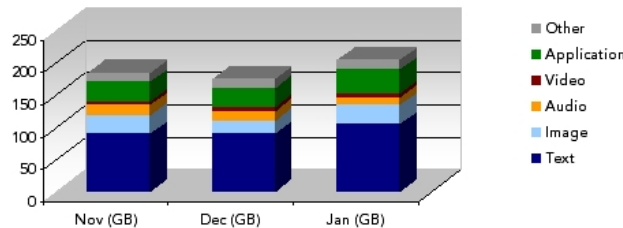
**Group and port access policies** assign access rules to groups of network resources like IP addresses and ports and are granularly definable.

The following figure shows the **real time** visibility of **essential operational key figures and statistics** that is provided by the Mission Control Cockpit. All statistics are processed by the time viewing. A single click on one summarizing graph expands the detailed view with peak values and scales for the last 24 hours, last week, last month and last year. It shows details about **traffic by protocol, mime type, internal hosts**, 1st respectively 2nd level **domains, web request durations** and the policy **violation attempts**. Detailed spam and malware statistics are displayed as well if the corresponding modules are subscribed. Graphs of the **network usage** and the **system load** are provided for the machines underlying the Mission Control Internet Proxy.



Monthly **browser compliance and traffic volume reports**, tailored to **executive management** audience, provide excellent overview of the company's browser distribution and web traffic. The figures are benchmarked to the overall performance of all Mission Control Internet Proxy services worldwide. The reports are downloadable in Excel format, giving full reusability to the statistical data.

### Traffic Volumes



Content Type	Nov (GB)	Dec (GB)	Jan (GB)	Change	Jan (%)	Benchmark*
Text	90	90	105	+17%	51%	30%
Image	29	20	29	+45%	14%	22%
Audio	15	15	12	-20%	6%	6%
Video	6	6	6	+0%	3%	6%
Application	30	30	38	+27%	19%	29%
Other	14	14	14	+0%	7%	8%
<b>Total</b>	<b>184</b>	<b>175</b>	<b>204</b>	<b>+17%</b>		

### Browser Distribution



**Conformity Degree\*\*** **Benchmark\***  
35% **66%**

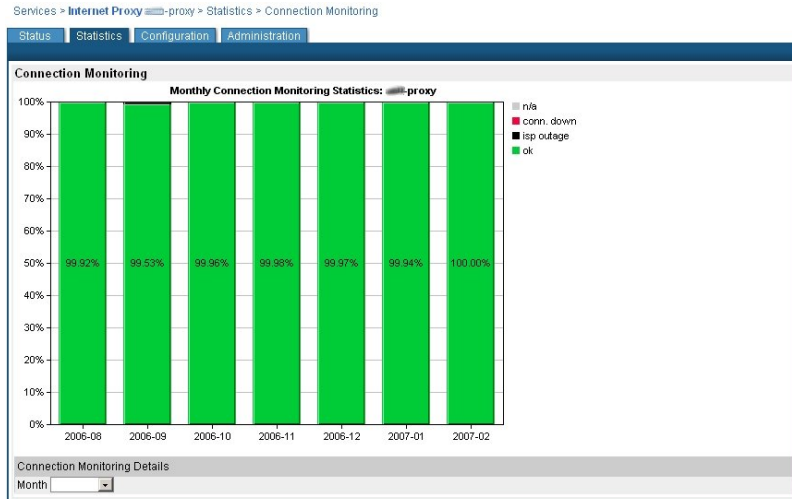
\*\*The Conformity Degree describes how homogeneous your corporate browser patch levels are. Increase your companies security and risk auditability by optimizing browser conformity.

**Hierarchical proxy cascading** allows forwarding all requests to another proxy server. It is used to direct all requests to a global proxy or to separate a sub network with a web proxy.

Streaming applications like RealOne, Quicktime, Windows Media Player, etc. are candidates to flood the whole bandwidth and cut the performance of business applications. The Mission Control Internet Proxy can **manage the bandwidth of**

**streaming applications** and limit their bandwidth usage as soon as it is needed by business applications. Additional and customizable groups of traffic with managed bandwidth are available with the module Quality of Service.

The following two figures show the **graphical and statistical connection monitoring**. The graphical overview shows the availability per month, colored in uptime, ISP outage and connection down. Clicking on one pillar opens the details as shown in the second figure. It lists every **ISP outage or lost connection** and the corresponding ticket if the threshold was reached and **escalated to Mission Control**.



After extensive testing procedures, all required security updates and patches are automatically installed, ensuring that all systems operated by Mission Control are always up-to-date. **Dual partition boot configuration** is implemented on every component, which provides an efficient recovery process if required. Further more, all device and environment specific configurations are **automatically generated**, based on the Mission Control operated **configuration database**. This is an essential part for an **efficient disaster recovery processes** since it enables to generate and reinstalled the identical configuration in a very short time.

## Module description

### High Availability

The High Availability module increases the availability of the Mission Control Internet Proxy with additional hardware for load balancing or redundancy reasons. **Load balancing** is performed on the **client side**, whereby the proxy PAC file defines how web browsers choose a proxy. The decision can be based on a hash function of the URL. The **redundancy** configuration sets the additional hardware into hot standby mode and takes over as soon as the master device is no more available.

If the Mission Control Internet Proxy is running on more than one machine, **reporting, access policies and administrative actions** are extended to all enforcement points, giving a lucid **cluster presentation** to the customer.

## URL Filter

The URL Filter **enforces the company's Internet access policy** and protects against risks associated with the employee's Internet use. It reduces legal liability, enhances Web security, increases productivity and preserves bandwidth for business-related activities.

The URL Filter does **category based content filtering** with both **predefined and customizable** categories. All rules are further customizable with **time based** conditions. The predefined categories are managed and monitored, which provides a comprehensive and proven source of millions of global URLs that are organized into over 100 categories.

**Real-time URL violation attempt reports** display the number of requests that were rejected by the URL Filter.



An extract of the **monthly executive management** report is shown in the following figure. It summarizes the total **number of violation attempts** and the top five categories. The total number of connection requests and denied attempts are broken down per category, giving a clear overview of the **composition of the company's internet traffic**.



## Malware Protection

The module performs **proactive malware protection** with **protocol scanning technologies for HTTP and FTP**. It uses a combination of several proactive filters to detect both unknown and known malware.

Malware Protection further provides additional proxy functionality with an **FTP proxy** by doing FTP to FTP conversion. This enables FTP access for **native FTP clients**. SSL connections are checked against the security policy and if granted, tunneled through.

**Real-time virus protection reports** are available online on the Mission Control Cockpit.



Count	Virus Name	Last Occurrence
23	Exploit.Agent.B	Tue Feb 13 00:14:44 2007
8	Exploit.Win32.MSWord-CodeExec[CVE-2007-0...	Wed Feb 14 23:31:50 2007
7	TrojPsyme-DL	Mon Dec 11 15:49:58 2006
4	TrojDloadr-ACN	Mon Dec 11 15:50:00 2006
4	EICAR-AV-Test	Sat Jan 13 14:36:42 2007
4	TrojFemad-E	Mon Dec 11 15:50:00 2006
4	Trojan.Zlob.Gen	Tue Feb 13 01:41:26 2007
4	TrojDownLdr-NO	Mon Dec 11 15:49:58 2006
4	Script.Feebs.Gen	Thu Feb 8 17:42:57 2007
4	EICAR-test-file	Sat Jan 13 19:37:09 2007

**Executive Management Reports** are automatically delivered on a monthly basis, summarizing the logs of all Malware Protection modules operated by Mission Control. They provide an excellent overview of the **top and last viruses** including the change from the last month.



### Executive Management Report January 2007

Mission Control Internet Proxy: Virus Protection

#### Top 5 Viruses

Virus Name	Jan Change	Benchmark*
<a href="#">Exploit.Agent.B</a>	36% -	39%
<a href="#">Exploit.Win32.MS05-002.gen</a>	12% -	2%
<a href="#">Exploit.VML.D</a>	9% -	1%
<a href="#">EICAR-test-file</a>	7% -	9%
Other	37% -63%	50%

#### Last 30 Viruses

Virus	Source	Date	Time
Trojan.Spy.Banker.vk.1	http://snk-seiya.net/guiasaintseiya/banner-demos.jpg	01/31/2007	14:22:00
Script.Dldr.Inor.a.3	http://www.teenpalacetgp.info/index.shtml	01/31/2007	12:51:00

## SSL Scanning

SSL Scanning is an amendment to the modules URL Filter and Malware Protection and **applies the existing security and internet usage policy** to the **HTTPS protocol**. It prevents any viruses, spyware, trojans and URL filtering enforcement to be bypassed by using the HTTPS tunnel, a very common and unprotected open hole in the perimeter.

It allows **validating server certificates** and defining **customized actions** to be taken for not fully trusted certificates. Depending on the policy, those certificates can be allowed, blocked or the decision can be passed on to the users.

All connections with **client certificates** involved are **tunneled** through without scanning.

## Passport Authentication

Passport Authentication restricts the user's access to the internet according to the authentication to the Mission Control Passport Server. All features including password authentication and **strong token authentication** are available, leading to security and accountability.

## External Authentication

The External Authentication module performs **Microsoft Integrated Authentication**. It is also known as Active Directory (AD) authentication and allows **Single Sign On (SSO) capability with an Active Directory**. The Active Directory of the company's infrastructure is used to adapt the global policy with transparency to the user.



---

## QoS / Traffic Shaping

---

Quality of Service (QoS) / Traffic Shaping classifies the internet traffic into groups and **controls their bandwidth usage**. The base system of the Mission Control Internet Proxy does already QoS / Traffic Shaping for steaming applications like RealOne, Quicktime, and Windows Media Player etc. This module extends this feature with additional customized traffic groups.

Two different techniques are available on the Mission Control Internet Proxy. QoS / Traffic Shaping by **guaranteed throughput** both limits and guarantees throughput up to a customizable rate. The groups can be defined based on IP addresses, protocols, ports, times, URL's and browser names.

QoS / Traffic Shaping by **flexible queue allocation** gives also a guarantee on the bandwidth but does no limiting if more throughput is required. It optimizes the overall bandwidth by limiting only if other bandwidth guarantees could no be met. In contrast to the guaranteed throughput, the group definitions are less flexible and can solely be based on IP addresses, protocols and ports.

This module is commonly used to provide fair access to network resources among departments or to guarantee network bandwidth for business applications.

---

## Additional Processing Capacity

---

The module Additional Processing Capacity increases the number of concurrent **HTTP/HTTPS and FTP** sessions that are handled per second. The effective throughput enhancement depends on the consisting setup and is calculated on demand.

---

## Electronic Log Files Distribution

---

The log of the proxy can be obtained directly from the Mission Control Internet Proxy at the site. It contains details about the requests that were sent including the requested URL, the proxy's decision based on all filters and the type of the browser. It can be retrieved through **SSH or FTP** file transfers in customizable and **periodic** time intervals. **Syslog forwarding** continuously forwards the syslog entries as soon as they are available on the proxy.