

SecureGUARD

Security Appliances for a wide field of application

ISP-Redundancy
NAP-Support
URL-Filtering
SSTP (VPN over HTTPS)
One-Time-Password
SIP-Support
Network Inspection System
DirectAccess
Multi-Engine AV
Central Management
Fast Recovery



art of defence

IKARUS
security software

PointSharp



Microsoft
Forefront™
Threat Management Gateway 2010

Comprehensive threat management,
secure Internet access, and secure
remote access.



Microsoft
Forefront™
Unified Access Gateway 2010

Easy and secure remote access solution
with a focus on application intelligence and
granular access control.

SecureGUARD Operating System

The SecureGUARD operating system is supplied with every appliance. It provides all functions necessary for the administration of the appliance.

- **Intelligent deployment**
The Appliance Management allows the SecureGUARD appliance to be taken into operation quickly and initial configuration to be carried out rapidly.
- **Intelligent management**
Administration of the SecureGUARD appliance can be carried out completely via the Appliance Management without using a console.
- **Intelligent disaster recovery**
The disaster recovery tool integrated into the SecureGUARD Operating System (OS) makes it possible to return the device to the original delivery status with just one click.
- **Support**
Rapid assistance and comprehensive support from the experienced and competent support team are other trademarks of SecureGUARD GmbH.

SecureGUARD is synonymous with long years of experience in the development and production of security appliances designed with the requirements of practical use in mind. Combined with Microsoft Forefront TMG 2010 or UAG 2010 the appliances provide practical user-friendly security solutions designed to protect company networks.

SecureGUARD Appliances ...

Hardware, software and support all from one supplier

SecureGUARD appliances combine high-performance hardware with tried-and-tested security solutions and comprehensive support to form a ready-to-use all-in solution for ensuring perimeter security and allowing web caching, the connection of branch offices or the protection of server farms.

Ideal protection for all applications

The modular structure of the SecureGUARD appliances ensures flexible adjustment to meet the specific requirements of your company – from compact, low-noise models for medium-sized companies to complex enterprise solutions with maximum performance.

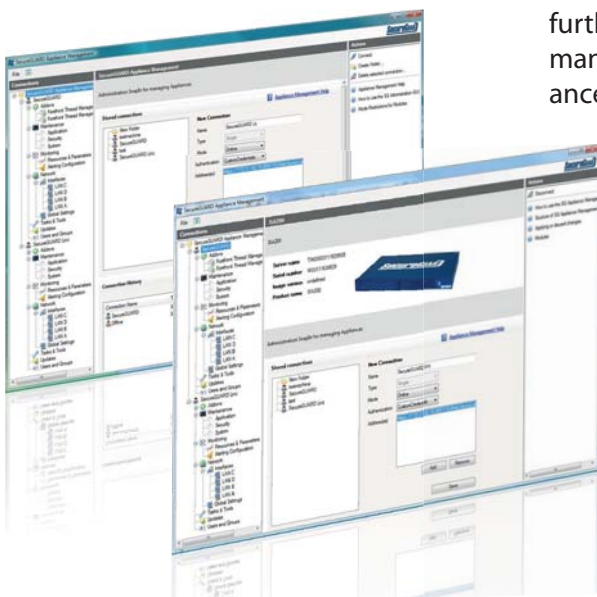
Easy operation and administration

The SecureGUARD Appliance Management supports the taking into operation of the SecureGUARD TMG and UAG appliances and allows rapid initial configuration as well as simple further operation. There is a uniform management interface for all appliances, regardless of whether they are TMG or UAG appliances. The preinstalled thirdparty applications can also be activated quickly and conveniently via the appliance management interface.



Optimum performance and personal support

The high density of Ethernet ports and the sophisticated hardware allow SecureGUARD appliances to map complex networks with countless subnetworks and DMZs with no loss of performance. Other characteristics of the SecureGUARD solution are the rapid assistance and comprehensive support provided by our competent, experienced support team.



New features in comparison

The always changing and expanding requirements in information technology regard-ing security and mobility demand fast and continous advancements and extensions in security gateway products.

The following two tables display an overview of new features imlemented in the Microsoft Forefront Threat Management Gateway 2010 and the Mirrosoft Forefront Unified Access Gateway 2010 in comparison with their predecessors.

	ISA 2006	TMG 2010
Network and Application Firewall	✓	✓
Internet Access Protection (Proxy)	✓	✓
Basic OWA & SharePoint Publishing	✓	✓
VPN Endpoint (remote & site-to-site)	✓	✓
Windows Server 2008, native 64-Bit	✗	✓ new
Secure Web-Proxy (AV, Url-Filter)	with 3 rd Party	✓ new *)
HTTPS-Inspection (Forward Proxy)	with 3 rd Party	✓ new
SIP Filter, ISP Failover / LB, E-NAT	✗	✓ new
SSTP, NAP, Intrusion Prevention (NIS)	✗	✓ new
Static one-to-one NAT Support	✗	✓ new **)

*) Client Access License (CAL) required; 3rd Party implementation possible.

***) with the integrated SecureGUARD NAT filter.

	IAG 2007	UAG 2010
Application Intelligence and Publishing	✓	✓
End Point Security	✓	✓
SSL Tunneling	✓	✓
Information Leakage Prevention	✓	✓
NAP Integration, Terminal Service Integration	✗	✓ new
Array Management	✗	✓ new
Enhanced Management and Monitoring	✗	✓ new
Enhanced Mobile Solutions	✗	✓ new
Direct Access and SSTP Integration	✗	✓ new

IKARUS

To further secure the webtraffic IKARUS security.proxy is preinstalled on the gate-way. It provides a security instance for url-filtering and antivirus.

This software packet includes an annual licece for 5 users and therefore ensures web security out of the box.



Art of Defence

Hyperguard is a pure software distributed Web application firewall.

It enables centralised security monitoring, reporting and alerting and provides custom protection for your Web applications against known and unknown attacks at the application layer.



PointSharp

PointSharp ID is an identification server that uses hardware tokens as well as mobile- or smartphones for authentication.

Secure ActiveSync from PointSharp makes it easy to deploy and maintain a Microsoft ActiveSync solution while still being secure.

PointSharp ID and Secure ActiveSync are both preinstalled and include an annual 10 user licence.



SecureGUARD UAG Appliance

SecureGUARD UAG appliance is a highly integrated, multifunctional security platform and offers a reasonably priced, ready-to-use all-in solution with a comprehensive firewall function on network level, IPsec, SSTP, SSL-VPN Fähigkeiten, DirectAccess, robust application optimization and an integrated disaster recovery system for optimum availability.

SecureGUARD provides various different hardware appliances which allow your individual performance requirements to be met in an optimum way. The hardware ranges from the starter model to a high-end solution with a total of 8 CPU cores in one single appliance.

Unified Access Gateway 2010

- **Safeguarding of Content**
Differentiated and policy-controlled access to company data, content checking and filtering as well as management of endpoint security
- **Secure Remote Access**
Access for employees, partners and customers – practically regardless of device and location
- **Direct Access**
UAG 2010 provides the possibility to implement Direct Access (Always-on-VPN) in a fast and highly scalable manner.
- **Internet Access Protection**
More effective protection of the IT infrastructure against dangers coming from the Internet

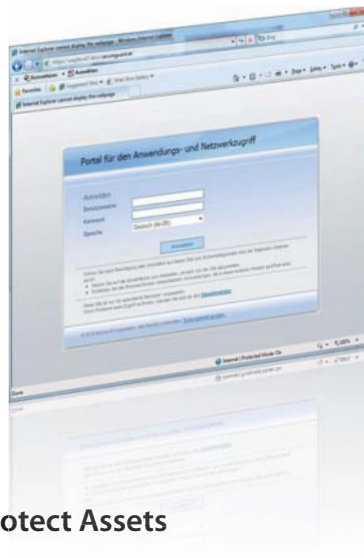
Microsoft Forefront Unified Access Gateway 2010

... bring the good guys in

Thanks to the integration of TMG 2010 and UAG 2010, SecureGUARD offers an appliance which provides secure remote access, security for branches and Internet access protection. The SecureGUARD Appliance Management supports the taking into operation of the SecureGUARD UAG 2010 appliances and allows speedy initial configuration as well as simple further operation of the appliances. The pre-installed third-party applications can also be activated rapidly and conveniently via the management interface.

Control Access

Secure, browser-based access to company applications and data from locations and terminal equipment without the necessity of installing and providing a client.



Protect Assets

The integrated application protection safeguards the integrity of the network and application infrastructure by blocking harmful data traffic and defending the network against attacks.

Safeguard Information

The consistent policy enforcement helps to comply with legal and company access regulations with regard to information use. This limits the risks run during access to sensitive company data.



Comprehensive Secure Access

The Unified Access Gateway (UAG) with application optimizer modules provides an SSL-VPN, a Web application firewall as well as functions for the management of endpoint security, thus allowing access control, authorization and content checking for a large number of line-of-business applications.

Combined, these technologies offer mobile and remote users simple and flexible access from a wide variety of places and devices such as kiosks, PCs and mobile devices. In addition, the UAG allows administrators to enforce compliance with directives on the use of applications and information with the help of a special remote access policy which depends on the terminal equipment, the user, the application and other company criteria.

Microsoft Forefront Threat Management Gateway 2010

... keep the bad guys out

The Microsoft Forefront Threat Management Gateway 2010 (TMG 2010) includes firewall functions with a stateful inspection package filter and an application layer firewall, VPN gateway functions and web proxy. It is an especially interesting proposition for use in homogenous Microsoft environments with central authentication.

TMG is integrated into a back-end application infrastructure such as Exchange Server and Windows SharePoint Services and thus offers a secure mechanism for authentication and access.



Tools such as wizards for the automatic publication of server resources, form-based pre-authentication, adjustable security settings for Exchange and Windows SharePoint Services as well as many other improvements make the Threat Management Gateway stand out in comparison with other security platforms.

Exactly where in my environment should the TMG 2010 be used?

Threat Management Gateway 2010 combines the strengths of a firewall on the application level with VPN, proxy and caching functions.

This solution can be used for the following purposes:

- As a branch office gateway to provide connectivity and security.
- To protect the publication of an application in order to safeguard the remote access of users to company resources
- As web access protection against threats from the Internet and ingenious attacks (AV, URL-Filtering).

The SecureGUARD TMG 2010 appliance is a convincing proposition as a result of a new optimized, inexpensive design which helps to reduce operating costs and makes it unnecessary to install several devices from various suppliers. The central IT department can now introduce a consolidated security appliance solution which is flexible and easy to implement.

Who profits most from the SecureGUARD TMG 2010 appliances?

Companies inundated by ingenious targeted attacks on their networks profit most from them. Companies from a wide range of sectors such as financial services, resellers or authorities and administrations can draw great benefits from the deployment of TMG appliances as protection for Internet clients and as a way of making internal resources available to remote employees.

TMG software editions

SecureGUARD TMG appliances are available in the following versions for the various different types of application.

All editions have the same basic functions – the various versions only differ in their clustering ability and their central management.

Workgroup Edition

This is intended for small and medium-sized companies with mainly one location which require a simple and functional management system. Following the all-in-one concept, it is often expanded by adding other 3rd-party applications. The Workgroup-25 users edition is available from the TMG200 onwards.

BranchOffice Edition

This is used to connect several branch offices to one centre (Enterprise Edition) while taking advantage of the benefits of a central management system. The Branch Office edition is the „special version“ of the Enterprise Edition for the branch offices. It is managed by the central Enterprise Edition. Each version of the SecureGUARD appliances can be delivered with the BranchOffice Edition.

Enterprise Edition

This is designed for use in large organizations requiring flexible distribution options and a high degree of availability and ease of administration. This version is characterized by its central management and its clustering capabilities. We recommend the Enterprise Edition in conjunction with the SecureGUARD appliances from model TMG1000 onwards.

SecureGUARD TMG200

The TMG200 is the ideal solution for small office environments because of its compact dimensions.

Standard specification:

CPU: Intel Dual Core 64-bit
Memory: 2048 MB
Hard Disk: 1x SATA 24x7
Ethernet: 4x 10/100/1000 NIC

Optional upgrades:

Remote Management (shared NIC)
Factory RAM Upgrade up to max. 4 GB (TMG-WG)



SecureGUARD TMG1000, UAG1000

These appliances combine maximum performance with minimum height. Thanks to the power provided by the 4 CPU cores, it can also be used by a large number of users simultaneously.

Standard specification:

CPU: Intel QuadCore XEON
Memory: mind. 4096 MB
Hard Disk: 2x SATA2 RAID1 (no Hotswap)
Ethernet: 4x 10/100/1000 NIC
Formfactor: 19", 1HE
Features: Remote Management

Optional upgrades:

Factory RAM upgrade up to max. 16 GB
Factory NIC upgrade up to max. 10 Interfaces



SecureGUARD TMG1100, UAG1100

The integrated LCD allows easy basic configuration and rapid rollout of the appliance without the necessity of connecting a monitor or keyboard.

Standard specification:

CPU: Intel QuadCore XEON
Memory: mind. 4096 MB
Hard Disk: 2x SATA2 HW RAID1
Ethernet: 4x 10/100/1000 NIC
Formfactor: 19", 1HE
Features: Remote Management

Optional upgrades:

Factory RAM upgrade up to max. 16 GB
Factory NIC upgrade up to max. 10 Interfaces
Redundant Power Supply



SecureGUARD TMG1600, TMG1650, UAG1600, UAG1650

These models belong to the most powerful and high-performance appliances on the market. The TMG1650 with 12 CPU cores meets the highest demands of the security field.

Standard specification 1600:

CPU: 2x Intel QuadCore XEON
Memory: 8-16 GB
Hard Disk: 2x SATA2 battery buffered HW RAID1
Ethernet: 4-10x 10/100/1000 NIC
Formfactor: 19", 1HE
Features: Remote Management,
Redundant Power Supply (optional)

Standard specification 1650:

CPU: 2x Intel SixCore XEON Xtreme
Memory: 16 GB
Hard Disk: 2x SAS battery buffered HW RAID1
Ethernet: 4-10x 10/100/1000 NIC
Formfactor: 19", 1HE
Features: Remote Management,
Redundant Power Supply



SecureGUARD Blade Edition

The Blade Edition combines the power of 12 TMG1000 appliances (48 cpu cores) in one machine and with the 3+1 redundant power supplies it achieves a very high degree of reliability. Whether cloud-computing security, highest performance for classic security systems or multilevel firewall concepts: SecureGUARD is the right choice to deliver outstanding performance.

Appearance and content of the interface are adjustable. Special images can be created for projects; this also includes 3rd-party applications.



Errors and errata excepted! As at 10/2010, product figures can deviate from the actual product!



Salesinfo:
office@secureguard.at
www.secureguard.at
Infohotline:
+43 (0) 732 60 14 40



Salesinfo:
sales@secureguard.de
www.secureguard.de
Infohotline:
+49 (0) 89 570 880 25

Microsoft
GOLD CERTIFIED
Partner

SecureGUARD

All available products at
www.secureguard.at

Copyright (c) SecureGUARD GmbH 2010
SecureGUARD is a registered trademark of SecureGUARD GmbH.
All other trademarks and registered trademarks are the property of their respective companies.