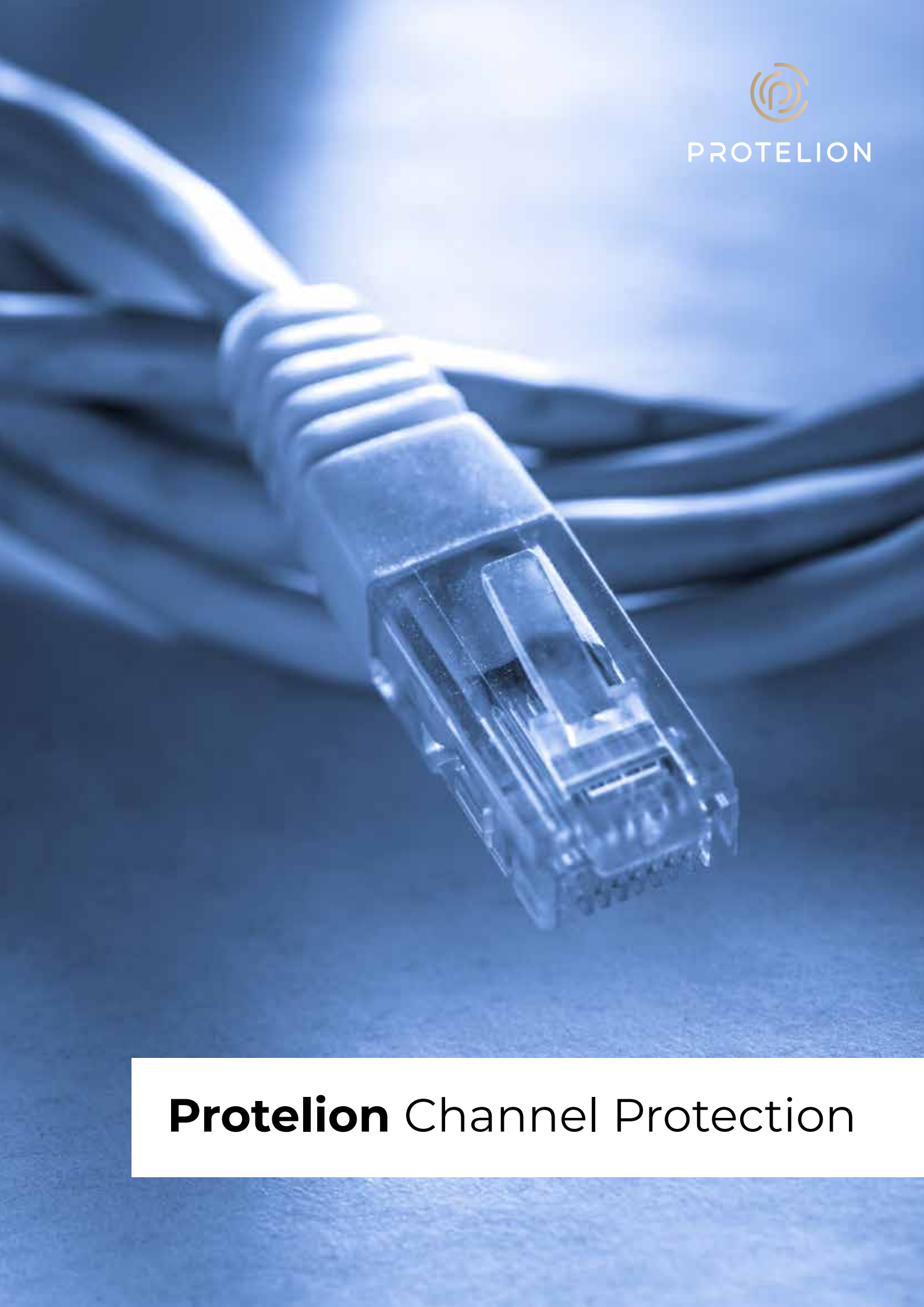


Protelion Channel Protection

Protelion Channel Protection is a product line designed to meet data security challenges in communications over public networks and dedicated data exchange channels.

Protelion Channel Protection products help you create a secure environment for restricted data exchange over public networks and dedicated communication channels as follows:

- By deploying a virtual private network (VPN), which supports centralized management, establishing systems for centralized control, audit and monitoring of the data protection tools in the distributed networks
- By establishing secure encrypted channels

Protelion Security Technology Advantages

Developed in accordance with world recognized standards such as FIPS 140-2 and Common Criteria, Protelion Channel Protection products allow you to establish secure scenarious (site-to-site, client-to-site, client-to-client) and topology (peer-to-peer, hub and spoke, full mesh) regardless of the physical type of the communication channel, physical network topologies, and the connection type (fixed broadband or mobile).

Protelion Security Technology advantages allow you to integrate information security tools into corporate networks of any topology and apply access control policies throughout your corporate network seamlessly to the IT services in place.

Protelion Security Technology allows you to work with both dynamic and static network/port address translation (NAT/PAT) to encapsulate traffic of different network services without affecting their features. Protelion Security Technology offers NAT-Traversal option to support connectivity with NAT in the network.

With the point-to-point network communication capability Protelion Security Technology protects communication channels without shifting the traffic processing load onto the central server hosts, thus ensuring all the centralized management benefits as well as transparently support all IT services including client-to-client.

The Protelion product line is mature and oriented towards minimizing implementation and ownership costs. Thanks to this, you can implement common scenarios of establishing secure connections and communications without changing the client and server settings.

The Protelion products have been developed in an inventive way to meet the demands of mobile communications and industrial automation ensuring a sufficient level of protection without trade-offs at the application layer and in operational scenarios.

Protelion Channel Protection Products

SECURITY GATEWAYS

MANAGEMENT AND CLIENT COMPONENTS

Protelion AR

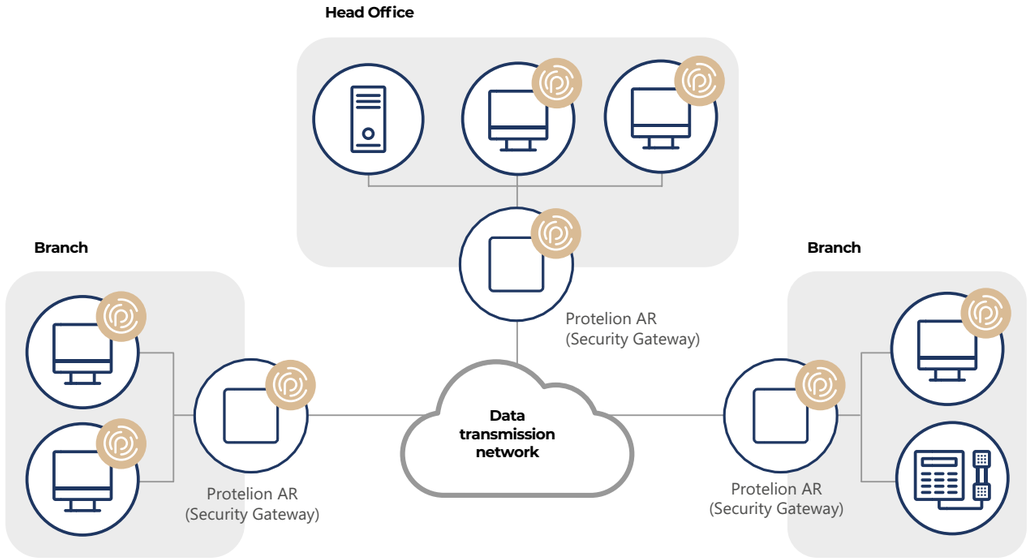
Security gateway for channel protection

The Protelion AR is our encryption hardware appliance to establish protected communication channels between sites.

Due to its uniquely features (cryptographic data protection, firewall, integrated network services), the Protelion AR constitutes a versatile solution for protecting corporate networks against unauthorized access to resources when transmitting data over public channels.

ADVANTAGES

- Failover cluster
- Centralized and remote management (SSH, WebUI)
- Unattended operation 24×7
- Support of modern, multiservice networks and full compatibility with:
  - DHCP, WINS, and DNS services
  - Dynamic address translation (NAT, PAT)
  - Multimedia protocols (SIP, H.323, SCCP, and others)



USE CASES

- Secure communication between branches of an organization (site-to-site and multi site-to-site)
- Protecting backbone links between data centers
- Network protection, also with wireless channels
- Protected access to corporate network for remote and mobile users
- Protecting multiservice networks (including IP telephony and videoconferencing)
- Differentiated data access in local networks, splitting local networks (for example, creating a DMZ)
- Communicating with Protelion networks of other organizations

FEATURES

VPN

- Network-layer gateway (L3)
- Data-link layer gateway (L2 over IP VPN)
- IP address server
- VPN router
- Traffic masking due to encapsulating the traffic to UDP and TCP

NETWORK FUNCTIONS

- Static routing
- Dynamic routing
- VLAN (dot1q) support
- Channel bonding (EtherChannel, LACP)
- Traffic classification and prioritization (QoS, ToS, DiffServ)

FIREWALL

- Stateful firewall
- Separate traffic filtering rules for unencrypted and encrypted IP traffic
- NAT / PAT
- Anti-spoofing
- Proxy server and third-party antivirus

INTEGRATED SERVICES

- DNS server
- NTP server
- DHCP server
- DHCP-Relay
- UPS support
- Failover cluster

Product Line AR

Hardware specifications

Available models	AR100	AR1000	AR2000	AR5000
Form factor	Desktop	1 RU	1 RU	1 RU
Dimensions (H × W × D)	170 × 41,5 × 138 mm	430 × 44 × 435 mm	444 × 44 × 383 mm	430 × 44 × 435 mm
Weight	0.5 kg (without power supply)	7 kg	8 kg	8 kg
Power supply configuration	External, +24V	Dual 300W AC	500W AC	Dual 300W AC
AC input voltage	100 to 240V AC	100 to 240V AC	100 to 240V AC	100 to 240V AC
Power Redundancy	N/A	1+1 Hot Swap	1+1 Hot Swap	1+1 Hot Swap

Performance

VPN throughput	175 Mbps	915 Mbps/2300 Mbps*	Up to 3.5 Gbps	Up to 6.0 Gbps/10 Gbps*
L2 over IP VPN throughput	Up to 175 Mbps	Up to 890 Mbps/2300 Mbps*	Up to 3.3 Gbps	Up to 6.0 Gbps/10 Gbps*
Number of connected available Protelion devices (tunnels)	2^{16} (65536)	2^{16} (65536)	2^{16} (65536)	2^{16} (65536)
Recommended number of VPN clients (depending on available bandwidth)	Up to 10	Up to 1,000	Up to 5,000	Up to 6,000

* Network Bonding refers to the combination of network interfaces on one host for redundancy and/or increased throughput.

Firewall

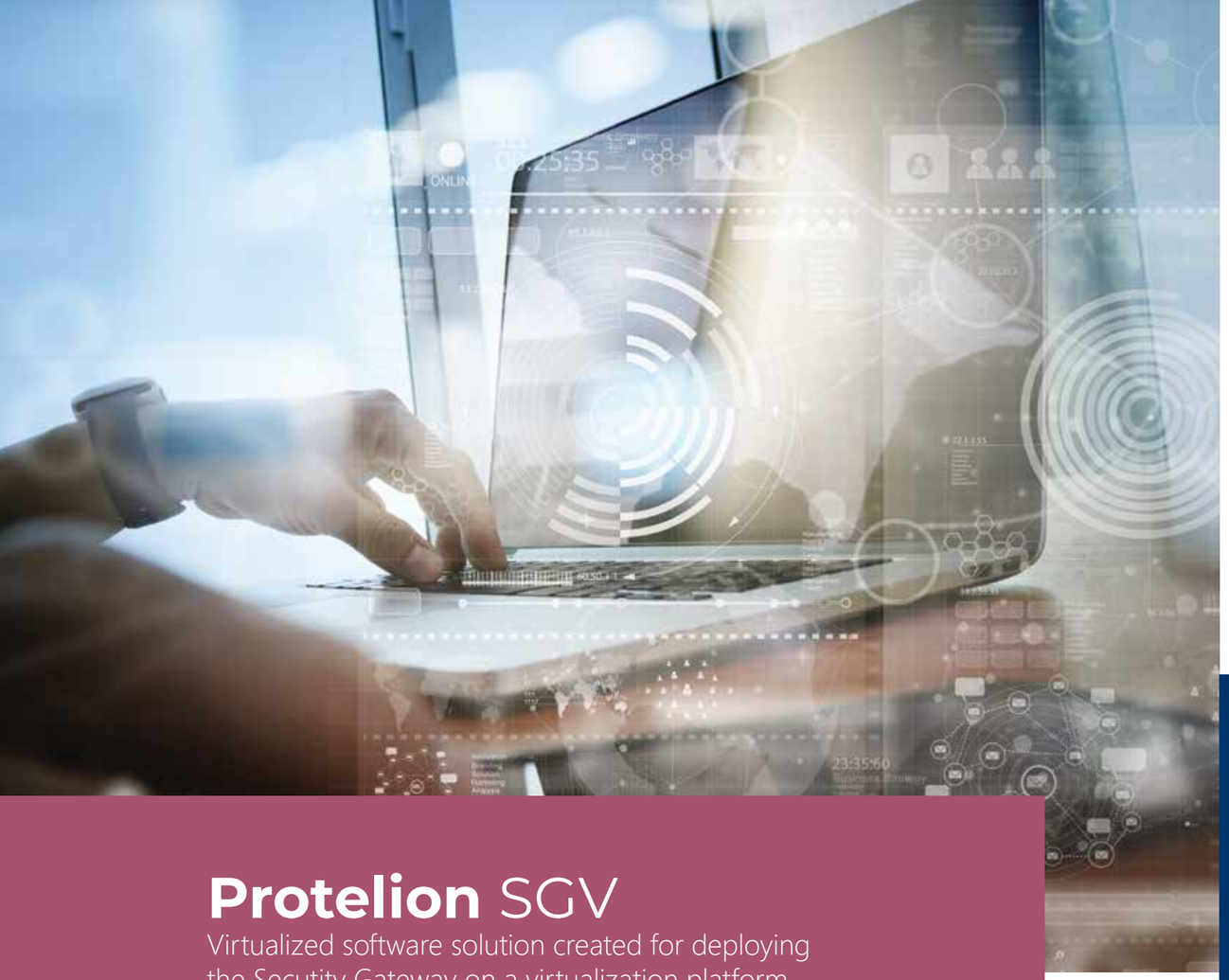
Firewall throughput (real world HTTP)	360 Mbps	Up to 930 Mbps/2700 Mbps*	Up to 9.3 Gbps	Up to 9.3 Gbps/13 Mbps*
Max number of concurrent connections	150,000	1,000,000	3,000,000	6,500,000

Network performance

Network interfaces (copper)	4× Rj45, 10/100/1000 Mbps	8× RJ45 1 Gbps	4× RJ45 1 Gbps	4× RJ45 1 Gbps
Network interfaces (optical)	1× SFP 1 Gbps	4× SFP 1 Gbps	4× SFP+ 10 Gbps	8× SFP+ 10 Gbps
Transceiver (included)	No	1× AFBR-5710PZ	2× Avago AFBR-709SMZ	2× Avago AFBR-709SMZ
Wireless interfaces	Optional: Internet WLAN or 3/4G Module	No	No	No

Availability and reliability

Failover cluster	Yes	Yes	Yes	Yes
Unattended operation 24 × 7	Yes	Yes	Yes	Yes
Power management with an uninterruptible power supply	Yes	Yes	Yes	Yes
MTBF (Mean time between failures)	30,000 hours	50,000 hours	50,000 hours	50,000 hours



Protelion SGV

Virtualized software solution created for deploying the Secutity Gateway on a virtualization platform

- The Protelion SGV virtual appliance is a versatile security gateway for deployment on a virtualization platform. It provides secure access to virtualized data centers in dynamic cloud environments, protecting against network attacks and unauthorized access
- The virtual appliance can be seamlessly integrated into an existing infrastructure and satisfies the most stingent functionality, usability, reliability, and fault tolerance requirements
- Protelion SGV is a virtual appliance version of the Protelion AR hardware device. It runs inside a hypervisor in a virtual host
- Protelion SGV Web Access for configuring security options

USE CASES

- Establishing secure communication channels between different company offices (site-to-site and multi-site-to-site)
- Protected access for remote and mobile users
- Protecting backbone links between data centers
- Protecting multiservice networks (including IP telephony and videoconferencing)
- Data access control in LANs
- Secure controlled access to the Internet

ADVANTAGES

- Virtualization technology offers freedom from having to solve compatibility issues with other vendors´ operating systems or applications and, morevover the implementation is seamless and does not affect a company's business processes. The virtual appliance is pre-installed on an adapted Linux OS and can be deployed on various virtualization platforms
- Up to 4,0 Gbps VPN Throughput for TCP protocol (or in certain conditions)
- No license restrictions for concurrent VPN connections through the Protelion Security Gateway
- Fully compatible with modern network services:
  - DHCP, WINS, DNS services
  - Dynamic address translation (NAT, PAT)
  - Multimedia protocols (SIP, H.323, SCCP, and others)
- Failover cluster enhances fault tolerance

Protelion SGV modification

Models	VA100	VA500	VA1000	VA2000
VPN throughput, Mbit/s	180	580	1400	4000
Firewall throughput, Mbit/s	330	940	3500	5500
Max number of concurrent sessions	150,000	500,000	1,000,000	3,000,000

* Testing was done on the server with 2x Intel® Xeon® CPU E processors. Each value was obtained in a separate performance test.

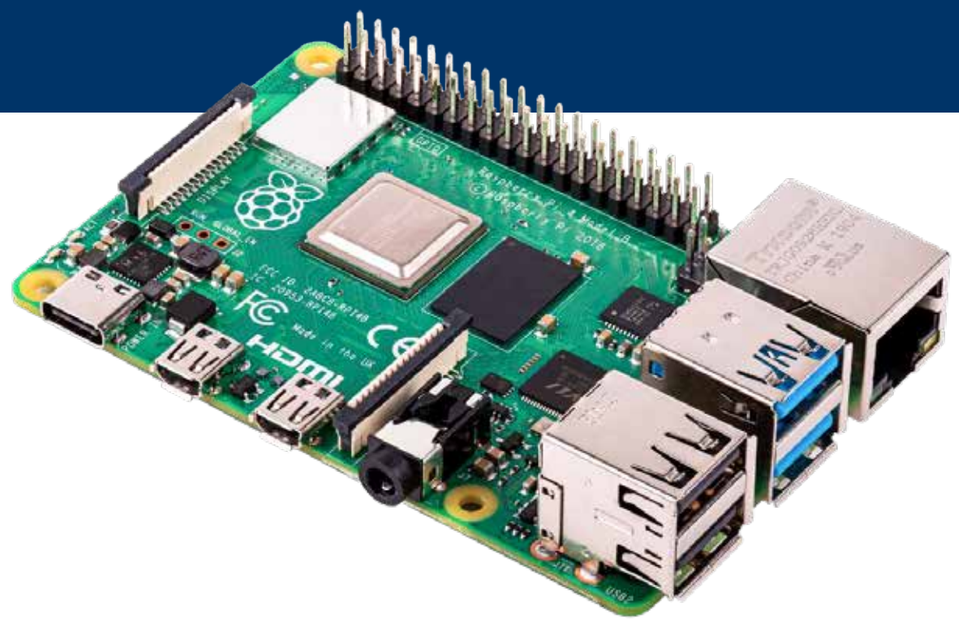
Protelion SG RPi

Compact VPN Security Gateway with firewall

Protelion SG RPi is a smart, affordable, secure encryption solution that runs on a an additionally protected Raspberry Pi platform. The single board computer has grown into a must have component of innovative business. The Protelion solution for Raspberry 4 model B consists of a Linux-based operating system and a Protelion Security Gateway. In combination with Raspberry Pi, the image forms a hardware appliance. The credit card-sized mini-computer acts as a fully-functional VPN gateway with a firewall based on Protelion Security Technology.

FEATURES

- Protelion SG RPi offers a wide range of services used on the server or on the client side
- VPN gateway: encrypted site-to-site and client-to-site connections
- Layer 3 Stateful Inspection Firewall: filters public traffic and VPN traffics by IP address, TCP/UDP port and VPN ID
- VPN router: Encrypted traffic is routed based on the Protelion host identifiers specified in the unencrypted part of IP packets, which is protected against falsification. The routing is performed over a proprietary protocol designed for secure dynamic routing of traffic
- Along with the routing, network address translation (NAT) is performed for encrypted traffic. All forward encrypted packets that are received by a Protelion SG RPi are sent to other hosts with the Gateway's IP address as their source IP address



ADVANTAGES

- Protelion SG RPi allows you to establish encrypted connections without a handshake. This speeds up secure communications within a VPN and makes them more reliable
- Fully compatible with modern network services:
  - DHCP, WINS, DNS services
  - Dynamic address translation (NAT, PAT)
  - Multimedia protocols (SIP, H.323, SCCP, and others)
- Centralized key management with Protelion SMC
- Independent Internet connection via optional 3G/4G, 5G, LTE modem enables many various use cases

USE CASES

Protelion Security Technology, combined with Raspberry Pi, is an efficient and promising solution for many application areas and particularly, for the Internet of Things (IoT).

It offers highly secure protection against both external and internal attacks for remote monitoring systems and industrial control systems – at a reasonable cost.

Common examples to use the solution are: to protect network computer-controlled cash systems, protect VoIP, printers, building infrastructure or IP video cameras. With Protelion SG RPi, you can reduce costs per location or per device / system.

The Protelion SG RPi is supplied as firmware for the Raspberry Pi 3 Model B+ and Raspberry Pi 4 Model B computers made by the Raspberry Pi Foundation.

Protelion SG RPi	
VPN throughput	Up to 50 Mbps
Firewall throughput	Up to 100 Mbps
L2 over IP VPN	Not available
Number of connected available Protelion devices (tunnels)	2^{16} (65536)
Modification	Raspberry Pi 3 Model B+ and Pi 4 Model B
Dimensions	85.6 D × 56.5 W × 17 H mm (without external case)
Weight	45 g (without AC/DC adapter)
Power supply	5V/2.5A DC via micro USB connector 5V DC via GPIO header Power over Ethernet (PoE) (requires separate PoE HAT) Network interfaces
Network interfaces (copper)	1× Ethernet RJ45 10/100/1000 Mbps
Wireless interfaces	1× Wireless Adapter (2.4 GHz and 5 GHz, 802.11.b/g/n/ac) External USB 3G/4G/5G/LTE modem support Availability and reliability
Failover cluster	No
Unattended operation 24×7	Yes

Protelion IG

Ruggedized encryption device to establish protected communication channels in Industrial Control Systems

Protelion IG is recommended for use:

- In information systems, where the equipment is required to run at low and high temperatures
- In Industrial Control Systems
- In Distributed Control Systems (DSC)

USE CASES

- Network segmentation
- Protecting wired and wireless communication channels
- Creating demilitarized zones (DMZ)
- Remote Support Access
- Secure remote access for mobile user
- Secure remote monitoring
- Secure remote maintenance
- Connecting to equipment securely through serial interfaces

Features

VPN

- Network-layer gateway (L3)
- Data-link layer gateway (L2 over IP VPN)
- VPN router
- Traffic masking due to encapsulating the traffic to UDP and TCP

NETWORK FEATURES

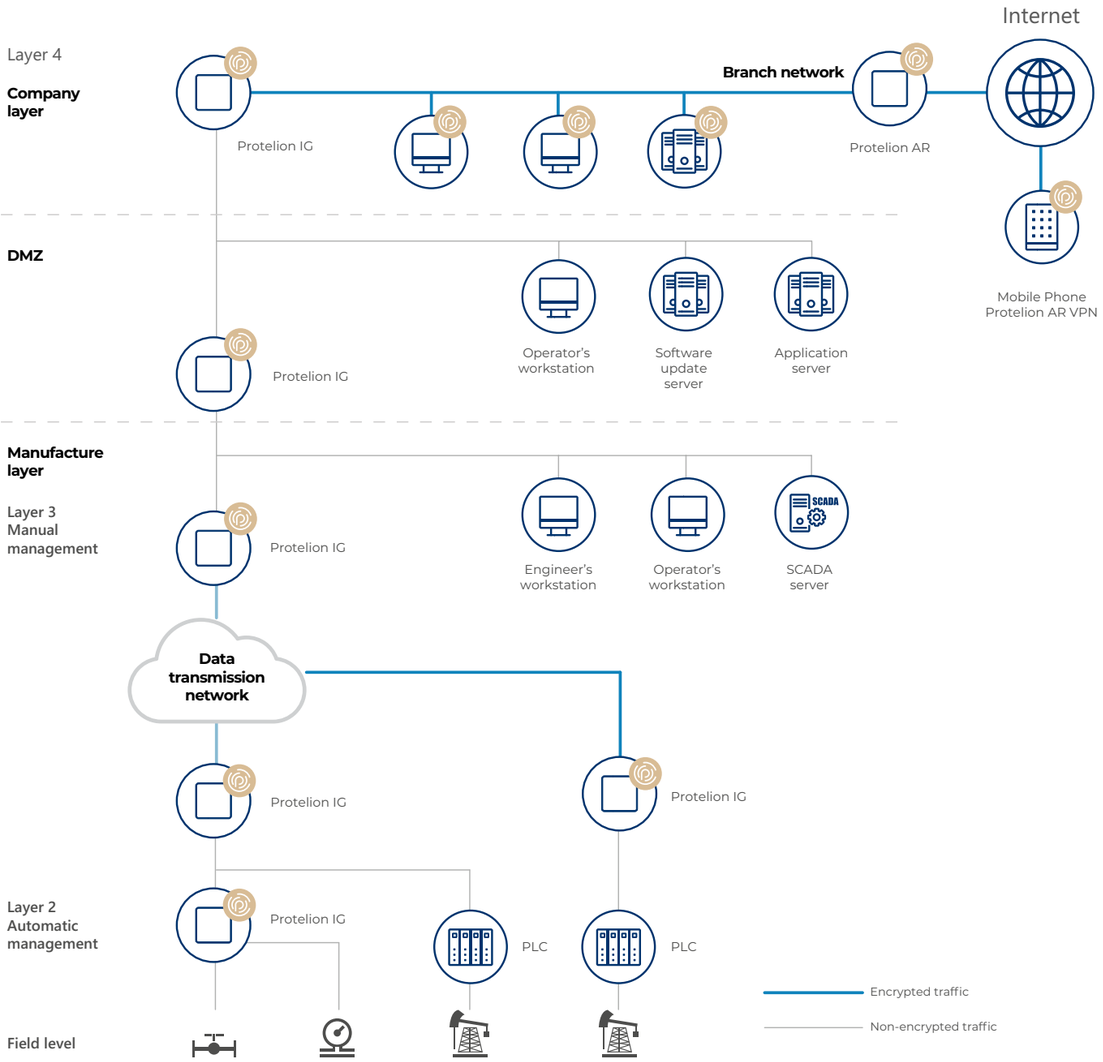
- Static routing
- Dynamic routing
- VLAN (dot1q) support
- Traffic classification and prioritization (QoS, ToS, DiffServ)
- Channel bonding (EtherChannel, LACP)
- Modbus TCP – Modbus RTU Gateway

INTEGRATED SERVICES

- DNS server
- NTP server
- DHCP server and DHCP-relay
- Failover cluster

FIREWALL

- Stateful firewall
- Separate traffic filtering rules for unencrypted and encrypted IP traffic
- Separate traffic filtering rules for each mode of the industrial system firewall
- NAT / PAT
- Industrial protocol filtering for Modbus, Profinet, Ethernet / IP, OPC UA, MMS, DNP3
- Deep packet inspection for Modbus protocol
- Anti-spoofing
- Proxy server
- Support for dynamic interfaces in the failover cluster
- Now Protelion IG allows you to deploy a failover cluster using Wi-Fi interfaces and 3G / 4G modem, as well as Ethernet interfaces with dynamic IP address. Modems and Wi-Fi modules may be configured differently



ADVANTAGES

- Protecting wireless networks
- Connecting the RS-232, RS-422 and RS-485 devices
- Protecting IS and ICS in various modes: normal, maintenance, and emergency modes
- Support for failover cluster mode
- Industrial design and suitability for use in harsh environments
- Remote management
- Compatibility with Protelion Channel Protection products to ensure end-to-end security

Protelion IG10

Hardware specifications

Form factor	DIN-rail mountable
Dimensions (W × H × D)	52 × 132 × 120 mm
Power supply	12–24 V DC
Power consumption	Up to 10 W
Operating temperature	–20 (– 40) ... +60°C
IP protection class	IP30

Information and Industrial System Firewall

Firewall throughput	Up to 10 Mbps
Max number of concurrent connections	Up to 1,000
Failover cluster	Yes

Performance

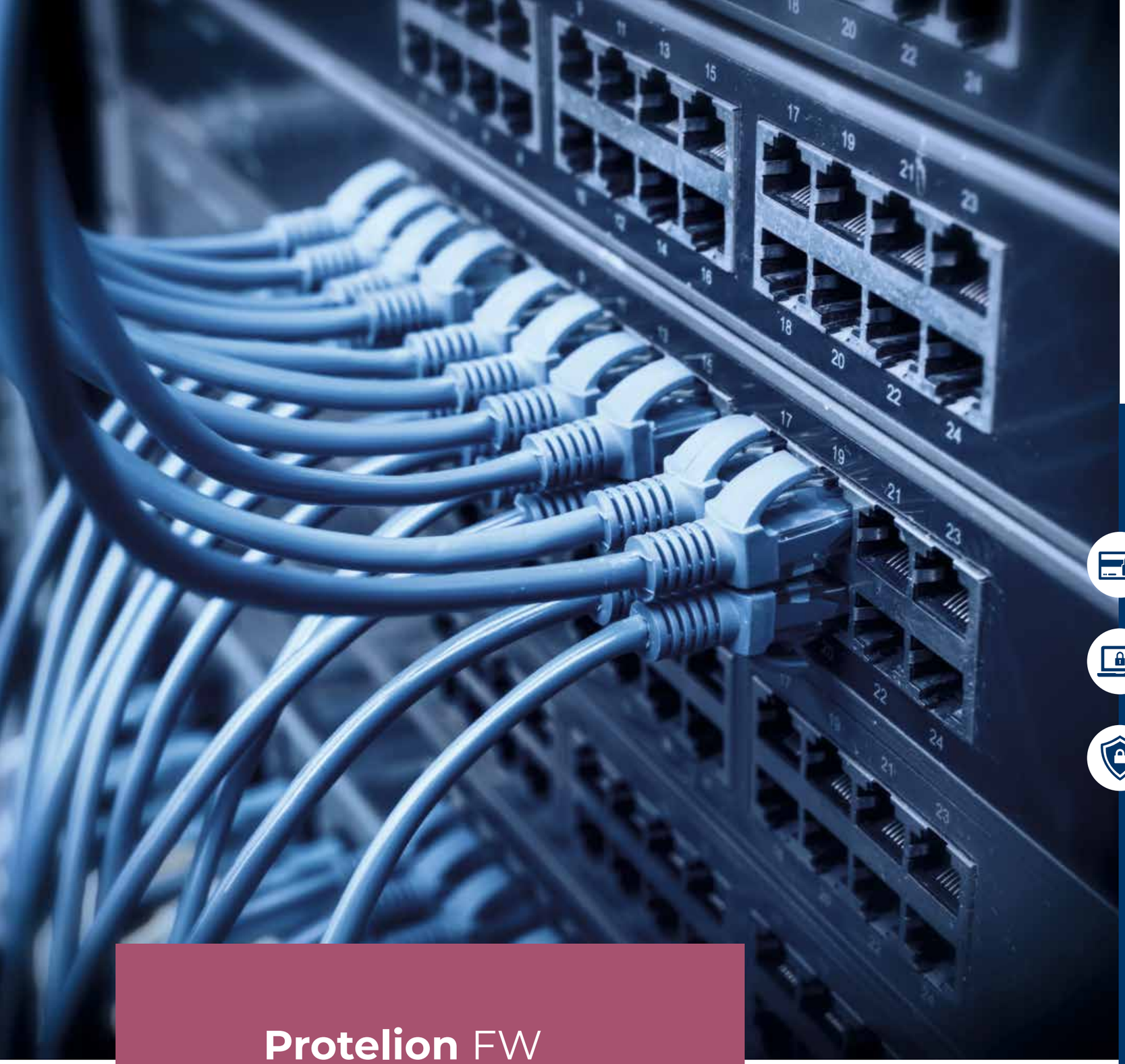
VPN throughput	Up to 10 Mbps
Number of connected available Protelion devices	2^{16} (65536)
Recommended number of VPN clients (depending on available bandwidth)	Up to 10

Input-output ports

Ethernet ports	3×RJ45 10/100/1000 Mbps
USB ports	2
Mobile telephony	GSM/ GPRS/ EDGE/ UMTS/ HSPA, 1× SIM card slot
Wireless interfaces	Wi-Fi 2.4 GHz + antenna (SMA)
GPIO	1-In/1-Out
RS-232/485	+

Availability and reliability

Unattended operation, 24×7	Yes
MTBF (Mean time between failures)	350,000 hours



Protelion FW

Next Generation Firewall

Protelion FW is a deep-packet inspection firewall that moves beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall.

ADVANTAGES

Granular security policy based on
User – Application – Allow/Block concepts

Secure use of personal devices at work ensuring full compliance with the company's security policies – BYOD (Bring Your Own Device)

Detection and blocking of over 2,000 application protocols and applications like games, social networks, torrents and so on:

- Reduced Internet traffic costs
- Minimized attack surface

Protelion FW analyzes the traffic using the signature and heuristic methods based on the Intrusion Prevention Rules (IPS rules). It automatically detects and eliminates the following types of threats:

- Attacks against network services
- Attempts to exploit software vulnerabilities of protected network objects
- Abnormal traffic
- Viruses

FEATURES

Application-layer firewall with DPI

Detects and blocks over 2,000 application protocols including:

- Games
- Social networks
- Instant message services
- Videoconferencing
- P2P services, Torrent
- File hosting
- Tunneling, VPN
- Remote control
- Industrial protocols

Firewall

- Stateful firewall with session control
- NAT / PAT Address Translation
- Anti-spoofing protection
- Supports Protelion TDA

Network Features

- Well-developed static routing
- Dynamic routing
- VLAN (dot1q) support
- Channel bonding (LACP, EtherChannel)
- QoS, ToS, DiffServ support

Integrated Services

- DNS server
- NTP server
- DHCP server
- DHCP-Relay

DPI (DEEP PACKET INSPECTION)

DPI uses different techniques to identify users' application traffic based on ports and protocols, signature method, heuristic method. With these methods, the products can detect even applications with encrypted or masked traffic.

Users Identity

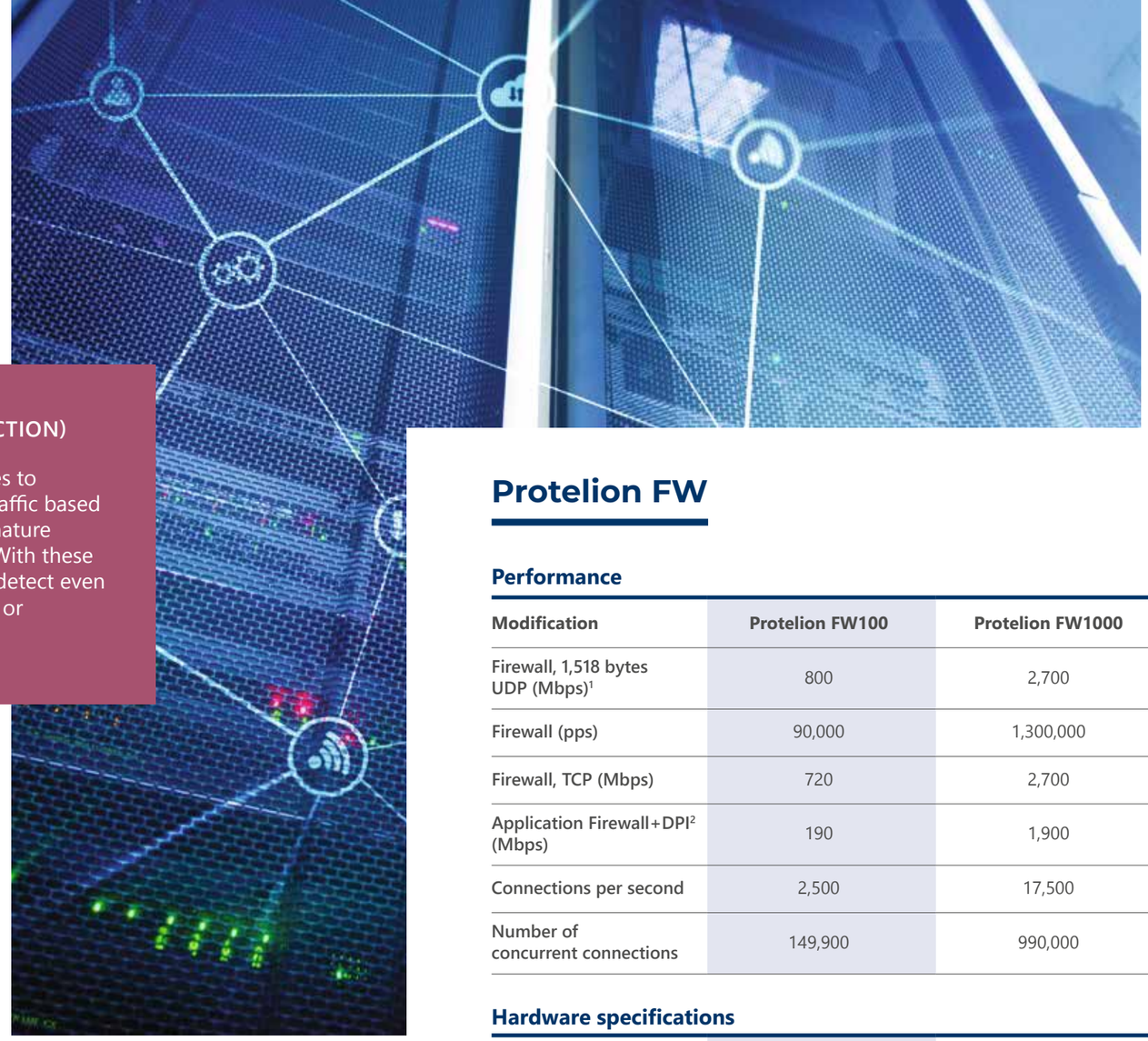
- Microsoft AD
- Captive Portal with LDAP directory

Proxy Server

- Support for HTTP
- Traffic control and filtering by the file's MIME type and the HTTP request method
- Traffic scanning by third party antivirus over ICAP

High availability and clustering

- Failover cluster
- UPS support



Protelion FW

Performance

Modification	Protelion FW100	Protelion FW1000	Protelion FW5000
Firewall, 1,518 bytes UDP (Mbps)[1]	800	2,700	19,000
Firewall (pps)	90,000	1,300,000	4,000,000
Firewall, TCP (Mbps)	720	2,700	9300
Application Firewall+DPI[2] (Mbps)	190	1,900	7,100
Connections per second	2,500	17,500	17,500
Number of concurrent connections	149,900	990,000	9,900,000

Hardware specifications

Modification	Protelion FW100	Protelion FW1000	Protelion FW5000
Form factor	MiniPC	19' Rack 1U	19' Rack 1U
Dimensions (W×H×D)	170 × 41.5 × 138 mm	430 × 43.4 × 380 mm	444 × 44 × 383 mm
Weight	1 kg	7.2 kg	13 kg
Power supply	DC 12B; 5A	Embedded power supply, 110-240 V, 250 W	Embedded power supply, 110–240 V, 500 W
Input-output ports	1× VGA 2x USB	2× VGA 1× PS/2 1× COM DB9 6× USB	1x VGA 1× PS/2 KB/Mouse port 1× COM DB9 2× USB
Network ports	4× RJ45 1 Gbps 1× SFP 1 Gbps	xF1000 C: 6× RJ45 10/100/1000 Mbps xF1000 D: 4× RJ45 10/100/1000 Mbps 2× SFP 10/100/1000 Mbps	4× RJ45 1 Gbps 4× SFP+ 10 Gbps

[1] Results obtained using Protelion methods.
[2] Results obtained for the EMIX traffic, which is a traffic mix of different application protocols: BitTorrent, HTTP, HTTPS, Oracle DB, SMTP, SSH, and others

Protelion SMC

All-in-one system to manage Protelion products and solutions

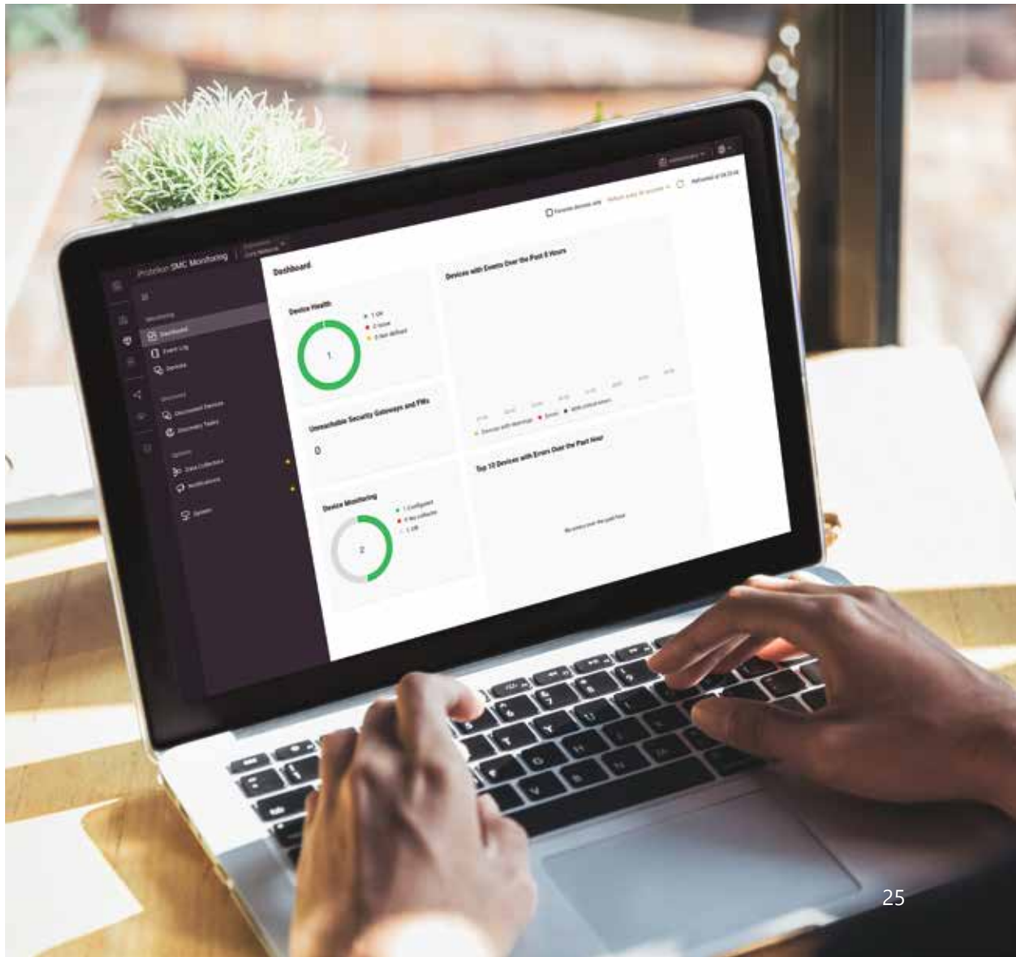
Description

Protelion SMC is a security management center to manage Protelion products in an all-in-one scalable device.

Delivering simplicity and consolidation, Protelion SMC aims to relieve the IT administrator's daily effort and increases convenience for service providers.

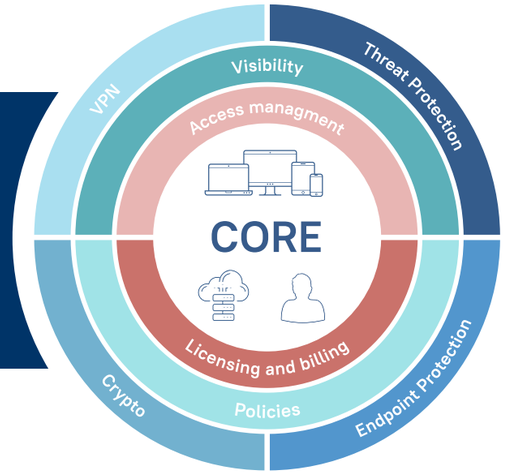
Protelion SMC facilitates Protelion security products deployment, management, key generation and delivery and license management.

Protelion SMC provides easy-to-use tools for multiple host monitoring and asset management and automates routine tasks, such as software updates and security policies configuration.



How it works

Protelion SMC is a modular platform with a management core providing a consolidated information area and interoperability for functional modules.



Performance

Protelion SMC features are

- Maintaining Protelion VPN topology, hosts, users and connections
- Generating and managing secret keys
- Automated Protelion software update
- Easy security policies management
- Network monitoring and critical events alerting
- Protelion products license management
- Billing reports creation

PROTELION SMC SUPPORTS THE FOLLOWING MODULES

Protelion SMC – VPN Module

- Protelion virtual private network structure creation and management for hosts, users and links
- Establishing corporate connections with a secure VPN channel between networks
- Establishing secure access to Protelion VPN objects for trusted organizations
- Secret key generation and distribution

Protelion SMC – Rollout Center Module

- Quick deployment of Protelion VPN devices in large distributed networks including mobile devices
- Activation of VPN Clients via email and SMS in a Protelion protected VPN network

Protelion SMC – Network Visibility Module

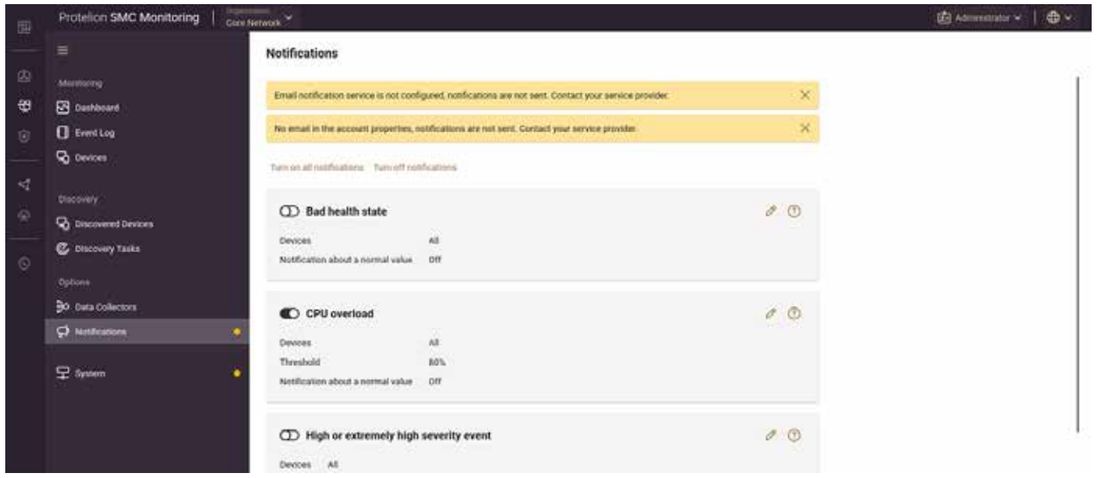
- Protelion network monitoring
- Protelion network device activity details and summary
- Protelion network important events alerts

Protelion SMC – Policy Manager Module

- Creating security policy rules
- Applying security policies either to specific hosts, host groups or entire network
- Controlling policies distribution and applying to Protelion VPN hosts

USE CASES

- Ready-to-use security service provider platform
- Protelion security infrastructure management platform

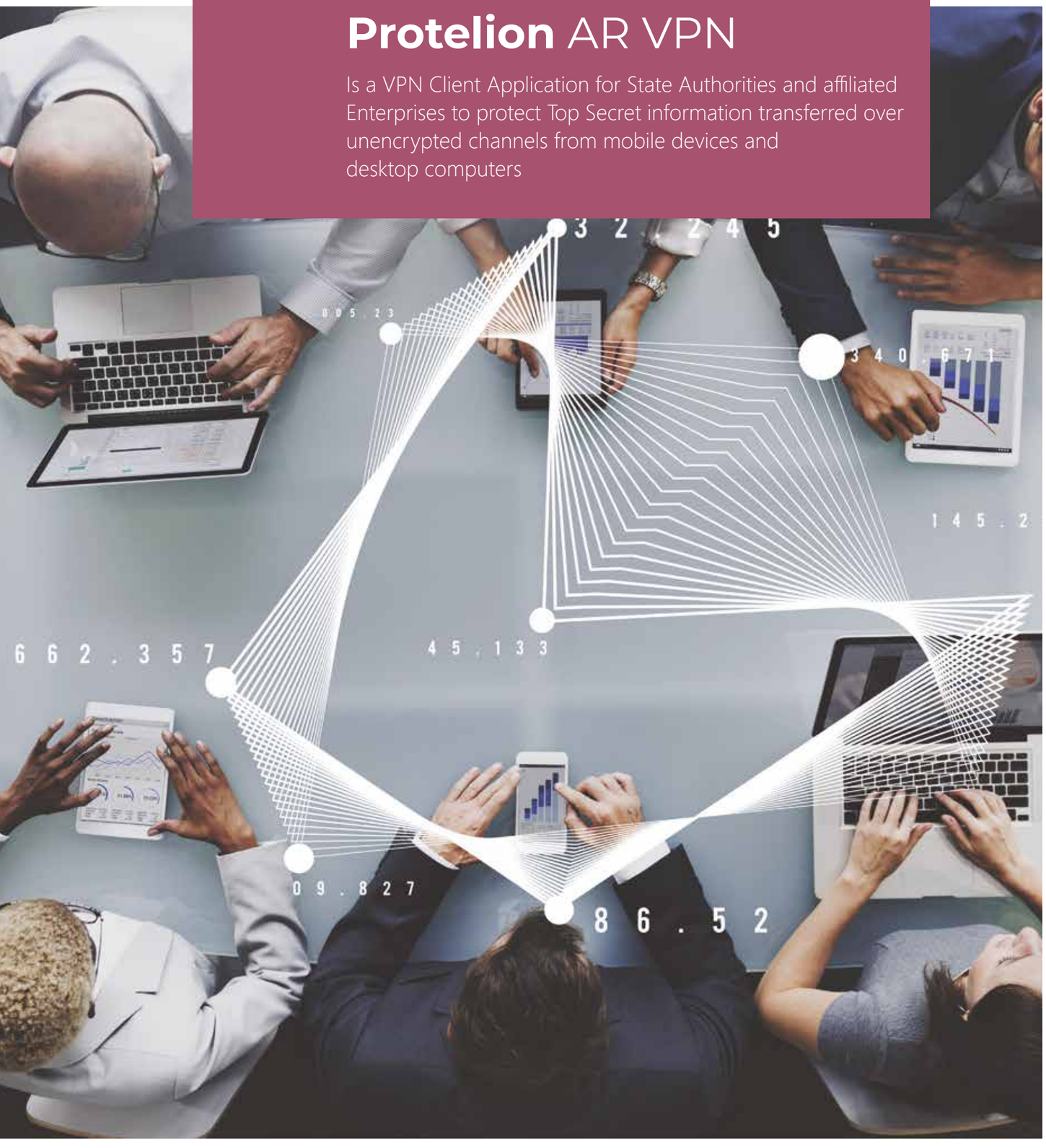


ADVANTAGES

- User-friendly administrative web console
- Multitenant SaaS ready platform
- Consolidated information area with advanced role access management
- Centralized authentication service
- Unified policy management
- Centralized asset discovery and monitoring
- Easy-to-use billing and license management systems
- User account imports from the Microsoft Active Directory and external sources

Protelion AR VPN

Is a VPN Client Application for State Authorities and affiliated Enterprises to protect Top Secret information transferred over unencrypted channels from mobile devices and desktop computers



The Protelion AR VPN Client solution protects a device against internal and external attacks, and provides secure access to corporate resources over the Internet.

FEATURES

- With this product, you can ensure uniform and highly secure access to the resources of corporate information systems from anywhere in the world using any TCP/IP networks
- Due to its traffic encryption, the product can protect voice traffic, video communi-cation, VoIP connections, mail exchange, and other services in TCP/IP networks in real time
- The Protelion Security Technology behind the product allows you to operate geographically distributed information systems via a single control center and distribute encryption keys and software over a secure channel
- The product architecture can ensure concurrent work with resources of different corporate network segments

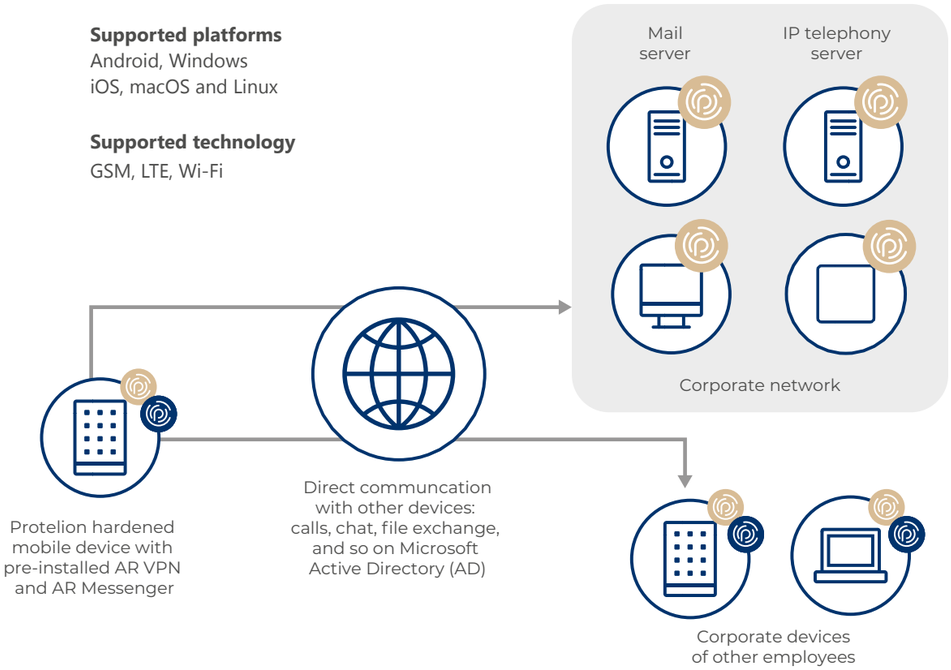
SPECIAL FEATURES

AR VPN Client: point-to-point encryption and MAC protection of IP packets using the AES algorithm with symmetric 256-bit keys

Use Cases, Mobile and Desktop Protection

Supported platforms
Android, Windows
iOS, macOS and Linux

Supported technology
GSM, LTE, Wi-Fi



USE CASES

1 Secure remote client-to-site and client-to-client connections to corporate resources and services over encrypted channels. The client-to-client (point-to-point) connection mode provides protection not only when data is exchanged via public communication channels but also when the Protelion AR VPN Client is used in a corporate network, thus protecting the confidential information against internal intruders as well.

2 In addition to the protection scenarios, you can add optional secure communication tools, such as a secure messenger (Protelion AR Messenger), to your existing protected Protelion network.

3 Protelion AR VPN Client does work as a virtual appliance thus allowing you to use Protelion protection tools in VDI (Virtual Desktop Infrastucture) environments.

4 Protelion AR VPN Client can be used as an overlay security tool to protect your existing mail, document exchange, and video conferencing systems. Without changing of your application software.

5 With Protelion AR VPN Client, you can block direct Internet access on your device so it is able to access the Internet only through the corporate traffic cleaning zone, which uses a set of security tools, such as proxy servers, DLP systems and content filtering systems. This approach ensures multilevel device protection and applies corporate data security measures even to devices that physically leave the secure perimeter.

PROTELION

Protelion GmbH
Oberwallstrasse 24
D-10117 Berlin
+49 30 206 43 66-0
info@protelion.de
gov.protelion.com

GD – DKV23.1