

# SOPHOS

Security made simple.

## Sophos UTM

### Unified Threat Management makes security simple

Sophos UTM gives you complete security from the network firewall to endpoint antivirus in a single modular appliance. It simplifies your IT security without the complexity of multiple-point solutions. The intuitive interface will help you quickly create policies to control security risks. And clear, detailed reports will give you the insight you need to improve your network performance and protection

#### Highlights

- ▶ Every feature available on every appliance
- ▶ Firewall, VPN, ATP, IPS, email, web filtering and app control
- ▶ Hardware, virtualized, software or cloud-based appliance
- ▶ Intuitive browser-based interface
- ▶ Built-in reporting on all models
- ▶ Two-factor authentication with one-time password (OTP) in many areas
- ▶ Integrated wireless controller

#### Consolidated network security platform—no compromise

Protect your network using multi-layered proven protection technologies including Advanced Threat Protection (ATP), IPS, VPN, email and web filtering combined with the industry's simplest admin interface. We've engineered our software and hardware to give you the throughput speeds you need. And, you can choose the level of protection you need with modular subscriptions as every feature is available on every appliance.

#### All the Next-Gen Firewall features you need

We'll give you complete control to block, allow, shape and prioritize applications. Our Deep Layer-7 inspection (Next-Generation Firewall) ensures true application identification and has regular automatic updates. And you'll get feedback on unclassified applications too.

#### Intuitive management and detailed reporting

You'll know what's happening with your users and you'll have complete control over all the features you need, with none of the complexity. Easily build policies while getting detailed real-time and historical data with our on-box reporting, helping you to fix problems fast. And our Free Sophos UTM Manager lets you centrally administer several appliances through a single login.

#### Connect remote offices with easy VPN and Wi-Fi

Sophos RED (Remote Ethernet Device) provides secure remote access to your off-site locations. It's the first security gateway that requires no technical skills at the remote site. Once installed, it forwards traffic to the UTM for complete security. Sophos UTM also works as a wireless controller; access points are automatically set up and receive complete UTM protection.

*"We chose Sophos UTM for its all-in-one approach, trouble-free installation and management at an affordable price".*

Martin Bělohlávek, Systems Administrator, MAN ČR, MAN Group



## Choose your security applications

Our Linux-based OS includes a free Essential Network Firewall. It provides fundamental security like firewalling, networking tools, routing and secure remote access. And our modular approach lets you add layers of protection as your needs evolve.

**UTM Network Protection** stops sophisticated attacks that a firewall alone can't stop.

- ▶ ATP combines multiple technologies to identify and block outgoing traffic to command-and control hosts. Combine with Web to add cloud-based selective sandboxing to constantly improve protection
- ▶ Configurable intrusion protection system and flood protection against denial of service attacks
- ▶ IPsec and SSL tunnels provide flexible site-to-site and remote-access VPN connections

**UTM Email Protection** stops spam and viruses and keeps sensitive data safe.

- ▶ Provides simple infrastructure-free email encryption and policy-based DLP to protect sensitive data and easily stay compliant
- ▶ Let users manage their spam quarantine and search a personalized mail log
- ▶ Keep infected emails out of your mailbox and protect confidential emails against illegitimate access

**UTM Wireless Protection** gives you secure Wi-Fi in minutes.

- ▶ Centrally manage access points through the UTM's built-in wireless controller
- ▶ Easily set up wireless hotspots and grant guest access using backend authentication or a customizable voucher-based system.

**UTM Web Protection** lets you protect your employees from web threats and control their time online.

- ▶ Step-by-step guidance to create fully transparent user-based policies with authentication by device type
- ▶ Limit use of unwanted applications while giving priority to business critical resources
- ▶ Use the policy tester to check if your policy is working and create dynamic reports
- ▶ Integrates with SEC managed endpoints, allowing you to keep your existing Sophos antivirus and use the UTM for Web policy

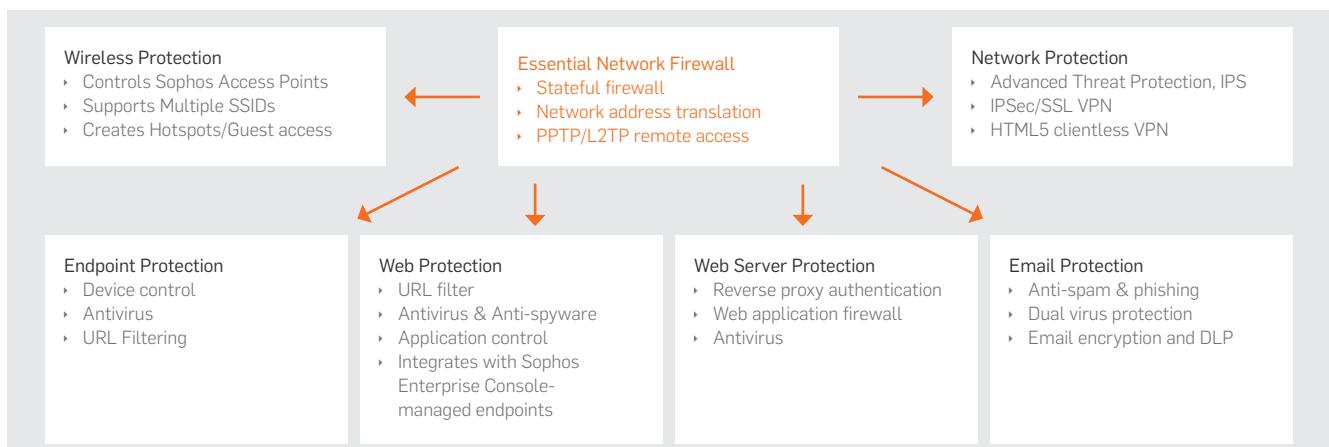
**UTM Webserver Protection** hardens web servers and apps ensuring compliance with a web application firewall.

- ▶ Reverse proxy authentication (offloading) inspects information submitted via forms on your websites to prevent server exploits
- ▶ Protect personally identifiable information like credit card and social security numbers

**UTM Endpoint Protection** provides desktops, laptops, and servers with antivirus, device and web control.

- ▶ Scans files, webpages and devices blocking or cleaning threats and providing admin alerts
- ▶ Device control reduces the risk of data loss and malware by managing removable devices
- ▶ Built-in URL filtering ensures users get the same level of web protection outside of the office as they do inside

## Add modules when you need them



*"With the Sophos appliances, we experienced greater productivity, reduced risk and costs savings."*

William Strucke, Systems Manager, The Ohio State University

### Choose your license

We give you the flexibility to license our protection modules individually. Or, you can choose one of our pre-packaged licenses. Whatever suits your needs.

	Next-Gen Firewall	BasicGuard	FullGuard
<b>Modules - Choose the ones you need</b>	<a href="#">Try It For Free</a>	<a href="#">Try It For Free</a>	<a href="#">Try It For Free</a>
<b>Essential Firewall - Free</b> Network Firewall, NAT, Native Windows Remote Access	Full	Full	Full
<b>Network Protection</b> IPSec/SSL, ATP, VPN, IPS, DoS Protection	Full	Basic	Full
<b>Web Protection</b> URL Filtering, Application Control, Dual Engine Antivirus	Full	Basic	Full
<b>Email Protection</b> Anti-spam, Email Encryption and DLP, Dual Engine Antivirus	Optional	Basic	Full
<b>Wireless Protection</b> Wireless Controller, Multi-SSID Support, Captive Portal	Optional	Basic	Full
<b>Webserver Protection</b> Web Application Firewall, Reverse Proxy, Antivirus	Optional	-	Full
<b>Endpoint Protection</b> Antivirus, HIPS, Device Control	Optional	Optional	Optional

### Extend your security

**Sophos RED** Simply secures your branch offices by forwarding all traffic to the central Sophos UTM. Installation requires no technical training and there is no ongoing maintenance.

**Wi-Fi Access Points** Configurationless access points are instantly protected by the UTM, letting you create secure mesh networks

**VPN Clients** Secure SSL or IPsec VPNs provide mobile and home workers with secure remote access from any location at any time.

**Free UTM Manager** Centrally manages multiple UTM devices through IPsec VPN tunnels; deploys policies in just a few clicks.



## Choose how to deploy

You can choose to install as hardware, software or a virtual appliance or even in the cloud.

**Hardware appliances** are purpose built, high-performance devices. They integrate our security applications with a hardened operating system (OS) on optimized Intel compatible server systems. Every feature is available on every appliance. See technical specifications.

**Software appliances** integrate all security applications with a hardened OS bundled within a single software image. Easily installs on your hardware of choice.

**Virtual appliances** are based on the software equivalent. Sophos UTM is the first unified threat management product to be certified as VMware Ready and Citrix Ready. It also runs in Microsoft Hyper-V and KVM virtual environments.

**Cloud-based appliances** using Amazon Virtual Private Cloud (VPC) let you run a UTM in the cloud. Or, you can use the Amazon VPC connector on the UTM at your office for secure and robust access to your Amazon-hosted resources.

## User Interface

The screenshot shows the Sophos UTM dashboard for 'dks-asg-01.qa.astaro.de' on Monday, Jan 13, 2014, at 11:14:29. The interface is divided into several sections:

- Management:** Model: ASG Software, License ID: 000000, Subscriptions: Base Functionality, Email Protection, Network Protection, Web Protection, Wireless Protection, Endpoint Antivirus, Uptime: 0d 0h 22m.
- Version information:** Firmware version: 9.152-2, Pattern version: 55986, Last check: 9 minutes ago.
- Resource usage:** CPU: 5%, RAM: 44% of 2.8 GB, Log Disk: 1% of 16.3 GB, Data Disk: 11% of 7.8 GB.
- Today's threat status:** Firewall: 45 packets filtered, IPS: 0 attacks blocked, Antivirus: 0 items blocked, AntiSpam: 0 emails blocked, AntiSpyware: 0 items blocked, Web Filter: 0 URLs filtered, WAF: 0 attacks blocked.
- Interface table:**

Interface	Name	Type	Status	Link	In	Out
all	All Interfaces		Up	Up	35.5 kbit	289.5 kbit
eth0	Internal	Ethernet	Up	Up	33.9 kbit	12.8 kbit
eth1	net-test-1	Ethernet	Up	Up	0.6 kbit	0
eth2	net-test-mm	Ethernet	Up	Up	1.1 kbit	277.5 kbit
eth3	unused					
- Advanced Threat Protection:** Botnet/command-and-control traffic detected (1 infected IP).
- Current system configuration:**
  - Firewall is active with 1 rules
  - Intrusion Prevention is active with 1689 of 16229 patterns
  - Web Filtering is inactive
  - Network Visibility is active, 0 Application Control rules active
  - SMTP Proxy is active, 0 emails processed, 0 emails blocked
  - POP3 Proxy is inactive
  - RED is inactive
  - Wireless Protection is inactive
  - Endpoint Protection is inactive
  - Site-to-Site VPN is inactive
  - Remote Access is inactive
  - Web Application Firewall is inactive
  - HA/Cluster is inactive
  - Sophos UTM Manager is not configured
  - Antivirus is active for protocols SMTP
  - AntiSpam is active for protocols SMTP
  - AntiSpyware is inactive

Hardware appliance	UTM 100	UTM 110	UTM 120	UTM 220	UTM 320	UTM 425	UTM 525	UTM 625
<b>Firewall throughput</b>	250 Mbit/s	1 Gbit/s	1.8 Gbit/s	3 Gbit/s	3.5 Gbit/s	6 Gbit/s	23 Gbit/s	40 Gbit/s
<b>VPN throughput</b>	60 Mbit/s	100 Mbit/s	180 Mbit/s	500 Mbit/s	800 Mbit/s	2.5 Gbit/s	4.2 Gbit/s	5.5 Gbit/s
<b>IPS throughput</b>	60 Mbit/s	140 Mbit/s	420 Mbit/s	1.1 Gbit/s	1.9 Gbit/s	5.5 Gbit/s	6.8 Gbit/s	9 Gbit/s
<b>Antivirus throughput (proxy)</b>	35 Mbit/s	50 Mbit/s	75 Mbit/s	235 Mbit/s	375 Mbit/s	1.4 Gbit/s	1.7 Gbit/s	3.8 Gbit/s
<b>Concurrent connections</b>	20,000	40,000	300,000	1 million	2 million	3 million	4.5 million	6 million
<b>Ethernet interfaces (copper)</b>	4*GE	4*GE	4*GE	8*GE	8*GE	6*GE	8*GE (default LAN module)	8*GE (default LAN module)
<b>Ethernet interfaces (SFP)</b>	-	-	-	-	-	2*GE	8*GE (special LAN-module)	8*GE (special LAN-module)

## Sophos UTM Certifications



United Kingdom and Worldwide Sales  
Tel: +44 (0)8447 671131  
Email: sales@sophos.com

North American Sales  
Toll Free: 1-866-866-2802  
Email: nasales@sophos.com

Australia and New Zealand Sales  
Tel: +61 2 9409 9100  
Email: sales@sophos.com.au

Asia Sales  
Tel: +65 62244168  
Email: salesasia@sophos.com

Oxford, UK | Boston, USA  
© Copyright 2014. Sophos Ltd. All rights reserved.  
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK  
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

1129-02.13DD.dsna.simple

