

Technical Update Workshop 2015

Version 9.3

Starts at 10:00 am GMT+1

Pre-Sales Engineering Team NSG - NEEMEA

presales-neemea@sophos.com



SOPHOS

Technical Update Workshop 2015

Version 9.3

Starting in 5 minutes...

Pre-Sales Engineering Team NSG - NEEMEA

presales-neemea@sophos.com



SOPHOS

Technical Update Workshop 2015

Version 9.3



Pre-Sales Engineering Team NSG - NEEMEA

presales-neemea@sophos.com

SOPHOS

Your speakers today



Agenda

- Interfaces & bridges
- Advanced Threat Protection
- Web Protection
- Email Protection
- Web Server Protection
- Wireless Protection
- New appliances and APs
- Roadmap update



Interfaces & bridges

What's new?

Interfaces



9.3 Interface & Routing features

- DHCP interface enhancements
- VLAN tagging for DHCP interfaces
- VLAN interfaces as addition to static or DHCP interface
- Multiple PPPoE interfaces
- Multiple bridge interfaces & VLAN support
- DHCP v6 relay
- IPv6 Router Advertisements: DNS Server Domain
- OSPF enhancements

Interfaces

DHCP interface enhancements

- Single interface type for static and DHCP
 - Ethernet
 - Ethernet Bridge
 - Ethernet VLAN
- 'Dynamic IP' option can be used for
 - Ethernet
 - Ethernet Bridge
 - Ethernet VLAN
- New option in the setup wizard



Type:	Ethernet
Hardware:	Group
Dynamic IP	3G/UMTS
IPv4 Address:	DSL (PPPOA / PPTP)
Netmask:	DSL (PPPOE)
IPv4 Default GW:	Ethernet
	Ethernet Bridge
	Ethernet VLAN
	Modem (PPP)

Add Interface

Name: VLAN If as DHCP Client

Type: Ethernet VLAN

Hardware: eth0 XEN network device

Dynamic IP ☒

VLAN Tag: 101

IPv4 Default GW: ☐

☐ Setup Internet connection later

Interface: eth1 Intel Corporation 82545EM

Internet uplink type: Standard Ethernet interface

Address type: Dynamic (DHCP)

☐ Please select:

Dynamic (DHCP)

Static

Interfaces

VLAN interfaces in DHCP client mode



search Interfaces

Dashboard
Management
Definitions & Users
Interfaces & Routing
 Interfaces
 Bridging
 Quality of Service (QoS)
 Uplink Monitoring
 IPv6
 Static Routing
 Dynamic Routing (OSPF)
 Border Gateway Protocol
 Multicast Routing (PIM-SM)
Network Services
Network Protection
Web Protection
Email Protection

Interfaces Additional Addr... Link Aggregation

+ New interface...

AI

🔍

Edit interface

Name: eth1 Intel Corporation 82576

Type: Ethernet VLAN

Hardware: eth1 Intel Corporation 82

Dynamic IP ☒

VLAN Tag: 2332

IPv4 Default GW: ☐

Comment:

⊕ Advanced

✓ Save ✗ Cancel

Interfaces



VLAN interfaces added flexibility

- VLAN interfaces can be created on hardware used by other Ethernet interfaces
 - Allows tagged and untagged traffic on the same interface

Action	Sort by:	Name	IP	
Edit Delete Clone		Ethernet [Up] on eth2 MTU 1500	[10.250.250.1/24]	
Edit Delete Clone		External (WAN) [Up] on eth1 MTU 1500 - DEFAULT GWY 192.168.1.254 Added by Installation wizard	[192.168.1.10/24]	
Edit Delete Clone		Internal [Up] on eth0 MTU 1500 Auto-created on installation	[172.16.1.101/24]	
Edit Delete Clone		VLAN [Up] on eth2 (VLAN 22) MTU 1500	[10.140.140.1/24]	

Interfaces



Multiple PPPoE interfaces

- Multiple PPPoE interfaces supported on the same hardware
- Connections differentiated by the username and password
- Interfaces must have different IP addresses

Interface	Status	Connection	IP Address	MTU	Notes
Internal	Up	on eth0	[10.8.2.135/20]	1500	DEFAULT GW 10.8.15.254 Auto-created on installation
ppp1	Up	on eth5	[10.159.255.1/32]	1492	Reconnect
ppp2	Up	on eth5	[10.159.255.2/32]	1492	Reconnect
ppp3	Up	on eth5	[10.159.255.3/32]	1492	Reconnect

Interfaces

Multiple bridge interfaces & VLAN support

- Simplified process
- Support for multiple bridge interfaces
- Does not require an IP address
- Simplified configuration
- Create a new bridge or convert an existing interface

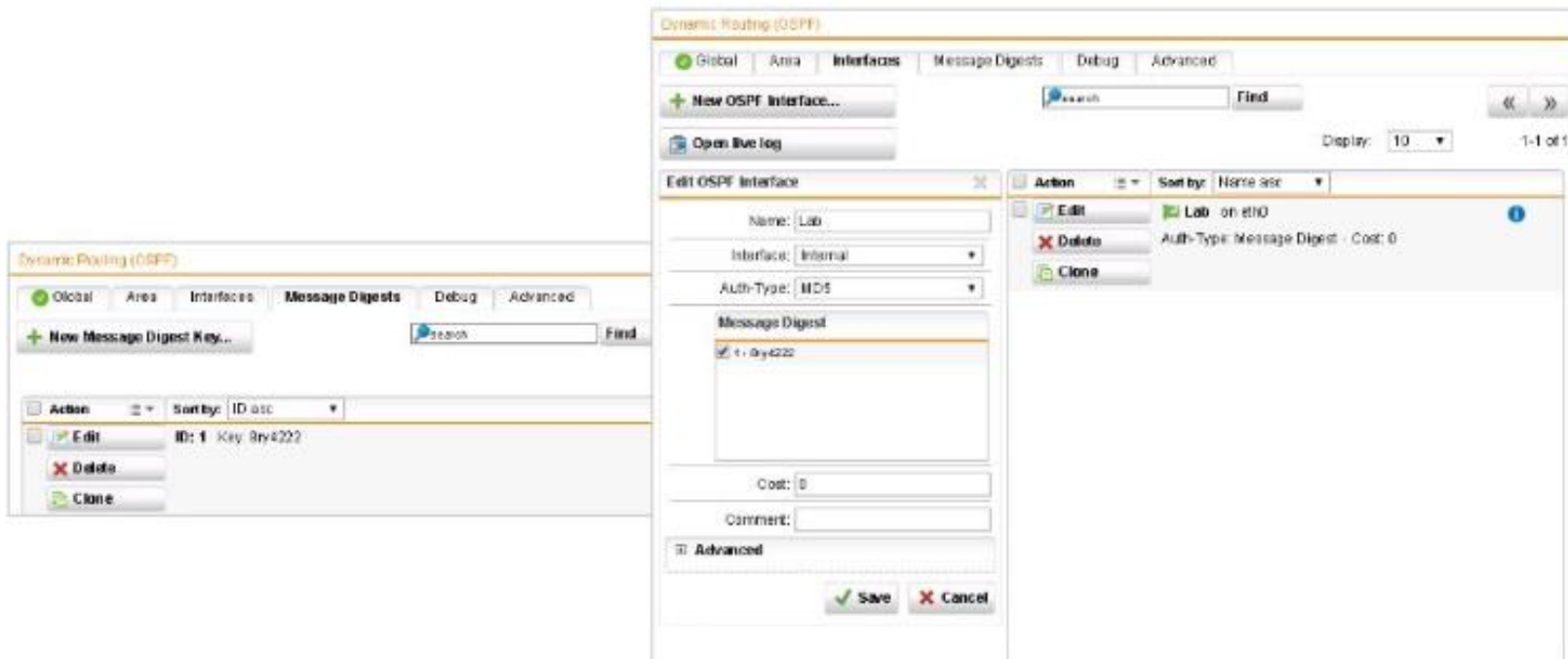
A screenshot of the 'Add Interface' configuration window in Sophos Firewall. The window has a title bar 'Add Interface'. Inside, there's a 'Name' field with 'Bridge' and a 'Type' dropdown set to 'Ethernet Bridge'. Below is a section 'Bridge selected NICs:' with a list of three interfaces: 'eth2 Intel Corporation 82546EM Gigabit Ethernet Controller (Copper)', 'eth3 Intel Corporation 82546EM Gigabit Ethernet Controller (Copper)', and 'eth4 Intel Corporation 82546EM Gigabit Ethernet Controller (Copper)'. There are checkboxes for 'Dynamic IP', 'IPv4 Address' (set to '0.0.0.0'), 'Netmask' (set to '24 (255.255.255.0)'), 'IPv4 Default GW', and a 'Comment' field. Below this is an 'Advanced' section with a sub-section 'Advanced Bridge'. It contains checkboxes for 'Allow ARP broadcasts', 'Spanning Tree Protocol', 'Allow IPv6 pass through', and a 'Virtual MAC' field set to '00:00:00:00:00:00'. At the bottom is a 'Forwarded Ether Types' list with '0x07'. At the very bottom are 'Save' and 'Cancel' buttons.

Interfaces

OSPF enhancements



- OSPF (Open Shortest Path First)
 1. Create a Message Digest key if you are going to use them
 2. Add interfaces you will be using



Interfaces DHCP, Bridge & VLAN



Demo

Advanced Threat Protection

What's new?

Advanced Threat Protection

Complete DNS security & IPv6 protection

- Before 9.3 the ATP detection has taken place in various ways such as via the UTM's DNS proxy.
- Direct DNS requests to public servers such as GoogleDNS (if allowed) however could not be secured by the ATP feature itself if not handled via the proxy.
- With version 9.3 any DNS request can be verified via our ATP intelligence provided by Sophos LABs
- Full ATP support for the IPv6 protocol

Web Protection

What's new?

Web Protection



Introducing more enterprise level features – powerful, flexible, simple

- **Site tagging** – enables sites to be tagged and tags to be used in policies (e.g. “customer sites” or “research sites”)
- **Time quota policy** - users can browse specified categories for a set period per day
- **Selective HTTPS Scanning** – automatically determines which encrypted connections to scan

Web Protection



Site tagging - Tag sites to create unlimited custom categories

SOPHOS UTM 9 | admin | ? | [Refresh] | [Settings]

search Filtering Options

Dashboard | Management | Definitions & Users | Interfaces & Routing | Network Services | Network Protection | **Web Protection** | Web Filtering | Web Filter Profiles | **Filtering Options** | Policy Helpdesk | Application Control | FTP

Exceptions | **Websites** | Bypass Users | PUAs | Categories | HTTPS CAs | Misc

+ New Site...

search Find

Display:

Site	Category	Reputation	Tagged as
macumors.com			Research Sites
wikipedia.org			Research Sites

Edit Filter Action

Categories | **Websites** | Downloads | Antivirus | Additional Options

Block these websites +

Allow these websites +

UTM WebAdmin

Control sites tagged in the Website List

Tags

Research Sites	Allow
DND	DND
DND	DND
DND	DND
DND	DND
DND	DND
DND	DND
DND	DND
DND	DND
DND	DND
DND	DND

<< Back >> Next [Save] [Cancel]

Use tags in policy just like other categories

Web Protection

Web Surfing Quotas

Policy: Select the categories and the time quota...



Edit Filter Action

Categories Websites Downloads Antivirus Additional Options

Name: Teacher Policy

☒ Allow all content, except as specified below
☐ Block all content, except as specified below

☒ Block Spyware infection and communication

Category	Action
Community / Education / Religion	Allow
Criminal Activities	Block
Drugs	Quota
Entertainment / Culture	Allow
Extremistic Sites	Block
Finance / Investing	Quota
Games / Gambles	Block
IT	Quota
Information and Communication	Quota
Job Search	Block
Uncategorized websites	Block

☐ Block websites with a reputation below a threshold of: Unverified

<< Back >> Next [Save] [Cancel]

Edit Filter Action

Categories Websites Downloads Antivirus Additional Options

Enforce Website Protection Features

☐ Google SafeSearch
☐ Bing SafeSearch
☐ Yahoo SafeSearch
☐ YouTube for Schools
School ID:
☐ Enforce allowed domains for Google Apps
Domains:

Quotas

Allowed minutes for all categories and tags included in quota: 60

Network Configuration

Parent Proxies: ☐ Blackwidow

Activity Logging

☒ Log accessed pages
☒ Log blocked pages

<< Back >> Next [Save] [Cancel]

User Experience

SOPHOS UTM 9 <http://www.sophos.com>

Quota time browsing

Browsing to this content is limited by a daily time quota.
You have 60 minutes of time quota remaining today.
Select how much of your quota to use now: 10
Close this tab or browse to a non-restricted site to avoid using your quota now. [Go]

Site: <http://www.absolut.com/ca/>
Report: Restricted Category (Alcohol)

SOPHOS Powered by UTM Web Protection

Helpdesk (Reset if needed)

SOPHOS UTM 9 | admin | [Help] [Refresh] [Settings]

search Policy Helpdesk

Dashboard Management Definitions & Users Interfaces & Routing Network Services Network Protection Web Protection

Policy Test Quota Status

search Find << >>

Display: 10 1-1 of 1

User	Filter Action	Minutes remaining
10.99.115.17	Default content filter action	50

Reset

Web Protection



Site tagging - Tag sites to create unlimited custom categories

Add Site(s)

URLs, domains, IP addresses, or CIDR ranges

tmz.com
facebook.com

☐ Include subdomains

Category
Do not override

Reputation
Do not override

Tags
Website Tags
DND DND DND
DND DND DND
DND DND DND

Comment

✓

Policy Test

Policy Test

Request Details

Destination Domain or URL
http://tmz.com/

Source IP Address
10.108.32.89

User (optional)

Time and day (optional)
☐ 00 : 00 Today

Request URL: http://tmz.com/

Request Time: 28 Aug, 07:56 (PDT)

Result: **Blocked**

Reason: Forbidden tag detected

Tag name: time_waste

URL Category: Entertainment,Blogs/Wiki

URL Reputation: Neutral

Policy name: Base Policy

Test

Web Protection

Selective HTTPS scanning – Increase privacy, only scan risks



SOPHOS UTM 9

| admin | ? C ⚙

HTTP

Web Filtering

Tags Research Sites

Global HTTPS Policies

HTTPS Scan Settings

Use this tab to configure how Web Filtering handles HTTPS traffic. To avoid browser warnings when using Decrypt and Scan, ensure the HTTPS Certificate Authority is deployed to end users.

☐ URL filtering only

☐ Decrypt and scan

☒ Decrypt and scan the following:

Scan these tagged websites

Research Sites

DND DND DND DND

DND DND DND DND

DND DND DND DND

DND DND DND DND

DND DND DND DND

DND DND DND DND

DND DND DND DND

Scan these categorized websites

Anonymizers

Anonymizing Utilities

Browser Exploits

Categorization Failed

Hacking/Computer Crime

Illegal Software

Malicious Downloads

Malicious Sites

Media Downloads

Media Sharing

☐ Do not proxy HTTPS traffic in Transparent Mode

Web Protection

Other noteworthy features



- **True File Type Detection** – can block archives based on the files they contain
- **Performance Improvements** – proxy optimizations resulting in 20% performance improvement and 75% memory reduction

Web Protection



Application control news

- **Updated App Control engine**
- broader app coverage (1300 Apps)
- No visible changes in Webadmin GUI
- AppControl now provides IPv6 Support
- Database upgraded from NAVL 3.x to Version 4.x
- NAVL 4.x: provides ability for quicker App pattern updates

Web Protection



Demo

Email Protection

What's new?

Email Protection

Improved SPX usability



- Adding attachments in the reply portal
- SPX recipient self-registration

Email Protection

SPX reply portal attachments



UTM SPX Email reply

From:
To: Employee <employee@example.com>
Subject: Re: Legal document

Hello mr. Employee,

Of course I can thanks to Sophos UTM with SPX encryption.
I will attach it to this message.

Yours faithfully,

Corporate Lawyer|

-----Original Message-----

From: lawyer@external.com
Sent: Wed, 04 Feb 2015 16:56:55 +0100
To: employee@example.com
Subject: Legal document

Hello mr. Lawyer,

Can you please send me the documents in a secure fashion?
I'd hate for our competitors to see these.

Best regards,

Employee

Send

Attachments



UTM SPX Email reply

Select attachment

Browse...

Upload

Attachments

Done

Delete

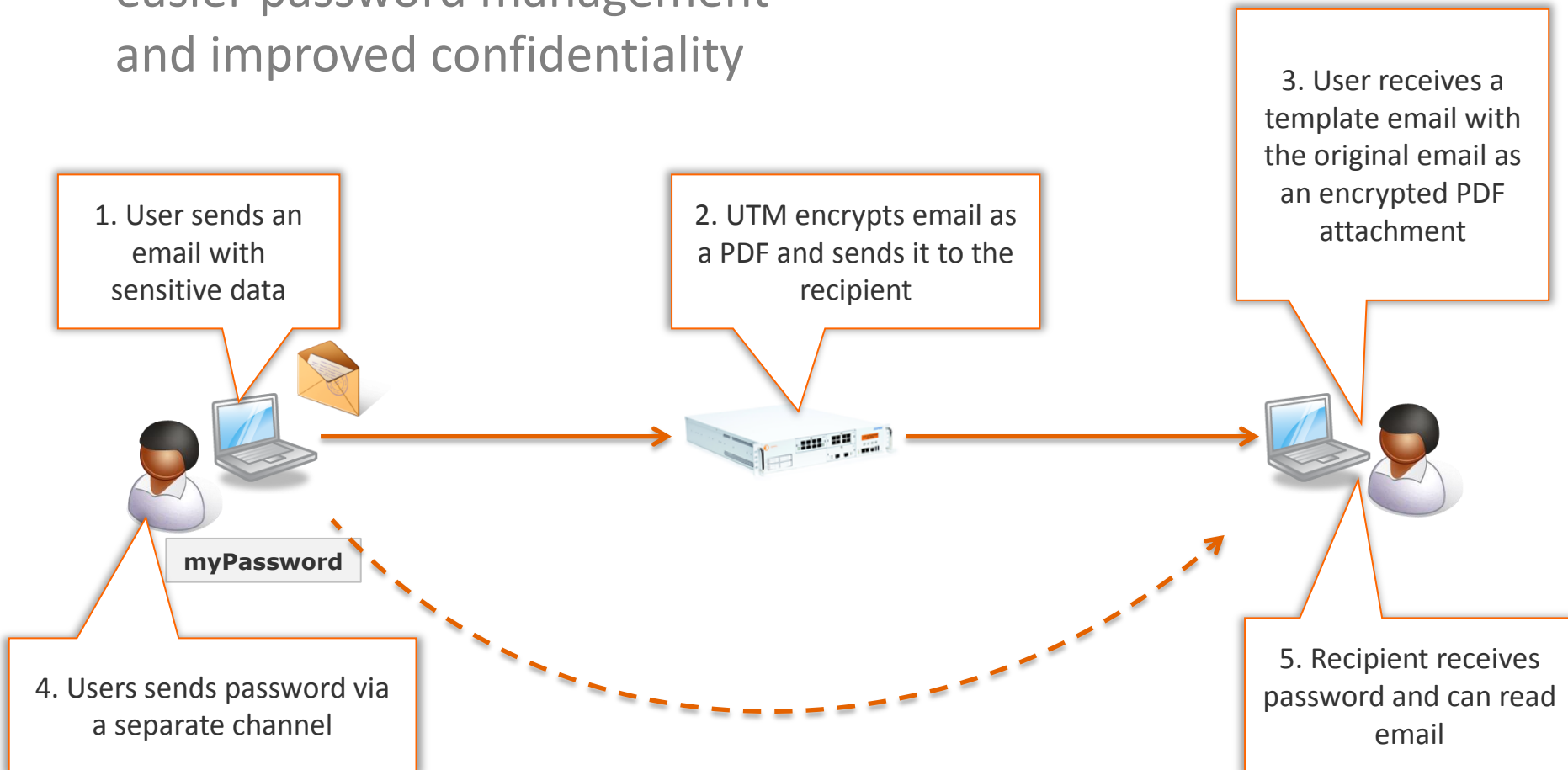
☐ Legal document.docx (16077 byte)

Email Protection

SPX recipient registration



- Recipient self registration for easier password management and improved confidentiality

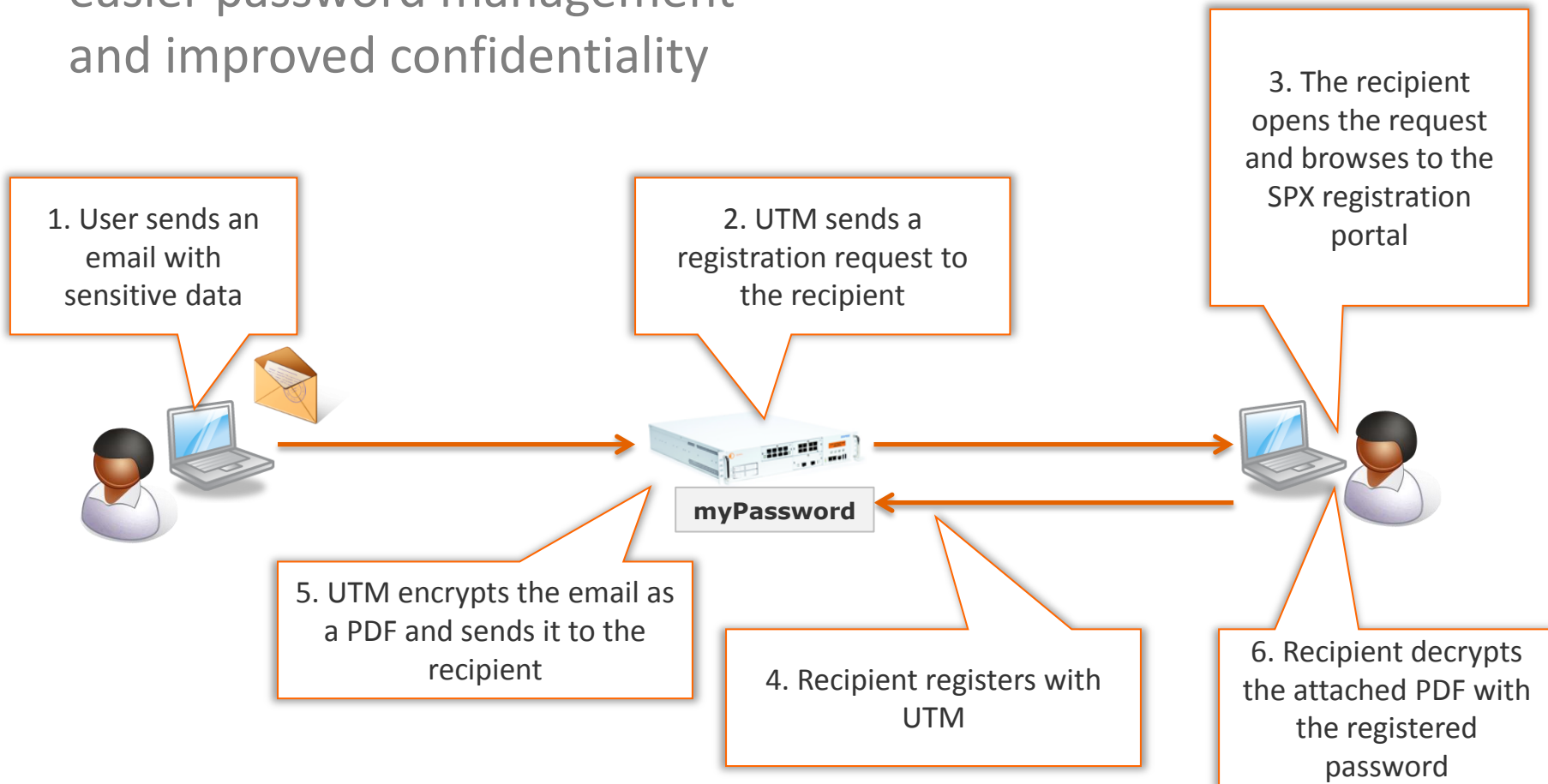


Email Protection

SPX recipient registration



- Recipient self registration for easier password management and improved confidentiality





Demo

Web Server Protection

What's new?

Web Server Protection

Improved compatibility, easier deployment



- NTLM support
- Reverse authentication UI update
- Authentication pre- and suffixing
- Improved exceptions
- Access control
- Scan size limits

Web Server Protection

NTLM support



- NTLM hashes and sessions are now recognized by the WAF and sent to the backend servers unchanged
 - Prevents “session clash” behavior previously present in UTM
 - Enables the use of NTLM based SSO with multiple backend systems (for example Microsoft Sharepoint)
 - Not supported as a reverse authentication delegation method

Web Server Protection

Reverse authentication UI update



Create Authentication Profile

Name:

Frontend mode:

Frontend realm:

Backend mode:

Users / Groups

DND	DND	DND	DND	DND
	DND	DND	DND	DND
DND	DND	DND	DND	DND
	DND	DND	DND	DND
DND	DND	DND	DND	DND
	DND	DND	DND	DND

Comment:

Advanced

Enable Session Timeout: ☒

Session Timeout:

Session Timeout Scope:

Limit Session Lifetime: ☒

Session Lifetime:

Session Lifetime Scope:

☒ Save ☐ Cancel



Add Authentication Profile

Name:

Virtual Webserver

Mode:

Users / Groups

DND	DND	DND	DND
	DND	DND	DND
DND	DND	DND	DND
	DND	DND	DND
DND	DND	DND	DND
	DND	DND	DND

Real Webserver

Mode:

User Session

Session Timeout: ☒

Limit to:

Session Lifetime: ☒

Limit to:

Comment:

☒ Save ☐ Cancel

Web Server Protection



Reverse authentication UI update

- “Frontend realm” and „cookie encryption secret” are removed from Webadmin
 - Automatically generate with a random string
 - Old values are reused during upgrade
- „Frontend Realm” field renamed to „Basic Prompt” for HTTP Basic Authentication
 - Old „frontend realm” value retained during upgrade

Virtual Webserver

Mode:

Basic prompt:

Web Server Protection

Authentication pre- / suffix



- Allows administrators to add information to login credentials used in reverse authentication
 - Both prefixing (“domain\username”) and suffixing (“username@domain”) can be used to solve default domain issues
 - Both methods can even be combined if required
- Simplifies deployments and changes required to backend systems

Add Authentication Profile

Name: Forms + basic passthrough

Virtual Webserver

Mode: Form

Form Template: Default Template

Users / Groups

Domain Members				
DND	DND	DND	DND	DND
DND	DND	DND	DND	DND
DND	DND	DND	DND	DND
DND	DND	DND	DND	DND

Real Webserver

Mode: Basic

User name affix: Prefix & Suffix

Prefix: None

Suffix: Prefix & Suffix

User Session

Session Timeout: ☒

Limit to: 5 Minutes

Session Lifetime: ☒

Limit to: 8 Hours

Web Server Protection

Improved exceptions

- Wildcards can be added anywhere in an exception path to simplify exceptions
- Accept unhardened form data
 - Previously, a missing FH token would result in a blocked request
 - Located under „Advanced“
 - Requires „Skip Form Hardening“ to be effective
 - Not enabled by default nor on upgrade



For all requests

Web requests matching this path

Paths

/example */index.html

and

Comment:

☒ **Advanced**


☒ Never change HTML during Static URL Hardening or Form Hardening

☒ Accept unhardened form data

Web Server Protection

Access control

- Limit or grant access to websites and site paths based on the source network of the request
 - Enabled by checkbox “Access control” in Site Path Route form
 - Allow access for IP addresses listed in “Allowed networks” (filled with “Any” network object by default)
 - Deny access for IP addresses listed in “Denied networks” (empty by default)
 - Deny access for any network not listed in “Allowed networks”



Edit Site Path Route

Name: /

Virtual Webserver: Example

Path: /

Reverse Authentication: :: No Profile ::

Real Webservers

1 ☒ Webserver #1 enabled

☒ Access control

Allowed networks

Any

DND	DND	DND	DND
DND	DND	DND	DND
DND	DND	DND	DND
DND	DND	DND	DND

Denied networks

1.2.3.0 /24

DND	DND	DND	DND
DND	DND	DND	DND
DND	DND	DND	DND
DND	DND	DND	DND

Comment:

Web Server Protection



Access control

- Client access is denied with “403 Forbidden” HTTP status code
- Log entries if access is denied:
2014:10:06-09:07:07 ... [authz_core:error]
... AH01630: client denied by server
configuration ...
2014:10:06-09:07:07 ... statuscode="403" ...

Web Server Protection

Scan size limit

- Scan size limit determines the maximum size of a transaction (upload/download) in a session
- Prevents timeouts due to predetermined limit found in 9.2

A screenshot of a web application security configuration window. The window has a light gray background and a thin border. It contains several settings: 'Cookie Signing' (unchecked), 'Static URL Hardening' (unchecked), 'Form Hardening' (unchecked), 'Antivirus' (checked), 'Mode' (dropdown menu set to 'Single Scan'), 'Direction' (dropdown menu set to 'Uploads only'), 'Block unscannable content' (checked), 'Limit scan size' (checked), 'Megabytes' (text input field containing '1024'), and 'Block clients with bad reputation' (unchecked). Below these is a 'Comment' text area. At the bottom, there is a section titled 'Threat Filter Categories' with a plus icon. At the very bottom right, there are two buttons: 'Save' with a green checkmark and 'Cancel' with a red X.

Web Server Protection



Scan size limit

- Multi-file upload:
 - Limit applies to complete upload request, not to individual files
 - Some files may get not (or only partly) scanned
- Enable log level info for mod_avscan to get feedback that limit is effective:

```
2014:10:06-11:12:25 ... [avscan:info] ... bypassing upload  
check after 2103915 bytes: size limit 2097152 reached ...
```

Wireless Protection

What's new?

Wireless protection

Better hotspots, better coverage



- Hotspot improvements
- Periodic scanning
- 802.11r Fast Roaming
- Various other enhancements

Wireless Protection

Hotspot improvements

- HTTPS support added for hotspot login page
- Customizable portal hostname
- Per hotspot administrative rights management



Add Hotspot

Name:

Interfaces:

Internal	DND	DND	DND
	DND	DND	DND
	DND	DND	DND

Administrative Users:

admin	DND	DND	DND
	DND	DND	DND
	DND	DND	DND

☒ Redirect to HTTPS

Hostname type:

Hostname:

Wireless Protection

Periodic scanning and 802.11r Fast Roaming



- Sophos UTM can now periodically scan the 2.4 and 5 GHz frequency band and select the optimal channel dynamically.
 - This improves coverage
 - Reduces noise and channel overlap
 - And boosts performance
- 802.11r Fast Roaming was added to 9.3 to reduce the station handoff delay to 3 ms
 - Real world full station to station roaming time is now less than 0.5 seconds

Advanced

Channel 2.4 GHz: Auto
Dyn Chan: ☒
Time-based scan: ☒

Select Scan-Time: +

<input checked="" type="checkbox"/>	Nighttime
<input type="checkbox"/>	Work hours
<input type="checkbox"/>	Lunch
<input type="checkbox"/>	Weekend

TX Power 2.4 GHz: 100%
Channel 5 GHz: Auto
Dyn Chan: ☒
Time-based scan: ☒

Select Scan-Time: +

<input checked="" type="checkbox"/>	Nighttime
<input type="checkbox"/>	Work hours
<input type="checkbox"/>	Lunch
<input type="checkbox"/>	Weekend

TX Power 5 GHz: 100%
STP: Disabled



Demo

Various other improvements

Various other improvements



Better compatibility and remote support

- **Hyper-V 3.5** – adds support for Microsoft Hyper-V Server 2012 R2 including MS Integration Tools v3.5 which will add HA/LB to Hyper-V
- **Remote Assistance In-a-Click** – enables webadmin access to the UTM by Sophos Support with the click of a single button

New hardware

New Hardware

New desktop SG models – with built-in wireless technology

- 4 new models (SG 105/115/125/135)
 - Newest Intel technology (two platforms)
 - 2-3x performance increase
 - SG105/115: Intel Baytrail, 4 ports
 - SG125/135: Intel Rangeley, 8 ports
- Also available with integrated wireless
 - SG 105w/115w: 4 ports plus Integrated wireless
 - SG 125w/135w: 8 ports plus Integrated wireless
 - Can be extended with Sophos APs

SG 1xx Series

Tech Specs

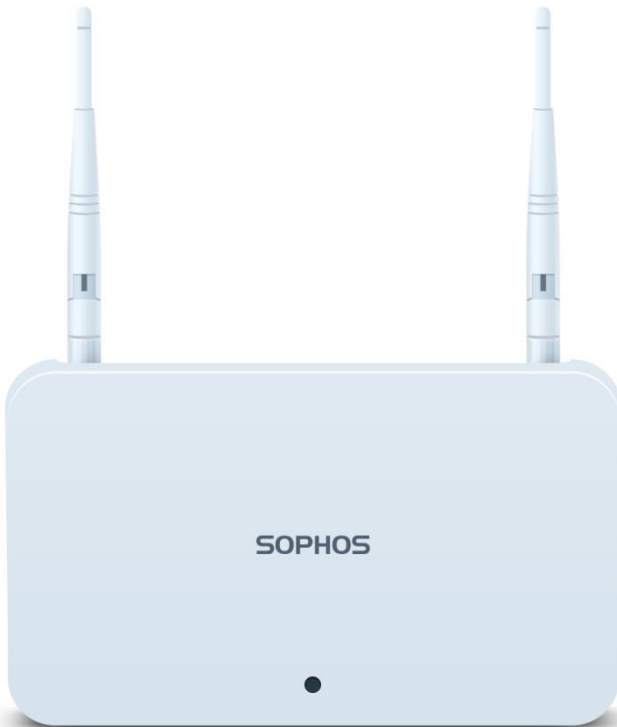
Model	Base model	CPU	Cores	GHz	RAM	Disks	GE Ports	Wireless card (on „w“ model)	other
SG105 SG105w	Nexcom DNA 120	Baytrail E3826	2	1.46	2	320 GB HDD	4	802.11 a/b/g/n 3x3 MIMO, Dual Band	fanless
SG115 SG115w	Nexcom DNA 120	Baytrail E3827	2	1.75	4	320 GB HDD	4	802.11 a/b/g/n 3x3 MIMO, Dual Band	fanless
SG125 SG125w	Nexcom DNA 1150	Rangeley C2358	2	1.7	4	320 GB HDD	8	802.11 ac/b/g/n (no DFS) 3x3 MIMO, Dual Band	Intel QuickAssist support
SG135 SG135w	Nexcom DNA 1150	Rangeley C2558	4	2.4	6	320 GB HDD	8	802.11 ac/b/g/n (no DFS) 3x3 MIMO, Dual Band	Intel QuickAssist support

All models:

- 2* USB 2.0 ports
- 1* VGA port
- 1*RJ45 console port

New Hardware

AP15



New Hardware

AP15, successor to AP10

- Form factor: desktop (plus wall-mount option)
- Number of radios: 1
- WLAN-Standard: 802.11 b/g/n 2.4 GHz
- Max. WiFi performance: 300 Mbps
- MIMO: 2x2:2
- Antennas: 2 x external (omni-directional)
- PoE: 802.3af
- Ethernet: 1 x 10/100/1000

New Hardware

AP100 Desktop



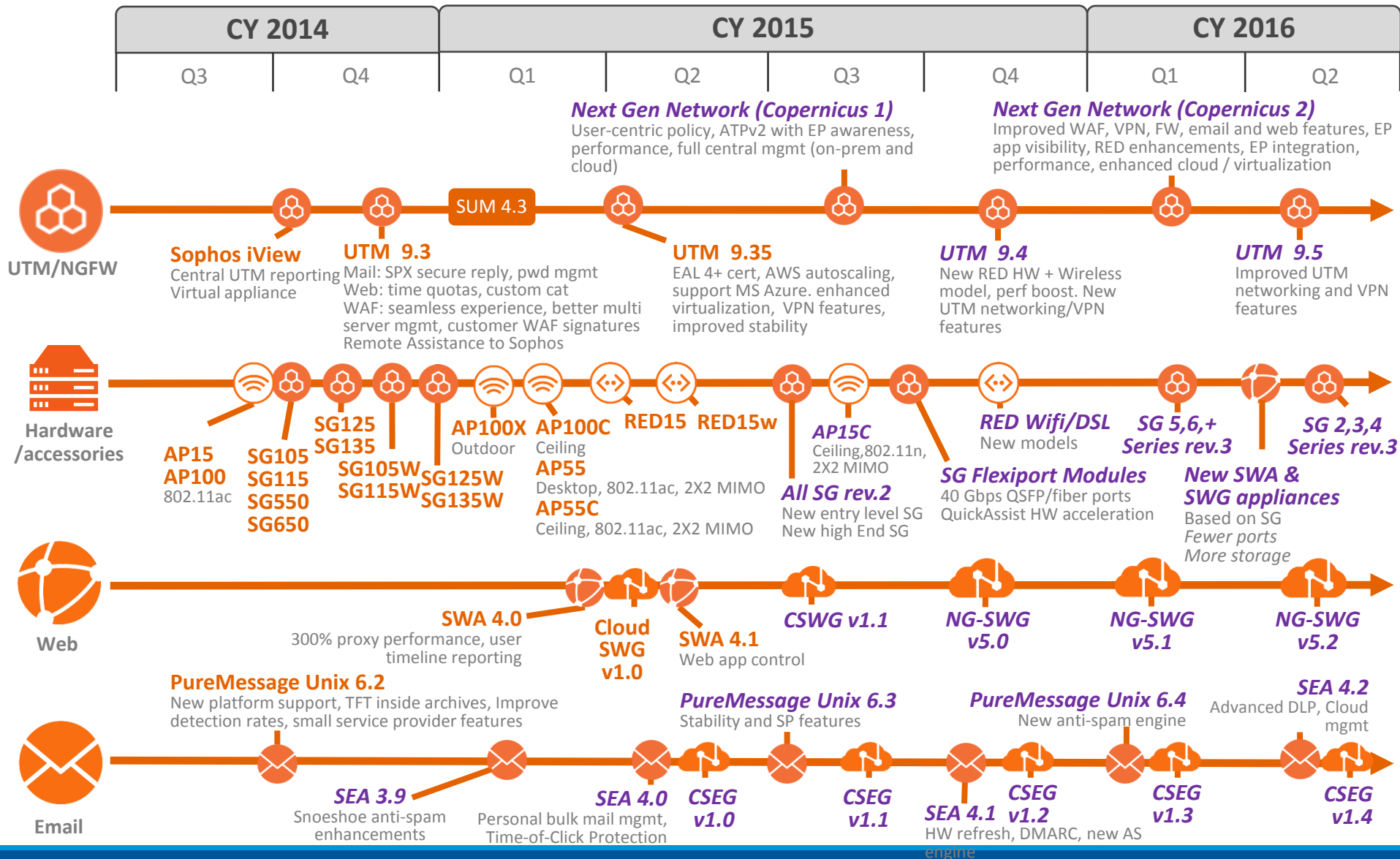
New Hardware

AP100, new top of the line AP

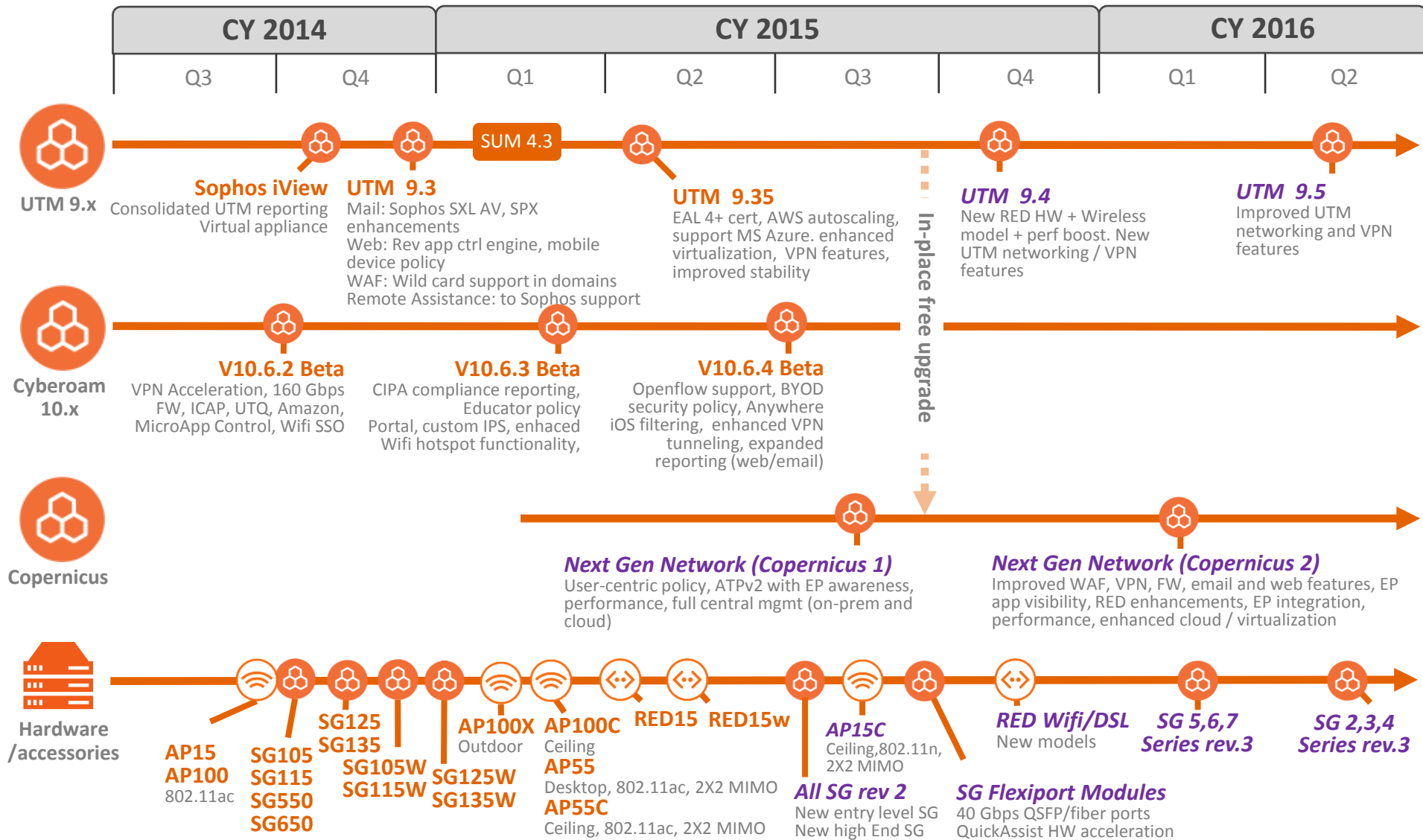
- Form factor: desktop (plus wall-mount option)
- Number of radios: 2
- WLAN-Standard: 802.11 a/b/g/n/ac 2.4 GHz and 5 GHz
- Max. WiFi performance: 1.3 Gbps
- MIMO: 3x3:3
- Antennas: 3 x external (RP-SMA)
- PoE: 802.3at
- Ethernet: 1x10/100/1000
- Console: 1 x RJ45 console port
- USB: 1 x USB port

Roadmap Update

Network Security Roadmap



UTM/NGFW Roadmap



Next Gen Network: Codename Copernicus



We're building our next generation operating system

To be released in 2015 a joint Sophos and Cyberoam development that blends the best of both products to create a new software platform for the future that will enhance protection, performance and user experience for both Cyberoam and Sophos customers



Sophos customers and partners will benefit at a time of their choosing

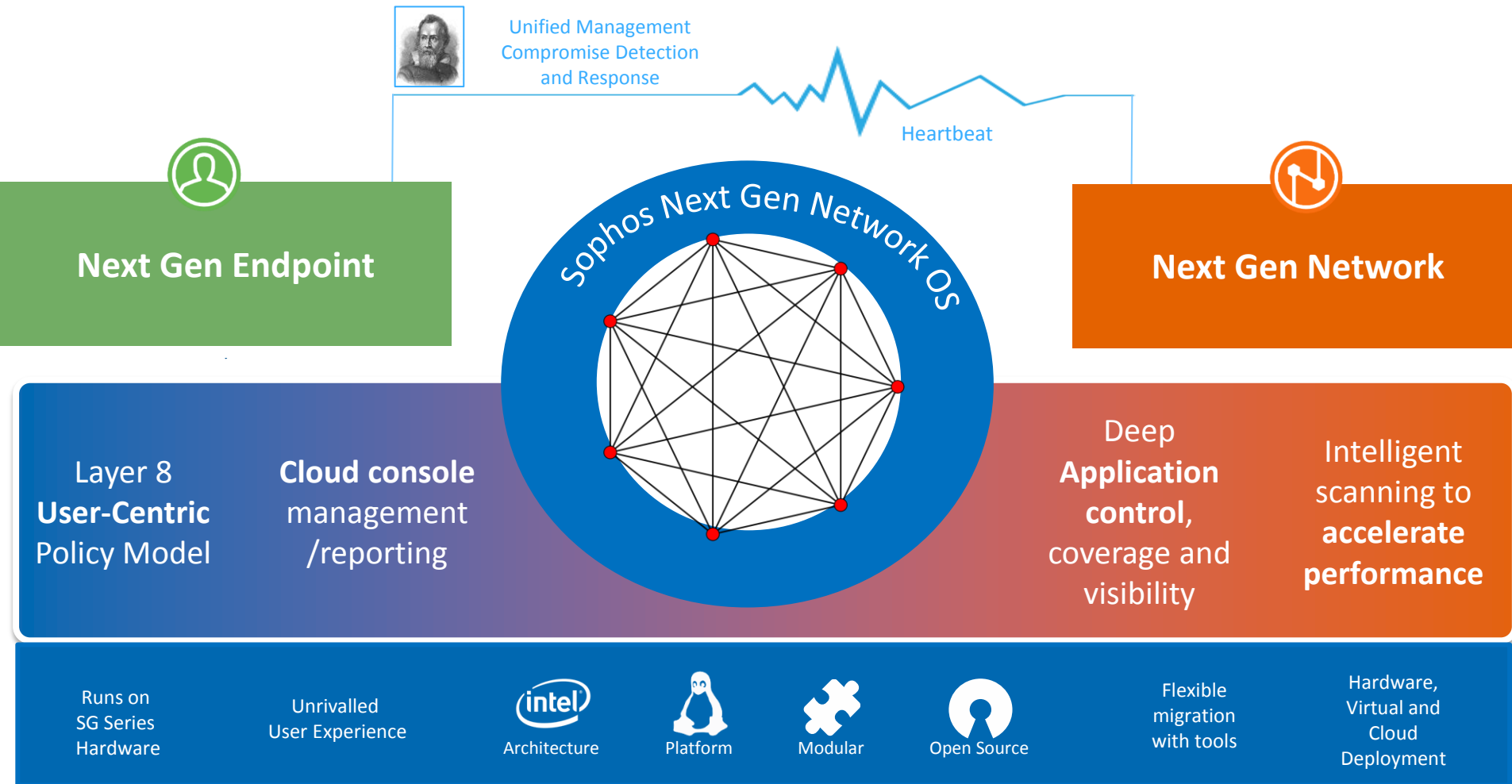
A carefully planned transition will enable customers and partners to move at the right time for them and let them run our new firewall operating system on today's Sophos SG Series appliances



We'll continue to improve both existing product sets in parallel

Sophos UTM will continue to receive investment for years to come and will be available alongside our new firewall operating system

Next Gen Network: Codename Copernicus



Questions?

Presales-NEEMEA@Sophos.com

SOPHOS