



Sophos Firewall v19.5 What's New

Aleš Kotmel

22-06-2023

SOPHOS

Sophos Firewall and Network Security Focus

Creating New Opportunities with Distributed and Enterprise Edge – Building-out SASE



HIGH AVAILABILITY

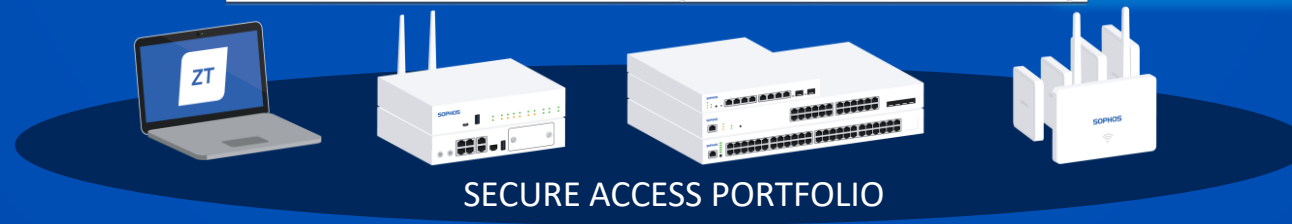
XSTREAM TLS INSPECTION



XSTREAM SD-WAN AND ROUTING



ZTNA as a Service



SECURE ACCESS PORTFOLIO

All While Making Complex Networks Easy to Deploy and Manage

A Key Part of our SASE Strategy



CONNECT ANYWHERE ANYHOW

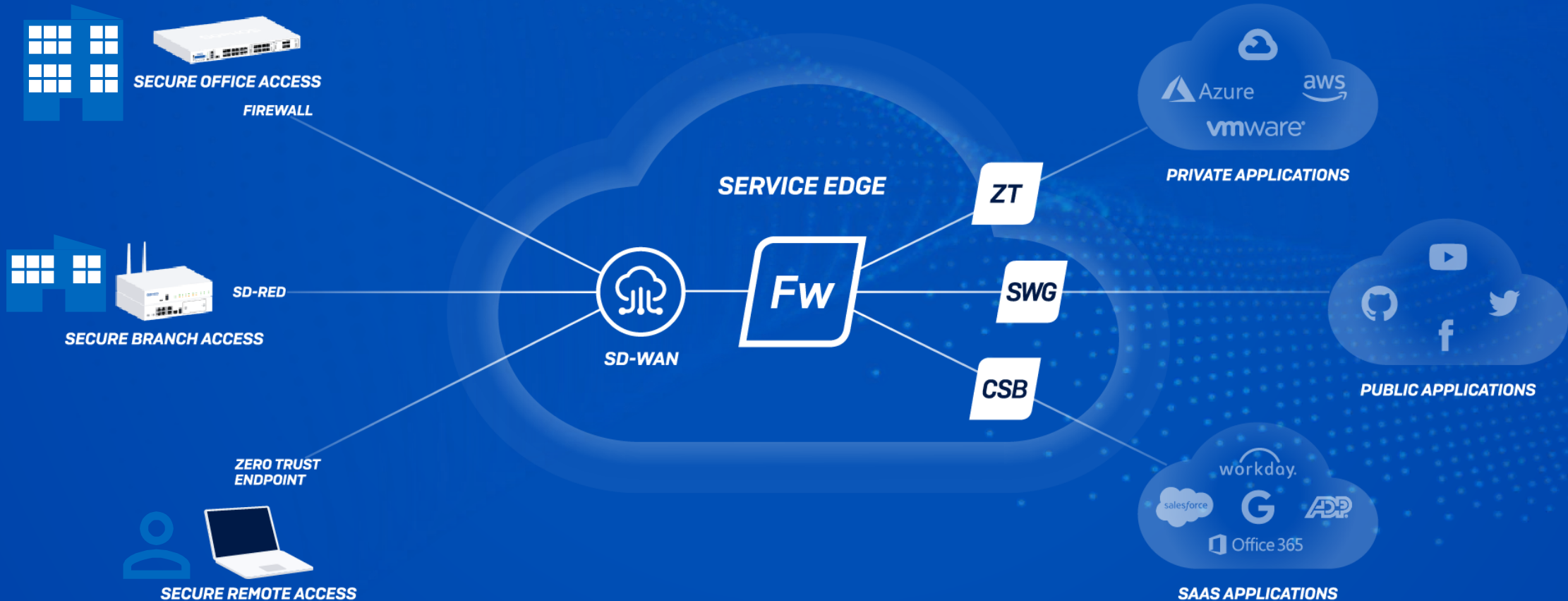
ZERO TRUST - XSTREAM SD-WAN
(SD-WAN | SD-RED | ZTNA | VPN)

SET POLICY ONCE - ENFORCE EVERYWHERE

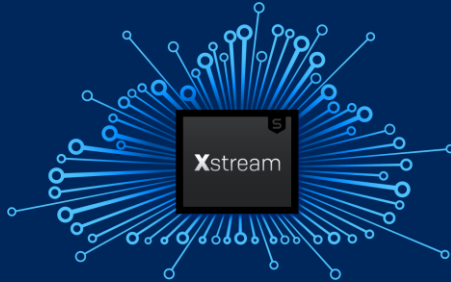
UNIFIED POLICY WITH INTELLIGENT ENFORCEMENT
(CLOUD | FW | EP)

POWERFUL PROTECTION

CROSS-PRODUCT THREAT DETECTION AND RESPONSE
(IDENTITY, POSTURE, SHADOW IT, THREATS)



Sophos Firewall OS v19 and 19.5



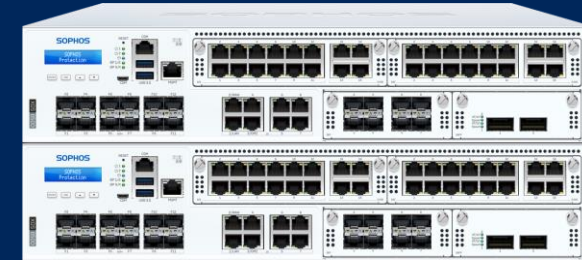
v19

Xstream SD-WAN

- Xstream FastPath for IPsec (Up to 5x IPsec throughput)
- SD-WAN profiles
- Performance-based link management
- Real-time monitoring
- SD-WAN log viewer module

VPN and Search

- SSL VPN capacity boost
- SSL remote-access assistant
- AWS VPC import
- Intuitive VPN management
- VPN log viewer module
- Navigation Search
- Network object search
- And more!



v19.5

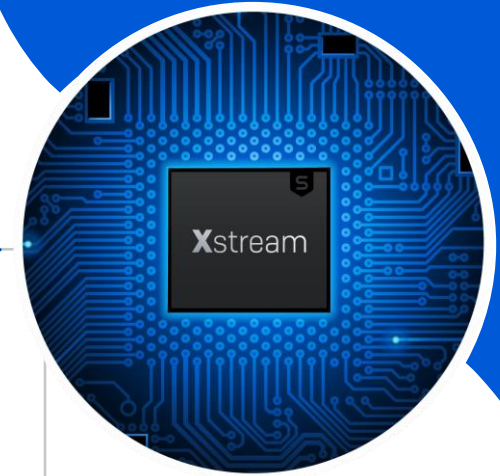
Xstream Performance

- Xstream TLS FastPath Offload
- Increased IPsec throughput and capacity
- SD-WAN load balancing
- New dynamic routing engine
- OSPFv3 dynamic IPv6 routing
- New search for Hosts and Services objects





High Availability

- Redundant HA links (Multiple, LAG, VLAN)
- VLAN interface monitoring
- Enhanced status
- New HA widget
- Custom node names

Sophos Firewall OS v19.5 – What's New



Now in
Early Access

-  Xstream Protection
-  SD-WAN and Routing
-  High Availability Enhancements
-  Quality of Life Improvements

Xstream Protection

- **TLS FastPath** – utilizing the Xstream Flow Processors in select XGS Series appliances to accelerate TLS traffic decryption for improved performance (XGS 4300, 4500, 5500, 6500)

SD-WAN and Routing

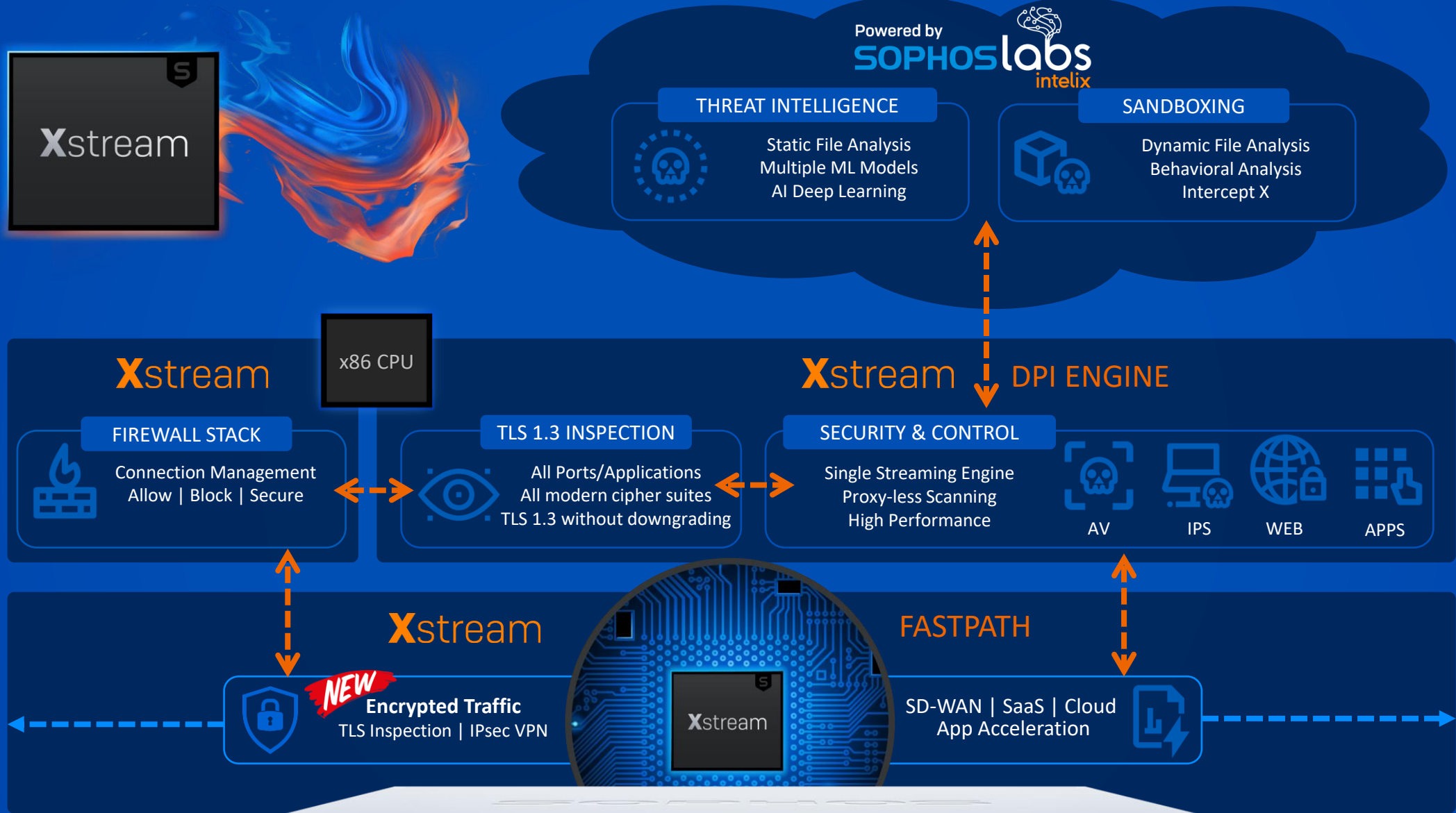
- **SD-WAN Load Balancing** – across multiple SD-WAN links for maximum performance
- **Double IPsec capacity** – with current tunnel support now at 10,000 up from 4,650
- **Dynamic Routing** – with OSPFv3 (IP6) support and a new next-gen routing engine

High Availability Enhancements

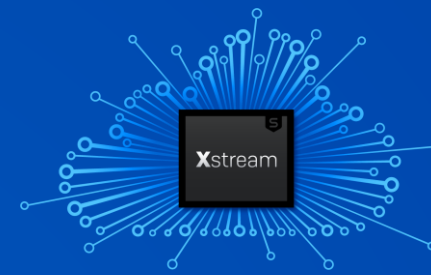
- **Status and Visibility** – with a new control center widget, enhanced status panel, and new node names for easy device identification
- **HA Link Redundancy** – supports up to 4 links for added redundancy
- **VLAN Support Enhancements** – for the dedicated HA link and VLAN interface monitoring

Quality of Life Improvements

- **Hosts and Service Object Search** – using free text
- **Enhanced .log File Storage** – for better troubleshooting
- **Azure AD SSO** – for web console UI login authentication
- **Enhanced 40G Interface Support** – including auto-detection of advanced port configurations and breakout of 40G interfaces

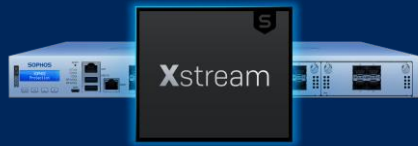


Xstream SD-WAN



SOPHOS FIREWALL SD-WAN HARDWARE

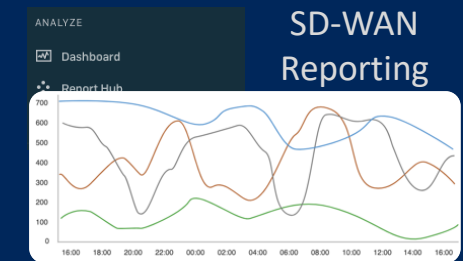
SOPHOS CENTRAL SD-WAN MANAGEMENT



Sophos Firewall XGS Series
Xstream FastPath Acceleration
SD-WAN | Apps | Cloud | IPsec



SD-RED 20/60
Zero-Touch Remote Edge Devices



XSTREAM SD-WAN IN SOPHOS FIREWALL OS



Performance SLA Link Selection
Jitter | Latency | Packet Loss
Zero-Impact Transitions



Link Management and Enhanced Routing
App | User | Service
Failover | Failback



Real-time Monitoring and Logging
Link Performance | Routing



SD-WAN Profiles with Multiple Gateways
Up to 8 Gateways



Link Load Balancing
Simultaneously routing of application traffic across multiple links
MPLS | WAN | VPN | RED



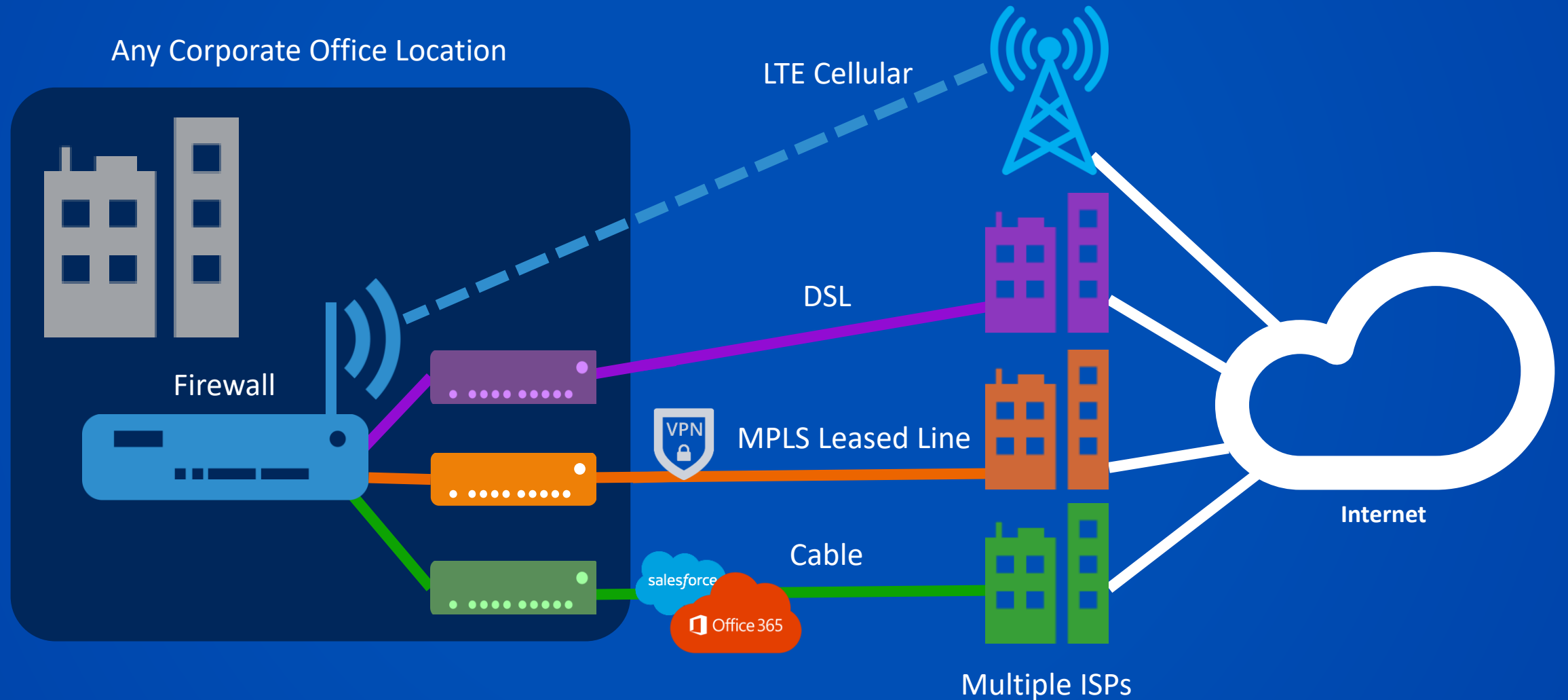
Synchronized App Control Awareness
Obscure and Custom Apps



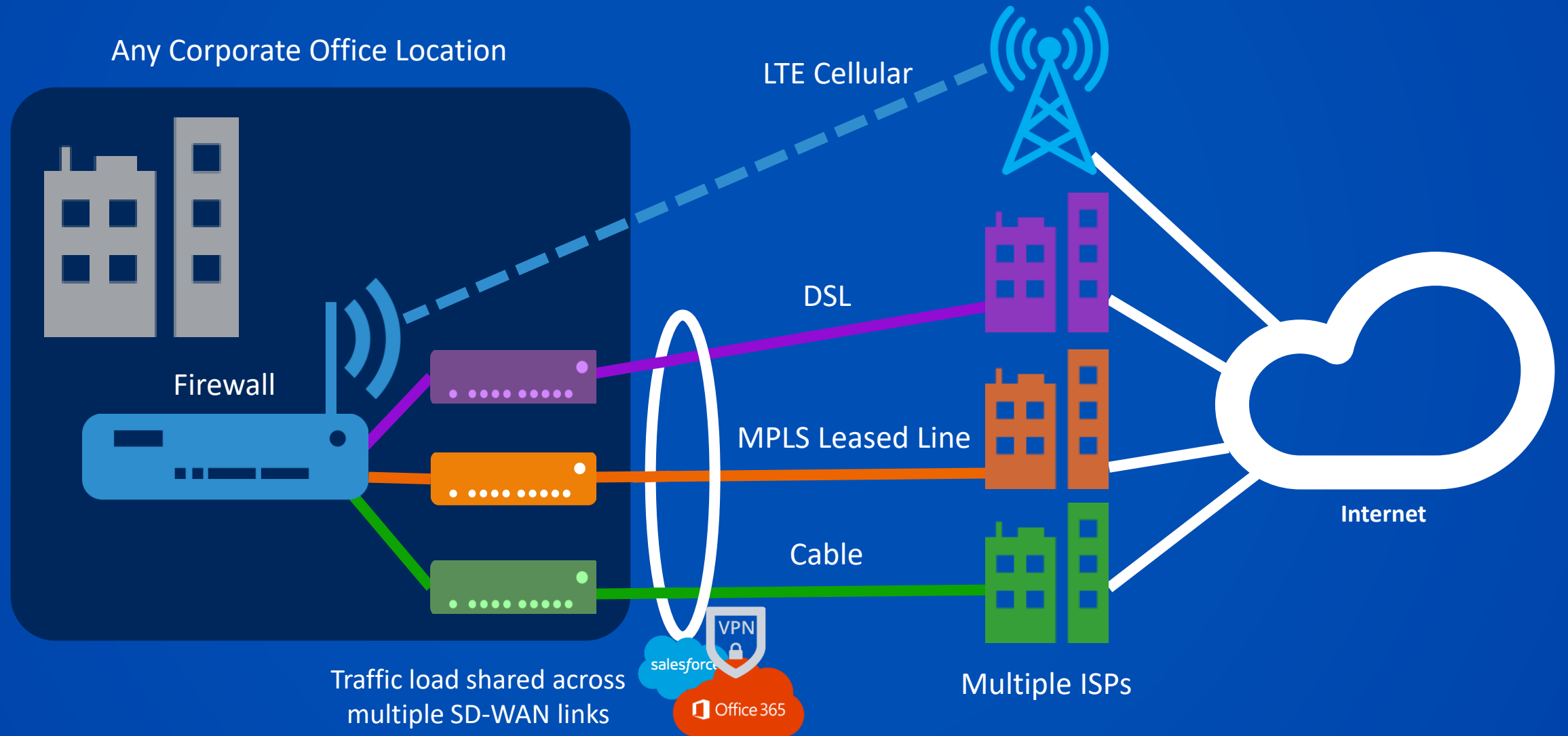
Azure Virtual WAN Support



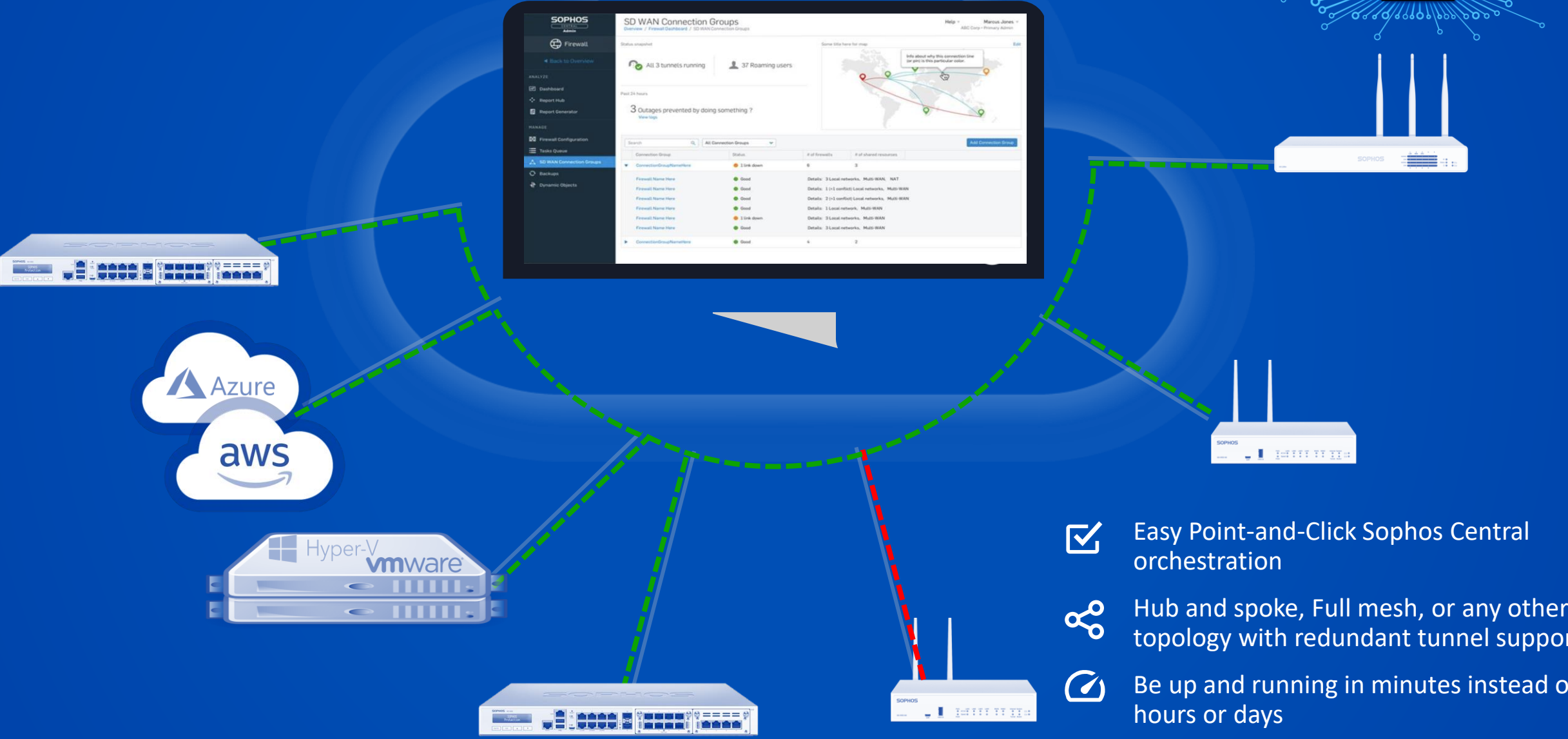
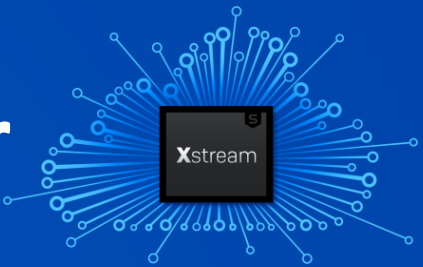
SD-WAN Example



SD-WAN Load Balancing



Central SD-WAN Orchestration – A Game Changer



- ✓ Easy Point-and-Click Sophos Central orchestration
- 🔗 Hub and spoke, Full mesh, or any other topology with redundant tunnel support
- 🕒 Be up and running in minutes instead of hours or days

SD-WAN LOAD BALANCING STATUS, LOGGING, REPORTING

Name: Load balance **Load balancing:** Round-robin
Probe target: 192.168.110:0 (Ping) **SLA strategy:** Custom SLA

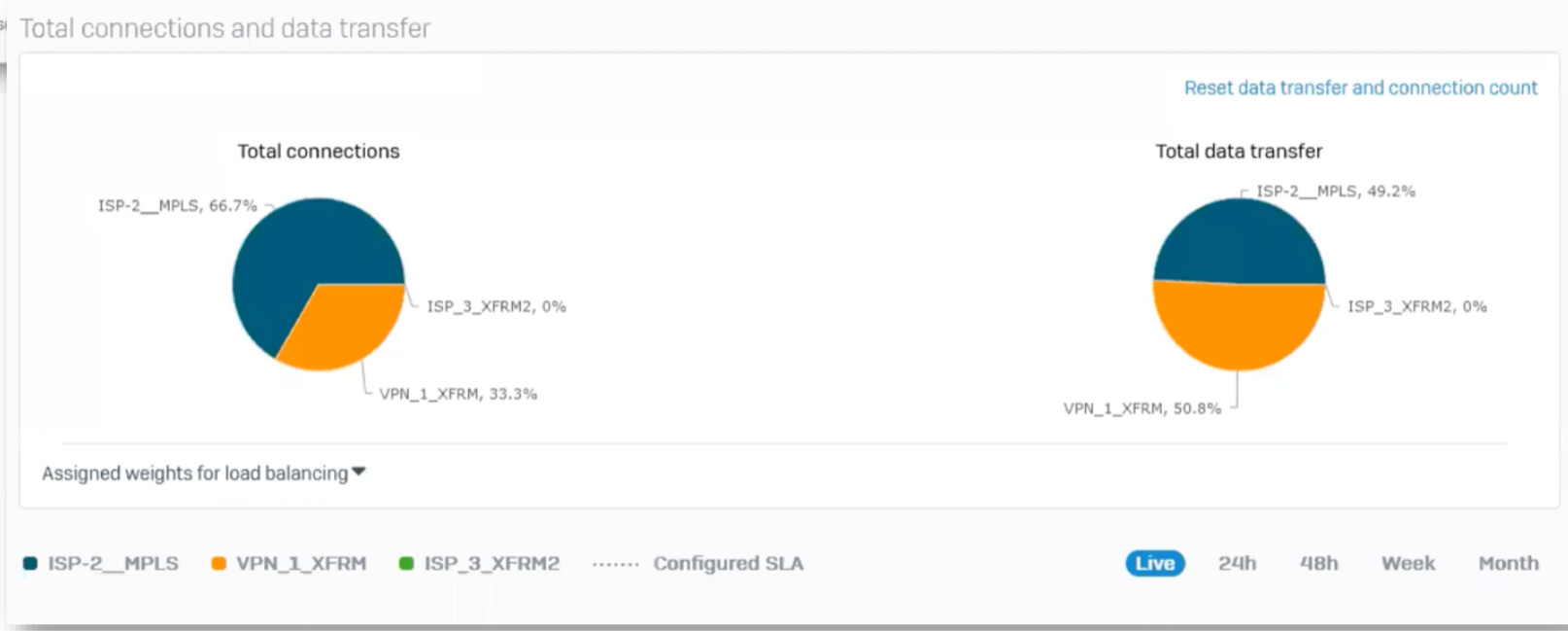
Gateways	Status	Latency	Jitter	Packet loss
ISP-2_MPLS (11111111)	✓	1 ms	0 ms	0 %
VPN_1_XFRM (111.2)	✓	1 ms	0 ms	0 %
ISP_3_XFRM2 (192.168.29.1)	●	-	-	100 %

✓ In use ● Available ● Unavailable ✓ In use

Log viewer

Filter: No filter active Add filter Timer filter Reset

Time	Message ID	Log comp	Log subtype	Status	SD-WAN profile	Gateway	Message
2022-09-21 15:03:40	19023	Profile	Health check	SLA met	Load balance	VPN_1_XFRM	SLA met for gateway 'VPN_1_XFRM' (1.1.1.2) using probe target '192.168.110'
2022-09-21 15:03:39	19023	Profile	Health check	SLA met	Load balance	ISP-2_MPLS	SLA met for gateway 'ISP-2_MPLS' (11111111) using probe target '192.168.110'
2022-09-21 15:03:38	19021	Profile	Health check	Available	Load balance	ISP-2_MPLS	Gateway 'ISP-2_MPLS' (11111111) available. Probe protocol 'PING' probe to '192.168.110' successful
2022-09-21 15:03:37	19021	Profile	Health check	Available	Load balance	VPN_1_XFRM	Gateway 'VPN_1_XFRM' (1.1.1.2) available. Probe protocol 'PING' probe to '192.168.110' successful



New Dynamic Routing Engine with OSPFv3 (IPv6) support

- Static routing enhanced with admin distance and metric
- Better dynamic routing decisions based on interface/bandwidth
- Improved scalability and performance
- Better logging and troubleshooting
- Fully interoperable with other vendors

The screenshot displays the Sophos Firewall web interface. At the top, there is a navigation bar with the Sophos logo and a search bar. Below this is a sidebar menu with categories: MONITOR & ANALYZE (Control center, Current activities, Reports, Zero-day protection, Diagnostics), PROTECT (Rules and policies, Intrusion prevention, Web, Applications, Wireless, Email, Web server, Advanced protection), and CONFIGURE (Remote access VPN, Site-to-site VPN, Network, Routing, Authentication, System services). The 'Routing' section is selected in the sidebar. The main content area shows the 'Routing' configuration page for OSPFv3. It includes a breadcrumb trail: SD-WAN routes > SD-WAN profiles > Gateways > Static routes > BGP > OSPF > OSPFv3 > Information > Upstream proxy. The 'Global configuration' section contains the following settings: Router ID (1.1.1.1), Default metric (0), ABR type (Standard), Auto-cost reference-bandwidth (100000), Default-information originate (Never selected), Redistribute connected (Enable checked), and Metric type (External type 2). An 'Apply' button is visible at the bottom of the configuration area.

High Availability Enhancements in v19.5

Redundant HA Links

Use multiple links, LAG, or VLAN to provide added redundancy

Enhanced Status

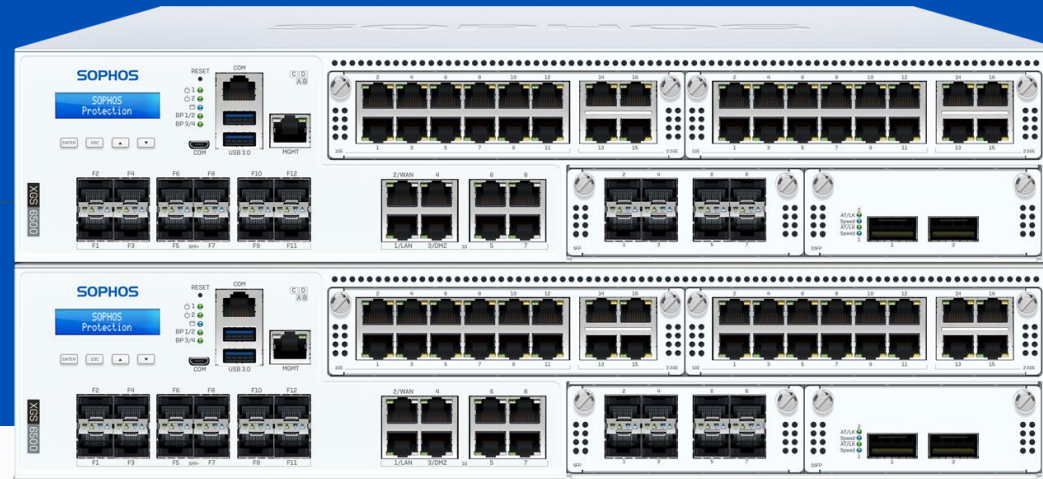
New HA status and widget provides clear insights at-a-glance

Custom Node Names

Provide unique names for each node to better identify them

VLAN Monitoring

Adds VLAN interface monitoring



High availability status

HA Connected (Active-Passive)
HA nodes are connected and fully functional.

Node name	Serial number	Current role	Current status	Last status change
Node1 (Local) Initial primary. Holds license for cluster.	SFDemo-c07-kabir-vm-21	Primary <i>i</i>	Active	03:54:58 AM, Apr 08, 2022
Node2 (Peer)	SFDemo-c07-kabir-vm-22	Auxiliary	Passive	03:54:39 AM, Apr 08, 2022

Sync auxiliary device

Disable HA

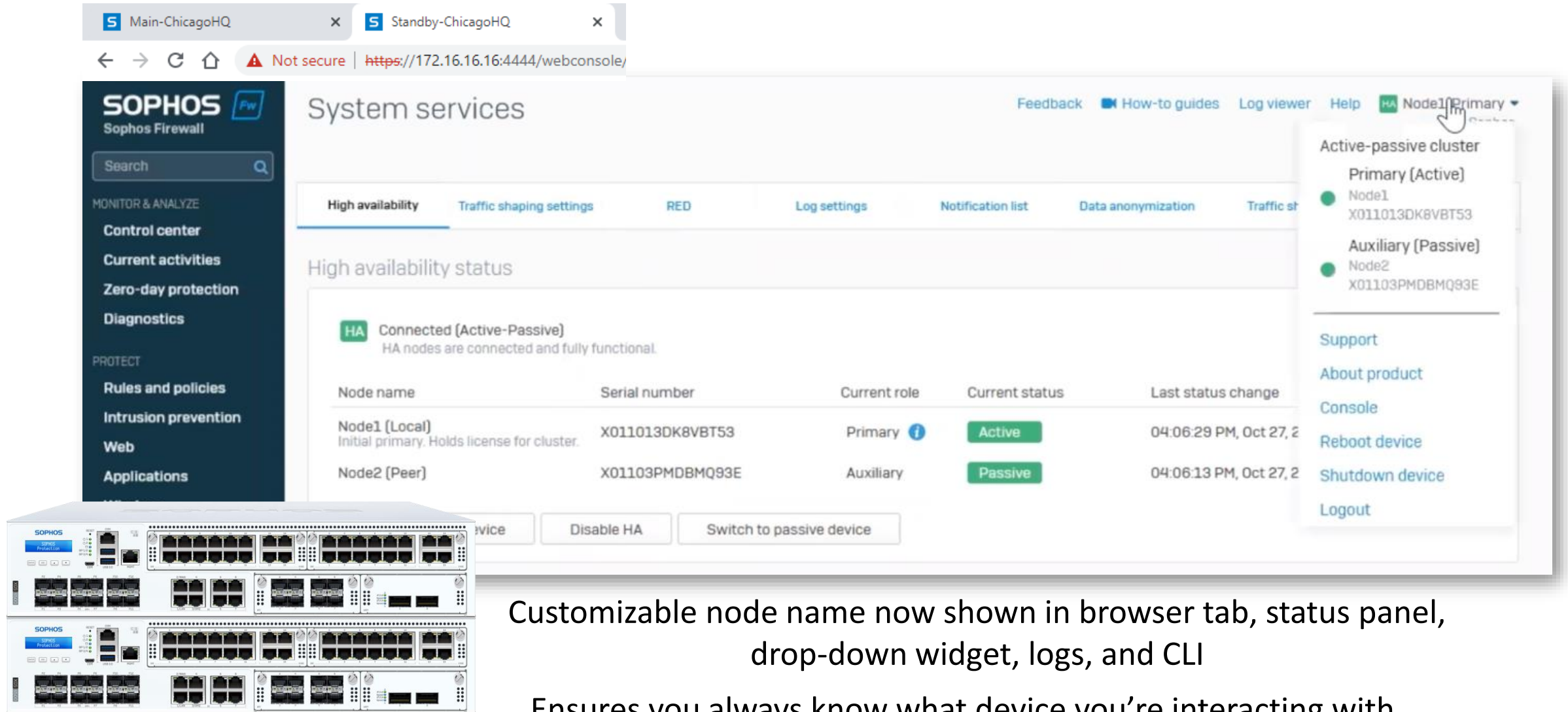
Switch to passive device

Sync auxiliary device

Disable HA

Switch to passive device

High Availability – Node Names and Status



The screenshot displays the Sophos Firewall web console interface. The browser tabs are labeled 'Main-ChicagoHQ' and 'Standby-ChicagoHQ'. The URL is 'https://172.16.16.16:4444/webconsole/'. The main content area is titled 'System services' and shows the 'High availability' status. A dropdown menu is open, showing the current node as 'Node1 Primary' and listing the cluster configuration: 'Active-passive cluster' with 'Primary (Active)' (Node1, X011013DK8VBT53) and 'Auxiliary (Passive)' (Node2, X01103PMDBMQ93E). The status panel below shows 'HA Connected (Active-Passive)' and a table of node details.

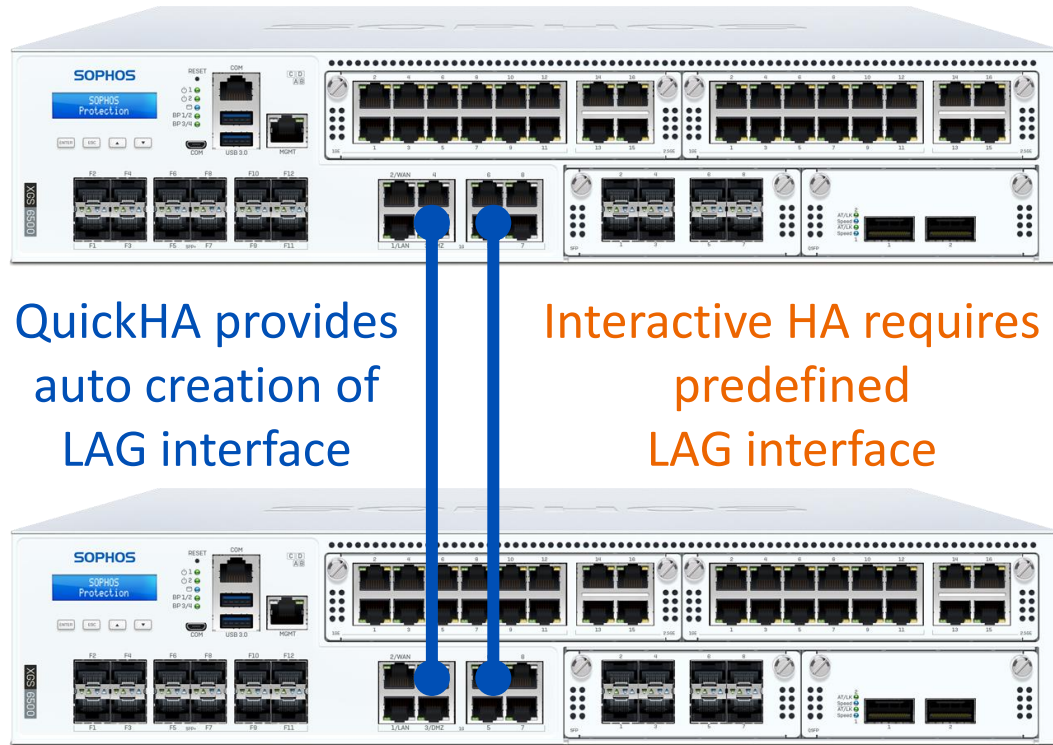
Node name	Serial number	Current role	Current status	Last status change
Node1 (Local) Initial primary. Holds license for cluster.	X011013DK8VBT53	Primary <i>i</i>	Active	04:06:29 PM, Oct 27, 2
Node2 (Peer)	X01103PMDBMQ93E	Auxiliary	Passive	04:06:13 PM, Oct 27, 2

Buttons at the bottom include 'Disable HA' and 'Switch to passive device'.

Customizable node name now shown in browser tab, status panel, drop-down widget, logs, and CLI

Ensures you always know what device you're interacting with

High Availability – Redundant Links



QuickHA provides auto creation of LAG interface

Interactive HA requires predefined LAG interface

High availability configuration

Initial device role *

Primary (active-passive) Auxiliary Primary (active-active)

⚠ The licenses of the device you configure initially as the primary device apply to the whole cluster. Make sure this device has the licenses you want.

HA configuration mode *

QuickHA mode Interactive mode

Node name *

Passphrase *

Dedicated HA link *

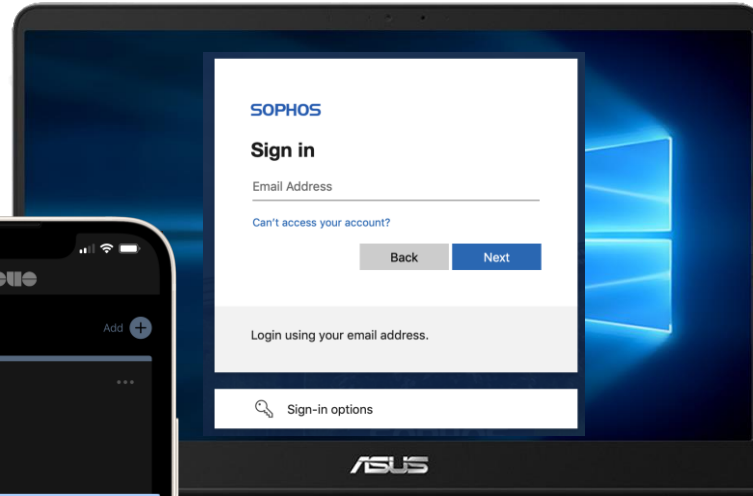
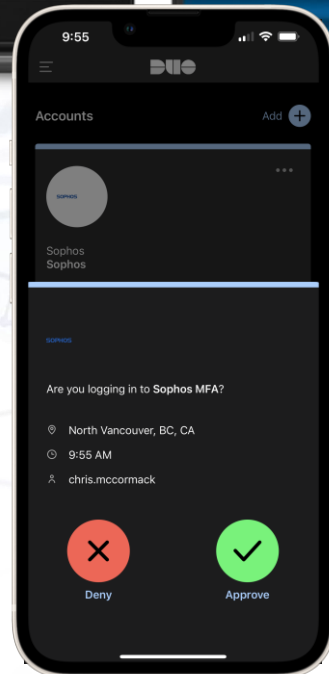
Supported interfaces: Physical, LAG, VLAN, or unbound interfaces

Up To 4 Interfaces: PHYSICAL | LAG | VLAN | UNBOUND

Azure AD Integration for Single Sign On



LOGIN



VERIFY IDENTITY



FIREWALL CONSOLE

Hosts and Services Object Search

The screenshot displays the Sophos Firewall management interface for 'Hosts and services'. The main view shows a list of system hosts with columns for Name, Type, and Address detail. A search bar at the top is highlighted with a red box, containing the text 'Search for Name, Address details'. Below the main list, a modal window is open, showing search results for the IP address '172.16.16', which is also highlighted with a red box. The modal window has tabs for 'IP host', 'IP host group', 'MAC host', 'FQDN host', and 'FQDN host group'. The search results table includes the following entries:

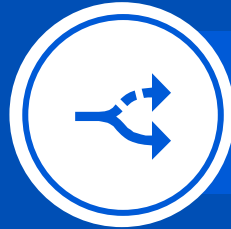
Name	Type	Address detail
#Port1	System host	172.16.16.16/255.255.255.255
<u>DNS_IP</u>	IP address	172.16.16.16/255.255.255.255
<u>LAN_Network</u>	IP subnet	172.16.16.0/255.255.255.0

Search by name, type, or value

Strengthening Our Value Proposition



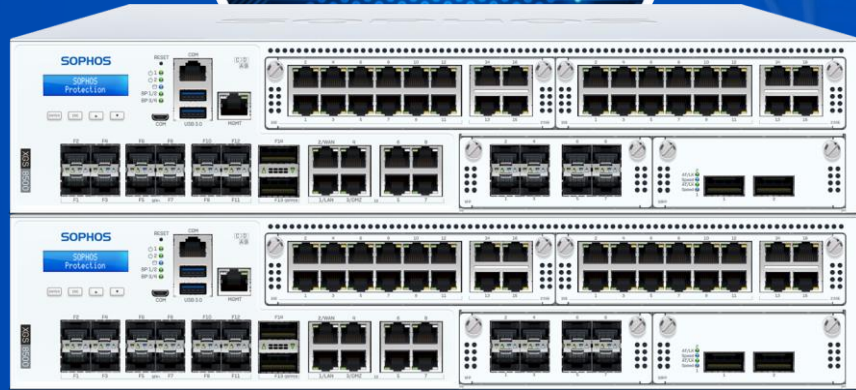
POWERFUL PROTECTION and PERFORMANCE



CONNECT ANYWHERE, ANYHOW



EASY MANAGEMENT



HA Enhancements (Detail Slides)

1. HA Link Redundancy

- LAG support for HA link redundancy
- Supports up to 4 interfaces
- QuickHA mode automatically sets up a LAG interface when multiple interfaces are selected
- Interactive mode supports pre-configured LAG interfaces



High availability configuration

Initial device role *

Primary (active-passive) Auxiliary Primary (active-active)

 Licenses are only required on the primary device. Make sure the primary device has the licenses you want."

HA configuration mode *

QuickHA mode Interactive mode

Node name

Passphrase *


Dedicated HA link *

Select up to four interfaces to configure redundant HA links.
The firewall creates a LAG [active-backup] interface for these in the DMZ.
Supported interfaces: Unbound interfaces, DMZ interfaces,
including LAG and VLAN

2. Eliminate confusion over which device is primary for licensing

High availability configuration

Initial device role * Primary [active-passive] Auxiliary Primary [active-active]

 Licenses are only required on the primary device. Make sure the primary device has the licenses you want."


HA configuration mode * QuickHA mode Interactive mode

Passphrase *

Dedicated HA link *

Select two interfaces for dedicated HA redundancy.
The system will create a LAG [802.3ad] interface using the interface you specify.

Primary [active-passive] Auxiliary Primary [active-active]

 The licenses of the device you configure initially as the primary device apply to the whole cluster. Make sure this device has the licenses you want.

QuickHA

Node1

X19ziOm(t

Port4

The licenses of the device you configure initially as the primary device apply to the whole cluster for active-passive HA.

We recommend that you configure the device with the most licenses as the primary.

Configure this device as the primary?

3. Node name for quick identification

- Added customizable node name to easily identify device
- Can be changed after setting up an HA cluster
- Will be shown in the browser tab, HA status page, HA logs, CLI, Control Center

High availability configuration

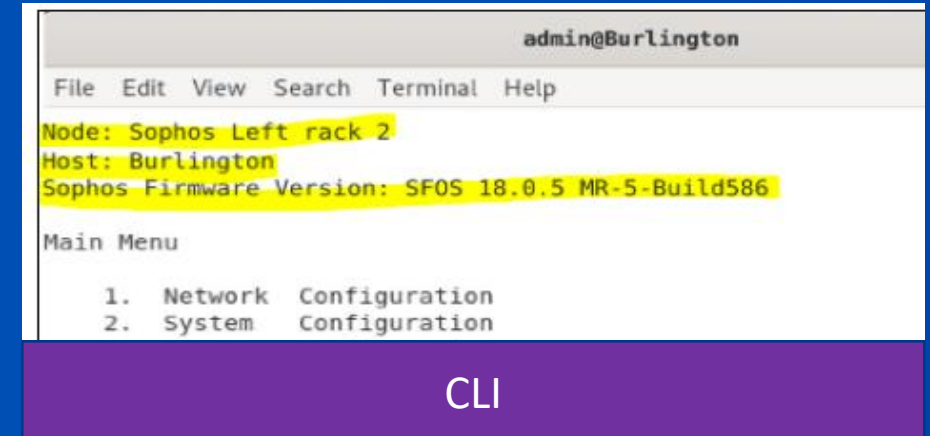
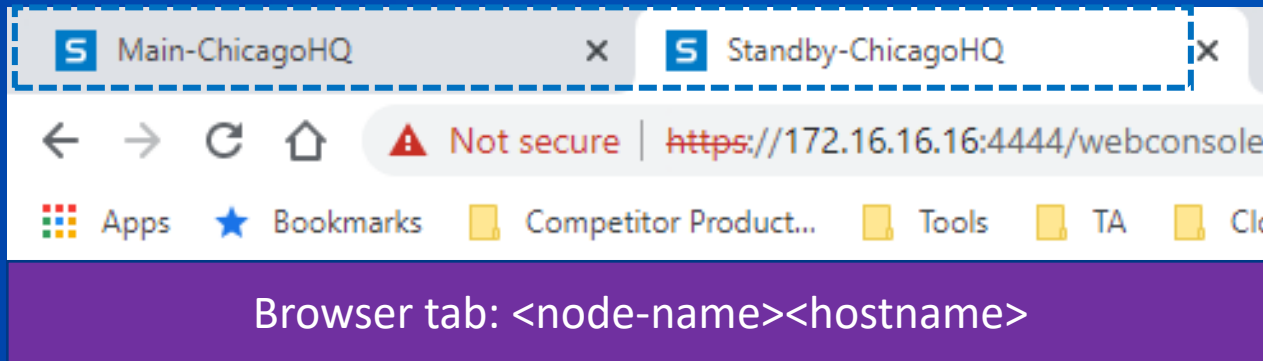
Initial device role * Primary (active-passive) Auxiliary Primary (active-active)
⚠ Licenses are only required on the primary device. Make sure the primary device has the licenses you want.*

HA configuration mode * QuickHA mode Interactive mode

Node name

Passphrase *

Dedicated HA link *



4. HA status page improvements

Node name to easily identify device

Initial primary and license source info (active-passive)

Separated current role and status for clarity

HA Connected (active-passive)
Both HA nodes are now connected and at full health.

Node name	Serial number	Current role	Current state	Last status change
XGS-rack-01 (Local) Initial primary and license source	XGS100ACNNAA124	Primary <i>i</i>	Active	Sep 08, 2021 13:54:52
XGS-rack-02 (Peer)	XGS200ACNNACV14	Auxiliary	Passive	Sep 08, 2021 13:52:43

Sync auxiliary device Switch to passive device Disable HA


Last status change info for troubleshooting

5. Updated preferred primary option

HA configuration mode * QuickHA mode Interactive mode

Cluster ID * (0-63)

Node name *


Dedicated HA link *  Unable to find a dedicated HA port.

Dedicated peer HA link IPv4 address *

Select ports to be monitored


Peer administration settings *

Interface	IPv4 address	IPv6 address
<input type="text" value="PortA"/> <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>

Preferred primary device 

Keepalive request interval Send a request every milliseconds (250-500)

Keepalive attempts Make attempts before determining it as device failure (16-24)

Use host or hypervisor-assigned MAC address 

Select device you want always to be a primary

6. Banner on Auxiliary for easy identification

The screenshot displays the Sophos Firewall web console interface. At the top, there are two browser tabs: "Node1-AHM_01-rackA1" and "Node2-AHM_01-rackA1". The address bar shows the URL: `https://c07-kabir-vm-22.manual.c07.pit.els.sophos:4444/webconsole/webpages/index.jsp#56393`. Below the address bar, there are two notification banners:

- A blue banner with an information icon: "Use of the Sophos Firewall is provided under an Early Access Program and subject to the Sophos End User Terms of Use." with a close button (X).
- An orange banner with an exclamation mark icon: "This is an auxiliary device. You can't change the configuration from this device." with a close button (X).

The main content area is titled "Control center" and includes the following sections:

- System:** Performance (0/0 RED), Services (0/0), Interfaces, and VPN (0).
- Traffic insight:** Web activity (0 max | 0 avg), Cloud applications (0 Apps, 0 B In, 0 B Out), Allowed app categories, Network attacks, Allowed web categories, and Blocked app categories.
- User & device insights:** Security Heartbeat (0 At risk), Synchronized Application Control (0 Apps), and Zero-day protection (0 Recent, 0 Incidents, 0 Scanned).

The left sidebar contains navigation options: "MONITOR & ANALYZE" (Control center, Current activities, Reports, Zero-day protection, Diagnostics) and "PROTECT" (Rules and policies, Intrusion prevention, Web, Applications, Wireless, Email, Web server).

7. Control Center

HA Icon gives quick view for overall cluster health

HA widget moved to admin drop-down. Always available on top for quick access

All cluster information (node name, serial number and status) is available in drop-down

The screenshot displays the Sophos Control Center interface for a Sophos XG Firewall. The top navigation bar includes 'How-to guides', 'Log viewer', and 'Help'. The main dashboard is divided into several sections:

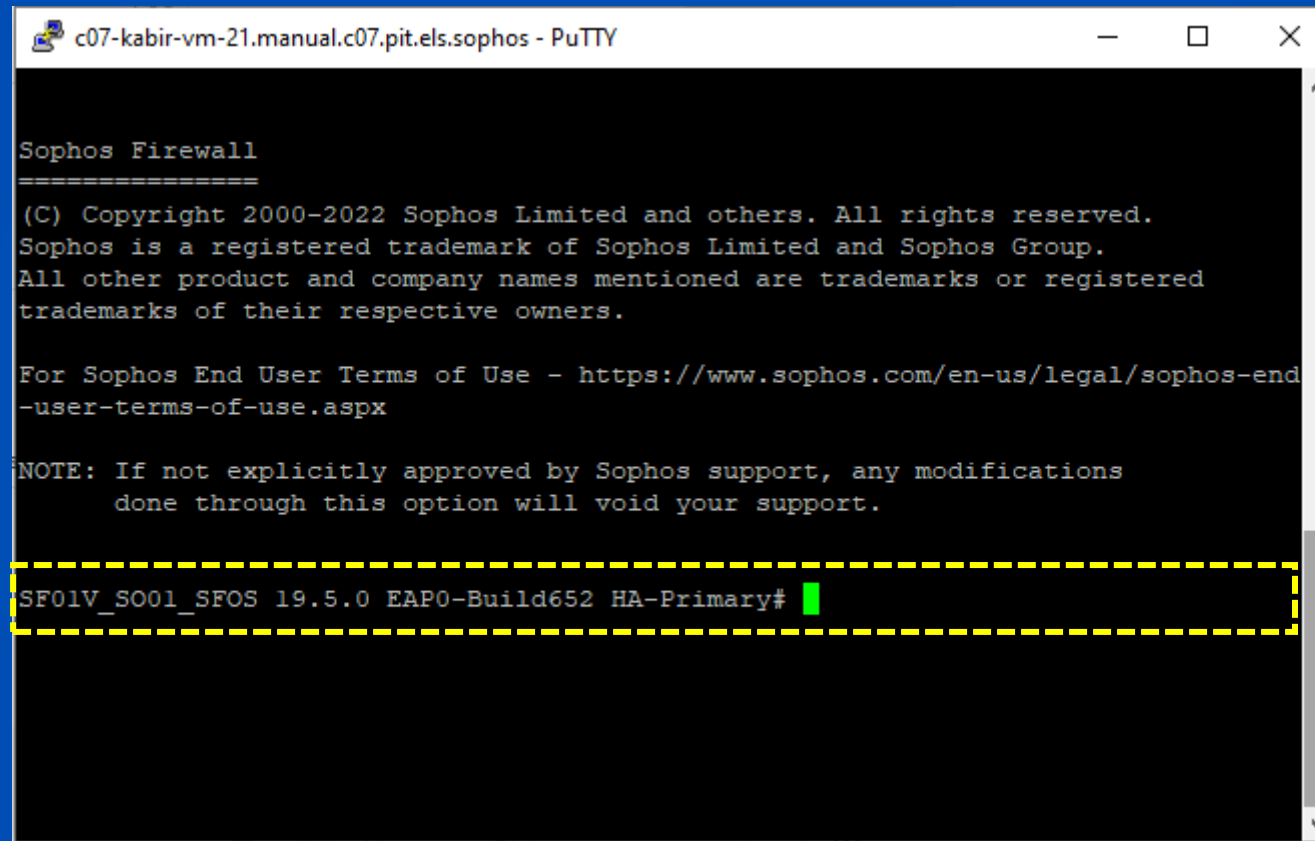
- System:** Shows performance metrics (0/0 RED, 0/0 Wireless APs), connected remote users (0), and live users (0). It also displays CPU usage (100%), memory usage (43%), bandwidth (5.7KB/s), and decryption capacity (0%). A high availability status is shown as 'Not configured'.
- Traffic insight:** Features a 'Web activity' graph (0 max | 0 avg) and 'Cloud applications' bar charts (0 Apps, 0 B In, 0 B Out).
- User & device insights:** Includes 'Security Heartbeat' (At risk, Missing, Warnings), 'Synchronized Application Control' (0 New, 0 Categorized), 'Threat intelligence' (0 Suspect), and 'ATP/UTQ' (0 Sources blocked, 0 Accounts at risk).
- Active firewall rules:** A summary bar shows 0 WAF, 2 User, 4 Network, and 6 Scanned rules.
- Reports:** A message states 'No reports to download.'
- Messages:** A warning message is visible: 'Warning: Managing firewall from Sophos Central' (7m ago).

A dropdown menu is open in the top right corner, showing the HA widget moved to the admin drop-down. The dropdown lists the cluster information:

- 4 Device in active-active cluster
- Primary [active] Nodename X23001RQQv66831
- Auxiliary 1 [active] Nodename X23001RQQv66831
- Auxiliary 2 [active] Nodename X23001RQQv66831
- Auxiliary 3 [active] Nodename X23001RQQv66831

Below the cluster information, there are links for 'Support', 'About product', 'Console', 'reboot device', 'Shutdown device', and 'Logout'.

8. Added HA role in CLI hash prompt for easy troubleshooting



```
c07-kabir-vm-21.manual.c07.pit.els.sophos - PuTTY

Sophos Firewall
=====

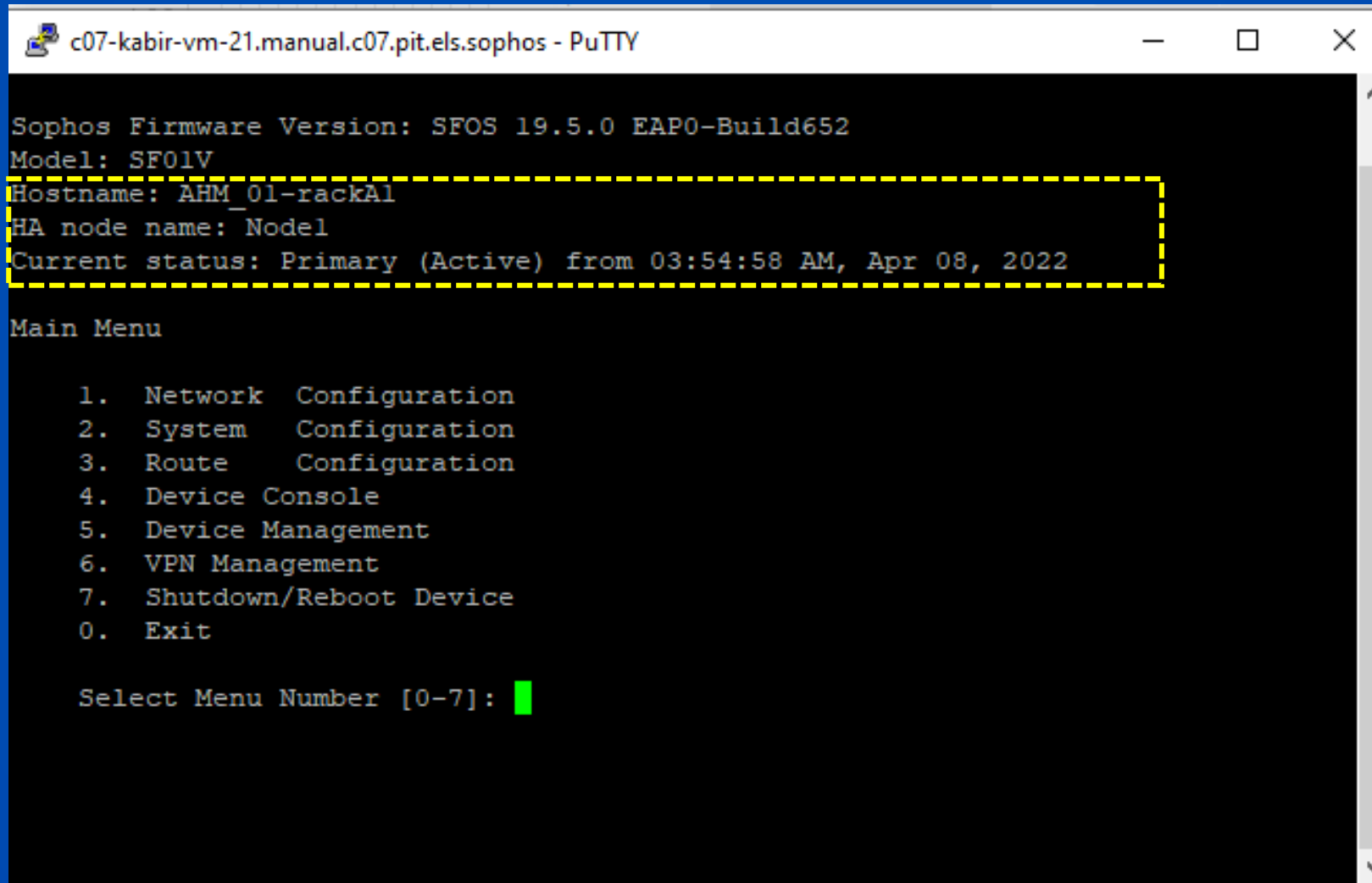
(C) Copyright 2000-2022 Sophos Limited and others. All rights reserved.
Sophos is a registered trademark of Sophos Limited and Sophos Group.
All other product and company names mentioned are trademarks or registered
trademarks of their respective owners.

For Sophos End User Terms of Use - https://www.sophos.com/en-us/legal/sophos-end-user-terms-of-use.aspx

NOTE: If not explicitly approved by Sophos support, any modifications
done through this option will void your support.

SF01V_SO01_SFOS 19.5.0 EAP0-Build652 HA-Primary# █
```

9. Added role and node name information in CLI



```
c07-kabir-vm-21.manual.c07.pit.els.sophos - PuTTY

Sophos Firmware Version: SFOS 19.5.0 EAP0-Build652
Model: SF01V
Hostname: AHM_01-rackA1
HA node name: Nodel
Current status: Primary (Active) from 03:54:58 AM, Apr 08, 2022

Main Menu

1. Network Configuration
2. System Configuration
3. Route Configuration
4. Device Console
5. Device Management
6. VPN Management
7. Shutdown/Reboot Device
0. Exit

Select Menu Number [0-7]: █
```

SOPHOS