

The logo features a stylized 'XG' in orange with a 3D effect, followed by the word 'FIREWALL' in white, uppercase, sans-serif font.

XG FIREWALL

The world's best visibility, protection and response.

Ivan Mateos Pascual
Sales Engineer Sophos Iberia

SOPHOS

A Dirty Secret

Network Firewalls are **Failing** to do their Job

What Network Admins Say are their top 3 complaints with their current firewall...



Visibility

45%

of traffic is going unidentified on average



Protection

16

infections per month on average



Response

7 days

every month spent responding to and fixing infected systems

Source: Survey conducted by Vanson Bourne, November 2017 of 2,700 IT decision makers in organizations from 100-5000 users in 10 countries across 5 continents

The Marketing...



...The Reality!

Dirty Secrets Report on News.Sophos.com

Sophos News

Your network firewall's dirty secrets

Corporate · Network · Survey · XG Firewall · XG Firewall v17

There are some things your firewall would rather you didn't know

18/04/2018 BY: CHRIS MCCORMACK



In our recent next-gen firewall series, we covered the evolution of the modern firewall, its failure to provide adequate protection or visibility, and its inability to respond to security incidents.

If you feel like your firewall isn't meeting your expectations in any of these areas, you're not alone.

A recent survey of 2,700 IT managers across 10 countries revealed just how pervasive and severe these problems are. Most network firewalls are failing to do their job adequately:

Firewalls are failing to deliver the protection organizations need

- Organizations are dealing with 10-20 infections per month.
- 79% of IT managers want better protection from their firewall.
- Better protection is the #1 desired firewall improvement.

IT Managers can't tell you how 45% of their bandwidth is consumed

- On average, 45% of network traffic is going unidentified, so can't be controlled.
- 85% of IT managers want their firewalls to deliver better visibility.

Ineffective Firewalls are costing you time and money

- It takes on average 3.3 hours to identify, isolate, and remediate infected computers.
- 97% of organisations would likely get their endpoint and firewall protection from the same vendor if it improved detection rates and automated incident responses.

You might also enjoy...



CORPORATE · NETWORK

How your firewall can save you from the next ransomware attack



CORPORATE · NETWORK

Taking firewalls to the next level



CORPORATE · NETWORK

The problem with firewalls

SOPHOS
Cybersecurity made simple.

The Dirty Secrets of Network Firewalls

Results of an independent survey of 2,700 IT managers in mid-sized organizations, sponsored by Sophos.

Introduction

In late 2017, Sophos sponsored an independent research study into the state of network security in mid-sized organizations across the globe. This research program explored the experiences, concerns, and future needs of IT managers, with particular focus on firewalls and network defenses.

Conducted by leading UK research house Vanson Bourne, the study surveyed 2,700 IT managers in organizations of 100 to 5,000 users in 10 countries, and across five continents.



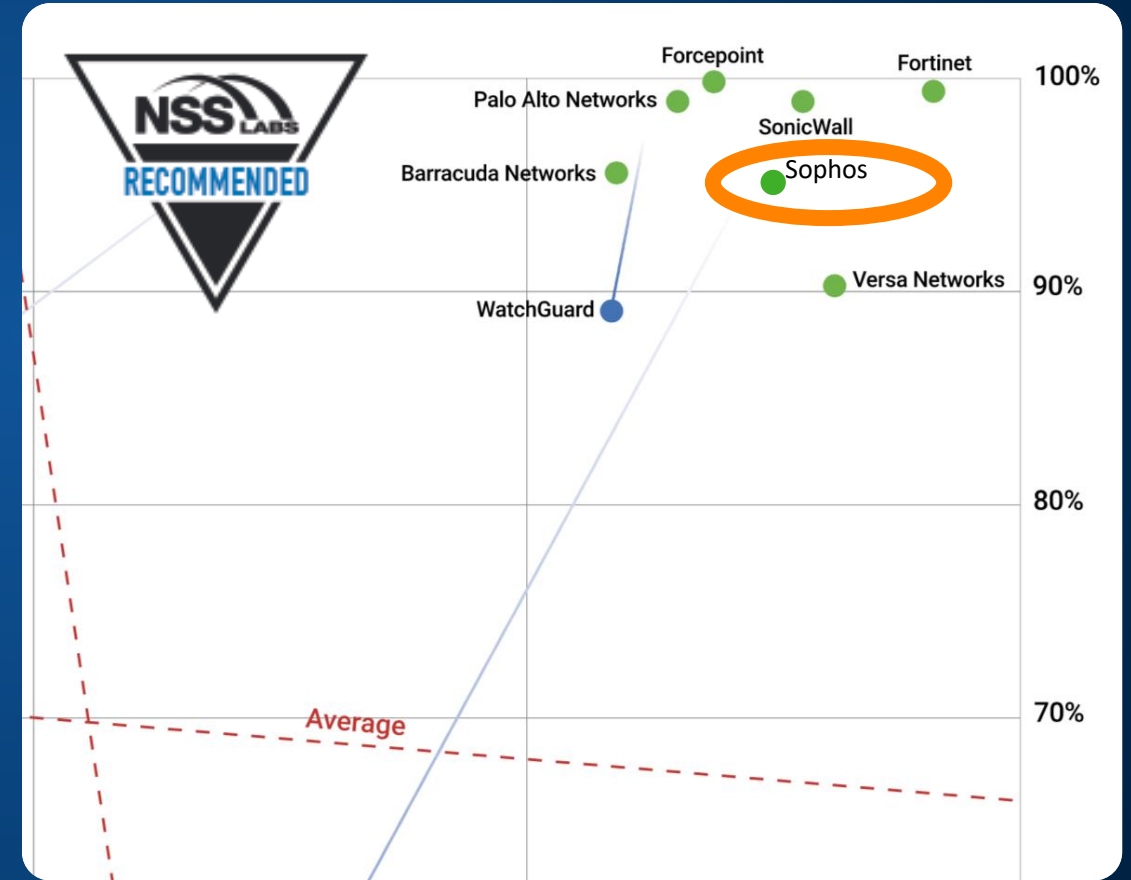
This resulting paper reveals the dirty secrets of today's firewalls, exposing how they are failing organizations in key areas of protection, visibility, and threat response, and the impact of these failures have on IT managers across the globe.



XG Firewall's Winning Advantages

Top Industry Recognition

Gartner, NSS Labs, and others agree, XG Firewall is an Industry Leading Firewall/UTM



XG Series Winning Advantages

Industry leading performance with unique connectivity, reliability, and management

Flexible Connectivity

Business **Continuity** & Easy Management

Industry Leading **Performance**



NEW APX – Wave 2 Access Points

Faster, Better WiFi



Faster Connectivity – up to 2.3Gbps

High density – high capacity

Optimized performance – per device

APX 740

Flagship 4x4:4 for the mid-market enterprise
(at load*, 3x the throughput of AP100)

APX 530

High performance 3x3:3 for all business
(at load*, 2x the throughput of AP100)

APX 320

2x2:2 Medium performance 2x2:2 for all orgs
(at load*, 2x throughput of AP55)

XG Firewall's Winning Advantages

Solving today's top problems with network security



1. Exposes Hidden Risks

- ✓ Visual dashboard & rich on-box reporting
- ✓ Identify unknown cloud & networked apps
- ✓ Identify risky users and suspicious payloads

2. Stops Unknown Threats

- ✓ Full suite of protection – easy to manage
- ✓ Deep learning
- ✓ Top performing IPS Engine

3. Isolates Infected Systems

- ✓ Unique Security Heartbeat™
- ✓ Integrates EP Health into rules
- ✓ Automatically isolate infected systems

SOPHOS XG Firewall

Control center

XG230 [SFOS 17.5.0 Beta-1] C240773Y2QQXTCA

MONITOR & ANALYZE
Control center
Current activities
Reports
Diagnostics

PROTECT
Firewall
Intrusion prevention
Web
Applications
Wireless
Email
Web server
Advanced threat
Central Synchronization

CONFIGURE
VPN
Network
Routing
Authentication
System services

SYSTEM
Profiles
Hosts and services
Admin...
Ba...

System

Performance: 0/0 RED
Services: 3/3 Wireless APs
Interfaces: 0
VPN: 11 Live users

CPU: 15%
Memory: 36%
Bandwidth: 40KB/s
Sessions: 64

High availability: **Not configured**
Sophos Firewall Manager: **Not configured**
Running for 12 day(s), 23 hour(s), 46 minute(s)

Traffic insight

Web activity: 621 max | 150 avg
Hits every 5 minutes

Cloud applications: 21 Apps, 204 MB In, 36.2 MB Out

Allowed app categories:
General Internet: 3,265.44M
Unclassified: 2,650.35M
Unknown: 2,510.58M
Infrastructure: 318.68M
File Transfer: 288.04M

Allowed web categories:
Information Tec...: 4.03K
CRL and OCSP: 1.93K
None: 876
Voice & Video C...: 502
Personal Networ...: 401

Network attacks:
Reconnaissance: 32.11K
Malware Commu...: 295
DNS: 40
Browsers: 4
Misc: 1

Blocked app categories:
General Internet: 265
P2P: 220
Proxy and Tunnel...: 4

User & device insights

Security Heartbeat®: 1 At risk, 1 Missing, 1 Warnings, 2 Connected

Synchronized Application Control™: 4 New, 217 Categorized, 282 Total

Sandstorm: 0 Malicious, 0 Clean, 0 Total

ATP: 2 Sources blocked
UTQ: 1 Acc. for 80% of risk

Reports

13 Total
15 Risky apps seen Yesterday
192 Objectionable web Yesterday
7821 MB Use web Yesterday
38897 Intru Yesterday

Messages

Warning: 1w ago
HTTPS-based management is allowed from the WAN. ...

Advantage #1

Visibility

XG Advantage: Interactive Control Center with Traffic-Light Indicators

SOPHOS XG Firewall

Control Center
XG230 (SFOS 17.1.0 Beta-3) C240773Y2QQXTCA

MONITOR & ANALYZE
Control Center
Current Activities
Reports
Diagnostics

PROTECT
Firewall
Intrusion Prevention
Web
Applications
Wireless
Email
Web Server
Advanced Threat
Synchronized Security

CONFIGURE
VPN
Network
Routing
Authentication
System Services

SYSTEM
Profiles
Hosts and Services
Administration
Backup & Firmware
Certificates

System
Performance: 0/0 RED
Interfaces: 0
Services: 3/3 Wireless APs
VPN: 8 Live Users
CPU: 16%
Bandwidth: 3MB/s
Memory: 36%
Sessions: 12
High Availability: **Not configured**
Sophos Firewall Manager: **Not configured**
Running for 0 day(s), 2 hour(s), 37 minute(s)

Traffic Insight
Web Activity: 818 max | 123 avg
Cloud Applications: 12 Apps, 154 MB In, 53.6 MB Out
Allowed App Categories: Unknown (1,190.07M), Infrastructure (905M), Unclassified (862.97M), Streaming Media (440.98M), General Internet (332.97M)
Allowed Web Categories: Information Te... (2.65K), None (2.04K), Personal Netw... (1.03K), Advertisements (784), General Business (352)
Blocked App Categories: P2P (2.34K), File Transfer (1)

User & Device Insights
Security Heartbeat: 1 Missing, 1 Warnings, 1 Connected
Synchronized Application Control™: 199 Categorized Apps, 28 New Apps, 227 Apps in total detected
Sandstorm: 10 Suspect, 10 Malicious, 0 Clean
ATP: 0 Source blocked
UTQ: 1 Acc. for 80% of risk

Active Firewall Rules
Business: 2 Unused, 1 Disabled, 3 Changed, 0 New
User: 7
Network: 4
Total: 13

Reports
3 Risky Apps seen Yesterday
65 Objectionable websites seen Yesterday
110 MB Used by Top 10 Web users Yesterday
22 Intrusion Attacks Yesterday

Messages
Warning: HTTPS-based management is allowed from the WAN... 14:24
Alert: New RED firmware is available for installation. Click Here 14:26

Threats & Systems at Risk

Unsanctioned Cloud Apps

Unknown Windows/Mac Apps

Suspicious Payloads

Risky Users

Advanced Threats

Risky Apps

Objectionable Websites

Intrusion Attacks

Identify Risky Endpoints

How-to guides Log viewer Help admin Sophos

User & device insights

Security Heartbeat®

1	1	1	2
At risk	Missing	Warnings	Connected

Synchronized Application Control

4	217	282
New	Categorized	Total

Sandstorm

0	0	0
Malicious	Clean	Total

ATP

2
Sources blocked

UTQ

1
Acc. for 80% of risk

Messages

Warning 1w ago
HTTPS-based management is allowed from the WAN. ...

SOPHOS XG Firewall

MONITOR & ANALYZE

- Control Center
- Current Activities
- Reports
- Diagnostics

PROTECT

- Firewall
- Intrusion Prevention
- Web
- Applications
- Wireless
- Email
- Web Server
- Advanced Threat
- Synchronized Security

CONFIGURE

- VPN
- Network
- Routing
- Authentication
- System Services

SYSTEM

Control Center

XG230 [SFOS 17.1.0 Beta-1-OMC] C240773Y2QQXTCA

How-To Guides Log Viewer Help admin Sophos

MONITOR & ANALYZE

SYSTEM CPU & MEMORY NETWORK HEARTBEAT ATP RED ALERT CONNECTIONS & INTERFACES

Show: Missing At Risk Warnings Connected

HOSTNAME, IP	USER	STATE CHANGED
Mac-Server 10.0.1.10	Chris	1 minute ago

Sophos Central
Please refer to Sophos Central to remediate endpoint issues.

Active Firewall Rules

2	1	0	0	13
Unused	Disabled	Changed	New	Total

Reports

- 7 Yesterday Risky Apps seen
- 179 Yesterday Objectionable websites seen
- 771 MB Yesterday Used by Top 10 Web users
- 372 Yesterday Intrusion Attacks

Messages

- Warning** 1m ago
HTTPS-based management is allowed from the WAN. ...
- Alert** 1m ago
New RED firmware is available for installation. [Click He...](#)

Synchronized Application Control

How-To Guides Log Viewer Help admin Sophos

User & Device Insights

Security Heartbeat®

- Risk: 1
- Warnings: 1
- Connected: 2

Synchronized Application Control™

- Categorized Apps: 183
- New Apps: 6
- 189 Apps in total detected

Sandstorm

- Suspect: 23
- Malicious: 1
- Clean: 10

ATP: 2 (Source blocked)

UTQ: 1 (Acc. for 80% of risk)

Messages

- Warning: 14:45 - HTTPS-based management is allowed from the WAN. ...
- Alert: Yesterday - New RED firmware is available for installation. [Click He...](#)

SOPHOS
XG Firewall

MONITOR & ANALYZE

- Control center
- Current activities
- Reports
- Diagnostics

PROTECT

- Firewall
- Intrusion prevention
- Web
- Applications**
- Wireless
- Email
- Web server
- Advanced threat
- Central Synchronization

CONFIGURE

- VPN
- Network
- Routing
- Authentication
- System services

SYSTEM

- Profiles
- Hosts and services
- Administration
- Backup & firmware
- Certificates

Applications

How-to guides Log viewer Help admin Sophos

Application filter Synchronized Application Control Cloud applications Application list Traffic shaping default

Synchronized Application Control

On this page you can modify application details for applications discovered with Synchronized Security from Sophos managed devices. You can change the name and category for the applications, information for some applications is already provided automatically from Sophos. You can use these applications in the overall application control feature on XG Firewall or you can directly assign the discovered applications to application filters to control the applications.

Acknowledge Hide Delete New applications

Application	Category	Endpoints	Occurrences	Last occurrence	Manage
<input type="checkbox"/> + Apple Maps Applications/.../MacOS/Maps	General Internet	Found on 1 Endpoints	11	2018-04-06 14:30	NEW ...
<input type="checkbox"/> + BitTorrent <UserProfile>...\bittorrentie.exe	P2P	Found on 1 Endpoints	69	2018-09-10 17:21	NEW ...
<input type="checkbox"/> + VirtualBox Applications/.../MacOS/VirtualBox	Infrastructure	Found on 2 Endpoints	16	2018-10-14 14:58	NEW ...
<input type="checkbox"/> + Vmware Fusion Applications/.../VMware Fusion	Infrastructure	Found on 1 Endpoints	1	2018-07-17 23:37	NEW ...

Identify Risky Downloads

How-to guides Log viewer Help admin Sophos

User & device insights

Security Heartbeat®

1	1	1	2
At risk	Missing	Warnings	Connected

Synchronized Application Control™

4	217	282
New	Categorized	Total

Sandstorm

0	0	0
Malicious	Clean	Total

Sources blocked: 2 Acc. for 80% of risk: 1

Messages

Warning 1w ago
HTTPS-based management is allowed from the WAN ...

SOPHOS XG Firewall

MONITOR & ANALYZE

- Control Center
- Current Activities
- Reports
- Diagnostics

PROTECT

- Firewall
- Intrusion Prevention
- Web
- Applications
- Wireless
- Email
- Web Server
- Advanced Threat**
- Synchronized Security

CONFIGURE

- VPN
- Network
- Routing
- Authentication
- System Services

SYSTEM

- Profiles
- Hosts and Services
- Administration
- Backup & Firmware
- Certificates

Advanced Threat

How-To Guides Log Viewer Help admin Sophos

Advanced Threat Protection Sandstorm Activity Sandstorm Settings

Date	Recipient	Source	File Type	Status	Manage
2018-04-10 10:49:43	User: joe IP: 192.168.1.2	www.universelaborator...	Unknown File Type	Malicious Show report	
2018-04-06 09:33:52	User: joe IP: 192.168.1.2	www.universelaborator...	Unknown File Type	Malicious Show report	
2018-04-05 06:51:57	User: joe IP: 192.168.1.2	www.universelaborator...	Unknown File Type	Malicious Show report	
2018-04-04 15:35:25	User: joe IP: 192.168.1.2	www.universelaborator...	Unknown File Type	Malicious Show report	
2018-03-30 18:35:08	User: vmuser IP: 10.0.1.58	www.tuact.com	Compressed Files	Clean Show report	
2018-03-30 18:34:25	User: vmuser IP: 10.0.1.58	ll.download3.utorrent.c...	Unknown File Type	Clean Show report	
2018-03-22 14:10:22	User: joe IP: 192.168.1.2	www.universelaborator...	Unknown File Type	Malicious Show report	
2018-03-22 14:08:07	User: joe IP: 192.168.1.2	downloadz.dewmobile...	Unknown File Type	Clean Show report	
2018-03-22 14:05:38	User: joe IP: 192.168.1.2	lon-01.lo4d.com	Unknown File Type	Clean Show report	

Identify Risky Users

How-to guides Log viewer Help admin Sophos

User & device insights

Security Heartbeat®

1	1	1	2
At risk	Missing	Warnings	Connected

Synchronized Application Control™

4	217	282
New	Categorized	Total

Sandstorm

0	0	0
Malicious	Clean	Total

ATP

2
Sources blocked

UTQ

1
Acc. for 80% of risk

Messages

Warning
HTTPS-based management is allowed from the WAN. ... 1w ago

SOPHOS XG Firewall

MONITOR & ANALYZE

- Control Center
- Current Activities
- Reports
- Diagnostics

PROTECT

- Firewall
- Intrusion Prevention
- Web
- Applications
- Wireless
- Email
- Web Server
- Advanced Threat

CONFIGURE

- VPN
- Network
- Routing
- Authentication
- System Services

SYSTEM

- Profiles
- Hosts and Services

Reports

Log Viewer Help admin Sophos

Show Reports Settings

Dashboards Applications & Web Network & Threats VPN Email Compliance Custom

Show: User Threat Quotient (UTQ)

2016-09-29 for Last 7 Days FROM: 2016-09-23 TO: 2016-09-29

Download: PDF EXCEL Bookmark Schedule

Users with high threat quotient

User	Relative Threat Score
serveradmin	33.25
[Other User]	~28
[Other User]	~24
[Other User]	~16

CASB Cloud App Visibility – Shadow IT Detection

SOPHOS XG Firewall

Control Center
XG230 (SFOS 17.1.0 Beta-3) C240773Y2QQXTCA

MONITOR & ANALYZE
Control Center
 Current Activities
 Reports
 Diagnostics

PROTECT
 Firewall
 Intrusion Prevention
 Web
 Applications
 Wireless
 Email
 Web Server
 Advanced Threat
 Synchronized Security

CONFIGURE
 VPN
 Network
 Routing
 Authentication
 System Services

SYSTEM
 Profiles
 Hosts and Services
 Administration
 Backup & Firmware
 Certificates

System

Performance Services
 Interfaces VPN

0/0 RED
 0
 Connected Remote Users

3/3 Wireless APs
 8
 Live Users

CPU 16% Memory 36%
 Bandwidth 3MB/s Sessions 12

High Availability: **Not configured**
 Sophos Firewall Manager: **Not configured**
 Running for 0 day(s), 2 hour(s), 37 minute(s)

Traffic Insight

Web Activity 818 max | 123 avg

Hits every 5 minutes

Cloud Applications

12 Apps
 154 MB In
 53.6 MB Out

Allowed App Categories

Unknown	1,190.07M
Infrastructure	905M
Unclassified	862.97M
Streaming Media	440.98M
General Internet	332.97M

Network Attacks

Operating Syst... 4
 Apache HTTP S... 1

Allowed Web Categories

Information Te...	2.65K
None	2.04K
Personal Netw...	1.03K
Advertisements	784
General Business	352

Blocked App Categories

P2P 2.34K
 File Transfer 1

Cloud Applications

12 Apps
 26 MB In
 231 MB Out

Categories: 227 Apps in total detected

Sandstorm: 10 Suspect, 10 Malicious, 0 Clean

ATP: 0 Source blocked
 UTQ: 1 Acc. for 80% of risk

Active Firewall Rules

2 Business, 7 User, 4 Network, 13 Total

2 Unused, 1 Disabled, 3 Changed, 0 New

Reports

3 Risky Apps seen Yesterday
 65 Objectionable websites seen Yesterday
 110 MB Used by Top 10 Web users Yesterday
 22 Intrusion Attacks Yesterday

Messages

Warning: HTTPS-based management is allowed from the WAN... 14:24
 Alert: New RED firmware is available for installation. [Click He...](#) 14:26

Click on widgets to open details

Cloud Applications

Legend:
 ● New (Blue)
 ● Sanctioned (Green)
 ● Unsanctioned (Red)
 ● Tolerated (Orange)

New	2
Sanctioned	6
Unsanctioned	2
Tolerated	2

12 Apps
 26 MB In
 231 MB Out

0% 50% 100%

Cloud App Visibility & Shadow IT Discovery

The screenshot displays the Sophos Applications dashboard. At the top, there are navigation links for 'How-To Guides', 'Log Viewer', 'Help', and 'admin' (Sophos). Below this, there are tabs for 'Application Filter', 'Synchronized Application Control', 'Cloud Applications' (selected), 'Application List', and 'Traffic Shaping Default'. The main content area shows a filter bar with 'From: 2018-06-01 To: 2018-06-01', 'Unsanctioned', 'All Categories', and 'Sort by Bytes Transferred'. Below the filter bar, there are two application entries: 'Dropbox Base' and 'Facebook Website'. Each entry shows its category, risk level, and status, along with traffic volume and user count. A table below the 'Dropbox Base' entry shows user-specific data for 'joe'.

Filter / Sort

Cloud Application

Classify

Traffic Shape

Users and Volume of Data

User	Host	Upload Data	Download Data
joe	192.168.1.2	218 MB	10 MB

The industry's best app visibility is now even better



Advantage #2

Protection

Threat Protection in XG Firewall

A full suite of technologies easily managed from a single screen



-  Dual-engine AV
-  Intrusion Prevention System
-  Advanced Threat Protection
-  Deep Learning Sandboxing
-  Web Protection & App Control
-  Email Protection
-  Full VPN Connectivity

Malware Scanning

- Scan HTTP
- Decrypt & Scan HTTPS
- Detect zero-day threats with Sandstorm
- Scan FTP

Advanced

User Applications

Intrusion Prevention

LAN TO WAN

Traffic Shaping Policy

User's policy applied

Web Policy

Default Workplace Policy

Apply Web Category based Traffic Shaping Policy

Application Control

Block very high risk (Risk Level 5) apps

Apply Application-based Traffic Shaping Policy

Synchronized Security

Minimum Source HB Permitted:

GREEN YELLOW No Restriction

Block clients with no heartbeat

Minimum Destination HB Permitted:

GREEN YELLOW No Restriction

Block request to destination with no heartbeat

NAT & Routing

Rewrite source address (Masquerading)

Use Gateway Specific Default NAT Policy

Use Outbound Address

MASQ

MASQ (Interface Default IP)

Primary Gateway

WAN Link Load Balance

Backup Gateway

None

DSCP Marking

Select DSCP Marking



Threat Protection in XG Firewall

A full suite of technologies easily managed from a single screen



 Dual-engine AV

 Intrusion Prevention System

 Advanced Threat Protection

 Deep Learning Sandboxing

 Web Protection & App Control

 Email Protection

 Full VPN Connectivity

Malware Scanning

- Scan HTTP
- Decrypt & Scan HTTPS
- Detect zero-day threats with Sandstorm
- Scan FTP

Advanced

User Applications Intrusion Prevention LAN TO WAN Traffic Shaping Policy User's policy applied Web Policy Default Workplace Policy <input type="checkbox"/> Apply Web Category based Traffic Shaping Policy Application Control Block very high risk [Risk Level 5] apps <input type="checkbox"/> Apply Application-based Traffic Shaping Policy	Synchronized Security Minimum Source HB Permitted: <input checked="" type="radio"/> GREEN <input type="radio"/> YELLOW <input type="radio"/> No Restriction <input type="checkbox"/> Block clients with no heartbeat Minimum Destination HB Permitted: <input type="radio"/> GREEN <input type="radio"/> YELLOW <input checked="" type="radio"/> No Restriction <input type="checkbox"/> Block request to destination with no heartbeat	NAT & Routing <input checked="" type="checkbox"/> Rewrite source address [Masquerading] <input type="checkbox"/> Use Gateway Specific Default NAT Policy Use Outbound Address MASQ MASQ [Interface Default IP] Primary Gateway WAN Link Load Balance Backup Gateway None DSCP Marking Select DSCP Marking
---	--	---



Threat Protection in XG Firewall

A full suite of technologies easily managed from a single screen



 Dual-engine AV

 Intrusion Prevention System

 Advanced Threat Protection

 Deep Learning Sandboxing

 Web Protection & App Control

 Email Protection

 Full VPN Connectivity

Malware Scanning

- Scan HTTP
- Decrypt & Scan HTTPS
- Detect zero-day threats with Sandstorm
- Scan FTP

Advanced

User Applications Intrusion Prevention LAN TO WAN Traffic Shaping Policy User's policy applied Web Policy Default Workplace Policy <input type="checkbox"/> Apply Web Category based Traffic Shaping Policy Application Control Block very high risk (Risk Level 5) apps <input type="checkbox"/> Apply Application-based Traffic Shaping Policy	Synchronized Security Minimum Source HB Permitted: <input checked="" type="radio"/> GREEN <input type="radio"/> YELLOW <input type="radio"/> No Restriction <input type="checkbox"/> Block clients with no heartbeat Minimum Destination HB Permitted: <input type="radio"/> GREEN <input type="radio"/> YELLOW <input checked="" type="radio"/> No Restriction <input type="checkbox"/> Block request to destination with no heartbeat	NAT & Routing <input checked="" type="checkbox"/> Rewrite source address (Masquerading) <input type="checkbox"/> Use Gateway Specific Default NAT Policy Use Outbound Address MASQ MASQ (Interface Default IP) Primary Gateway WAN Link Load Balance Backup Gateway None DSCP Marking Select DSCP Marking
---	--	---



Threat Protection in XG Firewall

A full suite of technologies easily managed from a single screen



-  Dual-engine AV
-  Intrusion Prevention System
-  Advanced Threat Protection
-  Deep Learning Sandboxing
-  Web Protection & App Control
-  Email Protection
-  Full VPN Connectivity

Malware Scanning

- Scan HTTP
- Decrypt & Scan HTTPS
- Detect zero-day threats with Sandstorm
- Scan FTP

Advanced

User Applications

Intrusion Prevention

LAN TO WAN

Traffic Shaping Policy

User's policy applied

Web Policy

Default Workplace Policy

Apply Web Category based Traffic Shaping Policy

Application Control

Block very high risk [Risk Level 5] apps

Apply Application-based Traffic Shaping Policy

Synchronized Security

Minimum Source HB Permitted:

GREEN YELLOW No Restriction

Block clients with no heartbeat

Minimum Destination HB Permitted:

GREEN YELLOW No Restriction

Block request to destination with no heartbeat

NAT & Routing

Rewrite source address [Masquerading]

Use Gateway Specific Default NAT Policy

Use Outbound Address

MASQ

MASQ [Interface Default IP]

Primary Gateway

WAN Link Load Balance

Backup Gateway

None

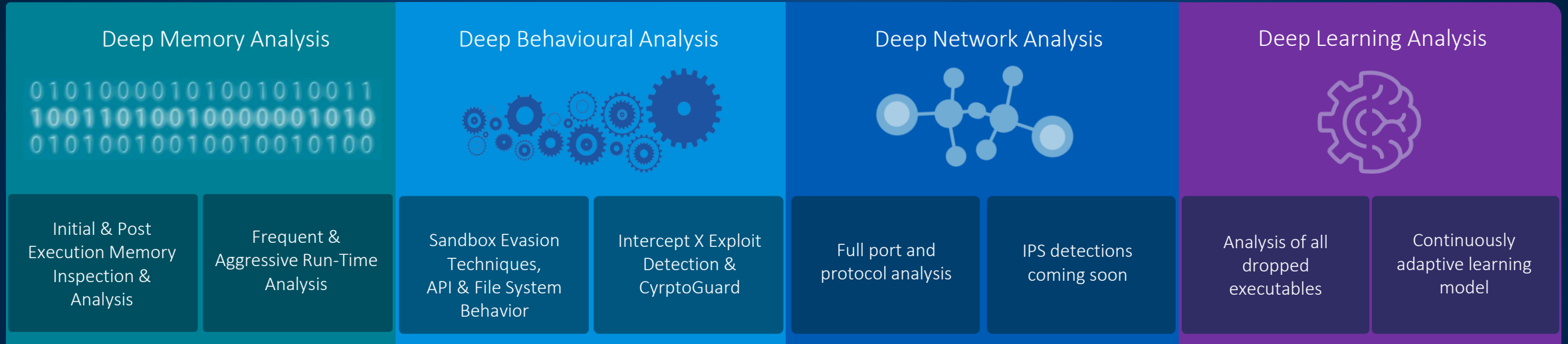
DSCP Marking

Select DSCP Marking



Sandboxing - Sandstorm Deep Threat Prevention

Your best protection from zero day threats



FIREWALL

Sophos Sandstorm

INTERCEPT



Deep Learning in Action

SOPHOS XG Firewall

MONITOR & ANALYZE

- Control Center
- Current Activities
- Reports
- Diagnostics

PROTECT

- Firewall
- Intrusion Prevention
- Web
- Applications
- Wireless
- Email
- Web Server
- Advanced Threat**
- Synchronized Security

CONFIGURE

- VPN
- Network
- Routing
- Authentication
- System Services

Advanced Threat

How-To Guides Log Viewer Help admin Sophos

Advanced Threat Protection Sandstorm Activity Sandstorm Settings

Date	Recipient	Source	File Type	Status	Manage
2018-03-30 18:35:08	User: vmuser IP: 10.0.1.58	www.tuact.com	Compressed Files	Clean Show report	
2018-03-30 18:34:25	User: vmuser IP: 10.0.1.58	ll.download3.utorrent.c...	Unknown File Type	Clean Show report	
2018-03-22 14:10:22	User: joe IP: 192.168.1.2	www.universelaborator...	Unknown File Type	Malicious Show report	
2018-03-22 14:08:07	User: joe IP: 192.168.1.2	downloadz.dewmobile...	Unknown File Type	Clean Show report	
2018-03-22 14:05:38	User: joe IP: 192.168.1.2	lon-01.lo4d.com	Unknown File Type	Clean Show report	
2018-03-21 16:07:14	User: joe IP: 192.168.1.2	www.universelaborator...	Unknown File Type	Malicious Show report	
2018-03-21 15:43:31	User: joe IP: 192.168.1.2	iweb.dl.sourceforge.net	Unknown File Type	Clean Show report	
2018-03-21 15:42:53	User: joe IP: 192.168.1.2	sea-02.lo4d.com	Compressed Files	Clean Show report	
2018-03-21 15:41:49	User: joe IP: 192.168.1.2	lon-01.lo4d.com	Unknown File Type	Clean Show report	

Deep Learning in Action

The screenshot displays the Sophos XG Firewall management console. On the left is a navigation sidebar with sections: MONITOR & ANALYZE (Control Center, Current Activities, Reports, Diagnostics), PROTECT (Firewall, Intrusion Prevention, Web, Applications, Wireless, Email, Web Server, **Advanced Threat**, Synchronized Security), and CONFIGURE (VPN, Network, Routing, Authentication, System Services). The main area is titled 'Advanced Threat' and shows a table of detected items. A modal window titled 'Sandstorm Item Details' is open, showing information for a file named 'BitlordSetup_VZ1aw9_1907513196.exe'. The file name is highlighted with a red box. The modal includes an overview, download details, file details, and sandstorm result.

SOPHOS
XG Firewall

MONITOR & ANALYZE

- Control Center
- Current Activities
- Reports
- Diagnostics

PROTECT

- Firewall
- Intrusion Prevention
- Web
- Applications
- Wireless
- Email
- Web Server
- Advanced Threat**
- Synchronized Security

CONFIGURE

- VPN
- Network
- Routing
- Authentication
- System Services

Advanced Threat

[Sandstorm Settings](#)

Date	Status	Manage
2018-03-30 18:35:08	lean	how report
2018-03-30 18:34:25	lean	how report
2018-03-22 14:10:22	alicious	how report
2018-03-22 14:08:07	lean	how report
2018-03-22 14:05:38	lean	how report
2018-03-21 16:07:14	alicious	how report
2018-03-21 15:43:31	lean	how report
2018-03-21 15:42:53	lean	how report
2018-03-21 15:41:49	lean	how report

Sandstorm Item Details

Overview
This item was downloaded 1 time by 1 user.

Download Details

Username	joe
User IP Address	192.168.1.2
Download Time	2018-03-22 14:10:22
Job ID	D03E 672D
Source Website	www.universelaboratorytoul.com
Source Category	None
Released	Not Released
Retrieved by User	No

File Details

Signature [SHA1]	3f6a595b1baf95a198e79ee997ca84c58ac19cd2
Signature [MD5]	44370c59fb05557155da1a7637613096
File Name	BitlordSetup_VZ1aw9_1907513196.exe
File Type (MIME)	application/octet-stream
File Size	1772256 Bytes
Sent for Analysis	2018-03-22 14:10:22

Sandstorm Result

Status	Malicious
Result Time	2018-03-22 14:16:32
Analysis Time	06m10s

Deep Learning in Action

MONITOR & ANALYZE

Control Center

Current Activities

Reports

Diagnostics

PROTECT

Firewall

Intrusion Prevention

Web

Applications

Wireless

Email

Web Server

Advanced Threat

Synchronized Security

CONFIGURE

VPN

Network

Routing

Authentication

System Services

Advanced Threat

Advanced

Date

2018-03-30 18:35:08

2018-03-30 18:34:25

2018-03-22 14:10:22

2018-03-22 14:08:07

2018-03-22 14:05:38

2018-03-21 16:07:14

2018-03-21 15:43:31

2018-03-21 15:42:53

2018-03-21 15:41:49

Sandstorm Item Details

Analysis Result

Evasion

- Checks the BIOS manufacturer
- Executes code to read CPU configuration
- Checks for the presence of a debugger
- Reads hardware information from the registry
- Executes code to check CPU timing behavior

Suspicious

- An executable with low reputation is detected by Machine Learning classifier
- Reads data from the local Windows system configuration

Memory

- Changes the permissions of a memory region used by system libraries

Network

- Issues one or more HTTP POST requests

Signature

- Exhibits known behavior for the InstallCore PUA family

Analysis Time 06m10s

Sandstorm Settings

Status

Manage

lean
how report

lean
how report

alicious
how report

lean
how report

lean
how report

alicious
how report

lean
how report

lean
how report

lean
how report

XG Firewall Powerful Per-Rule Protection made Simple

A full suite of technologies easily managed from a single screen

The image shows a screenshot of the XG Firewall configuration interface, specifically the 'Malware Scanning' and 'Advanced' sections. Blue callout lines point from various feature names to their corresponding settings in the interface.

Malware Scanning

- Scan HTTP
- Decrypt & Scan HTTPS
- Detect zero-day threats with Sandstorm
- Scan FTP

Advanced

User Applications

- Intrusion Prevention: LAN TO WAN
- Traffic Shaping Policy: User's policy applied
- Web Policy: Default Workplace Policy
- Apply Web Category based Traffic Shaping Policy
- Application Control: Block very high risk (Risk Level 5) apps
- Apply Application-based Traffic Shaping Policy

Synchronized Security

- Minimum Source HB Permitted: GREEN YELLOW No Restriction
- Block clients with no heartbeat
- Minimum Destination HB Permitted: GREEN YELLOW No Restriction
- Block request to destination with no heartbeat

NAT & Routing

- Rewrite source address (Masquerading)
- Use Gateway Specific Default NAT Policy
- Use Outbound Address: MASQ (Interface Default IP)
- Primary Gateway: WAN Link Load Balance
- Backup Gateway: None
- DSCP Marking: Select DSCP Marking

Callouts:

- Dual AV (points to Scan HTTP)
- SSL Inspection (points to Decrypt & Scan HTTPS)
- Sandboxing (points to Detect zero-day threats with Sandstorm)
- IPS (points to Intrusion Prevention)
- QoS (points to Traffic Shaping Policy)
- Web Filtering (points to Web Policy)
- App Control (points to Application Control)
- Heartbeat (points to Synchronized Security)
- NAT (points to Rewrite source address)
- Routing (points to Primary Gateway)
- Prioritization (points to DSCP Marking)

Advantage #3

Response

Sophos Endpoint + Sophos XG Firewall

1

Malware Detection

Sophos Endpoint detects a malware attack

2

Cross-Estate Communication

Sophos Endpoint shares infection status with the security system, triggering automatic responses

3

Device Isolation

XG Firewall instantly isolates the computer, preventing the attack from spreading, and communication with C2 servers.

Security Heartbeat™

5

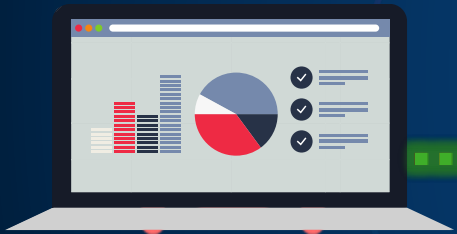
Access Restored

XG Firewall restores network access. Root Cause Analysis provides detailed view of what happened.

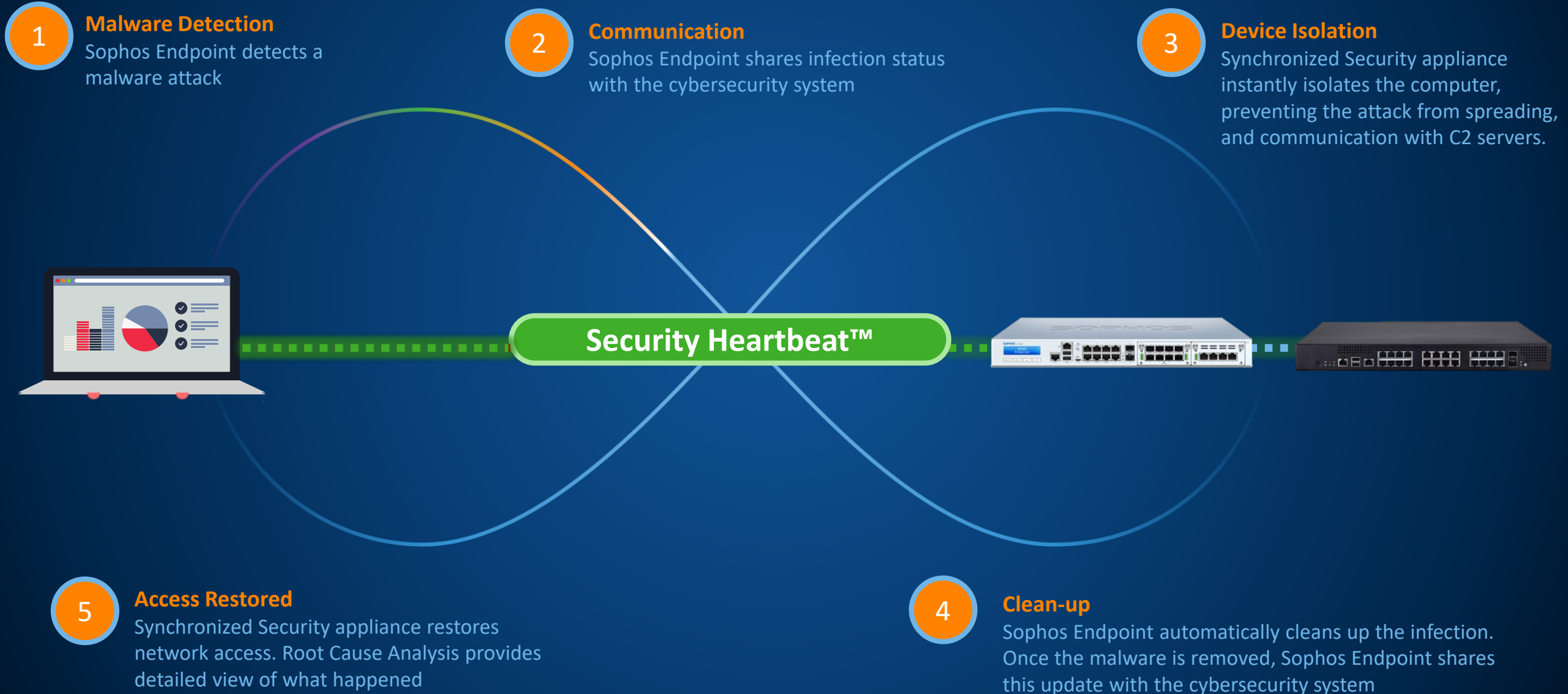
4

Clean-up

Sophos Endpoint automatically cleans up the infection. Once the malware is removed, Sophos Endpoint shares this update with the cybersecurity system



Sophos Endpoint + Sophos XG Firewall – in line



Sophos

Not secure | https://6.6.6.4444/webconsole/webp...

Sophos Personal Tools Cheats CSI Otros LAB Preventa Sophos Home

SOPHOS XG Firewall

Control center

SFVH (SFOS 17.5.3 MR-3) C01001Q7BC4MJ96

How-to guides Log viewer Help admin SOPHOS IBERIA

MONITOR & ANALYZE

Control center

Current activities Reports Diagnostics

PROTECT

Firewall Intrusion prevention Web Applications Wireless Email Web server Advanced threat Central Synchronization

CONFIGURE

VPN Network Routing Authentication System services

SYSTEM

Profiles Hosts and services Administration Backup & firmware Certificates

SYSTEM CPU & MEMORY NETWORK HEARTBEAT ATP RED ALERT CONNECTIONS & INTERFACES

0 At risk 1 Missing 0 Warnings 2 Connected

Show: Missing At risk Warnings Connected

HOSTNAME, IP	USER	STATUS CHANGED
server 172.16.16.1		4 days ago
Win7SophosTest 192.168.1.2	Sophos	17 minutes ago
PC_Windows7Test 172.16.16.2	demoadmin@sophosiberia.local	51 seconds ago

Sophos Central
Please refer to Sophos Central to remediate endpoint issues.

Active firewall rules

2 Business 3 User 7 Network 12 Total

3 Unused 2 Disabled 0 Changed 0 New

Reports

- 0 Risky apps seen Yesterday
- 0 Objectionable websites seen Yesterday
- 0 bytes Used by top 10 web users Yesterday
- 0 Intrusion attacks Yesterday

Messages

- Warning: Managing firewall from Sophos Central (3m ago)
- Alert: The default password for the user 'admin' has not been changed (Yesterday)
- Warning: HTTPS, SSH-based management is allowed from the... (Yesterday)

Click on widgets to open details

Win7SophosTest -FULL - VMware Workstation

File Edit View VM Tabs Help

Home SFOS_Virtual iView Windows7Test - Solo InterceptX Win7SophosTest -FULL

Recycle Bin DOCUMENT... on SGNServer

CryptoLocker Files

SophosTest...

Tools

Sophos Connect

Sophos Connect

SOPHOS Security made simple

12:42 PM 2/19/2019

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

Windows taskbar with various application icons including Internet Explorer, Firefox, Chrome, File Explorer, and the Start menu.



FIREWALL

v17.5

Summary - Key New Features in v17.5



Synchronized Security

Lateral Movement Protection

Automatic isolation at every point in your network

Synchronized User ID

User authentication through Security Heartbeat



Central Management

Sophos Central Management

XG Firewall joins Sophos Central:

Manage all your IT security from a single pane of glass



Wireless

APX Wireless Access Points

WAVE 2 Performance:

Faster connectivity, higher capacity and optimal performance

Top Requested Features

Education – Protection - Networking

- Chromebook Authentication
- Web Policy-based SafeSearch
- Classroom web policy overrides
- Email anti-spam enhancements
- Sophos Connect IPSec Client
- Firewall rule auto grouping
- Log viewer enhancements
- Client Authentication App Enhancements
- TALOS IPS Enhancements
- Airgap deployment support (MR1)



Visibility

- Central Management
- Synchronized User ID
- App Sync enhancements
- Chromebook Authentication
- Log viewer enhancements



Protection

- Email anti-spam enhancements
- TALOS IPS Enhancements
- Lateral Movement Protection

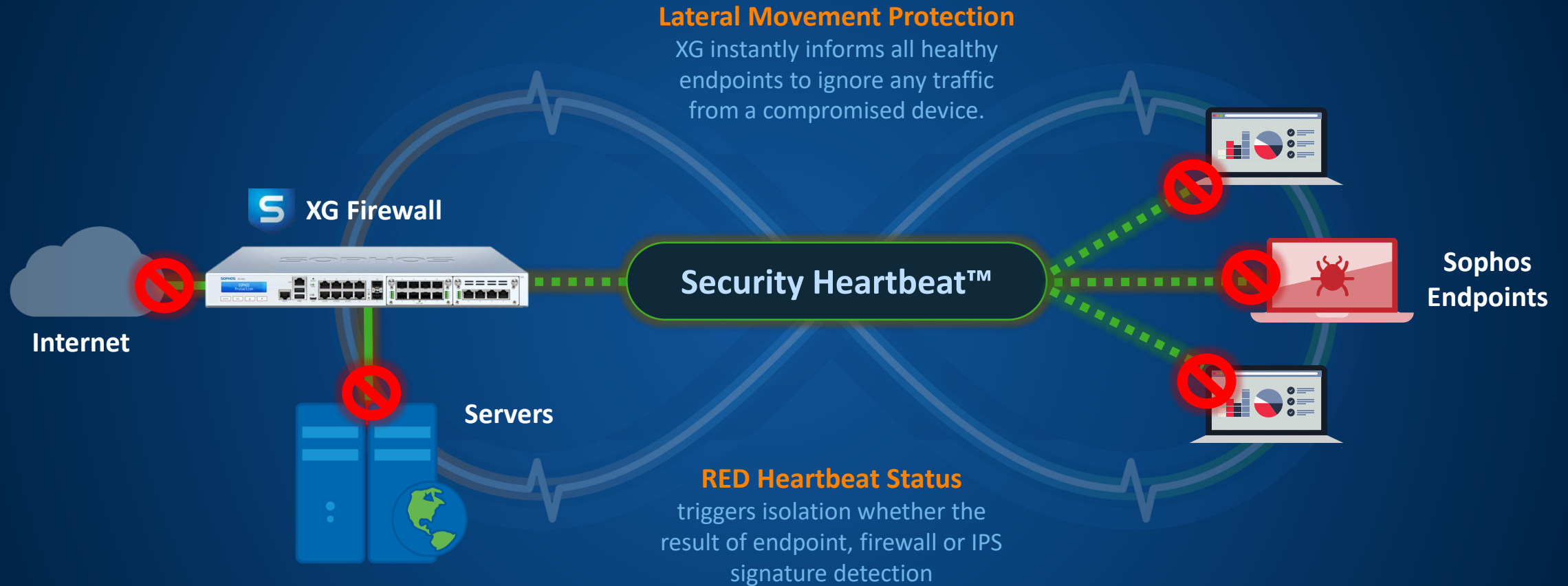


Productivity

- Firewall rule auto grouping
- Web policy overrides
- Web Policy-based SafeSearch
- IPSec Client
- Airgap deployment support

New in v17.5 - Lateral Movement Protection

Automatic system isolation – even on the same broadcast domain



Sophos Central Management

Your Complete IT Security Management Platform

One Console

- View **status and manage** XG alongside all other Sophos Central products
- Full device management via **SSO**
- **Secure remote access** to all your XG devices via Sophos Central
- Alerting and status for availability, license, performance, and security
- Manage **firmware updates**
- Option to store/maintain **backups** in Central
- **Zero-touch** setup of new appliances

Free for partners and customers!
No Additional License Required

The screenshot displays the Sophos Central Management console for a system named SF115_MR3. The interface is divided into several sections:

- System:** Shows performance metrics (0/0 RED, 0 Connected Remote Users), services (3/3 Wireless APs, 8 Live Users), and interfaces (VPN). It also displays CPU (16%), Memory (36%), Bandwidth (3MB/s), and Sessions (12).
- Traffic Insight:** Includes a line graph for Web Activity (818 max | 123 avg) and a bar chart for Cloud Applications (12 Apps, 154 MB In, 53.6 MB Out).
- User & Device Insights:** Features a Security Heartbeat with 1 Missing, 1 Warning, and 1 Connected status, and Synchronized Application Control with 199 Categorized Apps and 28 New Apps.
- Active Firewall Rules:** Shows 2 Unused, 1 Disabled, 3 Changed, and 0 New rules.
- Reports:** Lists 3 Risky Apps seen, 65 Objectionable websites seen, 110 MB Used by Top 10 Web users, and 22 Intrusion Attacks.
- Messages:** Contains a Warning about HTTPS-based management and an Alert about new RED firmware.

The left sidebar contains navigation menus for MONITOR & ANALYZE (Control Center, Current Activities, Reports, Diagnostics), PROTECT (Firewall, Intrusion Prevention, Web, Applications, Wireless, Email, Web Server, Advanced Threat, Synchronized Security), and CONFIGURE (VPN, Network, Routing).

XG Firewall in Sophos Central

See all of your firewalls under management

The screenshot displays the Sophos Central Admin interface for Firewall Management. The left sidebar contains navigation options: Dashboard, Alerts, Backup, Firewalls (selected), and Settings. The main content area is titled 'Firewall Management - Firewalls' and includes a breadcrumb trail: Overview / Firewall Management Dashboard / Firewalls. An 'Add Firewall' button is located at the top of the main area. Below it is a table listing three firewalls, all in a 'CONNECTED' state.

	FW Name, IP	OS Version, Model, Serial Number
CONNECTED	C0100139BBHDVD6 108.7.62.118	SN: C0100139BBHDVD6
CONNECTED	Burlington Lab VM 198.144.101.86	SN: C010016J436YT20
CONNECTED	Billerica Lab VM 1 108.7.62.118	SN: C01001CY9K2YPE0

Firewall Alerts

Manage Alerts for all firewalls in Sophos Central

SOPHOS CENTRAL Admin

Firewall Management

Marcus Jones | ABC Corp - Primary Admin

Alerts

Show all alerts | Mark As Acknowledged | Search Alerts

ALERTS	OCCURRED	DESCRIPTION	DEVICE	SUPPRESS ALERT PERMANENTLY
<input checked="" type="checkbox"/>	May 27, 2016 11:34 AM	The Network Protection module license for device with serial number C0100172YDJMTEF expires after 10 days	Karlsruhe_FW	<input checked="" type="checkbox"/>
<input type="checkbox"/>	May 27, 2016 11:34 AM	10% End-points Security Heartbeat changed to Red state for device with serial number C0100172YDJMTEF	India_FW	<input checked="" type="checkbox"/>
<input type="checkbox"/>	May 27, 2016 11:34 AM	RED tunnel Tunnel 1 at Branch India_FW is connected	India_FW	<input checked="" type="checkbox"/>

Store Backups Per Firewall

See and manage backups for your firewalls

The screenshot displays the Sophos Central Admin interface for Firewall Management. The left sidebar shows navigation options: Dashboard, Alerts, Logs, Reports, Backup (highlighted), Manage Firewalls, and Explore or Add Products. The main content area is titled "Firewall Management" and includes a user profile for Marcus Jones (ABC Corp - Primary Admin).

The "Backup" section is active, showing the "Schedule Backup" configuration. The "Backup Frequency" is set to "Weekly", and the "Backup Mode" is set to "Sophos Central". A list of devices includes "Firewall 2" with an "Add New Item" button. A "Save" button is located at the bottom of the configuration panel.

The "Manage Backup" section features a "Select Device" dropdown menu with "XG_Ind_D11A1" selected and a "Generate Backup" button. Below this is a table of backup records:

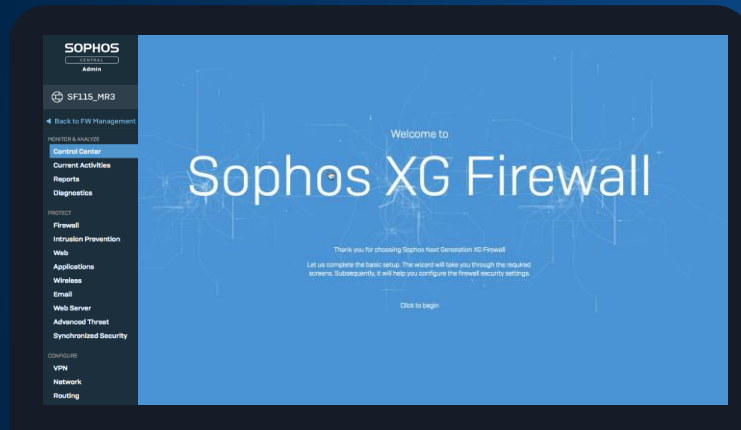
Backup Date	Backup Type
2017-11-20 23:45	Scheduled Backup / Manual Backup
2017-11-20 23:45	Scheduled Backup / Manual Backup
2017-11-20 23:45	Scheduled Backup / Manual Backup

A modal dialog titled "Manage firewall from Sophos Central" is overlaid on the right. It contains the following text: "Click apply to start managing and monitoring your firewall from Sophos Central. You can then log in to Sophos Central to approve managing this firewall or notify your Sophos Central administrator." There is a checked checkbox for "Send configuration backup to Sophos Central". The dialog has "Cancel" and "Apply" buttons at the bottom.

Zero-Touch Deployment

Remote device deployment without an on-site engineer

**1. Use the Setup Wizard in
Sophos Central**



**2. (Optional) Email the Config File
to the remote site**

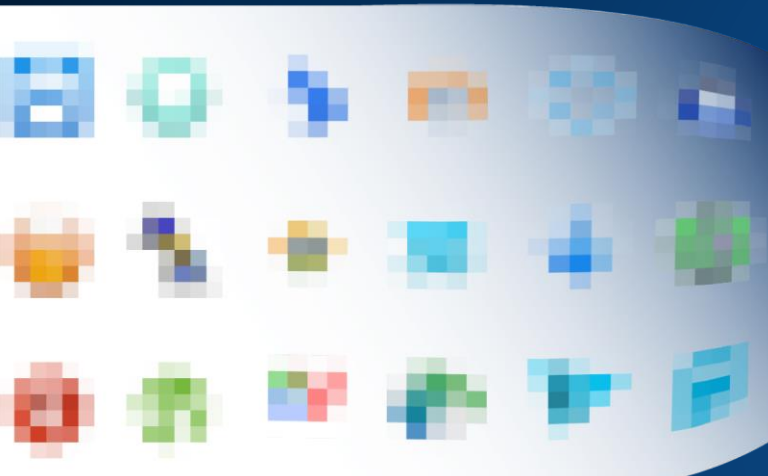


**3. Transfer the Config File to a
USB Stick**

**4. Start the device with the USB
stick connected**



Enhanced Sophos Synchronized App Control



Identify hidden Apps

Block or Control Unwanted Apps

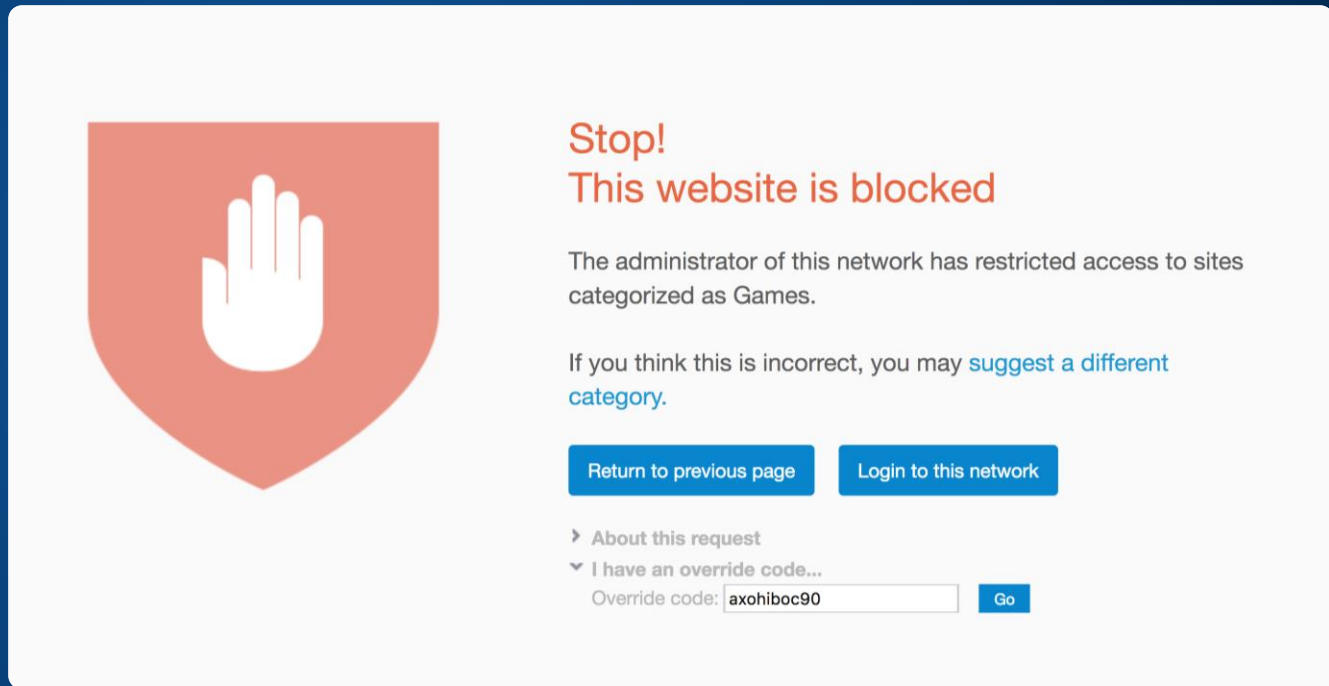
Prioritize Important Business Apps

New Web Policy Options

Greater flexibility for SafeSearch, YouTube and unblocking sites for education

What's New

- Override codes for blocked websites which can be configured/managed by teachers through the user portal



Stop!
This website is blocked

The administrator of this network has restricted access to sites categorized as Games.

If you think this is incorrect, you may [suggest a different category](#).

[Return to previous page](#) [Login to this network](#)

› About this request

▼ I have an override code...

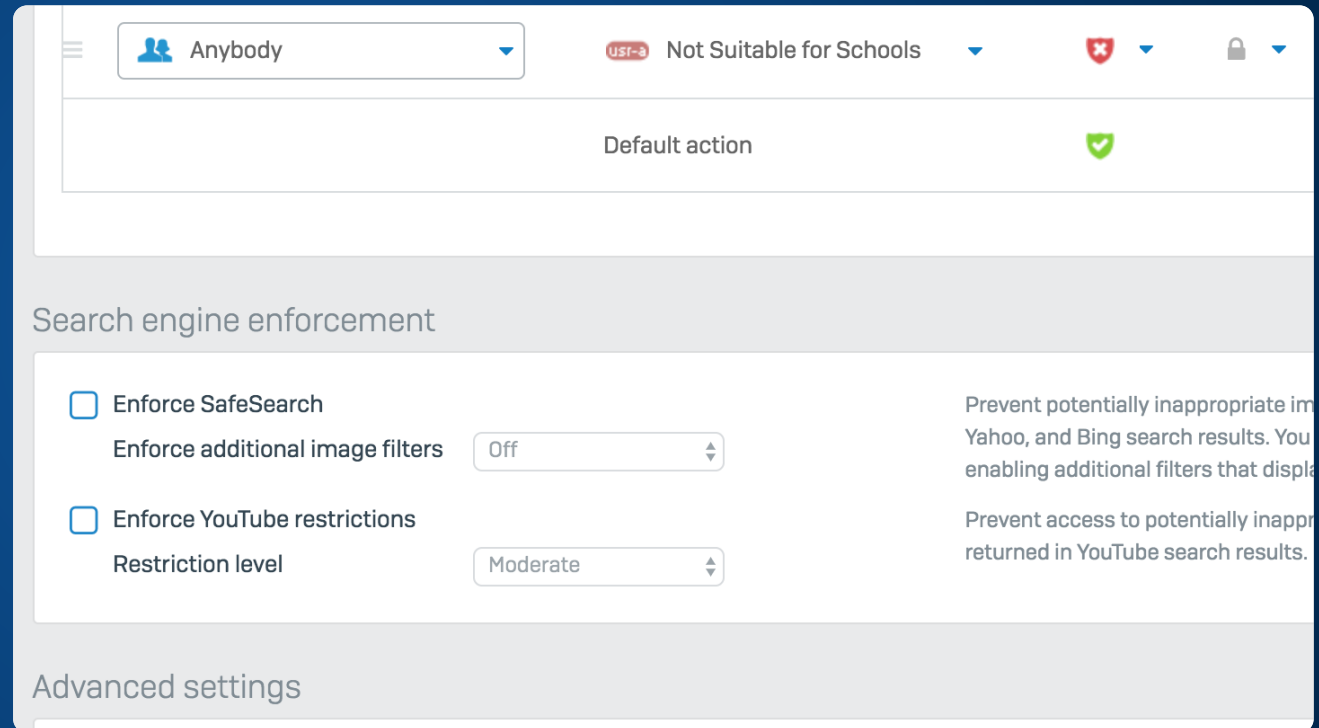
Override code: [Go](#)

New Web Policy Options

Greater flexibility for SafeSearch, YouTube and unblocking sites for education

What's New

- Override codes for blocked websites which can be configured/managed by teachers through the user portal
- **SafeSearch** and YouTube restrictions are now part of web filtering policy settings – enabling user/group based control of these features



JavaScript CryptoJacking Protection

One-Click Protection

The screenshot displays the Sophos XG Firewall management interface. The left sidebar shows navigation options under 'MONITOR & ANALYZE' (Control Center, Current Activities, Reports, Diagnostics) and 'PROTECT' (Firewall, Intrusion Prevention, Web, Applications, Wireless, Email, Web Server, Advanced Threat, Synchronized Security). The 'Web' option is selected. The main content area is titled 'Web' and includes a top navigation bar with links for 'How-To Guides', 'Log Viewer', 'Help', and 'Demo User'. Below this is a tabbed interface with 'General Settings' selected. A descriptive paragraph states: 'XG Firewall protects you by scanning HTTP and HTTPS traffic for unwanted content or malware, and enforcing SafeSearch restrictions. Use this page to modify protection settings, as well as settings for the proxy and web cache.' The 'Protection' section is titled 'Malware and Content Scanning' and contains several settings:

- Scan Engine Selection:** Single Engine (Optimal Performance). Note: Single scan engine is set to [Sophos](#). Sandstorm and content filters require use of the Sophos engine, either as the single scan engine or in Dual Engine mode.
- Scanning Mode:** Batch (Maximum Protection). Note: Real-time mode improves performance by allowing parts of a file to be downloaded before the scan is complete.
- Action on Malware Scan Failure:** Block (Best Protection). Note: Files that cannot be fully scanned because they are encrypted or corrupted may contain undetected threats.
- Do not scan files larger than:** 10 MB.
- Block potentially unwanted applications:** This checkbox is checked. Description: Protect users against downloading potentially unwanted applications. For more information about PUAs, please refer to the [Sophos website](#).
- Authorized PUAs:** A search/add field with a plus icon.

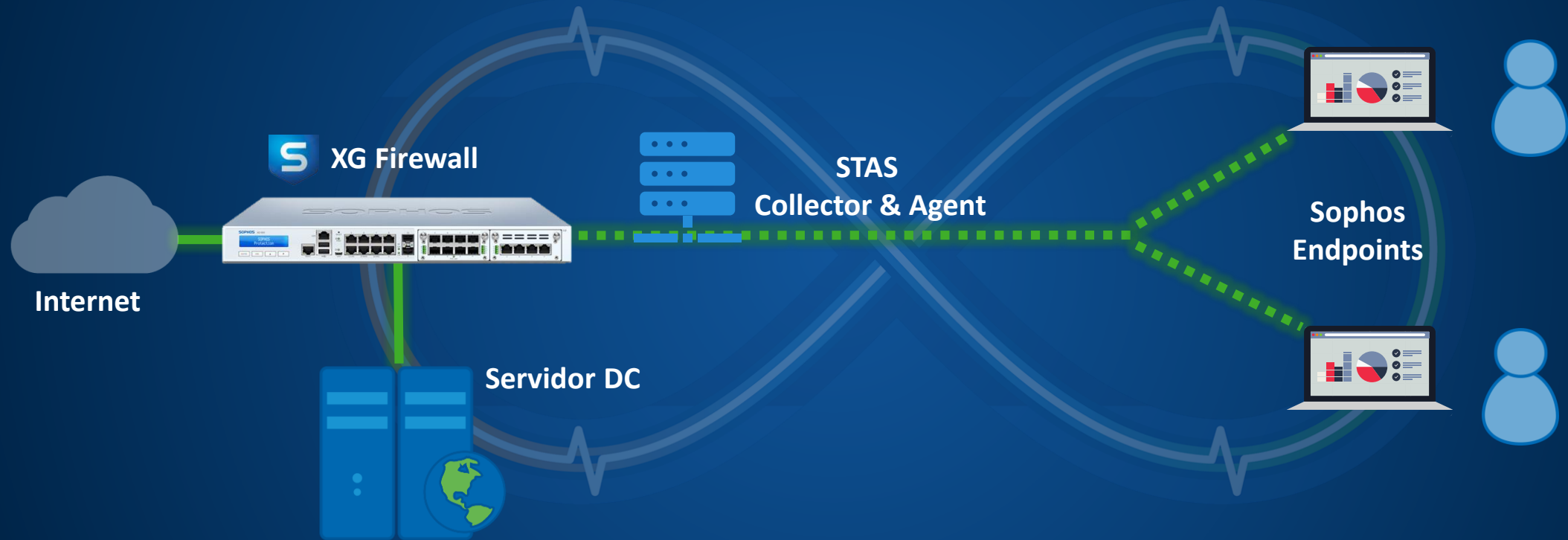
An 'Advanced Settings' link is located at the bottom left of the settings panel.

LAB



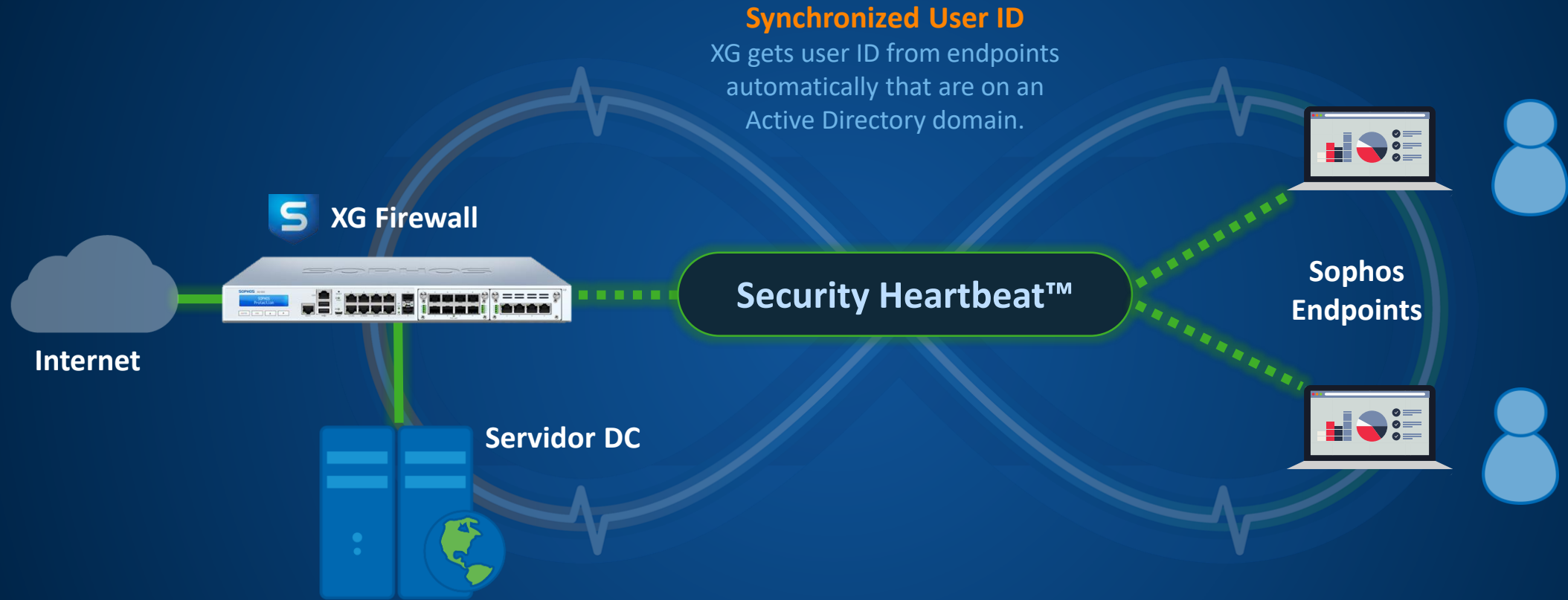
New Synchronized User ID

User identity synchronized between EP and Firewall automatically



New Synchronized User ID

User identity synchronized between EP and Firewall automatically



Log Viewer Enhancements

More powerful and streamlined trouble-shooting

What's New

- Column selector - select any 17 columns from a list of 44 possible fields
- Rule IDs referenced in logs are hyperlinked to open the related rule in the main console window
- Filters sorted alphabetically

The screenshot displays the Sophos Log Viewer interface. A 'Select columns' dialog box is open, allowing users to choose from 44 possible fields. The dialog is organized into several categories:

- General:** Time, Log comp, Action, Firewall rule, Status, Message, Message ID, Rule type, Log type.
- Network:** Src IP, Src port, Src zone, Src country, Src MAC, Src zone type, Dst IP, Dst port, Dst zone, Dst country, Dst zone type, In interface, Out interface.
- Protocol:** Src NAT IP, Src NAT port, Dst NAT IP, Dst NAT port, ICMP code, ICMP type, Protocol.
- Connection:** User name, User group, Bytes sent, Bytes received, Connection direction, Connection security.
- Threats and security:** HB status, IPS policy ID.
- Web and application:** Application, App filter policy ID, App category, App risk, App technology, Web policy ID.

The background shows a log table with the following columns: Dst IP, Src port, Dst port, Protocol, Rule type. The table contains several rows of log data, including entries for UDP and TCP traffic. A search bar and a 'Reset' button are visible at the top right of the log viewer.

Email Enhancements

Closing top requested feature gaps with SG UTM

What's New

- Recipient verification using Sender Policy Framework (SPF) for spoofing protection
- **Route to DNS Host**
- Improved MTA

The screenshot displays the Sophos XG Firewall web interface for configuring Email settings. The left sidebar shows the navigation menu with categories: MONITOR & ANALYZE (Control center, Current activities, Reports, Diagnostics), PROTECT (Firewall, Intrusion prevention, Web, Applications, Wireless, Email, Web server, Advanced threat, Synchronized Security), CONFIGURE (VPN, Network, Routing, Authentication, System services), and SYSTEM (Profiles, Hosts and services, Administration, Backup & firmware, Certificates). The main content area is titled 'Email' and includes a top navigation bar with links for How-to guides, Log viewer, Help, and admin. Below this is a sub-navigation bar with tabs: Policies & exceptions (selected), Data control list, SMTP quarantine, Mail spool, Mail logs, Encryption, General settings, Address group, and Relay settings. The main configuration area is titled 'Select the interface to route outbound mails' and contains the 'Spam protection' section. This section is currently turned ON and includes the following options: 'Check for inbound spam' (checked), 'Check for virus outbreak' (unchecked), 'Check for outbound spam' (unchecked), 'Use greylisting' (unchecked), 'Reject based on SPF' (checked, with a mouse cursor hovering over it), and 'Reject based on RBL' (unchecked). To the right of these options are two dropdown menus: 'Spam action' set to 'Drop' and 'Probable spam action' set to 'Warn'. Below these are fields for 'Prefix subject' (containing '[SPAM]') and 'Recipient verification' (set to 'Off (not recommended)'). At the bottom of the configuration area are 'Save' and 'Cancel' buttons.

IPS Enhancements

Added IPS policy granularity

What's New

- Added protection with TALOS (Cisco Sourcefire) pattern library augmented with additional patterns from Sophos Labs
- Increased granularity in policies with 60 categories (up from 21) with an easy inline search option

SOPHOS XG Firewall

MONITOR & ANALYZE

- Control center
- Current activities
- Reports
- Diagnostics

PROTECT

- Firewall
- Intrusion prevention**
- Web
- Applications
- Wireless
- Email
- Web server
- Advanced threat
- Central Synchronization

CONFIGURE

- VPN
- Network
- Routing
- Authentication
- System services

SYSTEM

- Profiles

Intrusion prevention

DoS attacks | **IPS policies** | Custom IPS si

Category Severity Platform Target

browser

- Browser-Chrome
- Browser-Firefox
- Browser-Ie
- Browser-Other
- Browser-Plugins
- Browser-Webkit

OK

SID	Category	Severity	Platform
2200304	Server-Webapp	2 - Major	Windows
9000495	Os-Windows	4 - Minor	Windows
9000496	Os-Windows	1 - Critical	Windows
1000070	Policy-Other	4 - Minor	

List of matching signatures [1 - 50 of 11206]

Action: Drop packet

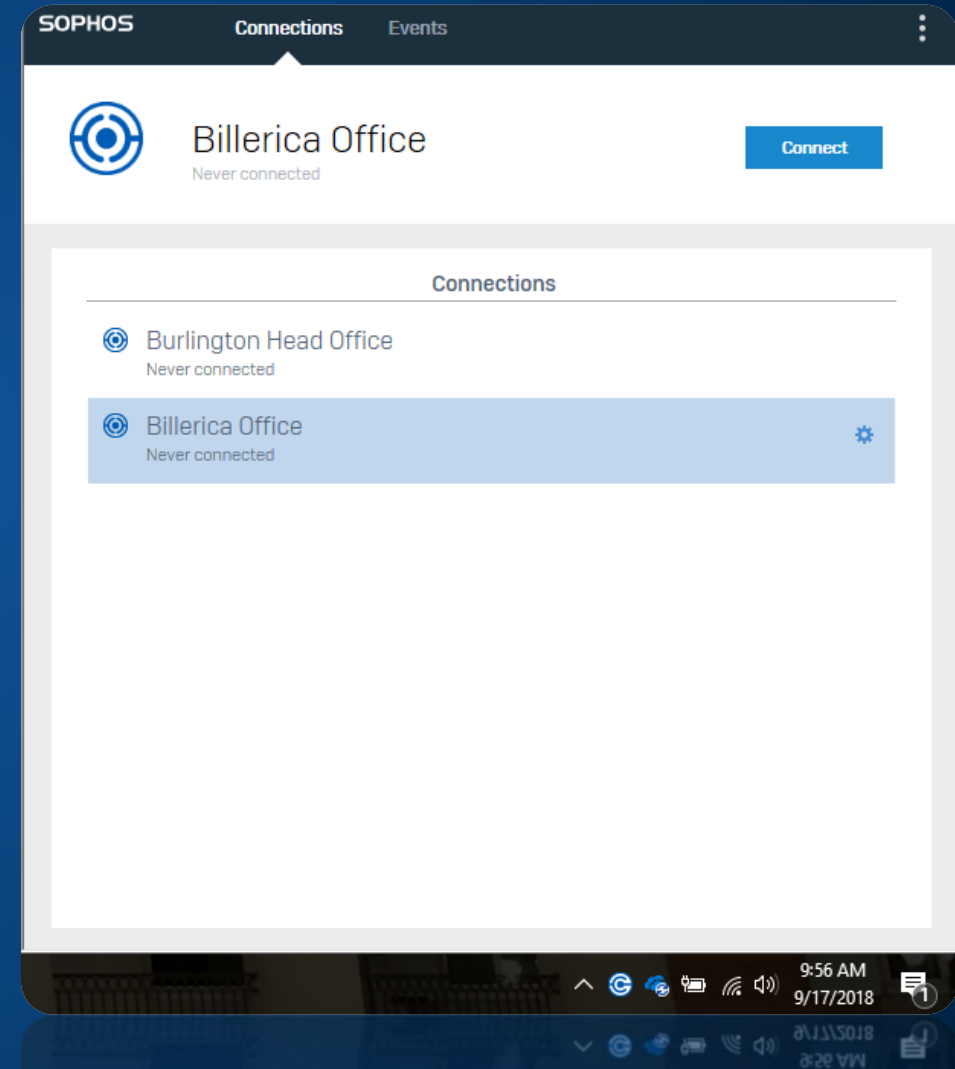
Synchronized Security via Remote VPN

Free client for easy, reliable remote connections

What's New

- IPsec VPN client for Windows/Mac
- Supports Synchronized Security for remote users
- Easy deployment and maintenance
- Simple operation requires no user education

Free for partners and customers!



Summary - Key New Features in v17.5



Synchronized Security

Lateral Movement Protection

Automatic isolation at every point in your network

Synchronized User ID

User authentication through Security Heartbeat



Central Management

Sophos Central Management

XG Firewall joins Sophos Central:

Manage all your IT security from a single pane of glass

[Ideas.sophos.com](https://ideas.sophos.com)

Top Requested Features

Education – Protection - Networking

- Chromebook Authentication
- Web Policy-based SafeSearch
- Classroom web policy overrides
- Email anti-spam enhancements
- Sophos Connect IPSec Client
- Firewall rule auto grouping
- Log viewer enhancements
- Client Authentication App Enhancements
- TALOS IPS Enhancements
- Airgap deployment support



Wireless

APX Wireless Access Points

WAVE 2 Performance:

Faster connectivity, higher capacity and optimal performance

SOPHOS

Cybersecurity made simple.