SOPHOS
Security made simple.

Keep your network under control

Why network admins need complete application visibility

The Evolution of the Firewall

Over the years, the role of the firewall has steadily evolved from protecting networks from external hacks and attacks to focus more attention inward – to identify and eliminate potential risks and enable compliance. Part of this evolution is a response to the shift in the threat landscape towards malware and intrusions designed to exploit vulnerabilities in applications rather than the network perimeter itself. In addition, the growing obligation to provide a reasonable level of compliance, protect against breaches and data loss, and optimize network performance has also contributed to this inward shift.

The next-generation firewall was essentially born out of the need to provide much needed visibility and control over users and their applications. The next-gen firewall literally rises above the ports and protocols of earlier stateful firewalls to higher layers in the OSI model to provide application and user awareness.

Next-gen firewalls use deep packet inspection to identify applications and associate them to users or hosts on the network so administrators can provide appropriate controls. For example, it's extremely helpful to be able to identify users running peer-to-peer file sharing apps and block them, while controlling excessive streaming media viewing, all while prioritizing important business applications like the ERP system, VoIP traffic, and CRM software.

A Sophos Whitepaper September 2017

How Next-Gen Firewall App Control Works

The way firewalls identify applications is by matching patterns in the traffic to known signatures. It's analogous to facial recognition. When you see a person's face you don't know, you can compare it to a bunch of pictures, if you get a match, you know who you're dealing with, if you don't get a match, you really have no idea who that person is.

"60% of network traffic is unidentified on average."

Application Control works exactly the same way. While some applications wear the equivalent of a name tag, making it easy to identify them, most apps don't and some even go out of their way to slip through unidentified. Of course, when a match is made and an app is positively identified, the firewall can control the application – using traffic shaping to prioritize or limit bandwidth consumption, or block it outright. But if there's no match, the firewall has no idea what it's dealing with and no control.

The Problems with Next-Gen Firewall App Control

As you can probably imagine, many applications will not provide a positive match. Many risky applications that would typically be blocked in most organizations such as BitTorrent clients use clever methods to constantly change their traffic patterns and the way they connect out of the organization in order to evade detection. This is not unlike a person changing their hair color and adding a moustache to evade facial recognition.

Other applications use encryption to avoid detection which is much like a person wearing a ski mask. And many other applications will pretend to be a browser so they can pass through the firewall unchecked. This is analogous to a bad person disguising themselves to look like a well known celebrity. And then there are applications that have recently changed or are one-off, custom, or simply too obscure to have a matching pattern. These are like people that have no recent photo on file.

In fact, as firewalls have gotten better and better at identifying and controlling unwanted applications, these applications have gotten better and better at avoiding detection.

The end result is that most of the traffic passing through a modern firewall these days is unknown, unidentified, or simply too generic to be classified or controlled.

Does your App Control Report look like this?

Top Applications

Application Name	Percentage of Applications
General UDP	25.45%
General HTTPS MGMT	24.26%
General DNS	17.8%
General TCP	14.39%
Service RPC Services (IANA)	8.86%
Bit Torrent Protocol - UDP Activity 1 (Reqs SIB 5)-63	1.60%

Conventional firewall dashboard showing categories that could not be identified

How big is the problem?

In an effort to get a better understanding of how widespread this issue is, Sophos recently conducted a survey of mid-sized organizations to determine how much of their application traffic was going unidentified and uncontrolled:

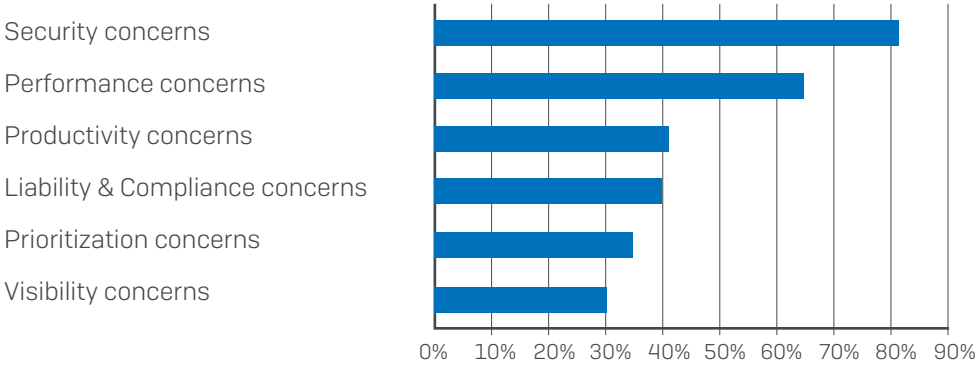
- Nearly 70% of organizations out there have a next-gen firewall or UTM with application awareness
- On average 60% of traffic is going unidentified… and many organizations reported that up to 90% of their application traffic was unidentified

If you're concerned about the security, liability, or performance impact this has on your organization, you're not alone…

- 82% of survey respondents are rightfully concerned about the security risk this lack of application visibility implies
- 65% were concerned with the impact this could be having on their network performance
- 40% were concerned with potential legal liability and compliance risks

Top concerns with the current lack of application visibility:

What are your concerns with unidentified network traffic? (Multiple choice)



The Top Evasive and Unidentified Applications

These evasive applications pose a high security risk due to vulnerabilities, a compliance risk due to potential inappropriate or illegal content, and a productivity and bandwidth consumption risk.

- IM and Conference Apps (e.g. Skype, TeamViewer)
- BitTorrent and other P2P Clients (e.g. uTorrent, Vuze, Freenet)
- Proxy and Tunnel Clients (e.g. Ultrasurf, Hotspot Shield, Psiphon)
- Games (e.g. Valve and Steam)

Unfortunately, it's nearly impossible for you to know if you have any of these apps running on your network – because firewall signatures are simply not going to find a match in most cases.

In addition to these applications, there are countless more apps that are both benign and potentially unwanted that have resorted to utilizing generic HTTP and HTTPS connections to communicate out through the firewall, counting on the fact that nearly every organization opens up their firewall for internet access on port 80 and 443. In your reports, these will simply appear as HTTP, HTTPS, SSL, Web Browsing, and other general non-helpful categories.

And perhaps most importantly, there are vertical applications, ERP solutions, CRM software and other business essential applications that may be unique to your organization that are going undetected, and potentially getting crushed under the weight of web surfing and other unwanted app traffic simply because they are not popular or prolific enough to have a signature.

Fortunately, there's a rather elegant solution to this problem.

The Solution

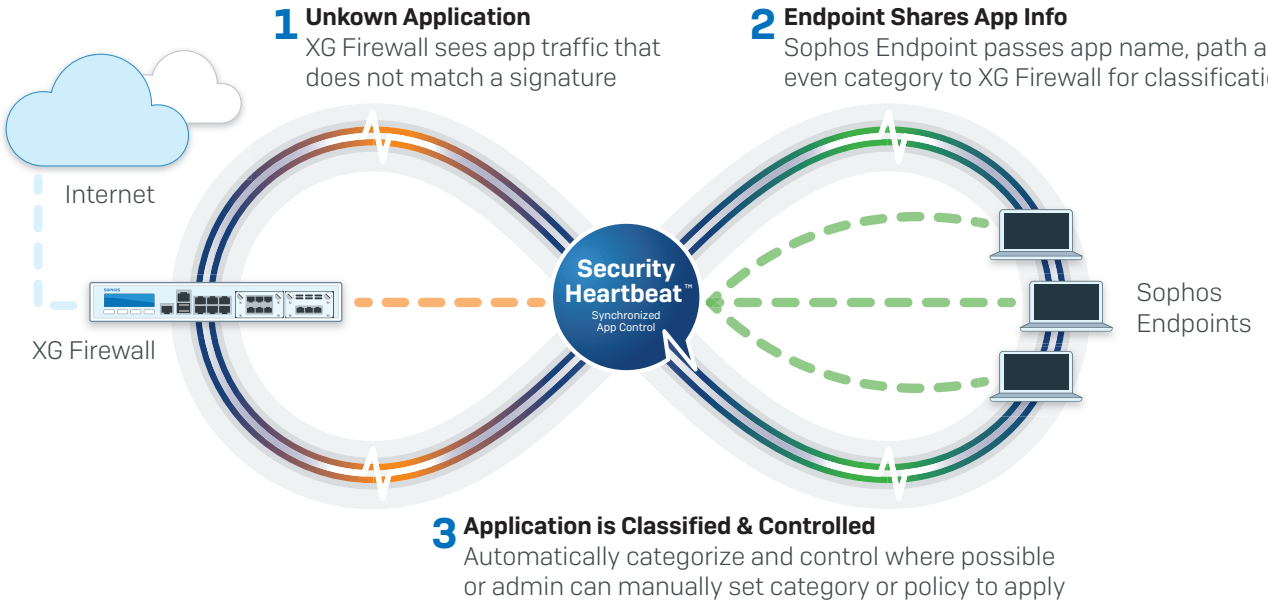
While next-gen firewalls need to rely on deep packet inspection, pattern matching, and signatures to try and identify applications as they traverse the network, the endpoint is in the unique position where it inherently knows with absolute clarity exactly what executables are generating all network traffic. Hence the solution, a rather obvious matter of connecting the endpoint with the firewall to share this valuable information. Fortunately, at Sophos, we have the technology in place to simply and effectively enable this: Synchronized Security.

Sophos Synchronized Security is a revolutionary new approach to IT security that enables security products to share information and work together to provide real-time insights, unparalleled protection, and automated incident response.

One of the first Synchronized Security innovations, Security Heartbeat™, connects Sophos Central managed endpoints with Sophos XG Firewall to share endpoint health status, enabling instant identification of systems at risk. When a compromise is detected at eithe r the endpoint or the firewall, traffic light style indicators and alerts are issued in real-time, immediately identifying the computer, user, and process involved. And perhaps the most important benefit of Security Heartbeat, is that the firewall can include endpoint health status in firewall rules, enabling automated response, either limiting access or completely isolating the compromised system until it can be cleaned up. This has reduced response time from hours to seconds and helps reduce the risk of infections spreading to other parts of the network.

Another Synchronized Security innovation is Synchronized App Control. As the name implies, Synchronized App Control leverages Sophos' unique Synchronized Security ecosystem to effectively and elegantly solve the problem with identifying unknown, evasive or custom application traffic on the network. Synchronized App Control leverages its information sharing ability with the Endpoint to determine the source of unidentified app traffic on the network, effectively removing this thick veil covering networks today.

Synchronized App Control in Action



It's the first major breakthrough in network application visibility and control since the next-gen firewall was conceived.

When a Sophos Central managed endpoint connects to a network with an associated XG Firewall, it will establish a Security Heartbeat™ connection to share health and security status and telemetry. In addition, the endpoint will now also use this connection to share the identity of all network applications with the firewall.

Where the firewall can't confirm the identity of the application using traditional signature techniques because the application is evasive, custom, new or using a generic connection, the app information provided by the endpoint will be utilized to identify, classify and control it. Where possible, the applications shared by the endpoint will be automatically classified into an appropriate category. This will automatically subject the newly identified and classified application to any app control policies that are already being enforced on the firewall.

For example, an evasive BitTorrent client will be automatically assigned to the Peer-to-Peer application category. And if the firewall has an app control policy in effect to block Peer-to-Peer apps, the new BitTorrent traffic will be automatically blocked – without any intervention by the network administrator.

The Benefits:

Identify Unknown Apps

Synchronized App Control reveals all the apps that are currently going unseen on the network including all new apps as well as tunneling, proxy and VPN applications that often use encryption to bypass firewall control – creating an enormous blind-spot as well as a variety of compliance, performance, and security risks. If there are existing policies in place to block or traffic shape these types of applications, the newly identified applications falling into this category will be subject to the same policies automatically. In addition the users and hosts involved will be easily identified enabling intervention and education where appropriate.

Prioritize Custom Apps

Synchronized App Control will immediately identify custom business applications that are completely invisible to your current firewall such as finance, CRM, ERP, manufacturing and other networked applications that are important to your organization. For the first time, Synchronized App Control provides an opportunity to apply traffic shaping and QoS policies to ensure these mission-critical applications are getting appropriate priority and optimal performance.

Control Evasive Apps

Synchronized App Control will automatically discover all evasive applications that are continuously changing the way they connect and communicate in order to evade detection and control. In effect, Synchronized App Control puts an end to these tactics once and for all. Regardless of how evasive these apps try to be, they will be completely unable to evade Synchronized App Control.

"It's the first major breakthrough in network application visibility and control since the next-gen firewall was conceived."

Which Sophos Products are Needed:

Sophos provides a full ecosystem of IT security products that integrate simply to provide Synchronized Security. Enabling Security Heartbeat™ and Synchronized App Control and all the added security, visibility and control they provide couldn't be easier. At a minimum, Sophos XG Firewall and Intercept X are required, but both products can be deployed alongside your existing IT security infrastructure in a complementary manner to provide Synchronized Security without any disruption or rip-and-replace.

Sophos XG Firewall can be deployed either in-line with your existing firewall or as your main firewall gateway. It also works in a reporting and visibility only mode when XG Firewall is connected to a switch mirror port in Discover Mode (also known as TAP mode).

On the endpoint, Intercept X can be deployed alongside your existing desktop AV solution, or you can choose Sophos Central Endpoint Advanced for complete endpoint protection from Sophos. Both products support Synchronized Security along with XG Firewall on both Windows and Mac platforms.

Summary

Next-gen firewalls are failing to deliver on their promise to provide application awareness. There's an inherent limitation in the effectiveness of signature based application detection techniques that means the majority of app traffic on today's networks is going unidentified and unchecked. It's a significant and serious problem. It presents enormous security, productivity, performance, and compliance risks.

Fortunately, there's an elegant and effective solution: Synchronized App Control leverages Sophos unique Security Heartbeat™ connection between Sophos Central managed endpoints and XG Firewall to share network application information with absolute clarity.

XG Firewall with Synchronized App Control is able to automatically identify, classify and control all unknown application traffic on the network. It's a major breakthrough in network visibility and control that renders all other next-gen firewalls obsolete.

Single Point of Contact provides comprehensive IT security consulting services to ensure the impact of a potential cyberattack is minimal. We tailor our services to ensure our clients stay secure around the clock, so you can ensure you are getting the best service possible. To learn more about how our services can protect you from a security breach, email or call us at 800-791-4300.

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

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

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

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

22-09-17 WPNA (NP)

single point of contact

SOPHOS