XG Firewall v18

Yannick Escudero

Settembre 2019

What's New in XG Firewall v18

Enhancements to Visibility, Protection, Performance and Networking

Xstream Architecture

Xstream DPI Engine

Xstream SSL Inspection

Xstream Network Flow FastPath

Threat Intelligence

Deep Learning Analysis

Threatometer

Detailed Threat Analysis Reports

Networking Flexibility

SD-WAN Features

PBR, NAT, Interfaces

Much More

XG Firewall v18.0 EAP 1

XSTREAM Architecture

- SSL inspection
- DPI engine
- FastPath

Rules and Policies

- Firewall rules
- SSL/TLS inspection
- Enterprise NAT

Network and Routing

- SD-WAN policy routing
- Interface enhancements

Protection and Filtering

- Web quotas
- DKIM and BATV
- Sandstorm and IPS

Logs, Reporting and Alerts

- Central reporting
- Logging
- Alerts

Other Enhancements and Upgrading

- Authentication
- Upgrading

XSTREAM Architecture

SSL Inspection

High-performance, high-connection capacity across all ports, protocols and applications

Enterprise-grade controls to optimize security, privacy and performance

Support for TLS 1.3 and all modern cipher suites

DPI Engine

Comprehensive threat protection in a single high-performance streaming DPI engine

Proxy-less scanning of traffic for AV, IPS, web threats, application control and SSL inspection

Decrypting traffic provides more effective protection from pattern changing applications

Network Flow FastPath

Intelligent offloading of traffic processing to transfer trusted traffic at wire speeds

Offloading can be controlled through policy or intelligently by the DPI engine based on traffic characteristics to accelerate important cloud application traffic

Firewall

xstream

Packet Processing Architecture

FastPath - Initial Connection

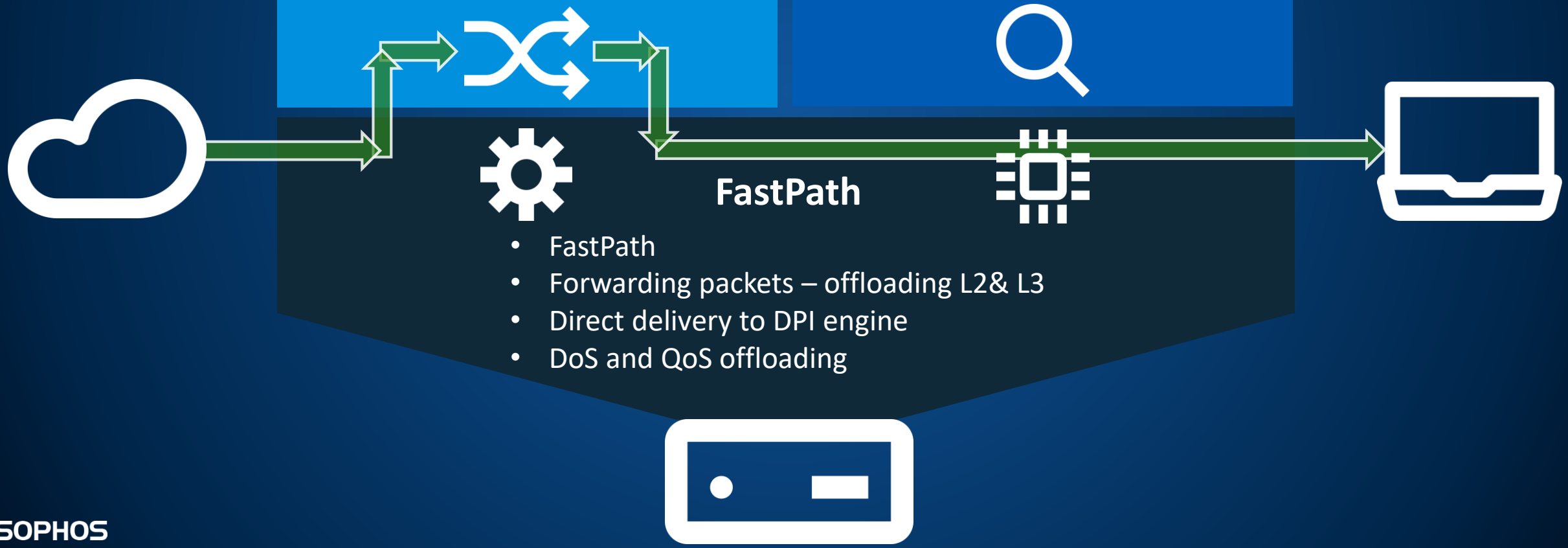
XSTREAM Architecture

Firewall Stack

- Connection management
- Allow, block, secure decisions
- DoS and QoS

DPI Engine

- Streaming DPI processing
- Intelligent offloading
- Proxyless web filtering
- SSL policy and inspection



FastPath

- FastPath
- Forwarding packets – offloading L2& L3
- Direct delivery to DPI engine
- DoS and QoS offloading

SOPHOS

FastPath – Full Offload

XSTREAM Architecture

Firewall Stack

- Connection management
- Allow, block, secure decisions
- DoS and QoS

DPI Engine

- Streaming DPI processing
- Intelligent offloading
- Proxyless web filtering
- SSL policy and inspection

FastPath

- FastPath
- Forwarding packets – offloading L2& L3
- Direct delivery to DPI engine
- DoS and QoS offloading

SOPHOS

FastPath - Initial Packet Delivery to DPI Engine

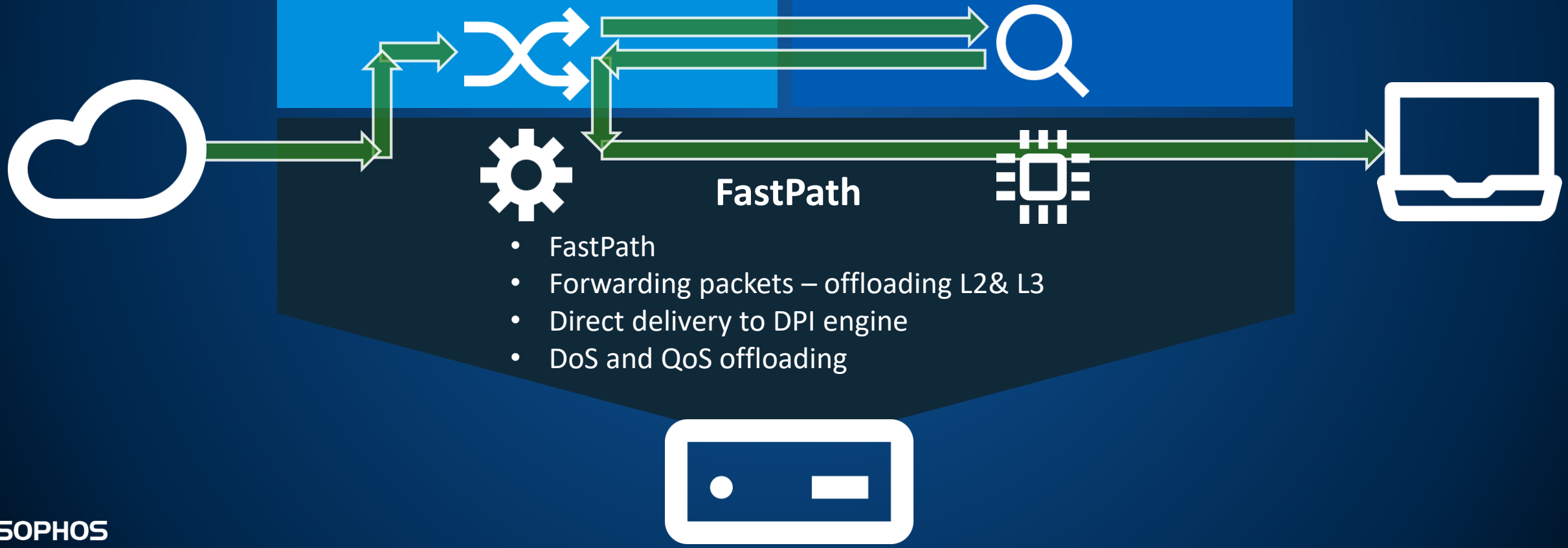
XSTREAM Architecture

Firewall Stack

- Connection management
- Allow, block, secure decisions
- DoS and QoS

DPI Engine

- Streaming DPI processing
- Intelligent offloading
- Proxyless web filtering
- SSL policy and inspection



FastPath

- FastPath
- Forwarding packets – offloading L2& L3
- Direct delivery to DPI engine
- DoS and QoS offloading

FastPath - Firewall Offload

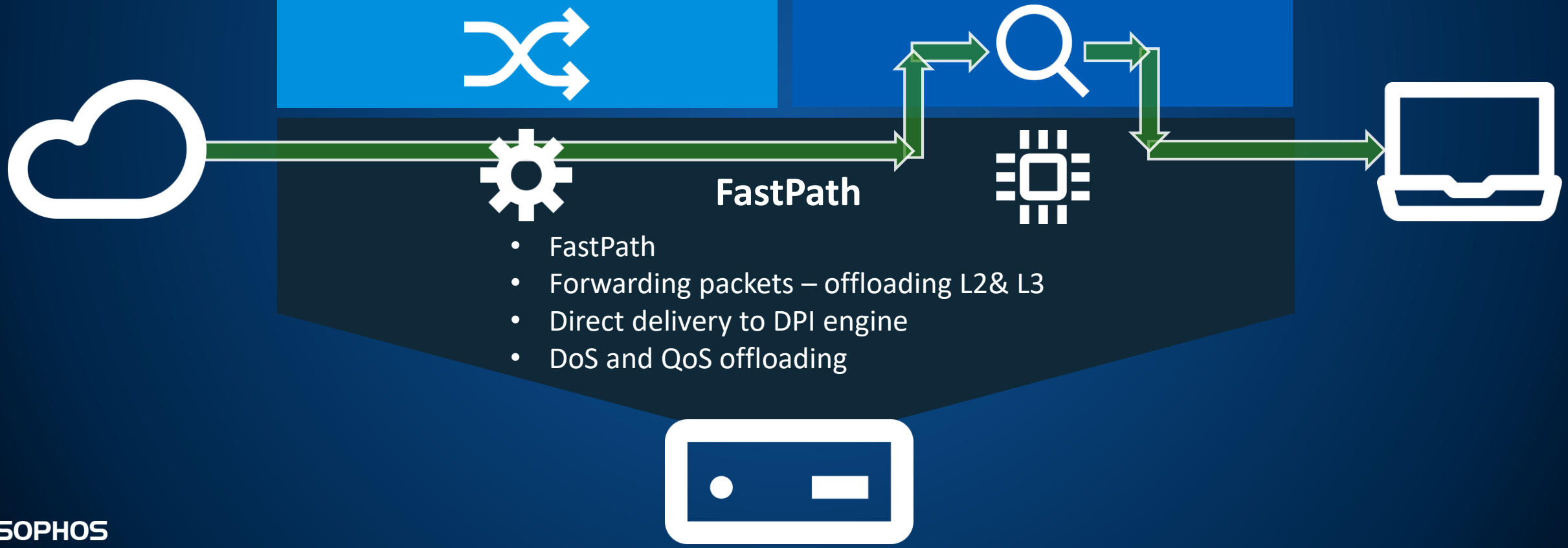
XSTREAM Architecture

Firewall Stack

- Connection management
- Allow, block, secure decisions
- DoS and QoS

DPI Engine

- Streaming DPI processing
- Intelligent offloading
- Proxyless web filtering
- SSL policy and inspection



FastPath

- FastPath
- Forwarding packets – offloading L2& L3
- Direct delivery to DPI engine
- DoS and QoS offloading

SOPHOS

FastPath - Full Offload of known safe connections

XSTREAM Architecture

Firewall Stack

- Connection management
- Allow, block, secure decisions
- DoS and QoS

DPI Engine

- Streaming DPI processing
- Intelligent offloading
- Proxyless web filtering
- SSL policy and inspection

FastPath

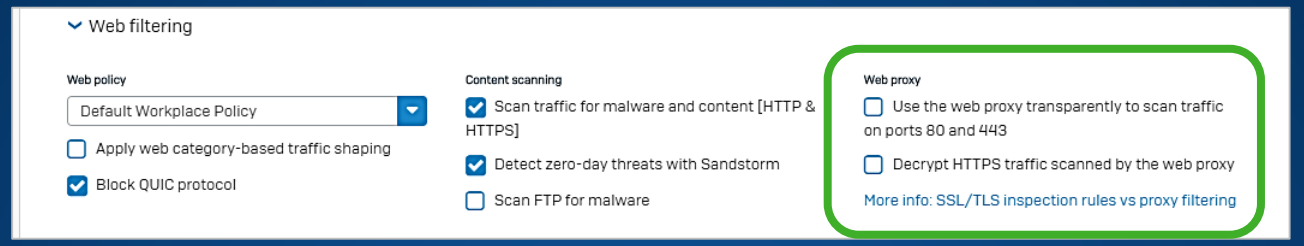
- FastPath
- Forwarding packets – offloading L2& L3
- Direct delivery to DPI engine
- DoS and QoS offloading

SOPHOS

The XSTREAM FastPath technology

- allows low latency high throughput packet forwarding at line speeds
- results in more responsive networking applications
- lowers load on the appliance

Firewall Rules: Web Filtering (DPI)



example.com on port **80**

example.com on port **443**

example.com on port **xyz**

Firewall

Decrypt HTTPS

Web Policy

Content Scan

Web Proxy

SSL/TLS Rules

Web Policy

Content Scan

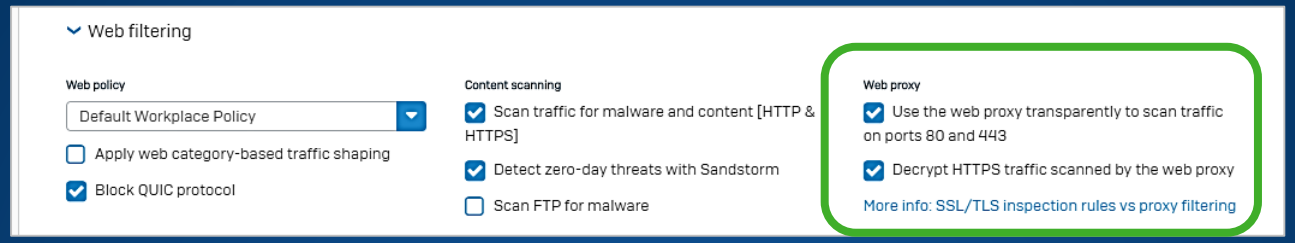
App Control

IPS

DPI Engine

FastPath

Firewall Rules: Web Filtering (Proxy)



example.com on port **80**

example.com on port **443**

example.com on port **xyz**

Firewall

Decrypt HTTPS

Web Policy

Content Scan

Web Proxy

SSL/TLS Rules

Web Policy

Content Scan

App Control

IPS

DPI Engine

FastPath

DPI Web Filtering is beneficial for

- High performance, low latency web filtering
- Capability to offload trusted connections to FastPath
- Lowering load on the appliance

Enterprise grade SSL/TLS Inspection Rules

New SSL inspection engine in v18 that is port and application agnostic

SSL policy is decoupled from firewall policies

Decrypted packets are sent to IPS, application control, web filtering and antivirus

Benefits of the new SSL/TLS inspection

- Port and application agnostic SSL/TLS scanning enhances security and visibility across all SSL/TLS encrypted traffic

- Allows granular, customizeable SSL/TLS decryption policies to comply personal security and regulatory requirements (as for example PCI-DSS etc.)

- Allows – uniquely in the market – specific application based SSL/TLS policies for Synchronized Security recognized Applications

Enterprise NAT

NAT rules have been decoupled from firewall rules

You can create a linked NAT rule that matches on the same criteria as the firewall rule it is linked to

NAT rules still require firewall rules to allow traffic

Supported NAT Types

SNAT (source NAT)

Dynamic IP and port (mapped internally)
Change the source port and/or IP address

DNAT (destination NAT)

Many-to-one, one-to-one, one-to-many
Change the destination port and/or IP address

Reflexive policy

One-click in UI
Allows traffic to traverse the NAT in the opposite direction

Loopback policy

One-click in UI
Allows internal traffic to access services using the public IP of the XG Firewall

Linked NAT policy

SNAT rule that will match on the same criteria as a linked firewall rule

NAT load balancing

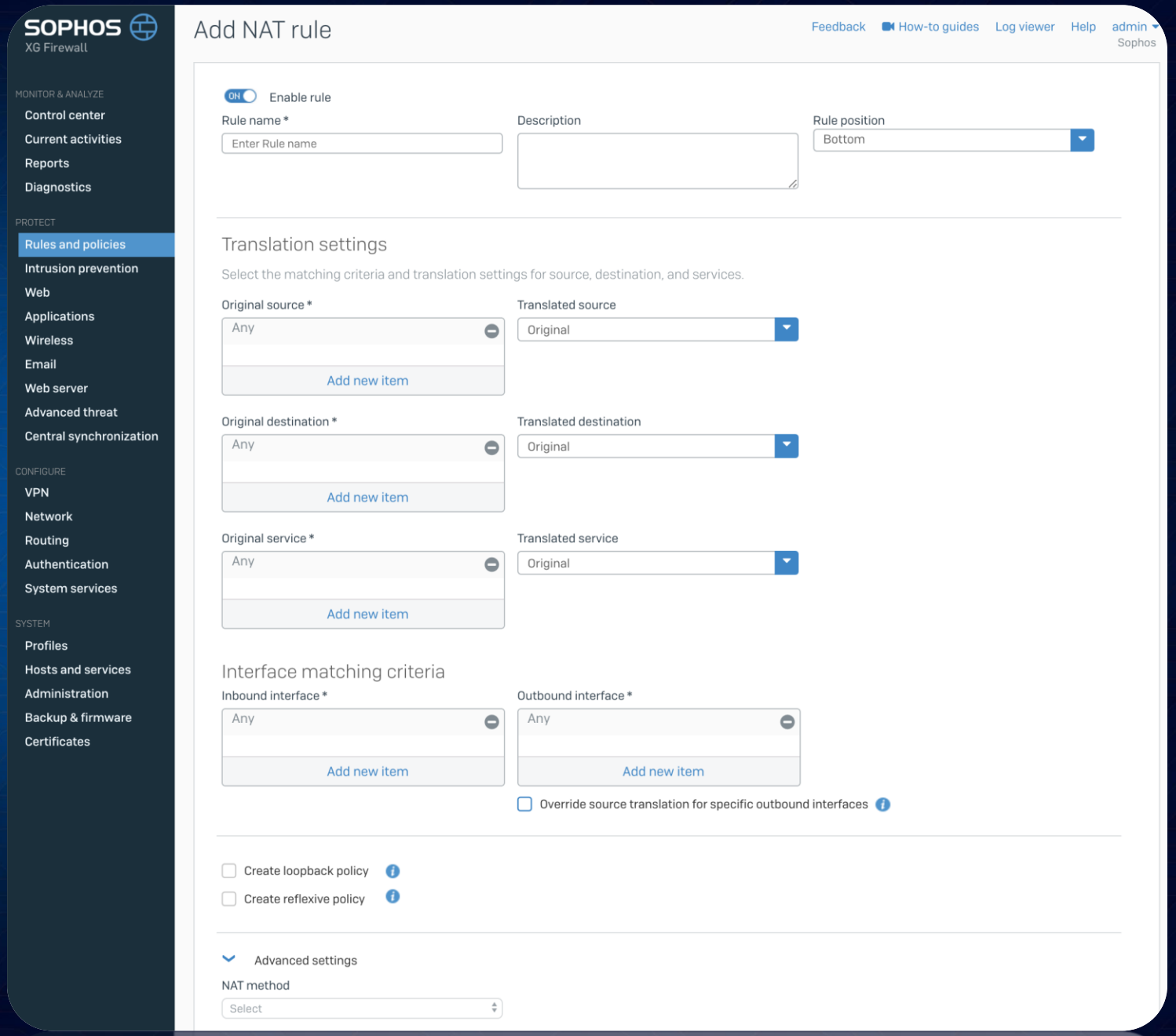
Round robin, random, sticky IP, first alive, one-to-one

Enterprise NAT

Added Power and Flexibility

Enhancements

- Dedicated Table for NAT Rules
- Source NAT and Destination NAT in a single rule – easier simpler NAT rules with better visibility
- Snap-in NAT Rules to Firewall Rules with inline creation
- One-click Loopback and Reflexive Policy Rule Options



Benefits of the Enterprise NAT features

- Simplified NAT handling due decoupling from firewall policies
- Full featured NAT capabilities to cover all upcoming NAT'ing demands
- NAT Loadbalacing allows redundancy and/or loadbalancing of NAT'ed connections

Many other V18 enhancements as…

- Renameable interfaces
- VLAN's on bridges
- SNMPv3
- Log viewer enhancements
- Firewall rule management enhancements
- Enhanced DDNS support
- Alerts & notifications enhancements
- DKIM & BATV Anti Spam Protection
- Kerberos Authentication
- Radius timeout with 2FA
- DHCP Relay enhancements
- Secure Syslog with standard Syslog
- Dynamic GeoIP Databse
- Jumbo Frame Support
- Bridge Interface enhancements
- Web policy enhancements
- Sandstorm Threat Intelligence Analysis
- SD-WAN Policy Routing

Planned V18 Schedule

- September 2019 – Public customer and partner Early Access Program (EAP) begins
- Beginning of 2020– General Availability

Between September and January 2020 there will be multiple EAP phases as the team continues to roll out updates to EAP participants.

Disclaimer: Plan may vary, as this is an outlook into the future…

SOPHOS

Security made simple.