# CÂMARA MUNICIPAL DE BELO HORIZONTE

**Of. COOINF Nº 019/2016**

Belo Horizonte, 08 de setembro de 2016.

À CPL

Senhora Pregoeira,

Em resposta à sua solicitação de avaliação técnica da Proposta Comercial da empresa Tracenet Treinamento e Comércio em Informática Ltda, referente ao Pregão Eletrônico nº 36/2016, temos as seguintes considerações:

Após análise preliminar verificamos que o produto ofertado pelo participante; equipamento marca SOPHOS, modelo XG550, pelo menos nos aspectos abaixo, não atende as características exigidas pelo edital.

| Item Termo de Ref. | Descrição | Comprovação da incapacidade de atendimento ao edital |
|---|---|---|
| **4.6.1.15** | Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For | Não foi identificada na documentação técnica do fabricante, a capacidade da solução de atender ao requisito técnico. A lista de opções descrita na documentação não engloba o exigido no requisito.<br>**Evidência: Vide páginas 422 e 572 (APPEND A – LOGS) do Administrator guide do produto.**<br><br>https://www.sophos.com/en-us/medialibrary/PDFs/documentation/Sophos-XG-Firewall-Administrator-Guide.pdf?la=en<br><br>UserAgent: identifica uma aplicação que acessou o recurso http (atende)<br>HTTP referer: endereço IP de quem acessou a página (atende)<br>X-Forwarded: identifica se foi um proxy que requisitou o acesso HTTP. Em geral ao usar transparent proxy não há uso dessa função ao menos que exista proxy explicito. iView identifica estes IPs de origem como sendo do proxy e não do usuário. (atende)<br><br>https://demo.sophos.com, com usuário: demo e senha: demo, pode ser consultados em relatórios os que identificamm as aplicações (user agent), IP de quem originou (HTTP referer) e se foi proxy ou não (X-forwarded). |
| **4.2.9** | Controle de inspeção e de-criptografia de SSH por política. | Não foi identificada na documentação técnica do fabricante, a capacidade da solução de atender ao requisito técnico. A lista de opções descrita na documentação não engloba o exigido no requisito.<br>**Evidência: Vide páginas 25/26 do Administrator guide do produto.** |

| | | |
|---|---|---|
| | | https://www.sophos.com/en-us/medialibrary/PDFs/documentation/Sophos-XG-Firewall-Administrator-Guide.pdf?la=en<br><br>Feito via IPS/proxy reverso, realizado a monitoração do SSH<br><br>https://kb.cyberoam.com/redirfile.asp?id=6427&fstore=&SID= |
| **4.2.10** | A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança | Não foi identificada na documentação técnica do fabricante, a capacidade da solução de atender ao requisito técnico. A lista de opções descrita na documentação não engloba o exigido no requisito.<br>**Evidência: Vide páginas 25/26 do Administrator guide do produto.**<br><br>https://www.sophos.com/en-us/medialibrary/PDFs/documentation/Sophos-XG-Firewall-Administrator-Guide.pdf?la=en<br><br>Feito via IPS/proxy reverso, realizado a monitoração do SSH<br><br>https://kb.cyberoam.com/redirfile.asp?id=6427&fstore=&SID= |
| **5.1.9** | 2 (duas) GBps interfaces dedicadas para alta disponibilidade útil. A contar do aceite da instalação | Não foi identificado na documentação técnica do fabricante, a existência de 02 portas GBps dedicadas a alta disponibilidade conforme requisite.<br><br>**Evidência: Vide Documento sophos-xg-series-appliances-brna.pdf - Pagina 13 – descritivo de produto**<br>https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophos-xg-series-appliances-brna.pdf?la=en<br><br>**Evidência: Vide seção HA a partir página 384 do Administrator Guide do produto.**<br><br>https://www.sophos.com/en-us/medialibrary/PDFs/documentation/Sophos-XG-Firewall-Administrator-Guide.pdf?la=en<br><br>Segue abaixo documento para escolhe de qualquer porta como dedicada ao HA.<br>https://community.sophos.com/kb/fr-fr/123174<br><br>Caso seja necessário 2Gbps de dados, pode ser feito um LAG destas interfaces para a junção de tráfego com limite de até 4 portas no conjunto LAG.<br><br>https://community.sophos.com/kb/en-us/123100 |
| **5.1.12** | Suporte a no mínimo, 10(dez) roteadores virtuais | Não foi identificado na documentação técnica do fabricante a |

| | | |
|---|---|---|
| | | existência de suporte a roteadores virtuais por parte da solução ofertada.<br><br>**Fonte de Pesquisa**: sophos-xg-series-appliances-brna.pdf / sophosxgfirewallflna.pdf<br><br>https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophosxgfirewallflna.pdf?la=en<br><br>https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophos-xg-series-appliances-brna.pdf?la=en<br><br>**Evidência: Vide seção Routing a partir página 236 do Administrator Guide do produto.**<br>https://www.sophos.com/en-us/medialibrary/PDFs/documentation/Sophos-XG-Firewall-Administrator-Guide.pdf?la=en<br><br>A Sophos tem a opção de criar ilimitados roteamentos virtuais diretamente na regra do firewall. É definido por zona e por qual link desejasse adicionar o roteamento desejado, além de contar com a possibilidade de aplicação de policy routing baseado por origem, serviço ou destino, atrelando o roteamento virtual sem limites nas regras dos firewalls.<br><br>XG v16 Whats new.pdf |

CONCLUSÂO:

O edital é claro quando informa que TODOS os tópicos devem ser atendidos tecnicamente para que a solução seja aceita. Apesar da proposta informar que: " Os produtos estão de acordo com todas as condições, especificações e características previstas no ANEXO TERMO de REFERÊNCIA" isto não foi comprovado pela documentação consultada.

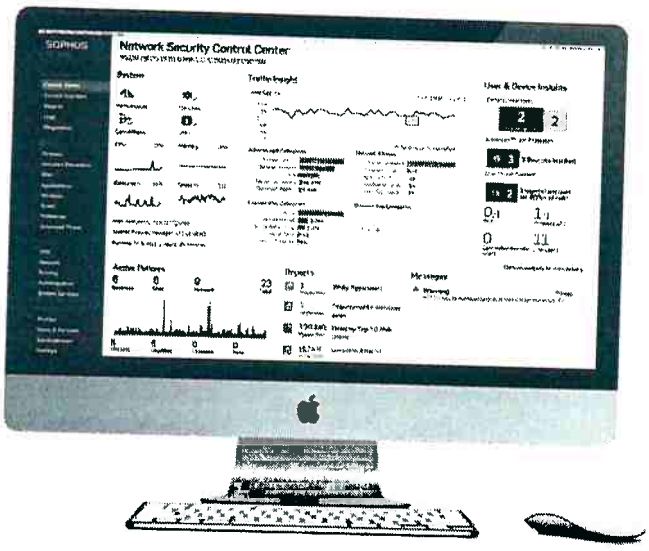
Atenciosamente.

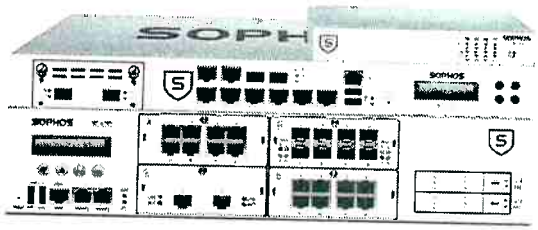
Paulo César Soares Furiati
Coordenador de Informática

SOPHOS
Security made simple.

# XG Firewall

## What's New in v16



## Control Center and Navigation

**Enhanced Control Center Widgets**
Several widgets have improved flip-card views or drill-down results including Reports, Interfaces, and Security Heartbeat.

**Direct Live Log Viewer Access**
Open the live log viewer in a separate window directly from the Control Center using the magnifying glass at the top of any screen.

**Left Navigation**
Left navigation has been expanded to improve access and gain consistency with Sophos Central. Menu items are grouped logically on the left side by task or activity.

**Tab-based 2nd Level Navigation**
Second level navigation is now tab-based enabling quicker 2-clicks-to-anywhere access to most frequently used configuration options. (Note: final tab layout and organization is still being worked on for a subsequent beta build)

## Firewall, Network and Device Configuration

**Firewall hostname**
You can now assign a custom hostname to your firewall

**Cloning**
Enables easy cloning of existing firewall rules, objects and policies.

**Per-rule routing**
Allows flexible routing to be done on a per-firewall-rule basis. There is no longer a need to create global routing rules to change the behavior of select traffic.

**Policy routes**
Route based on source, service or destination.

**Firewall to Firewall RED Tunnels**
Site-to-site RED tunnel support. Note that tunnels between SG UTM 9 and XG Firewall are not yet supported but this is planned before GA.

**Country filtering improvements**
Streamlined of implementing country or continent based filtering in firewall rules

**NAT Business Rule Creation**
Improved DNAT, Full NAT, and server load balancing rule creation is expected in an upcoming Beta release before GA.

## Authentication and Diagnostics

**One-Time Passwords**
Improved access security with support for OATH-TOTP one-time passwords directly on the firewall eliminating the need for a separate 2FA solution. Support for IPSec, SSL VPN, User Portal, and WebAdmin access. We recommend using the free Sophos authenticator app for iOS and Android.

**Live Log Viewer Enhancements**
An improved live log viewer which conveniently opens in a new window, with a 5-second refresh option, and color coded log lines – as well as a live packet filter packet level drill-down enabling easier real-time insights, visibility, and trouble-shooting.

# Web

**Redesigned Web Policy Model**
Flexible new user and group policy creation and in-line editing tools with inheritance that makes web policies more intuitive and easy to maintain while dramatically reducing firewall rule count in many situations

**Warn action**
A new web filtering action in addition to Block or Allow that enables users to proceed to websites only after acknowledging a warning that the site belongs to an inappropriate or undesirable category. This option can be ideal in situations where user education, awareness, and monitoring is desired without strictly prohibiting access.

**Unscannable content handling**
Options to allow or block content that cannot be scanned due to encryption or containers.

**Google Apps control**
Limit access to a selected Google Apps domain to reduce the risk of data loss from users transferring documents to their personal Google Apps.

**Creative Commons Enforcement**
Reduce the risk of exposure to inappropriate images by enforcing search engine filters for content with a Creative Commons license.

**External URL lists**
Import external URL lists that require enforcement in certain organizations or jurisdictions.

# Email

**Per domain routing**
Route incoming mail to the correct destination server, based on the target domain

**Full MTA – Store and forward support**
Enable business continuity, allowing the firewall to store mail when target servers are unavailable

**Spam features (HELO/RDNS)**
Added anti-spam technology to identify non-legitimate mail sending servers.

**SPX reply portal**
Enable recipients of SPX encrypted emails generated by the Firewall to reply securely using a portal on the Firewall to draft and send a response.

# Synchronized Security

**Missing Security Heartbeat**
Enables the Firewall to detect when a previously healthy Endpoint is generating network traffic with a missing Security Heartbeat and automatically identify the system and respond. This may be an indication the Endpoint AV has been tampered with or disabled.

**Real-time Application Visibility**
Enables the Firewall to solicit information from the Endpoint to determine the application responsible for generating uncategorized network traffic. This is valuable for gaining insights into network traffic that is unrecognized by other Firewall solutions.

**Destination-based Security Heartbeat**
Enables the Firewall to limit access to destinations and servers based on the status of their Heartbeat further bolstering protection from potentially compromised systems until they can be cleaned up. Combined with regular Heartbeat policy enforcement, this can effectively isolate a compromised system completely - both inbound and outbound.

## Other Features

**Improved Security Audit Report**
Improved layout, presentation and information for the customer facing Security Audit Report provided after a TAP-mode or Inline-mode Proof-of-Concept deployment.

**High Availability Enhancements**
HA support for configurations using dynamic (DHCP/PPPoE) interfaces

## Issues Addressed

**Open Issues Addressed**
In addition to new features, this release has closed hundreds of open issues identified since the release of v15 across all areas of the product.