CÂMARA MUNICIPAL DE BELO HORIZONTE

Of. COOINF Nº 020/2016

Belo Horizonte, 14 de setembro de 2016.

À CPL

Senhora Pregoeira,

Em resposta à sua solicitação de avaliação da resposta da diligência realizada para validação da proposta Proposta Comercial da empresa Tracenet Treinamento e Comércio em Informática Ltda, referente ao Pregão Eletrônico nº 36/2016, após análise da resposta encaminhada pela empresa temos as seguintes considerações e conclusões:

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. **Evidência: Vide páginas 422 e 572 (APPEND A – LOGS) do Administrator guide do produto.** https://www.sophos.com/en-us/medialibrary/PDFs/documentation/Sophos-XG-Firewall-Administrator-Guide.pdf?la=en UserAgent: identifica uma aplicação que acessou o recurso http (atende) HTTP referer: endereço IP de quem acessou a página (atende) 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) 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). **Análise da Resposta pela COOINF:Analisada a documentação apresentada pelo licitante e acessando o site informado, esta Coordenadoria entendeu ser aceitável a opção adotada, portanto, NESTE QUESITO, a solução ATENDE ao edital.**
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. **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 Feito via IPS/proxy reverso, realizado a monitoração do SSH https://kb.cyberoam.com/redirfile.asp?id=6427&fstore=&SID= **Análise da Resposta pela COOINF: Acessado o documento [1] indicado pelo link é confirmada à alegação inicial da COOINF de que O PRODUTO NÃO ATENDE AO EXIGIDO PELO EDITAL. O documento apresentado, em seu próprio titulo, demonstra apenas a funcionalidade de "MONITORAMENTO" do protocolo SSH. Em nenhuma parte do documento é declarada ou informada, configuração exigida pelo edital, que é a capacidade de "DE-CRIPTOGRAFIA" do protocolo, deixando claro que o equipamento não tem tal capacidade.**
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. **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 Feito via IPS/proxy reverso, realizado a monitoração do SSH https://kb.cyberoam.com/redirfile.asp?id=6427&fstore=&SID= **Análise da Resposta pela COOINF: Esta funcionalidade esta diretamente ligada à capacidade exigida no item 4.2.9, logo se o item anterior não é atendido este também não será. Visto que o documento que justifica tal funcionalidade é o mesmo.** **Breve explicação da funcionalidade: O tráfego SSH é criptografado de forma que pessoas alheias à comunicação não sejam capazes de identificar a informação que está trafegando durante a comunicação. Sabendo desta característica os possíveis atacantes utilizam este protocolo para trafegar informações nocivas ao ambiente computacional da organização. Só é possível evitar que esta situação seja**

[1] Cópia do Documento segue no ANEXO I

		explorada com a funcionalidade aqui exigida, onde o equipamento tem a capacidade de "decifrar" os dados trafegados durante a comunicação e, em caso de dados nocivos, os mesmos possam ser bloqueados. Desta forma, por consequência, também é confirmada à alegação inicial da COOINF que O PRODUTO NÃO ATENDE AO EXIGIDO PELO EDITAL.
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. **Evidência: Vide Documento sophos-xg-series-appliances-brna.pdf - Pagina 13 – descritivo de produto** https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophos-xg-series-appliances-brna.pdf?la=en **Evidência: Vide seção HA a partir página 384 do Administrator Guide do produto.** https://www.sophos.com/en-us/medialibrary/PDFs/documentation/Sophos-XG-Firewall-Administrator-Guide.pdf?la=en Segue abaixo documento para escolhe de qualquer porta como dedicada ao HA. https://community.sophos.com/kb/fr-fr/123174 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. https://community.sophos.com/kb/en-us/123100 **Análise da Resposta pela COOINF:Analisada a documentação apresentada pelo licitante esta Coordenadoria entendeu ser aceitável a opção adotada, portanto, NESTE QUESITO a solução ATENDE ao edital.**
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. **Fonte de Pesquisa**: sophos-xg-series-appliances-brna.pdf / sophosxgfirewallflna.pdf https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophosxgfirewallflna.pdf?la=en https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophos-xg-series-appliances-

		brna.pdf?la=en **Evidência: Vide seção Routing a partir página 236 do Administrator Guide do produto.** https://www.sophos.com/en-us/medialibrary/PDFs/documentation/Sophos-XG-Firewall-Administrator-Guide.pdf?la=en 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. XG v16 Whats new.pdf **Análise da Resposta pela COOINF: Acessado o documento [2] indicado pelo licitante e conforme pode ser verificado na pagina 2** (Firewall, Network and Device Configuration/ Per-rule routing) **, somente é possível criar "rotas por política de roteamento" e não ROTEADORES VIRTUAIS como é exigido no edital, que são funcionalidades totalmente distintas. Assim sendo, mais uma vez é confirmada à alegação inicial da COOINF de que O PRODUTO NÃO ATENDE AO EXIGIDO PELO EDITAL.**

CONCLUSÂO:

Diante das respostas apresentadas pelo licitante à diligência e pelo exposto neste documento, fica claro que a solução ofertada **NÂO ATENDE AOS REQUSITOS TÉCNICOS DO EDITAL**, portando a proposta **NÃO DEVE SER ACEITA** pois traria prejuízos para esta casa caso a solução seja adotada.

Atenciosamente.

Paulo César Soares Furiati
Coordenador de Informática
Paulo César Soares Furiati
Coordenador de Informática
CM 40.434

[2] Cópia do Documento segue no ANEXO II

ANEXO I

Applicable Version: 10.00 onwards

Overview

Secure Shell (SSH) is a cryptographic network protocol for secure data communication, remote command-line login, remote command execution, and other secure network services between two networked computers.

Like most protocols, SSH has its own set of vulnerability, which could provide an easy exploit for network hackers and intruders.

Cyberoam Intrusion Prevention System (IPS) helps in preventing such attacks by keeping a close watch on all incoming and outgoing SSH traffic. Cyberoam IPS protects against network and application-level attacks, securing organizations against intrusion attempts, malware, Trojans, DoS and DDoS attacks, malicious code transmission, backdoor activity and blended threats. Cyberoam's signature-based Intrusion Prevention System carries thousands of automatically updated signatures, enabling protection against the latest vulnerabilities.

Scenario

Configure Cyberoam to monitor all SSH traffic.

Prerequisite

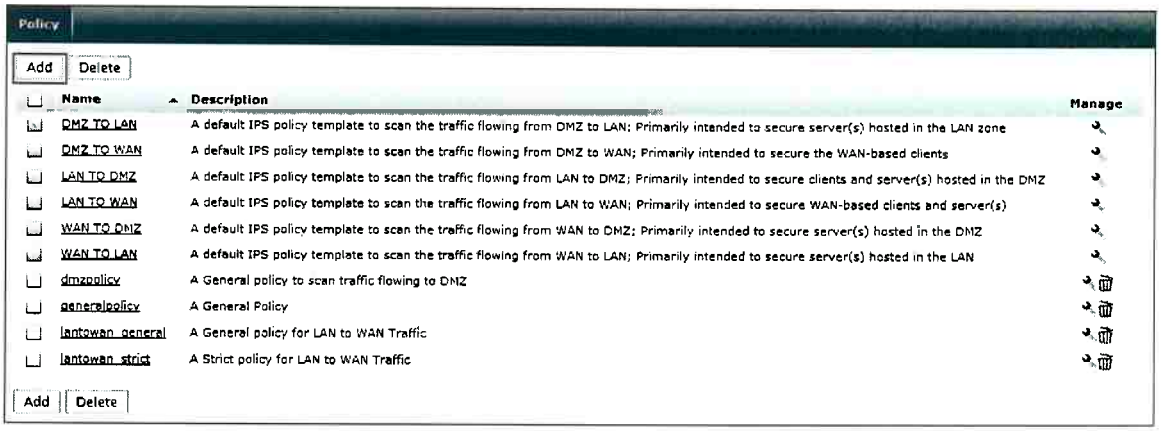
IPS Module should be subscribed

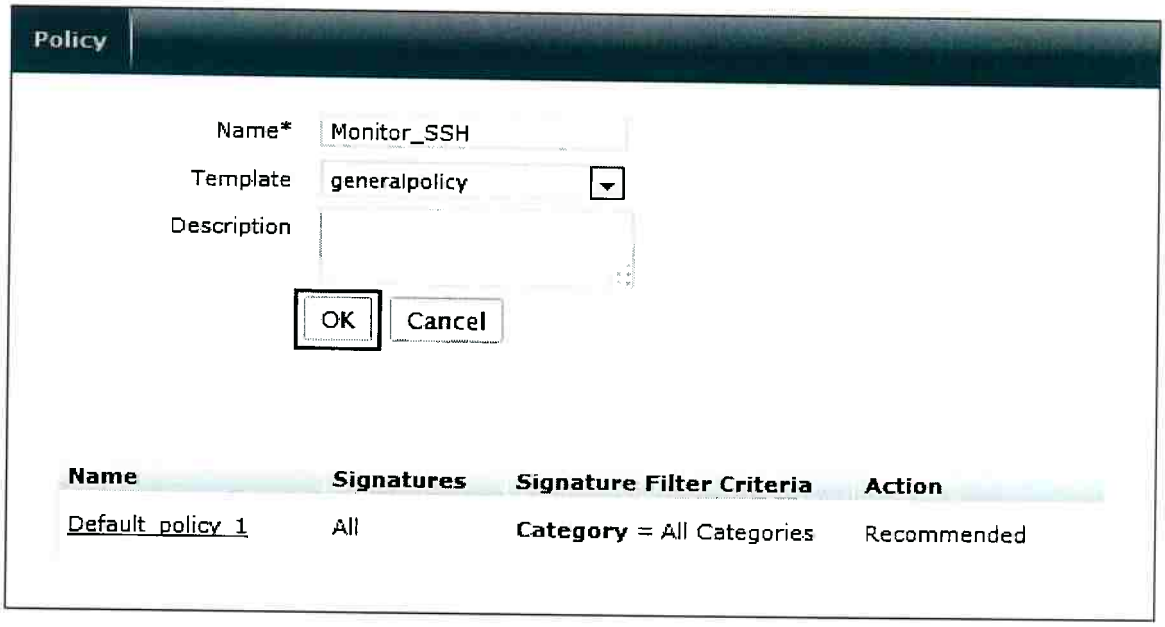
Configuration

You must be logged on to the Web Admin Console as an administrator with Read-Write permission for relevant feature(s).

Step 1: Create IPS Policy

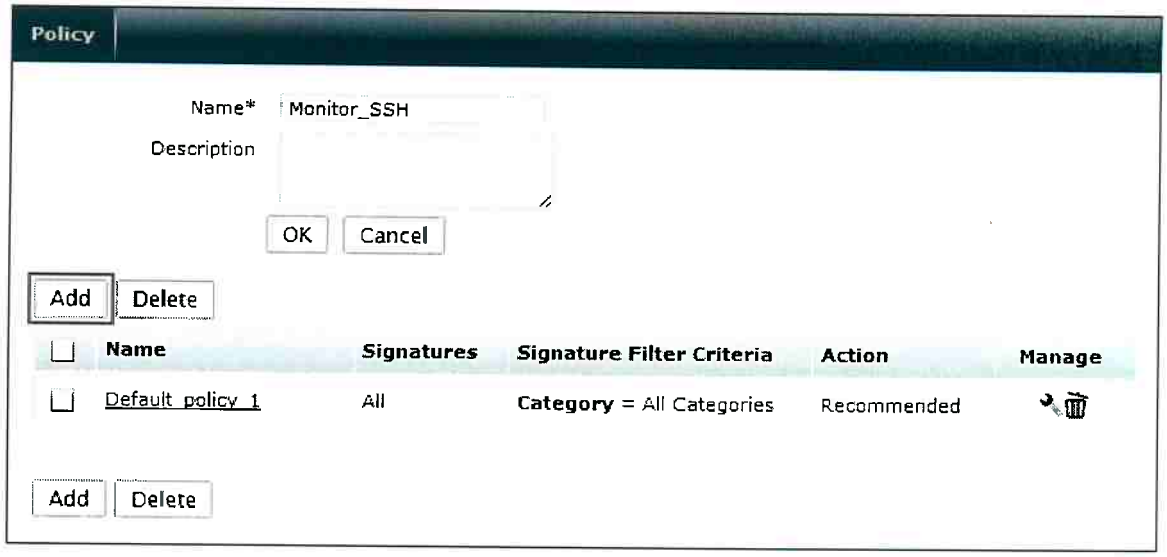
- Go to **IPS > Policy > Policy** and click **Add** to create a new IPS Policy named 'Monitor_SSH'.



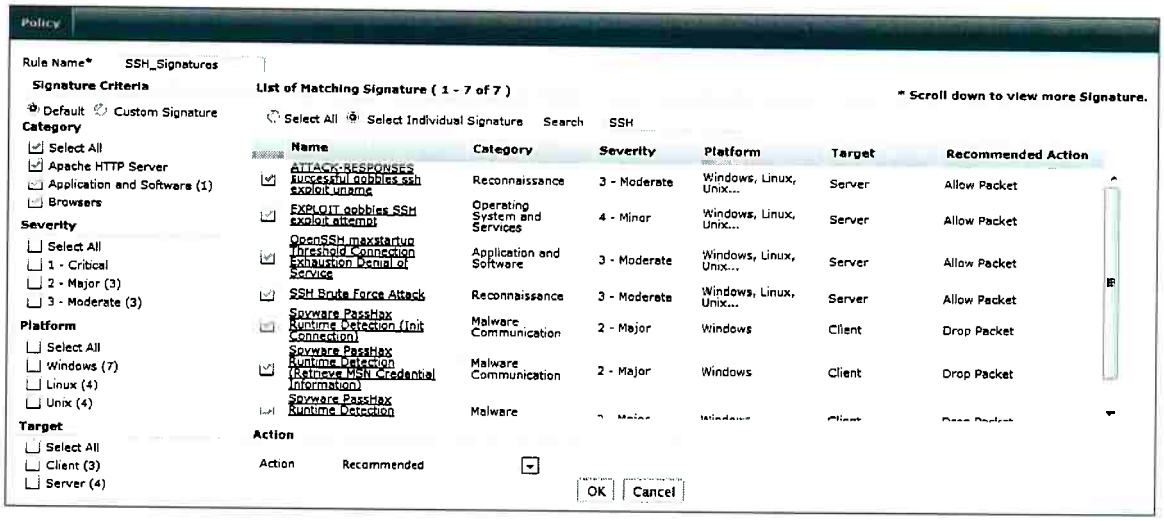


Click **OK** to create policy.

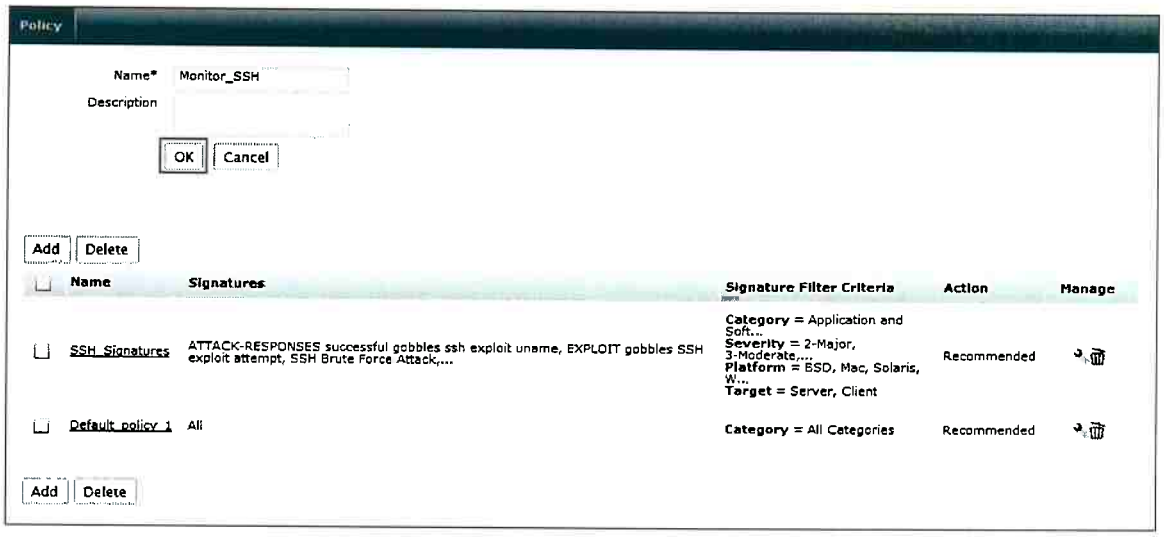
- Select the newly-made policy 'Monitor_SSH' and click **Add** to add Rule for the IPS Policy.



- Click **Select Individual Signature** and search for SSH signatures. Select the DDoS signatures and select **Action** as **Recommended**. Recommended action allows CyberoamOS to handle this alert level according to best-fit recommendations. Click **OK** to save the Rule.

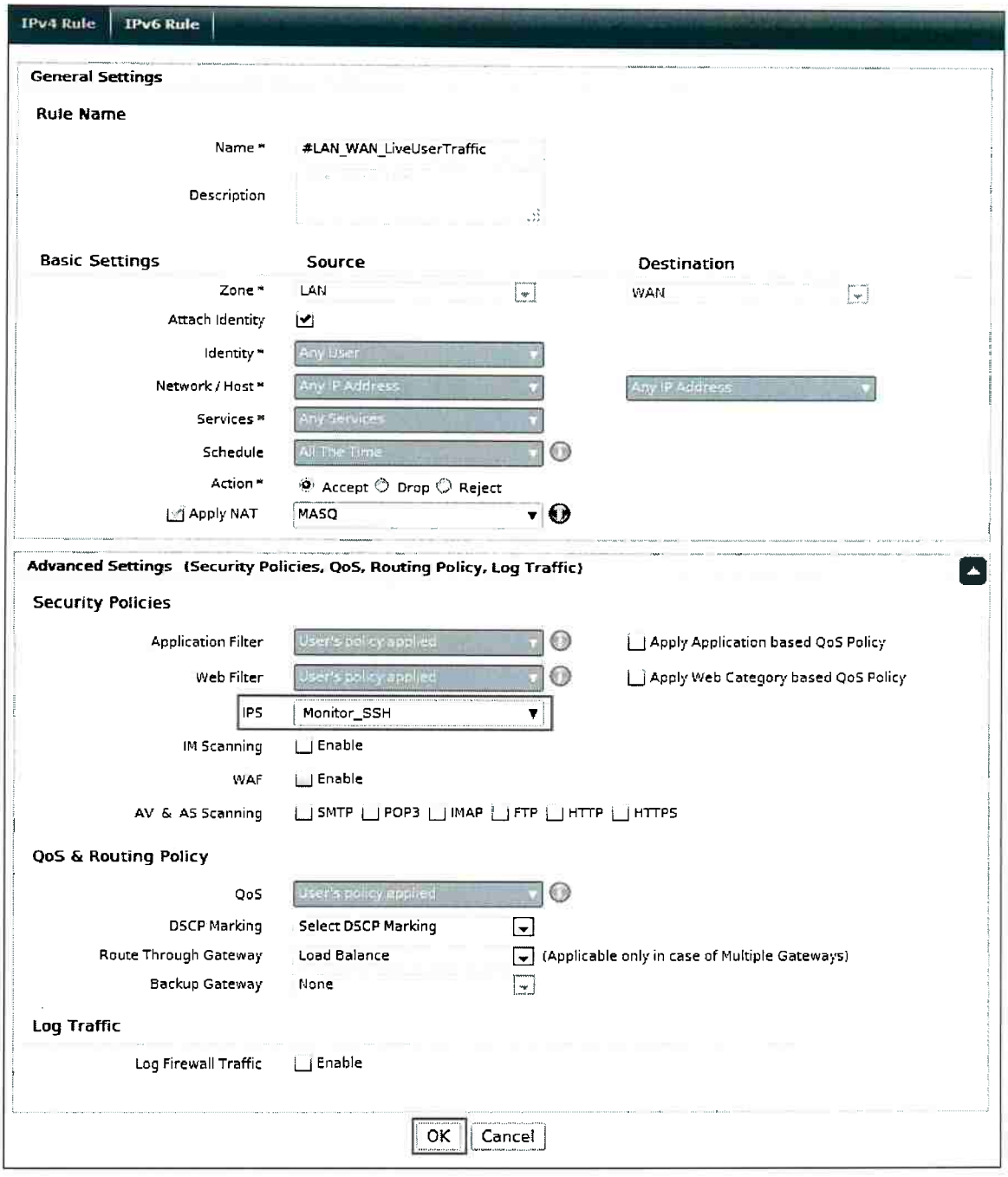


- Click **OK** to save policy.



Step 2: Apply Policy to Firewall Rule

Go to **Firewall > Rule > Rule** and apply the policy on the required Firewall Rule(s). Here, we have applied it on LAN_WAN_LiveUserTraffic.



Click **OK** to save the firewall settings.

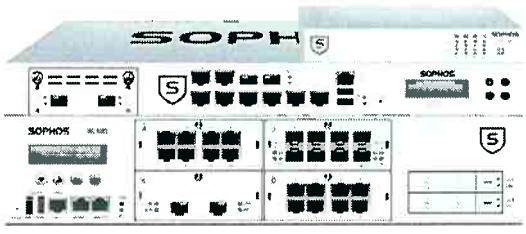
Once the IPS policy is applied, Cyberoam keeps a lookout for any packets that match the configured IPS signature(s). If any such packets are found, Cyberoam performs the recommended action.

ANEXO II

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.