Implementação de UTM em conformidade com a Lei Geral de Proteção de Dados.

Elaborador:	André Sotelo Martins
Orientador:	Márcio Roberto Baldo Taglietta

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS

Dados Internacionais de Catalogação-na-fonte

M341i MARTINS, André Sotelo

Implementação de UTM em conformidade com a lei geral de proteção de dados. / André Sotelo Martins. – Americana, 2019.

25f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Esp. Márcio Roberto Baldo Taglietta.

1 VPN – rede de computadores. I. TAGLIETTA, Márcio Roberto Baldo. II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: *681.519*

Fatec Americana
Ministro Ralph Biasi

Centro Paula Souza 50 anos 1969 - 2019

SÃO PAULO GOVERNO DO ESTADO

André Sotelo Martins

IMPLEMENTAÇÃO DE UTM EM CONFORMIDADE COM A LEI GERAL DE PROTEÇÃO DE DADOS.

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação, pelo CEETEPS/Faculdade de Tecnologia – Fatec/ Americana.
Área de concentração: Infraestrutura de redes.

Americana, 10 de junho de 2019.

Banca Examinadora:

Márcio Roberto Baldo Taglietta (Presidente)
Especialista
Fatec Americana

Juliane Borsato Beckedorff Pinto (Membro)
Especialista
Fatec Americana

Wagner Siqueira Cavalcante (Membro)
Mestre
Fatec Americana

SUMÁRIO

1 Introdução 6
2 Objetivo deste documento 6
3 Desenvolvimento 6
3.1 Lei Geral de Proteção de Dados (LGPD) 6
3.2 Problema x Solução 9
3.3 Conhecendo o UTM Sophos XG 135 9
3.4 Licença 13
3.5 Criação das Conexões 14
3.6 Autenticação de usuários 17
3.7 Criação das regras de Firewall 21
4 Resultados 22
4.1 Testes 22
4.2 Quadrante mágico Gartner 23
5 Conclusões e considerações finais 24

Lista de figuras

Figura 1 UTM Sophos XG 135 10
Figura 2 Modelo antigo (Sophos SG 220) 11
Figura 3 Demo Sophos..... 12
Figura 4 Ativação da Licença 13
Figura 5 Gerenciamento WAN..... 14
Figura 6 Gerenciamento WAN 2..... 15
Figura 7 Interface de Rede..... 16
Figura 8 DMZ 17
Figura 9 Autenticação AD..... 18
Figura 10 AD Adicionado..... 19
Figura 11 Configurando STAS..... 20
Figura 12 Regras de Firewall..... 21
Figura 13 Firewall Ativo 22
Figura 14 Quadrante Mágico Gartner 2018 23

Lista de tabelas

Tabela 1 Objetivos LGPD..... 9
Tabela 2 Faixas de IP..... 11
Tabela 3 Redundância de link 12

Lista de siglas

- **LGPD:** Lei Geral de Proteção de Dados.
- **UTM:** Unified Threat Management (Gerenciamento Unificado de Ameaças).
- **Firewall:** Dispositivo de proteção em redes de computadores.
- **DMZ:** Demilitarized zone (Zona desmilitarizada).
- **STAS:** Sophos Transparent Authentication Suite.
- **AD:** Active Directory (Diretório Ativo).
- **Gateway:** Ponte de ligação entre interfaces de rede.
- **Bridge:** Modo de roteamento.
- **NAT MASQ:** Permitir que a rede privada seja ocultada.
- **VLAN:** Virtual LAN (rede local virtual).
- **Phishing:** Ataque cibernético por meio de e-mails e sites falsos.

1 Introdução

A LGPD é a lei brasileira que estabelece normas reguladoras para proteger o uso de dados pessoais no Brasil. Ela foi aprovada pelo senado brasileiro em julho/2018, através da PLC 53/2018, nº 13.709/2018.

O grande objetivo dessa lei, é de garantir a todas as pessoas: a liberdade de expressão e o respeito à privacidade.

À medida que as tecnologias avançam e cada vez mais estão presentes no dia a dia, se torna um alvo em potencial o acesso a elas e consequentemente, a necessidade da valorização da informação.

Portanto, a LGPD que deverá entrar em vigor em agosto de 2020, deve não apenas "forçar" as empresas a aderirem à nova lei e seguirem as devidas conformidades, como também trazer segurança aos cidadãos de todo o território nacional, visando um relacionamento de transparência entre empresa e cliente.

2 Objetivo deste documento

Com a tecnologia atualmente, a conformidade em relação à essa lei se torna inevitável. Num cenário onde o acesso e controle de informação é primordial, o objetivo é garantir com que as empresas estejam em conformidade com a lei.

O propósito desse relatório é implementar e configurar um Firewall cujo foco é controlar todos os acessos à rede, efetuar a autenticação de usuários, criar filtros de protocolos, executar redirecionamento de portas, entre outros.

3 Desenvolvimento

Atualmente, o foco é desenvolver uma fórmula simplificada e eficiente para estar em conformidade com a nova lei, com destaque somente nos principais impactos que a lei poderia afetar na área de TI de uma organização.

Com a implementação do UTM Sophos XG 135, alguns dos principais pontos serão abordados, como a parte teórica da lei, com detalhes nos conceitos e objetivos dela, como também a implementação e devida configuração do UTM, cujo foco é a aplicação do Firewall.

3.1 Lei Geral de Proteção de Dados (LGPD)

> "*Por isso, a lei terá um impacto na sociedade como poucas antes tiveram, criando um regramento para o uso de dados pessoais no Brasil, tanto on-line quanto off-line, nos setores privado e público.*"
>
> Fonte: Machado, Meyer 2018.

O conceito da lei se baseia em como os dados serão tratados: eles são de propriedade exclusiva de seus respectivos donos, e não podem ser compartilhados entre organizações, como por exemplo:

- **Dados pessoais:** Qualquer informação relacionada a uma pessoa natural (física) que possa ser identificada a partir dos dados coletados. É um conceito central da LGPD, que busca proteger a privacidade dos titulares de dados pessoais que sejam objeto de tratamento (art. 5°, I).

- **Titular:** Pessoa natural (física) a quem se referem os dados pessoais que são objeto de tratamento (art. 5°, V)

- **Tratamento:** Toda operação realizada com dados pessoais, como coleta, utilização, processamento, armazenamento e eliminação (art. 5°, X).

- **Controlador:** Pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento de dados pessoais (art. 5°, VI).

- **Operador:** Pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador (art. 5°, VII).

- **Âmbito de Aplicação:** Pessoas físicas ou jurídicas, de direito público ou privado, que tratem dados pessoais no Brasil ou que coletem dados no Brasil ou, ainda, quando o tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços a titulares localizados no Brasil, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados (art. 3°).

- **Requisitos para o tratamento:** Os dados pessoais somente poderão ser tratados em uma das seguintes hipóteses (art. 7°):
    - Mediante consentimento do titular;
    - Para cumprimento de obrigação legal ou regulatória do controlador;
    - Para execução de políticas públicas pela administração pública;
    - Para realização de estudos por órgãos de pesquisa;
    - Quando necessário para execução de contrato ou procedimentos preliminares a um contrato do qual seja parte o titular, a pedido do titular;
    - Para o exercício regular de direitos em processos judiciais, administrativos ou arbitrais;
    - Para proteção da vida ou da incolumidade física do titular ou de terceiros;
    - Para tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
    - Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, salvo quando prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção de seus dados pessoais;
    - Para proteção do crédito.

- **Direitos do titular:** A nova legislação estabelece os seguintes direitos dos titulares (art. 18°):
    - confirmar a existência de tratamento de seus dados pessoais;
    - Acessar seus dados pessoais;
    - Corrigir dados pessoais incompletos, inexatos ou desatualizados;

- Anonimização, bloqueio ou eliminação de dados pessoais desnecessários, excessivos ou tratados em desconformidade com a LPD;
- Portabilidade de dados pessoais a outro fornecedor de produto ou serviço;
- Eliminação de dados tratados com o seu consentimento;
- Obtenção de informações sobre as entidades públicas e privadas com as quais o controlador realizou o compartilhamento de dados pessoais;
- Obtenção de informações sobre a possibilidade de não consentir com o tratamento de dados pessoais e sobre as consequências da negativa;
- Revogação do consentimento dado para o tratamento de dados pessoais.

- **Transferência Internacional de Dados:** É permitida somente nas hipóteses previstas na LGPD (art. 33°), entre elas:
  - Para países que proporcionem grau de proteção de dados pessoais adequado ao previsto na LGPD;
  - Quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiros;
  - Quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência.

Fonte: Machado, Meyer 2018.

Entre os principais objetivos da lei é de assegurar alguns itens conforme na Tabela 1.

Tabela 1 Objetivos LGPD

PRIVACIDADE	Garantir o direito à privacidade e proteger dados por meio de práticas transparentes e confiáveis.
TRANSPARÊNCIA	Definir de regras transparentes sobre dados pessoais.
DESENVOLVIMENTO	Contribuir com o crescimento tecnológico e ecológico.
PADRONIZAÇÃO	Padronização sobre tratamento de dados pessoais, independente de incompatibilidades sistêmicas.
PROTEÇÃO DO MERCADO	Segurança em relações jurídicas, livre iniciativa, a livre concorrência e a defesa das relações comerciais e de consumo.
CONCORRÊNCIA	Contribuir com a concorrência no mercado e portabilidade.

Fonte: Machado, Meyer 2018

Com a aprovação da lei, as organizações e empresas terão alguns impactos conforme mostrado a seguir.

Impacto:

- **Dificuldade na centralização dos dados:** Todas as corporações precisarão de uma base de dados unificada, para armazenar todas as informações de seus respectivos públicos. Sejam eles de coleta própria, ou externo, como terceiros.

- **Gerenciamento de dados pessoais pelos usuários:** Os usuários poderão gerenciar e alterar os seus dados, tornando a empresa somente uma hospedeira que coleta os dados, portanto o usuário é o proprietário das suas informações.

- **Clareza na coleta dos dados:** Uma vez que as empresam coletam esses dados, elas devem ter mais clareza e o porquê de cada informação capturada.

3.2 Problema x Solução

De acordo com a LGPD, o armazenamento de informações é de responsabilidade das empresas que as recolhem e utilizam, como primeiro passo no armazenamento dessas informações, uma solução com os seguintes pontos é primordial:

- Aumento de segurança utilizando uma solução confiável e sólida no mercado, além de proporcionar uma maior segurança a essa primeira barreira de proteção de dados.
- Suporte e Atualizações constantes de software de Servidores.
- Banco de dados aprimorado.
- Revisão constante de regras de Firewall.

3.3 Conhecendo o UTM Sophos XG 135

O modelo implementado e utilizado neste relatório foi o UTM Sophos XG 135, todas as configurações e informações que serão apresentadas se trata especificamente deste modelo, conforme mostrado na figura 1.

Figura 1 UTM Sophos XG 135

Fonte: Sophos

UTM Sophos XG 135 com visão frontal e traseira.

Para a escolha da solução, um modelo com Throughput de no mínimo 4 Gbps foi necessário, entre outras especificações conforme abaixo.

Especificações UTM Sophos XG 135:

Descrição do Hardware: 8 x GE RJ45 portas:

- Throughput de Firewall: 6 Gbps
- Sessões Concorrentes: 2.000.000
- Novas Sessões por Segundo: 36.000
- VPN Throughput: 1 Gbps
- IPS Throughput: 1.5 Gbps
- Antivirus Throughput (Proxy Based): 350 Mbps
- Configuração de Alta Disponibilidade (HA): Ativo/Ativo e Ativo/Passivo

Dados Ambientais:

- Dimensões (Altura x Largura x Profundidade): 44 x 288x 188 mm
- Peso líquido: 1,7 Kg
- Peso na Embalagem: 2,82 Kg
- Temperatura de Operação: 0-40ºC
- Temperatura de Armazenamento: -20-80ºC
- Humidade: 10% a 90% (sem condensação)
- Consumo de Energia Máximo: 26,16 Watts
- Dissipação de Calor: 89,2 BTU/h

O Sophos XG 135 foi adquirido com licenciamento para 3 anos, vem em substituição ao Sophos SG 220, como mostra na figura 2 que estava operando na rede, cujo vencimento foi em 15 de maio 2018.

Figura 2 Modelo antigo (Sophos SG 220)

Fonte: Sophos

O modo no qual o Sophos 220 se encontra instalado é o bridge, em modo transparente deixando as conexões por conta dos roteadores, faz ele assumir a posição de gateway na rede, filtrando todas as movimentações de dados. Essa rede opera com 4 faixas de IP conforme na tabela 2, sendo uma a principal controlada por um servidor Windows Server 2008 R2 Virtualizado.

Tabela 2 Faixas de IP

Faixa	Descrição
172.16.0.1/24	Servidores, sem DHCP Ativo
172.16.1.0/24	Estações Rede Principal – DHCP Controlado pelo Servidor Windows
192.168.2.0/24	Visitantes – Vlan1 limitado a 50 Dispositivos – Visitantes com controle de voucher e tempo permitido de acesso – DHCP SOPHOS
192.168.3.0/24	Funcionários Vlan2 Limitada a 80 Dispositivos – Funcionários para acesso particular a internet, previamente cadastrados, com termo de PSI – DHCP SOPHOS
192.168.4.0/24	Dispositivos Vlan3 Limitada a 50 Dispositivos – Dispositivos da empresa utilizados no trabalho – Celular corporativo, Tablet de conexão a internet etc – DHCP SOPHOS

Fonte: Autoria Própria

Não existe ferramenta para migração de configurações entre as duas versões (SG e XG), então toda a nova implementação ocorre manualmente.

Para a redundância de link, o que foi definido na implementação foram os 2 links via cabo e um modem 4G de backup, conforme na tabela 3.

Tabela 3 Redundância de Link

Quantidade	Links
01	PRINCIPAL NET CABLE MODEM 120 MB
01	VIVO FIBRA DEDICADO 10 MB – CONTENÇÃO 1
01	4G CLARO – CONTENÇÃO 2

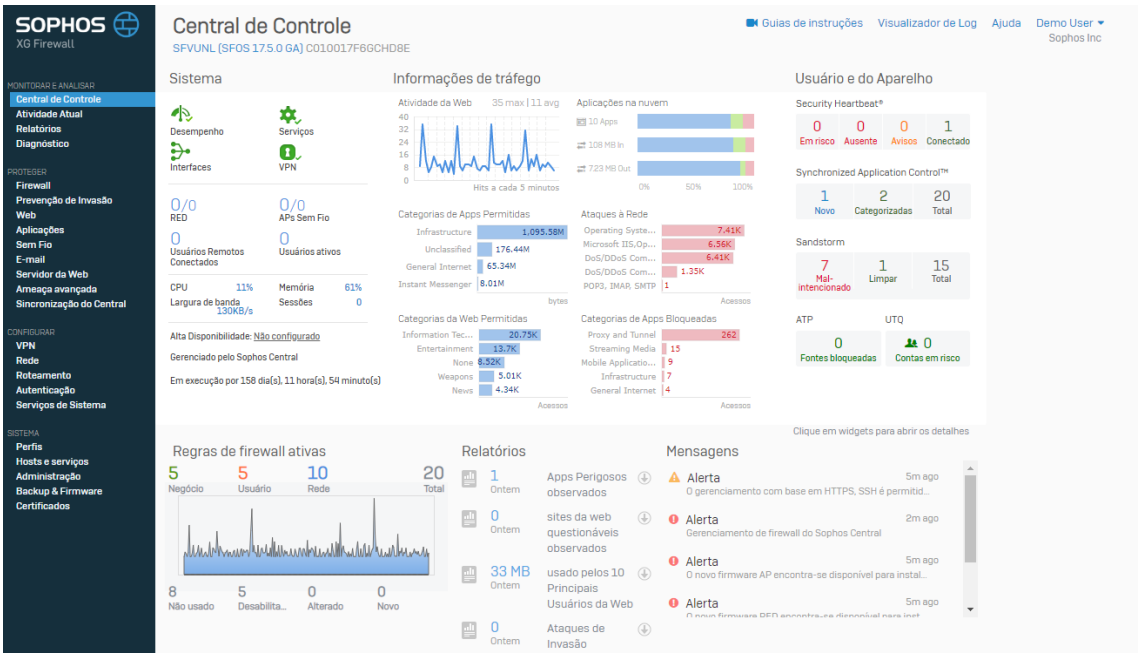
Fonte: Autoria Própria

Toda conexão é feita preferencialmente pelo link principal. Caso haja queda, o link é direcionado para a contenção 1 onde há uma perda considerável de velocidade. Caso os dois falhem é acionada a contenção 2 onde apenas algumas estações estratégicas para o negócio continuarão a ter acesso à internet (emissão de NF, Cartões, Bancos e Sistemas de monitoramento alarmes).

Demo Sophos:

O módulo de demonstração da Sophos na Web, que pode ser acessado em https://demo.sophos.com/webconsole/webpages/login.jsp, com usuário e senha: “demo” sem as aspas, será apresentado de modo a conservar a identidade da empresa na qual o sistema foi instalado. Na figura 3, é exibido a página de início do software da Sophos XG Firewall.

Figura 3 Demo Sophos



Fonte: Sophos

A tela principal consiste em apresentar o status do sistema de modo a permitir uma visualização rápida por painéis, facilitando a identificação de problemas e a tomada de decisão. Pode-se ver as informações de tráfego, alertas, ataques, regras de Firewall ativas, APs sem fio (caso sejam utilizados Switches e APs da Sophos, que permitem monitoramento integrado ao Firewall), aplicativos e categorias web com acesso permitido.

3.4 Licença

Na figura 4, a tela de ativação é feita de forma intuitiva e de um modo simples. Após a aquisição, o fabricante enviou dois e-mails constando o endereço web para ativação da licença e a chave de ativação.

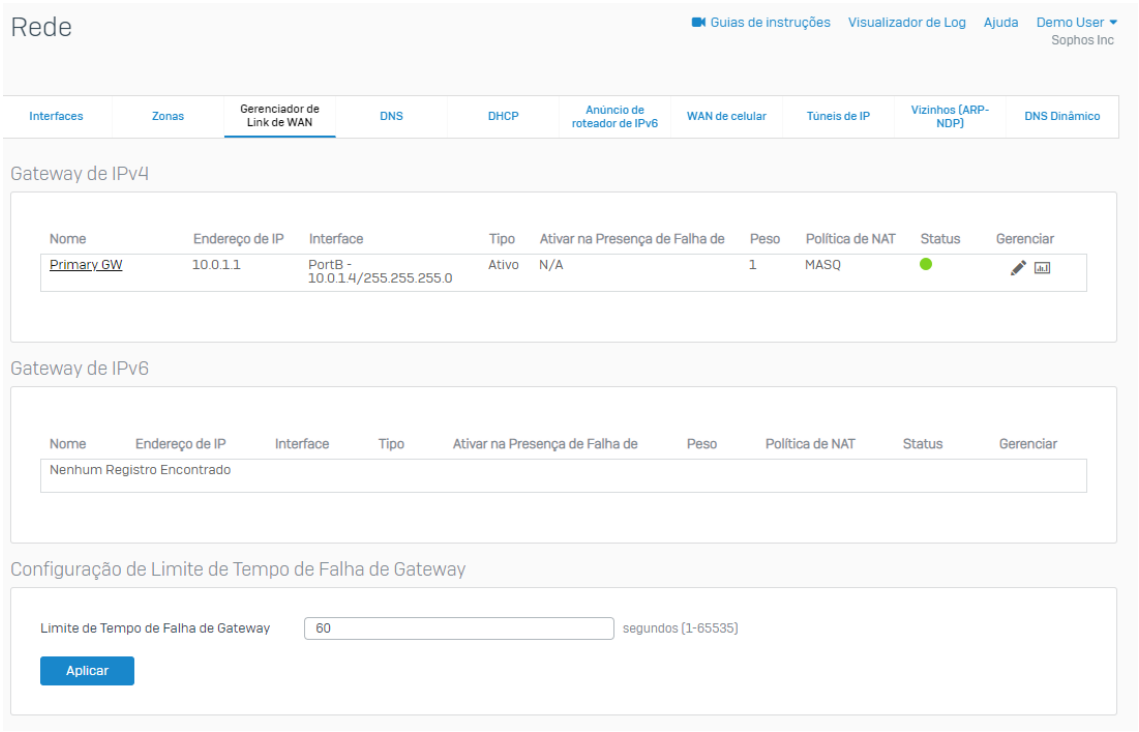
Figura 4 Ativação da Licença

Efetuada a ativação do UTM, verifica-se na web e ativa-se a o licenciamento. Neste caso, existem algumas opções que não foram adquiridas, nas outras tem-se a data de validade da licença e no firewall de base a ativação ilimitada por meio de configuração de regras a qual não expira.

3.5 Criação das Conexões

Em gerenciamento de link do WAN, tem-se as conexões com os *modems* conforme mostrado na figura 5.

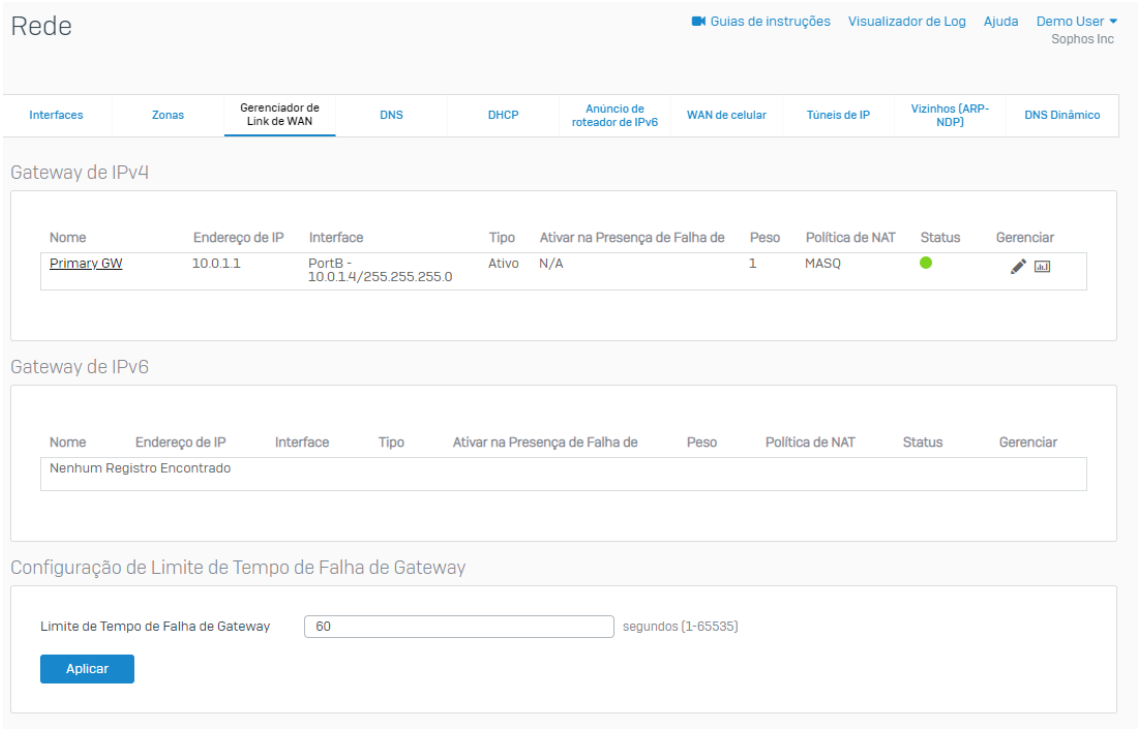
Figura 5 Gerenciamento WAN



Fonte: Autoria Própria

Com os *modems* configurados, é possível aplicar políticas para determinadas portas, conforme na figura 6.

Figura 6 Gerenciamento WAN 2



Fonte: Autoria Própria

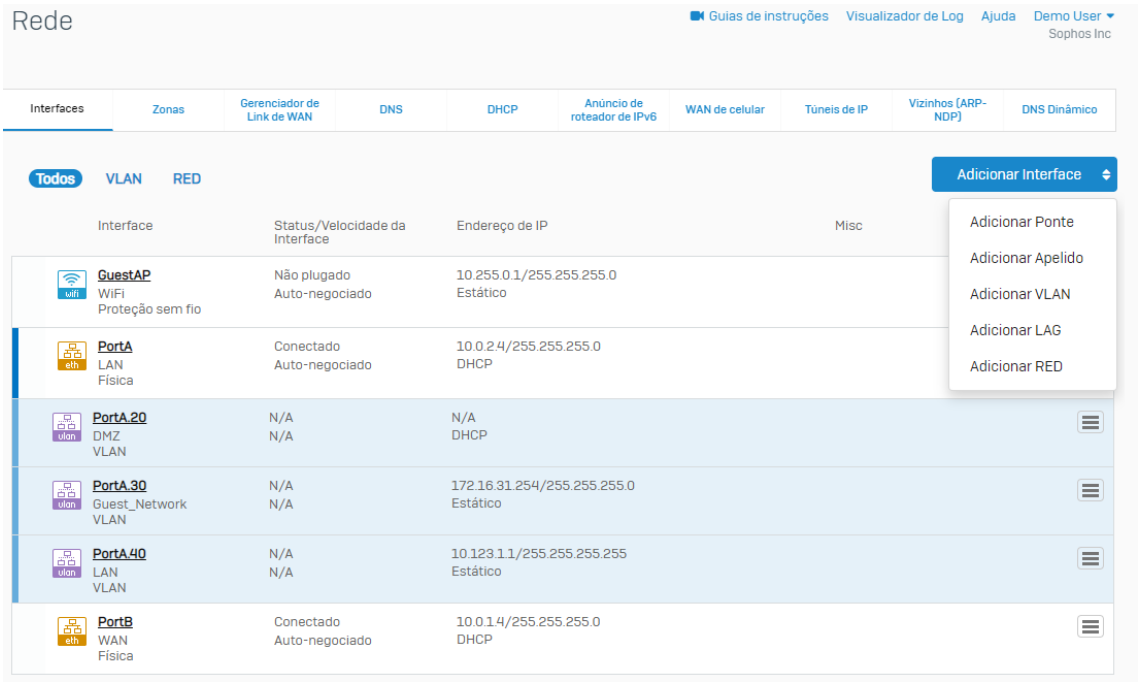
Na tela de conexão do ambiente de simulação conforme acima, tem-se uma conexão com modem ativa na porta, com uma política de *NAT MASQ* (mascarada).

- *NAT MASQ*: Uma utilização comum de política NAT, seria para mascarar o IP externo e permitir que dispositivos dentro de uma rede privada possam sair para a Internet com o endereço IP do equipamento que está fazendo esse tipo de NAT, ou melhor, para economia de endereços IPv4.

Na opção redes – interface, criamos a conexão com a rede e VLAN conforme na figura 7.

Na mesma tela de configuração pode-se adicionar e nomear as interfaces, definir o tipo de porta a ser adicionada como é o caso das VLANs, como no exemplo onde há uma porta como *DMZ*.

Figura 7 Interfaces de rede

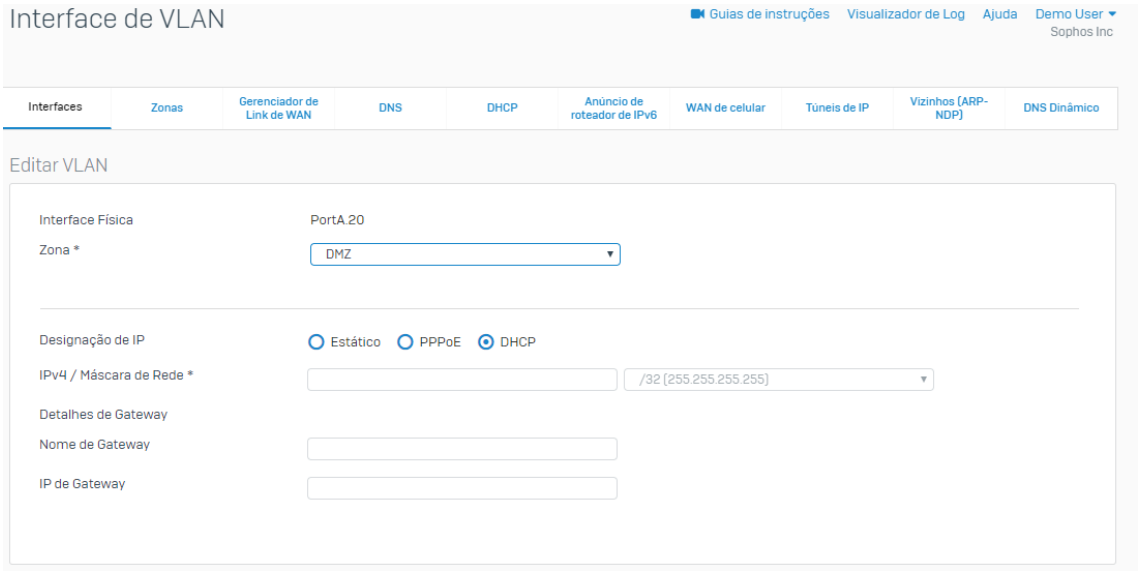


Fonte: Autoria Própria

Toda interface deve pertencer a uma zona de segurança.

Para isolar alguma interface da rede local foi utilizado uma porta *DMZ,* com regras de Firewall específicas. Na figura 8, demonstra onde inserir a interface à zona de segurança a qual pertence a designação de IP e sua faixa.

Figura 8 DMZ



Fonte: Autoria Própria

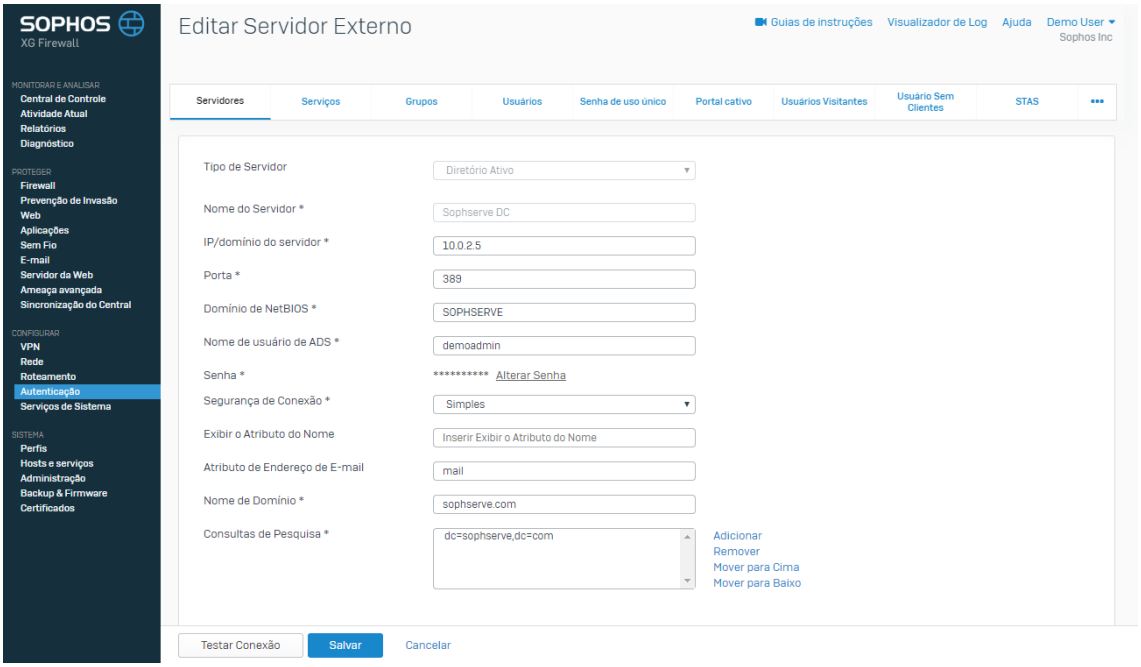
3.6 Autenticação de usuários

Para autenticação da rede e liberação do acesso utilizamos a integração com o *Active Directory (AD)* do Windows Server 2008, seguindo uma ordem de prioridade executadas nos procedimentos seguintes:

- Liberação do Firewall do Windows
- Autenticação do AD na rede
- Instalação do STAS (Sophos Transparent Authentication Suite)

Para a adicionar o Active Directory ou para qualquer outro Servidor, exibe-se a tela de configuração do UTM conforme na figura 9.

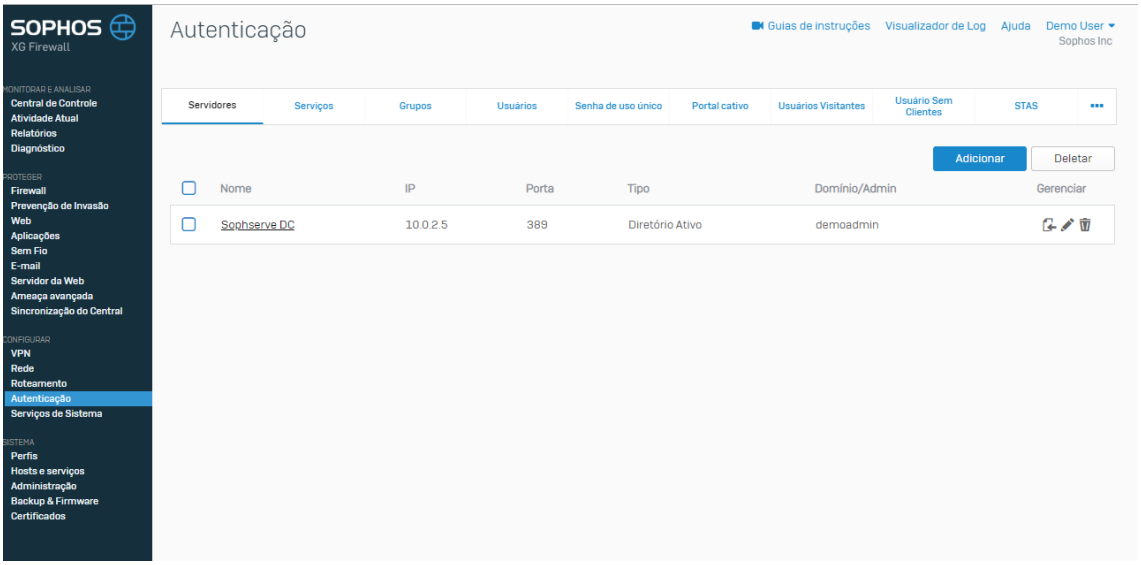
Figura 9 Autenticação AD



Fonte: Autoria Própria

Após a autenticação do AD na rede, ele fica representado como na figura 10.

Figura 10 AD adicionado



Fonte: Autoria Própria

Após o Active Directory (AD) ser inserido, a interface responsável por fazer a integração entre o AD é o Sophos XG, dessa forma a requisição chega para o servidor AD e ele informa de forma transparente o Firewall XG efetuando a liberação do acesso à internet

Após adicionado o AD, executamos o download do modulo *STAS (Sophos Transparent Authetication Suite)* e sua instalação no servidor AD.

STAS (Sophos Transparent Authetication Suite):

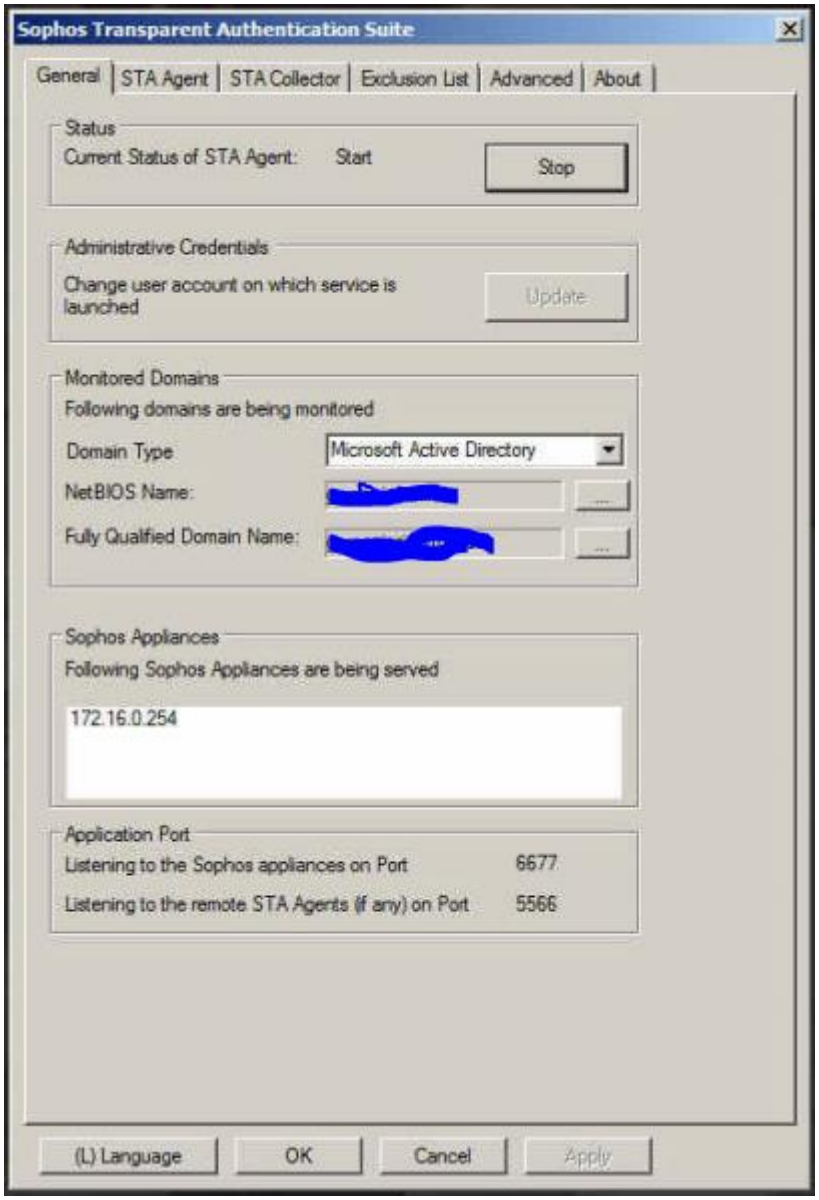
O STAS é um módulo que é integrado com o AD, toda a autenticação no AD é interligada por ele. É feita a verificação do que foi configurado no AD, comparando os acessos de usuários.

As portas que devem ser liberadas no Firewall do Windows, servem para que essa leitura seja feita entre ida e volta (conforme informado pela própria Sophos).

Através do STAS é possível fazer o monitoramento em nível de aplicação, portanto, os recursos de relatórios e gráficos que são possíveis realizar, precisam do módulo STAS ativado e devidamente configurado.

Na figura 11, pode-se ver a tela do serviço em funcionamento.

Figura 11 Configurando STAS



Fonte: Próprio Autor

Após a instalação do STAS, deve-se promover a liberação nas portas do servidor do Windows AD, conforme artigo:

https://community.sophos.com/kb/en-us/123156

Até o momento essas são as devidas configurações feitas no AD:

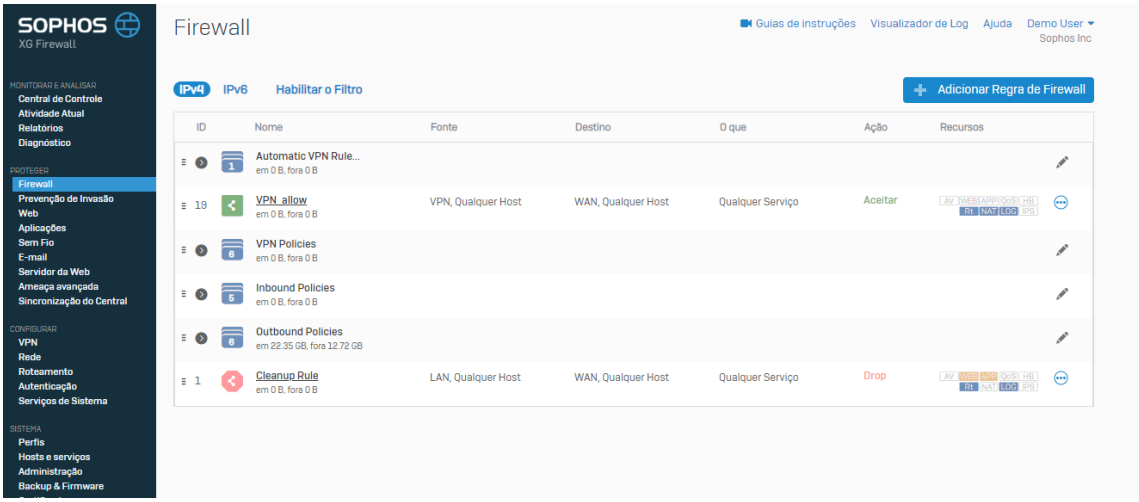
Servidor AD:

- Entrada UDP 6677
- Saída UDP 6060
- Saída TCP 135 e 445 (se estiver usando o WMI ou Acesso de Leitura do Registro)
- Saída ICMP (se estiver usando Ping de Detecção de Logoff)
- Entrada / Saída UDP 50001 (coletor de teste)
- TCP de saída 27015 (sincronização de configuração).

3.7 Criação das regras de Firewall

Agora inicia a configuração de algumas regras de firewall para permitir o acesso a determinados recursos dentro da rede, como é o caso dos usuários com liberação de acesso à internet. Na figura 12, ilustra onde identificam-se os usuários e libera-se o acesso via http/https para navegação web.

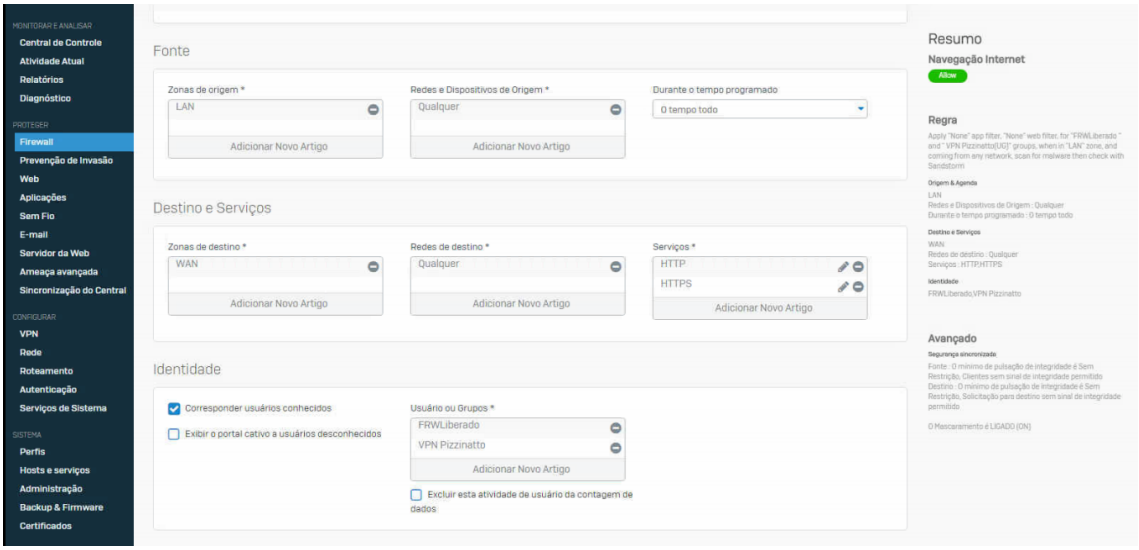
Figura 12 Regras de Firewall



Fonte: Próprio Autor

Na Figura 13, pode-se ver a definição da origem das requisições qual o destino e o tipo de serviço que pode ser utilizado.

Figura 13 Firewall Ativo



Fonte: Próprio Autor

Aqui pode-se definir o tipo de prevenção a invasão que será utilizado, modelar a política de tráfego e a política de web, bem como o tipo de endereçamento de saída.

Conforme a regra se torna válida, pode-se acompanhar os dados que são filtrados.

Neste momento já se tem o Firewall ativo. As demais regras ainda são configuradas devido à mudança de layout do mesmo com alguma dificuldade em relação a versão anterior ao modelo SG (linha anterior ao XG).

4 Resultados

O Sophos XG 135 foi escolhido por ser um UTM bastante completo em recursos e relatórios, além de um gerenciamento fácil e prático.

A sua escolha foi baseada em comparação com o candidato mais próximo: o Fortinet.

Com um custo de 35% menor que a solução cotada da Fortinet e pela facilidade ampla de relatórios que permitem serem extraídos do sistema, permitindo um gerenciamento mais fácil para pequenas e medias empresas, a solução se tornou mais viável, seguido de um ótimo custo benefício.

4.1 Testes

No ambiente de teste foi efetuado a configuração de forma controlada, em um ambiente sem riscos ou quaisquer ameaça para a rede principal. Simulações de falhas tanto no AD, quanto na autenticação de usuários foram realizadas, porém sem êxito, mantendo assim a efetividade da solução encontrada.

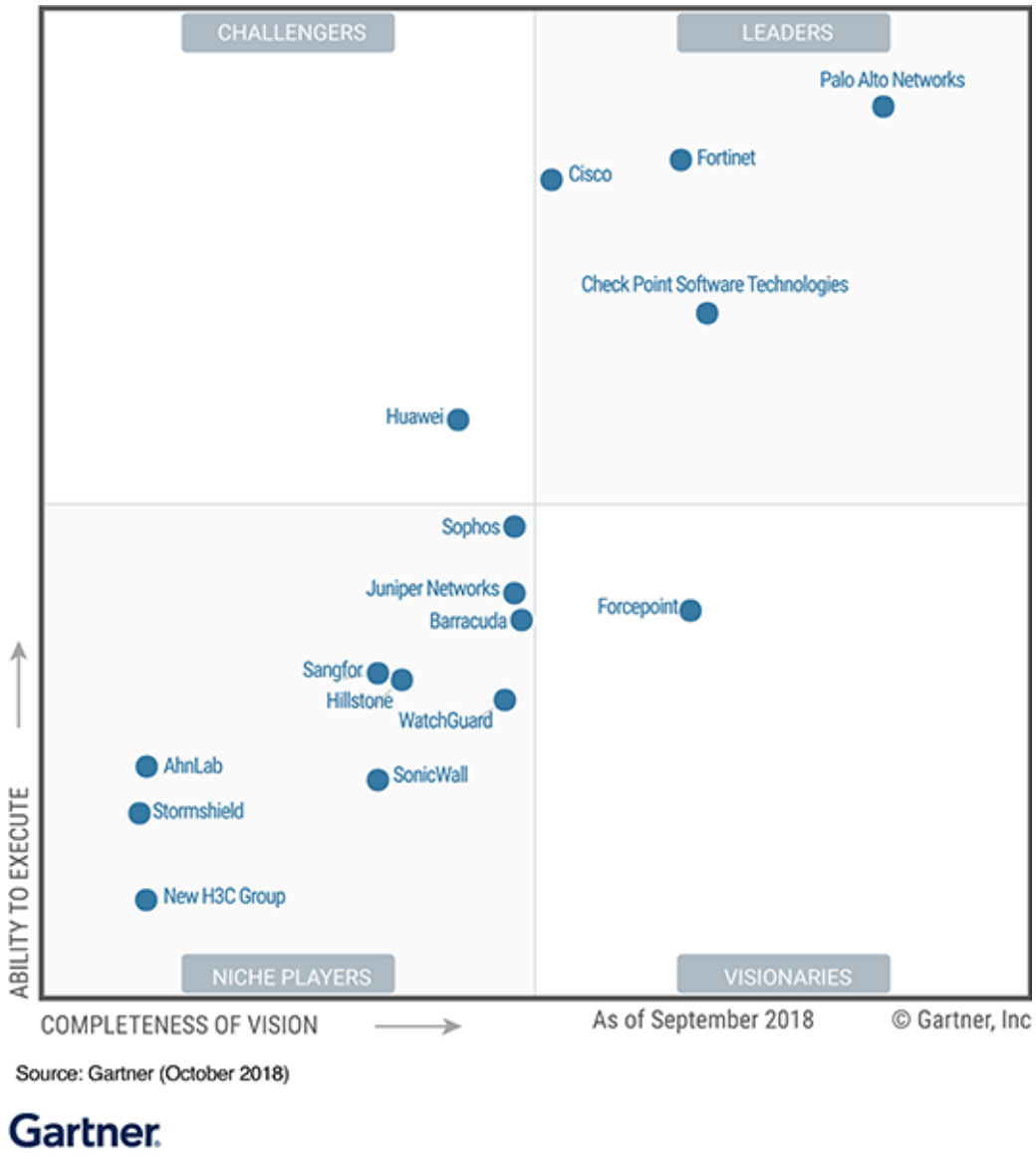
4.2 Quadrante mágico Gartner

A escolha do Sophos XG 135 se deu com base em sua facilidade de relatórios e com seu posicionamento no quadrante mágico da Gartner como observado na figura 14.

Alguns detalhes sobre o Quadrante:

http://introduceti.com.br/blog/quadrante-magico-do-gartner-2018/

Figura 14 Quadrante Mágico Gartner 2018



Fonte: Gartner

Avaliamos também outras soluções como a Fortinet, mas o custo da solução acabou tornando inviável, cerca de 35% a mais que a solução Sophos XG.

5 Conclusões e considerações finais

A implementação aqui demonstrada, ainda está sendo efetuada. Configurações como linhas de redundância, faixa de máquinas preferenciais, VPN ainda não foram terminadas visto o problema de tempo para finalização da implementação.

O Sophos XG 135 é um UTM com foco em empresas de pequeno e médio porte com uma solução abrangente em recursos e relatórios, bem destinada a ambientes onde o setor de TI é pequeno ou terceirizado. Portanto, a melhoria de segurança atinge o primeiro objetivo relacionado a LGPD, onde limita o acesso à informação, essa, porém ainda exige a formação do comitê interno, gerenciamento e definições de responsabilidades pelo trabalho e tratamento de informações, métodos para exclusão de dados conforme solicitado por clientes.

Embora possamos tomar todas as providências que o sistema permitir, creio que o mais complicado, é fazer com que os usuários entendam a sua responsabilidade com as informações, sendo que de toda forma eles alimentam o sistema e normalmente se tornam a parte mais fácil de ser atacada, com recursos de engenharia humana, *Phishing*, etc.

REFERÊNCIAS BIBLIOGRÁFICAS:

Camargo, Gabriel. Disponível em: <https://computerworld.com.br/2018/09/19/lgpd-10-pontos-para-entender-a-nova-lei-de-protecao-de-dados-no-brasil>. Acesso em: 02 mai. 2019.

Machado, Meyer. LEI 13.709/18 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS, 2018.

Oliveira, Déborah. Disponível em: <https://cio.com.br/5-razoes-pelas-quais-voce-deve-se-preocupar-com-a-lgpd>. Acesso em: 02 mai. 2019.

Pinheiro, Patricia Peck. Proteção De Dados Pessoais - Comentários À Lei n. 13.709/2018 – Lgpd, 2018.

Reuters, Thomson. Lei Geral de Proteção de Dados: Disponível em: <https://www.thomsonreuters.com.br/content/dam/openweb/documents/pdf/Brazil/white-paper/thomson-reuters-legal-whitepaper-lei-geral-de-protecao-de-dados.pdf>. Acesso em: 05 mai. 2019.