# Processo de migração de Firewall em um Ambiente Corporativo

**Willian Rigoni Zorzo[1], Marcos V. Corino[1]**

[1]Instituto Federal do Rio Grande do Sul (IFRS) - 95.330-000 -Veranópolis - RS - Brasil

willian.zorzo@hotmail.com, marcos.corino@veranopolis.ifrs.edu.br

***Abstract.*** *The impacts of the SARS-COV2 pandemic also affected organizations and their information systems. The adoption of the home office generated an increase in external access as well as in the volume of sensitive data circulating through the internet. Likewise, cyber-attacks and financial losses, data loss and information leakage have increased. Thus, this work presents the implementation of UTM-type Firewall to increase the security of a company's operations. With the adoption of application and content control services, failover and an SSL VPN, it was possible to reduce threats and provide a reliable environment for activities carried out in the company or at home.*

**Resumo.** Os impactos da pandemia do Sars-COV2 também atingiram as organizações e seus sistemas de informação. A adoção do home office gerou um aumento no acesso externo bem como no volume de dados sensíveis circulando através da internet. Da mesma forma aumentaram os ataques cibernéticos e os prejuízos financeiros, as perdas de dados e o vazamento de informações. Assim, este trabalho apresenta a migração de um *Firewall* do tipo UTM para aumentar a segurança das operações de uma empresa. Com a adoção dos serviços de controle de aplicativos e conteúdo, *failover* e uma VPN SSL foi possível reduzir as ameaças e prover um ambiente confiável para as atividades realizadas na empresa ou em casa.

## Introdução

A informação é um dos bens mais preciosos de uma empresa e que deve ser tratada com cuidado e precaução, requerendo processos de segurança em seu entorno [Fleming 2020]. Para isso cabe à organização planejar e implementar processos que busquem minimizar os riscos a seus sistemas de informação. Com o atual nível de desenvolvimento das redes de computadores, os mais variados tipos de operações desenvolvidas pelas organizações são direta ou indiretamente suportados pelas redes digitais. Fato que torna estas empresas fortemente dependentes da disponibilidade de comunicação por meio da internet. Somado a isso temos também o crescimento exponencial do volume de dados circulando através dos sistemas de informação [Ávila 2017]. Da mesma forma, cresceram os ataques cibernéticos que implicam às organizações prejuízos financeiros de alto montante, perdas de dados e vazamento de informações sensíveis [Prado 2021].

O ano de 2020 começou adicionando mais um problema, um novo vírus, o SARS-CoV-2, responsável pela COVID-19, que fez com que grande parte da população mundial entrasse em isolamento para conter o contágio e a proliferação do vírus. Diante desta

situação as organizações precisaram se adequar a essa realidade e aderir rapidamente ao home office para realizar suas operações. As equipes de TI precisaram rever regras de segurança para flexibilizar situações nunca permitidas, revisar processos de autenticação de usuários e controles de acesso, implantar novos serviços para aumentar a segurança das operações e das informações das empresas enquanto colaboradores têm acesso aos sistemas e dados a partir de sua residência.

O controle de rede de alto nível pode não ser suficiente para proteger contra violações de dados e demais ataques quando falamos em ataques cibernéticos [Check Point 2021]. Assim um *firewall* pode ser uma das primeiras e mais básicas linhas de defesa de uma rede, seja através de um hardware específico, um software ou uma combinação de ambos. No presente trabalho utilizou-se a combinação do hardware com o software, com a função inspecionar o tráfego de entrada e saída em uma rede e decidir qual tráfego pode ir de fora para dentro e de dentro para fora [Tittel 2016]. Quando este *firewall* mantém o gerenciamento unificado de ameaças (do inglês, *Unified Threat Management*, UTM), ele possibilita entre outras funções a adoção dos serviços de controle de aplicativos e conteúdo, *failover* e VPN SSL permitindo reduzir as ameaças e prover um ambiente confiável para as atividades realizadas na empresa ou em casa pelos colaboradores.

Este artigo segue apresentando na seção 2 uma revisão da literatura sobre a *firewall* e trabalhos relacionados a sua implantação, na sequência, na seção 3, o processo de implantação, na seção 4 a apresentação e discussão dos resultados e na seção 5 as considerações finais. Por fim são apresentadas as referências bibliográficas.

## 2. Fundamentação

Este capítulo descreve os conhecimentos teóricos básicos para a realização do estudo. Os tópicos são apresentados de forma resumida dado que o conhecimento da área é tido como pré-requisito para o entendimento dos temas centrais: soluções para segurança da informação e gerenciamento unificado de ameaças.

### 2.1 Firewall

O *firewall de rede* pode ser um hardware, um software ou uma combinação de ambos, que tem por função inspecionar o tráfego de entrada e saída em uma rede e decidir qual tráfego pode ir de fora para dentro e de dentro para fora [Tittel 2016]. Ele possibilita o controle do fluxo de dados entre a rede em que está instalado e o mundo externo, permitindo a definição de regras para o acesso externo ou interno, estabelecendo assim uma gestão do fluxo de tráfego de e para os recursos disponíveis. Essa ferramenta opera através da filtragem de pacotes, analisando alguns dados disponíveis no cabeçalho destes pacotes, como por exemplo, o IP e Porta de Origem e de destino, serviço e tamanho [Manfio 2016]. Com base nas regras implementadas, esses pacotes terão sua entrada ou saída permitida (allow) ou negada (deny).

### 2.2 Unified Threat Management (UTM)

Um *firewall* que mantém o gerenciamento unificado de ameaças (do inglês, *Unified Threat Management*, UTM, consiste em um vasto conjunto de segurança de rede, acesso

e funções de conectividade em um único dispositivo (appliance) com gerenciamento centralizado [Tittel 2016]. O UTM conta com ferramentas como AntiSpam, antivírus para web e e-mail, controle de aplicações, *firewall*, detecção/prevenção de intrusão, rede privada virtual e filtragem de conteúdo web, unificados em sete camadas para proteger redes corporativas. É possível encontrar também, em dispositivos mais atuais, funcionalidades adicionais como balanceamento de carga, prevenção contra perda de dados (*Data Loss Prevention* - DLP) e gerenciamento de banda [Piazza 2015].

O UTM disponibiliza estes recursos de forma flexível, deste a instalação, operação e o gerenciamento centralizado simplificado, apto para os desafios atuais e futuros dos ambientes de redes [SONICWALL 2021]. Essa flexibilidade começa na escolha das tecnologias a serem utilizadas, pois é possível implementar quantas forem necessárias, no local e momento necessário. Da mesma forma, o UTM dispõe de um modelo de licenciamento simples, dentro de uma gama de tecnologias no aspecto de borda de rede e segurança, acabando com a aquisição de módulos adicionais ou de licenças baseadas no número de usuários, algo substancial em requisitos de segurança de uma organização em constante evolução [Tittel 2016].

### 2.3 Wide Area Network Failover (WAN Failover)

A Internet corporativa é um componente fundamental das operações diárias de muitas organizações. É através dela que funcionários trabalham e se comunicam, fornecem serviços a clientes e fazem uso de recursos corporativos. A falha dessa conexão traz consequências negativas como perda de produtividade e redução de receita [UPX 2020]. O WAN Failover opera para evitar a interrupção das conexões de rede e do acesso externo, monitorando o desempenho da WAN e a integridade da conexão, identificando uma interrupção e redirecionando o tráfego para uma conexão ativa [Netgate 2021].

Os provedores de serviço de Internet não são a prova de falhas, sendo que em ambientes que utilizam este recurso como base para seus negócios, é recomendado o uso de redundância de link. O WAN Failover testa as conexões de Internet e, quando uma delas fica lenta ou falha, redireciona o tráfego de rede pelas demais conexões disponíveis. Além disso, efetua registros sobre a disponibilidade e performance de cada conexão, possibilitando ao administrador da rede avaliar o desempenho de seus provedores de serviço [Citrix 2020].

As soluções mais recentes utilizam tecnologia WAN definida por software (SD-WAN) que fornecem desempenho de failover aprimorado sem a necessidade de roteadores físicos ou outro hardware adicional, redirecionando o tráfego de forma inteligente ao longo dos próximos melhores caminhos disponíveis [Citrix 2020].

### 2.4 App Control (Application Control)

Embora um *Firewall* consiga identificar endereços IPs e números de portas, não existe uma garantia de exatidão para identificar o aplicativo que está produzindo determinado tráfego, impossibilitando a definição de políticas com base no fluxo de tráfego específico [Check Point 2021]. O objetivo do controle de aplicativos é identificar exclusivamente o tráfego de vários aplicativos em uma rede, permitindo desta forma que uma organização

consiga granularizar a segurança e definir políticas de roteamento de rede baseado em serviços, a partir da origem de um fluxo de tráfego específico, impedindo que aplicativos não autorizados representem risco para a organização. O controle de aplicativos combina diferentes tipos de tráfego de rede com modelos predefinidos, permitindo que o serviço diferencie um tipo de tráfego de outro [Check Point 2021].

Em seu modo de operação o tráfego de rede de um aplicativo é identificado combinando pacotes com modelos conhecidos de como o tráfego de diferentes aplicativos é estruturado. Desta forma, a identificação é mais precisa e permite que uma organização veja a combinação de tráfego em sua rede. Este nível de visibilidade também pode ser aplicado de várias maneiras diferentes e oferece vários benefícios para uma organização [Check Point 2021].

### 2.5 *Content Filter*

Os filtros de conteúdo normalmente costumam ser vistos em *Firewalls* como um serviço adicional, mas podem ser implementados como hardware ou software, com o propósito de segurança. Também são usados para implementar políticas de acesso de acordo com as normas da empresa relacionadas ao uso do sistema de informação, levando em consideração que todo conteúdo questionável, impróprio ou ilegal cria riscos para as organizações [Barracuda 2021].

O *Content Filter* é uma lista nomeada de termos, que pode ser usada para filtros de conteúdo em políticas para restringir o acesso a sites que contenham em seu cabeçalho qualquer um dos termos listados no conjunto padrão de filtros que contém diversos termos que são bloqueados em muitas organizações [Sophos 2018]. Assim este serviço possibilita filtrar/negar o acesso a páginas da web, sendo utilizado em empresas como componente adicional do *firewall*. Desta forma, ele trabalha especificando padrões de conteúdo, como *strings* de texto ou objetos dentro de imagens que, se combinados, indicam conteúdo impróprio que deve ser filtrado e sucessivamente bloqueado de acordo com as políticas pré-definidas [Barracuda 2021].

### 2.6 Virtual Private Network / SSL

A Virtual Private Network (VPN), em inglês rede privada virtual, é uma tecnologia que permite usar a Internet para comunicação dentro e fora da organização com privacidade neste processo [Forouzan 2010]. Esta tecnologia possibilita o estabelecimento de conexões entre as organizações através de enlaces virtuais que usam a capacidade de infraestrutura da Internet, ao invés das tradicionais linhas de transmissão dedicadas alugadas. Em comparação com o arranjo dedicado, a VPN oferece flexibilidade na reutilização de recursos [Tanenbaum and Wetherall 2011].

O Secure Sockets Layer (SSL), desenvolvido em 1994 pela Netscape, oferece serviços de segurança e de compressão para dados gerados na camada de aplicação. Os dados recebidos da aplicação são comprimidos, assinados e criptografados e em seguida, passados para um protocolo da camada de transporte confiável, como o TCP [Forouzan 2010]. A VPN com o uso do SSL permite que usuários individuais acessem a rede de uma organização, aplicativos cliente-servidor e utilitários e diretórios de rede internos,

fornecendo uma comunicação segura e protegida por meio de uma conexão criptografada para todos os tipos de dispositivos, independentemente de o acesso à rede ser via Internet pública ou outra rede segura [Fortinet 2021].

## 2.7. Trabalhos relacionados

Para realização da pesquisa bibliográfica foi feito o levantamento dos últimos 6 anos (2015 a 2021) com foco principal em implantações de *firewall* em ambientes corporativos. As buscas foram realizadas nos anais da Sociedade Brasileira de Computação (SBC) e portais de teses e dissertações da CAPES. Utilizou-se as palavras-chave: *firewall*, *firewall* UTM, segurança de redes e estratégias de segurança de redes. A seleção dos trabalhos levou em consideração o ambiente de aplicação com foco prático em relação a segurança em redes de computadores.

O trabalho de (Manfio 2016), baseou-se na implementação de um UTM *Firewall* em um ambiente público com o objetivo de unificar o gerenciamento e centralizar as configurações de segurança, demonstrando o seu funcionamento aplicando filtros, bloqueios, regras para acesso a aplicações web e os benefícios do uso da ferramenta no ambiente citado. No início da implementação o autor dividiu a rede em três zonas (WAN, DMZ e LAN) e não foi realizado nenhum bloqueio. Inicialmente foram criados os usuários para navegação com objetivo de analisar os conteúdos acessados por cada um. Após isso, foi realizada uma análise individual de acessos Web para cada usuário para ser realizado um filtro de conteúdo e análise de risco dos sites mais acessados pelos usuários. Para o Filtro Web o autor utilizou das categorias principais já pré-existentes no equipamento e criou algumas personalizadas, no Filtro de Aplicação o autor cria uma categoria personalizada bloqueando o acesso a redes sociais e ao tráfego .mp3 na rede. Realizou-se também o redirecionamento de portas através de uma regra específica WAN to LAN para os serviços da Área Remota do Windows na rede LAN. Como resultados obtidos o autor cita que grande parte do tráfego de rede antes da implementação do *firewall* era desperdiçado com acessos a páginas Web e Aplicações desnecessárias, o monitoramento em tempo real e a segurança na rede aumentaram significativamente devido ao auxílio da ferramenta.

Já (Piazza 2015), traz a instalação de um sistema de gerenciamento unificado de ameaças em três companhias de diferentes segmentos e portes, com o objetivo de documentar e analisar todo o processo, desde o projeto inicial, até o acompanhamento pós instalação. Realizou-se a análise de regras de negócio, regras de *firewall*, regras de roteamento, regras de navegação, exceções às regras e registro de logs visando fazer um levantamento com entrevistas sobre as melhorias promovidas pela ferramenta e o que motivou a escolha de um dispositivo UTM como solução de segurança de redes. Após o processo de implementação da ferramenta e a extração de relatórios, o autor pôde concluir que indiferente do porte da empresa onde a ferramenta é aplicada, houve um grande aumento da segurança na rede em cada um dos ambientes implementados, resumindo-se em administração de segurança facilitada. Como trabalhos futuros, o autor propõe a execução de experimentos com testes de stress com diferentes ferramentas UTM, testes de cargas específicas com o objetivo de estudar e compreender o comportamento destes

equipamentos em um ambiente real e realizar uma simulação de técnicas invasivas aplicadas para avaliar a efetividade prática da ferramenta.

Outro trabalho estudado foi o de (Pereira and Spiagori 2018) que demonstra como a elaboração de um plano de gerenciamento de escopo pode auxiliar a minimizar os impactos causados por uma implantação de um *firewall* em uma rede com 2000 usuários ativos que encontrava-se completamente desprotegida e sem qualquer tipo de análise nos dados trafegados entre a rede LAN e a rede WAN. O autor cita em um trecho de seu trabalho que a motivação para implantação de uma *firewall* se deu após 2 incidentes ocorridos na empresa: a invasão da Central Telefônica da empresa trazendo um prejuízo de R$ 500.000,00 em chamadas internacionais (DDI) feitas pelo invasor e a Invasão do Servidor de E-mails da empresa onde o invasor utilizava do servidor da empresa para enviar e-mails falsos, desta forma o domínio da empresa caiu em uma blacklist. Por fim, foi realizada uma análise com relatórios demonstrando o quão difícil é executar um projeto de implantação de *firewall* sem um planejamento adequado para definir quais são as funcionalidades que serão habilitadas, os setores que serão impactados e as exceções às regras impostas pela ferramenta.

Após a realização do levantamento bibliográfico sobre trabalhos relacionados foi possível perceber os problemas e dificuldades no que diz respeito a implantação de *firewall* em ambientes corporativos. Algumas dificuldades puderam ser contornadas com a utilização de documentações de fabricantes de equipamentos e fóruns sobre o assunto na internet.

## 3. A implantação

A etapa inicial deste trabalho teve como foco o mapeamento da infraestrutura e de equipamentos conectados à rede local da empresa que seriam impactados durante o processo de migração para o novo UTM *firewall* da SonicWall. Com isso, foi possível identificar serviços disponíveis e recursos compartilhados na rede. Com base nestes dados, a rede local foi dividida em setores de acordo com a atividade fim de cada um, o que possibilita ver com mais clareza os serviços e recursos que cada um deverá ter a sua disposição, bem como definir níveis de acesso adequados a cada um deles. A figura 1 ilustra o cenário ao qual foi realizado o presente trabalho.

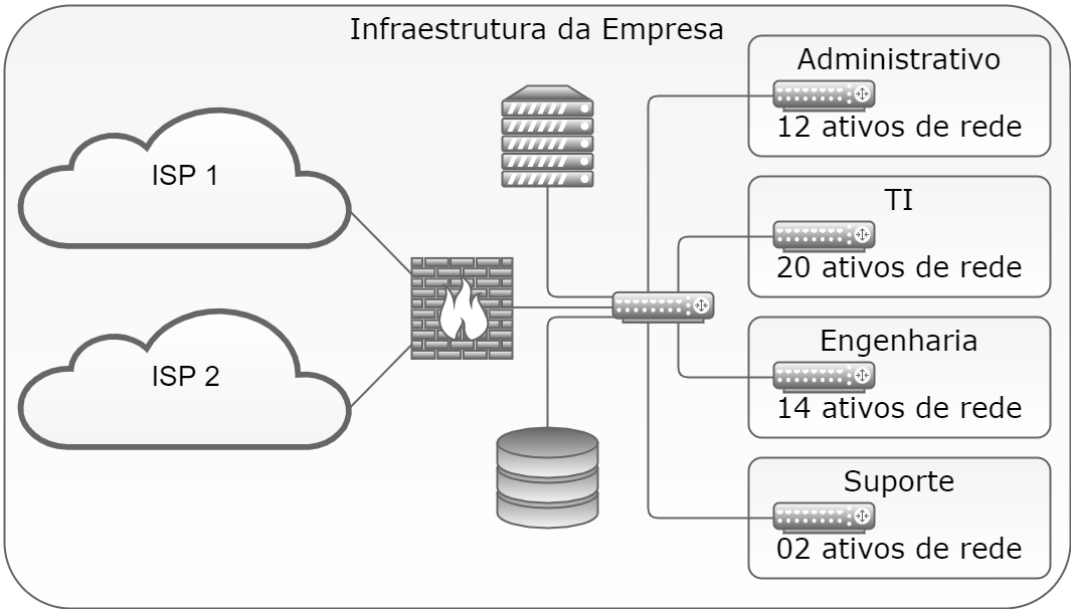


**Figura 1 – Diagrama de rede. Autoria própria.**

Posteriormente foram definidas as políticas de *failover* para as interfaces WAN-SD, uma vez que a empresa conta com dois links de comunicação providos por ISPs diferentes. Essas políticas contemplam desde a inoperância até a sobrecarga destas conexões. Na sequência foram definidas as regras de acesso internas e externas, os aplicativos permitidos na rede e os conteúdos indesejados, todos separados por departamento. Também foram elencados os colaboradores que teriam permissão de acesso a rede interna a partir de conexões externas por meio da VPN.

A partir do planejamento e com as configurações definidas partiu-se para a configuração do UTM *firewall* propriamente dito. Com a definição de interfaces locais e externas o equipamento foi adicionado à rede. As interfaces locais são responsáveis por interligar os diversos segmentos de rede da empresa. Para essas interfaces foi definido um escopo de endereçamento dinâmico, sendo reservado os primeiros IPs (*Internet Protocol*) para equipamentos que compõem a infraestrutura básica como central telefônica, central de alarme, servidores, máquinas virtuais e ativos de rede. Conforme orientação do fabricante também foi definido um DNS (*Domain Name System*) Proxy para que os dispositivos da LAN usem o *firewall* como o servidor DNS enviando as consultas diretamente a ele, o que possibilita o gerenciamento das consultas DNS da rede em um único ponto [SONICWALL 2021].

As interfaces definidas como externas (WAN), foram configuradas para receberem dois links de ISPs diferentes. As conexões com estes provedores são realizadas por meio de PPPoE (*Point-to-Point Protocol over Ethernet*). Após as conexões com a Internet serem efetuadas, foi habilitada a opção *Failover* e *Load Balancing* para permitir que o tráfego seja roteado apenas pela porta WAN secundária se a porta WAN primária não estiver disponível ou com sobrecarga. Isso permite que o *firewall* mantenha uma conexão persistente para o tráfego externo. Também foi ajustado um timer para verificação da atividade da porta para identificar problemas e efetuar a troca da interface. Esse parâmetro regula o número de vezes que o *firewall* testa a interface como inativa

antes de efetuar o *failover* para a interface secundária. Por fim, a última verificação é especificar o número de vezes que o *firewall* testa a interface como ativa antes de efetuar o *failback*, o retorno, para a interface primária [SONICWALL 2021]. Com essa funcionalidade espera-se redução ao menor índice possível de indisponibilidade ou lentidão dos serviços de rede bem como evitar a interrupção dos atendimentos de suporte a clientes remotos.

Nesta implantação utilizou-se o monitoramento lógico com a investigação da interface habilitada, configurando como condição que o teste é bem sucedido quando o alvo principal ou o alvo alternativo respondem. Para o teste de ambas as interfaces foi configurado para a interface principal a resposta ICMP para endereço IP externos 8.8.8.8. Já para a interface alternativa a resposta é aguardada do IP 1.1.1.1 e como opção padrão de destino foi utilizado o IP 204.212.170.23, endereço disponibilizado pela SonicWall.

Para implantação das políticas de controle de aplicativos foi realizada uma análise em todas as categorias para verificar suas respectivas assinaturas. Após a análise e levantamento de impacto nas operações da empresa, foi realizado o bloqueio das seguintes categorias: multimédia, p2p, proxy-access, remote-access, gaming, social-networking, scada-apps, stock-trading, miners. Dentro destas categorias foram permitidas algumas aplicações como Spotify, Youtube, Apple iTunes, Google Play, Amazon Prime Music, TeamViewer e AnyDesk, pois essas assinaturas foram dadas como produtivas e escaladas como importantes para o funcionamento da empresa, segundo a diretoria.

O UTM *firewall* possui integrado um objeto de filtro de conteúdo no qual é possível apenas realizar ajustes, não sendo possível excluí-lo. Por segurança, o fabricante indica a criação de novo objeto com as configurações desejadas. Isso se justifica pela facilitação do processo de restauração em caso de falha, pois assim é possível retornar para o filtro de conteúdo padrão, sem alterar as demais configurações do *firewall*. Para a configuração da implantação das políticas de controle de conteúdos foi realizada uma análise em todas as categorias. Após a análise e deliberação da diretoria da empresa, foi realizado o bloqueio das seguintes categorias: Violence/Hate/Racism, Intimate Apparel/Swimsuit, Nudism, Pornography, Weapons, Adult/Mature Content, Cult/Occult, Drugs/Illegal Drugs, Illegal Skills/Questionable Skills, Sex Education, Gambling, Alcohol/Tobacco, Malware. A fim de minimizar os riscos e ameaças na rede, se faz necessário a utilização de uma ferramenta que seja capaz de identificar e bloquear qualquer conteúdo prejudicial e malicioso por trás de páginas web, evitando diversos possíveis danos que um simples acesso indevido por um usuário pode causar para à empresa.

Devido à pandemia do coronavírus se fez necessário a adoção de um método para que os funcionários da empresa continuassem produzindo e exercendo as mesmas funções da empresa em home office, inclusive o acesso e atendimento a clientes remotos para suporte de uma forma segura como se estivessem dentro da empresa. Para implantação foi realizada a utilização da SSL VPN e para o acesso dos colaboradores remotos foi utilizado o cliente do *firewall*. O NetExtender é um cliente SSL VPN para Windows e Linux. Ele permite a execução de qualquer aplicativo além de acesso aos recursos disponíveis na rede com segurança utilizando o protocolo ponto a ponto (PPP).

Com base no levantamento inicial, foi realizada a configuração da VPN para os usuários elencados nesta etapa. A identificação dos usuários utilizou o e-mail institucional, sendo que após o primeiro login é realizada uma vinculação de chave TOTP (*Time-based One-Time Password*) para a autenticação em dois fatores. Cada usuário criado foi vinculado ao grupo SSLVPN Services com acesso total à zona LAN. Durante a configuração da VPN, foram criados 14 usuários com permissão para utilização da SSL VPN sendo que foram adquiridas 12 licenças para utilização da SSL VPN de forma simultânea. Por existir uma escala de plantão para atendimento, não ocorreram problemas ou dificuldades na utilização do serviço. Com essa ferramenta espera-se que o usuário em home office consiga exercer todas suas funções como se estivesse trabalhando dentro da empresa de forma segura.

## 4. Resultados e discussões

Durante a migração houve problemas recorrentes devido à existência de outro equipamento *firewall* na rede, o qual foi substituído pelo UTM. Entretanto, não foi previsto o gerenciamento que este exercia sobre os alguns equipamentos da rede. Por exemplo o Unifi Cloud Key. A ideia inicial era realizar a troca do *firewall* da Unifi pelo *firewall* da SonicWall sem modificar configurações no Cloud Key. Após a troca do equipamento, foram identificadas anomalias como lentidão na navegação e até falhas de comunicação. Para a resolução desses problemas foi necessário resetar todas as configurações de todos os equipamentos e iniciar a configuração novamente, agora com o Unifi Cloud Key gerindo apenas os equipamentos da Unifi (Switches e APs) e os pontos de acesso sem fio. Com isso foi restabelecido o desempenho esperado da rede.

Essa situação ratifica o exposto por (Pereira and Spiagori 2018) que demonstram a dificuldade de se executar um projeto de implantação de *firewall* sem um planejamento adequado, que defina corretamente as funcionalidades que serão habilitadas, os setores e equipamentos que serão impactados e as exceções às regras impostas pela ferramenta.

Na implantação do APP Control, ocorreram problemas com bloqueios de algumas aplicações devido algumas assinaturas contidas dentro das aplicações estarem bloqueadas. Para resolver o problema foi necessário realizar uma análise mais profunda dos logs para identificar o tipo de bloqueio que estava ocorrendo. Um deles foi a indisponibilidade do serviço de compartilhamento de vídeo *Vimeo*, utilizado em ambientes de estudo online. O bloqueio ocorreu devido à restrição da categoria Social-Networking, que continha a aplicação *Vimeo*, A figura 2 ilustra a tela de controle das aplicações disponíveis e restritas na rede. Para restabelecer o serviço bastou a inativação deste aplicativo na regra mãe na tela de controle.

| # | CATEGORY | APPLICATION | SIGNATURE NAME | RISK | BLOCK |
|---|---|---|---|---|---|
| 1 | P2P | Winny | Login | 3 / 5 | ✓ |
| 2 | P2P | eMule | Obfuscated Protocol | 3 / 5 | ✓ |
| 3 | PROXY-ACCESS | Non-SSL traffic over SSL port | Traffic Anomaly Detection | 3 / 5 | ✓ |
| 4 | MULTIMEDIA | Flash Video (FLV) | Download 1 | 3 / 5 | ✓ |
| 5 | MULTIMEDIA | Flash Video (FLV) | Download 2 | 3 / 5 | ✓ |
| 6 | P2P | BitTorrent Protocol | UDP Activity 1 [Reqs SID 5] | 2 / 5 | ✓ |
| 7 | P2P | BitTorrent Protocol | UDP Activity 3 [Reqs SID 5] | 2 / 5 | ✓ |
| 8 | REMOTE-ACCESS | AweSun Remote Desktop | HTTPS Activity | 1 / 5 | ✓ |
| 9 | MULTIMEDIA | Flash Video (FLV) | Download 3 | 3 / 5 | ✓ |
| 10 | P2P | Xunlei Thunder | Resource Searching 3 | 3 / 5 | ✓ |
| 11 | P2P | QQDownload | UDP Traffic 1 | 3 / 5 | ✓ |
| 12 | SOCIAL-NETWORKING | Netlog | HTTP Activity | 1 / 5 | ✓ |
| 13 | MULTIMEDIA | Microsoft Silverlight | HTTP Activity 3 | 3 / 5 | ✓ |
| 14 | MULTIMEDIA | PPStream | Channel Info | 1 / 5 | ✓ |
| 15 | MULTIMEDIA | PPStream | UDP Activity 1 | 1 / 5 | ✓ |
| 16 | MULTIMEDIA | PPStream | TCP Activity 1 | 1 / 5 | ✓ |
| 17 | P2P | GOGOBOX | Client Activity | 3 / 5 | ✓ |

**Figura 2 – Tela de controle de categorias. Autoria própria.**

Outro problema ocorreu com dispositivos Apple onde não funcionava o envio e recebimento de mensagens e ligações do WhatsApp. Para resolução do problema foi realizada a análise dos logs e verificou-se que dentro da categoria Proxy-Access havia uma aplicação chamada *Encrypted Key Exchange* com uma assinatura chamada TCP *Random Encryption* bloqueando os serviços do WhatsApp nos dispositivos da Apple. A assinatura citada é uma família de métodos de contrato de chave autenticada por senha [SONICWALL 2020]. Segundo o fabricante, por padrão uma sessão criptografada é apenas um conjunto de bytes aleatórios dentro da carga útil da camada de transporte, a forma como os bytes são interpretados somente os desenvolvedores do aplicativo sabem, desta forma todas as sessões criptografadas são semelhantes no *firewall*.

A utilização do serviço de VPN em conjunto com o Cliente VPN NetExtender se mostrou confiável e seguro gerando os resultados esperados e satisfação pelos usuários para acesso a rede interna. O dispositivo ainda conta com uma tela de gestão sobre as conexões em andamento informando sobre atividade e consumo de banda interna. Também foi necessário criar uma regra de roteamento para que os colaboradores ao conectar na VPN obtivessem permissão para acessar os clientes. Para isso, foi criada uma regra de *firewall* de roteamento com os IPs públicos de cada cliente e um grupo de objetos VPN Clients.

Sanados os problemas, constatou-se uma considerável queda no tráfego externo, resultante da aplicação dos recursos App Control e Content Filter que eliminaram o desperdício com acesso a aplicações e páginas não produtivas, tais como: vídeos, jogos online e apps multimídia diversos. Além da redução do tráfego internet obtido através dos filtros de conteúdo e de aplicação, a implantação do UTM deu capacidade de monitoramento em tempo real das atividades de rede, como usuários autenticados, registros de horário, tentativas de ataques externos e panorama sobre tráfego de download e upload. Esse monitoramento permite identificar anomalias no instante em que elas acontecem, sendo de grande utilidade para o administrador da rede. O gráfico 1 mostra em um período de 60 dias as anomalias registradas por categoria. É possível verificar o

grande número de ocorrências no que diz respeito ao filtro de conteúdo, fato que, como dito anteriormente, é um dos fatores na redução do tráfego externo.

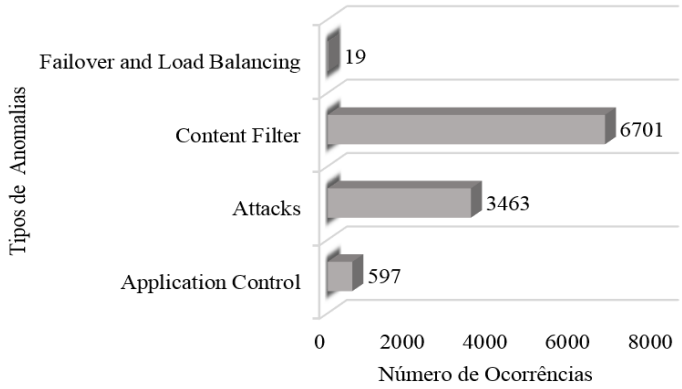


**Gráfico 1 – Ocorrências por tipo de anomalia em 60 dias. Autoria própria.**

Além disso, o gráfico mostra o elevado número de tentativas de ataque externo realizadas contra a rede da empresa. Isso demonstra a importância de um equipamento de proteção na borda da rede, realizando os controles de acesso a todos os recursos disponíveis. Nesta mesma imagem, é possível identificar que, em 60 dias, ocorreram 19 eventos de *failover*, ou seja, em 19 oportunidades, as operações da empresa teriam sido interrompidas pela falha de um link de comunicação. Assim o WAN *failover* mostra-se fundamental para a continuidade do negócio, sendo uma ferramenta de contingência eficiente.

## 5. Conclusões

Este trabalho aborda a migração de uma ferramenta de segurança da informação, o *firewall* com gerenciamento unificado de ameaças, *Unified Threat Management*, para gerir a ligação entre a rede interna e externa de uma empresa.

Diante dos resultados obtidos e das funcionalidades implementadas considera-se que o UTM *firewall* é uma solução eficaz e eficiente para gerir a segurança no ambiente corporativo onde foi implantado, proporcionando aumento no nível geral de segurança das redes em que atua. Este equipamento descomplica a rotina dos profissionais de TI envolvidos na gestão da rede pois facilita a criação e gestão de políticas e controles de acesso, a emissão de relatórios, o monitoramento em tempo real entre outros [Piazza 2015].

Sua implantação, em um breve período, se mostrou relevante diante do número de potenciais ameaças barradas pelo equipamento e suas funções de filtragem de aplicativos e conteúdo. Além disto, permite uma melhor utilização da banda disponível para as atividades fins da empresa e ainda tem potencial para economia financeira se considerarmos a redução da distração dos funcionários com acessos inadequados e improdutivos [Manfio 2016].

Cabe ressaltar que embora dito anteriormente que este equipamento facilita as operações de TI, sua implantação necessita de conhecimento específico de redes de computadores, protocolos e de segurança da informação. Uma vez que operam na

fronteira da empresa para o mundo externo, o planejamento do processo de implantação deve ser muito bem realizado para evitar interrupções de serviços e prejuízos às operações. Este fato é evidenciado aqui e em todos os trabalhos relacionados pesquisados. O que mostra a complexidade da implantação de um sistema como esse sem avaliar adequadamente as atividades e definir o plano corretamente.

Como sugestão para trabalhos futuros, pretende-se realizar um refinamento mais amplo para todos os serviços que foram implantados no presente trabalho, para que assim seja possível restringir cada vez mais os acessos dos colaboradores a conteúdos improdutivos, permitindo reduzir as ameaças e aumentar o nível de segurança no ambiente da empresa.

## Referências


Ávila, T. (2017) "O que faremos com os 40 trilhões de gigabytes de dados disponíveis em 2020?", https://ok.org.br/noticia/o-que-faremos-com-os-40-trilhoes-de-gigabytes-de-dados-disponiveis-em-2020, Janeiro.

Barracuda. (2021) "Content Filtering", https://www.barracuda.com/glossary/content-filtering, Outubro.

Check Point. (2021) "What is Application Control?", https://www.checkpoint.com/cyber-hub/network-security/what-is-application-control/, Outubro.

Citrix. (2021) "SD-WAN", https://www.citrix.com/solutions/sd-wan/wan-failover.html, Agosto.

Fleming, T. (2020) "Artigo: O impacto da Covid-19 na segurança de dados das empresas", https://casafirjan.com.br/coronavirus/artigo-o-impacto-da-covid-19-na-seguranca-de-dados-das-empresas, Janeiro.

Forouzan, B. A. (2010). *Comunicação de Dados e Redes de Computadores*. 4. ed. Porto Alegre: AMGH.

Fortinet. (2021) "SSL VPN", https://www.fortinet.com/resources/cyberglossary/ssl-vpn, Novembro.

Manfio, J. (2016). Implantação de uma Infraestrutura de Segurança da Informação Utilizando UTM Firewall. Antonio Meneghetti Faculdade.

Netgate. (2021) "Load Balancing and Failover with Gateway Groups", https://docs.netgate.com/pfsense/en/latest/multiwan/load-balance-and-failover.html, Agosto.

Pereira, R. E. and Spiagori, M. G. R. (2018). Planejamento de Escopo para o Projeto de Implantação de Firewall Corporativo na Empresa Prati, Donaduzzi e Cia LTDA. FAG Centro Universitário.

Piazza, T. (2015). Análise da Implantação e Utilização de Sistemas de Gerenciamento Unificado de Ameaças (Unified Threat Management – UTM) em Empresas de Diferentes Portes. Centro Universitário Univates.

Prado, F. (2021) “Brasil foi 5º país com mais ataques cibernéticos no ano: relembre os principais”, https://www.istoedinheiro.com.br/brasil-foi-5o-pais-com-mais-ataques-ciberneticos-no-ano-relembre-os-principais, Janeiro.

SonicWall. (2021) “Technical Documentation”, https://www.sonicwall.com/support/technical-documentation/?language=English, Julho.

Sophos. (2018) “Content Filters”, https://docs.sophos.com/nsg/sophos-firewall/v17.1.4/Help/en-us/webhelp/onlinehelp/index.html#page/onlinehelp/ContentFilterManage.html, Outubro.

TANENBAUM, A. and WETHERALL, D. (2011). *Redes de Computadores*. 5. ed. São Paulo: Pearson Prentice Hall.

Tittel, E. (2016). *Unified Threat Management For Dummies*. 2. ed. New York: John Wiley & Sons, Inc.

UPX. (2020) “Os 4 benefícios da redundância de links para o seu negócio!”, https://www.upx.com/post/redundancia-de-operadoras, Janeiro.