ARQUITETURA PARA MONITORAMENTO E GERENCIAMENTO REMOTO DE REDES COMO PRESTAÇÃO DE SERVIÇO

Diego Martins de Oliveira[1,2], Rafael T. de Sousa Jr[1], Daniel Alves da Silva[1],
Francisco L. de Caldas Filho[1], Georges Daniel Amvame-Nze[1] e Fábio Lúcio Lopes de Mendonça[1]
[1]*Universiade de Brasília – UnB, Brasil*
[2]*Instituto Federal de Brasília – IFB, Brasil*

RESUMO

Empresas, escritórios e negócios dos mais variados tipos, tamanhos e áreas de atuação, se beneficiam com o uso de recursos da tecnologia da informação. Para se comunicar com clientes, armazenar informações, realizar negócios e as mais diversas tarefas. Incidentes ou interrupções destes serviços ou recursos, muitas vezes podem significar não só perda de tempo e produtividade, mas também perdas financeiras. Daí a necessidade de profissionais capacitados para monitorar esses recursos de informática e atuar para sanar os problemas o mais rápido possível. Por outro lado, a manutenção de uma equipe fixa destes profissionais pode não se encaixar na realidade da empresa, seja por questões de custo ou de gerenciamento de pessoal. O que propomos neste trabalho é testar uma arquitetura que envolve uma gama de soluções em *software* para o monitoramento e gerenciamento remoto de uma infraestrutura de rede e serviços. O que viabilizaria o modelo de monitoramento e gerenciamento remoto como serviço prestado, ou seja, a possibilidade de empresas contratarem o serviço de monitoramento e gerenciamento remoto de suas redes.

PALAVRAS-CHAVE

Monitoramento Remoto, Gerenciamento de Redes, Serviços de Rede

1. INTRODUÇÃO

A utilização de recursos de tecnologia da informação (TI), em empresas e escritórios tem crescido e se tornado cada vez mais importante para os negócios, seja para realizar transações financeiras, armazenar informações ou viabilizar as mais diversas tarefas de seus colaboradores, até pequenos negócios ou escritórios necessitam de algum nível de informatização.

Mesmo estando presente em boa parte dos negócios, geralmente, a área de TI não é o foco principal da empresa, mas ainda é uma ferramenta importante para proporcionar condições de trabalho, para que a empresa atinja seus objetivos. Neste sentido, a depender das necessidades do negócio, a estrutura de TI, pode atingir uma complexidade que exija a contratação de profissionais especializados para garantir o bom funcionamento da rede e dos serviços, mesmo num escritório de médio porte, por exemplo.

A criação de uma equipe de TI apesar de necessária, muitas vezes não é compatível com o porte da empresa. Uma possível saída, é a contratação de prestadores de serviços de TI que podem agir em casos pontuais de necessidade manutenção, por outro lado, essa necessidade de manutenção na maior parte dos casos só é notada quando algo para de funcionar, o que pode se materializar em prejuízo financeiro à empresa. O que nos leva à necessidade de não só corrigir os problemas, mas também de monitorar a estrutura para uma possível antecipação do problema ou mesmo para uma reação mais rápida.

O objetivo deste trabalho é testar uma arquitetura que envolve uma gama de soluções em software gratuito que permita o monitoramento e gerenciamento remoto de redes e aplicações, como uma prestação de serviço por uma equipe especializada, e que exija pouca interferência física na estrutura já instalada da rede a ser monitorada.

2. REFERENCIAL TEÓRICO E MERCADO

Em *An Assessment of Practical Hands-On Lab Activities in Network Security Management*, os autores propõem uma arquitetura de rede em ambiente emulado com o *software* GNS3 para o aprendizado e prática de técnicas de segurança e gerenciamento de redes por estudantes (CHOU, HEMPENIUS, 2020). Neste trabalho utilizamos também um ambiente de rede emulado para testar a viabilidade de se montar um serviço de monitoramento em uma rede remota.

Escolhemos trabalhar com *softwares* e soluções gratuitas, porém para efeito de conhecimento do leitor, também comentamos sobre soluções que em suas versões completas são pagas. Lembrando que mesmo estes, exigem profissionais de TI para configurar e utilizar seus recursos.

2.1 Soluções de Mercado

PRTG Network Monitor, solução da empresa Paessler, segundo a empresa esta solução consegue monitorar: largura de banda, banco de dados, serviços de rede, servidores dentre outros, exibe painéis e mapas de rede. Possui uma versão de testes por tempo limitado e versão completa paga que varia de $1,799 a $15,999 (PAESSLER AG, 2022).

Datadog, solução da empresa de mesmo nome, a solução oferece monitoramento de desempenho e ativos de rede, serviços, aplicativos, contêiner dentre outros. As funcionalidades são divididas em módulos que devem ser adquiridos separadamente. As licenças são por meio de assinaturas mensais iniciam em $5 por mês/máquina a depender do módulo desejado (DATADOG, 2022).

2.3 Soluções Gratuitas

Zabbix, é uma solução gratuita para monitoramento de infraestrutura de TI, o software é capaz de monitorar ativos de rede, sistemas operacionais, serviços, servidores dentre outros. (ZABBIX LCC,2022).

PfSense *Community Edition* é um Sistema Operacional (OS) customizado para ser usando como *gateway* e *firewall* de rede. (RUBICON Communications, 2022)

DD-WRT é um *firmware* alternativo baseado em Linux disponível para uma grande variedade de modelos de roteadores. O sistema adiciona vários recursos ao equipamento e permite uma configuração mais refinada. (EMBEDD GmbH, 2022).

GNS3 é um emulador de rede, programa capaz de criar um ambiente de rede virtual emulado, onde cenários com diferentes configurações de rede podem ser criados e testados (SOLARWINDS, 2022).

3. METODOLOGIA

O cenário que pode ser visto na Figura 1, foi criado no GNS3.

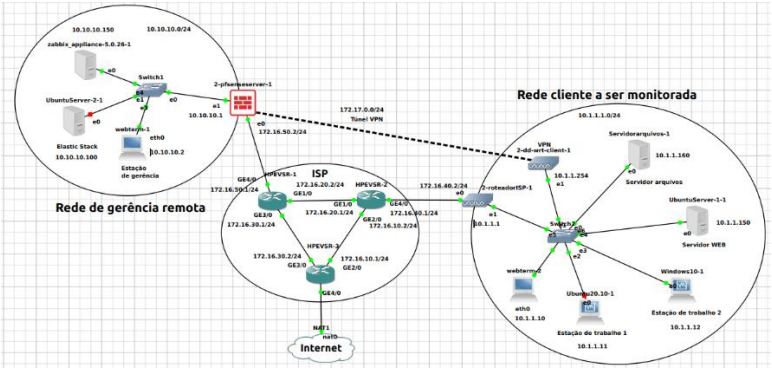


Figura 1. Cenário de experimento

O cenário proposto é composto pelos seguintes grupos:

Rede de gerência remota - rede para o monitoramento remoto, onde estão as máquinas e *softwares* utilizados no monitoramento, na saída da rede foi colocada uma máquina com pfSense para criação das regras de firewall e conexão VPN, com link para o *Internet Service Provider* (ISP).

Rede cliente - rede a ser monitorada, neste cenário, esta possui um servidor de páginas *WEB* e servidor de arquivos, duas estações de trabalho e o roteador geralmente fornecido pelo ISP na borda, outro roteador foi adicionado pelo prestador de serviço de monitoramento, este equipamento está com a *firmware* alternativa DD-WRT para funcionar como cliente de *Virtual Private Network* (VPN).

Redes ISP - um anel de roteamento para simular o provedor de serviços de internet, que faz a interligação física entre a rede do prestador de serviço de monitoramento remoto e a rede cliente que deve ser monitorada.

As configurações realizadas no experimento podem ser replicadas em um cenário real, já que foram realizadas em máquinas virtuais suportadas pelo VirutalBox e pelo GNS3.

3.1 Da Configuração

No início, a rede cliente já possui duas estações de trabalho, uma com OS Windows e outra com OS Linux *Desktop* para diversificar os sistemas e comprovar que ambos podem ser monitorados, possui ainda um servidor WEB e servidor de arquivos, ambos serviços com acesso apenas via rede interna/*intranet*, em máquinas com Ubuntu Server.

O roteador/*access point* que geralmente é fornecido pelo ISP, muitas vezes não tem opções de configurações avançadas ou mesmo, o ISP não fornece acesso às configurações dele, por isso optamos por instalar na rede um outro roteador/*access point*, esse com o *firmware* DD-WRT que nos permite configurar um cliente ou servidor de VPN, de modo que as máquinas que se conectarem à essa VPN tem acesso às duas redes.

Ainda sobre o cliente de VPN, nesta solução optamos pelo pequeno *access point* com DD-WRT porque este, num cenário real pode representar alguma economia financeira, já que o *firmware* pode ser instalado em equipamentos simples e baratos. Para uma solução mais robusta no caso de uma rede com maior tráfego, o cliente de VPN pode ser instalado em uma máquina do tipo servidor, neste caso poderíamos por exemplo utilizar o pfSense.

O software que utilizamos para o monitoramento foi o Zabbix, que pode ser usando não somente para monitoramento mas também para antecipação de problemas (MARTINS, R.S., MEDEIROS , R.M., SILVA, W.M.C,2015). Após alguns testes notamos que o monitoramento via agentes é mais estável do que o monitoramento simples via SMNP com autodescoberta que também é possível.

O tipo de VPN configurado no cenário foi *Site to Site*, ou seja, vai interconectar as duas redes, com SSL/TLS, o servidor de VPN foi configurado no pfSense na borda da rede do prestador de serviço, a autoridade certificadora, os certificados e chaves também foram criados nesta máquina. O roteador com DD-WRT na rede cliente foi configurado como cliente VPN, mesmo não estando na borda da rede. O túnel criado entre essas duas máquinas permite que as redes separadas geograficamente se comuniquem, regras de Firewall e rotas foram criadas nas duas redes para completar a configuração. O estado do túnel do lado do servidor, pfSense, pode ser visto na Figura 2.

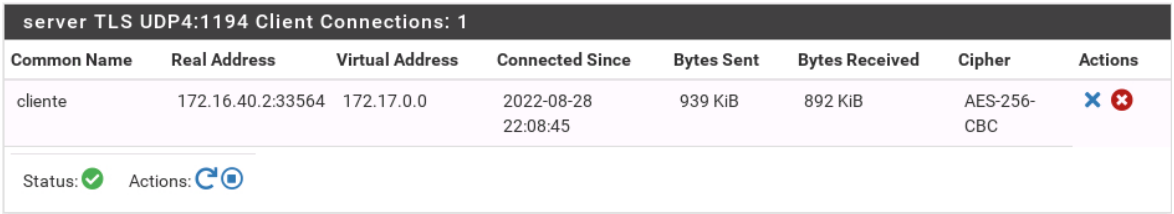


Figura 2. Estado da conexão VPN no servidor

Do lado da rede cliente o roteador com DD-WRT, o estado da conexão pode ser visto na Figura 3.

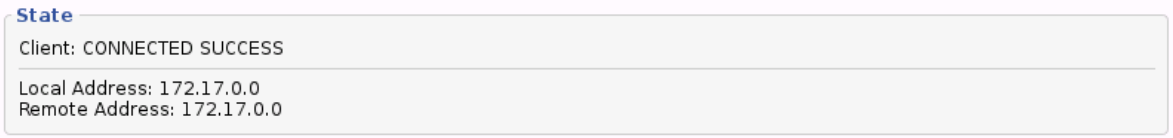
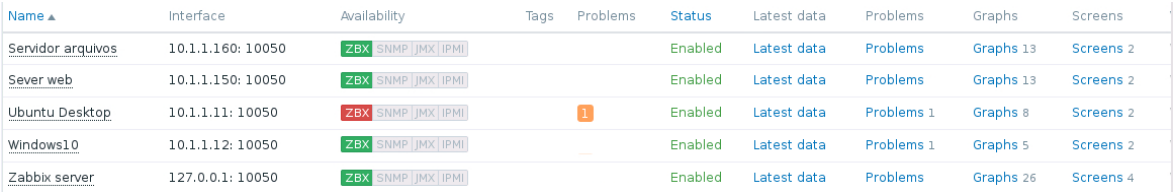


Figura 3. Estado da conexão VPN no cliente

No Zabbix após a criação da VPN foi possível se conectar aos agentes instalados nas máquinas da rede monitorada, e iniciar o monitoramento. A Figura 4 mostra a tela do Zabbix com a lista máquinas monitoradas e seus estados.



Name ▲	Interface	Availability	Tags	Problems	Status	Latest data	Problems	Graphs	Screens
Servidor arquivos	10.1.1.160: 10050	ZBX SNMP JMX IPMI			Enabled	Latest data	Problems	Graphs 13	Screens 2
Sever web	10.1.1.150: 10050	ZBX SNMP JMX IPMI			Enabled	Latest data	Problems	Graphs 13	Screens 2
Ubuntu Desktop	10.1.1.11: 10050	ZBX SNMP JMX IPMI		1	Enabled	Latest data	Problems 1	Graphs 8	Screens 2
Windows10	10.1.1.12: 10050	ZBX SNMP JMX IPMI			Enabled	Latest data	Problems 1	Graphs 5	Screens 2
Zabbix server	127.0.0.1: 10050	ZBX SNMP JMX IPMI			Enabled	Latest data	Problems	Graphs 26	Screens 4

Figura 4. Lista de máquinas monitoradas pelo Zabbix

Na Figura 4 é possível ver que uma das máquinas monitoradas está em estado de erro, representado pela cor vermelha.

4. CONCLUSÃO

Como primeiro ponto, gostaríamos de ressaltar que a instalação e configuração de todo este conjunto de soluções não é simples, e vai exigir bastante conhecimento do profissional que for realizar, por outro lado não é nada que fuja muito do que se espera de um administrador de redes.

Baseados na experiencia com a configuração do experimento, observamos que é sim possível criar uma arquitetura, baseada num conjunto soluções em *software* gratuitos, que permita o monitoramento e até mesmo o gerenciamento remoto de uma rede, uma vez estabelecida a conexão VPN entre as redes, além do monitoramento com uso das soluções apresentadas, o administrador de rede pode realizar acesso remoto nas máquinas da rede monitorada, logo caso o monitoramento aponte a necessidade de intervenção em alguma máquina ou serviço, é perfeitamente possível que um profissional consiga atuar para sanar ou prevenir problemas maiores.

Do lado da rede cliente a ser monitorada foi necessário apenas a adição de uma máquina, neste caso um único *access point* para estabelecer a conexão com a rede de monitoramento e a instalação dos agentes, o que podemos julgar como uma intervenção pequena numa rede pré-existente, uma vez que a rede em si não foi alterada.

Neste ponto voltamos a falar da necessidade de pequenos e médios negócios ou escritórios que não atuam na área de TI e não teriam condições de sustentar uma equipe própria, mas que precisão manter sua infraestrutura de TI funcionando, pelo bem do próprio negócio. Estes poderiam se beneficiar deste modelo de monitoramento e gerenciamento remoto como serviço prestado por outra empresa.

Assim a contratante teria a sua infraestrutura de TI monitorada e gerenciada sem ter uma equipe de TI fixa, e no caso de algum incidente ou indisponibilidade dos serviços, um profissional pode atuar para resolver o problema.

Como trabalhos futuros vemos a possibilidade de testar esta arquitetura em um ambiente real, onde a rede cliente a ser monitorada esteja em produção e servindo aos objetivos da instituição contratante, e para rede de monitoramento, que seja montado um ambiente em nuvem que permita escalabilidade e facilidade de replicação do ambiente quando um novo cliente for contratado, além da adição de plataformas de Gerenciamento e Correlação de Eventos de Segurança.

AGRADECIMENTOS

Os autores agradecem ao apoio em parte pelo CNPq – Conselho Nacional de Pesquisa (Nº PQ-2 312180/2019-5 sobre Cibersegurança nº 465741/2014-2), em parte em parte pelo Conselho Administrativo de Defesa Econômica (Nº CADE 08700.000047/2019-14), em parte pela Procuradoria Geral da União (nº AGU 697.935/2019), e em parte pela Procuradoria Geral da Fazenda Nacional (nº PGFN 23106.148934/2019-67) e Fundação de Amparo à Pesquisa do Distrito Federal – FAPDF. A aplicação prática deste trabalho foi garantida pela Vitae Soluções em Engenharia que abriu sua infraestrutura e base de dados para coleta e análise dos dados apresentados neste artigo.

REFERÊNCIAS

Chou, Te-Shun; Hempenius, Nicholas. An Assessment of Practical Hands-On Lab Activities in Network Security Management. Journal of Cybersecurity Education, Research and Practice, v. 2019, n. 2, p. 2, 2020.

Paessler Ag, 2022, PRTG Network Monitor, disponível em: www.paessler.com/br/prtg, acessado em agosto de 2022.

DATADOG, 2022, Infrastructure and Application Monitoring as a Service, disponível em: www.datadoghq.com/product/ , acessado em agosto de 2022.

ZABBIX LLC, 2022, Zabbix features overwiew, disponível em: www.zabbix.com/features#data_sources , acessado em agosto de 2022.

ELASTICSEARCH B.V.. 2022, ELK Stack, disponível em: www.elastic.co/pt/what-is/elk-stack, acessado em agosto de 2022.

RUBICON Communications, LLC (Netgate), 2022, Learn About the pfSense Project, disponível em: www.pfsense.org/about-pfsense/, acessado em agosto de 2022.

EMBEDD GmbH, 2022, DD-WRT About, disponível em: https://dd-wrt.com/about/, acessado em agosto de 2022.

Commer, Douglas E., 2016. Redes de computadores e internet .Bookman, Porto Alegre, Brasil.

ORACLE, 2022, Welcome to VirtualBox.org, disponível em: www.virtualbox.org/, acessado em abril de 2022.

SOLARWINDS LLC., 2022, software GNS3, disponível em: www.gns3.com/software, acessado em abril de 2022.

Martins, R.S., Medeiros , R.M., Silva, W.M.C, 2015, Análise e Gerenciamento de Redes usando uma Metodologia Proativa com Zabbix. HOLOS. disponível em: www.redalyc.org/articulo.oa?id=481547291024, acessado em agosto de 2022.