II Encontro de Iniciação Científica e Tecnológica
II EnICT
ISSN: 2526-6772
IFSP – Câmpus Araraquara
26 e 27 de Outubro de 2017

CONCEITOS SOBRE ETHERNET, SDN NO CONTEXTO DE SEGURANÇA

GABRIEL TOMASINE[1], VICTORIA ATHANAZIO[1], VITÓRIA CLARA[1], MARCELO FRATE[2]

[1]Aluno do Curso Técnico em Redes de Computadores Integrado ao Ensino Médio, IFSP Campus Boituva
[2]Docente do Instituto Federal de São Paulo – Campus Boituva - frate@ifsp.edu.br (Orientador)

Área de conhecimento (Tabela CNPq): Arquitetura de Sistemas de Computação – 1.03.04.02-9

RESUMO: O propósito deste artigo é indicar pontos que tratam de segurança em redes tendo em vista uma concepção geral, tanto na rede Ethernet, mais utilizada atualmente, quanto em uma rede mais moderna, SDN. A rede Ethernet apresenta falhas em sua segurança e elas acarretaram na criação da rede SDN, que surgiu na intenção de resolver algumas das falhas da rede atual. O atual artigo conta com uma introdução a ambas as redes, além de dar uma breve ênfase às suas seguranças. Contudo, o artigo não tem em vista concluir, favorecendo uma rede, mas esclarecer os profissionais e/ou pessoas da área, a diferença entre elas, a fim de ponderar se vale a migração, com segurança, para a nova rede.

PALAVRAS-CHAVE divulgação; segurança; redes de computadores; tipos de redes

INTRODUÇÃO

As Redes Definidas por Software, SDN, vêm crescendo em escala potencial nos últimos anos, muitas empresas estão aderindo ao novo modelo de rede. Dentre os muitos motivos e melhorias que as redes SDN oferecem, um dos principais é a possibilidade de aceleração de implantação e distribuição de aplicativos, reduzindo gastos com TI (Tecnologia da Informação) (SANTOS, 2015). Além disso, a tecnologia SDN habilita arquiteturas em nuvem, possibilitando o compartilhamento de aplicativos e serviços em uma velocidade e escala nunca alcançada com redes Ethernet. Outro ponto que merece reconhecimento é que as redes SDN possibilitam que os administradores de Data Centers (DC) virtualizem toda a sua infraestrutura física, podendo, assim, flexibilizar e agilizar configurações e aplicações de serviços em toda a sua rede, com maior agilidade e segurança. Entretanto, empresas ainda estão em transição para essa nova rede. O objetivo principal deste artigo é de esclarecer como são as duas redes, em termos gerais, e não favorecer nenhuma delas, pois também serão descrito alguns dos seus pontos fracos e fortes de ambas.

REDE ETHERNET

Ethernet é um sistema de comunicação que utiliza da transmissão por ramificação, podendo encaminhar pacotes entre estações computacionais localmente distribuídas. O meio utilizado para o transporte dos pacotes, que é fornecido pela Ethernet, tem sido utilizado para a construção de sistemas que podem ser interpretados como redes locais ou, meramente, como multiprocessadores acoplados. Uma facilidade de comunicação compartilhada na rede Ethernet é a Ether, que é um meio de transmissão passivo sem a necessidade de um centro de controle. A logística de acesso ao Ether para a transmissão de datagramas é distribuída entre as estações transmissoras, que utilizam de uma arbitragem estatística controlada. Ainda dentro de Ether, no momento da entrega dos pacotes ao seu destino, a rede transmite o endereçamento do datagramas, e a estação correspondente ao endereço irá receber o frame (packet). (METCALFE, 1976)

Definição de Segurança em Redes

Segurança de Rede é quando o usuário deseja enviar ou receber mensagens ou arquivos com segurança, sem que haja intrusos interceptando a comunicação. Diante disso podemos encontrar cinco formas de comunicação segura: Confidencialidade, Integridade, Autenticação, Não-Repúdio e, por último, Identificação de Entidade. (KUROSE, 2010)

Confidencialidade é quando apenas o destinatário e o remetente são capazes de entender o assunto enviado. Integridade é uma forma de envio em que a mensagem, o seu conteúdo, será integralmente encaminhada ao destinatário, sem que seja modificada em seu percurso. Autenticação é quando o destinatário e o receptor devem confirmar sua identidade para ter certeza que nada foi alterado no caminho. Não-Repúdio refere-se ao fato de o emissor não poder rejeitar uma mensagem, que ele mesmo encaminhou, por isso, deve haver confirmação para que o envio seja realizado. E, por último, Identificação de Entidade é quando o usuário precisa confirmar a identidade através de senhas e logins.

Um intruso pode obter acesso às informações do usuário através de monitoramento e modificação. Monitoramento é quando o intruso identifica e guarda os conteúdos da mensagem e modificação pode se tratar de mudanças no conteúdo da mensagem durante seu percurso de encaminhamento.

REDES SDN

As redes SDN (Redes definidas por software) vêm recebendo um grande aumento e reconhecimento nos últimos anos, e, com isso, diversas empresas estão transitando suas redes para esse novo modelo. Contudo, ainda há muitas perguntas sobre essa nova rede, e se a mesma vale a transição. É visível que, nos últimos anos, as redes atuais tornaram-se bem menos flexíveis e não atendem a requisitos recentes e apresentam novas demandas tais como: o crescimento das tabelas de roteamento, a complexidade de operações de protocolos diversificados, o suporte á mobilidade dos usuários, a implementação de recursos de segurança entre outros. Com isso, a comunidade acadêmica desenvolveu as redes SDN, as quais vêm como iniciativa para programar uma infraestrutura de maiores recursos na rede. (MARTINS; CAMPOS, 2015)

As redes SDN têm como base controladores, com protocolo Openflow, que permitem que o usuário centralize suas tarefas em uma só tela e, assim, possam controlar a rede inteira. Entretanto, as redes SDN, ainda que novas e bastante atrativas por muitos motivos, trazem limitações quanto a sua segurança, como, por exemplo, um componente malicioso dentro da rede pode comprometer o funcionamento de toda ela. Essas redes trazem algumas vulnerabilidades decorrentes das antigas redes, tais como: natureza centralizada do plano de controle, antivírus e firewalls não são suficientes para garantir a segurança da rede, e com isso, arquiteturas e mecanismos de autenticação têm de ser criados para assegurar melhor essas redes.

Esses problemas que vêm das redes legadas para as SDN, são problemas que originam outros novos exclusivos desse domínio (MARTINS; CAMPOS, 2015), fazendo com que as mesmas características atrativas dessa rede a tornem alvo de ataques, pois, quando dentro de uma rede, comprometer o controlador, ou ter o acesso do mesmo, compromete toda a rede. Contudo, para resolver alguns problemas dessa nova rede, arquiteturas e dispositivos de redes podem ser implementados, para que deste modo, seja mais difícil infectar a rede, ou principalmente, o controlador. (SANTOS, 2015)

CONCLUSÕES

Dentre todas as redes já desenvolvidas, é inegável que quase todas receberam e ainda recebem atualizações e melhorias com o tempo, e quando se trata de redes Ethernet e SDN, a história não é diferente. A rede Ethernet já recebeu inúmeros novos protocolos com o objetivo de solucionar problemas e

evitar quebras de segurança. E mesmo a rede SDN, sendo mais nova, a regra também se aplica a ela, que recebe melhorias constantes e cada dia mais usuários aderem a essa rede. Em suma, não há uma rede melhor ou pior, porém, vale ressaltar que, por a rede SDN ser mais nova e estar crescendo no mercado, a tendência é que a atenção e dedicação dos desenvolvedores de softwares de segurança se voltem a ela, seja por ser mais eficiente em alguns aspectos, ou por se mostrar um modelo que promete grandes avanços dentro da área de Tecnologia da Informação.

REFERÊNCIAS

KUROSE, James F.. **Redes de Computadores e a Internet:** Uma Abordagem Top-Down. 5. ed. São Paulo: Pearson, 2010. 614 p.

MARTINS, Joberto; CAMPOS, Maxli Barroso. **Uma Proposta de Arquitetura de Segurança para a Detecção e Reação a Ameaças em Redes SDN.** 2015. 14 f. Monografia (Especialização) - Curso de Programa de Pós-graduação em Sistemas e Computação, Universidade Salvador, Salvador, BA, 2015. Disponível em: <https://www.researchgate.net/profile/Joberto_Martins/publication/308735494_Uma_Proposta_de_Arquitetura_de_Seguranca_para_a_Deteccao_e_Reacao_a_Ameacas_em_Redes_SDN/links/5835863f08ae138f1c113ff1.pdf>. Acesso em: 13 mai. 2017.

METCALFE, Robert M.; BOGGS David R. Ethernet: distributed packet switching for local computer networks. Commun. ACM 19, 7 jul. 1976.Disponivel em: < http://dx.doi.org/10.1145/360248.360253. >

SANTOS, Alexsanderson Vieira. **Uma solução SDN para comunicação Mesh de Nós em uma rede Zigbee padrão 802.15.4.** 2015. 57 f. TCC (Graduação) - Curso de Tecnólogo em Redes de Computadores, Universidade Federal do Ceará, Quixadá, 2015. Disponível em: <http://www.repositoriobib.ufc.br/00001d/00001ddc.pdf> Acesso em: 24 mai. 2017.