Implementação do Padrão IEEE 802.1x na Rede de Dados da UnB

Alex A. Dantas Fidelis[1], **David Santos Abreu**[1]

[1]Centro de Informática – Universidade de Brasília (CPD/UnB)
Campus Universitário Darcy Ribeiro – Brasília – DF – Brazil – CEP 70910-900

alekez@unb.br, davidabreu@unb.br

Resumo. *O não repúdio ou irretratabilidade é um atributo essencial para assegurar a segurança de sistemas de informação. Esta propriedade diz que nenhum ente pode negar qualquer procedimento que tenha realizado relacionado à informação, seja qual for o tamanho do ato. Com a aprovação do Marco Civil da Internet (Lei Nº 12.965/14) no primeiro semestre de 2014, ficou evidenciado a importância do monitoramento e guarda das informações dos usuários das redes de computadores. Na Universidade de Brasília – UnB há um controle rigoroso sobre as atividades da rede sem fio, porém, este mesmo controle ainda não existe na rede cabeada. O trabalho a seguir apresenta os trabalhos realizados para implementar o padrão IEEE 802.1x na rede cabeada desta Instituição.*

1. Introdução

No ano de 2014, após um grande apelo de várias vertentes da sociedade, foi aprovada a Lei Nº 12.965/14 mais conhecida como Marco Civil da Internet. Entre a sua previsão de princípios, garantias, direitos e deveres no seu décimo terceiro artigo – no que tange à guarda de registros de conexão – há o seguinte texto: "Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento." [Presidência da República, 2014]. Isso ilustra a preocupação dos legisladores em atribuir a responsabilização dos usuários de rede pelos seus atos e, consequentemente, o aumento do controle de acesso pelos administradores de redes. Na UnB essa é uma preocupação constante dos seus gestores.

A UnB em virtude do seu alcance, tamanho e forma de trabalho, não consegue impor proteção física a todos os seus pontos de rede deixando-os expostos – em alguns casos – para possíveis usos maliciosos. Este é um dos argumentos para que já no ano de 2018 ainda estejamos utilizando atribuição de endereços IP manualmente nas nossas estações de trabalho. Mas com a constante pressão da Administração Pública Federal – APF para a iniciação do protocolo IPv6 nos seus entes – em fase inicial de implementação na UnB – vimos que com a utilização dos protocolos IPv4 e IPv6 simultaneamente (técnica de pilha dupla - [IPv6.br, 2012]) ficará inviável a atribuição manual dos IPs. Será necessária a utilização de DHCP (do Inglês, *Dynamic Host Configuration Protocol*) para atribuição automática dos endereçamentos. Para não incorrer nas atividades maliciosas provenientes de pontos de rede desprotegidos fornecendo IP automaticamente, foi pensado pela Administração e Suporte de Redes do Centro de Informática da UnB – ASR/CPD/UnB a utilização do padrão lançado pela IEEE (do Inglês, *Institute of Electrical and Electronics Engineers*) para controle de acesso à rede baseado em portas e políticas. Este padrão foi enumerado/nomeado como 802.1x [IEEE, 2010].

Considerado um mecanismo de controle de acesso a rede baseado em portas, o padrão IEEE 802.1x é usado para prover o controle de acesso a uma LAN, levando em consideração normas para autenticação dos dispositivos buscando autorização para se conectar à rede interna, podendo ser empregado em redes cabeadas ou sem fio. É, basicamente, composto de três elementos, sendo eles o Suplicante (*host* do usuário), Autenticador (*switch* ou *Access Point*) e Servidor de Autenticação (RADIUS) [IEEE, 2010].

Este trabalho irá apresentar os esforços da ASR/CPD em implementar o padrão IEEE 802.1x na infraestrutura de rede com fio da UnB.

2. Métodos

Embora tenhamos um ambiente de rede bastante heterogêneo, os comutadores de dados Rede de Dados da UnB – REDUnB contribuem para execução deste trabalho. De um total de 901 (novecentos e um) *switches* em produção 94% são da fabricante Enterasys/Extreme o que facilita a integração dos serviços. As fabricantes restantes utilizadas são D-Link, Dell, HP e Cisco, e todas suportam o padrão.

Nos métodos utilizados dois cenários foram considerados. O primeiro foi com os computadores que fazem parte do *Active Directory* – AD. Já o segundo cenário levou em consideração as estações de trabalho que não estão no AD.

O diagrama de rede utilizado no ambiente institucional é caracterizado pela divisão em camadas, possuindo ativos de núcleo, agregação e acesso. A interligação entre os núcleos é feita com a topologia *full-mesh* e o roteamento OSPF –(do Inglês, *Open Shortest Path First*) – dividindo o ambiente em áreas. A camada de agregação possui *switches* que são os responsáveis pela criação das redes para o usuário final, além de remetê-las via OSPF para a camada de núcleo. A camada de acesso faz a ligação entre o usuário final e a rede institucional.

O primeiro passo para a implementação do padrão IEEE 802.1x no escopo da UnB foi entender como ele seria integrado neste ambiente diferenciado. Para isso, elencaram-se desafios e objetivos. O principal desafio era a fidelidade das bases de usuários, do LDAP (do Inglês, *Lightweight Directory Access Protocol*) – e do AD. Os objetivos relacionados a este desafio foram: separação entre alunos e servidores, criação de um único LDAP integrado, melhor definição dos grupos das bases e atualização dos usuários. A fidelidade da base é essencial, pois a aplicação do serviço é feita baseada em respostas do servidor de autenticação para o autenticador. Em um local onde existe uma grande rotatividade de servidores, caso a base não seja atualizada continuamente, a aplicação atribuirá uma rede diferente, com outras políticas de acesso e em outro endereçamento, para o usuário final.

A simples conexão de um cabo de rede em um ponto de rede, normalmente introduz o usuário em um ambiente no qual ele terá acesso à internet. Com a aplicação do IEEE 802.1x, não se tem mais essa insegurança, pois é necessário algo que somente o usuário autorizado possui, as credenciais de acesso. No momento em que o usuário interliga um cabo de rede, o autenticador, que neste caso é o *switch*, coloca a porta em modo restrito, no qual somente o protocolo EAP (do Inglês, *Extensible Authentication Protocol*) fica disponível, impedindo varreduras e acesso não-autorizado à rede. Caso o dispositivo do usuário esteja devidamente configurado, será exibida uma tela solicitando

as credenciais de acesso. Elas serão remetidas ao servidor de autenticação, este informará ao autenticador com uma mensagem de aceite ou rejeição. Com base na resposta, o autenticador fará ou não a liberação da porta para o usuário.

A solicitação feita era de que usuários pudessem transitar dentro da UnB e tivessem acesso à rede sem precisar configurar a máquina para cada conexão diferente. Como as máquinas que acessam a rede da universidade vem de diversas fontes e com diversos sistemas operacionais, nem todas poderão fazer parte do AD institucional, devido a isso deve-se consultar duas bases de usuários. Além disso, foi necessário criar vários procedimentos diferentes para o acesso à rede, dois para usuários oriundos do AD e outros para usuários que não estejam no AD ou possuam sistemas operacionais diferentes.

No caso da UnB, a equipe do SRS decidiu usar o serviço de alocação dinâmica de VLAN (do Inglês, *Virtual Local Area Network*) por meio de políticas criadas nos *switches* de agregação e acesso, aplicadas por meio da resposta do servidor RADIUS. No ambiente é utilizado o *FreeRadius* e o local onde fica a configuração importante para o IEEE 802.1x é o arquivo *inner-tunnel*, no qual foram feitas alterações no tocante ao *Auth-Type* EAP que após a autenticação, se o usuário pertencer a determinada unidade organizacional do AD ou a algum grupo do LDAP, deve-se atualizar a resposta por meio de um *update-reply*, com o *Filter-Id := "policy=nome da unidade ou grupo"* – , no qual a política (em Inglês, *policy*) – terá o mesmo nome no *switch* autenticador. No autenticador, a política criada está ligada a uma VLAN que será aplicada na porta assim que receber o *Filter-Id* do RADIUS. No tocante aos usuários visitantes, existe uma consulta à eduroam [Eduroam, 2013], que caso o usuário faça parte, o RADIUS enviará uma política com o nome eduroam e o *switch* aplicará na porta a VLAN relativa a rede de visitantes e fornecerá acesso restrito somente às portas de comunicação 80, 443 e 8080.

2.1. Computadores no AD

Após algumas tentativas, dois procedimentos foram elencados, um por meio de GPO (do Inglês, *Group Policy*) e a outra via foi a utilização de um arquivo Batch (extensão .bat). Nos dois, o procedimento consiste em ativar o serviço "dot3svc" do Windows e exigir que o serviço inicie sempre. Além disso, um perfil de interface de rede é aplicado com as configurações necessárias.

As alterações necessárias na interface de rede foram a de escolha de método de autenticação como PEAP (do Inglês, *Protected Extensible Authentication Protocol*), método de autenticação como EAP-MSCHAPv2, usar credenciais de domínio, modo de autenticação como sendo de usuário e autenticação antes do logon no AD.

Ao longo dos testes, foi verificado que no momento em que a janela de autenticação era exibida após o usuário já logado na máquina, ao inserir as credenciais, o servidor de autenticação recebia a combinação "usuário:senha" e repassava para a base de usuários do AD. O problema era, caso o usuário não tivesse o perfil criado na máquina, ele não teria como se conectar ao AD, pois o *switch* limitaria a comunicação para somente o protocolo EAP. A solução era que a autenticação EAP fosse feita antes do AD, mas com as mesmas credenciais. Contudo, ao habilitar essa opção, as credenciais que chegavam no RADIUS eram ligeiramente diferentes, pois a combinação chegava "domínio\usuário:senha". Foi preciso criar uma regra no RADIUS para que toda vez que chegasse a combinação "domínio\usuário:senha" fosse retirada a parte "domínio\", para

que então a autenticação pudesse ser feita.

2.2. Computadores fora do AD

Dentre os usuários fora do domínio institucional, os procedimentos adotados na configuração são diferentes para cada sistema operacional. Os usuários de macOS atualizados não precisam executar nenhuma configuração, basta inserir o cabo de rede e esperar a janela de autenticação. Os usuários de Windows precisam adotar procedimentos diferentes para cada versão. Os usuários de distribuições Linux precisam somente ativar o serviço dentro das opções avançadas da interface de rede. Os procedimentos com as versões dos sistemas operacionais mais utilizadas estão disponíveis para o público da UnB, por meio de um guia com imagens do passo a passo.

Devido a esses usuários, consultas a duas outras bases tiveram que ser inseridas nas requisições, a base LDAP e a eduroam. Quanto ao LDAP, as consultas são feitas baseadas nos grupos que os usuários pertencem. Um usuário do grupo A receberá a rede definida para o grupo A e terá acesso customizado. Um usuário do grupo B receberá a rede definida para o grupo B. Existem casos em que vários grupos pertencem à mesma rede, neste caso basta definir no *inner-tunnel* do RADIUS para enviar um *Filter-Id* único para todos esses grupos, pois dentro do *switch* todos eles serão redirecionados para uma política que aplicará a configuração.

3. Resultados

Todo o processo de autenticação e distribuição de endereço é redirecionado para um servidor de registros. Na configuração dos *switches*, toda vez que uma política é aplicada em alguma porta, ele registra um log no servidor, guardando o endereço físico do dispositivo autenticado, além da data e do horário. No servidor RADIUS, toda tentativa de autenticação registra um log, salvando as informações do usuário, do endereço físico do dispositivo, da data e do horário. No servidor DHCP, toda atribuição de endereço é registrada, salvando o endereço atribuído, o endereço físico do dispositivo, a data e o horário. Hoje, o processo de cruzamento das informações ainda não está totalmente integrado, tendo que verificar os três registros para poder identificar exatamente o local, horário, data, usuário e o endereço atribuído. Medidas estão sendo tomadas a fim de facilitar o cruzamento dos dados e gerar informações importantes.

Testes estão sendo realizados na ASR (com AD) e no Módulo 14 do ICC – Instituto Central de Ciências (sem AD), ambos com endereçamentos atribuídos por DHCP. Nos dois casos, a navegabilidade dos dispositivos não foi afetada. O único caso preocupante são com as estações com Windows. São necessários 16 (dezesseis) passos para habilitar o serviço do 802.1x em algumas versões. Para isso foi criado um arquivo .bat para mecanizar e diminuir o tempo para aplicação das configurações.

Nos testes de acesso simulando ´´força bruta", foi constatado que o padrão – realmente – impede qualquer acesso de usuários que não tenham credenciais válidas. Em capturas de pacotes realizadas em portas de *switches* foi constatado que apenas os pacotes EAPoL (do Inglês, *EAP over LAN*) ficam trafegando naquele ambiente.

4. Conclusão

Após vários testes em diversos e diferentes modelos de *switches*, ficou constatado que a utilização do padrão IEEE 802.1x na REDUnB é bastante viável e que sua utilização trará

bastantes ganhos para a Instituição.

Os próximos passos são o refinamento do tratamento dos logs para que sejam concentrados em uma única base e mais facilmente interpretados (concentrá-los em um catalogador de logs como o graylog, por exemplo); e criação de um plano de implantação para toda a Universidade visando o menor impacto possível aos usuários finais dos serviços e disponibilizar a atribuição de endereçamentos IP via o protocolo DHCP.

Em breve estaremos aptos à responder por quaisquer solicitações de identificação de utilizadores dos IPs da Universidade de Brasília.

Referências

Presidência da República. LEI Nº 12.965, DE 23 DE ABRIL DE 2014. Acesso em 9 de abril de 2018, 2014. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

IPv6.br. Transição. Acesso em 13 de abril de 2018, 2012. http://ipv6.br/post/transicao/.

IEEE. IEEE 802.1X-2010 - IEEE Standard for Local and metropolitan area networks– Port-Based Network Access Control. Acesso em 14 de abril de 2018, 2010. https://standards.ieee.org/findstds/standard/802.1X-2010.html.

Eduroam. Eduroam. Acesso em 13 de abril de 2018, 2013. https://www.rnp.br/servicos/servicos-avancados/eduroam.