Projeto de redes Padrão IEEE 802

Definições A IEEE 802.1X é um protocolo padrão IEEE para controle de acesso de redes com base em portas (PNAC). Ele faz parte do grupo de protocolos de rede 802.1. Além disso, ele prevê mecanismos de autenticação para dispositivos que desejam se anexar a uma LAN ou WLAN. A IEEE 802.1X define o encapsulamento do Extensible Authentication Protocol (EAP) sobre IEEE 802, que é conhecido como "EAP over LAN" ou EAPOL. Qualquer computador que se conecta à rede deve primeiro fornecer informações de autenticação antes de ser permitido na rede. A autenticação IEEE 802.1X disponibiliza um bloqueio adicional para a intranet, podendo ser utilizada para evitar que máquinas convidadas, invasores ou dispositivos não gerenciados que não executam uma autenticação bem-sucedida conectem-se à intranet da sua empresa. Características O padrão IEEE 802.1X define um protocolo cliente e um controle de acesso baseado em autenticação de servidor que restringe os clientes não autorizados de se conectarem a uma rede local por meio de portas de acesso público. O servidor de autenticação autentica cada cliente conectado a uma porta do switch e atribui a porta a uma VLAN antes de disponibilizar todos os serviços oferecidos pelo switch ou LAN. Até que o cliente esteja autenticado, o controle de acesso 802.1X permite apenas o tráfego do Protocolo de autenticação extensível sobre LAN (EAPOL) através da porta a qual o cliente está conectado. Depois do sucesso da autenticação, o tráfego normal também pode passar pela porta. São utilizados 3 termos no padrão 802.1x: 1º – Suplicante: É o usuário ou cliente que quer ser autenticado; 2º – Servidor de autenticação: Geralmente é um servidor RADIUS o responsável por essa função; 3º – Autenticador: É o dispositivo entre eles, tal como switch ou AP (Access Point) para redes sem fio. A maioria das empresas querem fazer mais pela segurança do que simplesmente empregar nomes de usuários e senhas de acesso, de modo que um novo protocolo de autenticação, chamado Extensible Authentication Protocol (EAP), foi projetado. O EAP fica dentro do protocolo de autenticação PPP e fornece uma estrutura geral para vários métodos de autenticação diferentes. Supostamente, ele deve dirigir os sistemas de autenticação proprietários e permitir que senhas de tokens e certificados de chaves públicas de infraestrutura trabalhem sem problemas. Com uma EAP padronizada, a interoperabilidade e compatibilidade dos métodos de autenticação se torna mais simples. Por exemplo, quando você discar para um servidor de acesso remoto e usar EAP como parte de sua conexão PPP (Point-to-Point Protocol), o serviço de acesso remoto (RAS) não precisa saber quaisquer detalhes sobre seu sistema de autenticação. Somente você e o servidor de autenticação têm que estar coordenados. Ao apoiar a autenticação EAP, um servidor RAS sai do negócio de agir como homem médio, e apenas pacotes e reformula pacotes EAP para entregar a um servidor RADIUS que fará a autenticação real. Isso nos leva ao padrão IEEE 802.1X, que é simplesmente um padrão para a passagem de EAP através de uma LAN com fio ou sem fio. Com 802.1X, você empacota mensagens EAP em quadros Ethernet e não usa PPP. Existe duas formas de autenticação principais que podem ser usadas para autenticar o equipamento, PEAP (senhas) ou EAP-TLS (certificados digitais). PEAP normalmente usa a senha da conta de máquina do sistema no Active Directory, que é mantida pelo próprio Windows e que torna todo o processo de autenticação transparente. EAP-TLS (Transport Layer Security) fornece para autenticação mútua e baseada em certificado do cliente e a rede. Ela se baseia no lado do cliente e no lado do servidor certificados para fazer a autenticação e pode ser usado para gerar dinamicamente com base em usuários e baseada em sessão códigos WEP para garantir a comunicação subsequentes entre o cliente de rede local sem fio e o ponto de acesso. Normalmente essa autenticação 802.1X é usada como uma forma de segurança avançada para redes com fio, mas estão cada vez mais buscando implementar o padrão IEEE 802.1X como uma forma de proteger suas conexões de rede sem fio. Isso porque da mesma forma que um cliente de rede com fio autenticado deve enviar algumas credenciais para serem validadas antes de poder enviar quadros pela intranet de Ethernet com fio, um cliente de uma rede wireless IEEE 802.1X também precisa executar a autenticação antes de poder enviar pacotes de dados pela sua porta do ponto de acesso (AP) sem fio e através da rede. Tanto os padrões WPA quanto WPA2 utilizam 802.1x para fazer controle de acesso, e a literatura sobre a implementação de 802.1x em ambientes sem fio é

fartíssima, seja usando senhas ou certificados digitais. O WPA utiliza o algoritmo RC4, o mesmo sistema de encriptação utilizado no WEB: o TKIP (Temporal Key Integrity Protocol). O WPA2 se baseia na criptografia AES (Advanced Encryption Standard), que é mais segura que a TKIP, mas exige mais processamento e algumas placas mais antigas não suportam o WPA2 nem mesmo atualizado a firmware. WPA-PSK é uma criptografia forte em que as chaves de criptografia (TKIP) são frequentemente mudadas o que garante mais segurança protegendo de ataque hack, muito utilizado por usuários domésticos. WPA2-PSK e ainda mais seguro que o WPA-PSK onde sua criptografia (AES) é extremamente forte e resistente a ataques, adotado como padrão de criptografia do governo americano. Contudo, o modo de chave pré-partilhada (PSK ou Pre-Shared Key) do WPA ou do WPA2 não é seguro para ambientes empresariais. Quando se usa este modo, a mesma chave tem de ser inserida em cada dispositivo cliente. Assim, este modelo obriga à mudança de chave de cada vez que um funcionário sai ou quando um dispositivo é roubado ou perdido – situação impraticável na maioria dos ambientes. Fontes:
https://king.host/blog/2012/05/autenticacao-802-1x-para-seguranca-em-redes-wifi/
http://www.sj.ifsc.edu.br/~msobral/RCO2/slides/aula12.pdf
https://blogs.technet.microsoft.com/fcima/2006/10/30/o-que-voc-precisa-saber-antes-deimplementar-802-1x-em-redes-com-fio/ http://blog.ccna.com.br/2009/02/25/pr-o-que-e-8021x/
http://www.repositorio.uniceub.br/bitstream/123456789/3273/2/20115379.pdf
http://187.7.106.14/wiki2011/lib/exe/fetch.php?media=projeto11:artigo_rafael_c._marques_certo.pdf

FreeRadius

FreeRADIUS é a mais popular e o mais amplo servidor de RADIUS em código livre do mundo. FreeRADIUS provê autenticação, autorização e contabilidade (accounting) para muitas das empresas da Fortune 500, esse padrão é conhecido como AAA. FreeRADIUS é utilizado no mundo acadêmico, em instituições de pesquisa e educacionais. Criado a partir de 1999 por Alan DeKok e Miquel Van Smoorendburg, possui um desenho modular que encoraja o desenvolvimento comunitário de extensões.

FreeRADIUS é o servidor (em software livre) que suporta o maior número de tipos de autenticação e, atualmente, é o único servidor RADIUS de código livre que suporta o protocolo EAP - Extensible Authentication Protocol. Além disto, FreeRADIUS é o único que suporta virtualização, mantendo os custos de implantação e manutenção baixos. Seu desenho modular é fácil de entender, permitindo facilmente a inclusão ou remoção de módulos sem contudo afetar o desempenho, os requisitos de hardware, de memória ou a segurança do sistema. A modularidade permite executar FreeRADIUS em sistemas embarcados ou em servidores com vários núcleos e com gigabytes de memória RAM.

Benefícios do RADIUS

O protocolo RADIUS possui as seguintes vantagens:

- Solução em código aberto, padronizada e escalonável.
- Amplo suporte fornecido por uma variedade de implementações.
- Fácil modificação das configurações.
- Separação entre os processos de segurança e de comunicação.
- Adaptabilidade aos variados sistemas de segurança e autenticação existentes.

- Amplamente funcional com variados dispositivos que implementam o cliente.

A arquitetura cliente-servidor de RADIUS provê uma solução aberta, escalonável e suportada por uma base ampla de fornecedores de equipamentos. O consumidor pode modificar os servidores de autenticação para funcionar com um amplo número de sistemas de segurança atualmente disponíveis no mercado. Provedores de Internet tem utilizado RADIUS para criar serviços de VPN - Virtual Private Network - e, neste contexto, aumentar a segurança de sua infraestrutura.
A natureza distribuída de RADIUS (cliente-servidor) permite separar processos de segurança (autenticação) de processos de comunicação (pool de modems ou NAS - Network Access Server). O servidor RADIUS centraliza os processos de autenticação e autorização.

A arquitetura cliente-servidor de RADIUS provê uma solução aberta, escalonável e suportada por uma base ampla de fornecedores de equipamentos. O consumidor pode modificar os servidores de autenticação para funcionar com um amplo número de sistemas de segurança atualmente disponíveis no mercado. Provedores de Internet tem utilizado RADIUS para criar serviços de VPN - Virtual Private Network - e, neste contexto, aumentar a segurança de sua infraestrutura.
A natureza distribuída de RADIUS (cliente-servidor) permite separar processos de segurança (autenticação) de processos de comunicação (pool de modems ou NAS - Network Access Server). O servidor RADIUS centraliza os processos de autenticação e autorização.

FreeRADIUS

Ele é o mais popular e o mais amplo servidor de RADIUS em código livre do mundo. FreeRADIUS provê autenticação, autorização e contabilidade (accounting) para muitas das empresas da Fortune 500, esse padrão é conhecido como AAA. FreeRADIUS é utilizado no mundo acadêmico, em instituições de pesquisa e educacionais. Criado a partir de 1999 por Alan DeKok e Miquel Van Smoorendburg, possui um desenho modular que encoraja o desenvolvimento comunitário de módulos e extensões.
FreeRADIUS é o servidor (em software livre) que suporta o maior número de tipos de autenticação, e atualmente é o único servidor RADIUS open source que suporta EAP - Extensible Authentication Protocol. Além disto, é o único que suporta virtualização mantendo os custos de implantação e manutenção baixos. Seu desenho modular é fácil de entender, permitindo facilmente a inclusão ou remoção de módulos. A remoção ou inclusão não afetam o desempenho, os requisitos de hardware ou memória ou de segurança. Isso permite executar FreeRADIUS em sistemas embarcados ou em servidores com vários núcleos e com gigabytes de memória RAM.

Usabilidade

AAA é a sigla para autenticação, autorização e contabilidade (accounting). O padrão AAA define uma arquitetura que autentica e garante privilégios de autorização para os usuários além de, opcionalmente, manter precisos registros sobre sua atividade na rede (contabilidade de uso).

Quando os conceitos AAA não são utilizados, dizemos que a rede é aberta. Assim, qualquer um pode obter acesso ou fazer qualquer coisa sem ser rastreado. AAA é um sistema muito amplo, entretanto é possível implementar porções de um sistema AAA melhorando a segurança da rede.

Podemos nos ater em autenticação e autorização desprezando os recursos de rastreamento e contabilidade onde não são necessários. Sem AAA, o administrador deverá configurar a rede manualmente e de modo estático. Em sistemas pequenos isso pode até ser funcionalmente viável. Mas, comercialmente em ambiente empresarial isso é totalmente inviável.

Os serviços móveis foram responsáveis pela grande demanda de servidos de segurança e autenticação no padrão AAA nos últimos tempos. RADIUS possui um grande número de protocolos para autenticação, autorização e contabilidade.

Definições de AAA

Autenticação - É o processo que valida a identidade de um usuário combinando as credenciais fornecidas por ele (nome e senha) com os valores configurados no servidor AAA. Quando as credenciais combinam, o usuário é autenticado e obtém acesso a rede. Caso contrário, o acesso é negado e o usuário desconectado. Autenticação pode ser configurada para ser um processo seletivo baseado em características personalizadas de uso, de origem e principalmente em políticas de segurança.

Autorização - É o processo que determina quais permissões são garantidas para um usuário. Autorização pode permitir ou negar acesso a certas áreas da rede, a certos comandos ou recursos. O NAS envia uma requisição como um pacote de informações sobre o usuário, ao servidor RADIUS cabe garantir ou negar recursos baseado na comparação da solicitação com seus registros e políticas.

O servidor RADIUS possuí a política de autorização e cabe ao NAS impor essa política ao usuário final, por exemplo, o NAS envia para RADIUS uma requisição do usuário BOB, cuja senha é HelloWorld e o IP informado é 192.168.0.54. O servidor RADIUS compara essas informações com sua base de dados de usuários e informa ao NAS que o IP correto para BOB deveria ser 192.168.1.78. Observe que o servidor RADIUS nunca requisita informações diretamente da NAS. RADIUS é limitado a consultas SQL simples. RADIUS faz declarações sobre registros dizendo coisas do tipo "como algo é" ou sobre "como algo deveria ser". Cabe ao NAS impor essas condições e políticas aos clientes finais. Se o cliente não puder atender essas condições ele deve ser imediatamente desconectado da NAS.

Autenticação e Autorização

A seguinte analogia ilustra a diferença entre autenticação e autorização:
Imagine que está dirigindo um carro por uma estrada e é parado por um policial. O oficial pede que você se identifique. Você pode apresentar uma identidade, um passaporte, uma carteira de motorista ou outro documento oficial que "autentica" quem é você. Agora, o policial pede sua licença de motorista. Neste caso, somente a licença de motorista deve ser apresentada. A licença de motorista deve ser original, dentro da validade e adequada ao tipo de veículo conduzido. Essa licença "autoriza" você a conduzir esse veículo.
Assim a autorização deve estar de acordo com a política do servidor RADIUS. Informações adicionais, como o endereço MAC, podem ser automaticamente adicionadas pelo NAS na requisição para reforçar a qualidade do processo de decisão.

Contabilidade (Accounting) - É o processo que se refere a gravação de registros sobre como o usuário utilizou recursos autorizados. Informações como o tempo de uso, a quantidade de dados enviada e recebida são armazenadas para fins de cobrança ou limitações de uso e controle. Corporações podem usar contabilidade internamente para controlar acesso por horário ou por questões de segurança e auditoria. As corporações não cobram de seus funcionários pelo uso da rede (não dê essa ideia!). Informações como quais os sítios visitados, os protocolos utilizados (HTTP ou SMTP) são armazenadas na NAS e não interessam para RADIUS. Informações detalhadas sobre as atividades do usuário são obtidas por outros protocolos como sFlow ou NetFlow. Esses protocolos são independentes e não são integrados aos sistemas RADIUS.

Auditoria - É o processo de análise proativa dos registros da contabilidade e de outros metadados (sFlow ou NetFlow) buscando relacionar o usuário com suas atividades na rede. Auditoria busca analisar o comportamento após a autenticação e adequar o uso a política visando evitar comportamentos inadequados. Auditoria também pode ser utilizada para checar a segurança da NAS e saber se ela foi comprometida. Auditoria combate violações intencionais da política de segurança.

O processo de uma sessão RADIUS

Uma sessão consiste dos seguintes passos:

1. Um usuário remoto conecta a um cliente RADIUS (o NAS) usando um dos protocolos com PPP, 802.1x ou qualquer outro protocolo de link de dados e inicia um login. O NAS inicia a conversação para autenticação com RADIUS.
   As informações enviadas são a critério do NAS (cliente).
   O servidor RADIUS não controla o que NAS envia.

2. O NAS se comunica com o servidor RADIUS usando um mecanismo secreto compartilhado, através de pacotes UDP, na porta UDP/1812 para autenticação e na porta UDP/1813 para contabilidade.

3. O NAS envia para o servidor RADIUS uma mensagem (Access-Request).
   Essa mensagem contém informações sobre o usuário, o username, credenciais de autenticação e serviços requisitados.
   Em adição, a mensagem pode conter informações sobre o NAS, como o seu hostname, endereço MAC ou SSID wireless.
   A mensagem é enviada usando um protocolo de autenticação de senhas como PAP, um desafio-resposta como CHAP ou um protocolo estendido de autenticação como EAP. O servidor deve definir se para autenticar ou autorizar irá se basear somente nas informações recebidas do NAS. Se o NAS enviar um pacote com um protocolo que o servidor RADIUS não suporta, ele deve descartar a requisição.

4. O servidor RADIUS processa a requisição e verifica a solicitação de login contra bases de dados locais ou contra um servidor de autenticação na rede. Serviços de autenticação podem incluir servidores LDAP para validação do domínio, Active Directory em redes Windows, servidores de Kerberos, servidores SQL de qualquer tipo.

5. O servidor RADIUS envia a validação de volta ao NAS nos seguintes formatos: Access Reject, Access Challenge ou Access Accept.
   Access Reject tranca o usuário fora da rede tornando-o um usuário inválido ou não autorizado, o acesso aos recursos solicitados é negado.
   Access Challenge ocorre quando o servidor requer informações adicionais do usuário. Uma vez que os pacotes RADIUS são limitados em questões de tamanho podem ocorrer várias dessas trocas.
   Access Accept fornece acesso ao usuário ao recurso e contém a política que a NAS deve utilizar para prover os serviços, forçando um comportamento do usuário final. Um access accept pode ser enviado separadamente para cada recurso solicitado e não há herança de um recurso para outro. O acesso pode ser revisado temporariamente para verificar sua validade.
   Uma resposta Access Accept resulta na NAS servindo serviços remotos ao cliente. Isso pode ser um endereço IP dinâmico ou estático, um TTL para a sessão, permissões de uma ACL ou a configuração de parâmetros como L2TP, Vlan ou QoS para a sessão.

6. Uma vez estabelecida a sessão entre o cliente RADIUS, o processo de contabilidade pode ser inicializado.
   Uma requisição Accounting-Request (start) é enviada pelo NAS ao servidor, indicando o início da sessão de contabilidade.
   Uma requisição Accounting-Request (stop) indica o fim da sessão de contabilidade que deve ser gravada e fechada.
   A base de dados utilizada para contabilidade é usada para fins de informações e relatórios de uso.
   Podem ser registrados o tempo de sessão, o número de pacotes ou o total de dados transmitido em ambas direções, identidade da máquina, identidade do usuário, endereços de rede e portas utilizadas.

Tutorial de Instalação de servidor Freradius

o Freradius vai autenticar em um servidor de domínio com samba já em produção

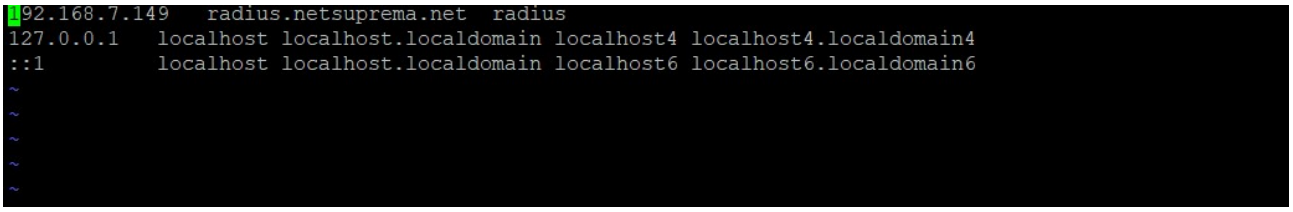
Foi utilizado um servidor CentOS7
Instalaçao do freeradius e samba

yum install freeradius-krb5 freeradius-devel freeradius-utils freeradius samba samba-winbind realmd

configurando o servifor de radius para autenticar com o domínio

deve alterar o nome do servidor
hostnamectl set-hostname radius.dominio.local

configurar o arquivo vim /etc/hosts
192.168.7.149 radius.dominio.local radius



o name server deve apontar para o servidor de domínio Vim /etc/resolv.conf
domain DOMINIO.LOCAL
search DOMINIO.LOCAL
nameserver 192.168.7.235

realm join --client-software=winbind -U administrator DOMINIO.LOCAL
será solicitada a senha do domiínio

systemctl enable winbind
systemctl enable smb
systemctl enable nmb

** configurado o freeradius

Editando oa arquivo vim /etc/raddb/clients.conf, neste arquivo configuro o acesso pelo roteador/wifi

adiciono no começo do arquivo

client tplink {

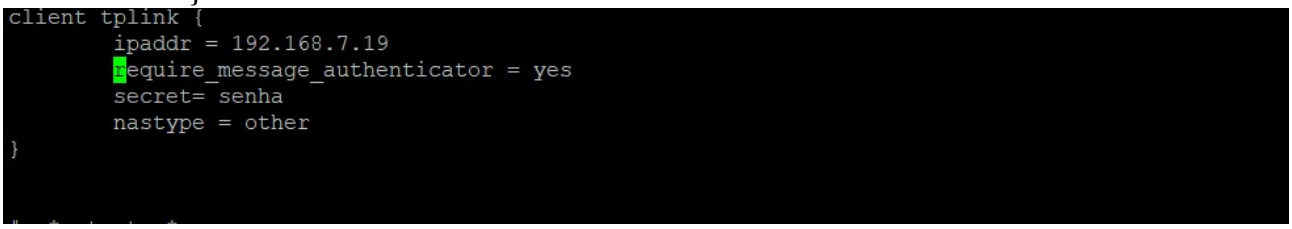
ipaddr = 192.168.7.19

require_message_authenticator = yes

secret= senha

nastype = other

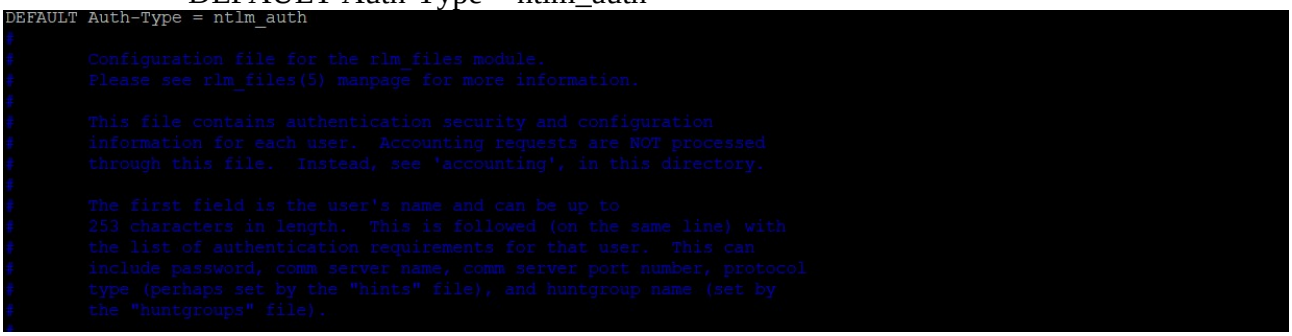
}



depois altero o arquivo vim /etc/raddb/users

adiciono a seguinte linha no inicio do arquivo

DEFAULT Auth-Type = ntlm_auth



depois modifico o arquivo vim /etc/raddb/mods-available/ntlm_auth

altero para:

exec ntlm_auth {

wait = yes

program = "/usr/bin/ntlm_auth --request-nt-key --domain=dominio.local –username=%{mschap:User-Name} --password=%{User-Password}"

}

depois modifico o arquivo /etc/raddb/sites-available/default

dentro do bloco 'authorize' descomento o a linha #ntlm_auth

authorize {

...

ntlm_auth

...

}

dentro do bloco 'authenticate' adiciono os seguintes parametros

authentication {

...

Auth-Type ntlm_auth {

ntlm_auth
}
...
}

```
#
#  For testing ntlm_auth authentication with PAP
#
#  If you have problems with authentication failing, even when the
#  password is good, it may be a bug in Samba:
#
#       https://bugzilla.samba.org/show_bug.cgi?id=6563
#
exec ntlm_auth {
        wait = yes
        program = "/usr/bin/ntlm_auth --request-nt-key --domain=netsuprema.net --username=%{mschap:User-Name} --password=%{User-Password}"
        #program = "/usr/bin/ntlm_auth --request-nt-key --domain=netsuprema.net --username=%{mschap:User-Name} --password=%{LM-Password}"
        #program = "/usr/bin/ntlm_auth --request-nt-key --domain=netsuprema.net --username=%{mschap:User-Name} --password=%{Cleartext-Password}"
}
~
~
~
```

systemctl restart radiusd
systemctl enable enable

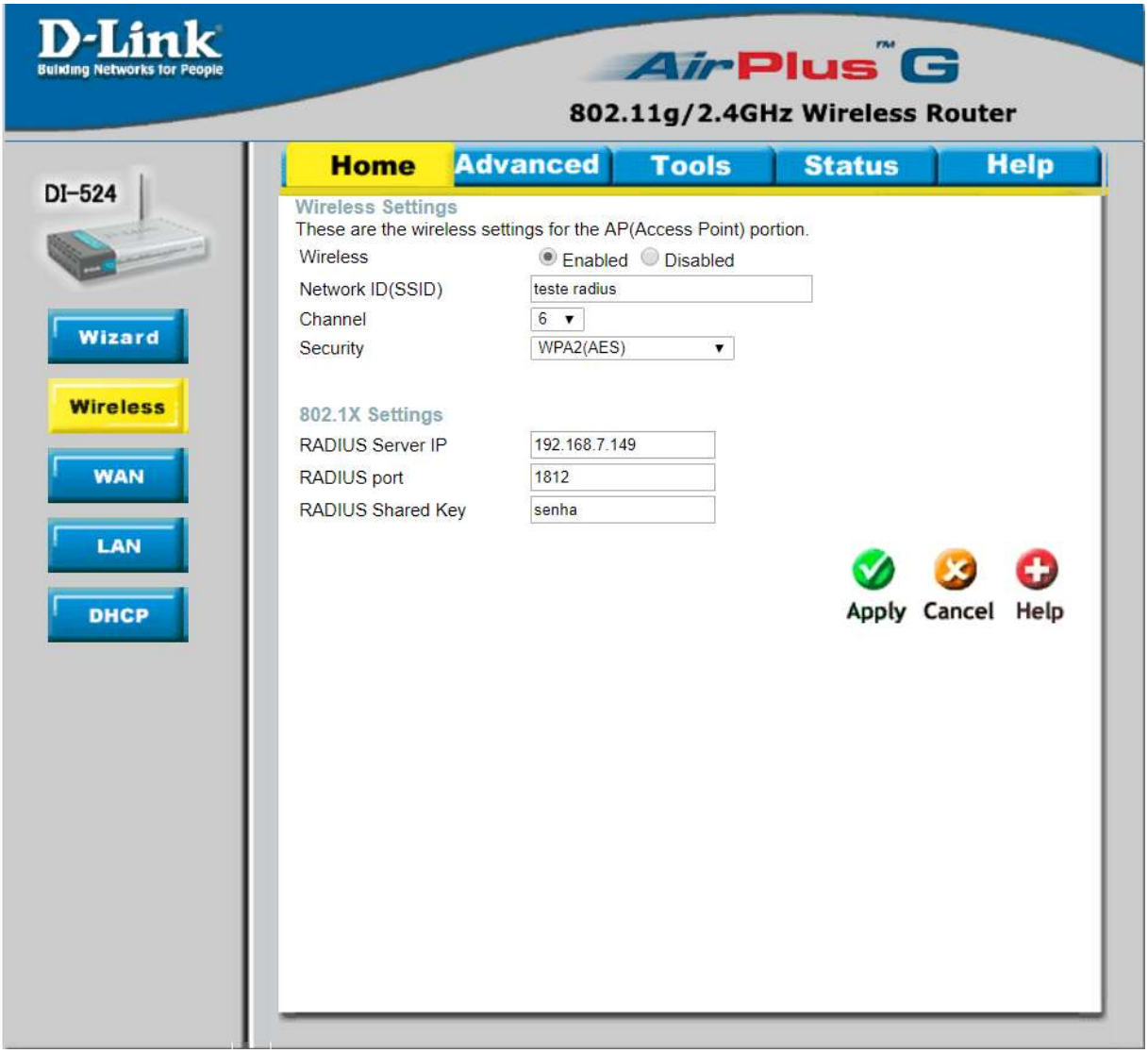
para conexções via smartphone deve autenticar da seguinte maneira:
EAP Method: TTLS
Fase 2 de Autenticação PAP
Identidade: NomeUsuarioDominio
Senha: SenhaDominio

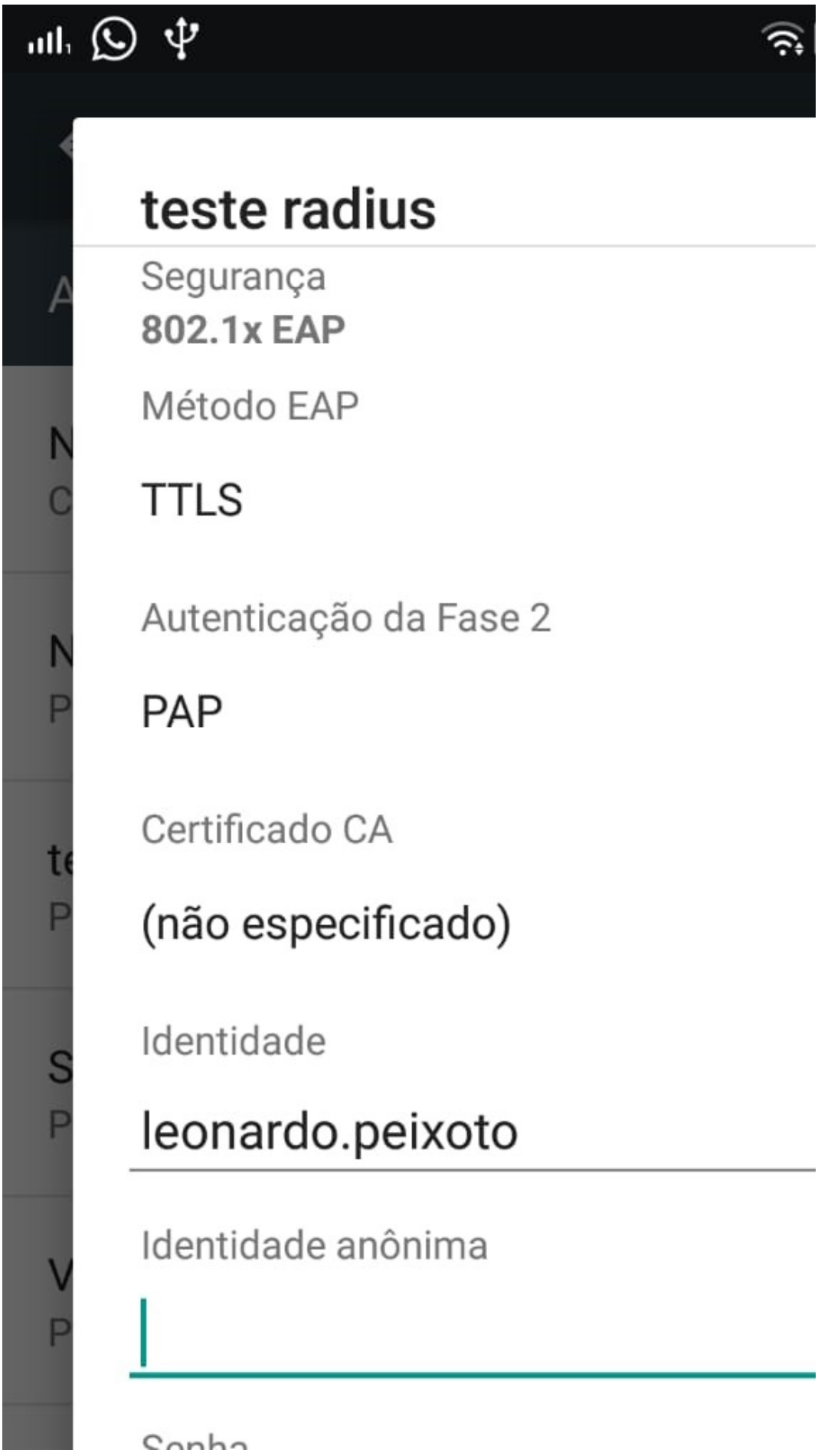
pode ser iniciado o freeradius em modo debug para identificar algum tipo de falha

radiusd -X

```
(5) files: users: Matched entry DEFAULT at line 1
(5)       [files] = ok
(5)       [expiration] = noop
(5)       [logintime] = noop
(5)       [pap] = noop
(5) ntlm_auth: Executing: /usr/bin/ntlm_auth --request-nt-key --domain=netsuprema.net --username=%{mschap:User-Name} --password=%{User-Password}:
(5) ntlm_auth: EXPAND --username=%{mschap:User-Name}
(5) ntlm_auth:    --> --username=gustavo.sobral
(5) ntlm_auth: EXPAND --password=%{User-Password}
(5) ntlm_auth:    --> --password=net@123
(5) ntlm_auth: Program returned code (0) and output 'NT_STATUS_OK: The operation completed successfully. (0x0)'
(5) ntlm_auth: Program executed successfully
(5)       [ntlm_auth] = ok
(5)     } # authorize = ok
(5)   Found Auth-Type = NTLM_AUTH
(5)   # Executing group from file /etc/raddb/sites-enabled/inner-tunnel
(5)     Auth-Type NTLM_AUTH {
(5) ntlm_auth: Executing: /usr/bin/ntlm_auth --request-nt-key --domain=netsuprema.net --username=%{mschap:User-Name} --password=%{User-Password}:
(5) ntlm_auth: EXPAND --username=%{mschap:User-Name}
(5) ntlm_auth:    --> --username=gustavo.sobral
(5) ntlm_auth: EXPAND --password=%{User-Password}
(5) ntlm_auth:    --> --password=net@123
(5) ntlm_auth: Program returned code (0) and output 'NT_STATUS_OK: The operation completed successfully. (0x0)'
(5) ntlm_auth: Program executed successfully
(5)       [ntlm_auth] = ok
(5)     } # Auth-Type NTLM_AUTH = ok
(5)   # Executing section post-auth from file /etc/raddb/sites-enabled/inner-tunnel
(5)     post-auth {
(5)       if (0) {
(5)       if (0)  -> FALSE
(5)     } # post-auth = noop
(5)   Login OK: [gustavo.sobral/[redacted]] (from client tplink port 0 via TLS tunnel)
(5) } # server inner-tunnel
(5) Virtual server sending reply
(5) eap_ttls: Got tunneled Access-Accept
(5) eap: Sending EAP Success (code 3) ID 6 length 4
(5) eap: Freeing handler
(5)     [eap] = ok
(5)   } # authenticate = ok
(5) # Executing section post-auth from file /etc/raddb/sites-enabled/default
(5)   post-auth {
(5)     update {
(5)       No attributes updated
(5)     } # update = noop
(5)     [exec] = noop
(5)     policy remove_reply_message_if_eap {
(5)       if (&reply:EAP-Message && &reply:Reply-Message) {
```

Configuração do roteador Wifi




teste radius
Segurança
802.1x EAP
Método EAP
TTLS
Autenticação da Fase 2
PAP
Certificado CA
(não especificado)
Identidade
leonardo.peixoto
Identidade anônima

C