Módulo V – Aula 3

ACESSANDO O FIREWALL PELO SSH

(SECURE SHELL)

TENHO QUE IR ATÉ O CPD TODA VEZ QUE PRECISAR ACESSAR O CONSOLE DO PFSENSE?

Não precisa não. Assim como administramos servidores linux pela linha de comandos remotamente usando o protocolo de Shell Remoto Seguro (SSH), podemos também acessar o console do pfSense pela rede e ter acesso ao terminal para executar comandos. Isto vai ser útil apenas quando você perder acesso a administração web por alguma regra mal cofigurada ou por alguma eventualidade, e antes de ir até o CPD e acessar o console do firewall, ou ter que implorar pro pessoal de infra liberar o acesso do Host de virtualização, você pode fazer o acesso SSH pela rede (desde que já tenha liberado).

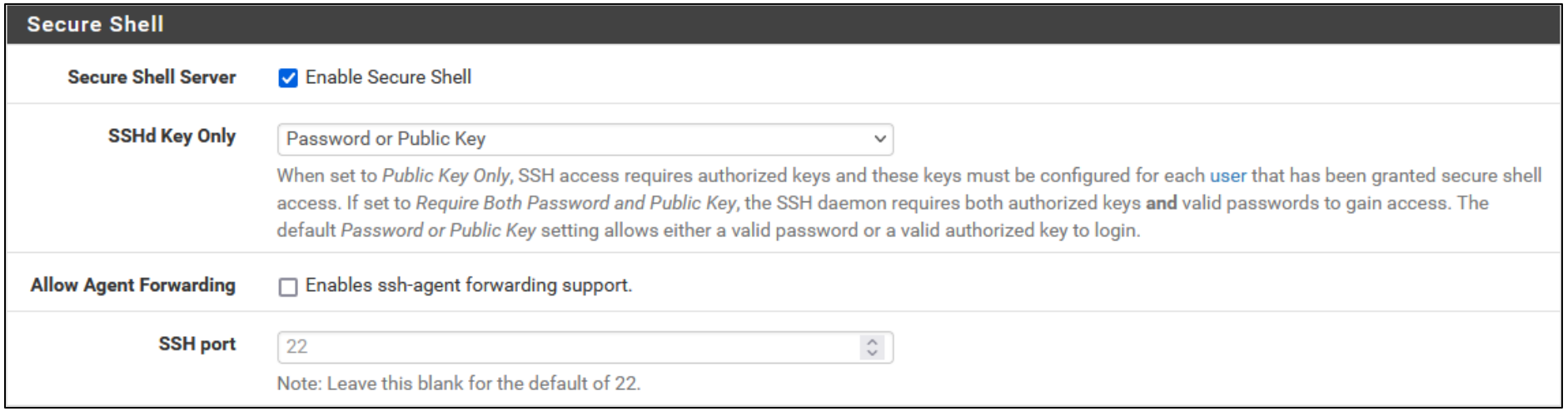
O SSH por padrão é desabilitado, sendo necessário manualmente habilitá-lo.

HABILITANDO O SSH

Um vez na Administração web do firewall, vá no menu System -> Advanced.

Role a tela para baixo até encontrar a seção Secure Shell. Marque a opção para habilitar o serviço SSH, e, opcionalmente altere a porta padrão que é 22 para uma outra porta de sua preferência. Esta questão de trocar a porta é uma tentativa de dificultar a vida de quem estiver tentando acessar seu firewall sem ter a permissão, alterando a porta a pessoa vai ter mais dificuldade em descobrí-la.

Role até o fim da página e clique em salvar.



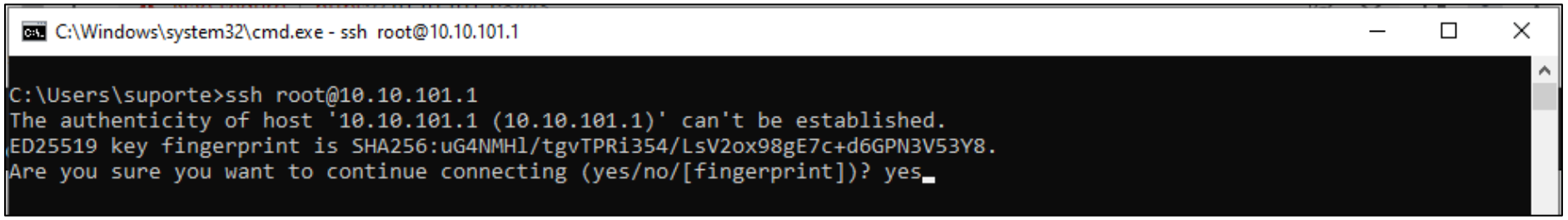
ACESSANDO O FIREWALL USANDO O SSH

Uma vez habilitado o serviço SSH, você agora pode acessá-lo de sua estação de trabalho com windows 10/11 ou linux.

Abra um prompt de comandos e digite:

```
ssh root@192.168.1.1
```

No primeiro acesso deverá aparecer algumas informações referentes a chave RSA de host. Digite **yes** e pressione **ENTER** para aceitar.



Agora digite a senha do usuário admin (**por curiosidade, a senha do usuário admin sempre será a mesma senha do usuário root, então por mais que usemos o usuário root para acessar, a senha que deve ser digitada é a do admin que você definiu anteriormente).

```
C:\Users\suporte>ssh root@10.10.101.1
Password for root@router01.home.arpa:
Microsoft Azure - Netgate Device ID: 525727f2843e3da757fa

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on router01 ***

 WAN (wan)       -> hn0        -> v4/DHCP4: 192.168.10.13/24
 WAN_VIVO (lan)  -> hn1        -> v4: 180.99.131.169/29
 WAN_ALGAR (opt1) -> hn2        -> v4: 181.45.11.9/29
 WAN_CLARO (opt2) -> hn3        -> v4: 200.40.34.17/29
 OPT3 (opt3)     -> hn4        ->
 VLAN_101 (opt4) -> hn4.101    -> v4: 10.10.101.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Disable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

E estamos dentro! Agora é o mesmo console que você já conhece.

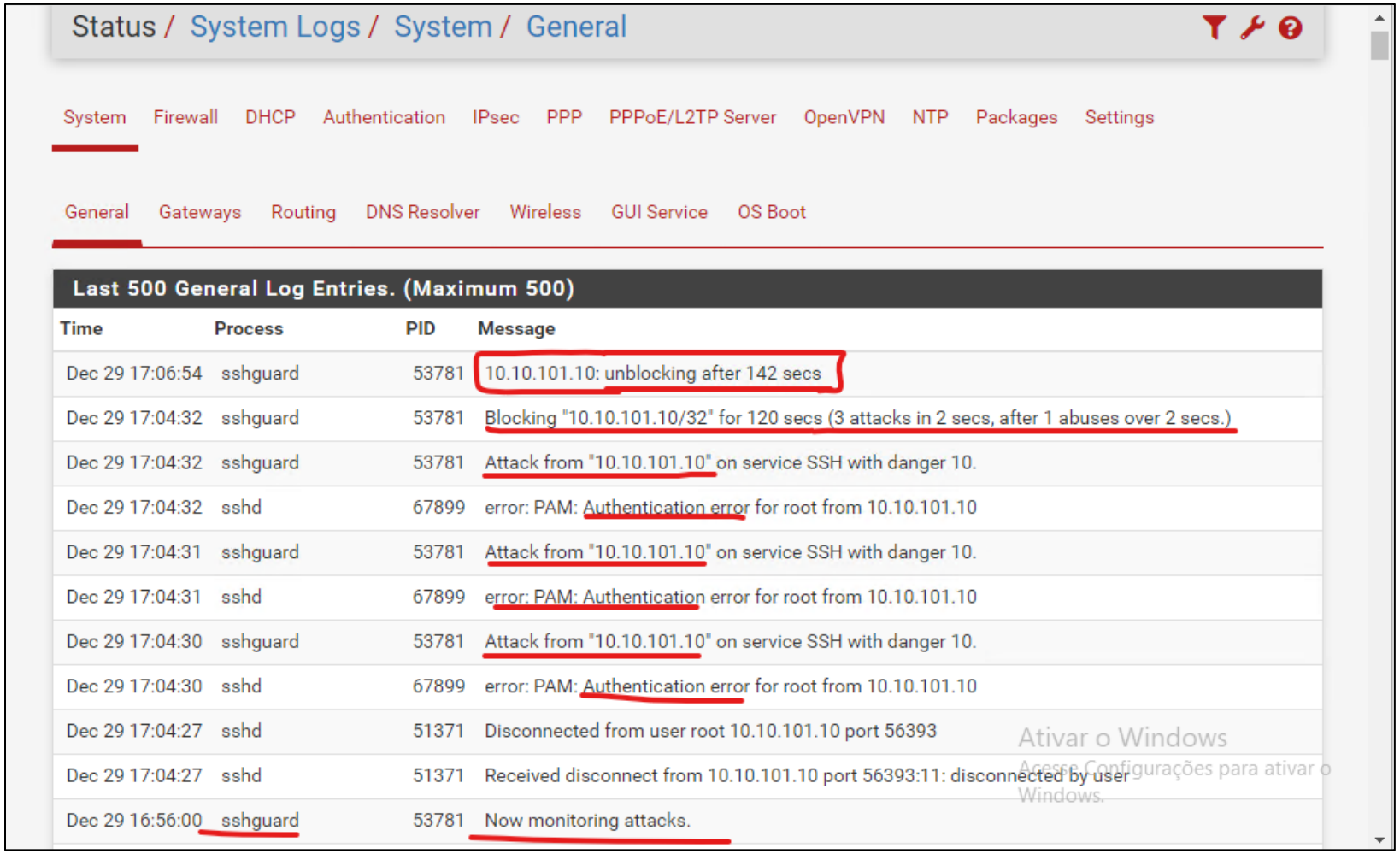
ESSE NEGÓCIO DE AUTENTICAÇÃO SSH COM SENHA NÃO É INSEGURO NÃO?

Pois bem, é uma pergunta capciosa! Temos maneiras mais seguras de proteger o login do Firewall pelo SSH. Mas antes gostaria que soubesse que, o pfSense de forma nativa possui proteção ao serviço SSH. Caso alguém tente acessá-lo com a senha errada por mais de 3 vezes, a cada nova tentativa, o firewall irá bloquear o IP que está tentando o acesso, e não sendo o suficiente, a cada novo bloqueio irá travar 1.8 vezes o tempo a mais.

Paga entender como funciona esse comportamento, erre a senha propositalmente do acesso ao firewall (via ssh) por algumas vezes, você perceberá que na quarta vez, não conseguirá acessar mais o firewall. Aguarde alguns instantes e tente novamente.

Quando voltar o acesso, desta vez vá até os logs de sistema e veja a informação que é gerada:

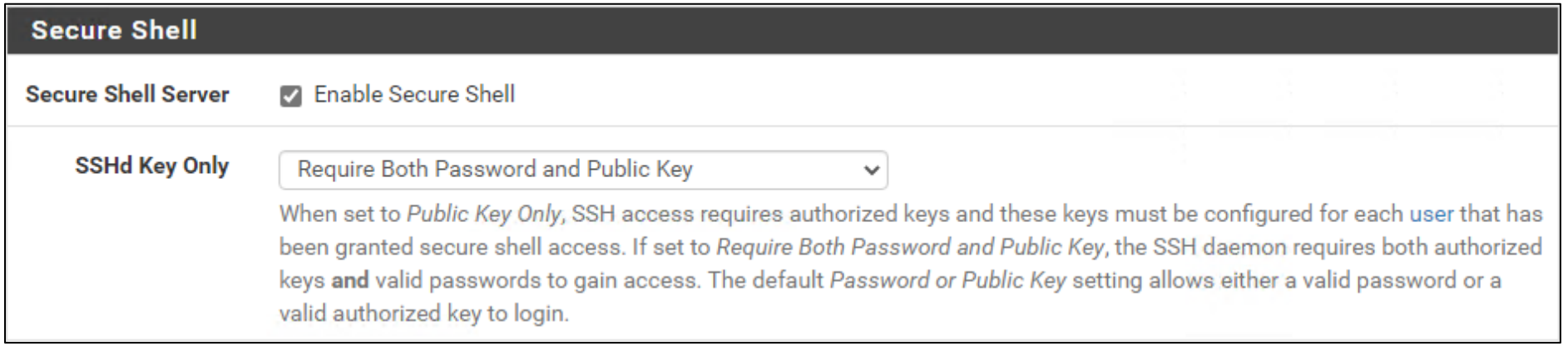
```
C:\Users\suporte>ssh root@10.10.101.1
Password for root@router01.home.arpa:
Password for root@router01.home.arpa:
Password for root@router01.home.arpa:
root@10.10.101.1's password:
ssh_dispatch_run_fatal: Connection to 10.10.101.1 port 22: Connection timed out
```



Na figura acima, podemos ver as tentativas de ataque ao serviço SSH, o bloqueio após 3 tentativas e o bloqueio do IP do computador pelo tempo de 142 segundos.

DIFICULTANDO AINDA MAIS O ACESSO SSH

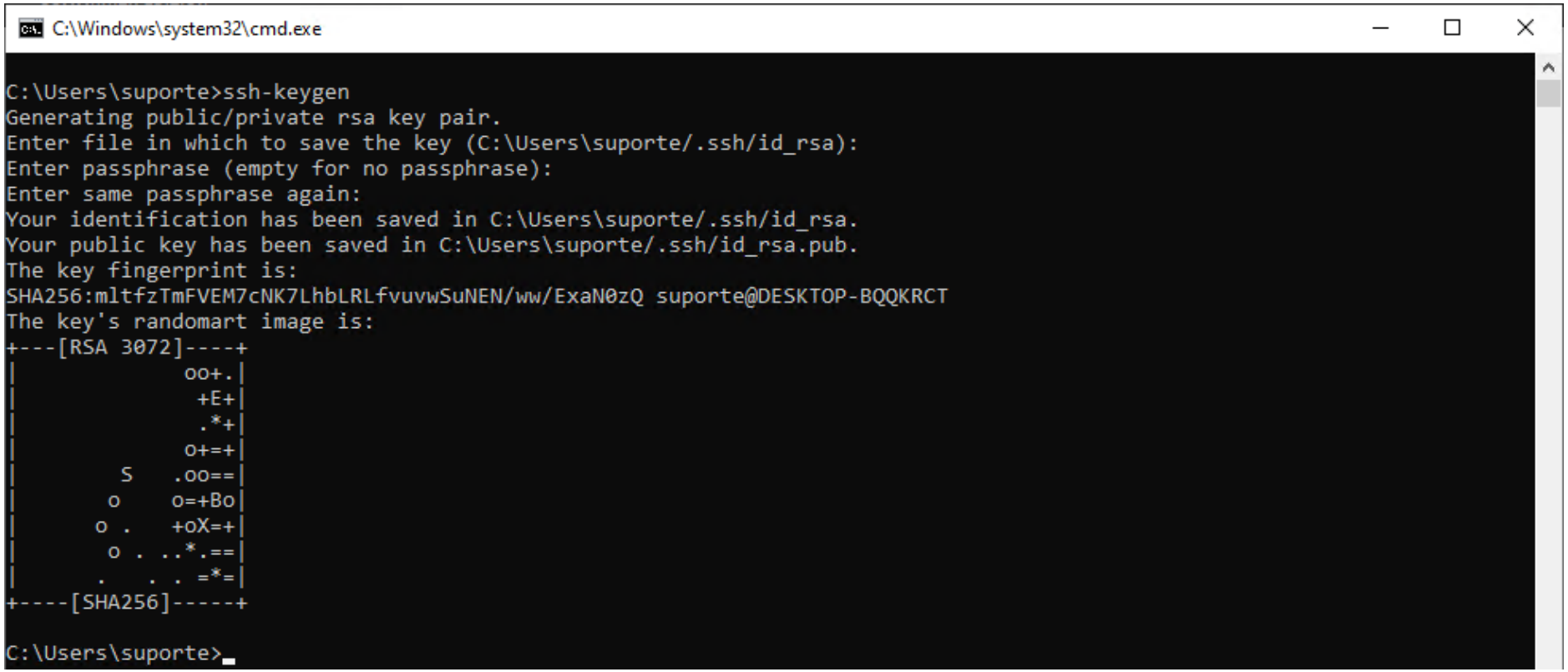
Se você quer elevar ainda mais o nível de segurança no acesso SSH, saiba que tem como. Basta fazer o seguinte: vai no pfsense, no menu System -> Advanced. Vai na seção Secure Shell e marca a opção SSHd Key Only como “Require Both Password and Public Key” e salva novamente a configuração ao final da página. Assim, para que alguém consiga se autenticar no firewall, não bastará ter apenas a senha de usuário, será necessário também portar a chave privada que é um arquivo com uma senha gigantesca.



Após ter salvo a configuração, tente acessar o firewall via ssh novamente. Você deverá receber a mensagem de que a autenticação foi negada porque não há chave pública.

Agora no Windows 10/11, executa o comando ssh-keygen e confirme apertando apenas enter as questões na tela.

Opcionalmente você pode ou não definir uma senha (passphrase) quando solicitado. Indico que não coloque ainda, senão você terá 3 fatores de autenticação (a chave privada, a senha do usuário e a senha da chave privada). Vamos nos ater a apenas 2 para demonstração.



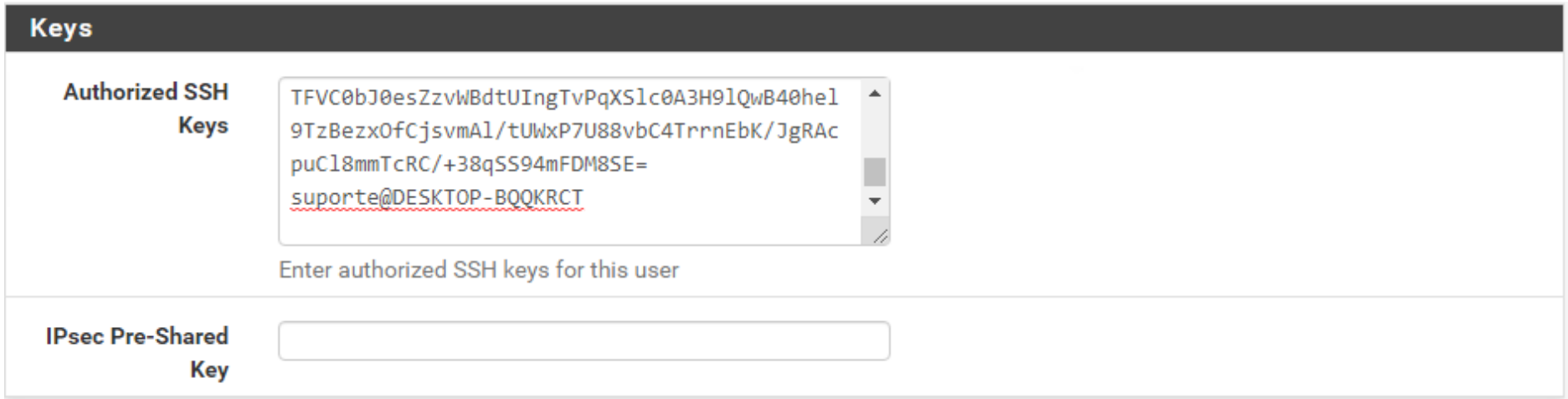
Repare que na saída do comando, foi informado o caminho do arquivo de chave pública gerada. Copie o caminho e abra o arquivo no bloco de notas. Copie todo o conteúdo.

Your public key has been saved in C:\Users\suporte/.ssh/id_rsa.pub

Copie todo o conteúdo do arquivo (Control+C).

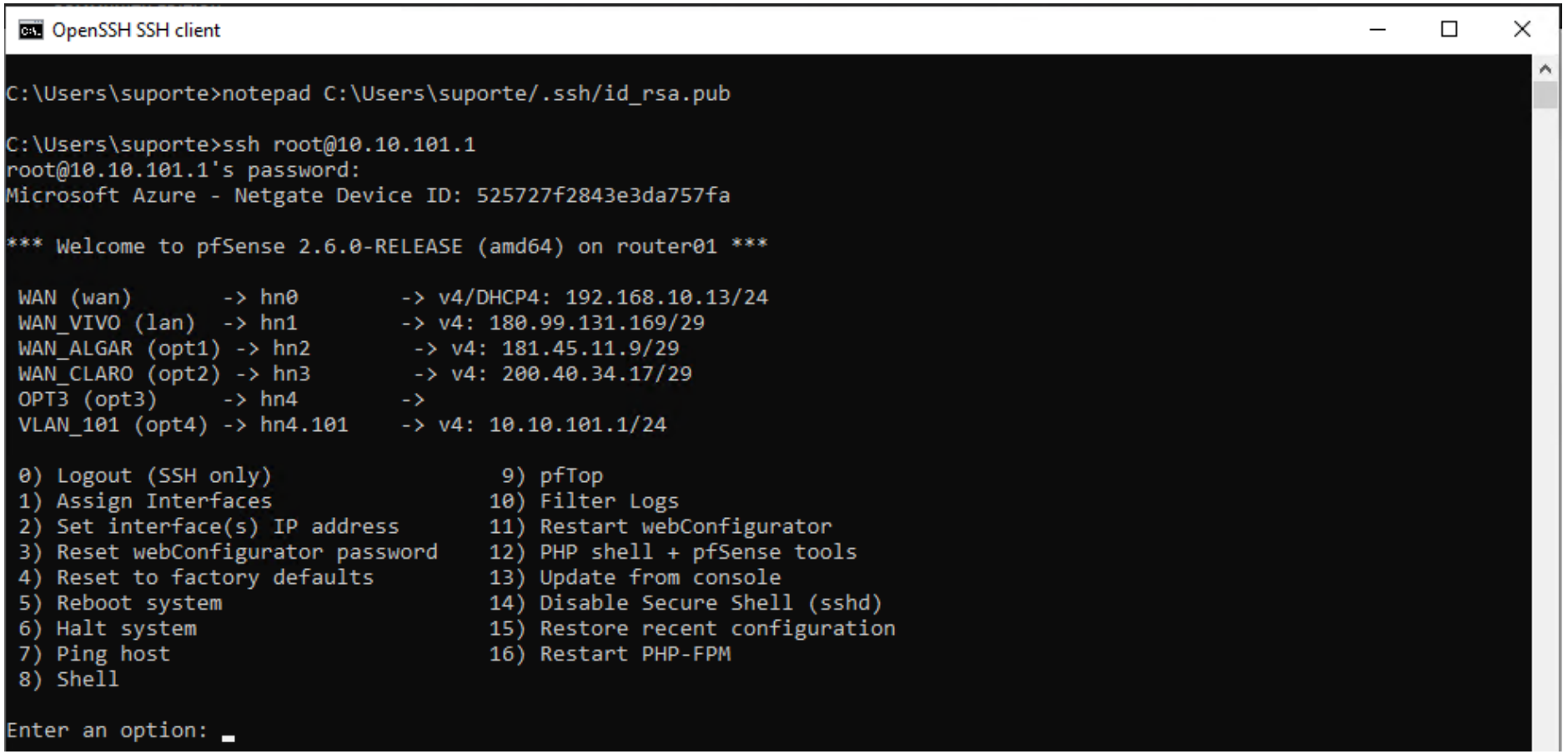
Agora novamente na interface do pfSense, acesse o gerencimaento de usuários (Menu system -> User manager) e clique para editar no usuário admin.

Ao final da página, no campo Authorized SSH Keys, cole o texto copiado anteriormente.



Salve a configuração usando o botão Save ao final da página.

Tente novamente acessar o firewall uando o ssh e desta vez deverá pedir a senha. Insira a senha do usuário admin e deverá ver o console.



Repare que, para a autenticação funcionar, você deverá ter sempre em mãos o arquivo de chave privada que foi gerado pelo comando ssh-keygen. Então se você for utilizar a autenticação por meio de chave privada, trate de realizar cópias de segurança (backup) dos arquivos que foram gerados com o comando ssh-keygen.

TAREFA

Realize a configuração do firewall para acesso via SSH usando Chave privada e senha.

Faça acesso ao firewall sem gerar a chave privada. Apareceu o erro (publickey) como descrito neste material?

Crie o par de chaves (publica e privada) ssh com o comando ssh-keygen. Copie a chave pública para o firewall (em algum usuário) e tente acessar novamente o firewall. Obteve sucesso?

“SE VOCÊ APAGASSE TODOS OS ERROS DO SEU PASSADO, APAGARIA TODA A SABEDORIA DO SEU PRESENTE.”