Manual de Instalação de Certificado – NGINX

Você recebeu do Site Blindado um zip contendo dois arquivos, são eles:

- *www_seudominio_com_br.crt* **(CERTIFICADO)**

- *www_seudominio_com_br.ca-bundle* **(CERTIFICADO INTERMEDIÁRIO)**

Ao solicitar o seu certificado você gerou uma chave CSR e uma chave privada, esta chave privada está em seu servidor e você irá utilizar nesta instalação.

www_seudominio_com_br.key **(CHAVE PRIVADA)**

1º Passo : Concatene o seu certificado e o seu certificado intermediário transformando-os em um único arquivo através do seguinte comando :

*cat www_seudominio_com_br.crt www_seudominio_com_br.ca-bundle >> **ssl_bundle.crt***

2º Passo: Mova o recém-criado **ssl_bundle.crt** para o local onde você salva os arquivos de certificados (ex. **/etc/ssl/certs/**).

3º Passo: crie/modifique o arquivo de configuração do seu site, que pode estar nos seguintes locais:

*** /etc/nginx/sites-available/**

*** /usr/local/nginx/sites-available/**

4º **Passo:** Certifique-se dos seguintes itens:

- 'ssl' deve estar em 'on'.
- Configure 'listen' para a sua porta SSL; geralmente a 443.
- Configure 'ssl_certificate' para o local onde você salvou o certificado.
- Configure 'ssl_certificate_key' para o local onde você salvou a chave privada.

5º **Passo:** Você também pode configurar o seguinte:

-- ssl_ciphers ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM;
-- ssl_protocols SSLv3 TLSv1; #Habilita SSLv3/TLSv1

Exemplo de um Virtual Host Nginx com SSL configurado:

```
server {
listen 443;

ssl on;
ssl_certificate /etc/ssl/certs/ssl_bundle.crt;
ssl_certificate_key /etc/ssl/private/www_seudominio_com_br.key;
#Habilita SSLv3/TLSv1, mas não SSLv2, que é fraco e não deve mais ser utilizado.
ssl_protocols SSLv3 TLSv1;
#Desabilita todas as cifras fracas
ssl_ciphers ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM;

server_name seudominio.com.br;
}
```

FIM, agora basta reiniciar o Nginx!!