NORMA DE GESTÃO DE PERÍMETRO

1. INTRODUÇÃO

Essa norma de segurança da informação serve para complementar a Política de Segurança da Informação, definindo as diretrizes para a devida configuração e gestão dos firewalls e roteadores da ELUBEL.

2. OBJETIVO

O objetivo desta norma é estipular diretrizes que se deve seguir para escolher, configurar e gerenciar firewall e roteador visando sempre a maior segurança e controle do ambiente.

3. ABRANGÊNCIA

Todos os firewall de appliance, software e host (servidores, desktops e notebooks), além dos roteadores.

4. ESCOPO

O escopo deste documento é orientar ao que pode e não pode ser feito em relação aos firewalls e roteadores, no ambiente de produção e do escritório.

5. DIRETRIZES

5.1. Os ambientes devem ter preferencialmente um firewall dedicado tanto na cloud como no escritório, que pode ser via appliance ou sistema.

5.2. O firewall deve atender a função de antispoofing, IDS (sistema de monitoramento) e IPS (sistema de controle).

5.3. O firewall deve ter bloqueio full por padrão, para a internet ou qualquer rede pública. As liberações devem ser gradativas de acordo com a necessidade.

5.4. O firewall da rede corporativa, deve bloquear tudo aquilo que não for necessário utilizar.

5.5. A zona desmilitarizada (DMZ) deve ser isolada da rede por um firewall, sendo que as conexões com a rede interna devem ser restritas e liberadas conforme a necessidade.

5.6. Todo processo de criação, alteração e exclusão de regra, deve seguir um processo formal de regra de firewall e/ou roteador.

5.7. Todas as regras de firewall existentes em cada equipamento, deve estar documentada em um arquivo único, a ser identificado no documento procedimento de perímetro, que deve conter no mínimo a origem, destino, protocolo, porta, serviço, justificativa, solicitando, aprovador e data de liberação.

5.8. É necessário ter um diagrama de rede atualizado, compatível com o cenário atual, tanto do ambiente de cloud (produção), como do ambiente interno (escritório).

5.9. O documento procedimento de perímetro deve descrever os grupos, funções e responsáveis pelo gerenciamento dos componentes da rede. Assim como também atribuir a responsabilidade a cada individuo particularmente.

5.10. Portas, serviços e/ou protocolos não seguros que vierem a ter a necessidade de serem utilizados, deverão ter medidas para mitigar o risco e tais medidas deverão ser documentadas conforme orientação no documento procedimento de perímetro.

5.11. Sempre verificar a viabilidade de utilizar o protocolo e/ou serviço mais atualizado possível.

5.12. Protocolos, serviços e portas que não for utilizado deverá estar desabilitado.

5.13. As regras de firewall e suas respectivas documentações deverão ser revisadas periodicamente, mas não ultrapassando o prazo de seis meses entre uma revisão e outra.

5.14. Os roteadores devem estar atualizados com o cenário atual, sincronizados e ter um backup das configurações.

5.15. O firewall e o roteador devem estar com o patch de atualização aplicado.

5.16. Se for necessário ter uma rede sem fio de visitante a mesma deve estar em uma rede apartada, da rede do escritório e produção. Preferencialmente em um link dedicado apenas para Wi-Fi.

5.17. A DMZ deve ter limitadores de tráfego de entrada, provenientes de redes públicas e/ou não confiáveis.

5.18. O tráfego de saída do ambiente de produção (cloud) não sendo a DMZ, para internet, só deve ocorrer depois de avaliado, testado, validado e autorizado.

5.19. O tráfego só deve ocorrer por uma comunicação segura, autorizada e restrita.

5.20. É veemente proibido a divulgação não autorizada de endereços IPs privados/internos e informações de roteamento.

5.21. Todos os equipamentos como desktop e notebook, devem possuir um firewall de host e ele deve estar ativo e devidamente configurado, conforme o documento procedimento de perímetro.

5.22. O acesso as configurações do firewall de host devem ser bloqueadas aos usuários.

5.23. Os firewalls, roteadores e dispositivos de segurança devem passar periodicamente por um processo de hardening, conforme descrito no documento procedimento de perímetro.

6. RESPONSABILIDADE

É de responsabilidade da Comissão de Segurança a manutenção, gerenciamento, segurança e cobrança de prestadores de serviços.

7. SANÇÕES E PUNIÇÕES

O descumprimento dessa norma pode acarretar sanções e punições ao envolvidos

8. REVISÃO

Esta norma deverá ser revisada anualmente ou extraordinariamente, a qualquer momento se for necessário.