INSTITUTO FEDERAL
FARROUPILHA
Campus São Vicente do Sul

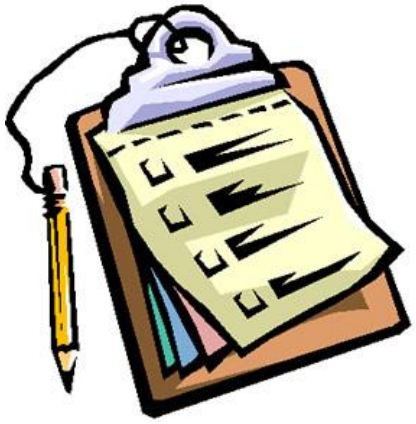
Fonte: http://www.ezequieljuliano.com.br/wp-content/uploads/2014/09/iso27001.jpg

Gestão da Segurança da Informação e Firewall

Prof. Gleizer B. Voss

Roteiro

- Revisão da(s) última(s) aula(s)
- Gestão da Segurança da Informação e Normas
  - Análise de Riscos;
  - Atividade prática!
  - Firewall;
  - Atividade prática!



Última aula...

- Revisão da Última Aula;
  - Análise da ISO/IEC 27009, ISO/IEC 27010, ISO/IEC 27011, ISO/IEC 27012, ISO/IEC 27013, ISO/IEC 27015, ISO/IEC 27016, ISO/IEC 27019, ISO/IEC 27035, ISO/IEC 27036, ISO/IEC 27043, ISO/IEC 27044 e ISO/IEC 27799;
  - Google Hacking;

Questionamento / Objetivo

- Norma 27000
  - O que são?
  - De onde vem?
  - Como se formam?
  - O que fazem?

- Proporcionar a construção de saberes aos alunos com a apresentação dos principais conceitos, relações e componentes envolvidos no emprego de Normativas de Segurança da Informação.

Análise de Riscos e Ativos

- Ferramenta utilizada na segurança da informação;
- Relacionada à regra 27002, 27005 e 27032;
- Objetivo principal é esclarecer se as ameaças são relevantes para os processos operacionais e identificar os riscos associados;

Análise de Riscos e Ativos

- Combinação da **probabilidade** de um determinado evento ocorrer e de suas **consequências** (**impacto**);
- Evento é a relação entre as ameaças, as vulnerabilidades e os danos causados – consequências;

Análise de Riscos e Ativos

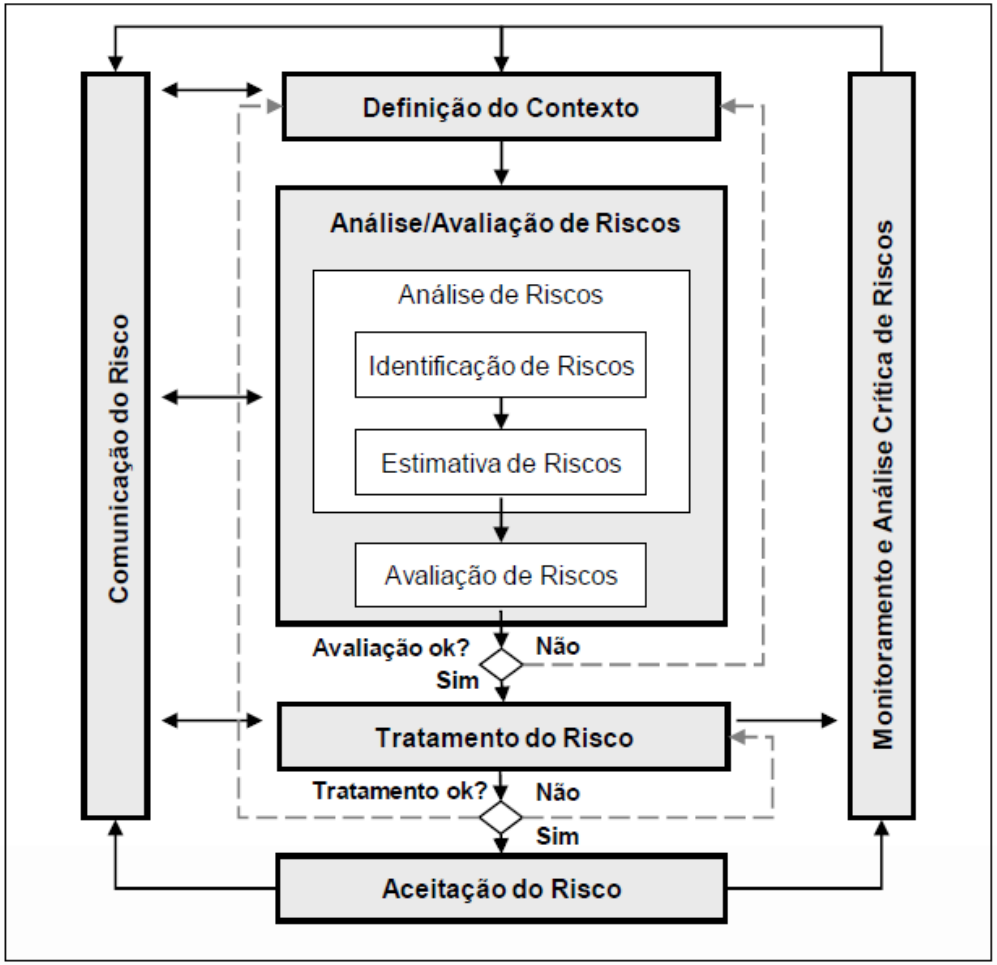
- Garantir que as medidas de segurança sejam implantadas com boa relação custo-benefício;
- Resposta eficaz às ameaças.
- Em virtude da falta de conhecimento, se gasta muito dinheiro em medidas falhas de segurança;
- Auxiliar a empresa a avaliar corretamente os riscos;
- Tomada de decisão;

Análise de Riscos e Ativos

- Possui 4 objetivos principais
  - Identificar quais os bens e valores;
  - Determinar vulnerabilidades e ameaças;
  - Quais são ameaças tem o potencial de se tornar riscos e podem interromper o processo;
  - Equilíbrio entre custos de um incidente e custos de uma medida de segurança (custo-benefício);
- Cuidados especiais na análise dos riscos;

Análise de Riscos e Ativos

- Processo de Gestão dos Riscos



Análise de Riscos e Ativos

- Definição do Contexto
  - Critérios Básicos
  - Escopo;
  - Limites da Gestão de Riscos;
  - Organização apropriada

Análise de Riscos e Ativos

- Análise e Avaliação dos Riscos
  - Identificação;
  - Quantificação/Qualitativo;
  - Priorização;
  - Consiste nas seguintes atividades:
    - Análise de Riscos (Identificação e Estimativa de Riscos);
    - Avaliação de Riscos.

Análise de Riscos e Ativos

- Tratamento dos riscos
- Devem ser selecionadas opções para o tratamento dos riscos;
  - Reduzir;
  - Reter;
  - Evitar;
  - Transferir;
- Plano de tratamento de riscos (PTR).

Análise de Riscos e Ativos

- Tratamento dos Riscos
  - Risco residual;
  - Plano de tratamento de riscos;
  - Estes riscos precisam ser estimados.

reduzir, reter, evitar ou transferir os riscos

Análise de Riscos e Ativos

- Aceitação dos Riscos
  - Tomada de decisão;
  - Registro das ações;
  - Responsabilidade pelas ações;
  - Politica de gestão.

Análise de Riscos e Ativos

- Comunicação dos Riscos
  - Devem ser compartilhadas;
  - As partes envolvidas devem se comunicar;
  - Consenso entre as partes.

Análise de Riscos e Ativos

- Monitoramento dos Riscos
  - Riscos e seus fatores devem ser monitorados;
  - Análise crítica;
  - Identificação rápida;
  - Mudanças no contexto e visão global dos riscos.

Análise de Riscos e Ativos

- Abordagem reativa X proativa;
- Reativa
  - Quando ocorre um incidente;
  - Análise e tomada de decisão;
- Proativa
  - Busca a prevenção;
  - Redução da probabilidade.

Análise de Riscos e Ativos

- Análise do Risco = Probabilidade X Impacto;

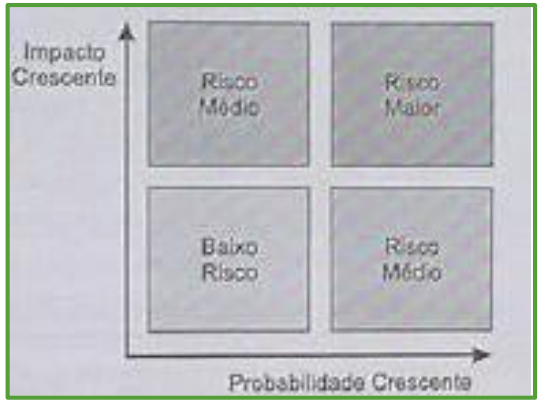
Data Gathering Template

Identify assets that your group is responsible for developing, managing, supporting, or maintaining.

Asset Name	Asset Classification (High, Medium, or Low Business Impact)
1.	

For each asset, complete the following:

Defense-in-Depth Layer	What You Are Afraid of or Are Trying to Avoid: (Threats)	How It May Happen: (Vulnerabilities)	Exposure Level (H,M,L)	**Current Controls Descriptions**	Probability (H,M,L)	**Control Concerns, Potential New Controls**
Physical						
Application						
Host						
Network						
Data						



Fonte: Dillard, 2004 / MARSHALL, 2002, pág. 46

Análise de Riscos e Ativos

- Matriz de Riscos
  - Ferramenta que classifica, qualitativamente, os pesos de impacto e probabilidade;

Probabilidade / Impacto	Sem Impacto	Leve	Médio	Grave	Gravíssimo
Quase certo	Risco Elevado	Risco Elevado	Risco Extremo	Risco Extremo	Risco Extremo
Alta	Risco Moderado	Risco Elevado	Risco Elevado	Risco Extremo	Risco Extremo
Média	Risco Baixo	Risco Moderado	Risco Elevado	Risco Extremo	Risco Extremo
Baixa	Risco Baixo	Risco Baixo	Risco Moderado	Risco Elevado	Risco Extremo
Raro	Risco Baixo	Risco Baixo	Risco Moderado	Risco Elevado	Risco Elevado

Fonte: https://blog.luz.vc/como-fazer/aprenda-a-fazer-analise-de-riscos-com-o-metodo-william-t-fine/

Análise de Riscos e Ativos

- Como fazer a análise dos riscos
  - Probabilidade;
  - Impacto;
- Método William T. Fine;
  - Leva em conta os fatores citados e a parte financeira;
  - Existem 2 variáveis essenciais
    - Grau de Criticidade - matriz de risco que leva em consideração 3 variáveis: consequência (similar ao impacto), exposição ao risco (que é a frequência que o risco costuma se manifestar) e probabilidade;
    - Justificativa de Investimento – grau de criticidade em comparação com o fator de custo (que analisa o valor a ser investido) e o grau de correção (que demonstra o quanto do risco será corrigido de fato);

Análise de Riscos e Ativos

- Método William T. Fine
- Grau de Criticidade
  - Fator **Consequência** – Determine o nível de consequência caso o risco/problema ocorra:
    - Catastrófico quebra da atividade fim da empresa – 100
    - Severo – Prejuízos – 50
    - Grave – 25
    - Moderado – 15
    - Leve – 5
    - Nenhum – Pequeno impacto – 1

Análise de Riscos e Ativos

- Método William T. Fine
- Grau de Criticidade
  - Fator **Exposição** ao Risco – Determine a frequência com que esse risco/problema ocorre ou pode ocorrer:
    - Várias vezes ao dia – 10
    - Uma vez ao dia, frequentemente. – 5
    - Uma vez por semana ou ao mês, ocasionalmente. – 3
    - Uma vez ao ano ou ao mês, irregularmente. – 2
    - Raramente possível, sabe-se que ocorre, mas não com frequência – 1
    - Remotamente possível, não sabe se já ocorreu – 0,5

Análise de Riscos e Ativos

- Método William T. Fine
- Grau de Criticidade
  - Fator **Probabilidade** – Determine a chance do risco / problema ocorrer
    - Espera-se que aconteça – 10
    - Completamente possível – 50% de chance – 6
    - Coincidência se acontecer – 3
    - Coincidência remota – 1
    - Extremamente remota, porém possível – 0,5
    - Praticamente impossível, uma chance em um milhão – 0,1

Análise de Riscos e Ativos

- Método William T. Fine
- Grau de Criticidade
  - GC maior e igual a 200 – **Correção imediata** – risco tem que ser reduzido;
  - GC menor que 200 e maior que 85 – **Correção urgente** – requer atenção;
  - GC menor que 85 – Risco **deve ser monitorado**.

GRAU DE CRITICIDADE – GC	PRIORIDADES – AÇÕES A TOMAR
GC MAIOR OU IGUAL A 200	CORREÇÃO IMEDIATA – RISCO TEM QUE SER DIMINUÍDO
GC ABAIXO DE 200 E MAIOR OU IGUAL A 85	CORREÇÃO URGENTE – REQUER ATENÇÃO
GC MENOR QUE 85	RISCO DEVE SER ELIMINADO

Análise de Riscos e Ativos

- Método William T. Fine
- Justificativa do Investimento
  - JI = GC / (Fator de Custo x Grau de Correção);
  - Fator de Custo
  - Grau de Correção

$$JI = \frac{GC}{\text{Fator de Custo X Grau de Correção}}$$

Análise de Riscos e Ativos

- Método William T. Fine
- Fator Custo – é uma valoração de quanto custaria para prevenir o risco de acontecer
  - Maior que R$150.000 – 10
  - Entre R$75.000 e R$150.000 – 6
  - Entre R$30.000 e R$75.000 – 4
  - Entre R$3.000 e R$30.000 – 3
  - Entre R$300 e R$3.000 – 2
  - Entre R$75 e R$300 – 1
  - Menos que R$75 – 0,5

CLASSIFICAÇÃO	VALOR
MAIOR QUE US$ 50.000	10
ENTRE US 25.000 E US$ 50.000	6
ENTRE US$ 10.000 E US$ 25.000	4
ENTRE US$ 1.000 E US$ 10.000	3
ENTRE US$ 100 E US$ 1.000	2
ENTRE US$ 25 E US$ 100	1
MENOS QUE US$ 25	0,5

Análise de Riscos e Ativos

- Método William T. Fine
- Grau de Correção – Indica o quanto do risco será eliminado
  - Risco elimina[illegible]00% – 1
  - Risco Reduz[illegible] – 2
  - Risco Red[illegible]% e 75% – 3
  - Risco Re[illegible] e 50% – 4
  - Risco Reduzido menor que 25% – 6

CLASSIFICAÇÃO	VALOR
RISCO ELIMINADO – 100%	1
RISCO REDUZIDO – 75%	2
RISCO REDUZIDO ENTRE 50% E 75%	3
RISCO REDUZIDO ENTRE 25% E 50%	4
RISCO REDUZIDO MENOR QUE 25%	6

Análise de Riscos e Ativos

- Método William T. Fine
- Justificativa de investimento precisa ser plotada em uma escala de valoração que tem 3 respostas possíveis:
  - IJ menor que 10 – investimento duvidoso
  - IJ entre 10 e 20 – investimento normalmente justificado
  - IJ maior que 20 – investimento totalmente justificado

Análise de Riscos e Ativos

- Método William T. Fine
- Exemplo:

Risco Identificado	Grau de Criticidade
Galpão com possibilidade de explodir	Correção urgente – requer atenção
Cano do gás vazando	Risco deve ser monitorado
Cano do gás vazando	Risco deve ser monitorado
Quebra de caminhão	Correção urgente – requer atenção
Galpão com possibilidade de explodir	Correção imediata – risco tem que ser reduzido
Cano do gás vazando	Correção imediata – risco tem que ser reduzido
Quebra de cano da plataforma	Correção urgente – requer atenção
Qubra de transporte	Risco deve ser monitorado
Defeito na fritadeira	Risco deve ser monitorado
Defeito na fritadeira	Risco deve ser monitorado
Galpão com possibilidade de explodir	Correção imediata – risco tem que ser reduzido
Qubra de transporte	Risco deve ser monitorado
Galpão com possibilidade de explodir	Correção urgente – requer atenção
Defeito na fritadeira	Risco deve ser monitorado
Quebra de cano da plataforma	Correção imediata – risco tem que ser reduzido

Medida Preventiva para evitar Risco	Investimento	Grau de correção	Índice de Justificação
Comprar um novo galpao	R$ 10.000,00	Risco eliminado – 100%	Investimento plenamente justificado
Trocar o cano	R$ 2.000,00	Risco reduzido – 75%	Investimento duvidoso
Trocar o cano	R$ 1.000,00	Risco eliminado – 100%	Investimento duvidoso
Consertar	R$ 2.500,00	Risco reduzido entre 50% e 75%	Investimento normalmente justificado
Comprar um novo galpao	R$ 50.000,00	Risco eliminado – 100%	Investimento plenamente justificado
Trocar o cano	R$ 50.000,00	Risco reduzido menor que 25%	Investimento plenamente justificado
Trocar o cano	R$ 10.000,00	Risco reduzido entre 25% e 50%	Investimento duvidoso
Consertar	R$ 1.500,00	Risco reduzido entre 25% e 50%	Investimento duvidoso
Comprar uma nova	R$ 1.000,00	Risco reduzido entre 50% e 75%	Investimento duvidoso
Comprar uma nova	R$ 900,00	Risco reduzido – 75%	Investimento normalmente justificado
Comprar um novo galpao	R$ 15.000,00	Risco reduzido entre 50% e 75%	Investimento plenamente justificado
Consertar	R$ 2.000,00	Risco reduzido menor que 25%	Investimento duvidoso
Comprar um novo galpao	R$ 75.000,00	Risco eliminado – 100%	Investimento plenamente justificado
Comprar uma nova	R$ 2.000,00	Risco reduzido entre 50% e 75%	Investimento duvidoso
Trocar o cano	R$ 50.000,00	Risco reduzido entre 25% e 50%	Investimento normalmente justificado

TABELA

O Fator Consequência	
Classificação	Valor
Catastrófico quebra da atividade fim da empres	100
Severo - Prejuízos	50
Grave	25
Moderado	15
Leve	5
Nenhum - Pequeno impacto	1

O Fator Exposição ao Risco	
Classificação	valor
Várias vezes ao dia.	10
Uma vez ao dia, frequentemente.	5
Uma vez por semana ou ao mês, ocasionalmente.	3
Uma vez ao ano ou ao mês, irregularmente.	2
Raramente possível, sabe-se que ocorre, mas não com frequ	1
Remotamente possível, não sabe se já ocorreu	0.5

O Fator probabilidade	
Classificação	valor
Espera-se que aconteça.	10
Completamente possível - 50% de chance	6
Coincidência se acontecer	3
Coincidência remota	1
Extremamente remota, porém possível	0.5
Praticamente impossível, uma chance em um milhã	0.1

Grau de correção	Valor
Risco eliminado - 100%	1
Risco reduzido - 75%	2
Risco reduzido entre 50% e 75%	3
Risco reduzido entre 25% e 50%	4
Risco reduzido menor que 25%	6

Grau de criticidade	
Grau de Criticidade (GC)	Tratamento do Risco
0	Risco deve ser monitorado
85	Correção urgente - requer atenção
200	Correção imediata - risco tem que ser reduzido

Escala de valoração do índice de justificação	
0	Investimento duvidoso
10	Investimento normalmente justificado
20	Investimento plenamente justificado

Fator de Custo	Valor
R$ 0.00	0.5
R$ 50.00	1
R$ 200.00	2
R$ 2,000.00	3
R$ 20,000.00	4

Fonte: https://luz.vc/products/planilha-de-mapeamento-de-riscos

Análise de Riscos e Ativos

- Boas práticas
  - Processo permanente;
  - Análise dos riscos;
  - Identificação da vulnerabilidade e ameaça;
  - Estrutura adequada;
  - Cultura de gestão de riscos;
  - Patamares aceitáveis.

Análise de Riscos e Ativos

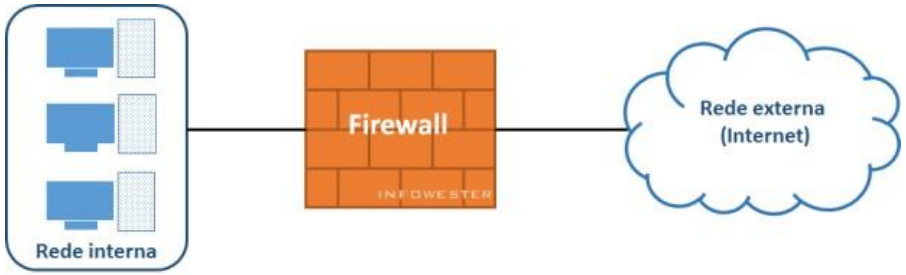
- Erros comuns na análise de riscos
  - Ignorar ou subestimar a gestão de riscos;
  - Escolha do método adequado;
  - Registro de riscos em excesso;
  - Mitigar riscos em excesso;
  - Gerenciar riscos apenas na fase de planejamento;
  - Limitar a gestão de riscos ao gerente de projetos;
  - Eventos passados ajudam na prevenção futura;
  - Focar em riscos com restrições menos relevantes.

FIREWALL

Firewall

- “Parede de Fogo”
- Dispositivo de rede que bloqueia certos tipos de tráfego;
- Como em uma casa, precisamos de segurança;
- Tranca todas as entradas do computador;
- Possuem definições previamente estabelecidas de quais portas podem estar abertas para serem utilizadas por programas.

Fonte:
https://www.infowester.com/firewall.php



Firewall

- Aplicativos ou equipamentos que ficam entre um *link* de comunicação e um computador, checando e filtrando todo o fluxo de dados;
- Possuem definições previamente estabelecidas de quais portas podem estar abertas para serem utilizadas por programas.

Fonte: https://www.estudopratico.com.br/wp-content/uploads/2015/08/firewall.png

Firewall

- Responsável pelo controle dos dados transferidos de e para o seu computador através da Internet;
- Previne que informações pessoais ou confidenciais sejam transmitidas pelo seu computador para a Internet e impedir a invasão da máquina por software malicioso;
- Mas e o antivírus?

Firewall

Funcionamento do Firewall

- Tanto Hardware e Software operam de maneira similar;
- Compara os dados recebidos com as diretivas de segurança e libera ou bloqueia os pacotes;
- Política default de Bloqueio;
- Política default de Permissão.

Firewall

Domínios dos Firewalls

- Existem 3 categorias:
  - Rede;
  - Local;
  - Aplicação;

Firewall

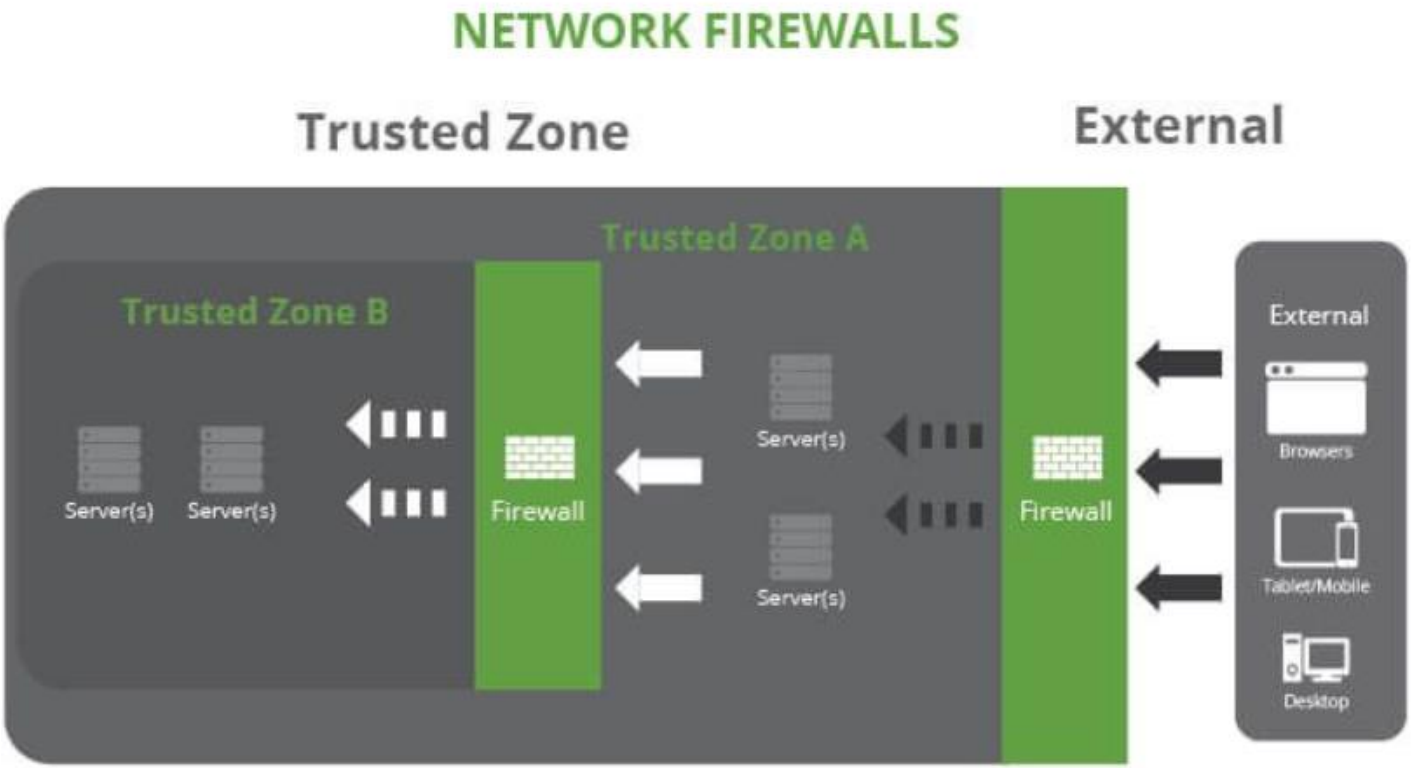
Domínios dos Firewalls

- Rede
  - Implantações em grande escala;
  - Pode ser encontrado em roteadores domésticos ou firewalls adicionais para isolar diferentes partes de uma rede, protegendo os ativos da rede;
  - São projetados para analisar as tentativas de conexão de rede para várias portas de rede, bem como analisar os pacotes de entrada e suas metadados associadas.

Firewall

Domínios dos Firewalls

- Rede



Fonte: https://blog.sucuri.net/wp-content/uploads/2222/03/04122016_DifferentiateFirewalls_01_NetworkFireWalls_V3-650x450.jpg

Firewall

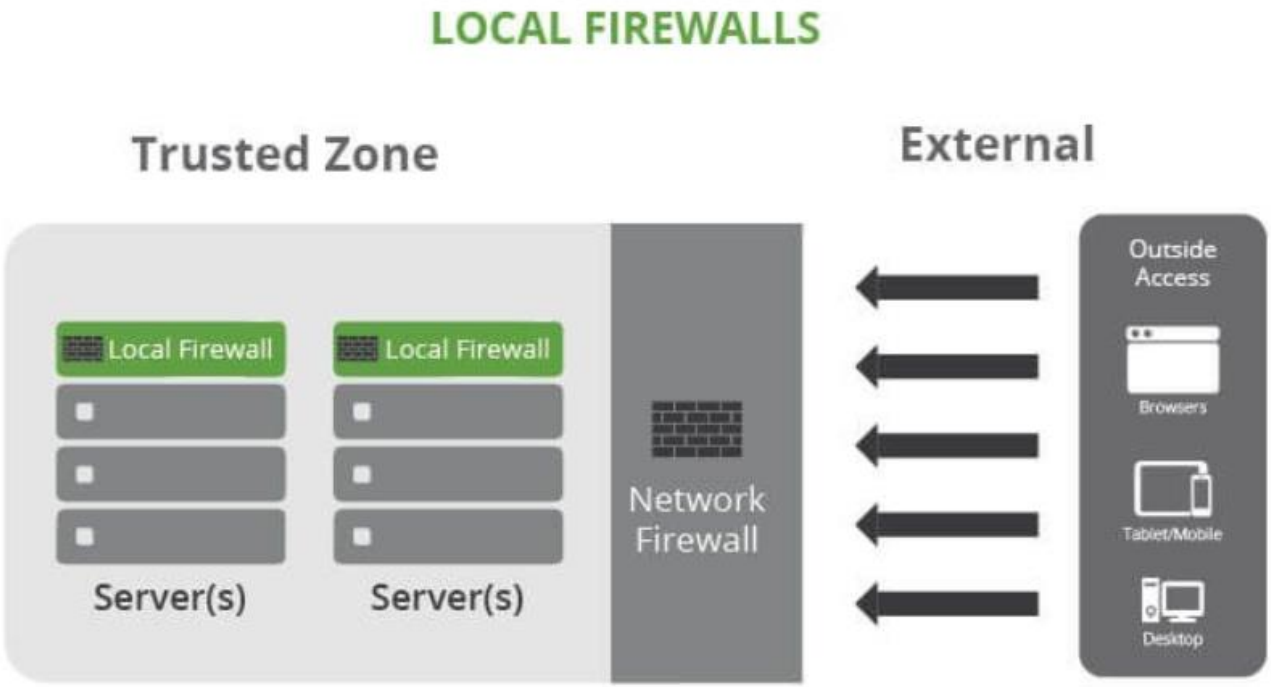
Domínios dos Firewalls

- Local
  - Projetados para proteger ambientes confiáveis dos ambientes não confiáveis;
  - Estão focados em um ambiente específico, seja um servidor ou um desktop;
  - Ao trabalhar com o seu host, o seu acesso ao firewall local pode ser limitado, dependendo do tipo de configuração que você tem.

Firewall

Domínios dos Firewalls

- Local



Fonte: https://blog.sucuri.net/wp-content/uploads/2222/03/04122016_DifferentiateFirewalls_02_LocalFireWalls_v3-650x450.jpg

Firewall

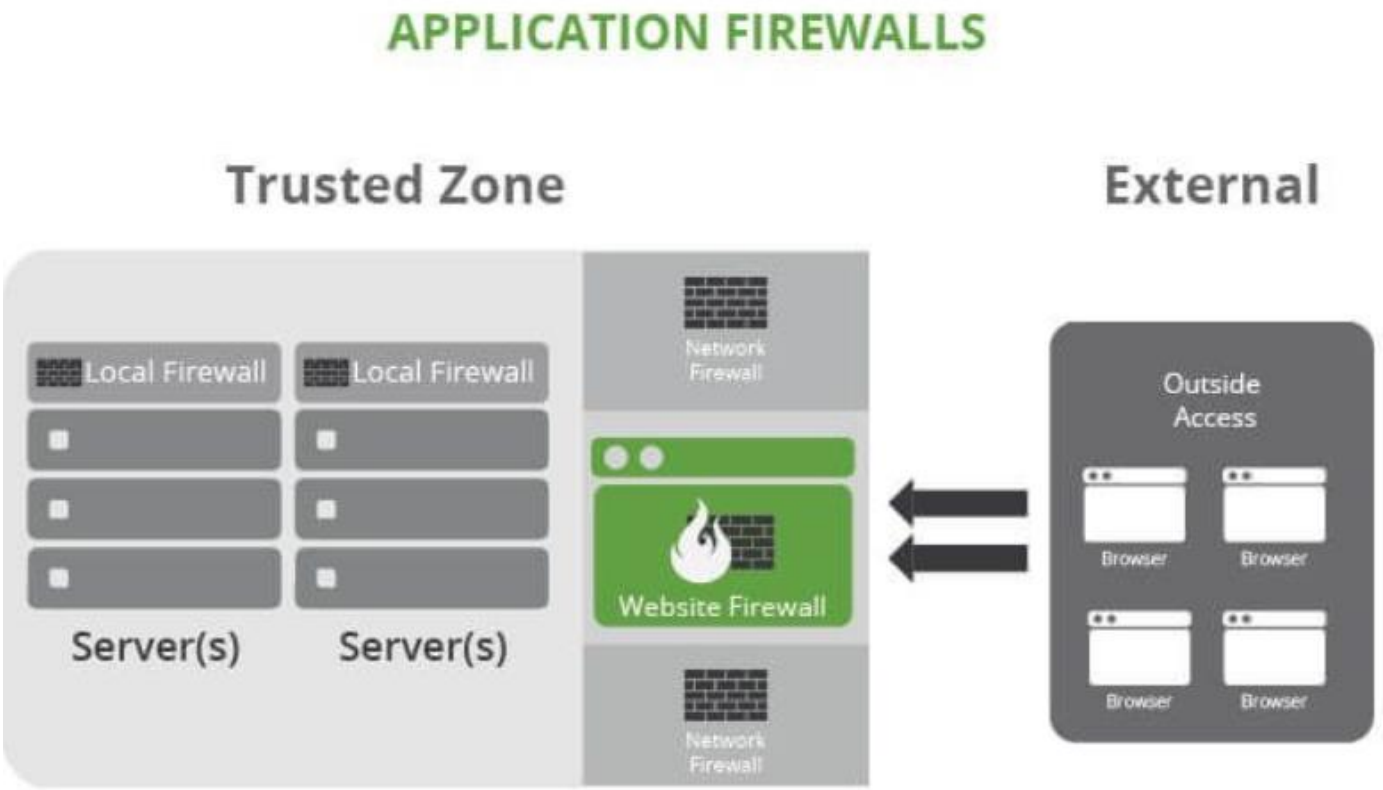
Domínios dos Firewalls

- Aplicação
  - Vão além dos metadados dos pacotes que estão sendo transferidos ao nível da rede e focam-se na transferência dos dados reais;
  - São projetados para compreender o tipo de dado permitido dentro de protocolos específicos (SMTP ou HTTP;

Firewall

Domínios dos Firewalls

- Aplicação



Fonte: https://blog.sucuri.net/wp-content/uploads/2222/03/04122016_DifferentiateFirewalls_03_ApplicationFireWalls_v3-650x451.jpg

Firewall

Tipos de Firewall

- Dependendo do tipo de conexão, podemos usar 2 tipos de firewall;
  - Hardware;
  - Software;

Firewall

Firewall por Hardware

- Geralmente vem incorporados aos roteadores e modens de banda larga;
- Uma rede com mais de uma máquina estará com todos PC's ligados a um roteador;
- Podemos utilizar políticas de bloqueio ou liberação de portas;
- Permite ajustes individuais em cada máquina.

Firewall

Firewall por Hardware

- Equipamentos específicos para este fim são mais comumente usados em aplicações empresariais;
- Roteadores domésticos também possuem algum nível de segurança;
  - Habilitação para acessar a rede.

Firewall

Firewall por Software

- Geralmente é parte integrante do Sistema Operacional;
- Uso de regras de segurança;
  - Pacotes aprovados;
  - Pacotes descartados;

Firewall

Firewall por Software

- Empresas geralmente utilizam computadores específicos como “guardiões da rede”;
- Podemos aplicar regras personalizadas para locais e máquinas;

Firewall

Firewall por Software

- Filtros podem ser usados para haver um maior controle;
- Filtros por portas;
- Filtros por aplicativos;

Firewall

Firewall e Antivírus

- Funciona como filtro de conexões;
- Portas abertas para uso, inclusive padrões;
- Nenhum firewall substitui software antivírus;
- Política de segurança do usuário;

Firewall

Packet Filtering Firewall

- Possui uma lista de regras de segurança que podem bloquear o tráfego baseado em protocolo de IP, endereço IP e/ou número da porta;
- Sob esse programa de gerenciamento de firewall, todo tráfego web será permitido, incluindo ataques;

Fonte: https://www.infowester.com/firewall.php

Firewall

Packet Filtering Firewall

- Podem ser estáticos ou dinâmicos;
- Estático
  - Dados são bloqueados ou liberados meramente com base nas regras, não importando a ligação que cada pacote tem com outro;
- Dinâmica
  - Os filtros consideram o contexto em que os pacotes estão inseridos para "criar" regras que se adaptam ao cenário, permitindo que determinados pacotes trafeguem, mas somente quando necessário e durante o período correspondente.

Firewall

Proxy

- Método utilizado para restringir os dados que trafegam na rede;
- Funciona como a passagem de uma rede para outra de uma aplicação específica;
- Computador “General”, que comanda todo o tráfego da rede;
- Filtra as solicitações permitindo acesso ou não (Falso Positivos).

Firewall

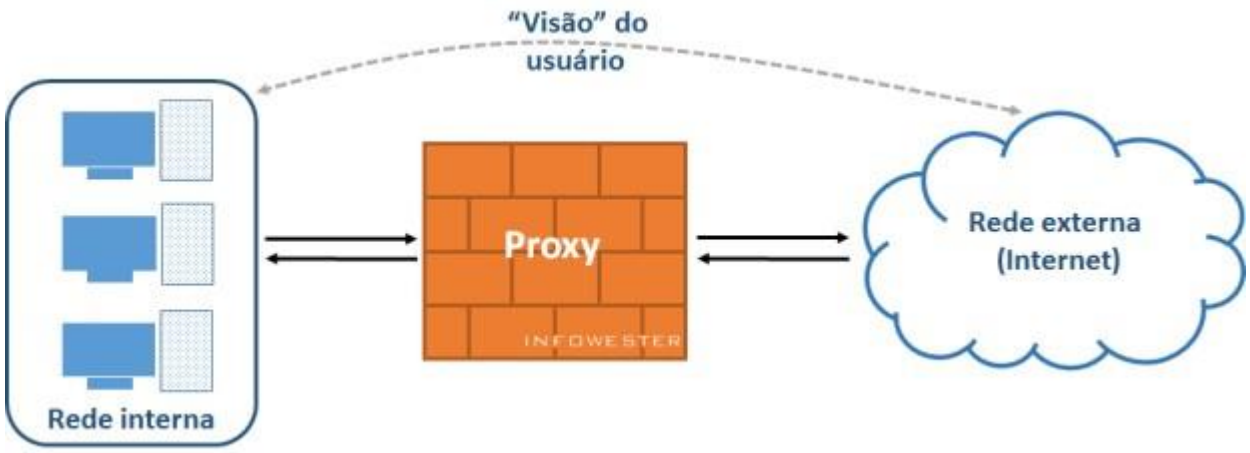
Proxy

- Todas requisições feitas ao servidor (o site que você quer acessar) passarão pelo seu proxy;
- O IP do proxy fica registrado no cache do seu destino e não o seu;
- Risco com os Hackers;
  - Invasão do computador;
  - Navegação com o seu IP.

Firewall

Proxy

- IP é nossa identificação na rede;
- O proxy faz a mascara do número legítimo;
- Pode proporcionar maior velocidade;
- Proxy Transparente.



Fonte: https://www.infowester.com/firewall.php

Firewall

WebProxy

- Esconde o seu IP real e lhe permite navegar anonimamente;
- Muito utilizado em empresas e universidade;

OpenProxy

- Tipo mais perigoso para os crackers;
- Instala um proxy na sua máquina e pode acessar quando quiser.

Redes Proxy

- São baseadas em códigos criptados que permitem a comunicação anônima entre os usuários (P2P).

Firewall

Firewall com inspeção de estado

- Permite ou bloqueia tráfego de acordo com o estado, a porta e o protocolo;
- Monitora toda atividade desde o momento em que uma conexão é aberta até que ela seja fechada;
- As decisões de filtragem são tomadas de acordo com as regras definidas pelo administrador e com o contexto.

Firewall

Deep Packet Inspection Firewall

- Examina o dado contido no pacote, de forma que pode procurar por ataques em camadas contidos nas aplicações;
- Funções Deep;
- Poder de processamento;
- Ataques.

Firewall

Application-Aware Firewall

- Neste caso, o firewall compreende alguns protocolos e pode analisá-los, de forma que as assinaturas ou regras podem endereçar alguns campos específicos no protocolo;
- Embora tenha essa proteção, alguns ataques podem passar despercebidos.

Firewall

Firewall de Gerenciamento unificado de ameaças (UTM)

- Um dispositivo UTM combina, de maneira flexível, as funções de um firewall com inspeção de estado e prevenção contra intrusões e antivírus;
- Ele também pode incluir serviços adicionais e, às vezes, gerenciamento em nuvem.

Firewall

Firewall de próxima geração (NGFW)

- A maioria das empresas está implantando firewall de próxima geração para bloquear ameaças modernas, como malware avançado e ataques na camada da aplicação;
- Novas funcionalidades
  - Recursos padrão de firewall;
  - Prevenção de invasão integrada;
  - Reconhecimento e controle da aplicação para detectar e bloquear aplicativos nocivos;
  - Atualização de caminhos para incluir feeds futuros de informação;
  - Técnicas para lidar com as ameaças à segurança em evolução.

Firewall

Firewall de próxima geração (NGFW)

- NGFW focado em ameaças
  - Saber quais recursos sofrem um risco maior com reconhecimento completo de contexto;
  - Reagir rapidamente a ataques com automação de segurança inteligente que define políticas e fortalece suas defesas de forma dinâmica;
  - Detectar melhor as atividades evasivas e suspeitas com a correlação de eventos de rede e endpoint;
  - Reduzir expressivamente o tempo entre a detecção e a limpeza com segurança retrospectiva que monitora continuamente atividades e comportamentos suspeitos mesmo após a inspeção inicial;
  - Facilitar a administração e reduzir a complexidade com políticas unificadas que oferecem proteção durante todo o ciclo de ataque.

Firewall

Funcionamento do Firewall

- Não é 100% eficiente;
- Hackers;
- Se especializam em quebrar essas regras;
- Disfarçam os pacotes;
- Hardware ou Software?

Firewall

Arquitetura do Firewall

- Podem ser implementados de várias formas para atender às mais diversas necessidades;
- Existem basicamente 3 formas
  - Arquitetura Dual-Homed Host;
  - Screened Host;
  - Screened Subnet.

Firewall

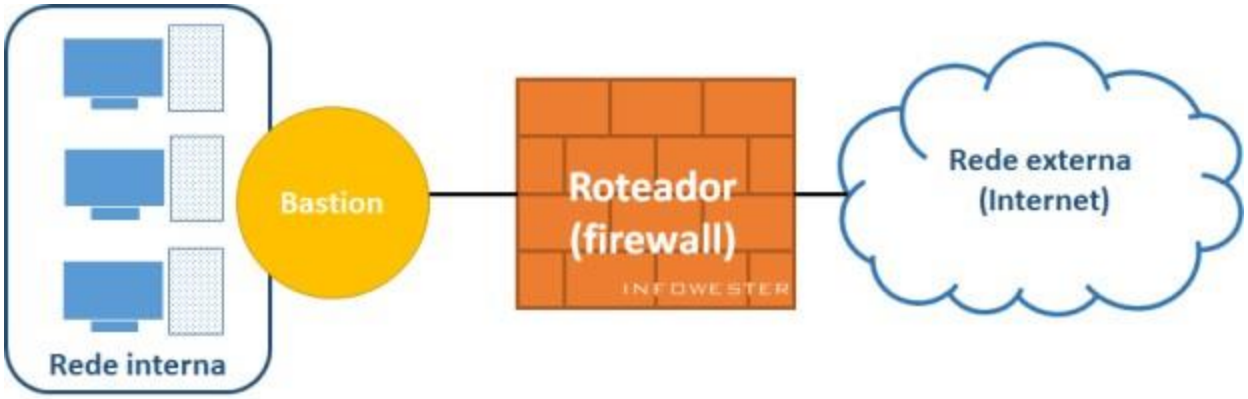
Arquitetura Dual-Homed Host

- Há um computador chamado dual-homed host que fica entre uma rede interna e a rede externa;
- Todo o tráfego passa por este firewall, não havendo acesso da rede interna para a rede externa (e vice-versa) diretamente;
- Utilizado principalmente com proxy.

Firewall

Arquitetura Screened Host

- Em vez de haver uma única máquina servindo de intermediadora entre a rede interna e a rede externa, há duas: uma que faz o papel de roteador (screening router) e outra chamada de bastion host;
- O bastion host precisa ser bem protegido.

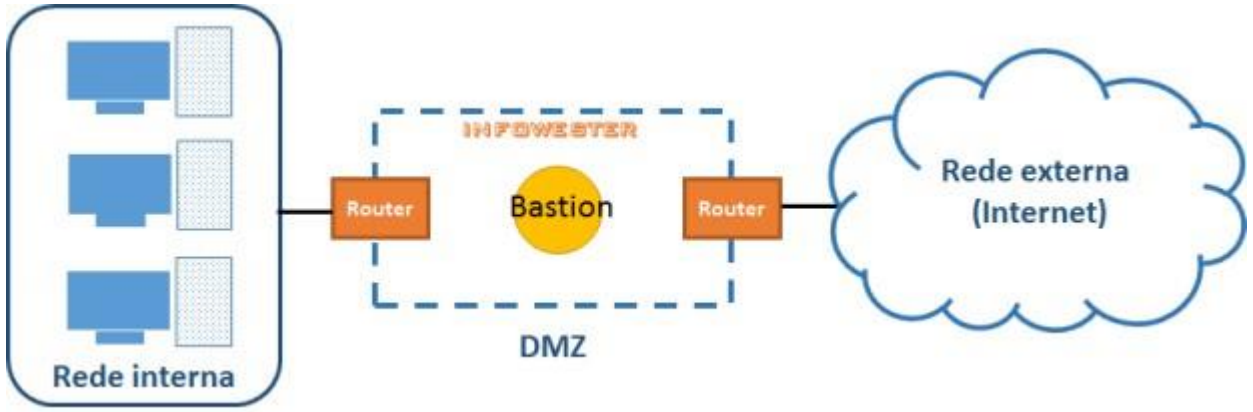


Fonte: https://www.infowester.com/firewall.php

Firewall

Arquitetura Screened Subnet

- Também conta com a figura do bastion host, mas este fica dentro de uma área isolada: DMZ;
- Demonstra mais segurança;
- Mais complexa e cara.



Fonte: https://www.infowester.com/firewall.php

Firewall

Funções do Firewall

- O que faz?
  - Impede que sua máquina seja invadida;
  - Impede que dados indesejáveis entrem no PC;
  - Bloqueia o envio de dados provenientes da sua máquina que não estejam especificados nas configurações.
- O que não faz?
  - Não protege contra programas baixados pelo usuário;
  - Não impede que programas de e-mail baixem spam;
  - Não impede que o usuário crie exceções errôneas que podem colocar o computador em risco.

Firewall

Limitações do Firewall

- Pode comprometer o desempenho da rede;
- Revisão periódica de políticas;
- Novos serviços ou protocolos podem não ser devidamente tratados por proxies já implementados;
- Um firewall pode não ser capaz de impedir uma atividade maliciosa que se origina e se destina à rede interna;
- Firewalls precisam ser "vigiados".

Firewall - Softwares

- ZoneAlarm
  - https://www.zonealarm.com/software/firewall/
- Sophos
  - https://www.sophos.com/en-us/products/next-gen-firewall.aspx
- Comodo
  - https://personalfirewall.comodo.com/best-free-firewall.html
- GlassWire
  - https://www.glasswire.com/
- Free Firewall
  - http://www.evorim.com/en/free-firewall
- Windows Firewall Control
  - https://sayrodigital.com/seguranca/melhores-firewalls-e-programas-para-proteger-sua-privacidade-de-2017-2/
- Firewall App Blocker
  - http://www.mediafire.com/file/ew451b4lql364if/fab_v1.4.zip
- Tinywall
  - https://tinywall.pados.hu/
- Anti NetCut3
  - http://www.tools4free.net/

Firewall - Softwares

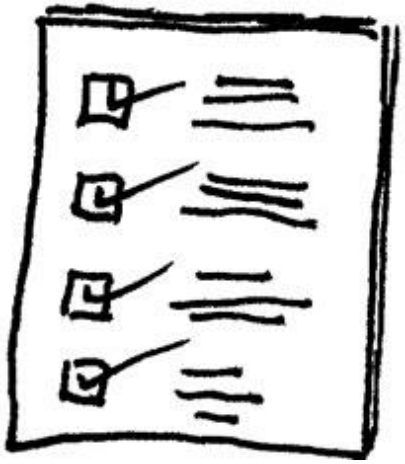
- PeerBlock
  - http://forums.peerblock.com/
- Little Snitch [Mac]
  - https://www.obdev.at/products/littlesnitch/index.html
- Private Eye [Mac]
  - https://www.obdev.at/products/littlesnitch/index.html
- ClearOS
  - http://www.clearos.com/clearfoundation/software/clearos-7-community
- IPCop
  - http://www.ipcop.org/
- OPNsense
  - https://opnsense.org/
- IPFire
  - http://www.ipfire.org/
- pfSense
  - http://www.pfsense.org/
- Smoothwall Express
  - http://www.smoothwall.org/

Atividade Prática - Firewall

- Pesquisar os tipos de ferramentas que podem ser utilizadas para implementar um Firewall;
- Deve conter o nome da ferramenta e uma descrição básica de seu funcionamento e plataforma;
- Pesquisar 2 tipos de roteadores com Firewall;

Resumo da Aula

- Revisão da Última Aula;
- Análise de Riscos e Ativos;
- Firewall;
- Atividade prática.



Referências Bibliográficas

- Site da Internet – TechMundo - https://www.tecmundo.com.br/firewall/182-o-que-e-firewall-.htm.
- Site da Internet – TechMundo - https://www.tecmundo.com.br/seguranca/3329-como-funciona-o-firewall-.htm
- Site da Internet – Cisco - https://www.cisco.com/c/pt_br/products/security/asa-firepower-services/index.html
- Site da Internet – Real Protect - https://realprotect.net/blog/seguranca-basica-o-que-e-seguranca-de-firewall/
- Site da Internet – Sucuri Blog - https://blog.sucuri.net/portugues/2016/04/diferencas-entre-firewalls-de-seguranca.html
- Site da Internet – InfoWester - https://www.infowester.com/firewall.php

Próxima aula

- Apresentação da versão 1.0 da política, gestão de riscos e firewall;
- Segurança em Aplicações;
- Segurança em Nuvem.