



FIREWALL

BACKUP

DAVI VENTURA CARDOSO PERDIGÃO
ERIC HENRIQUE DE CASTRO CHAVES

01

INTRODUÇÃO

02

FUNCIONAMENTO

03

IMPLEMENTAÇÃO

04

**DESAFIOS E
TENDÊNCIAS
FUTURAS**

05

CONCLUSÃO



01 | INTRODUÇÃO

FIREWALL

Firewalls são barreiras de segurança que protegem redes contra ameaças cibernéticas e acesso não autorizado. Eles monitoram e filtram o tráfego de dados, impedindo ataques e a propagação de malware. Além disso, ajudam a garantir conformidade regulatória e estabelecem um ambiente seguro para atividades comerciais. Existem diferentes tipos de firewalls, como os de rede, de host e de próxima geração. Em suma, firewalls são essenciais para a segurança e integridade dos dados em um mundo conectado.



BACKUP

O backup é uma prática essencial para garantir a segurança dos dados. Ele consiste em criar cópias de segurança armazenadas de forma segura, permitindo a recuperação dos dados em caso de perda ou danos. O backup evita interrupções nos negócios, prejuízos financeiros e danos à reputação. Existem diferentes métodos, como o backup local em mídias físicas e o backup em nuvem. Considerar fatores como frequência, criptografia e validação regular é fundamental para um sistema de backup eficaz. Em suma, o backup protege os dados e garante a continuidade das operações.





02

FUNCIONAMENTO

FIREWALL

INSPEÇÃO DO TRÁFEGO

Examina o tráfego de rede, analisando pacotes de dados individuais ou conexões inteiras

FILTRAGEM DE PACOTES

Verifica pacotes de dados com base em regras, que permitem ou bloqueiam pacotes (IP origem/destino, número de porta, protocolo)

VERIFICAÇÃO DE ESTADO

Utiliza a inspeção de estado para rastrear a comunicação e garantir apenas conexões legítimas

POLÍTICAS DE SEGURANÇA

Decidir como lidar com diferentes tipos de tráfego (permitir ou bloquear determinados protocolos, portas específicas, etc.)

REGRAS DE ACESSO

Conjunto de regras de acesso que determinam quais conexões são permitidas ou negadas

REGISTRO E MONITORAMENTO

Monitorar a atividade da rede, identificar potenciais ameaças e tomar medidas apropriadas para melhorar a segurança

BACKUP

IDENTIFICAÇÃO DOS DADOS

Identificar os dados que serão incluídos (arquivos, documentos, bancos de dados)

SELEÇÃO DO MÉTODO

Backup completo e backup incremental, etc. A escolha depende das necessidades e dos recursos

LOCAL DE ARMAZENAMENTO

Determinar onde o backup será armazenado (mídias físicas, removíveis, ou em nuvem)

AGENDAMENTO DO BACKUP

Definir uma programação regular para a realização do backup (períodos diários, semanais, mensais)

EXECUÇÃO DO BACKUP

Os dados são copiados do sistema original para o local de armazenamento escolhido

VERIFICAÇÃO DE INTEGRIDADE

É importante verificar se a cópia está íntegra e se pode ser restaurada. Algumas soluções oferecem essa verificação automática

BACKUP

ARMAZENAMENTO SEGURO

Deve ser armazenado em um local seguro, protegido contra acesso não autorizado, danos físicos ou falhas técnicas. Isso pode incluir o armazenamento em um local físico seguro, criptografia dos dados ou utilização de serviços de armazenamento em nuvem confiáveis

TESTES PERIÓDICOS

É recomendado realizar testes periódicos de restauração dos dados a partir do backup. Isso garante que o backup está funcionando corretamente e que os dados podem ser recuperados com sucesso, caso seja necessário



03

IMPLEMENTAÇÃO

FIREWALL

01 AVALIAÇÃO DE NECESSIDADES E REQUISITOS

02 SELEÇÃO DO TIPO DE FIREWALL

A

REDE (PERÍMETRO)

Instalado entre a rede interna e a Internet, atuando como primeira linha de defesa. Inspecciona o tráfego de entrada e saída, filtrando pacotes com base em regras de segurança predefinidas.

B

HOST

Implementada em um dispositivo específico, como um servidor ou uma estação. Controla o tráfego de rede para e do dispositivo em que está instalado, fornecendo uma camada adicional de segurança.

C

PRÓXIMA GERAÇÃO

Vão além da simples filtragem de pacotes. Oferecem recursos como inspeção profunda de pacotes, prevenção de intrusões, detecção de malware e gerenciamento de aplicativos.

FIREWALL

03 SELEÇÃO DO HARDWARE E SOFTWARE

04 CONFIGURAÇÃO DAS REGRAS E POLÍTICAS DE SEGURANÇA

05 TESTES E AJUSTES

06 MONITORAMENTO E MANUTENÇÃO CONTÍNUA

BACKUP

01 AVALIAÇÃO DE NECESSIDADES E REQUISITOS

02 SELEÇÃO DO MÉTODO E TECNOLOGIA

A

COMPLETO

Envolve a cópia de todos os dados selecionados em um determinado momento. Requer mais tempo e espaço de armazenamento.

B

INCREMENTAL

Apenas os dados que foram alterados desde o último backup são copiados. Isso reduz o tempo de backup e a quantidade de espaço de armazenamento necessário.

C

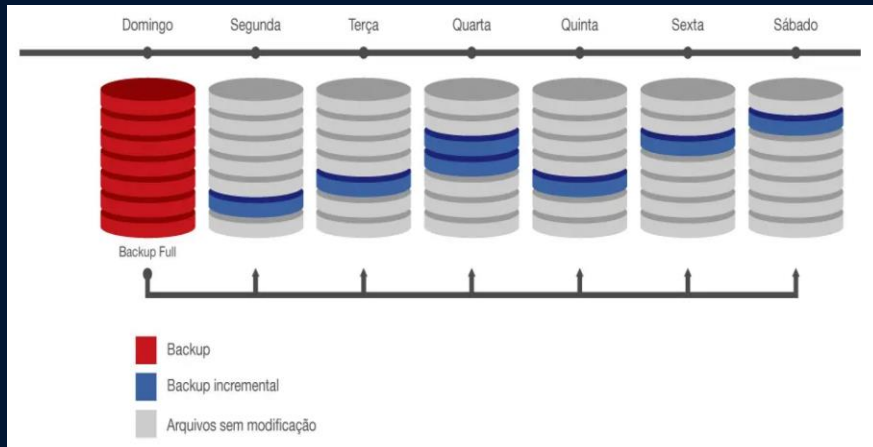
DIFERENCIAL

Copia apenas os dados alterados. No entanto, diferencia-se pelo fato de que cada backup diferencial contém todas as alterações desde o último backup completo.

BACKUP

INCREMENTAL

Figura 1: Processo de backup incremental.

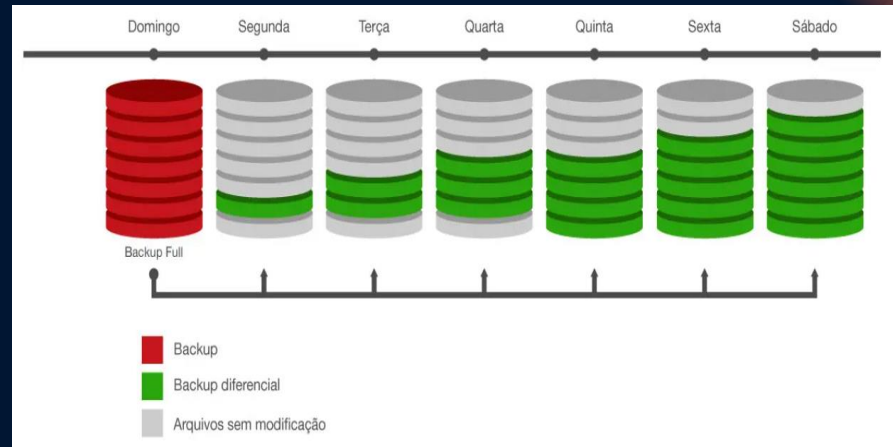


Fonte: ControleNet, 2020.



DIFERENCIAL

Figura 2: Processo de backup diferencial.



Fonte: ControleNet, 2020.

BACKUP

03 ESCOLHA DO SOFTWARE

04 PLANEJAMENTO DA INFRAESTRUTURA

05 DEFINIÇÃO DAS POLÍTICAS

06 TESTES E VALIDAÇÃO

07 MONITORAMENTO E MANUTENÇÃO CONTÍNUA



04

**DESAFIOS E
TENDÊNCIAS
FUTURAS**

FIREWALL

- **CRIPTOGRAFIA E INSPEÇÃO PROFUNDA DOS PACOTES**

análise mais detalhada e identificação de ameaças mesmo em comunicações criptografadas

- **FIREWALL DE APLICATIVO WEB (WAF)**

projetados especificamente para aplicações web contra ataques, como injeção de SQL, cross-site scripting (XSS) e de força bruta

- **INTEGRAÇÃO COM OUTROS SISTEMAS DE SEGURANÇA**

soluções de prevenção de perda de dados (DLP), sistemas de gerenciamento de eventos e informações de segurança (SIEM) e autenticação multifator. Permite uma resposta mais eficaz a incidentes

FIREWALL

- **FIREWALLS DEFINIDOS POR SOFTWARE (SD-WAN)**

implantados virtualmente em nuvem e fornecem segurança consistente em ambientes distribuídos e em expansão

- **SEGURANÇA DE DISPOSITIVOS MÓVEIS E IOT**

os firewalls estão se adaptando para fornecer recursos de segurança específicos, como filtragem de tráfego, gerenciamento de acesso e autenticação

BACKUP

- **VOLUMES CRESCENTES DE DADOS**
requer soluções escaláveis e eficientes em termos de armazenamento e transferência de dados
- **VELOCIDADE E DESEMPENHO**
requer soluções que possam lidar com altas taxas de transferência de dados e minimizar o impacto no desempenho dos sistemas em produção
- **COMPLEXIDADE DOS AMBIENTES DE TI**
soluções flexíveis e compatíveis com vários ambientes se tornam essenciais para garantir a integridade dos dados em diferentes plataformas

BACKUP

- **PROTEÇÃO CONTRA AMEAÇAS CIBERNÉTICAS**

soluções devem incluir recursos de segurança, como criptografia, autenticação e isolamento

- **BACKUP EM NUVEM E SERVIÇOS GERENCIADOS**

oferecem maior flexibilidade, escalabilidade e redução de custos em comparação com soluções tradicionais baseadas em infraestrutura própria



05 | CONCLUSÃO

- Firewalls atuam como barreira de proteção contra ameaças externas, previnem e detectam ataques cibernéticos;
- Backups permitem a recuperação rápida dos dados em caso de perdas ou violações, garantindo a continuidade dos negócios ;
- Estratégia em camadas fortalece a postura de segurança da organização;
- Proteção dos ativos de informação e resiliência dos negócios garantidas;

A combinação de firewalls e backups oferece uma estratégia de segurança abrangente, protegendo contra ameaças externas e permitindo a recuperação rápida dos dados em caso de perdas ou violações.

The background features a dark teal color with abstract, wavy, dotted patterns in a lighter teal shade. A bright orange and yellow lens flare is positioned in the center-left area.

OBRIGADO!

REFERÊNCIAS BIBLIOGRÁFICAS

- Carissimi, A., & Silva, F. V. (2015). **Fundamentos de Segurança da Informação**. Sagra.
- Cheswick, W. R., & Bellovin, S. M. (2003). **Firewalls and Internet Security: Repelling the Wily Hacker (2nd ed.)**. Addison-Wesley.
- Galante, A., & Zani, J. (2012). **Backup e Recuperação de Dados: Guia Prático para Administradores de Redes**. Novatec Editora.
- Guedes, A. V. L., & Santos, R. C. (2016). **Segurança da Informação: Firewall**. Novatec Editora.
- Rios, E. (2014). **Backup & Recovery: Implementação e Administração de Ambientes de Backup**. Brasport.
- Rouse, M. (2020). **What is a Firewall? Definition, Types, and How They Work**. TechTarget.
- Tanenbaum, A. S., & Bos, H. (2014). **Modern Operating Systems (4th ed.)**. Pearson.