Aula 6

Segurança em Sistemas de Informação

Prof. Douglas Eduardo Basso

1

Conversa Inicial

2

Conversa Inicial

- **Nesta aula, vamos falar sobre servidores proxies, suas funções e funcionamento, o processo de tradução de endereços (NAT) e conceitos de sistemas de detecção de ataques e detecção de intrusos. Também será abordado o controle de conteúdo e, em seguida, veremos as proteções *antimalware.* Por fim, estudaremos os conceitos de *firewall*, suas características, estrutura e os *firewalls* de nova geração, bem como as soluções UTM**

3

Proxy

4

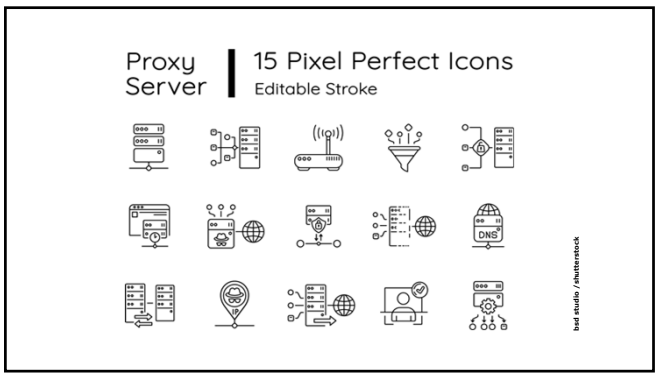
Proxy

- **O proxy é um servidor que age como um intermediário para requisições de clientes solicitando recursos de outros servidores. Um cliente conecta-se ao servidor proxy solicitando algum serviço, como um arquivo, conexão, página web ou outros recursos disponíveis de um servidor diferente, e o proxy avalia a solicitação, como um meio de simplificar e controlar sua complexidade**

5

- **Funções do Proxy:**
  - **Firewalls**
  - **Filtros de conteúdo**
  - **Contorno de filtros de conteúdo**
  - ***Caching***
  - **Segurança**
  - **Compartilhamento e centralização de conexões de internet**

6

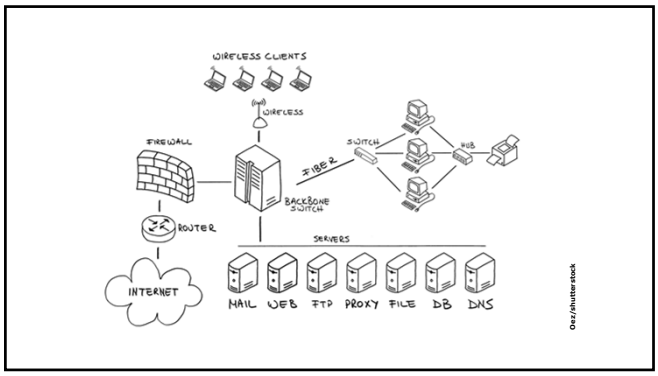


7

Funcionamento do Proxy

- **Um proxy fica à frente do cliente ou de uma rede de clientes e faz a intermediação do tráfego. Ele é um equipamento com uma interface conectada diretamente à internet e possui um endereço IP**
- **Com uma estrutura com proxy, os clientes se comunicam apenas com o proxy e, de antemão, o servidor proxy encaminha toda comunicação à internet**

8



9

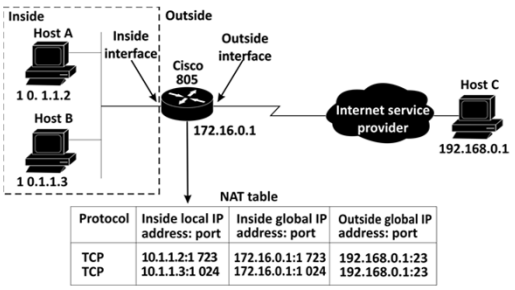
Tradução de Endereços (NAT)

- **NAT (network address translation) apresenta um conceito mais específico que fazer uma correlação de endereços lógico. Na prática, é uma tradução entre endereços IPs de redes diferentes.**
- **Normalmente, essa tradução envolve vários endereços de rede privados que se traduzem em endereços públicos através da alteração das informações de rede e informações de endereço encontradas no cabeçalho IP dos pacotes de dados**

10

- **Tipos de NAT:**
  - **Sobrecarga ou Tradução de Endereço Portuário (PAT)**
  - **NAT dinâmico**
  - **NAT estático**
  - **Redirecionamento de portas**

11



12

IDS/IPS

13

IDS/IPS

- Os sistemas de detecção de intrusos (IDS) permitem fazer uma verificação com detalhes de todo o tráfego de rede em diversos pontos da estrutura. É possível identificar vários tipos de atividade maliciosa
- Já os sistemas de detecção de intrusos (IPS) são sistemas que desempenham uma função de controle, e têm no firewall o seu complemento
- Falaremos de firewall mais adiante

14

Tipos de IDS

- Existem dois tipos de implementação de sistemas IDS:
  - Host Based IDS (HIDS)
  - Network Based IDS (NIDS)

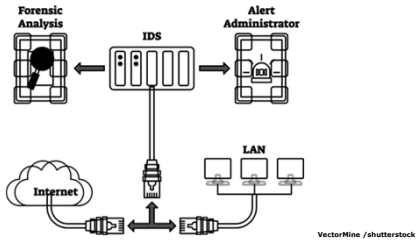
15

Funcionamento IDS

- Ao localizar um evento que atente contra a política de segurança, o IDS faz a análise e armazena um registro detalhado do evento malicioso ao administrador de rede

16

Intrusion Detection



17

Tipos de IPS

- O IPS tem alguns métodos de detecção para identificar as explorações e tentativas de invasão, são elas:
  - Detecção baseada em assinatura
  - Detecção baseada em anomalias
  - Detecção baseada em diretivas

18

Ações dos IPS

- Faz envios de alertas e alarmes ao administrador de rede
- Elimina ameaças
- Executa o bloqueio imediato do tráfego perigoso à rede, através do endereço de origem do fluxo de dados
- Reativa a conexão de rede ao interpretar tráfegos legítimos como ameaças

19

Diferenças entre IDS e IPS

- Levando em conta as características dos dois dispositivos, podemos dizer que a maior diferença entre eles se encontra no elevado grau de autonomia do IPS, o que tende a tornar sua utilização a escolha mais eficiente e eficaz

20

Controle de conteúdo

21

Controle de conteúdo

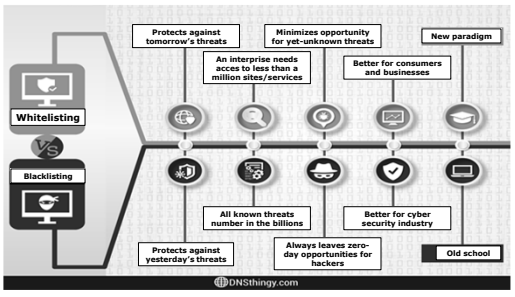
- Controlar o conteúdo da Internet é uma das camadas dessa segurança da informação. Ou seja, é essencial aplicar um controle de conteúdo, um filtro *web* de acordo com as políticas de segurança empresariais

22

Lista branca e lista negra

- As listas brancas e negras basicamente consistem, respectivamente:
  - Na permissão de acessos a determinados endereços de Internet
  - Na proibição de acessos a determinados endereços de Internet
- Isto é, uma estratégia que restringe acessos a determinados sites, aplicativos, conteúdos e categorias

23



24

Funcionamento dos filtros de conteúdo

- A aplicação desses filtros pode funcionar usando uma lista branca ou uma lista negra
- A lista branca faz a permissão de acesso somente a sites especificamente escolhidos por quem criou e elaborou a lista
- A lista negra faz a restrição do acesso a sites e aplicações indesejáveis conforme determinado pelos padrões nela criados e nos filtros de palavras-chave

25

- Os filtros de conteúdo de Internet também são utilizados como ferramenta de prevenção de *malwares* e vírus, pois bloqueiam o acesso a sites que costumam hospedar esse tipo de ameaças, sites com conteúdo pornográfico, jogos de azar, terrorismo, entre outros

26

- Benefícios dos filtros de conteúdo:
  - Aumento da segurança e proteção
  - Segurança e proteção contra conteúdos impróprios
  - Melhoria de produtividade de colaboradores
  - Confiabilidade de acesso
  - Relatórios de acesso
  - Categorização de conteúdo

27

naum/shutterstock

28

Uso de internet

- A utilização de maneira livre e liberada da Internet pode criar diversos reflexos positivos e negativos para as organizações, tudo vai depender do modelo de negócio, do cenário de utilização, do perfil dos colaboradores, entre outros fatores

29

Proteção *antimalware*

30

Proteção antimalware

- As proteções *antimalware* são os elementos especiais de qualquer solução de segurança da informação para organizações. Os objetivos desse recurso são identificar ações e arquivos maliciosos e fazer o bloqueio, impedindo que quaisquer danos ocorram com os equipamentos de TI

31

Funcionamento da proteção *antimalware*

- De maneira geral, esses *softwares* utilitários fazem a análise de determinado arquivo, código, plugin, aplicação ou amostra, investigando se há algum tipo de risco ou perigo

32

Tipos de detecção *antimalware*

- Os métodos e técnicas de detecção de vírus e *malwares* são elencados de diferentes maneiras:
  - Detecção baseada na assinatura
  - Detecção baseada em heurística
  - Detecção comportamental
  - Detecção baseada em nuvem
  - Detecção de malwares invisíveis

33

Recomendações contra *malwares*

- Utilizar proteção *antimalware*
- Proteger telefones celulares
- Utilizar aplicações legítimas e genuínas
- Identificar detalhes de desenvolvimento
- Fazer avaliações de utilizadores

34

35

Recomendações contra *malwares*

- Número de downloads executados
- Solicitação de permissões
- Links inseguros
- Atualização de sistemas operacionais e *softwares*
- Cuidado com redes sem fio
- Utilização de dispositivos removíveis

36

37

Futuro das proteções *antimalware*

- **A inteligência artificial e o aprendizado de máquinas são os novos elementos dos avanços da tecnologia *antimalware*. A inteligência artificial traz a possibilidade de máquinas executarem algumas tarefas que não tenham sido pré-programadas especificamente**

38

Futuro das proteções *antimalware*

- **O aprendizado de máquina é outro elemento de programação capaz de fazer reconhecimento de padrões em dados novos. Posteriormente, faz a classificação desses dados de maneira que o aprendizado "ensine" as máquinas a tomar decisões**

39

Futuro das proteções *antimalware*

- **Seguindo essa linha de evolução, outras duas formas relativamente novas de *malware* contribuíram para o avanço e desenvolvimento de métodos de detecção sem assinatura:**
  - **Exploits**
  - **Ransomware**

40

***Firewall* e *firewall* de nova geração**

41

Firewall

- **Um firewall é uma solução (*software* e/ou *hardware*) que tem a função de reforçar a segurança de informação entre uma rede privada interna segura e uma rede insegura e não muito confiável como a Internet. O firewall tem a responsabilidade de criar e manter uma barreira de segurança para todos os dados trafegados pela rede, criando um obstáculo contra ameaças**

42

Estrutura de firewall

- **Em relação à sua estrutura, um firewall pode ser um computador, um servidor, um roteador, um *mainframe* ou a combinação destes elementos. Normalmente, um *firewall* é implementado no ponto onde rede interna e a rede externa se cruzam; fica no chamado *perímetro da rede* e tem a função de controlar e filtrar todo o tráfego**

43

Soluções UTM

- **O UTM é, teoricamente, uma evolução do *firewall* tradicional, unindo a execução de várias funções de segurança em um único dispositivo: firewall, prevenção de intrusões de rede, antivírus, VPN, filtragem de conteúdo, balanceamento de carga, geração de relatórios informativos e gerenciais, funções como IPS e muito mais**

44

Benefícios do UTM

- **Reduz o custo e os gastos com a internet através de controle do uso dos *links* de dados**
- **Melhora o desempenho do *link* de Internet com filtros de navegação web**
- **Aumenta a disponibilidade dos *links* de Internet com o balanceamento destes**

45

Benefícios do UTM

- **Protege os usuários com antivírus de navegação**
- **Conexão de qualquer lugar e rede com acesso seguro aos dados corporativos com VPN**
- **Integração de unidades remotas com maior segurança e confiabilidade**

46

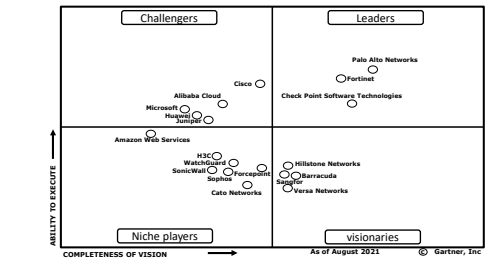
Funcionalidades das soluções UTM

- **Os *firewalls* UTM são uma evolução dos *firewalls* tradicionais. Um produto de segurança abrangente que inclui proteção contra várias ameaças, em uma plataforma unificada com diversas outras funcionalidades**
- **Vamos apresentar algumas dessas funcionalidades:**

47

- **Controle de aplicações**
- **Antivírus**
- **Filtragem de conteúdo**
- **Antispam**
- **Acelerador de WAN**
- **VPN**
- **IPS**
- **DLP**
- **Relatórios gerenciais**

48



fonte : https://powerbi.microsoft.com/pt-pt/blog/gartner-recognizes-microsoft-as-a-leader-in-analytics-and-bi-platforms-for-11-consecutive-years/

49

Fabricantes de UTM

- **Cada fabricante tem seus pontos fortes e fracos. A qualidade e desempenho dos produtos variam amplamente, porém, a partir de uma perspectiva puramente de características, eles são todos iguais. As diferentes abordagens de inspeção de aplicativos, antivírus, IPS podem explicar seu desempenho ou precisão, porém não muda o fato de que o núcleo de recursos é o mesmo**

50