Estratégia Concursos

Aula 00

SEFAZ-RJ (Auditor - Área TI) Arquitetura e Sistemas Operacionais

Autor:
Evandro Dalla Vecchia Pereira

15 de Dezembro de 2022

Índice

SERVIÇO DE RESOLUÇÃO DE NOMES (DNS)

Conceitos

Os equipamentos conectados à Internet necessitam de um endereço IP. Através dele conseguimos identificar "quem" acessou determinado conteúdo ou realizou determinada ação, por exemplo. Mas, quem "gosta" de números é a máquina! Nós, meros mortais, temos dificuldade em memorizar muitos números (endereços IP, por exemplo). E os servidores (Web, de e-mail, de arquivos etc.) são acessados através do endereço IP que foi alocado a eles.

Uma solução para isso foi a criação de um serviço que "faz o meio de campo", ou seja, traduz nomes (bem mais fáceis de memorizar) para os endereços IP equivalentes. É o famoso *Domain Name System* (DNS). Assim, é possível acessar uma página Web através de um nome, sendo que de forma transparente ao usuário, esse nome é traduzido ao endereço IP onde se encontra o servidor Web que contém a página e a requisição é realizada a esse servidor.

Um conceito mais formal (Tanenbaum) é o seguinte: o DNS é definido como um esquema hierárquico de atribuição de nomes baseado no domínio e de um sistema de banco de dados distribuído. O DNS atua na camada de aplicação e utiliza como protocolo de transporte o UDP para as consultas/respostas e o TCP para transferências de zonas (entre servidores DNS). Tanto com o UDP como com o TCP, a porta utilizada é a 53.

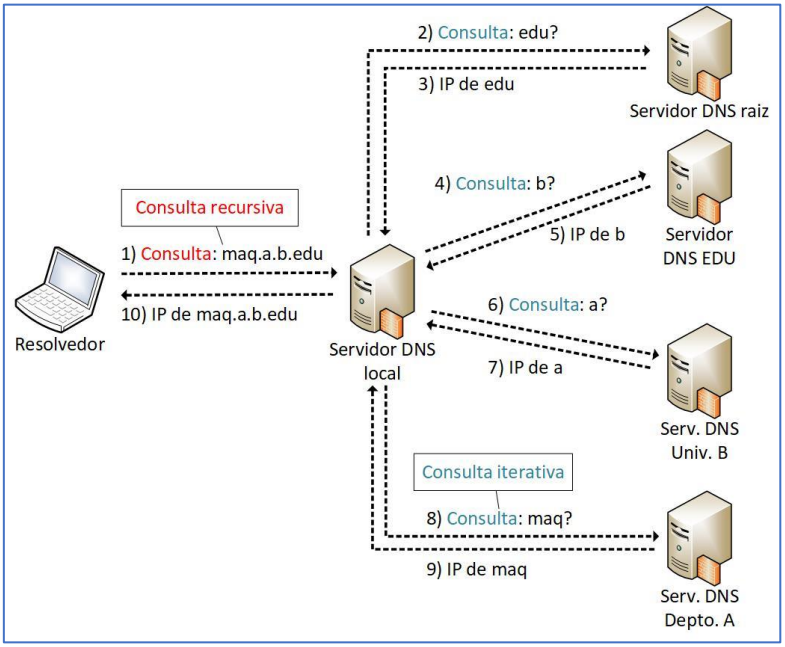
Abaixo é mostrada uma tela com a resposta para o comando *ipconfig /all*, mostrando, entre outras informações, os servidores DNS locais.

Um passo a passo de uma solicitação de um cliente DNS (seu computador, por exemplo) a um servidor DNS local é mostrado a seguir.

O aplicativo (ex.: navegador) chama o **resolvedor**, passando o nome que se deseja a tradução para endereço IP;

1) O resolvedor realiza uma consulta ao servidor DNS local;
2) O servidor DNS local responde ao resolvedor;
3) O resolvedor informa o endereço IP ao aplicativo.

Ok, mas e se for um nome que o servidor DNS local não conhece? Seja porque nunca foi solicitado, ou porque tal informação já não se encontra mais em sua *cache*? Bom, aí é melhor olhar a figura abaixo.



A consulta realizada ao servidor DNS local é chamada **consulta recursiva**, pois o resolvedor envia a consulta e recebe a resposta final, sem precisar enviar uma consulta a cada servidor DNS de nível superior. Já em **consultas iterativas**, a resposta à requisição DNS pode ser parcial, obrigando o solicitante a encaminhar novas requisições DNS a outros servidores até obter a resposta final desejada.

A delegação de domínios de mais alto nível (*top-level domain* - TLD), tais como “.com”, “.edu”, “.br”, “.mx”, entre outros, é de responsabilidade da ICANN (*Internet Corporation for Assigned Names and Numbers*). Para o Brasil (TLD .br), o responsável é o CGI.br[1], conforme podemos ver abaixo.

[1] Base de dados de domínios TLD disponível em <http://www.iana.org/domains/root/db>.

.booking	generic	Booking.com B.V.
.boots	generic	THE BOOTS COMPANY PLC
.bosch	generic	Robert Bosch GMBH
.bostik	generic	Bostik SA
.boston	generic	Boston TLD Management, LLC
.bot	generic	Amazon Registry Services, Inc.
.boutique	generic	Binky Moon, LLC
.box	generic	NS1 Limited
.bq	country-code	Not assigned
.br	country-code	Comite Gestor da Internet no Brasil
.bradesco	generic	Banco Bradesco S.A.
.bridgestone	generic	Bridgestone Corporation
.broadway	generic	Celebrate Broadway, Inc.
.broker	generic	DOTBROKER REGISTRY LTD

Note que existe um TLD ".bradesco", relacionado ao Banco Bradesco. Faça um teste em seu navegador: digite "bradesco.com.br" e "bradesco.bradesco". Qual o resultado? No momento em que testei, ambos direcionam para uma nova URL: "https://banco.bradesco/html/classic/index.shtm", pertencente ao domínio ".bradesco".

Então, se alguém quiser registrar um domínio com o sufixo ".br", pode verificar se há disponibilidade desse domínio, através da URL <http://registro.br>, que é uma **entidade de registro**. Se houver, pode realizar a solicitação, efetuar o pagamento e informar as configurações solicitadas pelo CGI.br sobre o provedor onde a página será hospedada (servidores DNS).

Na medida em que novos domínios são cadastrados, eles são propagados pela Internet e em poucas horas todos os servidores DNS do mundo são capazes de traduzir o domínio para o endereço IP equivalente onde está hospedado o serviço. A figura abaixo mostra a estrutura DNS, desde a raiz, os TLDs, domínios de segundo e terceiro níveis e o computador lá na ponta.

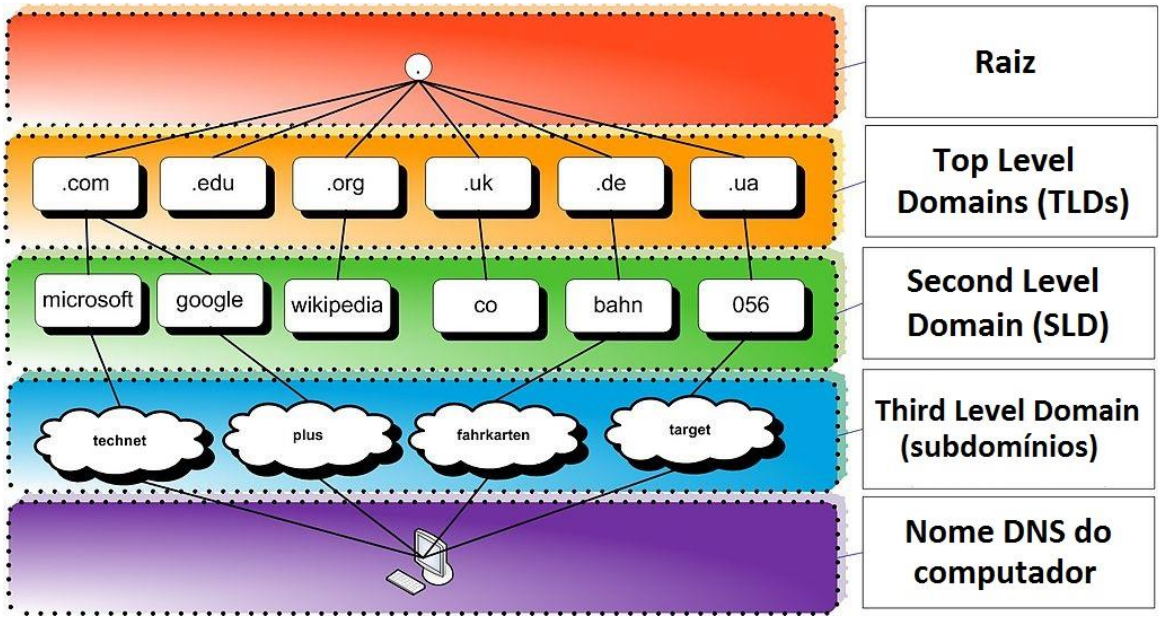
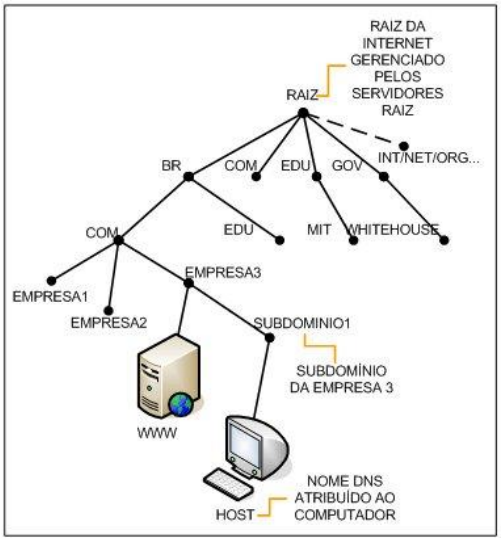


Figura adaptada de https://hugoemiliano.info/2017/07/05/servicos-e-protocolos-dns/

Por exemplo, a URL <www.microsoft.com> pode ser compreendida da seguinte forma:

- .com: Top Level Domain (TLD);
- microsoft: Second Level Domain (SLD);
- **não há terceiro nível (subdomínio) para essa URL;**
- www: Nome do computador ("www" é um nome padrão para servidores Web).

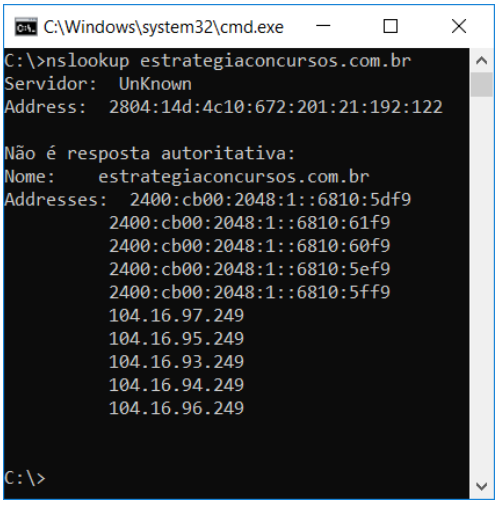
Abaixo uma outra figura, mostrando um exemplo com subdomínio. Nesse caso a URL completa para acessar o "HOST" seria <HOST.SUBDOMINIO1.EMPRESA3.COM.BR>.



Fonte: http://www.abusar.org/dns_como.html

Para não haver consultas constantes a servidores DNS de mais alto nível (mais próximos da raiz, ou a própria raiz), os servidores DNS possuem uma memória cache[2], permitindo a resposta imediata ao solicitante (quando tiver a informação). Quando não tiver a informação, deve-se buscar nos níveis superiores.

É possível também, em sistemas operacionais como Windows e Linux, configurar em traduções fixas, de domínio para endereço IP (arquivo hosts, como já vimos). Uma ferramenta comum ao Windows e Linux para obter informações sobre registros de DNS de um determinado domínio, host ou IP é o *nslookup* (vale a pena utilizá-la, pois há questões que cobram o seu conhecimento):

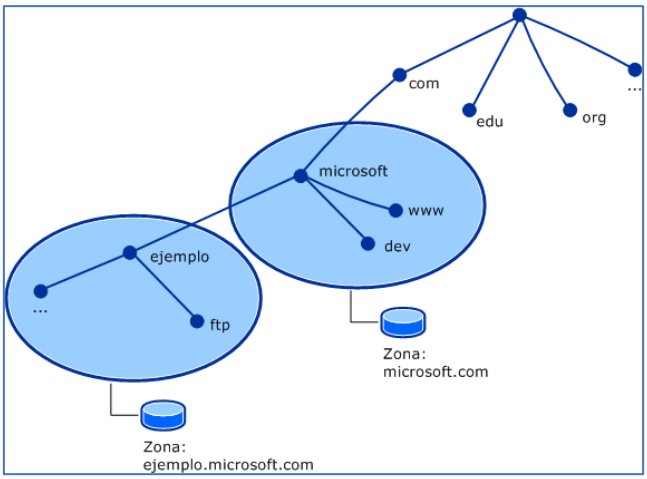


Em relação ao padrão Unix, o servidor de nomes mais conhecido é o BIND, que é conjunto de softwares DNS, que contém um *daemon* servidor de nomes (*named*), uma biblioteca *resolver* (nosso "resolvedor") e outros programas. O Bind é mantido pela ISC (*Internet Software Consortium* - <https://www.isc.org/downloads/bind/>).

O arquivo de configuração para o resolvedor é o resolv.conf e fica localizado em /etc. Trata-se de um arquivo em texto plano usualmente criado pelo administrador ou por aplicações que gerenciam tarefas de configuração.

O espaço de nomes do DNS é dividido em zonas não superpostas. Cada zona está associada a um ou mais servidores de nomes, que mantêm o banco de dados para a zona. A figura abaixo mostra tal conceito:

[2] Responsável por armazenar consultas recentes, respondendo ao solicitante diretamente.



Fonte: http://un-newbie.blogspot.com.br/2014/03/introduccion-transferencia-de-zona-y.html

Os **registros de recursos (RRs)** são o banco de dados do DNS. São compostos por tuplas de cinco campos: <nome_domínio, tempo_vida, classe, tipo, valor>, descritos abaixo:

- Nome: chave de pesquisa primária para atender as consultas;
- Tempo_vida (TTL): tempo que deve permanecer em *cache* (em segundos);
- Classe: geralmente IN (Internet);
- Tipo: SOA, A, AAAA, etc. (tabela a seguir);
- Valor: número, nome de domínio ou *string* ASCII.

Tipo	Significado	Valor
SOA	Início de autoridade (*Start of Authority*).	Parâmetros para essa zona.
A	Endereço IPv4.	Inteiro de 32 bits.
AAAA	Endereço IPv6.	Inteiro de 128 bits.
MX	Troca de mensagens de e-mail.	Prioridade, domínio disposto a aceitar e-mails.
NS	Servidor de nomes.	Nome de um servidor para este domínio.
CNAME	Nome canônico (*alias* = apelido).	Nome de domínio.
PTR	Ponteiro (usado para o DNS reverso[3])	Nome alternativo de um end. IP.
SPF	Estrutura de política do transmissor.	Codificação de texto da política de envio de mensagens de e-mail.
SRV	Identifica computadores que hospedam serviços específicos.	Host que o oferece.
TXT	Informações sobre um servidor, rede, *datacenter*, etc.	Texto ASCII com descrições.

[3] Envia um endereço IP como consulta e recebe o nome como resposta.

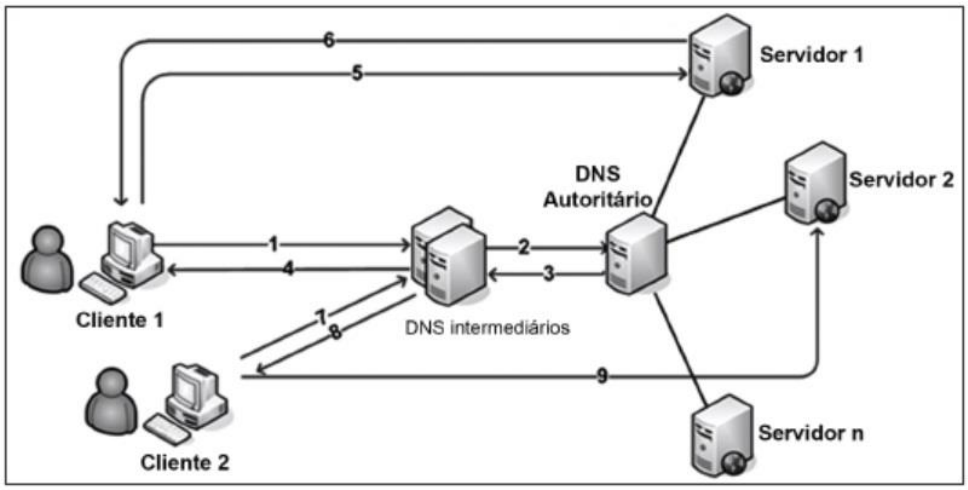
Outro conceito cobrado em provas de concurso é a resposta autoritativa ou não-autoritativa. Vejamos suas definições a seguir.

Um servidor DNS autoritativo possui autoridade sobre um nome de domínio. O DNS autoritativo dita qual será o apontamento da tabela de DNS do seu sítio. Uma **resposta autoritativa**[4] de um servidor é a garantia de estar atualizada, enquanto uma **resposta não-autoritativa** pode estar desatualizada (*cache* com informações antigas, por exemplo). Existe um percentual elevado de respostas não autoritativas que estão perfeitamente corretas, casos em que mudanças de endereçamento são raros.

Servidores primários e secundários são autoritativos para os seus domínios, porém não o são sobre informações a respeito de outros domínios mantidas em *cache*. **Servidores *caching-only* nunca são autoritativos**, mas possuem a vantagem de reduzir a quantidade de tráfego DNS na rede.

Uma política que pode ser adotada para equilibrar as vantagens de cada técnica é colocar um servidor secundário ou *caching-only* em cada segmento de rede ou sub-rede. É admissível uma máquina ser servidora primária para um domínio e servidora secundária para outros domínios.

Para não sobrecarregar servidores, existe uma abordagem popular e simples: o **balanceamento de carga por DNS**. Considere a figura abaixo e o passo a passo mostrado na sequência.



Fonte: Prova FCC – 2016 – ELETROSUL – Profissional de Nível Superior/Informática

1. Cliente 1 tenta acessar o *site*, é realizada uma pesquisa no DNS local para determinar qual é o endereço IP correspondente;
2. O pedido de endereço chega ao servidor de DNS autoritário do domínio;
3. A primeira vez que esta consulta é feita, o servidor DNS remoto pode retornar todos os registros de endereços que ele tem para o site;
4. O servidor DNS local, em seguida, determina o endereço de registro para retornar ao cliente;
5. Se todos os registros são retornados, o cliente utilizará o primeiro que lhe é atribuído;
6. O servidor responde ao cliente e atende ao pedido;
7. A cada pedido, o algoritmo Round Robin roda os endereços e retorna pela ordem em que eles estão;

8. Cada consulta DNS irá resultar em um cliente usando um endereço diferente;
9. Esta rotação de endereços irá distribuir pedidos para os servidores.

QUESTÕES COMENTADAS

1. **(CESPE/TRE-GO - 2015) Quando o cliente de um serviço DNS (domain name system) envia um pedido de resolução de nomes a um servidor, esse pedido é transportado pelo TCP, que se encarrega de buscar os servidores DNS primário e secundário.**

Comentários:

O DNS atua na camada de aplicação do TCP/IP e, como já vimos, o protocolo de transporte utilizado para requisições de DNS é o UDP. Para a transferência de zonas de DNS, o protocolo de transporte utilizado é o TCP. Portanto, a questão está **errada**.

2. **(FCC/CNMP - 2015) O serviço de nome de domínios (DNS) possui uma arquitetura do tipo cliente/servidor na qual a base de dados é distribuída por toda internet. Nessa arquitetura, o acesso ao servidor DNS para buscar o relacionamento IP/Domínio é feito pelo cliente que é o**

A) Browser.

B) DNS Cache.

C) DNS Resolver.

D) DNS Searcher.

E) Gateway.

Comentários:

Conforme vimos, o browser (navegador) não resolve o nome! Supondo que uma URL seja solicitada através de um browser, o "resolvedor DNS" terá o papel de resolver o DNS (o próprio nome já diz isso). Pode ser através do arquivo hosts (máquina local) ou através de solicitação ao servidor DNS "mais próximo" (mais comum - geralmente o servidor DNS utilizado pelo provedor de acesso à Internet). Se o servidor DNS tiver a informação em cache, ele responde, senão faz uma busca nos servidores superiores na hierarquia DNS, atualiza sua cache e responde ao "resolvedor". Portanto, a **alternativa C** está correta e é o gabarito da questão.

3. **(CESPE/FUB - 2015) O protocolo DNS (domain name service), localizado no nível de aplicação da camada de transporte do TCP, é responsável pelo mapeamento de nomes e de endereços.**

Comentários:

O DNS está localizado na camada de aplicação. A questão misturou "nível de aplicação da camada de transporte do TCP". Portanto, a questão está **errada**.

4. (FGV/TCE-SE - 2015) Um programa precisa simular o comportamento de um cliente DNS. Para funcionar adequadamente, o programa precisa enviar as consultas para um servidor DNS, especificamente para a sua porta:

A) udp/23

B) icmp/34

C) tcp/22

D) ip/50

E) udp/53

Comentários:

Como já vimos, o protocolo de transporte utilizado para consultas DNS é o UDP e a porta é a 53. Essas informações devem estar enraizadas em seu cérebro! Para a transferência de zonas de DNS, é utilizado o TCP (na mesma porta: 53) como protocolo de transporte. Portanto, a **alternativa E** está correta e é o gabarito da questão.

5. (CESPE/TRE-MT - 2015) Acerca do servidor DNS/BIND (Domain Name System/Berklay Internet Domain), cuja funcionalidade é resolver nomes da rede, assinale a opção correta.

A) Cada domínio tem seus registros de recursos e o registro de domínio denominado NS (name server), o qual é utilizado para definir propriedades básicas do domínio e sua zona.

B) Um servidor DNS utiliza LDAP para fazer armazenamento das zonas de domínio para uma rápida resolução de um nome.

C) O BIND, que utiliza a porta 53, é um programa de código aberto utilizado pela maior parte dos servidores DNS.

D) Os domínios de um servidor DNS são organizados na Internet sobre uma estrutura de dados do tipo lista encadeada, sendo o primeiro elemento da lista um ponto.

E) O protocolo HTTP implementa, por padrão, um servidor de resolução de nomes amplamente utilizado na Internet conhecido como DNS.

Comentários:

Para quem não está acostumado com essa parte de servidores, memorize o seguinte: servidor DNS é quase sinônimo de BIND! Se você ainda não o conhece e não leu sobre ele, recomendo uma passada rápida na URL https://www.isc.org/downloads/bind/. Portanto, a **alternativa C** está correta e é o gabarito da questão.

6. (CESPE/TRE-PI - 2016) É correto afirmar que o DNS (Domain Name System)

A) utiliza bancos de dados centralizados e em rede para armazenar suas tabelas de identificação e rotas.

B) provê resolução de nomes independentemente do protocolo de transporte.

C) provê serviço de distribuição de carga entre servidores web replicados.

D) tem interação direta com os usuários, por ser uma aplicação web.

E) utiliza o paradigma P2P na camada de aplicação para prover apelidos (aliasing) de hospedeiros.

Comentários:

Uma das funcionalidades do DNS é o serviço de distribuição de carga entre servidores web replicados, através do uso do algoritmo Round Robin. Portanto, a **alternativa C** está correta e é o gabarito da questão.

7. (CESPE/Polícia Federal - 2018) As atualizações entre servidores DNS utilizam o UDP, enquanto as consultas feitas a servidores DNS utilizam o TCP (ou, opcionalmente, o SCTP).

Comentários:

Mesmo que você não lembre do que vimos em aula, vamos tentar utilizar a lógica: o UDP é bem mais leve, então deve ser utilizado em consultas DNS, pois tais consultas ocorrem em grande número na Internet e se alguma mensagem for perdida não há grandes problemas, bastando realizar uma nova consulta. As atualizações entre servidores DNS são bem menos frequentes que as consultas e é importante que mensagens não sejam perdidas pela rede, logo, é interessante que se utilize TCP, correto? Bom, essa lógica é a utilizada no DNS! E, como podemos ver, a questão inverteu o TCP com o UDP. Portanto, a questão está **errada**.

8. (CS UFG/AL-GO - 2015) Um usuário de uma distribuição Ubuntu Linux deseja configurar o serviço de DNS em seu computador. O nome do arquivo de configuração em que devem ser inseridos os endereços IP dos servidores DNS apropriados à rede desse usuário é:

A) /etc/svc.conf

B) /etc/nsswitch.conf

C) /etc/resolv.conf

D) /etc/nameserver.conf

Comentários:

Essa questão é fácil para quem tem contato com configuração do DNS no Linux. Para quem não tem, é só lembrar do resolver (“resolvedor”) e ver que o único nome parecido é resolv.conf. A questão ajudou e não

colocou diretórios variados, colocou apenas o "/etc", que é o correto (padrão). Portanto, a **alternativa C** está correta e é o gabarito da questão.

9. (IADES/CRC-MG - 2015) Quanto ao programa que é normalmente utilizado para testar se um servidor DNS (Domain Name Server) está funcionando corretamente, ou seja, resolvendo nomes para os endereços IP, assinale a alternativa correta.

A) ping

B) tracert

C) nslookup

D) ipconfig

E) net host

Comentários:

(A) Serve para ver se "está vivo"; (B) Serve para traçar uma rota (roteadores intermediários); (C) Exatamente! ns = name server, lookup = "dar uma olhada", se você nunca usou, experimente agora no prompt: nslookup estrategiaconcursos.com.br; (D) verifica configurações das interfaces de rede; (E) o comando net não possui o parâmetro host! Portanto, a **alternativa C** está correta e é o gabarito da questão.

10. (FGV/IBGE - 2016) Ao tentar acessar o site intranet da sua organização, www.intranet.xxx.com, um usuário notou que o navegador retornava uma falha. Chamado para identificar a causa do problema, o suporte verificou que funcionava normalmente um ping da máquina do usuário para o endereço IP do servidor que hospedava a intranet. Nesse servidor, verificou também que o apache estava no ar, funcionando sem problemas. O suporte concluiu que uma possível causa do problema seria uma falha:

A) no switch local que atende o usuário;

B) na determinação do endereço MAC destino;

C) na resolução de nomes;

D) na configuração do gateway default;

E) na tabela local de roteamento.

Comentários:

Sempre que determinado equipamento estiver ativo e um determinado serviço também (ex.: servidor Web Apache), será possível acessá-lo através do endereço IP do equipamento (se não houver restrições de acesso, claro). Mas se houver algum problema na resolução de nomes, não apontando o nome (ex.:

<www.intranet.xxx.com>) para o endereço IP correspondente, ocorrerá o problema descrito na questão. Portanto, a **alternativa C** está correta e é o gabarito da questão.

11. (CESPE/TCE-SC - 2016) Após o servidor local SMTP aceitar uma mensagem para subsequente envio, é necessário determinar o endereço do servidor de email do destinatário. Essa etapa é realizada mediante consulta DNS a um servidor de nomes capaz de prover a informação, no qual serão verificados os registros especiais MX (mail exchange).

Comentários:

Vamos relembrar a tabela, focando na linha sobre "MX":

Tipo	Significado	Valor
SOA	Início de autoridade (*Start of Authority*).	Parâmetros para essa zona.
A	Endereço IPv4.	Inteiro de 32 bits.
AAAA	Endereço IPv6.	Inteiro de 128 bits.
MX	Troca de mensagens de e-mail.	Prioridade, domínio disposto a aceitar e-mails.
NS	Servidor de nomes.	Nome de um servidor para este domínio.
CNAME	Nome canônico (*alias* = apelido).	Nome de domínio.
PTR	Ponteiro (usado para o DNS reverso[1])	Nome alternativo de um end. IP.
SPF	Estrutura de política do transmissor.	Codificação de texto da política de envio de mensagens de e-mail.
SRV	Identifica computadores que hospedam serviços específicos.	Host que o oferece.
TXT	Informações sobre um servidor, rede, *datacenter*, etc.	Texto ASCII com descrições.

Portanto, a questão está **correta**.

12. (CESPE/Polícia Científica-PE - 2016) Na operação de um serviço DNS, se uma consulta a um servidor de alto nível retornar uma resposta positiva para o servidor DNS local, o mapeamento nome/endereço será

A) armazenado definitivamente no banco de dados do servidor DNS local.

B) replicado para todos os servidores DNS alcançáveis para que estejam disponíveis a outras consultas.

C) repassado pelo módulo tradutor a um servidor raiz para confirmar a resposta recebida.

D) armazenado em cache local e pode ser mantido por um tempo definido por configuração.

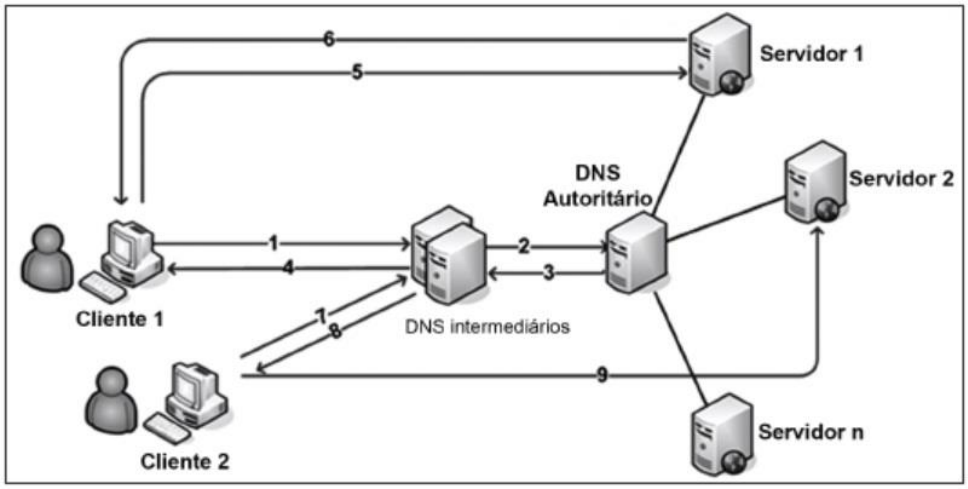
[1] Envia um endereço IP como consulta e recebe o nome como resposta.

E) repassado ao módulo tradutor do provedor de serviços para realizar a entrega à aplicação.

Comentários:

Quando o servidor DNS local busca uma informação nova, ele guarda na cache, por tempo determinado. Esse tempo varia de segundos/minutos a um dia, por exemplo. Depende do tempo definido no campo TTL. Portanto, a **alternativa D** está correta e é o gabarito da questão.

13. (FCC/ELETROSUL - 2016) O balanceamento de carga por DNS é uma abordagem popular e simples para as solicitações de balanceamento de servidores. Considere a figura abaixo.



De acordo com a figura, geralmente são estes os passos que ocorrem assim que é feita uma consulta DNS:

1. Quando um cliente tenta acessar o site, é realizada uma pesquisa no DNS local para determinar qual é o endereço I..... correspondente;

2. O pedido de endereço chega ao servidor de DNS II..... do domínio;

3. A primeira vez que esta consulta é feita, o servidor DNS remoto pode retornar todos os registros de endereços que ele tem para o site;

4. O servidor DNS III....., em seguida, determina o endereço de registro para retornar ao cliente;

5. Se todos os registros são retornados, o cliente utilizará o primeiro que lhe é atribuído;

6. O servidor responde ao cliente e atende ao pedido;

7. A cada pedido, o algoritmo Round Robin roda os endereços e retorna pela ordem em que eles estão;

8 . Cada consulta DNS irá resultar em um cliente usando um endereço IV.....;

9. Esta rotação de endereços irá distribuir pedidos para os servidores.

As lacunas de I a IV são, correta e respectivamente, preenchidas com:

A) TCP - autoritário - local - TCP igual ao obtido em 1

B) IP - autoritário - local - IP diferente

C) do servidor - local - autoritário - de um servidor

D) do servidor - autoritário - local - do servidor igual ao obtido em 1

E) IP - local - autoritário - IP igual ao obtido em 1

Comentários:

Quando um cliente tenta acessar o site, é realizada uma pesquisa no DNS local para determinar qual é o endereço IP (DNS traduz nome em endereço IP) correspondente; O pedido de endereço chega ao servidor de DNS autoritário (após o servidor DNS local, chega ao servidor que possui os registros atualizados = autoritário) do domínio; O servidor DNS local (depois de retornar do servidor autoritário, o servidor local atualiza a cache e envia ao cliente), em seguida, determina o endereço de registro para retornar ao cliente; Cada consulta DNS irá resultar em um cliente usando um endereço IP diferente (essa é a ideia do algoritmo Round Robin, o balanceamento de carga). Portanto, a **alternativa B** está correta e é o gabarito da questão.

14. (MPE-RS/MPE-RS - 2015) Em relação ao Domain Name System (DNS), considere as seguintes afirmações.

I. O DNS é o sistema de nomes empregado na Internet e se caracteriza por oferecer um espaço de nomes hierárquico, onde os nomes e seus respectivos atributos são mantidos em registros denominados de RR (Resource Records) e que são consultados com o auxílio do protocolo DNS.

II. Os servidores DNS são organizados em três níveis: servidores DNS raiz (root), servidores DNS de domínio de alto nível (Top Level Domain - TLD) e servidores DNS autoritativos (authoritativE).

III. Em uma consulta recursiva, um cliente DNS faz uma requisição DNS e recebe apenas uma resposta final correspondente a essa requisição. Já em consultas DNS iterativas, a resposta à requisição DNS pode ser parcial, obrigando o cliente DNS a encaminhar novas requisições DNS a outros servidores DNS até obter a resposta final desejada.

Quais estão corretas?

A) Apenas I.

B) Apenas II.

C) Apenas I e II.

D) Apenas II e III.

E) I, II e III.

Comentários:

Essa questão é um excelente resumo de DNS! Sem entrar nos detalhes, claro. Leia mais uma vez para ficar bem claro...A **alternativa E** está correta e é o gabarito da questão.

15. (CESPE/TCE-PR - 2016) Uma consulta DNS inicial típica, originada de uma máquina de usuário e encaminhada ao servidor de nomes local para um nome de domínio externo não armazenado em cache DNS, será do tipo

A) raiz.

B) domínio de alto nível.

C) iterativa.

D) recursiva.

E) direta.

Comentários:

O foco da questão é a consulta realizada de um equipamento ao servidor DNS local, supondo que a informação não esteja na cache desse servidor local. Nesse caso, o servidor DNS local irá requisitar ao servidor DNS TLD, receberá como resposta o próximo servidor DNS a ser consultado e repetirá o processo até ter toda a informação desejada. Armazenará em sua cache e responderá ao cliente (equipamento que fez a solicitação inicial). Note que o cliente fez uma requisição apenas e obteve uma resposta, mas o servidor DNS local realizou consultas recursivas. Portanto, a **alternativa D** está correta e é o gabarito da questão.

16. (FUNRIO/CM Nova Iguaçu - 2016) Um administrador de rede está configurando o DNS de um servidor e vai trabalhar com o registro que define as características da zona a ser configurada, tais como, o nome da zona e o nome do servidor, que é a autoridade para a referida zona, ou seja, o servidor DNS no qual está a zona que foi criada originalmente. Esse registro é conhecido pela sigla

A) HINFO.

B) MX.

C) SOA.

D) CNAME.

Comentários:

Mais uma vez aquela tabela, agora copiei apenas a linha sobre o "SOA":

SOA Início de autoridade (Start of Authority). Parâmetros para essa zona.

Ou seja, se falar sobre características/parâmetros de uma zona, trata-se do registro Start of Authority (SOA).

Portanto, a **alternativa C** está correta e é o gabarito da questão.

17. (FCC/PRODATER - 2016) No Serviço de Nomes de Domínio - DNS existem diferentes tipos de servidores distribuídos hierarquicamente que armazenam informações também de forma hierárquica. Considerando o nome: www.empresa.com, o domínio .com é gerenciado pelo servidor

A) Global.

B) PDR.

C) Authoritative.

D) TLD.

E) Root.

Comentários:

Os domínios de mais alto nível são classificados em genéricos (“.com”, “.edu”, “.bradesco”, etc.) ou códigos de países (“.br”, “.mx”, “.uy”, “.jp”, etc.). Em inglês é conhecido como TLD (Top Level Domain) e os servidores DNS TLD gerenciam tais domínios. Abaixo podemos ver mais exemplos de TLDs genéricos e dois exemplos de códigos de países. Portanto, a **alternativa D** está correta e é o gabarito da questão.

18. (IBFC/EBSERH-HUAP - 2016) O Domain Name System (DNS) é um sistema de gerenciamento de nomes hierárquicos e distribuídos. A funcionalidade do DNS Reverso vem a ser:

A) reverter a funcionalidade básica de um DNS padrão obtendo o endereço MAC.

B) resolver um endereço IP, buscando o nome de domínio associado ao host.

C) resolver o nome do domínio de um host qualquer para seu endereço IP correspondente.

D) com base na região geográfica, obter automaticamente um endereço IP local.

E) resolver o problema da reversão do IPv6 para o IPv4 de uma forma rápida e automática.

Comentários:

A questão começa com a definição de DNS, segundo o Tanenbaum. O DNS tem a função de traduzir um nome em um endereço, então o DNS reverso faz o contrário: traduz um endereço em um nome. É definido através do registro PTR:

PTR Ponteiro (usado para o DNS reverso) Nome alternativo de um end. IP.

Portanto, a **alternativa B** está correta e é o gabarito da questão.

19. (FCC/CREMESP - 2016) O sistema de gerenciamento de nomes de domínio é composto de servidores distribuídos hierarquicamente nos vários níveis do domínio da internet. Nesse sistema, quando um computador cliente faz uma solicitação de nome de domínio, ele envia a solicitação para o

A) servidor de nomes local da rede em que está o computador.

B) resolver localizado no próprio computador.

C) servidor de nomes raiz da internet.

D) gerenciador de solicitações localizado no servidor de nomes.

E) controlador de nomes de domínio de topo.

Comentários:

Como vimos, quando um aplicativo (navegador, cliente FTP, ping, etc.) precisa resolver um nome, ele solicita a um "resolvedor" no próprio computador (a questão colocou em inglês - resolver), o resolvedor consulta o servidor DNS local, e assim por diante. Portanto, a **alternativa B** está correta e é o gabarito da questão.

20. (FGV/COMPESA - 2016) O sistema de Nomes de Domínio - DNS permite transformar nomes digitados em um navegador WEB em um endereço de rede. O nome do host e o nível do domínio para o domínio "system.master.com" são, respectivamente,

A) system e segundo nível.

B) system e terceiro nível.

C) master e terceiro nível.

D) master e segundo nível.

E) .com e terceiro nível.

Comentários:

Um servidor DNS raiz "aponta" para servidores de primeiro nível (TLD). No domínio mostrado, o TLD é o ".com", que aponta para um servidor DNS responsável por "master" (segundo nível), que por sua vez, aponta para um terceiro nível, o host "system", no caso da questão. Portanto, a **alternativa B** está correta e é o gabarito da questão.

21. (IBFC/Polícia Científica-PR - 2017) Servidores DNS (Domain Name Server) são responsáveis pela conversão do nome dos diversos servidores espalhados pela Internet para seu número IP e vice-versa. Servidores de DNS trabalham de forma colaborativa e hierárquica. Assinale a alternativa a que apresenta o nome dado aos servidores que se encontram no topo da hierarquia de DNS:

A) Root Name Servers

B) Main servers

C) International Name Servers

D) Controllers Servers

E) Master Servers

Comentários:

A hierarquia DNS é uma árvore invertida, ou seja, os servidores raiz (Root Name Servers) ficam no topo, logo abaixo ficam os TLDs (Top Level Domains), depois os de segundo nível e assim por diante. Portanto, a **alternativa A** está correta e é o gabarito da questão.

22. (IBFC/Polícia Científica-PR - 2017) Servidores de DNS (Domain Name System) têm como função converter endereços IP em seu respectivo nome e vice-versa. Para sua configuração, são utilizados arquivos denominados mapas de domínio (zonE). Esses arquivos são compostos por entradas chamadas RR (Resource Record). O tipo básico de RR que estabelece a correspondência entre um nome canônico e um endereço IP é indicado por:

A) PTR

B) MX

C) NS

D) A

E) SOA

Comentários:

Quando é realizada uma consulta pelo nome, esperando como resposta um endereço IP, os RRs possíveis são:

A	Endereço IPv4.	Inteiro de 32 bits.
AAAA	Endereço IPv6.	Inteiro de 128 bits.

Como a questão não mostra “AAAA” como alternativa, sobrou apenas o “A”, que retorna um endereço IPv4.

Portanto, a **alternativa D** está correta e é o gabarito da questão.

23. (FAURGS/UFRGS - 2015) Considere as afirmativas abaixo com relação a mecanismos de resolução de nomes na Internet.

I - Domain Name System (DNS) baseia-se em informações que podem estar distribuídas em vários computadores da Internet.

II - A técnica de host file permite resolver nomes sem ter que acessar a Internet.

III - Atualmente, a técnica de DNS está sendo substituída pela técnica de host file, na resolução de nomes.

Quais estão corretas?

A) Apenas I.

B) Apenas I e II.

C) Apenas I e III.

D) Apenas II e III.

E) I, II e III.

Comentários:

(I) É um sistema com bancos de dados distribuídos, senão ficaria inviável o uso de DNS com o tamanho que a Internet adquiriu há um bom tempo! (II) É o famoso arquivo hosts no Windows ou Linux, por exemplo, uma tradução direta, sem consultar servidores DNS. (III) Nada disso! Host file é uma exceção, o padrão é consultar servidores DNS. Aliás, existem malwares que utilizam essa técnica para enviar a vítima para o lugar errado para determinadas URLs! Portanto, a **alternativa B** está correta e é o gabarito da questão.

24. (FGV/IBGE - 2017) Servidores DNS podem ser configurados para compartilhar e distribuir cargas a um grupo de servidores da rede por meio da técnica de balanceamento de carga denominada:

A) Backbone;

B) Round-robin;

C) DNS reverso;

D) Packet sniffer;

E) IP spoofing.

Comentários:

Um algoritmo utilizado em algumas áreas da computação, como por exemplo, o gerenciamento de processos em um sistema operacional, é o Round-Robin. No caso do gerenciamento de processos, frações de tempo são atribuídas para cada processo em partes iguais e de forma circular, evitando a monopolização do processador. Para o balanceamento de carga DNS, o princípio é o mesmo, mas o rodízio é realizado de acordo com os acessos. Por exemplo, se há três servidores que respondem pelo nome X, a primeira consulta será

realizada no servidor 1, depois no 2 e a seguinte no 3. A quarta consulta será realizada no servidor 1 e assim por diante. Portanto, a **alternativa B** está correta e é o gabarito da questão.

25. (FGV/MPE-BA - 2017) Uma instituição precisou alterar no seu servidor DNS o número IP de seu servidor Web. Em relação a essa situação, é correto afirmar que:

A) realizada a atualização do endereço IP, o protocolo DNS garante que essa mudança seja refletida imediatamente em todos os servidores autoritativos do domínio;

B) para apontar para outro endereço IP, no servidor DNS houve a mudança do registro do tipo PTR;

C) servidores secundários DNS só serão atualizados após o fim do expire value do campo SOA;

D) consultas DNS que retornarem respostas não autoritativas podem ainda mostrar o endereço IP antigo do servidor Web;

E) clientes DNS compatíveis com a RFC 2308 sempre retornarão o novo endereço IP, por não implementarem cache negativo.

Comentários:

Imagine a seguinte situação: você alterou no servidor DNS de sua empresa o endereço IP do servidor Web, de 200.100.100.55 para 200.100.100.99. Então: (A) não há atualização automática aos servidores autoritativos do domínio! (B) PTR serve para o DNS reverso; (C) O nome correto do campo para essa finalidade é Refresh; (D) Respostas não autoritativas são aquelas que estão em cache, então enquanto a cache não for atualizada, ainda terá o endereço IP 200.100.100.55 (o antigo); (E) O título da RFC 2308 já diz tudo: “Negative Caching of DNS Queries (DNS NCACHE)”, ou seja, implementa o cache negativo. Portanto, a **alternativa D** está correta e é o gabarito da questão.

26. (FEPESE/CIASC - 2017) Analise as afirmativas abaixo com relação ao serviço de resolução de nomes DNS.

1. Consulta Recursiva é o tipo de consulta que ocorre quando servidor DNS não sabe ou não é responsável pela resolução do nome. O Servidor neste caso realiza consultas recursivas na hierarquia de nomes em busca da resposta para a consulta realizada.

2. Consulta Interativa é o tipo de consulta que ocorre quando servidor DNS não sabe ou não é responsável pela resolução do nome. O Servidor neste caso realiza consultas recursivas na hierarquia de nomes em busca da resposta para a consulta realizada.

3. Consulta Interativa é o tipo de consulta que ocorre quando o servidor DNS apenas responde a consulta caso ele seja responsável pela resolução do nome consultado.

4. Um problema bastante comum de configuração é permitir que qualquer máquina na Internet faça consultas ao servidor DNS recursivo de uma determinada rede. Servidores com esse problema são comumente chamados de servidores DNS recursivos abertos.

Assinale a alternativa que indica todas as afirmativas corretas.

A) São corretas apenas as afirmativas 1 e 2.

B) São corretas apenas as afirmativas 2 e 3.

C) São corretas apenas as afirmativas 1, 2 e 4.

D) São corretas apenas as afirmativas 1, 3 e 4.

E) São corretas apenas as afirmativas 2, 3 e 4.

Comentários:

(1) Exato, conforme a consulta número 1 da figura; (2) Misturou consulta iterativa com recursiva! (3) Exato, temos vários exemplos na figura: consultas 2, 4, 6 e 8; (4) Esse "problema" pode causar ataques de negação de serviço, com a solicitação de diversas consultas ao servidor DNS, que não deveriam estar disponíveis a "qualquer um". O nome dado a essa situação é servidor DNS recursivo aberto, mais um aprendizado... Portanto, a **alternativa D** está correta e é o gabarito da questão.

27. (FAURGS/BANRISUL - 2018) Um cliente DNS, ao fazer a requisição DNS para resolver o nome www.banrisul.com.br, recebe como resposta uma mensagem do tipo non authoritative. Esse tipo de resposta é obtido por meio de um registro DNS (resource record - RR) armazenado

A) em um cache de DNS.

B) em um servidor interativo sem cache DNS.

C) em um servidor recursivo sem cache DNS.

D) no arquivo de zona do DNS primário.

E) no arquivo de zona do DNS secundário.

Comentários:

Um servidor DNS autoritativo possui autoridade sobre um nome de domínio. O DNS autoritativo dita qual será o apontamento da tabela de DNS do seu sítio. Uma resposta autoritativa de um servidor é a garantia de estar atualizada, enquanto uma resposta não-autoritativa pode estar desatualizada (cache com informações antigas, por exemplo). Existe um percentual elevado de respostas não autoritativas que estão perfeitamente corretas, casos em que mudanças de endereçamento são raros.

Servidores primários e secundários são autoritativos para os seus domínios, porém não o são sobre informações a respeito de outros domínios mantidas em cache. Servidores caching-only nunca são autoritativos, mas possuem a vantagem de reduzir a quantidade de tráfego DNS na rede. Portanto, a **alternativa A** está correta e é o gabarito da questão.

TRADUÇÃO DE ENDEREÇOS DE REDE (NAT)

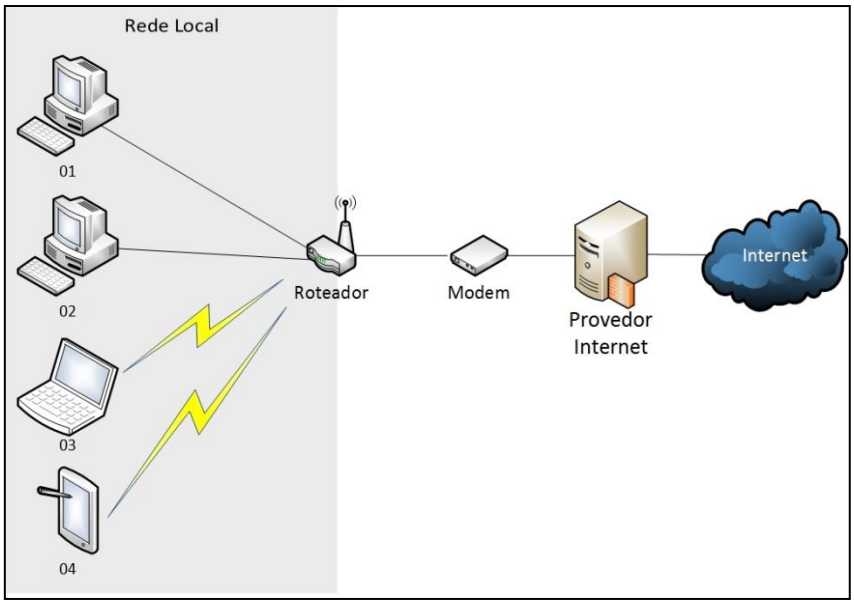
Conceitos

Quando surgiu o protocolo IPv4, não se imaginava que um dia suas faixas de endereçamento ficariam escassas. Uma estratégia adotada foi a utilização de endereçamento privado[1] (aquele que não é roteável). As faixas reservadas para o endereçamento privado são mostradas na tabela abaixo.

Classe	Faixa de endereços privados	Prefixo
A	10.0.0.0 a 10.255.255.255	10/8
B	172.16.0.0 a 172.31.255.255	172.16/12
C	192.168.0.0 a 192.168.255.255	192.168/16

Mas o que são os endereços IP não roteáveis? São aqueles que os roteadores não consideram válidos e, por consequência, não encaminham os pacotes. Como isso ocorre? Simples, na implementação do roteamento, as faixas mostradas na tabela ficam "de fora", seguindo o que determina a RFC 1918. Ok, mas eu posso implementar um roteador que ignore isso? Pode, mas será um roteador "fora do padrão". Aliás, é possível implementar qualquer coisa fora do padrão, basta querer!

Bom, e como um endereço IP não roteável consegue "se comunicar" na Internet? Através do NAT (*Network Address Translation*), um serviço que traduz endereços privados (não roteáveis) em públicos (roteáveis) e vice-versa. Geralmente esse serviço (NAT) fica habilitado em roteadores ou modems/roteadores. Para entender melhor, dê uma olhada na figura abaixo.



Fonte: Dalla Vecchia, E. Perícia Digital – da investigação à análise forense. 2. ed. Campinas: Millennium, 2019.

[1] RFC 1918 - Address Allocation for Private Internets. Disponível em <http://www.rfc-editor.org/rfc/rfc1918.txt>.

Podemos verificar uma rede local com apenas quatro dispositivos, um cenário típico de uma residência com computadores, *tablets*, *smartphones* etc. Na figura, dois deles possuem conexão com cabo e dois sem fio. O roteador está separado do modem, por questões conceituais, mas na vida real geralmente vemos uma única "caixinha" com as funções de modem e de roteador, além de outras.

Nesse roteador é comum termos um servidor DHCP (*Dynamic Host Configuration Protocol*), *firewall*, serviço NAT, entre outros. Para exemplificar, vamos analisar a configuração de um roteador D-Link e o roteador ligado a um *cable modem*, como mostrado na figura. O padrão desse equipamento é ter a rede local 192.168.0.0/24, tendo o endereço IP da interface ligada à LAN 192.168.0.1. Vamos supor que o servidor DHCP esteja ligado e configurado para distribuir endereços na faixa 192.168.0.11 a 192.168.0.200. Assim, podemos ter o seguinte:

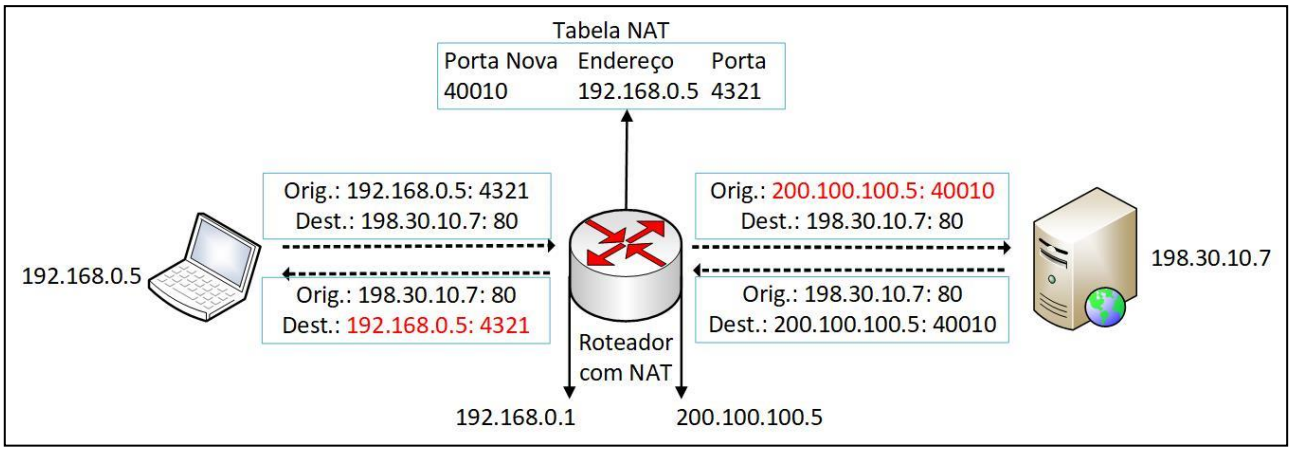
Roteador:
End. IP da interface LAN: 192.168.0.1
End. IP da interface WAN: 189.6.138.222 (recebido pelo provedor Internet)
Dispositivos na rede local:
01: 192.168.0.11
02: 192.168.0.12
03: 192.168.0.13
04: 192.168.0.14

Se um usuário utilizar o Dispositivo 02 para acessar uma página Web, a solicitação será encaminhada ao gateway padrão (192.168.0.1), que traduzirá o endereço IP origem 192.168.0.12 para 189.6.138.222 e encaminhará a solicitação ao servidor da página solicitada.

O retorno será do servidor ao roteador (endereço IP externo - 189.6.138.222), que traduzirá para o endereço 192.168.0.12 e enviará ao Dispositivo 02. Na prática, a grande maioria das empresas utiliza o cenário apresentado. Isto quer dizer que se alguém cometer algum ilícito através da Internet a partir da rede local de uma empresa e essa empresa utilizar NAT, a investigação terá condições de realizar o rastreamento até o local físico apenas, sem saber que máquina foi utilizada (em um primeiro momento).

Para saber qual das máquinas foi utilizada, algum tipo de controle interno (*logs*) poderia ajudar, e na falta disso, somente uma análise de todos os equipamentos para saber quem foi o responsável, um trabalho e tanto! Não é à toa que estabelecimentos como hotéis, restaurantes, entre outros, começaram a exigir autenticação de seus clientes (através de cadastro prévio), mesmo quando a Internet não é cobrada.

Para entender o funcionamento do NAT, vamos analisar a figura abaixo.



A figura mostra um navegador em uma rede local (LAN) com endereçamento privado, acessando uma página Web em um servidor na Internet. O passo a passo é mostrado a seguir:

1. Um computador com endereço IP privado 192.168.0.5 realiza uma requisição HTTP para o endereço IP 198.30.10.7, sendo que o navegador está utilizando a porta 4321;
2. O roteador com NAT substitui o endereço origem pelo endereço válido 200.100.100.5, troca a porta origem por 40010 e coloca em uma tabela NAT uma associação dessa porta nova com o endereço origem e porta origem originais;
3. O servidor Web responde para o roteador;
4. O roteador verifica na tabela NAT que a porta 40010 deve realizar a seguinte substituição: colocar 192.168.0.5 como endereço destino e 4321 como porta destino;
5. O navegador recebe o retorno.

Além de possibilitar o uso de um único endereço IP público por vários dispositivos da LAN (rede local), o **NAT** também é considerado um **mecanismo de segurança**, pois, por padrão, permite que os pacotes se originem da rede local, e aos pacotes que "desejam" entrar na rede, só permite aqueles que se tratam de respostas das solicitações da LAN.

Vamos ver os três tipos de NAT mais conhecidos:

- **NAT *Overload* (PAT)**: é a técnica mais utilizada, a qual acabamos de ver. Tem-se um único endereço público e por ele conseguimos fazer sair vários dispositivos (1:N). Essa "mágica" ocorre através da utilização das portas, como vimos na última figura. Por isso também é conhecido como PAT (*Port Address Translation*);

- **NAT Estático**: um endereço privado é traduzido em um endereço público (1:1);

- **NAT Dinâmico**: existe um conjunto de endereços públicos (*pool*), que as máquinas que utilizam endereços privados podem utilizar (N:M).

Do jeito que vimos até agora, nem sempre é possível utilizar o NAT. Por exemplo, o protocolo ESP (utilizado no IPsec) não utiliza o mesmo conceito de portas utilizado nos protocolos TCP e UDP, o que impossibilita a

tradução de endereço através da utilização da informação de portas de origem e destino como forma de multiplexação das conexões.

Para que uma conexão VPN funcione quando existe um equipamento fazendo NAT entre os pontos que estão estabelecendo a VPN é necessário que haja um mecanismo para garantir que os pacotes sejam traduzidos adequadamente, desde a origem até o destino final. Esse mecanismo é chamado de **NAT Traversal**.

O **NAT Traversal** primeiramente verifica se os dois equipamentos que estão estabelecendo a conexão possuem suporte para NAT Traversal, em seguida os dois equipamentos devem detectar se existe ou não a tradução de endereços. Por fim, deve-se negociar os parâmetros do protocolo (portas utilizadas para encapsulamento, utilização de *cookies* etc.) e em seguida iniciar a transmissão de dados utilizando pacotes encapsulados (detalhes em RFC 3947[2]).

Para a **descoberta de endereços e de portas alocados por NAT Traversal**, em conjunto com outros protocolos (ICE - *Interactive Connectivity Establishment*, SIP - *Session Initiation Protocol*, WebRTC etc.), o **protocolo STUN** é uma solução. Ele fornece uma ferramenta para a descoberta da presença de um tradutor de endereço de rede e a descoberta do mapeamento IP/porta que o NAT realizou para os fluxos UDP de aplicações de hosts remotos.

Sei que misturei novos protocolos aqui, sem entrar em detalhes, mas fiz isso para que possamos resolver algumas questões que começaram a aparecer, sem precisar entrar nos detalhes de alguns protocolos. Lembre-se que o nosso foco é acertar a questão!

Também já vi questões cobrando um outro tipo de NAT, o **NAT-PT** (NAT-Protocol Translation)[3]. Resumidamente, ele **traduz endereços IPv6 para IPv4** e é direcionado às redes internas de uma organização.

[2] RFC 3947 - Negotiation of NAT-Traversal in the IKE. Disponível em <https://tools.ietf.org/html/rfc3947>.

[3] RFC 2766 - Network Address Translation - Protocol Translation (NAT-PT). Disponível em <https://tools.ietf.org/html/rfc2766>.

QUESTÕES COMENTADAS

1. (FCC/TRT 15ª Região - 2015) Em uma rede sem fio de computadores (WLAN), as funções de gerenciamento da WLAN são desempenhadas pelo dispositivo comercialmente chamado de Roteador Wireless. Dentre as funções do Roteador está a de designar um endereço IP válido para as mensagens que saem da LAN para a WAN, uma vez que, na LAN, é utilizado um endereço IP virtual. No Roteador, essa função é desempenhada pelo

A) DNS.

B) Gateway.

C) DHCP.

D) Firewall.

E) NAT.

Comentários:

Hoje em dia aquela "caixinha" que chamamos de modem/roteador, possui também as funcionalidades de switch, conexão sem fio, servidores DHCP, NAT, firewall etc. Mas a função descrita na questão se refere ao NAT (tradução de endereço IP privado em público e vice-versa). Portanto, a **alternativa E** está correta e é o gabarito da questão.

2. (FCC/TRT 3ª Região - 2015) O NAT (Network Address Translation), que realiza a substituição de um IP privado por um público para os pacotes de mensagens que saem de uma rede local, evitou que o escasseamento dos endereços IPv4 inviabilizasse o crescimento do número de computadores conectados na internet. O relacionamento entre o IP privado que gerou o pacote enviado para a rede pública com um IP válido é realizado por meio do uso do campo

A) Type do cabeçalho Ethernet.

B) Flag do cabeçalho IP.

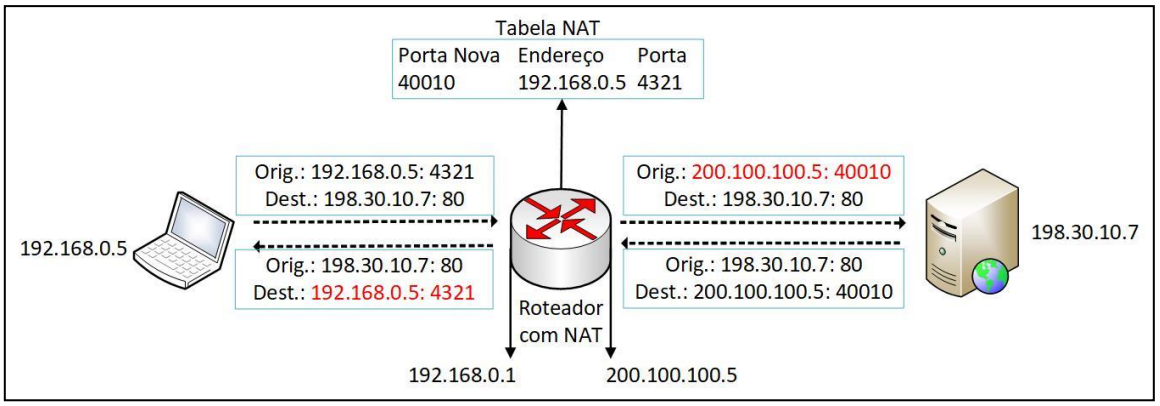
C) Número de Sequência do cabeçalho TCP.

D) Porta Origem do cabeçalho TCP.

E) TTL do cabeçalho IP.

Comentários:

Um belo resumo de NAT! Vamos relembrar o funcionamento do NAT:



Ou seja, a porta origem do TCP é utilizada como "índice" na tabela NAT. Portanto, a **alternativa D** está correta e é o gabarito da questão.

3. (CESPE/TCE-RN - 2015) O NAT (network address translation) é uma solução para distribuir IPs públicos que são acessados via Internet. Um tipo de NAT é o NAT-PT, que traduz automaticamente endereços IPv6 para IPv4 e é direcionado às redes internas de uma organização.

Comentários:

Exato! Dificilmente cobrarão mais detalhes do funcionamento do NAT-PT. O Cespe fez um bom resumo do assunto. A questão está **correta**.

4. (FCC/TRT 9ª Região - 2015) A adoção de um sistema de NAT (Network Address Translation) no roteador de uma LAN apresenta a vantagem de segurança, pois

A) o NAT realiza a filtragem dos pacotes IPs que saem da LAN.

B) o NAT realiza a função de um servidor Proxy de conteúdo.

C) o NAT realiza a filtragem dos pacotes TCP que entram na LAN.

D) um pacote gerado na LAN é encapsulado e criptografado para sair da LAN.

E) um acesso ou pacote gerado externamente à LAN é automaticamente descartado.

Comentários:

Há quem considere o NAT um tipo de firewall, mesmo ele tendo sido criado para a finalidade de tradução de endereços. Mas como ele não aceita pacotes gerados externamente à rede local (LAN), não deixa de ser uma "barreira". Obviamente que a resposta do que é solicitado pela LAN deve ser aceita (pacotes enviados de redes externas para a LAN). Portanto, a **alternativa E** está correta e é o gabarito da questão.

5. (CESPE/TC-DF - 2014) A tradução de endereços de rede, ou NAT (network address translation), deve ser utilizada quando a quantidade de endereços IP atribuídos pelo provedor de Internet for

insuficiente, ou seja, quando a rede possuir uma quantidade maior de computadores que a quantidade de endereços disponíveis.

Comentários:

Mais um belo resumo de NAT feito pela Cespe. Para utilizar a Internet, o equipamento deve possuir um endereço IP. Se não houver endereços suficientes, pode-se utilizar endereços IP privados em uma rede local, com a devida tradução por um endereço IP válido através do serviço NAT. Portanto, a questão está **correta**.

6. (CESPE/TCE-PA - 2016) A tecnologia NAT permite conectar a Internet a uma rede de dispositivos com espaço de endereçamento próprio, exigindo, para tanto, apenas um endereço IP válido.

Comentários:

Questão recorrente da Cespe...dois anos depois e o conteúdo é o mesmo da questão anterior. Questão **correta**.

7. (FUMARC/AL-MG - 2014) A escassez de endereços IPs promoveu a criação da técnica conhecida como NAT. Considerando essa técnica, analise as seguintes afirmativas:

I. Três faixas de endereços são reservadas para uso dentro da rede isolada pelo equipamento que faz o NAT, são elas: 10.0.0.0/8, 192.2.0.0/16 e 172.0.0.0/8.

II. O mapeamento de acesso da máquina interna para a internet é feito considerando endereços IPs e portas.

III. Se dois computadores da rede interna acessarem o mesmo site de destino na internet, ambos os acessos terão como IP de origem o endereço verdadeiro atribuído ao NAT.

Está CORRETO apenas o que se afirma em:

A) II.

B) III.

C) I e III.

D) II e III.

Comentários:

(I) O erro está na segunda faixa apresentada: a correta é 192.168.0.0/16; (II) Exato! Quando o serviço NAT faz a tradução, ele substitui a porta origem por uma de controle dele, para saber "o que fazer" quando do retorno (resposta); (III) Isso mesmo, dois, três, quinze computadores...todos os pacotes originados por eles terão o endereço IP origem substituído pelo "endereço verdadeiro" atribuído ao NAT. Portanto, a **alternativa D** está correta e é o gabarito da questão.

8. (FCC/TRT 11ª Região - 2017) Para aumentar a segurança na rede local sob sua responsabilidade, um Analista Judiciário decidiu instalar o NAT em complementação a outros recursos. A percepção de que o NAT fornece segurança complementar é porque

A) um pacote entra na rede local somente em resposta a um pacote originário daquela rede.

B) um pacote sai da rede local somente se for checado pela tabela MIB.

C) os pacotes transmitidos da rede local para a rede ampla são certificados pela tabela MIB.

D) reescreve o endereço IP origem do pacote que sai da rede local para um IP virtual, por exemplo, 10.0.0.0.

E) reescreve o número da Porta origem do cabeçalho IP com um valor criptografado.

Comentários:

Questão semelhante ao que vimos em questão anterior, porém de outra banca. Como falei, o NAT pode ser considerado um tipo de firewall. Portanto, a **alternativa A** está correta e é o gabarito da questão.

9. (IBFC/Polícia Científica-PR - 2017) O esquema de endereçamento IP prevê um conjunto de endereços chamados de privados. Esses endereços podem ser utilizados em redes privadas, mas não permitem utilização na rede pública da Internet. Assinale a alternativa que apresenta um mecanismo capaz de resolver o problema de um computador de uma rede interna acessar a rede pública da Internet:

A) DHCP (Dynamic Host Configuration Protocol)

B) VPN (Virtual Private Network)

C) NAT (Network Address Translation)

D) VoIP (Voice over IP)

E) SSH (Secure Shell)

Comentários:

Endereços privados não são roteáveis, precisam ser traduzidos para um endereço válido (roteável) e o serviço que faz isso é o NAT. Portanto, a **alternativa C** está correta e é o gabarito da questão.

10. (FGV/IBGE - 2017) Para contornar a escassez de endereços IP de sua organização, Júlio adotou o NAT para mapear os endereços IP dos pacotes de origem de sua rede interna para a Internet e vice-versa. Apesar de solucionar o problema da escassez de IP, Júlio poderá enfrentar a seguinte desvantagem do NAT:

A) simplificação do plano de mapeamento dos endereços IP;

B) comportamento transparente para algumas aplicações que usam várias conexões TCP/IP ou portas UDP predefinidas;

C) violação do modelo arquitetônico do IP, que estabelece que todo endereço IP identifique de forma exclusiva uma única máquina;

D) redução da segurança por possibilitar rastrear o caminho do pacote fim a fim;

E) redução da segurança quando for combinado em um dispositivo com um backbone do ISP.

Comentários:

Esse é o grande problema em investigações. Imagine que um crime eletrônico tenha ocorrido a partir de um computador de uma empresa que possui centenas de equipamentos, todos utilizando endereço IP privado. Ao realizar o rastreamento, a polícia conseguirá chegar até a empresa, mas, apenas com o endereço IP investigado, não terá condições de saber qual máquina foi utilizada para cometer o ilícito! Portanto, a **alternativa C** está correta e é o gabarito da questão.

11. (NUCEPE/PC-PI - 2018) O NAT (Network Address Translation) é uma técnica utilizada para reescrever endereços IPv4 nos cabeçalhos e dados das aplicações, permitindo que estações e redes privadas não sejam visíveis externamente na Internet, ou seja, pode ser utilizado como mecanismo de segurança. Sobre o NAT, marque a única alternativa INCORRETA.

A) Em um NAT do tipo estático há associação de um endereço privado a um endereço público. Por exemplo: um Inside Local IP Address (10.0.2.8) é mapeado para um Inside Global Address (200.137.169.80).

B) Em um NAT do tipo dinâmico existe uma relação de muitos para muitos em uma associação dinâmica dos IPs privados para endereços públicos.

C) O NAT não funciona como um firewall, contudo pode prevenir que intrusos iniciem conexões com os hosts internos, uma vez que o NAT tem a capacidade de ocultar a estrutura interna da rede, dificultando a usuários externos visualizar endereços dos dispositivos internos.

D) Uma das características do NAT overload é a de funcionar normalmente com portas internas compartilhadas para cada dispositivo local interno. Por exemplo: os dispositivos (10.0.2.8) e (10.0.2.11) usam a mesma porta 5900.

E) Uma associação de muitos endereços privados para um único endereço público por meio de diferentes portas TCP/UDP recebe o nome de NAT overload ou PAT (Port Address Translation).

Comentários:

(A) NAT Estático: um endereço privado é traduzido em um endereço público (1:1); (B) NAT Dinâmico: existe um conjunto de endereços públicos (pool), que as máquinas que utilizam endereços privados podem utilizar (muitos para muitos, ou N:M); (C) Realmente não funciona como um firewall, pois não possui regras de filtros, mas dificulta o acesso de usuários externos à rede interna, o que o torna um mecanismo de segurança; (D) NAT Overload (PAT): tem-se um único endereço público e por ele conseguimos fazer sair vários

dispositivos (1:N). Ou seja, não são compartilhadas portas internas, senão não teria como fazer o mapeamento posterior para saber que máquina fez determinada solicitação! Alternativa INCORRETA! (E) Exato! Como explicado no comentário da alternativa anterior. Portanto, a **alternativa D** está correta e é o gabarito da questão.

12. (FAURGS/BANRISUL - 2018) Qual protocolo, entre os listados abaixo, serve para a descoberta de endereços e de portas, alocados por NAT, de um destinatário e que pode ser utilizado na implantação de NAT-Traversal em conjunto com SIP?

A) NAT-D.

B) STUN.

C) NAT-OA.

D) NAT-PCP.

E) IGDP.

Comentários:

(A) Não encontrei nada relacionado ao assunto com essa sigla! (B) Para a descoberta de endereços e de portas alocados por NAT Traversal, em conjunto com outros protocolos (ICE, SIP, WebRTC etc.), o protocolo STUN é uma solução. Ele fornece uma ferramenta para a descoberta da presença de um tradutor de endereço de rede e a descoberta do mapeamento IP/porta que o NAT realizou para os fluxos UDP de aplicações de hosts remotos; (C) NAT-OA = NAT Original Address; (D) PCP = Port Control Protocol. Permite um host IPv4 ou IPv6 o controle de como pacotes IPv4 ou IPv6 são traduzidos e encaminhados através de NAT ou de um firewall; (E) Não encontrei nada relacionado ao assunto com essa sigla! Portanto, a **alternativa B** está correta e é o gabarito da questão.

SERVIDORES WEB

Apache

O Apache é um servidor Web livre (possui código-fonte aberto) que funciona em ambiente multiplataforma (Windows, Novell, OS/2, Unix, Linux, FreeBSD etc.). No Linux o servidor utiliza o *daemon* httpd. Suas funcionalidades são mantidas através de uma estrutura de módulos, permitindo inclusive que o usuário escreva seus próprios módulos.

Em ambientes Unix-like os **arquivos de configuração**, por padrão, ficam localizados no diretório /etc/apache. O servidor é configurado por um arquivo denominado **httpd.conf** e opcionalmente pode haver configurações para cada diretório utilizando arquivos com o nome **.htaccess**, onde é possível utilizar autenticação de usuário pelo próprio protocolo HTTP (combinação de arquivo .htaccess com um arquivo .htpasswd, que guardará os usuários e senhas criptografadas).

Existem dois tipos de páginas que podem ser adicionadas ao Apache: a página raiz e subpáginas. A página raiz é especificada através da diretiva **DocumentRoot** e será mostrada quando se entrar no domínio principal, como http://www.estrategiaconcursos.com.br. Na configuração padrão do Apache, DocumentRoot aponta para o diretório /var/www. Esse diretório será assumido como raiz caso os diretórios não sejam iniciados por uma /:

home/estrategia → aponta para /var/www/home/estrategia

/home/estrategia → Aponta para /home/estrategia

Apachectl (*Apache HTTP Server Control Interface*): trata-se de um *front end* para o servidor Apache. É utilizado para ajudar o administrador a controlar o funcionamento do *daemon* httpd. O *script* apachectl pode operar em dois modos:

- *Front end* simples que configura quaisquer variáveis de ambiente necessárias e então chama o httpd, passando argumentos de linha de comando;
- *Script* de inicialização, recebendo argumentos simples como *start*, *restart*, e *stop*, traduzindo-os em sinais apropriados ao httpd.

Quando utilizado no **modo de script de inicialização**, o apachectl aceita como **argumentos** (pode-se utilizar "-k" antes do argumento):

- start: inicializa o *daemon* httpd;
- stop: finaliza o *daemon* httpd;
- restart: reinicializa o *daemon* httpd. Se não estiver rodando, o httpd é inicializado;
- fullstatus: mostra um relatório completo do status do mod_status. Para isso, o módulo mod_status deve estar habilitado;
- status: mostra um relatório resumido do status. Similar à opção fullstatus, mas a lista de requisições correntes que estão sendo servidas é omitida;

- graceful: reinicializa o *daemon* de forma “gentil”. Se não estiver rodando, o httpd é inicializado. A diferença para uma inicialização normal é que as conexões correntes não são abortadas;
- graceful-stop: finaliza o *daemon* de forma “gentil”. A diferença para uma finalização normal é que as conexões correntes não são abortadas;
- configtest: executa um teste no arquivo de configuração. Após verificar a sintaxe, informa se está ok ou aponta os erros encontrados.

Para inicializar o httpd, vimos que um comando possível é **apachectl start**, mas há outras formas também, dependendo da distribuição utilizada:

- Red Hat: **service httpd start**;
- Ubuntu: **/etc/init.d/apache2 start**.

O argumento “start” pode ser trocado por “restart”, “stop” etc., para as demais ações.

Segurança: o servidor dispõe de um módulo “mod_ssl”, o qual adiciona a capacidade do servidor atender requisições utilizando o protocolo HTTPS. Esse protocolo utiliza uma camada SSL para criptografar todos os dados transferidos entre o cliente e o servidor, provendo maior grau de segurança, confidencialidade e confiabilidade dos dados. A camada SSL é compatível com certificados X.509, que são os certificados digitais fornecidos e assinados por grandes entidades certificadoras no mundo.

Diretivas

Diretrizes (ou diretivas) nos arquivos de configuração (httpd.conf e .htaccess) podem ser aplicadas ao servidor inteiro ou podem ser restritas na aplicação de determinados diretórios, arquivos, hosts ou URLs. Vamos ver o significado de algumas delas:

<Directory> é utilizada para definir um grupo de diretrizes que devem ser aplicadas apenas ao diretório definido, seus subdiretórios, e aos arquivos dentro deles. Exemplo:

```
<Directory "/usr/local/httpd/htdocs">

    Options Indexes FollowSymLinks

</Directory>
```

<Files> limita o escopo das diretrizes pelos de nomes de arquivos. Funciona igual ao <Directory>, mas agora o foco são arquivos. Exemplo:

```
<Files "?at.*">

    # Aplica-se a cat.html, bat.html, hat.php etc., pois “?” significa um caractere qualquer

    # e * significa qualquer coisa daquela posição em diante

    # Colocar as diretrizes aqui...

</Files>
```

<VirtualHost> permite servir mais de um *site* no mesmo servidor (*sites* virtuais). Podem ser utilizadas diretivas específicas para o controle do *site* virtual, como nome do administrador, erros de acesso a página, controle de acesso e outros dados úteis para personalizar e gerenciar o *site*.

Virtual Hosts baseados em nome: utiliza nomes para identificar os *sites* servidos e requerem somente um endereço IP. Assim é possível servir um número ilimitado de *sites* virtuais. O navegador do cliente deve suportar os cabeçalhos necessários para garantir o funcionamento desse recurso (os navegadores mais comuns possuem tal suporte). Exemplo:

```
<VirtualHost www.site1.com.br>

        ServerName www.site1.com.br

        ServerAdmin site1@site1.com.br

        DocumentRoot /var/www/www_site1_com_br

        TransferLog /var/log/apache/site1/access.log

        ErrorLog /var/log/apache/site1/error.log

        User www-data

        Group www-data

</VirtualHost>

<VirtualHost www.site2.com.br>

        ServerName www.site2.com.br

        DocumentRoot /var/www/www_site2_com_br

        CustomLog /var/log/apache/site2/access.log combined

        ErrorLog /var/log/apache/site2/error.log

</VirtualHost>
```

A diretiva **Listen** instrui o httpd a escutar endereços IP específicos ou portas específicas. Por padrão o servidor responde a requisições em todas interfaces IP. **Essa diretiva é obrigatória (a partir da versão 2.4)**, ou seja, se não estiver presente no arquivo de configuração, o servidor falhará ao iniciar. Diretivas múltiplas podem ser utilizadas para especificar diferentes endereços ou portas. Exemplo:

```
        Listen 80

        Listen 8000
```

Para especificar duas interfaces e suas portas, utiliza-se, por exemplo:

```
Listen 192.188.1.1:80

Listen 192.188.1.2:8000
```

Endereços IPv6 devem ser colocados entre colchetes:

```
Listen [2001:db8::a00:20ff:fea7:ccea]:80
```

Para o protocolo HTTPS (HTTP seguro), a porta padrão é 443, ou seja, se nada for especificado, o servidor assume essa porta. Para configurar outra porta:

```
Listen 192.188.1.2:9443 https
```

A diretiva **IndexIgnore** adiciona à lista de arquivos a serem escondidos quando listar um diretório. Pode utilizar caracteres coringas (“?” e “*”). Múltiplas diretivas IndexIgnore acrescentam na lista, ao invés de substituir. Por padrão, a lista contém “.” (o diretório corrente). Exemplo:

```
<Directory "/var/www">

    IndexIgnore *.bak .??* *~ *# HEADER* README* RCS CVS *,v *,t

</Directory>
```

A diretiva **KeepAlive** habilita/desabilita conexões HTTP persistentes. **MaxKeepAliveRequests** define o número máximo de requisições permitidas (0 = sem limite). **KeepAliveTimeout** define o tempo (em segundos) a esperar para a próxima requisição do mesmo cliente (na mesma conexão). Exemplo:

```
KeepAlive On

MaxKeepAliveRequests 50

KeepAliveTimeout 10
```

QUESTÕES COMENTADAS

1. **(CESPE/FUB - 2015) O Apache, que provê páginas por meio do protocolo HTTP, possui código-fonte aberto, funciona em ambiente multiplataforma, tanto no Windows quanto no Linux.**

Comentários:

O Apache é um servidor Web livre (possui código-fonte aberto) que funciona em ambiente multiplataforma (Windows, Novell, OS/2, Unix, Linux, FreeBSD etc.). Portanto, a questão está **correta**.

2. **(CESPE/STJ - 2015) Com relação ao servidor Apache, julgue o próximo item.**

As diretrizes <Directory> e <Files> são utilizadas em arquivos htaccess para permitir que usuários controlem o acesso a seus arquivos.

Comentários:

Essas duas diretrizes servem para delimitar quais diretrizes devem ser aplicadas a um diretório (<Directory>) e a arquivos (<Files>). Portanto, a questão está **errada**.

3. **(CESPE/STJ - 2015) Com relação ao servidor Apache, julgue o próximo item.**

Um administrador pode incluir uma configuração para determinado diretório por meio da diretriz <Directory>.

Comentários:

<Directory> é utilizada para definir um grupo de diretrizes que devem ser aplicadas apenas ao diretório definido, seus subdiretórios, e aos arquivos dentro deles. Exemplo:

```
<Directory "/usr/local/httpd/htdocs">
    Options Indexes FollowSymLinks
</Directory>
```

Portanto, a questão está **correta**.

4. **(FCC/Prefeitura de Teresina-PI - 2016) Uma das formas de se iniciar o servidor Apache é por meio do comando**

A) apache inic

B) apachectl start

C) apachectl run

D) apachectl go

E) apache send

Comentários:

Quando utilizado no modo de script de inicialização, o apachectl aceita como argumentos:

- start: inicializa o daemon httpd;
- stop: finaliza o daemon httpd;
- restart: reinicializa o daemon httpd. Se não estiver rodando, o httpd é inicializado;
- etc.

Portanto, a **alternativa B** está correta e é o gabarito da questão.

5. (CESPE/TRT8 - 2016) A diretiva que limita a apresentação dos arquivos que têm a extensão .conf, em um servidor Apache Web Server, é

A) Deny *.conf

B) Allow - conf

C) Directory *.conf

D) Location - conf

E) IndexIgnore *.conf

Comentários:

A diretiva IndexIgnore adiciona à lista de arquivos a serem escondidos quando listar um diretório. Pode utilizar caracteres coringas (“?” e “*”). Múltiplas diretivas IndexIgnore acrescentam na lista, ao invés de substituir. Por padrão, a lista contém “.” (o diretório corrente). Exemplo:

```
<Directory "/var/www">
        IndexIgnore *.conf
</Directory>
```

Portanto, a **alternativa E** está correta e é o gabarito da questão.

6. (FIOCRUZ/FIOCRUZ - 2016) São exemplos de comandos para reiniciar o Apache nas versões linux RedHat e Ubuntu, respectivamente:

A) service apache restart ou /etc/init.d/http restart.

B) service httpd restart ou /etc/init.d/apache2 restart.

C) /etc/init.d/apache2 reload ou /etc/init.d/apache2 restart.

D) /etc/init.d/httpd reload ou /etc/init.d/apache2 restart.

E) service apache reload ou /etc/init.d/http reload.

Comentários:

Para inicializar o httpd, vimos que um comando possível é apachectl start, mas há outras formas também, dependendo da distribuição utilizada:

- Red Hat: service httpd start;
- Ubuntu: /etc/init.d/apache2 start.

O argumento "start" pode ser trocado por "restart", "stop" etc., para as demais ações. Portanto, a **alternativa B** está correta e é o gabarito da questão.

7. (CCV-UFC/UFC - 2016) Qual das diretivas abaixo deve ser configurada no arquivo de configuração do servidor Apache para informar se serão aceitas ou não conexões HTTP persistentes?

A) Mutex.

B) Timeout.

C) KeepAlive.

D) CacheEnable.

E) HostnameLookups.

Comentários:

A diretiva KeepAlive habilita/desabilita conexões HTTP persistentes. MaxKeepAliveRequests define o número máximo de requisições permitidas (0 = sem limite). KeepAliveTimeout define o tempo (em segundos) a esperar para a próxima requisição do mesmo cliente (na mesma conexão). Exemplo:

```
KeepAlive On
MaxKeepAliveRequests 50
KeepAliveTimeout 10
```

Portanto, a **alternativa C** está correta e é o gabarito da questão.

8. (CS-UFG/CELG-GT-GO - 2017) Na configuração do Apache HTTP Server (httpd), o uso da diretiva <virtualHost> indica que o servidor Web irá

A) executar em uma máquina virtual.

B) executar em um servidor virtual em ambiente de nuvem

C) rodar mais de um website em uma mesma máquina.

D) ser replicado em várias máquinas, embora aparente ser um único host.

Comentários:

<VirtualHost> permite servir mais de um site no mesmo servidor (sites virtuais). Podem ser utilizadas diretivas específicas para o controle do site virtual, como nome do administrador, erros de acesso a página, controle de acesso e outros dados úteis para personalizar e gerenciar o site.

Portanto, a **alternativa C** está correta e é o gabarito da questão.

9. (SUGEP-UFRPE/UFRPE - 2018) Numa instalação com o Servidor Apache existe a necessidade de alterar o arquivo de configuração. O arquivo de configuração padrão do Apache é o arquivo:

A) httpd.conf

B) apch.ini

C) http.confg

D) apache.ini

E) apch.conf

Comentários:

No Linux é muito comum que o arquivo de configuração tenha a "extensão" .conf e muitas vezes o nome do arquivo é o mesmo nome do daemon, então fica httpd.conf. Ok, e no Windows? Segue o mesmo nome! Portanto, a **alternativa A** está correta e é o gabarito da questão.

10. (CESPE/ABIN - 2018) A determinação da porta e do endereço que o servidor Apache irá escutar deve ser feita por meio da diretiva listen. Sem sua definição, o servidor Apache se mantém fora de operação.

Comentários:

A diretiva Listen instrui o httpd a escutar endereços IP específicos ou portas específicas. Por padrão o servidor responde a requisições em todas interfaces IP. Essa diretiva é obrigatória (a partir da versão 2.4), ou seja, se não estiver presente no arquivo de configuração, o servidor falhará ao iniciar.

Pessoal, a questão não deixa claro qual a versão do Apache! Segundo a documentação, a partir da versão 2.4 seria obrigatória a diretiva listen! Na minha opinião, caberia recurso, pois a banca definiu como errada a questão!

Portanto, a questão está **errada**.

11. (Quadrix/CRM-PR - 2018) Um servidor Apache pode hospedar muitos sites web diferentes, simultaneamente, com o uso do método chamado de Virtual hosting.

Comentários:

Exato! E através de diretivas, pode ser utilizada a <VirtualHost>. Portanto, a questão está **correta**.

12. (FGV/Prefeitura de Niterói-RJ - 2018) O arquivo httpd.conf é o arquivo de configuração principal do servidor Web Apache. Ele contém diretivas que controlam o funcionamento do servidor.

Assinale a opção que indica a diretiva que pode ser usada para especificar endereço e portas alternativas para o servidor web receber requisições externas.

A) ServerRoot

B) Listen

C) AcceptFilter

D) Redirect

E) SetInputFilter

Comentários:

Para especificar duas interfaces e suas portas, utiliza-se, por exemplo:

Listen 192.188.1.1:80

Listen 192.188.1.2:8000

Portanto, a **alternativa B** está correta e é o gabarito da questão.

13. (CESPE/EBSERH - 2018) Para que arquivos para funcionamento de um sítio web armazenados no diretório /var/www/sitio01 fiquem acessíveis via HTTP usando o Apache, é necessário incluir, no arquivo de configuração do servidor, a seguinte linha.

DocumentRoot /var/www/sitio01

Comentários:

Existem dois tipos de páginas que podem ser adicionadas ao Apache: a página raiz e subpáginas. A página raiz é especificada através da diretiva DocumentRoot e será mostrada quando se entrar no domínio principal, como http://www.estrategiaconcursos.com.br. Na configuração padrão do Apache, DocumentRoot aponta

para o diretório /var/www. Esse diretório será assumido como raiz caso os diretórios não sejam iniciados por uma /:

home/estrategia -> aponta para /var/www/home/estrategia

/home/estrategia -> Aponta para /home/estrategia

Portanto, a questão está **correta**.

14. (FCC/SEMEF Manaus-AM - 2019) Um programador deseja reiniciar o Servidor HTTP Apache Versão 2.4 de forma que os visitantes ativos do site possam concluir os downloads em andamento antes de o servidor ser reiniciado. Para isso deve usar o comando

A) apachectl -k graceful

B) apachectl -j restart

C) restartserver -j graceful

D) start -s graceful-stop

E) runserver -j restart

Comentários:

Quando utilizado no modo de script de inicialização, o apachectl aceita como argumentos (pode-se utilizar "-k" antes do argumento):

- start: inicializa o daemon httpd;
- stop: finaliza o daemon httpd;
- restart: reinicializa o daemon httpd. Se não estiver rodando, o httpd é inicializado;
- graceful: reinicializa o daemon de forma "gentil". Se não estiver rodando, o httpd é inicializado. A diferença para uma inicialização normal é que as conexões correntes não são abortadas;
- graceful-stop: finaliza o daemon de forma "gentil". A diferença para uma finalização normal é que as conexões correntes não são abortadas;
- etc.

Portanto, a **alternativa A** está correta e é o gabarito da questão.

IIS (Internet Information Services)

O IIS (*Internet Information Services*) é um servidor Web criado pela Microsoft para seus sistemas operacionais para servidores. A versão mais recente é o IIS 10 (Windows Server 2016 e Windows 10). A função do IIS no Windows Server é oferecer uma plataforma para a **hospedagem de sites, serviços e aplicativos**, permitindo a integração das seguintes tecnologias: ASP.NET, FTP, PHP, WCF e o próprio IIS.

Uma de suas funcionalidades mais utilizadas é a geração de páginas HTML dinâmicas, através da tecnologia proprietária ASP (*Active Server Pages*), mas também pode utilizar outras tecnologias com adição de módulos de terceiros. Depois do lançamento da plataforma .NET (em 2002), o IIS ganhou também a função de gerenciar o ASP.NET. Este é formado basicamente por dois tipos de aplicações:

- Páginas Web: tradicionais acessadas por usuários (extensão ASPX);
- Web Services: funções disponibilizadas pela rede, chamada por aplicativos ASMX.

O ASP.NET é compilado antes da execução, trazendo vantagens no desempenho em relação às opções interpretadas, como o ASP e o PHP.

Algumas características do IIS são:

- Maximiza a segurança da Web através de um consumo de servidor reduzido e do isolamento automático de aplicativo;
- Implanta e executa o ASP.NET, o ASP clássico e os aplicativos Web do PHP no mesmo servidor;
- Faz o isolamento de aplicativo concedendo aos processos de trabalho, por padrão, uma identidade exclusiva e uma configuração de área restrita (maior segurança);
- Adiciona e remove os componentes internos do IIS, e até mesmo os substitui por módulos personalizados;
- Agiliza o site através de um cache dinâmico interno e de uma compactação avançada;
- Usa o Gerenciador do IIS para configurar recursos do IIS e administrar sites;
- Usa o protocolo FTP (*File Transfer Protocol*) para permitir que proprietários de site carreguem e baixam arquivos;
- Usa o Windows PowerShell para automatizar o gerenciamento da maioria das tarefas de administração do servidor Web;
- Configura vários servidores Web em um *farm* de servidores que podem ser gerenciados usando o IIS;
- O diretório base do site padrão é “UNIDADE:\Inetpub\wwwroot”, geralmente “C:\Inetpub\wwwroot”;
- O diretório base para o FTP é “UNIDADE:\Inetpub\ftproot”, geralmente “C:\inetpub\ftproot” (note que só muda o “www” por “ftp”).

Vamos falar um pouco sobre pool de aplicativos (*application pool* - IIS7/7.5):

Um pool de aplicativos define um grupo de um ou mais processos de trabalho, configurado com definições comuns que atendem uma ou mais aplicações atribuídas a este pool. Cada pool de aplicativos utiliza 1 ou 2 modos de integração .NET (**modo integrado e modo clássico**) para executar aplicações ASP.NET. O modo definido para o pool de aplicativos define como será processado qualquer requisição que chegar a esse pool.

Modo integrado: permite que o IIS processe requisições no pool de aplicativos utilizando o "Integrated Pipeline", o que permite que os módulos do ASP.NET participem do processamento das requisições.

Modo clássico: utiliza o pipeline de processamento do IIS 6, inicialmente as requisições são processadas através dos módulos do IIS7, as requisições do ASP.NET são transportadas para os "ISAPI Filter – aspnet_isapi.dll", o pipeline de processamento do ASP.NET é separado do pipeline de processamento do IIS7. Ou seja, o fluxo de processamento é muito mais lento do que o modo integrado.

Daria para entrar em detalhes em alguns itens abordados acima, mas para fins de concurso não vale a pena. Vamos focar no que as bancas costumam pedir!

Segurança: No Windows Server, durante a instalação do IIS, há opção de segurança "**Filtragem de solicitações**", que serve para analisar as requisições feitas ao servidor Web e impedir alguns ataques de manipulação de URL. Por padrão, a filtragem de solicitações no IIS 7.0 permite um comprimento máximo de URL de 4096 caracteres e de cadeia de caracteres de consulta um máximo de 2048 caracteres.

A "Filtragem de solicitações" verifica todas as requisições recebidas no servidor e as filtra com base nas regras definidas pelo administrador. Muitos ataques maliciosos compartilham características em comum, como URLs muito longas ou solicitações de uma ação rara. Ao filtrar as solicitações, há uma tentativa de reduzir o impacto desses tipos de ataques.

Mais duas informações importantes, que valem para os outros servidores Web também:

- A porta padrão para **requisições HTTP é a 80**;
- A porta padrão para **requisições HTTPS** (HTTP seguro) é a **443**.

QUESTÕES COMENTADAS

1. (CESPE/MEC - 2011) A partir da instalação do IIS é disponibilizado um sítio-padrão cujas pastas estão instaladas no servidor, no caminho físico c:\Inetpub\wwwroot.

Comentários:

O diretório base do site padrão é "UNIDADE:\Inetpub\wwwroot", geralmente "C:\Inetpub\wwwroot". Portanto, a questão está **correta**.

2. (FCC/TRT19 - 2011) O serviço que faz do Windows 2003 um Servidor Web é o IIS (Internet Information Services). Quando o IIS é instalado da maneira padrão, é disponibilizado um site com uma única página chamada iisstart.htm. Essa página pode ser encontrada no caminho físico

A) c:\Inetpub\wwwroot

B) c:\root\

C) c:\root\www

D) c:\http\www

E) c:\net\web

Comentários:

As bancas gostam dessa...repetindo:

O diretório base do site padrão é "UNIDADE:\Inetpub\wwwroot", geralmente "C:\Inetpub\wwwroot". Portanto, a **alternativa A** está correta e é o gabarito da questão.

3. (Quadrix/SERPRO - 2014) IIS e Apache são servidores cuja finalidade é:

A) prover serviços de impressão para o Windows e o Linux, respectivamente.

B) prover serviços WEB.

C) prover serviços de WEB e e-mail, respectivamente.

D) prover serviços de WEB para Linux e Windows, respectivamente.

E) viabilizar programas para execução de páginas HTML também conhecidos como browsers.

Comentários:

O Apache surgiu para sistema Unix-like, mas é multiplataforma (existe para Windows, por exemplo). O IIS é proprietário da Microsoft. Ambos são servidores Web. Portanto, a **alternativa B** está correta e é o gabarito da questão.

4. (UFRJ/UFRJ - 2015) Considere as seguintes afirmativas acerca do servidor Web IIS 7:

I – Nesta versão do IIS não é possível mais instalar e configurar o serviço FTP.

II - No IIS 7, os pools de aplicativos podem ser executados dos seguintes modos: integrado ou clássico.

III – No IIS 7, a porta padrão para servir páginas em HTTPS é a 4343.

Pode-se afirmar que:

A) apenas II e III estão corretas.

B) apenas I e II estão corretas.

C) apenas II está correta.

D) apenas I está correta.

E) I, II e III estão corretas.

Comentários:

(I) O FTP nunca foi desabilitado para o uso com o IIS. (II) Um pool de aplicativos define um grupo de um ou mais processos de trabalho, configurado com definições comuns que atendem uma ou mais aplicações atribuídas a este pool. Cada pool de aplicativos utiliza 1 ou 2 modos de integração .NET (modo integrado e modo clássico) para executar aplicações ASP.NET. O modo definido para o pool de aplicativos define como será processado qualquer requisição que chegar a esse pool. (III) A porta padrão para o HTTPS é 443 e a do HTTP é a 80. Portanto, a **alternativa C** está correta e é o gabarito da questão.

5. (Colégio Pedro II/Colégio Pedro II - 2016) Assinale a alternativa que NÃO apresenta uma característica do servidor de aplicação IIS.

A) Gera páginas HTML dinâmicas.

B) Também é um servidor de aplicativo.

C) Executa códigos PHP, Perl, Javascript e ASP.

D) Usa o protocolo FTP para permitir que proprietários de sites carreguem e baixem arquivos.

Comentários:

De tudo o que é descrito nas alternativas, sabemos que o IIS não executa códigos Perl! Lembrando: O IIS implanta e executa o ASP.NET, o ASP clássico e os aplicativos Web do PHP no mesmo servidor. Portanto, a **alternativa C** está correta e é o gabarito da questão.

6. (IBFC/EBSERH - 2016) Ao ser instalado o IIS (Internet Information Services), no disco rígido C:, por padrão os diretórios que serão criados para hospedagem de páginas e para FTP serão respectivamente:

A) C:/iisserver/wwwroot e C:/iisserver/ftproot

B) C:/inetpub/wwwroot e C:/inetpub/ftproot

C) C:/iisserver/wwwdir e C:/iisserver/ftpdir

D) C:/inetpub/wwwdir e C:/inetpub/ftpdir

E) C:/inetpub/rootwww e C:/inetpub/rootftp

Comentários:

Para hospedagem, já vimos em algumas questões que é "C:\inetpub\wwwroot" (note que a barra está invertida nas alternativas, mas tudo bem). Para o FTP é só substituir o "www" por "ftp": "C:\inetpub\ftproot".

Portanto, a **alternativa B** está correta e é o gabarito da questão.

7. (FCC/TRE-SP - 2017) Hipoteticamente, o Técnico, responsável pela administração do servidor com Windows Server 2012 do TRE-SP, realizou a instalação do serviço IIS com a configuração padrão de fornecimento. Considerando-se que ele não atribuiu o endereço IP e desligou o servidor da rede de computadores para evitar acesso externo, para que esse profissional realize o teste local do servidor IIS, ele deve utilizar um navegador e acessar, na Barra de endereços do navegador, a URL:

A) http://127.0.0.1

B) ftp://10.0.0.1

C) https://192.168.0.1

D) http://192.168.0.1

E) https://255.255.255.0

Comentários:

Na verdade, essa não é uma questão exclusiva para o IIS, pode ser para o Apache ou outro servidor Web! Para testar o servidor Web que está instalado na própria máquina é só fazer referência ao protocolo HTTP e o endereço do localhost (127.0.0.1), ou seja: "http://127.0.0.1". Se você colocar agora em seu navegador não deve aparecer uma mensagem como "Não é possível acessar esse site", a não ser que você tenha instalado um servidor Web (IIS, Apache ou outro)! Portanto, a **alternativa A** está correta e é o gabarito da questão.

8. (INAZ do Pará/DPE-PR - 2017) No Windows Server 2012, durante a instalação do Servidor WEB (IIS), que opção de segurança deve ser utilizada para analisar as requisições feitas ao servidor Web e impedir os ataques manipulando URLs?

A) Autenticação Digest, resolve o problema do firewall e de redes internas e externas.

B) Autenticação de Mapeamento de Certificado de Cliente.

C) Autenticação do Windows.

D) Restrições de IP e Domínio.

E) Filtragem de solicitações.

Comentários:

Segurança: No Windows Server, durante a instalação do IIS, há opção de segurança "Filtragem de solicitações", que serve para analisar as requisições feitas ao servidor Web e impedir alguns ataques de manipulação de URL. Por padrão, a filtragem de solicitações no IIS 7.0 permite um comprimento máximo de URL de 4096 caracteres e de cadeia de caracteres de consulta um máximo de 2048 caracteres.

A "Filtragem de solicitações" verifica todas as requisições recebidas no servidor e as filtra com base nas regras definidas pelo administrador. Muitos ataques maliciosos compartilham características em comum, como URLs muito longas ou solicitações de uma ação rara. Ao filtrar as solicitações, há uma tentativa de reduzir o impacto desses tipos de ataques.

Portanto, a **alternativa E** está correta e é o gabarito da questão.

9. (IBFC/IDAM - 2019) Quanto às diferenças entre os servidores Apache e IIS, analise as afirmativas abaixo, dê valores Verdadeiro (V) ou Falso (F).

( ) o Apache pode rodar em várias plataformas como o Windows, Unix e Linux.

( ) normalmente o servidor IIS utiliza a sua linguagem proprietária o ASP.

( ) somente o Apache é capaz de responder as requisições HTTP de máquinas clientes.

Assinale a alternativa que apresenta a sequência correta de cima para baixo.

A) V, F, F

B) V, V, F

C) F, V, V

D) F, F, V

Comentários:

(V) O Apache é multiplataforma, se você entrar do site http://apache.org/, poderá ver opções de download para Windows e Linux, por exemplo.

(V) Não somente o ASP, que é proprietária a Microsoft, como também outras linguagens.

(F) Claro que não! O IIS também faz isso! Além de outros servidores Web, pois isso é o conceito fundamental!

Portanto, a **alternativa B** está correta e é o gabarito da questão.

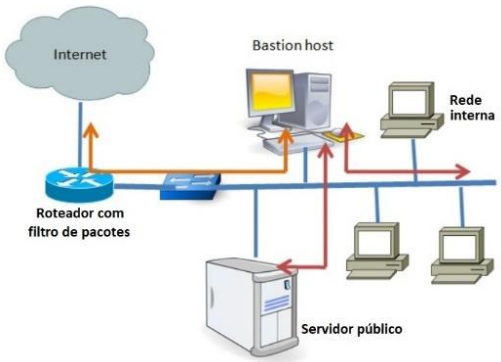
PROXY

Um proxy (procurador), também conhecido como gateway de aplicação, firewall de aplicação ou firewall proxy, implementa um nível de segurança mais robusto do que um filtro de pacotes (firewall que atua nas camadas de rede e transporte do modelo OSI, ex.: iptables). O proxy é um sistema capaz de receber uma conexão, decodificar protocolos na camada de aplicação e interceptar a comunicação entre cliente/servidor para aplicar regras de acesso. Abaixo vemos um exemplo de proxy, onde percebemos que o cliente tem a impressão que acessa diretamente o servidor, mas na verdade tem um intermediário.

Podemos ver que o proxy recebe o fluxo de conexão, tratando as requisições como se fossem uma aplicação e originando um novo pedido sob a responsabilidade do mesmo firewall (**proxy não transparente**) para o servidor de destino. A resposta para o pedido é recebida pelo proxy e analisada antes de ser entregue para o solicitante original. Ou seja, tem alguém no meio do caminho, fazendo o "cara-crachá", "bisbilhotando" todos os dados. Para que o proxy não transparente funcione é necessária a configuração de proxy nos navegadores dos clientes (Google Chrome, Internet Explorer etc.).

Outra arquitetura é o **proxy transparente**, que permite que o navegador cliente não saiba da existência do proxy (por isso tem esse nome!). Ele acha que está solicitando o recurso diretamente ao servidor original, sendo que o **proxy se encarrega de capturar e processar a solicitação**. A principal vantagem nessa arquitetura é que não é necessária a configuração de proxy nos navegadores dos clientes.

Os gateways de aplicações conectam as redes corporativas à Internet através de estações seguras (***bastion hosts***) que rodam aplicativos especializados para tratar e filtrar os dados (os proxies). Esses gateways, ao receberem as requisições de acesso dos usuários e realizarem uma segunda conexão externa para receber esses dados, acabam por esconder a identidade dos usuários nessas requisições externas, oferecendo uma proteção adicional contra a ação de invasores/criminosos. Abaixo vemos um exemplo de bastion host utilizado dentro da rede local e não no roteador, mas poderia ser o próprio roteador, tudo depende da arquitetura escolhida pelo administrador.



Como principal desvantagem temos que para cada novo serviço que aparece na Internet, o fabricante deve desenvolver o seu correspondente agente de Proxy. Por exemplo, um fabricante qualquer desenvolve um aplicativo de chat e cria seu próprio protocolo de comunicação. Como é um protocolo novo no mercado, os proxies levam algum tempo para "compreendê-lo", tornando o cliente vulnerável enquanto o fabricante não libera o agente específico.

Outro problema é que os proxies introduzem perda de desempenho na rede, já que as mensagens devem ser processadas pelo agente do proxy. Por exemplo, o serviço FTP manda um pedido ao agente do proxy para FTP, que por sua vez interpreta a solicitação e fala com o servidor FTP externo para completar o pedido.

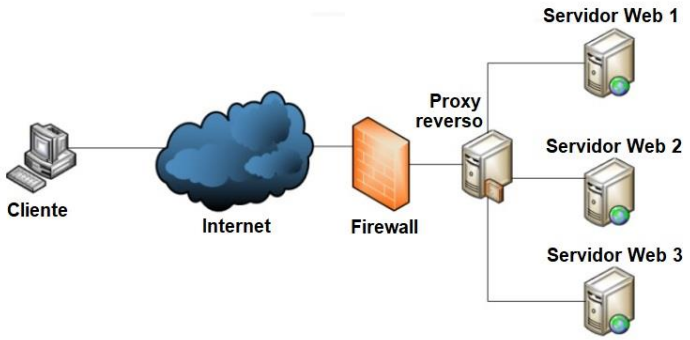
Alguns exemplos de regras típicas são todas as regras implementadas em filtros de pacotes, mais:

- Restringir acesso FTP a usuários anônimos;
- Restringir acesso HTTP para determinadas URLs (ex.: www.teste.com.br);
- Restringir acesso a protocolos desconhecidos na porta 443 (443 é a porta padrão do HTTPS no servidor);
- Entre outras.

Estamos acostumados com o conceito de proxy "de dentro para fora", ou seja, o cliente na rede local (LAN) e o servidor na WAN, até mesmo porque geralmente se utiliza o serviço de NAT (*Network Address Translation*) e não seria possível que "alguém lá de fora acessasse alguém da rede local". Bom, mas existe uma forma de fazer isso. Trata-se do **proxy reverso**, que funciona da seguinte maneira:

- Um servidor de rede geralmente instalado para ficar na frente de um servidor Web;
- Todas as conexões originadas externamente são endereçadas para um dos servidores Web através de um roteamento feito pelo servidor proxy, que pode tratar ele mesmo a requisição ou encaminhar a requisição toda ou parcialmente a um servidor Web, que a tratará.

Um proxy reverso repassa o tráfego de rede recebido para um conjunto de servidores, tornando-o a única interface para as requisições externas. Por exemplo, um proxy reverso pode ser usado para balancear a carga de um cluster de servidores Web. Isso é exatamente o oposto de um "proxy convencional", que age como um despachante para o tráfego de saída de uma rede, representando as requisições dos clientes internos para os servidores externos à rede a qual o servidor proxy atende. Abaixo podemos ver um exemplo de proxy reverso.



As **principais características de um proxy reverso** são:

- **Segurança**: o servidor proxy pode oferecer uma camada adicional de defesa através da separação ou isolamento do servidor que está por trás de um proxy reverso;

- **Criptografia**: a criptografia SSL pode ser delegada ao próprio servidor proxy, em vez dos servidores Web. Nesse caso, o servidor proxy pode ser dotado de aceleradores criptográficos de alto desempenho;

- **Balanceamento de carga**: o proxy reverso pode distribuir a carga para vários servidores, cada servidor responsável por sua própria aplicação. Dependendo da arquitetura da rede onde o servidor proxy reverso está instalado, o proxy reverso pode ter que modificar as URLs válidas externamente, para os endereços da rede interna;

- **Cache**: um proxy reverso pode aliviar a carga dos servidores Web através de um cache para o conteúdo estático (ex.: imagens) ou dinâmico (ex.: página HTML gerada por um sistema de gerenciamento de conteúdo);

- **Compressão**: um servidor proxy pode otimizar e comprimir o conteúdo, tornando o acesso mais rápido;

Spoon feeding **("colher de chá")**: uma página dinamicamente gerada pode ser produzida e enviada instantaneamente para o servidor proxy, que pode enviá-la aos poucos para o cliente requisitante. Assim, a aplicação Web não precisa esperar (e consumir recursos do servidor) caso o cliente apresente restrições de capacidade para receber conteúdo solicitado.

Squid

O Squid é o servidor proxy mais conhecido. Suporta FTP, HTTP, HTTPS, ICAP, ICP, HTCP, entre outros protocolos. Ele reduz a utilização da conexão e melhora os tempos de resposta armazenando cache de requisições frequentes de páginas Web. Ele pode também ser usado como um proxy reverso.

O Squid foi escrito originalmente para rodar em sistemas operacionais tipo Unix, mas também funciona em sistemas Windows desde sua versão 2.6.

Os navegadores podem usar o Squid local como um servidor Proxy HTTP, reduzindo o tempo de acesso aos objetos e reduzindo a utilização da conexão. Isso é muito utilizado por provedores no mundo todo para melhorar a velocidade de navegação para seus clientes e também em redes locais que compartilham a mesma conexão à Internet. Ele pode fornecer anonimato e segurança, pois é um intermediário no acesso aos objetos. No entanto a sua utilização pode gerar preocupações a respeito da privacidade pois o Squid é capaz de armazenar registros sobre os acessos, incluindo URLs acessadas, a data e hora exatas, e quem acessou. Isto é usado frequentemente nas empresas para controlar o acesso à Internet dos seus funcionários.

A aplicação cliente (geralmente o navegador) deverá especificar explicitamente o servidor proxy que quer utilizar (proxy não transparente), ou poderá utilizar um proxy transparente, em que todos os pedidos HTTP para "fora", são interceptados pelo Squid e todas as respostas são armazenadas em cache, não sendo necessário configurar o navegador.

O arquivo que permite configurar o Squid em ambiente tipo Unix, tais como o número da porta HTTP (**padrão = 3128**), pedidos de entrada e saída, informações de timeout e dados de acesso ao firewall é o **/etc/squid/squid.conf**. Abaixo podemos ver exemplos de linhas de configuração para definir um proxy transparente ou não:

```
# Proxy manual: Socket para conexões destinadas manualmente ao proxy (não transparente)

http_port 8080

# Proxy transparente: Socket para conexões redirecionadas ao proxy

http_port 3128 intercept
```

QUESTÕES COMENTADAS

1. **(Quadrix/CFO-DF - 2017) Um proxy pode ser considerado, ao mesmo tempo, como um servidor e um cliente.**

Comentários:

Abaixo vemos um exemplo de proxy, onde percebemos que o cliente tem a impressão que acessa diretamente o servidor, mas na verdade tem um intermediário.

Podemos ver que o proxy recebe o fluxo de conexão, tratando as requisições como se fossem uma aplicação e originando um novo pedido sob a responsabilidade do mesmo firewall (proxy não transparente) para o servidor de destino. A resposta para o pedido é recebida pelo proxy e analisada antes de ser entregue para o solicitante original. Ou seja, tem alguém no meio do caminho, fazendo o "cara-crachá", "bisbilhotando" todos os dados.

Nesse exemplo vemos que o proxy é servidor quando recebe uma solicitação do cliente e é cliente quando faz a solicitação para um servidor que está na Internet.

Portanto, a questão está **correta**.

2. **(Quadrix/CFO-DF - 2017) Os proxies são mecanismos eficientes na busca de páginas dos servidores. No entanto, eles não possuem recursos para filtrar conteúdo, como, por exemplo, impedir que funcionários acessem certos sites.**

Comentários:

A principal função de um proxy é filtrar dados, pois é um firewall que atua em todas as camadas. Alguns exemplos de regras típicas são todas as regras implementadas em filtros de pacotes (ex.: iptables), mais:

- Restringir acesso FTP a usuários anônimos;
- Restringir acesso HTTP para determinadas URLs (ex.: www.teste.com.br);
- Restringir acesso a protocolos desconhecidos na porta 443 (443 é a porta padrão do HTTPS no servidor);
- Entre outras.

Portanto, a questão está **errada**.

3. **(UTFPR/UTFPR - 2017) A respeito do SQUID, é correto afirmar que:**

A) não é possível realizar Proxy transparente, mas é possível aplicar políticas de controle de acesso a páginas da internet.

B) é um servidor Proxy cache com suporte para FTP, ICAP, ICP, HTCP e HTTP.

C) ele realiza o controle de acesso à internet, mas não permite o armazenamento dos Logs por mais de três dias.

D) ele não permite aplicar regras em horários agendados.

E) seu principal arquivo de configuração é o smbquid.conf.

Comentários:

O Squid é o servidor proxy mais conhecido. Suporta FTP, HTTP, HTTPS, ICAP, ICP, HTCP, entre outros protocolos. Ele reduz a utilização da conexão e melhora os tempos de resposta armazenando cache de requisições frequentes de páginas Web. Ele pode também ser usado como um proxy reverso. Portanto, a **alternativa B** está correta e é o gabarito da questão.

4. (IBFC/TJ-PE - 2017) Assinale a alternativa tecnicamente correta quanto ao conceito básico de Proxy Reverso:

A) servidor que recebe requisições de aplicações de clientes da internet e entrega a um único ponto de acesso à rede local.

B) equipamento ou hardware de rede utilizado para a interligação de redes idênticas mas com protocolos distintos.

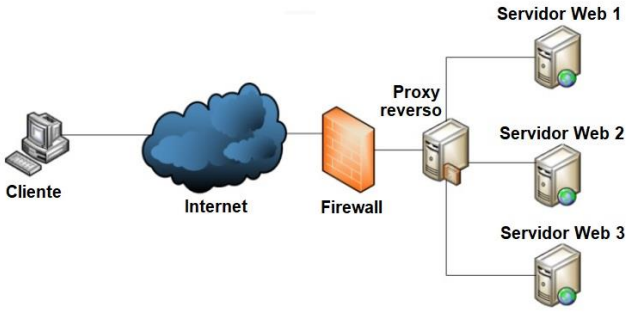
C) equipamento ou dispositivo de rede usado para fazer a comutação de protocolos com topologias diferentes de rede.

D) dispositivo de rede que cria uma rede agregada a partir de várias redes de computadores ou vários segmentos de rede.

E) dispositivo ou hardware de rede que demodula o sinal analógico recebido da internet e converte para o formato digital original.

Comentários:

Como vemos na figura abaixo, o cliente está na Internet e tem acesso a um único ponto na rede local (o proxy reverso) e ele distribui para o servidor adequado.



Portanto, a **alternativa A** está correta e é o gabarito da questão.

5. (IBFC/TJ-PE - 2017) O gerente de informática solicita a instalação de um proxy reverso. Para tanto, existem diversas razões para se instalar um proxy reverso. Identifique abaixo uma das características que NÃO se aplica tipicamente a um proxy reverso:

A) compressão

B) balanceamento de carga

C) tunelamento

D) caching

E) segurança

Comentários:

As principais características de um proxy reverso são:

- Segurança: o servidor proxy pode oferecer uma camada adicional de defesa através da separação ou isolamento do servidor que está por trás de um proxy reverso;

- Criptografia: a criptografia SSL pode ser delegada ao próprio servidor proxy, em vez dos servidores Web. Nesse caso, o servidor proxy pode ser dotado de aceleradores criptográficos de alto desempenho;

- Balanceamento de carga: o proxy reverso pode distribuir a carga para vários servidores, cada servidor responsável por sua própria aplicação. Dependendo da arquitetura da rede onde o servidor proxy reverso está instalado, o proxy reverso pode ter que modificar as URLs válidas externamente, para os endereços da rede interna;

- Cache: um proxy reverso pode aliviar a carga dos servidores Web através de um cache para o conteúdo estático (ex.: imagens) ou dinâmico (ex.: página HTML gerada por um sistema de gerenciamento de conteúdo);

- Compressão: um servidor proxy pode otimizar e comprimir o conteúdo, tornando o acesso mais rápido;

- *Spoon feeding* (“colher de chá”): uma página dinamicamente gerada pode ser produzida e enviada instantaneamente para o servidor proxy, que pode enviá-la aos poucos para o cliente requisitante. Assim, a aplicação Web não precisa esperar (e consumir recursos do servidor) caso o cliente apresente restrições de capacidade para receber conteúdo solicitado.

Portanto, a **alternativa C** está correta e é o gabarito da questão.

6. (FGV/SEPOG-RO - 2017) Filtrar e monitorar o tráfego da Internet é uma função muito importante que pode ser realizada pelo programa squid instalado em um servidor proxy transparente com uso de NAT. Considerando uma versão maior ou igual a 3.1 desse programa, e que utiliza a porta 3128 do protocolo IPv4, assinale a opção que apresenta a diretiva a ser colocada no arquivo de configuração proxy.conf para realizar adequadamente a função de proxy transparente com NAT.

A) http_port 3128 proxy

B) http_port 3128 nat

C) http_port 3128 gateway

D) http_port 3128 accel

E) http_port 3128 intercept

Comentários:

O arquivo que permite configurar o Squid em ambiente tipo Unix, tais como o número da porta HTTP (padrão = 3128), pedidos de entrada e saída, informações de timeout e dados de acesso ao firewall é o /etc/squid/squid.conf. Abaixo podemos ver exemplos de linhas de configuração para definir um proxy transparente ou não:

```
# Proxy manual: Socket para conexões destinadas manualmente ao proxy (não transparente)

http_port 8080

# Proxy transparente: Socket para conexões redirecionadas ao proxy

http_port 3128 intercept
```

Portanto, a **alternativa E** está correta e é o gabarito da questão.

7. (SUGEP-UFRPE/UFRPE - 2018) No Linux, as regras que permitem ou não acessos à Internet são configuradas no proxy server. O mais popular proxy server no Linux é:

A) Squid.

B) NIS.

C) PAM.

D) Gnome.

E) CUPS.

Comentários:

Squid é o servidor proxy mais conhecido, sem sombra de dúvidas!

NIS (Network Information Service) é um protocolo de serviço de diretório cliente/servidor para dados de configuração de sistemas distribuídos.

Gnome é um ambiente desktop completo para sistemas operacionais das famílias GNU/Linux e UNIX

CUPS (Common Unix Printing System) é um sistema de impressão modular para sistemas operacionais do tipo Unix.

Portanto, a **alternativa A** está correta e é o gabarito da questão.

8. (FCC/DPE-AM - 2018) Existem diferentes tipos de firewall para serem selecionados em uma implantação em uma rede local. A escolha do Técnico de Suporte foi pelo Proxy transparente devido à característica

A) da filtragem de pacotes maliciosos em que não há identificação do emissor.

B) de ser posicionado entre a Switch e o roteador da rede local, sendo transparente para o usuário.

C) da não necessidade de configurar cada um dos computadores com o endereço do Proxy.

D) de realizar a modificação do endereço IP destino do pacote de dados de forma automática.

E) da comunicação automática do IP e da Porta destino original para o Proxy quando o Gateway está em outra máquina.

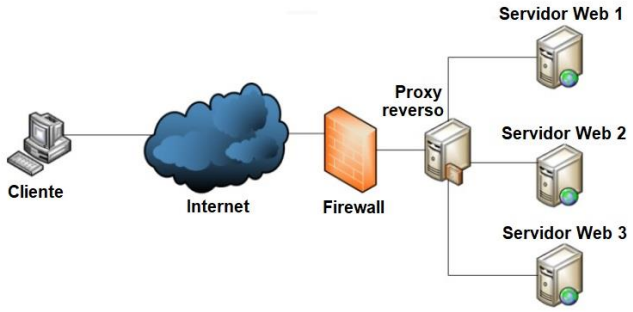
Comentários:

A arquitetura de proxy transparente permite que o navegador cliente não saiba da existência do proxy (por isso tem esse nome!). Ele acha que está solicitando o recurso diretamente ao servidor original, sendo que o proxy se encarrega de capturar e processar a solicitação. A principal vantagem nessa arquitetura é que não é necessária a configuração de proxy nos navegadores dos clientes. Portanto, a **alternativa C** está correta e é o gabarito da questão.

9. (CESPE/EMAP - 2018) O proxy reverso é um aparelho que busca a melhor forma de interconectar as requisições da porta 80 para Internet.

Comentários:

Na verdade, o proxy reverso recebe da Internet para a rede local, como podemos relembrar com a figura:



Portanto, a questão está **errada**.

10. (CESPE/Polícia Federal - 2018) Servidores proxy que atuam em nível de aplicação conseguem bloquear acesso a arquivos executáveis em conexões HTTP, o que não pode ser realizado com filtros de pacotes.

Comentários:

O proxy atua na camada 7 do modelo OSI (Aplicação), então pode "ler" tudo, os cabeçalhos e os dados! Então, consegue verificar e bloquear arquivos executáveis enviados via HTTP. E isso não pode ser realizado com filtros de pacotes, pois atuam nas camadas 3 (Rede) e 4 (Transporte) do modelo OSI. Os filtros de pacotes podem bloquear, por exemplo, endereços IP de origem ou destino, portas de origem ou destino, entre outras informações dos cabeçalhos das camadas 3 e 4. Portanto, a questão está **correta**.

11. (CESGRANRIO/Transpetro - 2018) O perímetro de segurança da técnica de defesa em profundidade é formado por componentes de segurança que funcionam de forma integrada para proteger a rede.

O componente que visa a intermediar a comunicação do nível de aplicação entre as estações da rede interna e os servidores da rede externa é o

A) IPS

B) IDS

C) Gateway VPN

D) Firewall de Estado

E) Firewall Proxy

Comentários:

IPS: Sistema de prevenção de intrusão.

IDS: Sistema de detecção de intrusão.

Firewall de estado: consegue analisar os pacotes dentro de uma mesma conexão.

Firewall proxy ou proxy: atua no nível de aplicação (camada 7 do modelo OSI).

Portanto, a **alternativa E** está correta e é o gabarito da questão.

12. (COMPERVE/UFRN - 2019) Existe um serviço que pode ser adicionado a uma rede local para garantir mais controle administrativo nos acessos dos usuários, filtrar conteúdo, prover mais segurança e ainda fornecer mecanismos de cache em redes. Esse serviço é conhecido por

A) Proxy.

B) HTTP.

C) QoS.

D) SMTP.

Comentários:

Um servidor proxy tem como principal função atuar como um firewall de camada de aplicação. Mas os servidores proxy comumente oferecem outras funcionalidades, como por exemplo caching. Portanto, a **alternativa A** está correta e é o gabarito da questão.

13. (VUNESP/Prefeitura de Valinhos-SP - 2019) Assinale a alternativa que apresenta uma funcionalidade de um servidor proxy reverso.

A) Balancear carga para servidores web.

B) Rotear pacotes na camada 3.

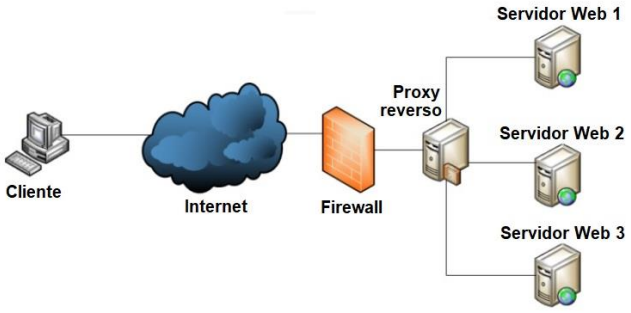
C) Prover serviços de monitoramento e gerenciamento de rede por SNMP.

D) Prover resolução de nomes de domínios em endereços IP.

E) Obter o endereço físico de rede (MAC address) a partir de um endereço IP.

Comentários:

Uma das funcionalidades é o balanceamento de carga. Na figura abaixo, por exemplo, pode ser aplicado um algoritmo para que cada requisição seja distribuída para um servidor Web, na ordem 1, 2, 3, volta para o 1, 2, 3, e assim por diante.



Portanto, a **alternativa A** está correta e é o gabarito da questão.

SERVIDORES DE E-MAIL

Protocolos de E-mail

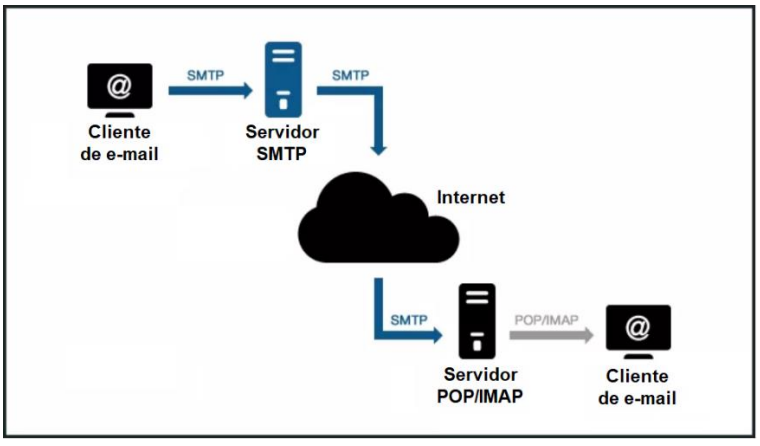
Antes de compreender como funcionam alguns serviços (servidores) de e-mail, é importante entender a diferença dos 3 protocolos mais utilizados para esse serviço. Esqueça por um instante a utilização de HTTP ou HTTPS, no caso dos Webmails, vamos focar nos protocolos exclusivos para e-mail mesmo, vamos lá...

SMTP (*Simple Mail Transfer Protocol*): utilizado quando o e-mail é entregue a partir de um cliente de e-mail (Outlook, Thunderbird, entre outros) a um servidor de e-mail ou quando o e-mail é entregue a partir de um servidor de e-mail para outro servidor. Ou seja, se você enviar um e-mail a partir de um software cliente, ele utilizará o SMTP até o seu servidor e depois o seu servidor utilizará também o SMTP para entregar ao servidor destino, quando este ficará na caixa de e-mails do usuário destinatário. **A porta padrão de um servidor SMTP é a 25**.

IMAP (*Internet Message Access Protocol*): também chamado de IMAP4, possui acesso a todas as pastas da conta de e-mail e deixa o *status* das mensagens igual tanto no servidor como no software e realiza a sincronia das mensagens, mantendo a conexão para que as alterações e mensagens novas recebidas sejam atualizadas quase que em tempo real. **A porta padrão de um servidor IMAP é a 143**.

POP (Post Office Protocol): mais conhecido como POP3, esse protocolo baixa as mensagens do servidor e as armazena localmente no computador, não deixando uma cópia das mensagens no servidor (a menos que seja marcada a opção "deixar uma cópia no servidor") nas configurações do programa de e-mail. Esse protocolo tem acesso apenas à Caixa de Entrada, não conseguindo baixar nenhuma outra pasta da conta de e-mail. **A porta padrão de um servidor POP3 é a 110**.

Abaixo podemos ver o relacionamento entre os 3 protocolos.



Podemos ver que a diferença principal é que o POP baixa as mensagens para o cliente local (permite que elas sejam armazenadas no servidor, mas não existe sincronia nesse processo). O IMAP4 é a evolução do POP3, sincronizando a caixa de e-mails com o conteúdo do servidor, permitindo que um e-mail seja sincronizado entre vários locais sem perda de mensagens entre locais diferentes (salvo diretórios locais, todas as mensagens dentro do diretório do e-mail são sincronizadas).

QUESTÕES COMENTADAS

1. (FCC/Prefeitura de Manaus-AM - 2019) Um Assistente de TI foi incumbido de configurar o protocolo para ser utilizado na troca de mensagens entre dois servidores de e-mail. A escolha correta do protocolo para essa finalidade é:

A) IMAP.

B) POP3.

C) SNMP.

D) SMTP.

E) POP4.

Comentários:

SMTP (Simple Mail Transfer Protocol): utilizado quando o e-mail é entregue a partir de um cliente de e-mail (Outlook, Thunderbird, entre outros) a um servidor de e-mail ou quando o e-mail é entregue a partir de um servidor de e-mail para outro servidor. Ou seja, se você enviar um e-mail a partir de um software cliente, ele utilizará o SMTP até o seu servidor e depois o seu servidor utilizará também o SMTP para entregar ao servidor destino, quando este ficará na caixa de e-mails do usuário destinatário. A porta padrão de um servidor SMTP é a 25. Portanto, a **alternativa D** está correta e é o gabarito da questão.

2. (UFMG/UFMG - 2019) Quais protocolos de envio e recebimento de mensagens os servidores de e-mails utilizam com frequência?

A) SMTP, Kerberos ou IMAP.

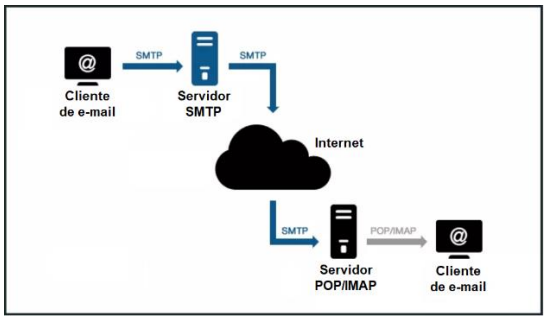
B) SMTP, POP3 ou LDAP.

C) SMTP, POP3 ou IMAP.

D) SMTP, Telnet ou IMAP.

Comentários:

Uma imagem fala mais que 1000 palavras 😊:



Portanto, a **alternativa C** está correta e é o gabarito da questão.

3. (FCC/Prefeitura de Manaus-AM - 2019) O protocolo IMAP (Internet Message Access Protocol)

A) baixa e exclui do servidor cada e-mail recebido.

B) é um protocolo apenas de envio, não permitindo que as mensagens de um servidor sejam descarregadas pelo usuário.

C) não fornece mecanismos para criar, destruir e manipular várias caixas de correio no servidor, recurso exclusivo do protocolo POP3.

D) pressupõe que todas as mensagens de correio eletrônico permanecerão no servidor indefinidamente, em várias caixas de correio.

E) supõe que o usuário limpará a caixa de correio em cada contato e trabalhará off-line depois disso.

Comentários:

IMAP (Internet Message Access Protocol): também chamado de IMAP4, possui acesso a todas as pastas da conta de e-mail e deixa o status das mensagens igual tanto no servidor como no software e realiza a sincronia das mensagens, mantendo a conexão para que as alterações e mensagens novas recebidas sejam atualizadas quase que em tempo real. A porta padrão de um servidor IMAP é a 143. Portanto, a **alternativa D** está correta e é o gabarito da questão.

MICROSOFT EXCHANGE SERVER E POSTFIX

Na sequência veremos alguns detalhes dos dois servidores mais cobrados em provas de concurso, o MS Exchange (para Windows) e o PostFix (para Linux).

Microsoft Exchange Server

O **Exchange Server** provê serviços de correio eletrônico e colaboração (principalmente organização em forma de calendário eletrônico). Esse servidor roda exclusivamente no sistema operacional Windows Server. Inicialmente utilizava o serviço de diretório X.400, mas migrou para o Active Directory (AD).

No início, o Exchange Server utilizava um protocolo proprietário para se comunicar com os clientes, o MAPI, mas teve que se render e adicionar suporte aos protocolos POP3, IMAP e EAS. O protocolo SMTP é utilizado para a comunicação com outros servidores de e-mail na Internet.

Há a possibilidade de licenciamento como *on-premises* (instalado e executado no computador) ou SaaS (*Software as a Service*). Na opção on-premises, os clientes adquirem licenças (CALs - *Customer Access Licenses*) e na opção SaaS, a Microsoft cobra uma taxa mensal.

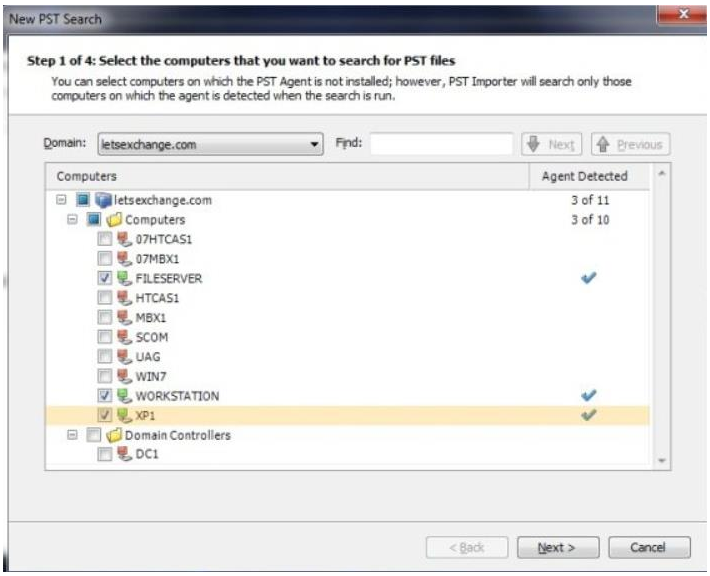
Retenção de Litígio

Colocar uma caixa de correio em "Retenção de Litígio" preserva todo o conteúdo da caixa de correio, incluindo itens excluídos e versões originais de itens modificados. Ao colocar uma caixa de correio em "Retenção de Litígio", a caixa de correio de arquivo morto do usuário (se habilitada) também é colocada em retenção. Itens excluídos e modificados são preservados por um determinado período, ou até a caixa de correio ser removida da retenção de litígio. Todos esses itens de caixa de correio são retornados em uma descoberta eletrônica na pesquisa do Exchange Server.

A retenção de litígio preserva itens na pasta "Itens Recuperáveis" **na caixa de correio do usuário**. O tamanho padrão dessa pasta é 30 GB. Dependendo da quantidade e do tamanho dos itens excluídos ou modificados, o tamanho da pasta Itens Recuperáveis da caixa de correio pode aumentar rapidamente. A pasta Itens Recuperáveis está configurada com uma cota alta por padrão.

Importante: A retenção de litígio pode ser aplicada em caixas de correio individuais ou em toda a empresa!

Microsoft Exchange PST Capture: ferramenta utilizada para descobrir e importar arquivos ".PST" para "dentro" do Exchange Server ou do Exchange Online. O PST Capture ajuda a organização a ter mais controle sobre os repositórios de e-mails, colocando-os "dentro" do Exchange. Os administradores podem determinar onde os arquivos ".PST" são colocados e quem é o dono do arquivo através do console da ferramenta PST Capture. Abaixo uma imagem que mostra uma busca por e-mails na rede.



Criação e Gerenciamento de Grupos de Distribuição

Através do Centro de Administração do Exchange (EAT) ou do PowerShell do Exchange Online, é possível criar um novo grupo de distribuição ou habilitar um grupo existente para e-mail.

Há dois tipos de grupos que podem ser utilizados para distribuir mensagens:

- Grupos de distribuição universal habilitados para e-mail (também chamados de grupos de distribuição): podem ser usados apenas para distribuir mensagens;
- Grupos de segurança universais habilitados para e-mail (também chamados de grupos de segurança): podem ser usados para distribuir mensagens, bem como para conceder permissões de acesso a recursos.

É importante observar as diferenças de terminologia entre o Active Directory e o Exchange Online. No Active Directory, um grupo de distribuição se refere a qualquer grupo que não tenha um contexto de segurança, seja ele habilitado para e-mail ou não. Por outro lado, no Exchange, todos os grupos habilitados para e-mail são chamados de grupos de distribuição, tenham ou não um contexto de segurança.

***Clustering* e *High Availability* (Alta disponibilidade)**: o Exchange Server Enterprise Edition suporta clustering com até 4 nodos utilizando o Windows 2000 Server, e até 8 nodos com o Windows Server 2003. O Exchange Server 2003 introduziu o active-active clustering, mas apenas para *cluster* com dois nodos. Nessa configuração, ambos os servidores do cluster são permitidos a serem ativos simultaneamente. Isso é o oposto do modo mais comum, o *active-passive*, no qual os servidores *failover* (servidor que assume um determinado serviço se outro servidor tem problemas) não podem ser utilizados enquanto o seu servidor correspondente estiver ativo. Por problemas de desempenho, o suporte ao modo ativo-ativo foi descontinuado com o Exchange Server 2007.

Versão 2019

Algo que chama a atenção é que o Exchange Server 2019 **só pode ser executado no Windows Server 2019**! Uma das novidades é que o Exchange Server pode ser executado no Windows Server Core. Além disso, **foi retirada a mensagem unificada (UM - *Unified Messaging*)**, que continua existindo no Exchange Online

(requer licença). O servidor UM integra correio de voz com e-mail (“tradicional”) no Exchange. Ou seja, com um servidor UM é possível que uma organização que utilize o Exchange o armazenamento de correio de voz e faxes (se ainda utilizam) junto com e-mails, calendário e contatos nas caixas de e-mail dos usuários. A versão 2019 suporta a execução em até 48 núcleos de processadores e 256 GB de memória RAM.

PostFix

No **Linux**, os servidores de e-mail mais comuns são o **sendmail** e o **postfix**. O postfix é considerado um MTA (Mail Transfer Agent) que se apresenta como alternativa ao sendmail, tendo como objetivo ser mais rápido, seguro e fácil de configurar que o sendmail, além de tentar manter a compatibilidade com ele. Vamos ver um pouco dos arquivos de configuração e funcionamento do postfix a seguir.

O postfix contém um arquivo denominado **main.cf**, no qual estão as configurações gerais do daemon, localizado no diretório **/etc/postfix**, pela instalação padrão. Abaixo serão demonstrados os principais parâmetros de configuração para ter-se um servidor de e-mail funcional. Nos exemplos abaixo será utilizado o nome do servidor como “mail.dominio.com.br” e o domínio “dominio.com.br”, apenas para ilustração.

myhostname = mail.dominio.com.br

mydomain = dominio.com.br

O parâmetro “mydestination” deve receber os domínios que o servidor de e-mail é responsável. Por exemplo, mail.dominio.com.br, ftp.dominio.com.br, www.dominio.com.br, dominio2.com.br etc.:

mydestination = $myhostname, localhost.$mydomain, $mydomain, mail.$mydomain, www.$mydomain, dominio2.com.br

O parâmetro “mynetworks” serve para determinar as redes do provedor:

mynetworks = 192.168.0.0/16, 127.0.0.0/8

Também podem ser informados os domínios em um arquivo:

mynetworks = /etc/postfix/mynetworks

Pela configuração padrão do postfix, ele permite relay de e-mails das suas redes e de seus domínios. Se houver clientes que não fazem parte da rede e que necessitam utilizar o seu servidor de e-mail para o envio de mensagens, é possível criar um arquivo com a lista de clientes através do parâmetro "smtpd_recipient_restrictions" e habilitar o envio de mensagens, como mostrado abaixo:

smtpd_recipient_restrictions = permit_mynetworks

check_client_access hash:/etc/postfix/client_access

check_relay_domains

Exemplo do arquivo /etc/postfix/client_access:

dial.amigos.com.br OK

10.0.0 OK

falcatrua.com.br REJECT

Esse parâmetro não consta na configuração padrão do postfix e pode ser incluído no final do arquivo de configuração main.cf.

A **entrega de e-mails no postfix** pode ser feita de diversas formas: enviando os e-mails para "/var/spool/mail/user" (padrão), no formato "Maildir/" (utilizado pelo qmail) entre outros.

Iniciando o servidor: # postfix start

Caso seja feita alguma alteração na configuração do servidor de e-mail, para atualizá-lo, basta digitar o comando: # postfix reload

Para desativar o servidor de e-mail: # postfix stop

Uma característica importante no Linux são os logs, que, na sua maioria, são armazenados em /var/log. Esse é o caso também dos logs relacionados aos servidores de e-mail, útil quando são necessárias informações sobre postfix, smtpd ou qualquer serviço relacionado ao e-mail que esteja sendo executado no servidor. Por padrão, esses logs ficam em **/var/log/maillog** ou **/var/log/mail.log**.

QUESTÕES COMENTADAS

1. **(FUNIVERSA/PC-DF - 2012) Em um servidor de e-mail com sistema operacional Linux, especialmente quando se utiliza o serviço Postfix, pode-se auditar o tráfego de entrada e saída de mensagens de correio eletrônico por meio dos registros conhecidos por logs. Em que arquivo desse sistema operacional encontram-se os logs das atividades de envio e recebimento de mensagens de correio eletrônico (e-mail)?**

A) No diretório “/etc/postfix”.

B) No arquivo “/var/log/maillog”.

C) Na pasta "/var/mail/<nome_do_usuário>".

D) No arquivo “/usr/local/bin/postfix”.

E) No arquivo de registro “/dev/tty”.

Comentários:

Uma característica importante no Linux são os logs, que, na sua maioria, são armazenados em /var/log. Esse é o caso também dos logs relacionados aos servidores de e-mail, útil quando são necessárias informações sobre postfix, smtpd ou qualquer serviço relacionado ao e-mail que esteja sendo executado no servidor. Por padrão, esses logs ficam em /var/log/maillog ou /var/log/mail.log. Portanto, a **alternativa B** está correta e é o gabarito da questão.

2. **(FUNCAB/MDA - 2014) São exemplos de servidores de correio eletrônico do Linux:**

A) postfix e sendmail.

B) fetchmail e sendmail.

C) pine e postfixe.

D) mail e pine.

E) samba e postfixe.

Comentários:

Alguns exemplos de servidores de e-mail no Linux: qmail, postfix e sendmail. Portanto, a **alternativa A** está correta e é o gabarito da questão.

3. **(FGV/TJ-GO - 2014) A empresa Y passou a adotar uma política de uso de software livre e resolveu mudar o seu correio eletrônico, que era baseado em Microsoft Exchange. O novo ambiente deveria**

rodar em ambiente Linux. Uma das possíveis escolhas do novo software de correio eletrônico recai no programa:

A) nginx;

B) puppet;

C) apache;

D) postfix;

E) bind.

Comentários:

Alguns exemplos de servidores de e-mail no Linux: qmail, postfix e sendmail. Portanto, a **alternativa D** está correta e é o gabarito da questão.

4. (CESPE/ANATEL - 2014) A unificação de mensagens do Microsoft Exchange Server 2010 combina mensagem de voz e email em uma caixa de entrada que pode ser acessada a partir do telefone e do computador.

Comentários:

Na versão 2019 do Microsoft Exchange Server, foi retirada a mensagem unificada (UM - Unified Messaging), que continua existindo no Exchange Online (requer licença). O servidor UM integra correio de voz com e-mail ("tradicional") no Exchange. Ou seja, com um servidor UM é possível que uma organização que utilize o Exchange o armazenamento de correio de voz e faxes (se ainda utilizam) junto com e-mails, calendário e contatos nas caixas de e-mail dos usuários. Como a questão fala da versão 2010, ainda tinha a unificação de mensagens. Portanto, a questão está **correta**.

5. (FGV/TJ-GO - 2014) A empresa Y passou a adotar uma política de uso de software livre e resolveu mudar o seu correio eletrônico, que era baseado em Microsoft Exchange. O novo ambiente deveria rodar em ambiente Linux. Uma das possíveis escolhas do novo software de correio eletrônico recai no programa:

A) nginx;

B) puppet;

C) apache;

D) postfix;

E) bind.

Comentários:

Nginx = servidor Web “leve”, proxy reverso, proxy de e-mail IMAP/POP3;

Puppet = utilitário para gerenciamento de configuração de código livre;

Apache = servidor Web;

Postfix = servidor de e-mail (software livre);

Bind = servidor DNS.

Portanto, a **alternativa D** está correta e é o gabarito da questão.

6. (CESPE/ANATEL - 2014) No Microsoft Exchange Server 2010, federação é uma tecnologia usada para a gestão de grupos de usuários, que são integrados a serviços de LDAP, o que permite que as contas de usuários sejam administradas e organizadas por meio de uma estrutura de árvores.

Comentários:

Um servidor de federação de conta emite tokens de segurança aos usuários com base na autenticação do usuário. O servidor autentica o usuário, extrai os atributos relevantes e as informações de associação de grupo do repositório de atributos, empacota essas informações em declarações, gera e assina um token de segurança (que contém as declarações) para retornar ao usuário, seja para ser usado em sua própria organização ou para ser enviado para uma organização parceira. Conceito bem diferente do apresentado na questão! Portanto, a questão está **errada**.

7. (Quadrix/COREN-BA - 2014) No Microsoft Exchange Server 2010 onde pode ser definida a Retenção de Litígio?

A) Nos arquivos e pastas compartilhados.

B) Nos arquivos e pastas exclusivos de cada usuário.

C) Na sessão iniciada por usuários de determinado grupo.

D) Nos grupos de usuários.

E) Em caixas de correio individuais ou em toda a empresa.

Comentários:

Colocar uma caixa de correio em “Retenção de Litígio” preserva todo o conteúdo da caixa de correio, incluindo itens excluídos e versões originais de itens modificados. Ao colocar uma caixa de correio em “Retenção de Litígio”, a caixa de correio de arquivo morto do usuário (se habilitada) também é colocada em retenção. Itens excluídos e modificados são preservados por um determinado período, ou até a caixa de

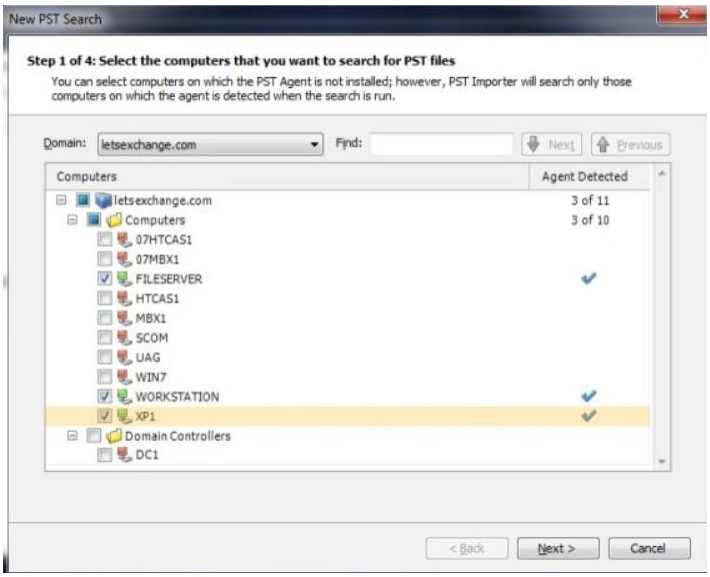
correio ser removida da retenção de litígio. Todos esses itens de caixa de correio são retornados em uma descoberta eletrônica na pesquisa do Exchange Server.

Importante: A retenção de litígio pode ser aplicada em caixas de correio individuais ou em toda a empresa! Portanto, a **alternativa E** está correta e é o gabarito da questão.

8. (CESPE/MEC - 2015) A ferramenta Exchange PST Capture possibilita a localização de arquivos PST nos computadores da rede e a importação automática nas caixas de correio do Exchange.

Comentários:

Microsoft Exchange PST Capture: ferramenta utilizada para descobrir e importar arquivos ".PST" para "dentro" do Exchange Server ou do Exchange Online. O PST Capture ajuda a organização a ter mais controle sobre os repositórios de e-mails, colocando-os "dentro" do Exchange. Os administradores podem determinar onde os arquivos ".PST" são colocados e quem é o dono do arquivo através do console da ferramenta PST Capture. Abaixo uma imagem que mostra uma busca por e-mails na rede.



Portanto, a questão está **correta**.

9. (FGV/TCE-SE - 2015) Em um ambiente com Active Directory, deseja-se usar o Exchange para enviar e-mails para um conjunto de usuários, usando um tipo de grupo do AD DS. Trata-se do Grupo:

A) de distribuição;

B) de envio;

C) de segurança;

D) universal;

E) de diretório.

Comentários:

Há dois tipos de grupos que podem ser utilizados para distribuir mensagens:

- Grupos de distribuição universal habilitados para e-mail (também chamados de grupos de distribuição): podem ser usados apenas para distribuir mensagens;
- Grupos de segurança universais habilitados para e-mail (também chamados de grupos de segurança): podem ser usados para distribuir mensagens, bem como para conceder permissões de acesso a recursos.

É importante observar as diferenças de terminologia entre o Active Directory e o Exchange Online. No Active Directory, um grupo de distribuição se refere a qualquer grupo que não tenha um contexto de segurança, seja ele habilitado para e-mail ou não. Por outro lado, no Exchange, todos os grupos habilitados para e-mail são chamados de grupos de distribuição, tenham ou não um contexto de segurança.

Portanto, a **alternativa A** está correta e é o gabarito da questão.

10. (CESPE/TCE-PA - 2016) Para utilizar o clustering de failover nos servidores Windows, os serviços como Microsoft Exchange Server podem ser executados em máquinas físicas, mas não em máquinas virtuais.

Comentários:

Nem tem isso no conteúdo da aula, mas é algo intuitivo! Quando falamos em clustering, redundância de servidores etc., uma das tecnologias que mais tem sido utilizada é a virtualização! Não tem lógica um produto a ser instalado em um servidor não permitir a execução dentro de uma máquina virtual! Portanto, a questão está **errada**.

11. (UPENET-IAUPE/UPE - 2017) Qual grupo abaixo do AD DS em um ambiente com Active Directory deve ser, necessariamente, empregado para o envio de mensagens eletrônicas, utilizando o Exchange?

A) Ativo

B) Envio

C) Distribuição

D) Segurança

E) Usuários

Comentários:

Note que esse assunto já foi abordado por outra banca! Vou replicar justificativa abaixo, para reforçar...

Há dois tipos de grupos que podem ser utilizados para distribuir mensagens:

- Grupos de distribuição universal habilitados para e-mail (também chamados de grupos de distribuição): podem ser usados apenas para distribuir mensagens;
- Grupos de segurança universais habilitados para e-mail (também chamados de grupos de segurança): podem ser usados para distribuir mensagens, bem como para conceder permissões de acesso a recursos.

É importante observar as diferenças de terminologia entre o Active Directory e o Exchange Online. No Active Directory, um grupo de distribuição se refere a qualquer grupo que não tenha um contexto de segurança, seja ele habilitado para e-mail ou não. Por outro lado, no Exchange, todos os grupos habilitados para e-mail são chamados de grupos de distribuição, tenham ou não um contexto de segurança.

Portanto, a **alternativa C** está correta e é o gabarito da questão.

12. (FCC/Prefeitura de Manaus-AM - 2019) Um Assistente de TI foi incumbido de configurar o protocolo para ser utilizado na troca de mensagens entre dois servidores de e-mail. A escolha correta do protocolo para essa finalidade é:

A) IMAP.

B) POP3.

C) SNMP.

D) SMTP.

E) POP4.

Comentários:

SMTP (Simple Mail Transfer Protocol): utilizado quando o e-mail é entregue a partir de um cliente de e-mail (Outlook, Thunderbird, entre outros) a um servidor de e-mail ou quando o e-mail é entregue a partir de um servidor de e-mail para outro servidor. Ou seja, se você enviar um e-mail a partir de um software cliente, ele utilizará o SMTP até o seu servidor e depois o seu servidor utilizará também o SMTP para entregar ao servidor destino, quando este ficará na caixa de e-mails do usuário destinatário. A porta padrão de um servidor SMTP é a 25. Portanto, a **alternativa D** está correta e é o gabarito da questão.

FTP (File Transfer Protocol)

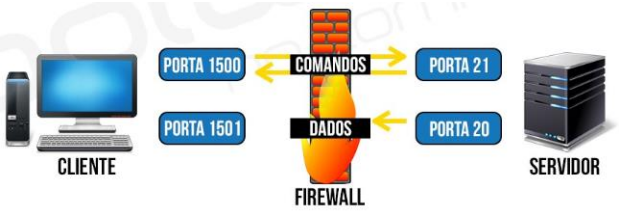
Como o próprio nome deixa claro, o FTP é um protocolo de transferência de arquivos. Trata-se de um protocolo padrão, independente de hardware. O FTP é baseado no protocolo de transporte TCP, o que garante a entrega dos pacotes. O servidor FTP utiliza as **portas 20 para os dados e a 21 para o controle**. Vamos ver como ele funciona:

Um cliente realiza uma conexão TCP para a porta 21 do servidor. Essa conexão (conexão de controle) permanece aberta ao longo da sessão enquanto uma segunda conexão (conexão de dados), é estabelecida na porta 20 do servidor e em alguma porta do cliente (comunicada no diálogo entre cliente e servidor). A conexão de controle (porta 21) é utilizada para administração da sessão (comandos, identificação) entre cliente e servidor.

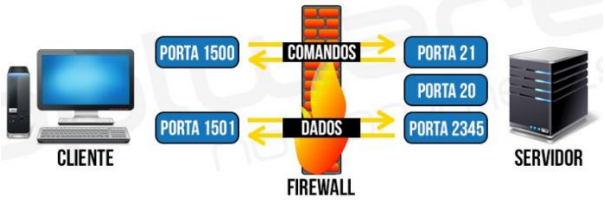
O servidor responde na conexão de controle com três dígitos de código de estado em ASCII com uma mensagem de texto opcional. Por exemplo, “200” ou “200 OK” significa que o último comando obteve êxito. Os números representam o número do código e o texto opcional representa as explicações ou parâmetros necessários. Uma transferência de arquivo em progresso, sobre uma conexão de dados, pode ser abortada utilizando uma mensagem de interrupção enviada sobre a conexão de controle.

O FTP pode ser executado em modo ativo ou passivo, os quais determinam como a conexão de dados é estabelecida. No **modo ativo**, o cliente envia para o servidor o endereço IP e o número da porta na qual ele irá ouvir e então o servidor inicia a conexão TCP. No exemplo abaixo vemos que o cliente informou ao servidor que a porta 1501 aguardará uma conexão vinda do servidor para receber os dados.

Mas e se houver um firewall que não tenha liberado a porta 1501? Olhe o que acontece:



Em situações onde o cliente está atrás de um firewall e inapto para aceitar entradas de conexões TCP, o **modo passivo** pode ser utilizado. O cliente envia um comando PASV para o servidor e recebe um endereço IP e um número de porta como resposta, os quais o cliente utiliza para abrir a conexão de dados com o servidor. Na figura abaixo podemos ver que o cliente solicitou uma conexão no modo passivo e o servidor “disse”: “Vou abrir a porta 2345 e você pode se conectar nela para receber os dados”. Então, nesse caso, a porta 20 não será utilizada.



A transferência de dados pode ser feita em qualquer um dos três modos a seguir:

- Modo fluxo: dado é enviado como um fluxo contínuo, liberando o FTP de fazer algum processamento. Todo processamento é deixado para o TCP. Nenhum indicador de fim de arquivo é necessário, a menos que o dado esteja dividido dentro de registros;
- Modo de bloco: o FTP quebra o dado dentro de vários blocos (bloco de cabeçalho, contagem de byte e campo de dado) e então passa-o para o TCP;
- Modo comprimido: dado é comprimido utilizando um algoritmo simples.

O **acesso a servidores FTP** pode ocorrer de dois modos: através de uma interface ou através da linha de comando. Tanto usuários Linux como usuários Windows podem acessar através dos dois modos. O modo linha de comando está presente em qualquer distribuição Linux-like e Windows.

A partir de qualquer navegador credenciado (Internet Explorer, Chrome, Firefox, entre outros), também é possível acessar um servidor FTP digitando na barra de endereço:

ftp://[username]:[password]@[servidor]

ou

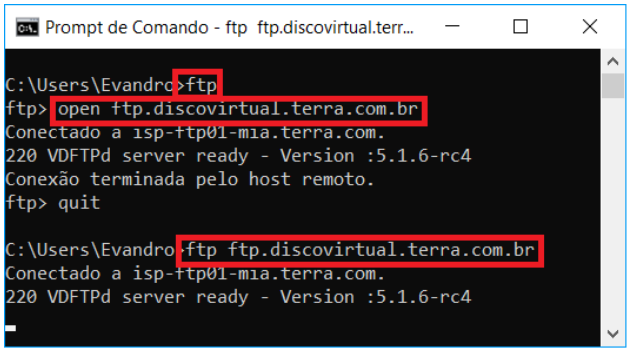
ftp://[username]:[password]@[servidor]:[porta]

Os **comandos** abaixo podem ser executados no FTP **através da linha de comando**. Os comandos do FTP podem ser abreviados, desde que não formem expressões ambíguas.

- !: executa o comando na máquina local;
- ?: semelhante a help;
- append: adiciona dados a um arquivo existente;
- ascii: configura o tipo de transferência de arquivos para ASCII;
- bell: emite um bip quando um comando é executado;
- binary: configura o tipo de transferência de arquivos para binário;
- bye: encerra a sessão FTP;
- cd: seguido de caminho/diretório muda para o diretório informado;
- delete: apaga um arquivo. Para mais de um arquivo utiliza-se mdelete;
- debug: estabelece a modalidade de depuração;
- dir: mostra o conteúdo do diretório servidor atual;
- disconnect: semelhante a bye;
- get: obtém um arquivo do servidor. Para mais de um arquivo utiliza-se mget;
- glob: seleciona a expansão para nomes de arquivo;
- hash: demonstra cada bloco do arquivo durante a transferência. Cada bloco compõe-se de 1024 bytes;

- help: lista sumariamente todos comandos disponíveis;
- literal: permite enviar comandos arbitrários;
- ls: mostra uma lista abreviada do conteúdo do diretório servidor. Para mais de uma pasta utiliza-se mls;
- mkdir: cria um diretório ou subdiretório no servidor;
- prompt: ativa/desativa o modo interativo;
- put: envia um arquivo ao servidor. Para enviar mais de um arquivo utiliza-se mput;
- pwd: mostra o diretório de trabalho;
- quit: finaliza a sessão FTP;
- quote: envia subcomandos do servidor FTP, como se encontram no servidor;
- recv: similar a get;
- remotehelp: solicita ajuda do servidor FTP remoto;
- rename: renomeia um arquivo;
- send: semelhante a put;
- status: obtém informações de estado do servidor;
- trace: demonstra o caminho percorrido pelo arquivo na transferência;
- type: especifica o tipo de representação;
- user: inicia a sessão no servidor;
- verbose: ativa/desativa a modalidade literal.

Para o cliente se conectar ao servidor via linha de comando, pode executar “ftp” e depois utilizar o comando “open”, ou executar com o endereço como parâmetro: “ftp endereço”:



QUESTÕES COMENTADAS

1. (FGV/MPE-AL - 2018) O FTP (File Transfer Protocol) é um protocolo de aplicação da arquitetura TCP/IP, utilizado para transferência de arquivos entre o servidor e os clientes.

Considerando as características de funcionamento do FTP, assinale a afirmativa correta.

A) O FTP utiliza o protocolo UDP na camada de transporte, a fim de garantir o estabelecimento da conexão de controle.

B) A RFC 959 define a porta 21/TCP como porta padrão de conexão ao servidor para transferência dos dados, a qual é utilizada também para a conexão de controle.

C) Ao configurar um servidor FTP como enjaulado (chroot), os clientes têm acesso a toda a árvore de diretórios do servidor.

D) Nas conexões anônimas, o servidor FTP utiliza a porta 20 para conexões de dados e controle de sessão, para diferenciá-las das conexões autenticadas.

E) Em uma rede em que haja um firewall entre o servidor e os clientes, é necessário autorizar o acesso ao servidor nas portas 20 e 21.

Comentários:

Um servidor FTP, por padrão, "escuta" a porta 21 para receber conexões de clientes. Depois utiliza a porta 20 para solicitar uma conexão com o cliente para enviar os dados. Ou seja, a porta 21 serve para o controle (comandos) e a 20 para os dados em si (arquivos). Por isso, se houver um firewall entre os clientes e o servidor, as portas 20 e 21 (TCP) devem estar liberadas. Portanto, a **alternativa E** está correta e é o gabarito da questão.

2. (COMPERVE/UFRN - 2018) A especificação original do protocolo FTP foi publicada pela RFC 114, em 1971 e, em 1980, foi substituída pela RFC 765. A versão atual da especificação desse protocolo é a RFC 959 que foi publicada em outubro de 1985. Desde sua implementação, esse protocolo vem sendo de grande importância no cenário das redes de computadores.

Com relação ao protocolo FTP, considere os seguintes objetivos apresentados abaixo.

I Promover a transferência de arquivos de maneira eficiente.

II Possibilitar diretamente a troca de mensagens entre usuários de computadores remotos.

III Permitir o controle de acesso de usuários a programas remotos em execução.

IV Encorajar indiretamente ou implicitamente (via programas) o uso de computadores remotos.

Dentre esses objetivos, os que dizem respeito ao protocolo FTP são

A) III e IV.

B) II e III.

C) I e II.

D) I e IV.

Comentários:

(I) O propósito do FTP é a transferência de arquivos, até o nome deixa bem claro isso. (II) O FTP possibilita o envio de comandos e a transferência de arquivos, não tem nada a ver com mensagens. (III) FTP não tem a função de controlas o a cesso de usuários, isso seria a função de mecanismos de segurança. (IV) Um pouco forçada essa, mas é o que sobrou...então podemos dizer que o FTP "encoraja" o uso de computadores remotos. Portanto, a **alternativa D** está correta e é o gabarito da questão.

3. (FGV/MPE-AL - 2018) Utilizando o FTP através de linha de comando (CLI), indique o comando que você deve utilizar para se conectar a um servidor de FTP depois de iniciar o cliente.

A) connect, seguido pelo endereço do servidor.

B) login, seguido pelo endereço do servidor.

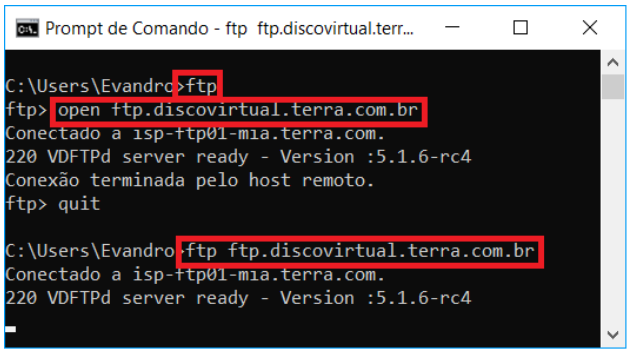
C) logon, seguido pelo endereço do servidor

D) open, seguido pelo endereço do servidor.

E) server, seguido pelo endereço do servidor.

Comentários:

Para o cliente se conectar ao servidor via linha de comando, pode executar "ftp" e depois utilizar o comando "open", ou executar com o endereço como parâmetro: "ftp endereço":



Portanto, a **alternativa D** está correta e é o gabarito da questão.

ESSA LEI TODO MUNDO CONHECE:
PIRATARIA É CRIME.

Mas é sempre bom revisar o porquê e como você pode ser prejudicado com essa prática.

1. 

Professor investe seu tempo para elaborar os cursos e o site os coloca à venda.

2. 

Pirata divulga ilicitamente (grupos de rateio), utilizando-se do anonimato, nomes falsos ou laranjas (geralmente o pirata se anuncia como formador de "grupos solidários" de rateio que não visam lucro).

3. 

Pirata cria alunos fake praticando falsidade ideológica, comprando cursos do site em nome de pessoas aleatórias (usando nome, CPF, endereço e telefone de terceiros sem autorização).

4. 

Pirata compra, muitas vezes, clonando cartões de crédito (por vezes o sistema anti-fraude não consegue identificar o golpe a tempo).

5. 

Pirata fere os Termos de Uso, adultera as aulas e retira a identificação dos arquivos PDF (justamente porque a atividade é ilegal e ele não quer que seus fakes sejam identificados).

6. 

Pirata revende as aulas protegidas por direitos autorais, praticando concorrência desleal e em flagrante desrespeito à Lei de Direitos Autorais (Lei 9.610/98).

7. 

Concurseiro(a) desinformado participa de rateio, achando que nada disso está acontecendo e esperando se tornar servidor público para exigir o cumprimento das leis.

8. 

O professor que elaborou o curso não ganha nada, o site não recebe nada, e a pessoa que praticou todos os ilícitos anteriores (pirata) fica com o lucro.

Deixando de lado esse mar de sujeira, aproveitamos para agradecer a todos que adquirem os cursos honestamente e permitem que o site continue existindo.