# UNIDADE 4 – CONCEITOS INTRODUTÓRIOS DE SEGURANÇA DE REDES: NAT, PAT, ACL E DMZ

## MÓDULO 1 – MECANISMOS DE CONTROLE E DEFESA.

01

## 1 - PROPRIEDADES DE UMA COMUNICAÇÃO SEGURA

Conforme Monteiro & Boavida (2011) as boas práticas são decorrentes de uma política de segurança, um instrumento para proteger uma instituição contra ameaças à segurança da informação que a ela pertence ou que está sob responsabilidade dela.

A rede, principalmente a Internet, torna-se recurso de comunicação crítico para a generalidade das organizações que, dificilmente, conseguem exercer a sua atividade sem acesso à rede. Há boas comunidades, porém há os "maus" utilizadores. Por isso vários protocolos Internet suportam mecanismos de segurança. Ex.: SMTP que não valida endereços de envio e de destino.

A segurança não é assegurada exclusivamente por um firewall. É uma tarefa complexa que necessita de planejamento e uma estratégia de implementação e sempre utilize uma combinação de firewall, controle de acesso IEEE 802.1X e VPN TLS/SSL.

Ainda conforme os autores citados, uma comunicação segura deve ter as seguintes **propriedades**:

**1-Confidencialidade**

**2-Integridade**

**3-Autenticidade**

Essas propriedades são implementadas com recursos de técnicas de criptografia, chaves simétricas e de chaves públicas, utilizadas em diversos protocolos.

Confidencialidade

Conteúdo da mensagem conhecido somente pelas entidades envolvidas na comunicação. O emissor cifra a mesma e o receptor a decifra. Ex.: criptografia de chave pública RSA a ser vista mais adiante.

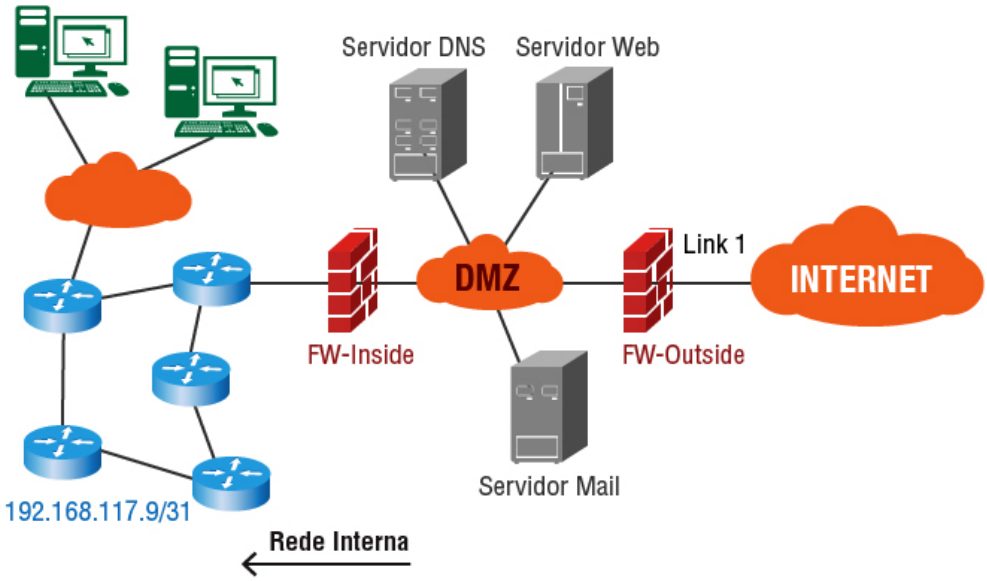
Integridade

Mensagem sem sofrer alterações intencionais ou acidentais no corpo da mesma durante a sua transmissão. Usa mecanismos de hashing para evitar as modificações.

| Autenticidade<br><br>Propriedade que permite as entidades, envolvidas na comunicação, confirmar mutuamente as mesmas. |
|---|

02

A figura a seguir mostra uma típica conexão de uma rede corporativa (rede interna) ao mundo externo. A DMZ (DeMilitarized Zone) abriga os elementos que têm aceso direto e irrestrito ao mundo externo. No caso a FW-inside (firewall) e os servidores DNS e Web seriam os primeiros a serem atacados.




**Cenário da proteção à rede interna**

Conforme SANTOS (2011) um **Firewall** filtra pacotes que entram e que saem da rede de modo a evitar que pacotes contendo conteúdo nocivo atinjam a rede e causem prejuízos. Os filtros examinam as informações do pacote desde o número da porta de comunicação até a assinatura da aplicação que está sendo transportada. Analisam as informações da camada 3 (IP de origem, IP de destino); camada 4 (portas TCP e UDP) e camada 7 (cabeçalhos de determinadas aplicações). No caso da Cisco, conforme a CCNA (2005), ela tem um firewall chamado **ASA** (Adaptative Security Appliance).

03

## 2 – Identificação de Ameaças - Ataques

A identificação de ameaças, abaixo listadas, conforme NAKAMURA (2007) pode ser realizada da forma que se segue:

**a)** **DoS** (Denial of Service – em português, ataques de negação de serviço) - tem o propósito de parar determinados serviços ou elementos da rede. Podem ser do tipo:

- Destroyers;
- Crashers;
- Flood.

**b)** **Reconnaissance Attacks** (Ataques de reconhecimento) - têm por objetivo obter informações importantes que possam ser utilizadas em um ataque de acesso. Seu efeito colateral é derrubar a rede. Por exemplo: descobrir os endereços IP dos servidores ou dos roteadores de uma rede, para depois identificar quais são os mais vulneráveis a determinado ataque.

**c)** **Access Atacks** - são ataques que objetivam roubar dados, buscando-se vantagem financeira. Roubo de informações privilegiadas sobre alguma corporação que possa ser vendidas aos concorrentes. Exemplos de ataque: acesso aberto via rede Wireless (wifi); Laptops infectados; funcionários insatisfeitos.

Para esses ataques, a Cisco tem uma ferramenta chamada de **NAC** (Network Admission Control) que previne contra os dois primeiros tipos de ataque.

Os ataques **DoS** (Denial of Service) e **DDoS** (Distributed Denial of Service) são os mais corriqueiros e comuns.

| Destroyers |
| --- |
| Danificar alvos por meio de comprometimento dos dados ou de *software*. |

| Crashers |
| --- |
| Rompem conexões do host com a rede. |

| Flood |
| --- |
| Inundam a rede com pacotes tornando-a inutilizável. |

| NAC |
| --- |
| Essa ferramenta monitora a primeira conexão dos dispositivos de rede impedindo que um PC se conecte à rede sem ter a base de assinatura antivírus atualizada e implementa um sistema de autenticação com nome de usuário e senha para evitar que qualquer pessoa sem autorização tenha acesso à rede. |

04

De acordo com a definição do **CERT** (**C**omputer **E**mergency **R**esponse **T**eam), os ataques **DoS** (Denial of Service), também denominados Ataques de Negação de Serviços, consistem em **tentativas de impedir que usuários legítimos utilizem determinados serviços** de um computador ou de um grupo de computadores.

Para isso, são aplicadas várias técnicas para:

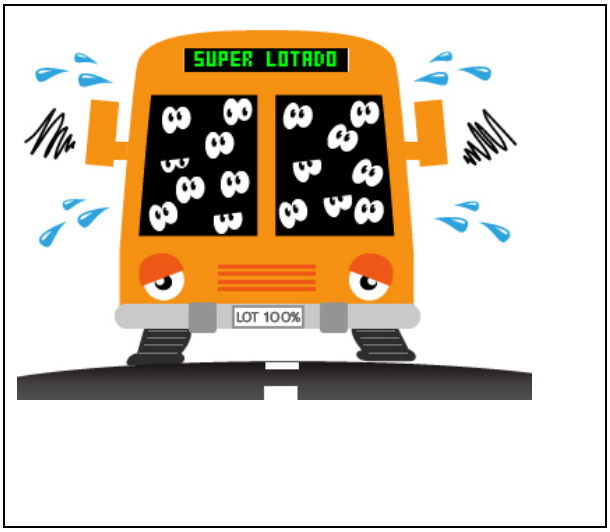
a) sobrecarregar uma rede a tal ponto em que os verdadeiros usuários não consigam utilizá-la;

b) derrubar uma conexão entre dois ou mais computadores;

c) fazer uma quantidade grande de requisições a um site até que os servidores deste não consigam mais ser acessados, e

d) negar acesso a um sistema ou a determinados usuários.

**Para melhor entendimento**: imagine o caso em que você utiliza um ônibus regularmente para ir ao trabalho. No entanto, em um determinado dia, uma quantidade enorme de pessoas furou a fila e entrou no veículo, deixando-o tão lotado que você e os outros passageiros regulares não conseguiram entrar. Imagine que você tenha conseguido entrar no ônibus, mas este ficou tão cheio que não conseguiu sair do lugar por excesso de peso. **Conclusão**: este ônibus acabou negando o seu serviço - o de transportá-lo até um local -, pois recebeu mais solicitações - neste caso, passageiros - do que é capaz de suportar.




Quando um computador/site sofre ataque DoS, ele não é invadido, mas sim **sobrecarregado**.

Conforme NAKAMURA (2007) os ataques do tipo DoS mais comuns podem ser feitos devido às características do protocolo TCP/IP (Transmission Control Protocol / Internet Protocol), possível de ocorrer em qualquer computador que o utilize.

05

Ainda conforme o autor, o ataque mais conhecido e ocorre da seguinte forma:

**1) *SYN Flooding***

Quando um computador tenta estabelecer uma conexão com um servidor através de um sinal do TCP conhecido por SYN (Synchronize). Se o servidor atender ao pedido de conexão, enviará ao computador solicitante um sinal chamado ACK (Acknowledgement). Em ataques desse tipo, o servidor não consegue responder a todas as solicitações e então passa a recusar novos pedidos.

**2) *UPD Packet Storm***

Quando um computador faz solicitações constantes para que uma máquina remota envie pacotes de respostas ao solicitante. A máquina fica tão sobrecarregada que não consegue executar suas funções.

Ainda conforme NAKAMURA (2007) os ataques **DDoS** (Distributed DoS), são ataques DoS de grandes dimensões. Utilizam-se milhares de computadores para atacar uma determinada máquina. Esse é um dos tipos mais eficazes de ataques e já prejudicou sites bastante conhecidos.

Historicamente, servidores da CNN, Amazon, Yahoo, Microsoft e eBay já foram vítimas.


Para que os ataques do tipo **DDoS** sejam bem-sucedidos, é necessário que se tenha um número grande de computadores para que estes façam parte do ataque. Uma das melhores formas encontradas para se ter tantas máquinas foi a de inserir programas de ataque **DDoS** em vírus ou em *softwares* maliciosos.

Inicialmente, as pessoas que organizavam ataques DDoS tentavam "escravizar" computadores que agiam como servidores na internet. Com o aumento na velocidade de acesso por causa das conexões banda larga, o interesse voltou-se aos usuários domésticos, já que estes representam um número extremamente grande de máquinas na internet e podem ser "escravizados" mais facilmente.

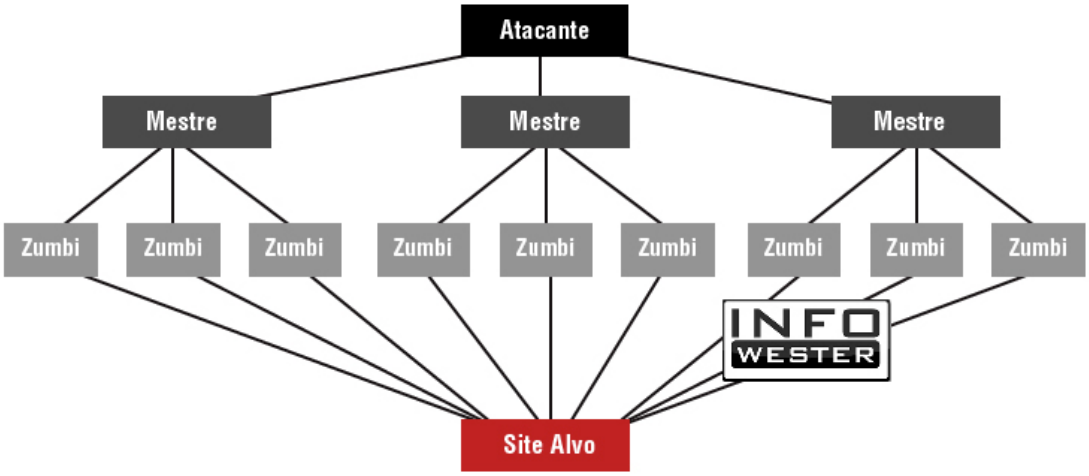
06

Para atingir a enorme quantidade de computadores conectados à internet, *malwares* (ou seja, vírus, cavalos-de-troia etc.) foram e são criados com a intenção de disseminar pequenos programas para ataques DoS. Quando um vírus contamina um computador, este fica disponível para fazer parte de um ataque DoS, sendo que o usuário dificilmente fica sabendo que sua máquina está sendo utilizada para tais fins.

Como a quantidade de computadores que participam do ataque é grande, é praticamente impossível saber exatamente qual é a máquina principal do ataque.

Quando o computador de um usuário doméstico é infectado por um *malware* com funções para ataques DoS, esta máquina passa a ser chamada de "zumbi". Após a contaminação, os zumbis entram em contato com máquinas chamadas de "mestres", que por sua vez recebem orientações (quando, em qual site/computador, tipo de ataque, entre outros) de um computador "atacante" ou "líder". Após receberem as ordens, os computadores mestres as repassam às máquinas zumbis, que efetivamente executam o ataque.

A imagem a seguir ilustra a hierarquia de computadores usadas em ataques **DDoS**.




**Hierarquia de computadores no ataque DDoS**
**Fonte: Internet-InfoWester, 2015**

Um computador mestre pode ter sob sua responsabilidade até milhares de computadores. Repare que, nestes casos, as tarefas de ataque **DoS** são distribuídas a um "exército" de máquinas escravizadas. Daí é que surgiu o nome **Distributed Denial of Service**.

07

Ainda conforme NAKAMURA (2007), apesar de não existir meio que consiga impedir totalmente uma ação DoS, é possível detectar a existência de ataques ou de computadores (zumbis) de uma rede que estão participando de atividades DDoS. Um dos meios, para isso, consiste em **observar se está havendo mais tráfego do que o normal** (principalmente em casos de sites, seja ele um menos conhecido, como o InfoWester, seja ele um muito utilizado, como o Google), se há pacotes TCP e UDP que não fazem parte da rede ou se há pacotes com tamanho acima do normal, por exemplo.

Outra dica importante é a utilização de *softwares* de IDS (**I**ntrusion **D**etection **S**ystem - Sistema de Identificação de Intrusos).


Para prevenção, uma das melhores armas **é verificar as atualizações de segurança** dos sistemas operacionais e softwares utilizados pelos computadores. Muitos malwares aproveitam as vulnerabilidades encontradas para efetuar contaminações sem que o usuário ou o administrador do sistema perceba.

Também é importante **filtrar** certos tipos de pacotes na rede, criar regras consistentes de *firewall* e desativar serviços que não são utilizados.

08

## 3 - Práticas Gerais para Mitigação de Riscos

A melhor solução para evitar problemas que mencionamos anteriormente, é a adoção de uma política efetiva de segurança em toda a rede. Há, também, algumas ferramentas disponíveis, que apresentaremos a seguir.

**a) ASA – Adaptative Security Appliance**

Conforme vimos anteriormente, ASA é um firewall da Cisco. O firewall filtra pacotes que entram e que saem da rede de modo a evitar que pacotes contendo conteúdo nocivo atinjam a rede e causem prejuízos.

**b) NAT - Network Address Translation**

Em termos gerais, NAT é um protocolo que faz a tradução dos endereços Ip e portas TCP da rede local para a Internet. Este item será estudado mais adiante em nossa disciplina.

**c) Anti-X**

Política de segurança com medidas preventivas a diferentes tipos de ataque e problemas. A Cisco utiliza o termo anti-X para se referir a toda uma classe de ferramentas de segurança para prevenção de problemas (instalação de um bom antivírus; um anti-spyware, um anti-spam, um anti-phishing, filtros de URL e filtros de e-mail).

**d) SSH - Secure Shell**

De forma simplista, podemos dizer que é um Telnet criptografado. Ative sempre o SSH em um dispositivo Cisco. Veja mais detalhes ao final deste módulo.

09

**e) VPN (Virtual Private Network)**

Com a crescente oferta de banda e melhora no desempenho dos links da internet, muitas empresas viram assim um modo mais econômico para interconectar dois pontos remotos. Porém, vale destacar que a internet é um meio público, que além de não pertencer a sua empresa, é compartilhado por milhões de pessoas, não oferecendo qualquer garantia de segurança. Assim, usa-se a VPN ou rede Virtual Privada, que possibilita a utilização de links internets na interconexão de localidades corporativas.

A VPN resolve dois problemas:

1) de segurança, pois os pacotes via VPN são criptografados e
2) resolve o problema de endereçamento e roteamento IP.

Quando um "túnel" VPN é fechado entre dois pontos, o que se tem é uma conexão ponto a ponto podendo-se configurar rotas ou rodar protocolos de roteamento que bem entendermos, como em uma rede privada.

Em uma VPN os elementos participantes (endpoints) necessitam autenticar-se antes que o túnel VPN seja criado.

10

## 4- Papel da Política de Segurança

A política de segurança atribui os direitos e responsabilidades às pessoas (usuários, administradores de redes e sistemas, funcionários, gerentes e demais usuários) que lidam com essa informação. A política define as expectativas que podem ter e quais são as suas atribuições em relação à segurança dos recursos computacionais com os quais trabalham.

Além disso, a política de segurança também estipula as penalidades às quais estão sujeitos aqueles que a descumprem.

Antes que a política de segurança seja escrita, é **necessário definir a informação a ser protegida**. Usualmente, isso é feito através de uma **análise de riscos**, que identifica:

1) recursos protegidos pela política;
2) ameaças às quais estes recursos estão sujeitos;
3) vulnerabilidades que podem viabilizar a concretização destas ameaças, analisando-as individualmente.

**11**

Uma política de segurança deve cobrir os seguintes aspectos:

a) abrangência e escopo de atuação da política;
b) definições fundamentais;
c) normas e regulamentos aos quais a política está subordinada;
d) quem tem autoridade para sancionar, implementar e fiscalizar o cumprimento da política;
e) meios de distribuição da política;
f) como e com que frequência a política é revisada.

Com respeito à **política de senhas** deve-se verificar:

a) requisitos para formação de senhas;
b) período de validade das senhas;
c) normas para proteção de senhas;
d) reuso de senhas e
e) senhas *default*.

**12**

**4.1– Direitos e Responsabilidade dos usuários na Política de Segurança**

Com relação aos **direitos e responsabilidades** dos usuários deve-se verificar:

a) utilização de contas de acesso;

b) utilização de *softwares* e informações, incluindo questões de instalação, licenciamento e copyright;

c) proteção e uso de informações como senhas, dados de configuração de sistemas e dados confidenciais da organização;

d) uso aceitável de recursos como email, news e páginas Web;

e) direito à privacidade;

f) condições nas quais esse direito pode ser violado pelo provedor dos recursos.


Uma condição obrigatória é o **uso de antivírus** em todos os dispositivos terminais de dados do sistema.

Os provedores de recursos devem exercer os direitos e prover responsabilidades nos itens relacionados:

a) *backups*;

b) diretrizes para configuração e instalação de sistemas e equipamentos de rede;

c) autoridade para conceder e revogar autorizações de acesso, conectar e desconectar sistemas e equipamentos de rede, alocar e registrar endereços e nomes de sistemas e equipamentos;

d) monitoramento de sistemas e equipamentos de rede e

e) normas de segurança física.

13

**4.2– Sanções impostas**

A política de segurança deve adotar **ações**, em caso de violação da política, relativas a:

a) diretrizes para tratamento e resposta de incidentes de segurança e

b) penalidades cabíveis.

Se cada organização possui um ambiente distinto e os seus próprios requisitos de segurança, então que desenvolva uma política de segurança que se molde às especificidades próprias.

14

**4.3 – Implantação da Política de Segurança**

Para que a política de segurança possa ser **implantada com sucesso** é necessário que:

a) tenha apoio por parte da administração superior;

b) seja ampla, cobrindo todos os aspectos que envolvem a segurança dos recursos computacionais e da informação sob responsabilidade da organização;

c) seja periodicamente atualizada de forma a refletir as mudanças na organização;

d) tenha uma pessoa ou grupo responsável por verificar se a política está sendo respeitada;

e) todos os usuários da organização tomem conhecimento da política e manifeste a sua concordância em submeter-se a ela antes de obter acesso aos recursos computacionais;

f) esteja disponível em um local de fácil acesso aos usuários, tal como a intranet da organização.

Dentre os itens acima, o apoio por parte da administração superior é essencial. Se a política de segurança não for encampada pela administração, ela rapidamente será deixada de lado pelos demais setores da organização. Além disso, é importante que os seus membros deem o exemplo no que diz respeito à observância da política de segurança.

Por outro lado, existem alguns **fatores que influem negativamente** na aceitação de uma política de segurança e podem levá-la ao fracasso, tais como:

a) ser demasiadamente detalhada ou restritiva;

b) excessivamente detalhada causando confusão ou dificuldades na sua implementação;

c) abertura de exceções para indivíduos ou grupos e

d) estar atrelada a *software*s e/ou hardwares específicos.

15

## 5- Instalação e Configuração Segura de Sistemas

Após estabelecer as políticas de segurança apropriadas para a rede de computadores deve-se partir para a configuração segura dos sistemas que habitam a rede.


Caso não exista uma documentação atualizada que detalhe a configuração de alguns ou todos os sistemas em uso na sua rede, é aconselhável que estes sistemas sejam reinstalados observando-se as recomendações de boas práticas, ou, pelo menos, que a sua configuração seja revisada e a documentação correspondente atualizada.

Alguns cuidados antes de conectar o sistema à internet devem ser tomados. A pressa em disponibilizar um sistema na internet pode levar ao seu comprometimento. Veja abaixo quatro desses cuidados.

16

**5.1- Preparação da Instalação**

A instalação de um sistema deve ser feita com ele isolado do mundo externo.

Os princípios a seguir são:

a) planeje a instalação, definindo o propósito do sistema a ser instalado; os serviços que este sistema disponibilizará; a configuração de hardware da máquina; como o disco será particionado dentre outros que julgar necessário;

b) providencie de antemão todos os manuais e mídias de instalação que serão utilizados;

c) instale o sistema a partir de dispositivos de armazenamento locais (CD, fita ou disco), desconectado da rede;

d) caso você precise ligar o sistema em rede (para fazer download de atualizações, por exemplo), coloque-o em uma rede isolada, acessível apenas pela sua rede interna;

e) evite concentrar todos os serviços de rede em uma única máquina, dividindo-os entre vários sistemas. Essa ação aumenta a disponibilidade dos serviços na sua rede e reduz a extensão de um eventual comprometimento a partir de um deles.

17

**5.2 - Estratégias de Particionamento**

Siga o princípio básico de **dividir o disco em várias partições** em vez de usar uma única partição ocupando o disco inteiro, pelas **razões** a seguir:

a) um usuário ou um programa mal-comportado pode lotar uma partição na qual tenha permissão de escrita. Se os programas do sistema estiverem em outra partição eles provavelmente não serão afetados, evitando que o sistema trave;

b) caso uma partição seja corrompida por alguma razão, as outras partições provavelmente não serão afetadas.

O uso de várias partições geralmente facilita o procedimento de *backup* do sistema, pois simplifica **funções**.

Recomenda-se avaliar a conveniência ou não da criação de partições separadas para as áreas onde são armazenados **itens** como:

a) programas do sistema operacional;

b) dados dos usuários;

c) logs;

d) arquivos temporários;

e) filas de envio e recepção de emails (servidores SMTP);

f) filas de impressão (servidores de impressão);

g) repositórios de arquivos (servidores FTP) e

h) páginas Web (servidores HTTP).


Podem existir outras áreas do sistema que mereçam uma partição separada. Consulte a documentação do seu sistema operacional para ver se ela contém recomendações a respeito do particionamento adequado dos discos.

Funções

Algumas funções que podem ser simplificadas são:

a) copiar partições inteiras de uma só vez;

b) excluir partições individuais do procedimento;

c) fazer *backups* em intervalos diferentes para cada partição.

18

**5.3- Documentação da Instalação e Configuração**

Faça um *logbook* (ou "diário de bordo"), que detalhe os componentes instalados no sistema e todas as modificações na sua configuração global. Esse logbook pode ser particularmente útil para determinar qual versão de determinado pacote está instalada no sistema ou para reconstituir uma dada instalação.

Muitas vezes um administrador precisa consultar diversas fontes e realizar várias tentativas antes de instalar e/ou configurar corretamente um determinado pacote de *software*. A existência de um documento que relate quais os passos exatos que tiveram que ser seguidos para que a instalação/configuração fosse bem sucedida permite que esse mesmo pacote possa ser instalado com correção e rapidez em outro sistema ou ocasião.

As **informações do logbook** devem ser, no mínimo, as seguintes:

a) data da modificação;

b) responsável pela modificação;

c) justificativa para a modificação;

d) descrição da modificação e

e) reconstituição da situação antes da mudança na configuração a partir de uma entrada.

19

**5.4- Senhas de Administrador**

Durante a instalação de um sistema, em determinado momento será solicitado que você informe uma senha de administrador (root ou Administrator). Procure estabelecer esta senha tão cedo quanto possível durante a instalação do sistema. De preferência, tenha uma senha já em mente quando começar a instalação.

Uma senha adequada é aquela fácil de ser lembrada e difícil de ser adivinhada. Ela deve respeitar, no mínimo, os seguintes **critérios**:

a) ter um comprimento mínimo de 8 caracteres;

b) ser formada por letras, números e caracteres especiais;

c) não ser derivada de seus dados pessoais, tais como nomes de membros da família, números de telefone, placas de carros, números de documentos e datas;

d) não deve ser adivinhada por quem conheça suas preferências pessoais (time para o qual torce, escritor, ator ou cantor favorito, nomes de livros, filmes ou músicas);

e) não estar presente em dicionários (de português ou de outros idiomas).


Uma sugestão para formar senhas:

1- olhai os lírios do campo,

2- eles não fiam e nem tecem,

3- porém nem Salomão conseguiu se vestir como um deles".

20

**5.5– Registros de Logs**

Log é o termo técnico para o registro de atividades diversas.

Algumas dessas atividades podem ser:

a) conexão (informações sobre a conexão de um computador à Internet);

b) acesso a aplicações (informações de acesso de um computador a uma aplicação de Internet).

**5.6 – Uso de Ferramentas anti*malware***

Ferramentas anti*malware* são aquelas que detectam, anulam ou removem os códigos maliciosos de um computador.

Antivírus, antispyware, antirootkit e antitrojan são exemplos de ferramentas deste tipo.

Entre as diferentes ferramentas existentes, a que engloba a maior quantidade de funcionalidades é o **antivírus**. Apesar de inicialmente eles terem sido criados para atuar especificamente sobre vírus, com o passar do tempo, passaram também a englobar as funcionalidades dos demais programas, fazendo com que alguns deles caíssem em desuso.

21

## 6 - Outros mecanismos

**6.1 – Filtros**

- **Filtro antiphishing**

Já vem integrado à maioria dos navegadores Web e serve para alertar os usuários quando uma página suspeita de ser falsa é acessada.

- **Filtro de janelas de pop-up**

Já vem integrado à maioria dos navegadores Web e permite o controle da exibição de janelas de pop-up.

- **Filtro de códigos móveis**

Filtros, como o NoScript, permitem o controle da execução de códigos Java e JavaScript.

- **Filtro de bloqueio de propagandas**

Filtros como o Adblock permitem o bloqueio de sites conhecidos por apresentarem propagandas - http://adblockplus.org/

22

**6.2 - Testes**

- **Teste de reputação de site**

Complementos, como o WOT (Web of Trust), permitem determinar a reputação dos sites acessados.

- **Anonymizer**

Sites para navegação anônima, conhecidos como *anonymizers*, intermediam o envio e recebimento de informações entre o seu navegador Web e o site a ser visitado.

23

## 7 – Configurações de dispositivos

Atualmente é comum administrar um roteador, servidor, switch acessando remotamente o console fornecido pelo dispositivo. Nem sempre os protocolos utilizados são os mais seguros.

**Switches** e **Roteadores Cisco** até hoje utilizam, por padrão, acesso remoto através de Telnet, que envia todas as informações (incluindo as de login) pela rede em texto puro. Esse fato constitui-se de uma

grande falha na segurança da rede, pois qualquer um que consiga “sniffar” o tráfego será capaz de “logar” no roteador.

Atualmente os equipamentos Cisco fornecem suporte à utilização de **SSH2**. Esta é uma grande adição à segurança destes equipamentos, já que todos os dados trocados entre a estação cliente e o roteador serão criptografados.

24

**7.1 – Configuração do SSH**

**Requisitos iniciais**: um nome de host e um nome de domínio devem estar configurados no equipamento (isso pode ser feito no modo de configuração global utilizando os comandos “hostname” e “ip domain-name”, respectivamente).

**Passo 1**

Acesse o roteador (por Telnet ou diretamente pelo Console) e entre no modo de configuração global:

```
roteador>enable
roteador#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
roteador(config)#
```

**Passo 2**

Gere as chaves que serão utilizadas na autenticação do SSH. O IOS suporta gerar certificados com criptografia de no mínimo 360 bits e no máximo 2048 bits. Considera-se 360 bits muito pouco, utilize como padrão o 2048 bits.

```
roteador(config)#crypto key generate rsa
How many bits in the modulus [512]:2048
% Generating 2048 bit RSA keys, keys will be non-exportable…[OK]
```

Informe o número de bits para o módulo do certificado. O padrão é 512, recomenda-se 2048 bits. Uma mensagem de alerta indicará sucesso ou falha na geração do certificado. Utilizando SSH2 com criptografia de 2048 bits torna muito difícil um atacante “sniffar - escutar” o tráfego na sua rede e descriptografar os pacotes conseguindo recuperar senhas, usuários e outros dados. Mas isso ainda é insuficiente. É necessário que se utilize senhas fortes e ACL‘s para controlar quem poderá tentar se conectar ao SSH2 do seu equipamento Cisco, mas sem dúvida dificulta o “crakeamento”.

25

**Passo 3**

Configure os parâmetros do serviço SSH como timeout, versão e outros.

```
roteador(config)#ip ssh version 2
```

Este comando especificará qual versão do protocolo SSH a utilizar. Para verificar quais versões estão disponíveis, execute o comando “show ip ssh” no modo “enable”. Se estiver indicando versão 2.0, você pode utilizar tanto a versão 1 quanto a versão 2. Se estiver indicando 1.X, você pode utilizar apenas a versão 1 do protocolo.

**Passo 4**

Configure o timeout:

```
roteador(config)#ip ssh time-out 50
```

Escolha qualquer valor no intervalo de 1 a 120 segundos. Sessão de cliente parada por mais tempo que o especificado desconecta automaticamente o mesmo.

**Passo 5**

Para dificultar os ataques, configure o valor de tentativas de login.

```
roteador(config)#ip ssh authentication-retries 2
```

Serão permitidas apenas 2 tentativas erradas. Pode especificar um valor entre 0 e 5 nesta opção.



**Passo 6**

Crie alguns usuários locais (válidos apenas no roteador) e defina o nível de acesso para cada um deles. Para criar um usuário chamado “administrador”, com permissão de fazer tudo no roteador, execute o comando:

```
roteador(config)#username administrador priv 15 secret senha-do-usuário
```

Você tem um usuário chamado “administrador” com permissão para realizar qualquer tipo de configuração no roteador onde ele foi criado. O que define se é um administrador ou não é a opção “**priv 15**”. O valor 15 indica que ele tem acesso total, pois o valor da função varia de 0 a 15: quanto menor o valor, menor o privilégio do usuário no sistema.

Por exemplo:

Modo EXEC de usuário: nível de privilégio 1

Modo EXEC de superusuário: nível de privilégio 15

**Passo 7**

Impeça que as linhas de Telnet aceite conexões Telnet e passem a aceitar apenas conexões SSH:

```
roteador(config)#line vty 0 4

roteador(config-line)#login local

roteador(config-line)#transport input ssh
```

SSH2 foi configurado para Telnet, teste a conexão para confirmação.

27

**Passo 8**

Teste a conexão ao roteador. Utilize qualquer cliente SSH para se conectar ao mesmo. Um deles pode ser o PuTTY, que funciona em Windows e possui uma boa quantidade de características que ajudam no dia a dia. Pode utilizar o cliente disponível em roteadores Cisco. Este funciona apenas em linha de comando e não possui a metade das opções oferecidas pelo PuTTY. Para usá-lo, faça o seguinte:

```
roteador>ssh -l administrador -v 2 192.168.1.1
```

Não é necessário estar em modo privilegiado para utilizá-lo. A opção "-l" (letra "L" minúscula) indica qual o nome de usuário será utilizado; a opção "-v" indica qual a versão do protocolo o cliente deverá utilizar (o valor pode ser 1 ou 2, como já foi dito anteriormente) e, finalmente, o IP do roteador ao qual você irá se conectar.

28

**7.2– Configuração nas Máquinas Locais**

Para a proteção adicional do PC, entre nos serviços do SO (Windows): Menu Iniciar -> Painel de Controle -> Ferramentas administrativas -> Serviços e **Desative os seguintes serviços**:

1 - Área de Armazenamento (desative só essa área de armazenamento, pois há também o armazenamento protegido que você deve deixar ativado);

2 - Auxiliar NetBIOS TCP/IP;

3 - Compartilhamento remoto da área de trabalho do NetMeeting;

4 - Gerenciador de conexão de acesso remoto automático;

5 - Gerenciador de sessão de ajuda de área de trabalho remota;

6 - Roteamento e acesso remoto;

7 - Registro remoto;

Para a desativação do protocolo ”Telnet” da máquina, clique com o botão direito do mouse sobre o serviço e escolha a opção: Propriedades -> em Tipo de inicialização selecione a opção: Desativado. -> Clique no botão: Aplicar e no botão: Ok.

Se aguma impressora não é compartilhada com outros computadores, desative-a: Menu -> Iniciar –> Painel de Controle –> Conexões de rede –> Clique com o botão direito do mouse sobre o ícone de alguma conexão que estiver ativa em seu computador e escolha a opção: Propriedades –> Clique na aba Rede (ou na aba Geral. Isso depende de qual conexão você está acessando) e selecione o serviço: “Compartilhamento de arquivos e impressoras para redes Microsoft” e clique no botão Desinstalar. Siga os passos que o programa de desinstalação ofertar.

Menu -> Iniciar –> Painel de Controle –> Sistema –> Remoto –> desmarque a opção: Permitir o envio de convites de assistência remota deste computador. (se esta opção já estiver desmarcada, então deixe-a como está) –> Clique no botão: Aplicar e no botão: Ok.

Os mecanismos de controle e defesa resumidos no texto acima é, por enquanto, o necessário e suficiente para desenvolvermos nossa unidade. A partir deste momento podemos começar a verificar os conceitos de Firewall baseados em NAT, PAT e ACL que serão mais adiante nesta disciplina.

29

## Resumo

As boas práticas são decorrentes de uma política de segurança, um instrumento para proteger uma instituição contra ameaças à segurança da informação que a ela pertence ou que está sob responsabilidade dela. A segurança não é assegurada exclusivamente por um firewall.

Como propriedades de uma comunicação segura, temos: Confidencialidade, Integridade e Autenticidade, cujos conceitos devem ser muito bem entendidos. Essas propriedades são implementadas com recursos de técnicas de criptografia, chaves simétricas e de chaves públicas, utilizadas em diversos protocolos.

Conforme SANTOS (2011) um Firewall filtra pacotes que entram e que saem da rede de modo a evitar que pacotes contendo conteúdo nocivo atinjam a rede e causem prejuízos.

Sobre a identificação de Ameaças, o DoS (Denial of Service) tem o propósito de parar determinados serviços ou elementos da rede; o Reconnaissance Attacks (Ataques de reconhecimento) têm por objetivo obter informações importantes que possam ser utilizadas em um ataque de acesso e os Access Atacks são ataques que objetivam roubar dados, buscando-se vantagem financeira.

Como práticas gerais para mitigação de riscos, foram citadas a ASA – Adaptative Security Appliance, o NAT, o Anti-X, SSH - Secure Shell e o VPN (Virtual Private Network).

Uma política de segurança deve cobrir os seguintes aspectos: abrangência e escopo de atuação da política; definições fundamentais; normas e regulamentos aos quais a política está subordinada; quem tem autoridade para sancionar, implementar e fiscalizar o cumprimento da política; meios de distribuição da política; como e com que frequência a política é revisada.

30

Com respeito à política de senhas deve-se verificar: a) requisitos para formação de senhas; b) período de validade das senhas; c) normas para proteção de senhas; d) reuso de senhas e e) senhas default.

São direitos e responsabilidades dos usuários: a) utilização de contas de acesso; b) utilização de *software*s e informações, incluindo questões de instalação, licenciamento e copyright; c) proteção e uso de informações como senhas, dados de configuração de sistemas e dados confidenciais da organização; d) direito à privacidade e e) condições nas quais esse direito pode ser violado pelo provedor dos recursos.

A política de segurança deve adotar ações, em caso de violação da política, relativas a: a) diretrizes para tratamento e resposta de incidentes de segurança e b) penalidades cabíveis.

Na implantação da política de segurança, é necessário que: tenha apoio por parte da administração superior; seja ampla, cobrindo todos os aspectos que envolvem a segurança dos recursos computacionais e da informação sob responsabilidade da organização; c) seja periodicamente atualizada de forma a refletir as mudanças na organização; tenha uma pessoa ou grupo responsável por verificar se a política está sendo respeitada; todos os usuários da organização tomem conhecimento da política e manifeste a sua concordância em submeter-se a ela antes de obter acesso aos recursos computacionais; esteja disponível em um local de fácil acesso aos usuários, tal como a intranet da organização.

Os testes são itens fundamentais, assim como a configuração dos dispositivos.

# UNIDADE 4 – CONCEITOS INTRODUTÓRIOS DE SEGURANÇA DE REDES: NAT, PAT, ACL E DMZ

## MÓDULO 2 – FIREWALL (NAT, PAT, ACL).

01

## 1 – NAT

O NAT (Network Address Translation) é um protocolo tradutor de endereços de camada-3 (rede) que visa:

1) minimizar os efeitos da escassez de endereços ipv4;

2) aumentar a segurança da rede interna das empresas.

3) conectar redes privadas à internet, pois traduzem IPs privados para ips públicos.

O NAT é um mecanismo para conectar redes privadas à Internet (rede externa, desconhecida e totalmente insegura), pois serve como ponto de tradução de IPs privados, não roteáveis na Internet, para IPs públicos, roteáveis na Internet.

Com a norma RFC-1918 foram criadas regras que permitem a utilização de endereços não roteáveis na internet (endereços privados: 10.0.0.0/8; 172.16.0.0/12 e 192.168.0.0./16) nas redes locais.

É possível que várias empresas utilizem as mesmas redes privadas nas redes internas delas, sem preocupação com o número de ips que suas redes demandam.

02

**1.1 – Tipos de NAT**

| NAT Estático | NAT Dinâmico |
|---|---|
| • É estabelecida uma relação entre endereços locais e endereços públicos (da Internet) de maneira fixa. Sempre um IP interno será traduzido para um mesmo IP externo. É recomendado para oferecer serviços na rede interna, por exemplo, quando um servidor está localizado na rede interna. Assim, quando houver um pedido de conexão ao roteador a um IP definido via NAT estático, o mesmo consulta a tabela de endereços e transcreve para o IP interno correspondente, permitindo qua seja possível fazer uma conexão no sentido da Internet para a rede interna. | • Ocorre um mapeamento de endereços locais e endereços da Internet de maneira fixa. E feito conforme a necessidade de uso. Há uma faixa de endereços que pode ser utilizada dinamicamente. Foi projetado para mapear um endereço IP privado para um endereço público. Não há uma relação fixa entre os IPs internos e públicos. Qualquer endereço IP de um pool de endereços IP públicos é atribuído a um host da rede. Não há possibilidade de abrir uma conexão a partir da Internet o que aumenta a segurança da rede interna. |

03

**1.2 – Termos técnicos**

No IOS da Cisco temos que saber alguns termos técnicos para melhor compreender a configuração do NAT.

a) **Endereço local interno** (*Inside local address*)

| |
|---|
| Endereço privado pertencente a rede interna. É o endereço a ser traduzido. |

b) **Endereço global interno** (*Inside global address*)

| |
|---|
| Endereço válido na Internet pertencente ao roteador que está com o NAT configurado. |

c) **Endereço local externo** (*Outside local address*)

| |
|---|
| Endereço do host remoto pertencente à Internet. |

d) **Endereço global externo** (*Outside global address*)

| |
|---|
| Endereço da rede remota. |

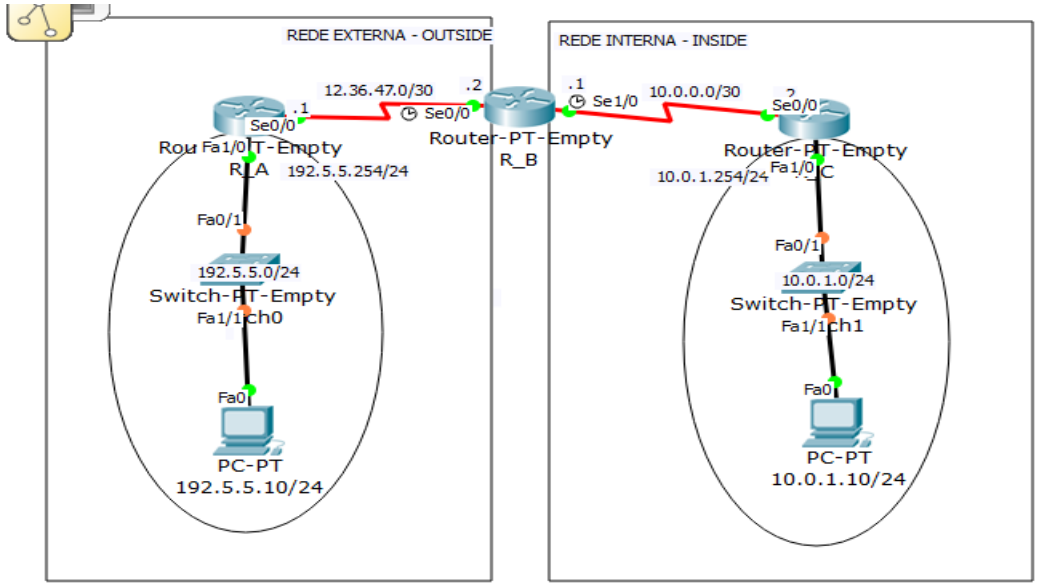



Figura 1 – Cenário NAT

Fonte: O autor, 2015.

Na figura acima o R_C faz parte da rede interna. Examine detalhadamente os IPs internos, os IPs externos, as redes que ligam R_A, R_B e R_C. Note que R_A e R_B estão interligados com uma rede /30, pois necessitamos somente de dois IPs para identificar cada uma das duas interfaces.

04

O host 10.0.1.10/24 tem um mapeamento estático em R_B com IP 12.36.47.2 pertencente à Internet. Ao acessar a Internet em busca do servidor WEB 192.5.5.10/24, o roteador R_B receberá o pacote pela interface Se1/0 e trocará o endereço de origem de 10.0.1.10 para 12.36.47.2 e enviará pela interface

Se0/0. O pacote chega ao R_A que a repassará ao servidor WEB. Este receberá a requisição, processará a mesma e passará as informações solicitadas para o IP 12.36.47.2. O R_B receberá esse pacote, verificará sua tabela de traduções do NAT e repassará as informações para o host 10.0.1.10.

Veja na tabela a seguir.

**Endereços IPs do cenário da Figura 1**

| **Address** | | | |
|---|---|---|---|
| **Inside global** | Inside local | Outside local | Outside global |
| **12.36.47.2** | 10.0.1.10 | 192.5.5.10 | 192.5.5.254 |

**Fonte: O autor, 2015.**

O R_B é um roteador de borda que faz a ponte entre a rede interna e a Internet. Este possui a interface Se1/0 que é a interna (inside) e a interface Se0/0 que é a externa (outside).

Se o roteador R_B fosse configurado com o NAT dinâmico, ao invés de termos um IP interno mapeado a um externo, teríamos uma faixa de IPs Internos mapeados a uma faixa fixa de IPs externos, possibilitando que mais de um host da rede interna acesse a Internet. O NAT dinâmico é mais dispendioso, pois necessita de vários IPs válidos para que o processo funcione de acordo com o esperado.

Veja a configuração feita no item a seguir.

05

**1.3 – Configuração do NAT estático**

Para a configuração do NAT estático basta definir o IP a ser traduzido e as interfaces *inside* e *outside* globais.

**1)** Defina uma tradução estática entre um inside local address e um inside global address:

```
Router(config)# ip nat inside source static <ip local> <ip global>,
```
onde:

Source static: definição da utilização do NAT estático;

<ip local>: IP privado interno a ser traduzido;

<ip global>: IP externo que servirá de interface com a Internet (que traduzirá o IP interno).

**2)** Defina a interface interna por onde i IP a ser traduzido acessa a rede externa (inside):

```
Router(config-if)# ip nat inside
```

**3)** Defina a interface que conecta a rede externa (outside):

```
Router(config-if)# ip nat outside
```

A aplicação a seguir mostra as duas implementações acima descritas (Estático e o Dinâmico).

Veja os exercícios a seguir.

**Clique aqui** para visualizar os exercícios. A aplicação mostra a implementação acima descrita (Estático).

Atenção: você deve ter instalado em sua máquina o **Packet Tracer**, disponível no ambiente do aluno.

06

**1.4 – Configuração do NAT dinâmico**

Para a configuração do NAT dinâmico há que se definir uma faixa de endereços externos (outside global) que será utilizada para tradução e também quais endereços internos (inside global) poderão ser traduzidos. Essa faixa de endereços externos recebe o nome de "**pool**" de endereços. A faixa de endereços internos é definida por meio de uma ACL.

Veja o exemplo a seguir.

Note que agora a rede não é mais /30 (somente dois IPs válidos para identificação de interfaces) e sim /28 (16 IPs, sendo 14 IPs válidos para identificação de conexões).

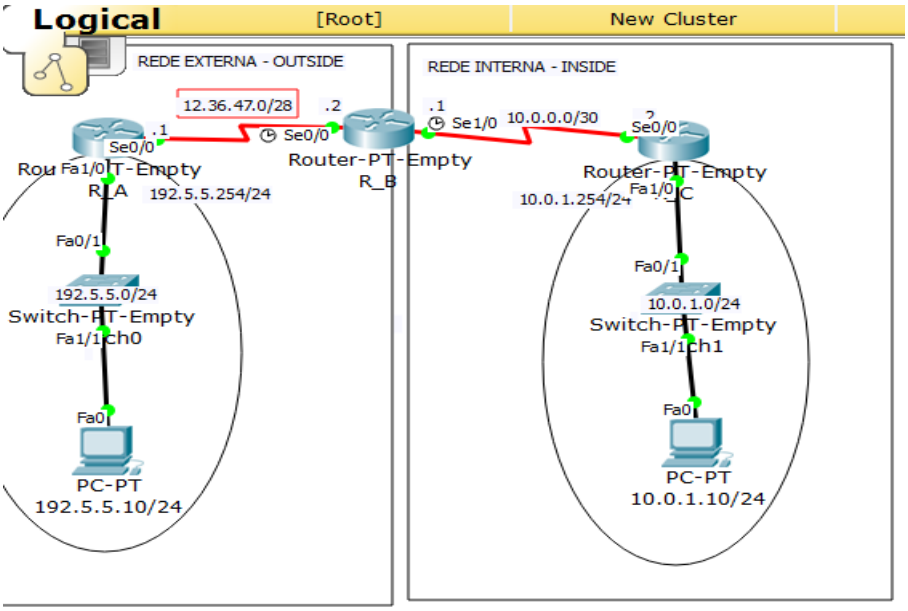



**Figura 2: Cenário do NAT dinâmico.**

**Fonte: O autor, 2015-06-26**

07

1) Crie um pool d endereços globais que serão alocados dinamicamente conforme a necessidade com o comando “ip nat pool”:

`Router(config)# ip nat pool <nome> <ip inicial> <ip final> netmask <máscara da rede>`, onde:

<nome>: nome do pool que será utilizado no comando “ip nat inside”;

<ip inicial>: IP do início da faixa da pool criada;

<ip final>: IP final da faixa da pool criada;

Netmask: palavra chave obrigatória a figurar depois do IP final da pool;

<máscara da rede>: máscara da rede (sub-rede) utilizada.

2) Configura uma ACL padrão permitindo os “inside local addresses” que poderão ser traduzidos:

`Router(config)# access-list <1 a 99> permit <IP da rede de origem> <máscara curinga da rede de origem>`

3) Estabeleça as traduções dinâmicas da origem, especificando a ACL definida no passo anterior para a seleção dos IPs que poderão ser traduzidos:

```
Router(config)# ip nat inside source list <nº da ACL criada> pool <nome da pool criada>
```

4) Defina a interface interna por onde o IP a ser traduzido acessa a rede externa (inside):

```
Router(config-if)# ip nat inside
```

5) Defina a interface que conecta a rede externa (outside):

```
Router(config-if)# ip nat outside
```

**Clique aqui** para visualizar os exercícios. A aplicação mostra a implementação acima descrita (Dinâmico).

Atenção: você deve ter instalado em sua máquina o **Packet Tracer**, disponível no ambiente do aluno.

08

**1.5 – Manutenção e Monitoramento do NAT**

Para a manutenção e monitoração do NAT utilize os comandos:

a) **show ip nat translations** – mostra as traduções feitas pelo NAT;

b) **show ip nat statistics** – mostras as estatísticas do NAT.

Abaixo, um exemplo do comando “show ip nat translations” e “show ip nat statistics” do cenário da figura 1:

R_B#show ip nat translations

Pro Inside global Inside local Outside local Outside global

icmp 12.36.47.3:10 10.0.1.10:10 192.5.5.10:10 192.5.5.10:10

icmp 12.36.47.3:11 10.0.1.10:11 192.5.5.10:11 192.5.5.10:11

icmp 12.36.47.3:12 10.0.1.10:12 192.5.5.10:12 192.5.5.10:12

icmp 12.36.47.3:13 10.0.1.10:13 192.5.5.10:13 192.5.5.10:13

icmp 12.36.47.3:14 10.0.1.10:14 192.5.5.10:14 192.5.5.10:14

icmp 12.36.47.3:15 10.0.1.10:15 192.5.5.10:15 192.5.5.10:15

icmp 12.36.47.3:16 10.0.1.10:16 192.5.5.10:16 192.5.5.10:16

icmp 12.36.47.3:17 10.0.1.10:17 192.5.5.10:17 192.5.5.10:17

icmp 12.36.47.3:18 10.0.1.10:18 192.5.5.10:18 192.5.5.10:18

icmp 12.36.47.3:19 10.0.1.10:19 192.5.5.10:19 192.5.5.10:19

icmp 12.36.47.3:20 10.0.1.10:20 192.5.5.10:20 192.5.5.10:20

icmp 12.36.47.3:21 10.0.1.10:21 192.5.5.10:21 192.5.5.10:21

icmp 12.36.47.3:5 10.0.1.10:5 192.5.5.10:5 192.5.5.10:5

icmp 12.36.47.3:6 10.0.1.10:6 192.5.5.10:6 192.5.5.10:6

icmp 12.36.47.3:7 10.0.1.10:7 192.5.5.10:7 192.5.5.10:7

icmp 12.36.47.3:8 10.0.1.10:8 192.5.5.10:8 192.5.5.10:8

icmp 12.36.47.3:9 10.0.1.10:9 192.5.5.10:9 192.5.5.10:9

R_B# show ip nat statistics

Total translations: 0 (0 static, 0 dynamic, 0 extended)

Outside Interfaces: Serial0/0

Inside Interfaces: Serial1/0

Hits: 21 Misses: 21

Expired translations: 21

Dynamic mappings:

-- Inside Source

access-list 1 pool TESTEDINAMICO refCount 0

pool TESTEDINAMICO: netmask 255.255.255.240

start 12.36.47.3 end 12.36.47.10

type generic, total addresses 8 , allocated 0 (0%), misses 0

09

## 2 – PAT – Port Address Translation

Assim como o NAT, o PAT é um tradutor de endereços de camada-3 (rede) que tem o mesmo objetivo que o NAT, ou seja, visa:

1) minimizar os efeitos da escassez de endereços ipv4;

2) aumentar a segurança da rede interna das empresas.

3) conectar redes privadas à internet, pois traduzem IPs privados para IPs públicos.

Assim como o NAT, o PAT é um mecanismo para conectar redes privadas à Internet (rede externa, desconhecida e totalmente insegura), pois serve como ponto de tradução de IPs privados, não roteáveis na Internet, para IPs públicos, roteáveis na Internet.

Com a norma RFC-1918 foram criadas regras que permitem a utilização de endereços não roteáveis na internet (endereços privados: 10.0.0.0/8; 172.16.0.0/12 e 192.168.0.0./16) nas redes locais. É possível que várias empresas utilizem as mesmas redes privadas nas redes internas delas, sem preocupação com o número de IPs que suas redes demandam.

10

### 2.1 – Funcionamento do PAT

O PAT (Port Address Translation) traduz o IP de origem e utiliza números de porta TCP e UDP de origem para distinguir cada uma das traduções que justifica o nome, ou seja, tradução de porta e endereço.

O número da porta TCP ou UDP é codificado com 16 bits, o que resulta em $2^{16}$ endereços internos que podem ser traduzidos para um único endereço externo, ou seja, há 65.536 possíveis traduções por indereço IP válido.

Na prática, aproximadamente 4.000 portas podem receber um único endereço IP.

O PAT preserva a porta TCP ou UDP de origem do segmento entrante. Se a porta de origem estiver em uso em outra tradução o PAT atribui o primeiro número de porta disponível para essa conexão. Quando não há mais portas disponíveis e há mais de um endereço IP externo configurado, o PAT passa para o próximo endereço IP, para tentar alocar novamente a porta de origem. Esse processo continua até que não haja mais portas disponíveis nem endereços IPs eternos.

Voltemos à configuração do nosso cenário da figura 1, discutida anteriormente.

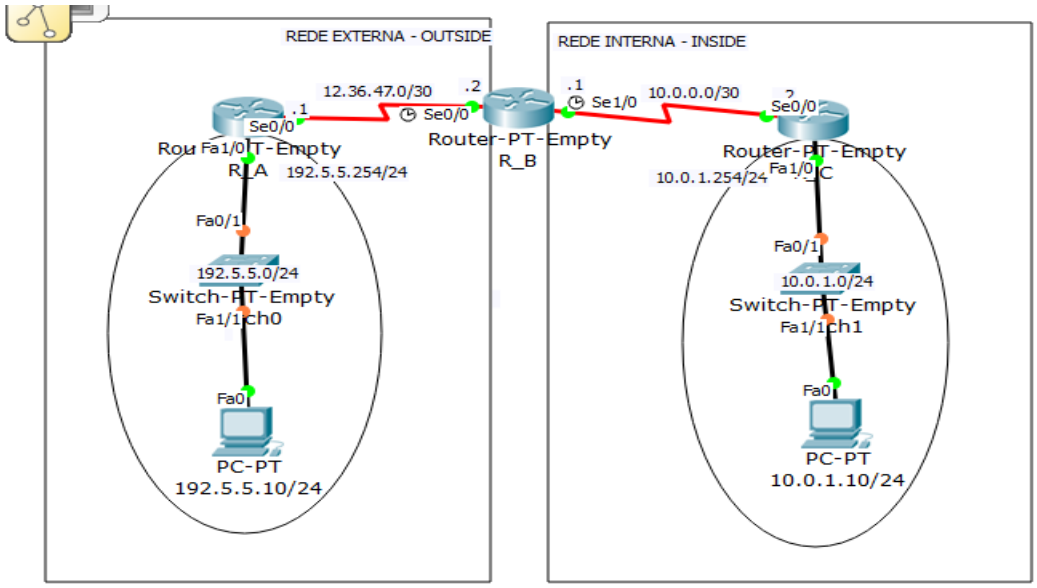



Figura 3: Cenário para o PAT.

Fonte: O autor, 2015.

Seja o roteador R_B configurado com PAT e apenas um IP válido na Internet foi disponibilizado para efetuar a tradução. Em determinado momento o host 10.0.1.10 e o host 10.0.1.20 (na figura ele não consta, mas vamos supor que ele se encontra na rede 10.0.1.0/24, a mesma do host 10.0.1.10) enviaram pacotes para conexão com o servidor WEB 192.5.5.10 simultaneamente.

11

Vejamos os pacotes que chegam à interface Se1/0 do R_B:

**Tabela 2: Endereçamento IPs do cenário para o PAT.**

| IP de origem | Porta de origem | IP de destino | Porta de destino |
|---|---|---|---|
| **10.0.1.10** | 1024 | 192.5.5.10 | 80 |
| **10.0.1.20** | 1025 | 192.5.5.10 | 80 |

**Fonte: O autor, 2015.**

O R_B receberá as solicitações e fará a tradução utilizando as portas TCP de origem preferencialmente iguais à dos pacotes originais, porém se as portas estiverem em uso ele utilizará outras.

Os pacotes são traduzidos e enviados à porta Se0/0 para o servidor 192.5.5.10.

**Tabela 3: Endereçamento IP do cenário para o PAT.**

| IP de origem | Porta de origem | IP de destino | Porta de destino |
|---|---|---|---|
| **12.36.47.2** | 1024 | 192.5.5.10 | 80 |
| **12.36.47.2** | 1025 | 192.5.5.10 | 80 |

**Fonte: O autor, 2015.**

O roteador montará uma tabela de relacionamento dos IPs e portas internas com os traduzidos, conforme tabela a seguir:

**Tabela 3: Endereçamento IP para o cenário PAT.**

| IPs da rede interna | | Tradução | |
|---|---|---|---|
| **IP de origem** | Porta de origem | IP de destino | Porta de destino |
| **10.0.1.10** | 1024 | 12.36.47.2 | 1024 |
| **10.0.1.20** | 1025 | 12.36.47.2 | 1025 |

**Fonte: O autor, 2015**

Quando o servidor responder a requisição para o IP 12.36.47.2, o roteador fará a separação para quem ele deve enviar o pacote após análise da tabela do PAT mostrada acima. Em consequência, quando o servidor responder para o 12.36.47.2 na porta 1024 ele passará para o host 10.0.1.10 e pela porta 1025 ele encaminhará para o host 10.0.1.20.

12

**2.2 – Configuração do PAT**

O PAT, além de traduzir o endereço IP, também utiliza os números de porta TP na tradução. Isso pode economizar números de IPs necessários, no lado externo, para a tradução, pois com apenas um IP externo pode-se executar até 65.535 traduções, aproximadamente, o número de portas TCP existentes.

1) Defina uma “access-list” padrão com os “inside local adresses” que serão traduzidos:

```
Router(config)# access-list <1 a 99> permit <rede de origem> <máscara curinga da rede de origem>
```

2) Estabeleça a tradução dinâmica dos endereços com o comando “ip nat inside” especificando os IPs internos que poderão acessar a rede externa via PAT com uso da ACL definida no passo anterior.

```
Router(config)# ip nat inside source list <número da ACL> interface <nome da interface> overload
```
, onde:

<número da ACL>: é o número da ACL criada no passo anterior, de 1 a 99;

<nome da interface>: coloque a interface de saída (outside global interface) que liga à rede externa;

Overload: parâmetro que ativa o PAT, ou seja, a tradução por IP e porta TCP ou UDP.

3) Defina a interface interna (inside) por onde o IP a ser traduzido acessa a rede externa.

```
Router(config)# ip nat inside
```

4) Defina a interface (outside) que se conecta com a rede externa.

```
Router(config)# ip nat outside
```

13

Veja a seguir a configuração no cenário:

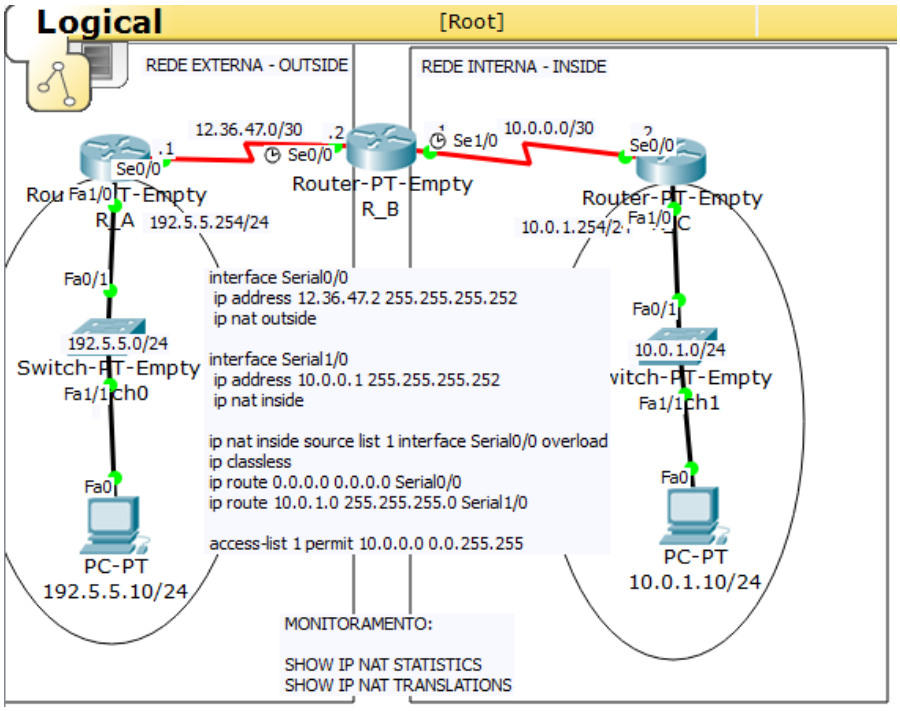



**Figura 4: Configuração do PAT.**

**Fonte: O autor, 2015.**

A configuração mostrada na figura acima é referente ao roteador R_B que faz as traduções PAT.

### 2.3 – Manutenção e Monitoramento do PAT

A manutenção e monitoração do PAT é semelhante ao do NAT. Para tal, utilize os comandos:

a) ***show ip nat translations*** – mostra as traduções feitas pelo NAT;

b) ***show ip nat statistics*** – mostras as estatísticas do NAT.

14

## 3 – ACL - Access Control Lists

As Access Control Lists ou Listas de Controle de Acesso de acesso de pacotes IP, também conhecidas como “access-lists” ou “ACLs”, são úteis para a manipulação do tráfego, podendo ser empregadas como métodos de packet filtering (ou filtro de pacotes), policy-based routing, route-maps, class-maps, NAT/PAT, entre outras aplicações.

A forma mais comum de utilização das ACLs é o **filtro de pacotes padrão**, o que seria um *firewall* básico filtrando pacotes utilizando-se do contexto de endereços de origem e destino, assim como portas de origem e destino. As access-lists podem ser configuradas para todos os protocolos roteáveis, como o TCP/IP, IPX, AppleTalk, e isto nos permite controlar o tráfego de entrada ou saída em um roteador Cisco.

Pacotes IP transportam qualquer tipo de informação em uma rede, as ACLs controlam o acesso de TUDO e de TODOS! É um conjunto de instruções que diz ao roteador para aceitar ou rejeitar determinados pacotes vindos de redes IP especificadas. Esse filtro atua até na camada “4”, onde é possível especificar portes TCP ou UDP que se deseja filtrar.

15

### 3.1 - Quais são os principais pacotes que podem ser filtrados pela ACL?

Os principais pacotes mais conhecidos estão listados na tabela a seguir.

**Tabela 4: Protocolos mais conhecidos.**

| Aplicação | Protocolo de Aplicação | Protocolo de Transporte |
|---|---|---|
| Correio eletrônico | SMTP | TCP |
| Login remoto | TELNET | TCP |
| WWW | HTTP | TCP |
| Transferência de arquivo | FTP | TPC |
| Servidor arquivo remoto | NFS | UDP |
| Gerenciamento de rede | SNMP | UDP |
| Protocolo de roteamento | RIP | UDP |
| Tradução de nomes | DNS | UDP |

| | | |
|---|---|---|
| Multimídia | proprietário | TCP ou UDP |
| Telefonia na Internet | proprietário | UDP |

**Fonte: Boavida & Bernardes, 2011.**

16

**3.2 – Como e por que utilizar a ACL?**

A ACL pode ser utilizada como um *firewall*, fornecendo recursos de filtragem básica, podendo ser aplicada como uma **barreira de proteção** com a finalidade de controlar o tráfego de dados entre sua rede interna e a Internet.

Além disso, as ACLs possuem múltiplas **aplicações**, e o emprego destas é certamente um dos recursos mais interessantes do Cisco IOS. Por exemplo, você pode:

- configurar ACLs para controlar o fluxo de tráfego por aplicação existente na sua rede;
- configurar uma Access Control List para impedir que *routing updates* (aqueles anúncios enviados pelos protocolos de roteamento) sejam propagados por uma determinada interface.
- usar a ACL nas situações em que você deseja eliminar certos protocolos do seu link de WAN.

Note que uma Access Control List nem sempre possui os recursos de um *firewall* inteligente (ex: *stateful inspection*), pois estes recursos estão presentes em versões específicas do Cisco IOS.

Caso o seu IOS não seja o "Cisco IOS Firewall", a implementação de access control lists não deverá ser feita com o propósito de proporcionar uma segurança elevada. De uma forma geral, as ACLs oferecidas pelas versões padrão do Cisco IOS (IP Plus, entre outras) são muito úteis para controlar o fluxo de tráfego ou para eliminar os protocolos desnecessários em certos segmentos de sua rede, mas não para prover uma segurança sólida.

Os cenários para a utilização de Access Control Lists são quase ilimitados. Você poderá permitir somente um host da sua rede a realizar certas tarefas ou transmitir certos protocolos, enquanto negando todo o resto. Configuração de políticas para roteamento, NAT, PAT, route-maps, entre muitos outros, são uma realidade com o esquema das Access Control Lists.

17

**3.3 - Quais são os parâmetros da ACL?**

São utilizados apenas dois parâmetros ao configurar uma ACL: **PERMIT** ou **DENY**.

Estes parâmetros são seguidos das definições DO QUE se deve **permitir** (PERMIT) ou **negar** (DENY).

As opções são:

1- ANY (tudo)

2- HOST [IP do host]

3- [sub-rede + wildcard]

4- [protocolo]

Ou seja, uma ACL sem nenhuma regra irá bloquear absolutamente todos os pacotes que são comparados com ela. Portanto, muito cuidado quando for aplicar uma ACL em uma interface.

18

**3.4 - Os tipos de ACLs mais comuns**

Estudaremos dois tipos de ACL mais comuns:

- **ACL Padrão (*standard*)** e
- **ACL estendida (*extended*).**

Existe também a variação, a **ACL nomeada (*named*)**, que ao invés de números, usa nomes para identificá-la.

É possível identificar as ACLs da seguinte forma:

ACLs **padrão** numeradas = de 1 a 99 e 1300-1999.

ACLs **estendidas** numeradas = 100 a 199 e 2000-2699.

A diferença básica entre os dois tipos de ACL é o **grau de inspeção do pacote IP**, antes de permitir ou negar seu acesso.


TODA ACL criada em um roteador Cisco termina com um DENY ANY implícito, negando TUDO a todos.

19

**3.5 - Como criar uma ACL?**

No IOS da Cisco pode-se criar a ACL no modo de configuração global e após aplicá-la em uma interface.

A sintaxe do comando para ACLs numeradas padrão é:

```
Router(config)# access-list [1-99] [permit/deny] [any/host {IP} (origem)]
[endereço IP / subrede]
```

Para ACLs estendidas numeradas é:

```
Router(config)# access-list [100-199] [permit/deny] [protocolo] [any/host
{IP} (origem)] [endereço IP / subrede] [any/host {IP} (destino)] [endereço
IP / subrede] [parâmetros adicionais]
```

Para ACLs nomeadas, o processo não muda, apenas eliminamos o número e substituímos pelo nome escolhido e tipo de ACL:

```
Router(config)# ip access-list standard [nome da ACL]

Router(config-std-nacl)# [permit/deny] [any/host {IP} (origem)] [endereço IP
/ subrede]

Router(config)# ip access-list extended [nome da ACL]

Router(config-ext-nacl)# [permit/deny] [protocolo] [any/host {IP} (origem)]
[endereço IP / subrede] [any/host {IP} (destino)] [endereço IP / subrede]
[parâmetros adicionais]
```

20

**3.6 - Quando devemos utilizar a ACL?**

Como já vimos, a ACL permite filtrar determinados pacotes, exatamente como um *firewall* faria, porém de uma maneira muito mais simplificada e com menos recursos. Utilizando ACLs no seu equipamento você pode, por exemplo:

- filtrar tentativas de conexões indo/vindo de/para hosts específicos;
- bloquear completamente um determinado protocolo antes de tal requisição entrar na sua rede (dependendo do posicionamento da ACL);
- controlar atualizações enviadas por protocolos de roteamento.

A ACL, portanto, tem uma grande importância e é essencial saber como trabalhar com elas. Vejamos alguns **casos em que devemos utilizar a ACL**:

1- Caso necessite bloquear um determinado host para o acesso a segmentos específicos da sua rede.

2- Caso possua um pool de endereços IP que precisam ser traduzidos aleatoriamente em um determinado perímetro de segurança, o posicionamento de uma Access List, em conjunto com os parâmetros do NAT, oferecerá uma solução completa.

3- Para compor o perímetro de segurança dentro da sua rede por meio dos roteadores. Por mais que você disponha de *firewalls* dedicados, a inserção de access control lists em um roteador Cisco oferecerá um nível de segurança adicional, garantindo ainda mais a integridade da sua rede.

4- Quando pretende manipular o tráfego utilizando recursos do Cisco IOS, conforme citamos anteriormente (route-maps, policy-map, class-map, NAT/PAT, etc.).

5- Quando quiser prover a segurança básica do seu roteador ou perímetro de segurança.

ACLs também podem ajudar a **miminizar alguns tipos de ataques** à rede, tais como:

- IP spoofing;
- DoS (Denial of Server) através de TCP SYN;
- Proteção contra ataques Smurf;

Além de atuar como um filtro de mensagens ICMP.

21

**3.7 - Quantas ACLs posso aplicar por interface?**

É possível aplicar somente uma ACL aplicada por Interface, por Protocolo e por Direção (conhecida, também, pela regra dos 3 “por”).

A **regra básica**: somente UMA ACL pode ser aplicada em uma mesma interface e direção, em um determinado router (ou switch). Em uma mesma interface você até pode ter mais de uma ACL, **desde que em sentidos opostos**.

Os sentidos possíveis são ilustrados no diagrama abaixo.

(IN) entrante —–> ROUTER ——> sainte (OUT)

Fique Atento!

O sentido em que uma ACL é aplicada determina qual o sentido do fluxo que deve ser examinado pelo router. Por este motivo, antes de aplicar uma ACL é necessário ter bem claro qual o efeito desejado.

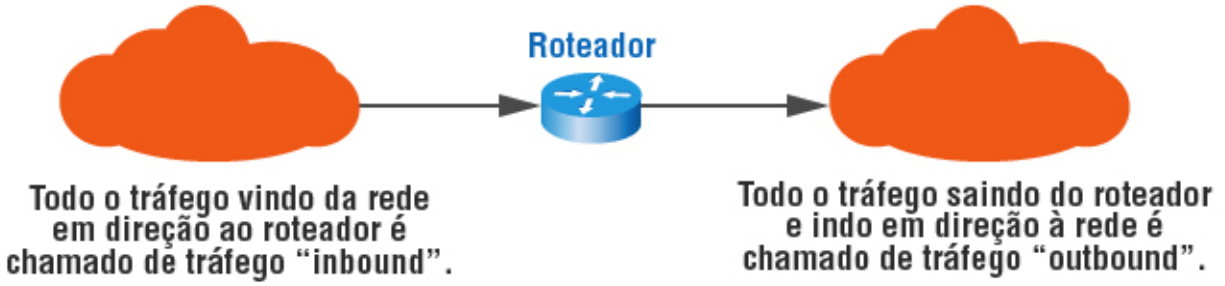



**Figura 5: Sentido de Tráfego de mensagens**

**Fonte: CCNA, 2015.**

**Veja aqui** o que você precisa saber **ANTES** de criar e aplicar ACLs.

Veja aqui

Pontos a saber **ANTES** de criar e aplicar ACLs:

1- A análise da ACL aplicada pelo roteador ocorre sempre de forma sequencial, de cima para baixo (top-down). Ou seja, as regras colocadas antes serão analisadas antes.

2- Uma vez que a regra testada resulte em positivo, nenhuma outra regra será analisada.

3- Lembre-se que, SEMPRE ao final de uma ACL existe uma regra DENY ANY escondida.

4- Atenção para o sentido de aplicação da ACL!

5- Faça sempre que possível um teste de mesa ANTES de aplicar uma ACL, para ter certeza que a mesma possui a lógica imaginada, e que irá funcionar de acordo.

Nunca remova uma ACL que se encontra aplicada a uma interface! Primeiro desaplique a ACL, DEPOIS remova.

22

### 3.8 - Quantas instruções podem ser definidas em uma ACL?

É possível ter **várias** instruções em uma ACL. Cada uma delas deve fazer referência ao mesmo nome ou número de identificação, para vincular as instruções à mesma ACL. O limite é o tamanho da memória disponível do roteador. Recomenda-se que divida as ACL por grupos de instruções afins e documente o

máximo possível.

A ACL atua por meio de instruções de permissões e de bloqueios, linha a linha, sendo que o último comando entrará no final da fila.


O IOS, por princípio, nega tudo. No final de toda ACL há um comando invisível “deny any” (nega qualquer tráfego), ou seja, rejeita todos os pacotes de quaisquer redes de protocolos. É necessário que toda ACL da Cisco contenha, pelo menos, um comando “permit” em quaisquer ACL.

**ACLs padrão** inspecionam apenas o endereço de origem no cabeçalho IP.

**ACLs estendidas** inspecionam o endereço IP de destino, o endereço IP de origem do pacote IP, além de inspecionar o cabeçalho de segmentos encapsulados no pacote IP.

### 3.9 - Como apagar uma ACL?

É necessário apagar toda a ACL negando a mesma (**no access-list <nº>**).

Não é possível apagar somente uma linha. Para corrigir uma linha, deve-se apagar toda a ACL e criar uma novamente com a linha correta.

23

### 3.10 - Prática

1) **ACL standard ou padrão**

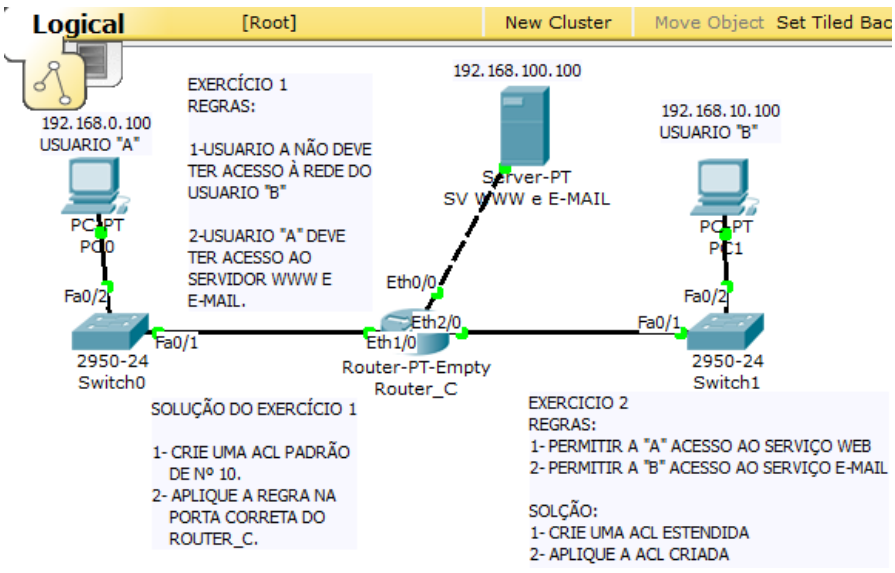



**Figura 6: Cenário para aplicação de ACL.**

**Fonte: O autor, 2015.**

Seja o diagrama da figura 6 dada acima.

Regras:

1- Usuário A não deve ter acesso à rede onde se encontra o computador do usuário B;

2- Usuário A deve ter acesso ao servidor de WEB e E-mail.

24

**Criação da ACL:**

```
Router(config)# access-list 10 deny host 192.168.0.100
```

!pacotes IP que tenham em seu cabeçalho o endereço de origem 192.168.0.100 serão imediatamente negados

```
Router(config)# access-list 10 permit any
```

! TODOS os outros serão permitidos

Não esqueça que tem um: Router(config)# access-list 10 deny any implícito, por isso a segunda linha da criação.

**Aplicação da ACL:**

```
Router(config)# int eth2/0
```

```
Router(config-if)# ip access-group 10 out
```

Opção da padrão nomeada:

**Criar a ACL:**

```
Router(config)# ip access-list standard NOMEDAACL
```

```
Router(config-std-nacl)# deny host 192.168.0.100
```

```
Router(config-std-nacl)# permit any
```

**Aplicar a ACL:**

```
Router(config)# int eth2/0
```

```
Router(config-if)# ip access-group NOMEDAACL out
```

25

### 2) ACL Extended

Seja o mesmo diagrama anterior.

Regras:

1-permitir ao usuário A somente o acesso ao serviço WEB no servidor;

2-permitir ao usuário B somente o acesso ao serviço de E-mail, no mesmo servidor.

**Criação da ACL:**

```
Router(config)# access-list 100 deny tcp host 192.168.0.100 host
192.168.100.100 eq 110
```

! nega o acesso do host A (192.168.0.100) ao servidor (191.168.100.100) somente ao serviço de E-mail (POP3 = porta TCP 110).

```
Router(config)# access-list 100 deny tcp host 192.168.10.100 host
192.168.100.100 eq 80
```

! nega o acesso do host A (192.168.10.100) para o host B (192.168.10.100) ao serviço WEB (HTTP = porta TCP 80).

```
Router(config)# access-list 100 permit ip any any
```

! permite o acesso de todo o resto, por todos.

**Aplicação da ACL:**

```
Router(config)# int eth0/0
```

```
Router(config-if)# ip access-group 100 out
```

Para uma ACL estendida:

**Criação da ACL:**

```
Router(config)# ip access-list extended NOMEDAACL
```

```
Router(config-ext-nacl)# deny tcp host 192.168.0.100 host 192.168.100.100 eq
110
```

```
Router(config-ext-nacl)# deny tcp host 192.168.10.100 host 192.168.100.100 eq
80
```

```
Router(config-ext-nacl)# permit ip any any
```

**Aplicação da ACL:**

```
Router(config)# int eth0/0
```

```
Router(config-if)# ip access-group NOMEDAACL out
```

Dicas:

1- ANY, quando se trata de ACLs, também pode ser escrito como 0.0.0.0 255.255.255.255

2- Quando for especificar uma rede, ao invés de um host, você precisa utilizar o wildcard, que seria uma espécie de máscara de rede invertida.

26

**3.11 - ACL pode fazer outra coisa que não filtrar o tráfego de rede?**

Sim. Elas podem ser utilizadas para definir tráfego que está sujeito ao Network Address Translation (NAT) e o tráfego que será criptografado em uma configuração de VPN, entre outras utilidades.

Nesse processo, o tráfego que entra no roteador é comparado com as entradas nas ACLs na ordem em que elas foram escritas.

**3.12 – Mais Exemplos de ACLs**

**Exemplo 1:** `access-list 101 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255`

**Exemplo 2:** `access-list 102 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255`

`access-list 102 deny ip any any`

Além de definir a origem e o destino do tráfego, como nos exemplos acima, pode-se definir portas de origem e destino, tipos de mensagens ICMP e outros parâmetros que restringem mais ainda as entradas das listas de acesso que serão aplicadas nas interfaces dos roteadores.

**Exemplo 3:**

```
access-list 102 permit icmp host 10.1.1.1 host 172.16.1.1 14
! permite todos os tipos de mensagens icmp
access-list 102 permit icmp host 10.1.1.1 host 172.16.1.1 eco-request
!  permite apenas um tipo de mensagem icmp
```

**Exemplo 4**

```
access-list 10 permit host 10.10.10.1

! apenas o host 10.10.10.1 será liberado

access-list 10 deny any

! todo o tráfego restante será negado.
```

**Exemplo 5**

```
Router(config)# access-list 101 deny icmp any 10.1.1.0 0.0.0.255 echo
```

```
! - nega o tráfego de ping

Router(config)# access-list 101 permit ip any 10.1.1.0 0.0.0.255

! - permite todo o tráfego ip

Router(config)# interface Ethernet0/1

Router(config-if)# ip address 172.16.1.2 255.255.255.0

Router(config-if)# ip access-group 101 in
```

Caso a palavra **in** ou **out** não for especificado, **out** fica **aplicado como padrão.**

**Exemplo 6**

```
Router(config)# ip access-list extended Saida

Router(config-ext-nacl)# permit tcp host 10.1.1.2 host 172.16.1.1 eq telnet

Router(config)# interface Ethernet0/0

Router(config-if)# ip address 10.1.1.1 255.255.255.0

Router(config-if)# ip access-group Saida in
```

27

**3.13- Comentários em listas de acesso**

Os comentários foram adicionados a partir do IOS 12.0.2.T para tornar mais fácil o entendimento da ACL. Pode ser utilizado em lista de acesso padrão e estendida.

```
Router(config)# access-list 101 remark permit_telnet

Router(config)# access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 eq
telnet
```

Ao editar uma ACL tenha sempre muita atenção. Se você pretende apagar uma linha de ACL numerada, como mostrado abaixo, a ACL inteira será apagada.

```
router#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

router(config)# access-list 101 deny icmp any any

router(config)# access-list 101 permit ip any any

router(config)# ^Z
```

```
router# show access-list
Extended IP access list 101
deny icmp any any
permit ip any any
router#
```

Os comandos abaixo apagam a ACL criada acima:

```
router# configure terminal
router(config)# no access-list 101 deny icmp any any
router(config)# ^Z
router# show access-list
router#
```


Sempre copie a ACL para um editor de texto, antes de fazer qualquer alteração e de preferência faça uma cópia de todas as configurações do equipamento que você está editando as regras, para que você tenha em mãos a última configuração válida, caso algum problema ocorra.

28

**3.14 - Wildcard masks nas ACLs**

As **wildcard masks** servem para definir quais sub-redes serão afetadas por uma determinada regra de ACL. Neste tipo de máscara 0 e 255 têm sentidos exatamente opostos à máscara de sub-rede que você já está acostumado.

Neste tipo de máscara, um bit 0 quer dizer que o octeto tem que “casar” exatamente, ou seja, será examinado e um bit 1 é ignorado (pode ser qualquer coisa). Exatamente o contrário do que se faz quando se usa uma máscara de sub-rede normal.

Exemplo:

Seja uma wildcard mask que reconheça todos os IPs da rede 192.168.0.0/24.

1- A máscara wildcard é 0.0.0.255. Os três primeiros 0s indicam que é obrigatório que 192.168.0 esteja presente no endereço IP do pacote sendo analisado. O bloco “255” indica que naquele octeto qualquer número é válido.

2- Para identificar todas as redes entre 192.168.16.0/24 a 192.168.31.0/24 afetadas por uma regra. A wildcard seria 192.168.31.0 – 192.168.16.0 = 0.0.15.255. Os dois primeiros 0s indicam que é obrigatório que o bloco "192.168" esteja presente, 15 é a soma dos bits para que as sub-redes desejadas casem com a regra (bits examinados pela regra). O 255 indica que o último octeto não importa, será associado a qualquer número.

3- Wildcard masks implica que tudo o que for "0" deverá ser processado (examinado ou considerado) pela ACL, enquanto os bits marcados como "1" deverão ser ignorados. É por este motivo que devemos inverter a máscara – no sentido dos bits – para podermos fazer o uso da ACL.

4- Como fazer para configurar uma access-control-list de forma a permitir todos os hosts da rede 200.157.18.200 para que os mesmos possam acessar uma determinada sub-rede em sua rede? Uma wildcard mask de "255.255.255.0" não funcionará, pois ela ignora os três primeiros bytes do endereço IP. O que deve ser feito, neste caso, é informar ao roteador para processar os três primeiros bytes do endereço IP de origem de cada pacote, ignorando o quarto byte, já que o objetivo é **permitir QUALQUER host** da rede 200.157.18.200. Portanto, a configuração do critério de inspeção da ACL seria conforme:

**200.157.18.0 0.0.0.255**

29

O roteador processa os três primeiros bytes e ignora o último byte, porque neste caso a wildcard mask está composta totalmente por "1" em sua composição binária (no último byte). Lembre-se: "0" deverá se processado, "1" não será processado. Na verdade, tudo deverá ser processado, mas somente os "0" deverão ser considerados pela ACL.

A filtragem de endereço ocorre com a utilização de máscaras wildcard para identificar o que é permitido ou bloqueado nos bits do IP. As máscaras wildcard para os bits de endereço IP utilizam o número 1 e o número 0 para a identificação do que deve ser filtrado nos bits do IP.

1- Uma máscara com valor 0 significa que o bit deve ser checado.

2- Uma máscara com valor 1 significa que o bit deve ser ignorado;

| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 | Observação |
|---|---|---|---|---|---|---|---|---|
| **0** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Verifica todos os bits |
| **0** | 0 | 0 | 0 | 0 | 1 | 1 | 1 | Ignora os últimos 3 bits |
| **1** | 1 | 1 | 1 | 0 | 0 | 0 | 0 | Verifica os últimos 4 bits |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **1** | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Ignora todos os bits do octeto |

**Figura 6: Exemplo de wildcard.**

**Fonte: O autor, 2015.**

30

**3.15 - Qual a relação entre a máscara de IP e a Wildcard?**

NÃO possuem relação alguma com as máscaras de IP. A máscara de sub-rede é utilizada para determinar quantos bits de um IP representam uma porção da sub-rede, ou seja, a máscara de sub-rede determina quais bits são importantes para definir uma sub-rede.

Um binário setado em 1 indica que o bit do endereço IP é parte de uma sub-rede, já o binário setado com 0 indica que o bit do endereço IP faz parte da porção host.

31

**3.16 - Como as máscaras de bits (0|1) bloqueiam ou permitem o tráfego de pacotes baseado no endereço IP?**

Suponha um administrador que deseja usar as máscaras wildcard para bits IP para verificar as sub-redes 172.30.16.0 até 172.30.31.0. Ele deseja testar um endereço IP por sub-rede (172.30.16.0 até 172.30.31.0), os dois primeiros octetos correspondem à rede (172.30), o terceiro octeto corresponde à sub-rede (16 até 31), o quarto octeto corresponde ao host.

Como fazer?

1- Inicialmente a máscara verifica os dois primeiros octetos 172.30, para isso usa 0s nos bits do wildcard;

2- Como não existe interesse em filtrar a parte host o quarto octeto será ignorado, para isso os bits devem ser setados para 1;

3- No terceiro octeto, onde está localizada a sub-rede, a máscara irá verificar a posição correspondente ao binário 16, ou seja, este bit deve estar com 0 bem como os bits superiores, já os bits abaixo do binário 16 devem ser ignorados, para que isso ocorra devem ser setados com 1s, assim temos:

| **128** | **64** | **32** | **16** | **8** | **4** | **2** | **1** |
|---|---|---|---|---|---|---|---|
| **0** | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| **verifica** | | | | ignora | | | |

**Figura 27: Exemplo de wildcard para IP 172.30.16.0 a 172.30.31.0.**

**Fonte: O autor, 2015.**

**Veja o resultado**.

Veja o resultado final

O resultado final é:

Para o endereço: 172.30.16.0

Com a máscara curinga: 0.0.15.255

Serão verificadas as sub-redes: 172.30.16.0 a 172.30.31.0

32

**3.17 – O que fazer para facilitar a utilização dos wildcard?**

Algumas sugestões:

1- Considere uma rede onde o administrador permite a entrada de qualquer endereço IP, ou seja, qualquer destino para sua rede é permitido. Para indicar qualquer endereço IP o administrador deve informar 0.0.0.0, agora para indicar que a lista de controle de acesso deve ignorar a verificação de qualquer bit a máscara deve ser setada com 1s, ignorar a verificação de qualquer bit significa aceitar todos, o resultado final será:

Endereço IP: 0.0.0.0
Máscara curinga: 255.255.255.255
Resultado: permite / aceita qualquer endereço
Neste caso, a máscara 255.255.255.255 pode ser substituída pela palavra **any**.

2- O administrador deseja criar uma regra que verifique um endereço IP específico. Dado o IP 172.30.1.29 deseja-se que a regra criada verifique todo o endereço, para que isso ocorra todos os bits devem ser setados com 0s, desta forma teremos:

Endereço IP: 172.30.1.29
Máscara curinga: 0.0.0.0
Resultado: verificação do endereço específico.
Neste caso a máscara 0.0.0.0 pode ser substituída pela palavra **host**.

33

**3.18 - Qual o risco de utilizar a máscara curinga incorreta?**

A utilização de máscara incorreta pode levar à implementação de listas de acesso com falhas.

Veja o exemplo a seguir:

Seja permitir todos os pacotes IP originados na sub-rede 10.10.0.0 255.255.0.0 com destino ao host 160.10.2.100 e todos os demais pacotes devem ser bloqueados.

```
absoluta(config)#

access-list 101 permit ip 10.10.0.0 0.0.0.0 160.10.2.100 0.0.0.0

absoluta(config)# exit

absoluta(config)# show  access-list  101

Extended IP access list 101

permit ip host 10.10.0.0 host 160.10.2.100
```

Foi criada uma lista de acesso usando a máscara 0.0.0.0.

Ao utilizar o comando "show access list" o roteador exibe uma entrada com "host". Isso significa que o endereço de origem deve ser exatamente 10.10.0.0, ou seja, somente será permitido o tráfego de pacotes com endereço IP de origem 10.10.0.0 e destino 160.10.2.100.

Todos os demais endereços serão bloqueados, inclusive 10.10.1.1, 10.10.1.2 etc. Não é isso que queremos. O nosso objetivo é **permitir o tráfego de todos os hosts** da sub-rede 10.10.0.0/16.

Veja a seguir o que fazer.

34

Deve-se, então, criar uma máscara que verifique os dois primeiros octetos "10.10" e ignore os dois últimos "0.0". Lembre-se que binário 0 significa verificar e binário 1 significa ignorar, baseado nesta informação, vamos novamente criar a lista de controle de acesso:

```
absoluta(config)#

access-list 101 permit ip 10.10.0.0 0.0.255.255 160.10.2.100 0.0.0.0

absoluta(config)# exit

absoluta(config)# show  access-list  101

Extended  IP  access  list  101

permit  ip  10.10.0.0  0.0.255.255  host  160.10.2.100
```

Agora o comando "show access list" mostra a nova máscara, desta vez de forma correta. Os dois últimos octetos contém todos os bits setados para 1 (o que equivale ao decimal 255).

Resumindo, para não complicar, tudo que se tem a fazer é subtrair a máscara de sub-rede em formato decimal de 255, isso para cada um dos octetos.

Vejamos um exemplo:

```
máscara de rede: 255.255.224.0

máscara wildcard:  ???.???.???.???

pimeiro octeto  =  255  -  mascara de rede  =  255  -  255  =  0

segundo octeto  =  255  -  mascara de rede  =  255  -  255  =  0

terceiro octeto  =  255  -  mascara de rede  =  255  -  224  =  31

quarto  octeto  =  255  -  mascara de rede  =  255  -  0     =  255

máscara wildcard: 0.0.31.255
```


Esta é a forma rápida e fácil de determinar as máscaras wildcard. Mas o importante é entender ***por que*** isso funciona e não simplesmente ***como*** funciona.

35

**3.19 - Como fica o desempenho do roteador com as Listas de Acesso?**

Sabe-se que as regras da lista de controle de acesso são analisadas sequencialmente, ou seja, regra-1, regra-2, regra-3 e assim sucessivamente até que seja encontrada uma regra, que coincida com o pacote analisado ou encontrar a última regra que bloqueia tudo que não está permitido.

Desta forma devemos observar alguns **procedimentos** que devem ser adotados no sentido de minimizar os possíveis **impactos negativos** que as listas de controle de acesso possam causar.

Uma sugestão de **estratégia de implementação** para minimizar o impacto negativo é:

1. Sempre que possível aplicar as listas de controle de acesso no sentido de entrada (in), pois desta forma os pacotes serão descartados antes de serem encaminhados para uma das interfaces de saída, consequentemente minimizando o processamento de roteamento de pacotes;
2. Implementar inicialmente as regras que contemplam o maior volume de transações da sua rede, agrupada por servidor/serviços;

**2.1.** Como a pilha IP inclui ICMP,TCP e UDP. Sempre insira primeiro as regras mais específicas, para depois colocar as mais genéricas;

**3.** Após a implementação da lista por grupo de servidor/serviço insira uma regra que bloqueia todos os demais pacotes do grupo, isso evita que o pacote passe pelo crivo de outros grupos ao qual não pertence.

Procedimentos

Procedimentos para **minimizar o impacto** que as listas de controle de acesso possam causar:

1. Mensurar os recursos do roteador (memória, processador, outros);
2. Avaliar os serviços habilitados no roteador (criptografia, outros);
3. Entender o tráfego da rede;
4. Mensurar o volume de pacotes;

Classificar o volume de tráfego por servidor, protocolo e sentido do tráfego.

36

### 3.20 – Um exemplo completo

Para os exemplos a seguir assuma a topologia de rede conforme a figura 2.8 abaixo.

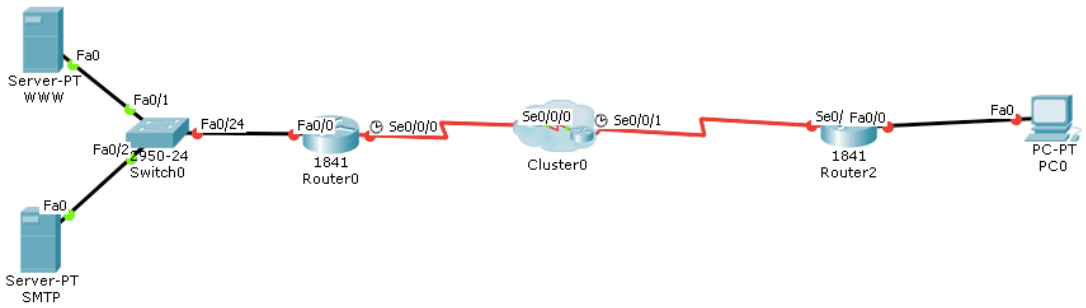



**Figura 8: Cenário para o exemplo completo.**

**Fonte: O autor, 2015.**

**a)** Montagem de regras para conexão de SMTP, de forma a permitir o envio e recebimento de e-mails.

| regra | direção | ip_org. | ip_dst. | Proto. | porta_dst. | ação |
|---|---|---|---|---|---|---|
| **A** | in | externo | interno | TCP | 25 | permite |

| | | | | | | |
|---|---|---|---|---|---|---|
| **B** | out | interno | externo | TCP | >1023 | permite |
| **C** | out | interno | externo | TCP | 25 | permite |
| **D** | in | externo | interno | TCP | >1023 | permite |
| **E** | ambas | qualquer | qualquer | qualquer | qualquer | bloqueia |

As regras A e B permitem a entrada de e-mail

As regras C e D permitem a saída de e-mail

A regra E é a regra default que bloqueia tudo

O servidor SMTP possui o IP 10.0.0.1 e alguém de uma rede externa com IP 172.16.2.3 tenta enviar um e-mail. A porta de origem utilizada pelo cliente externo é 1234 com destino para 25, analise esta situação de acordo com as regras implementadas:

| **pacote** | **direção** | **ip_orig.** | **ip_dest.** | **Protocolo** | **porta_dest.** | **ação** |
|---|---|---|---|---|---|---|
| **1** | in | 172.16.2.3 | 10.0.0.1 | TCP | 25 | permite (A) |
| **2** | out | 10.0.0.1 | 172.16.2.3 | TCP | >1023 | permite (B) |

Neste caso, as regras do roteador permitem a entrada dos pacotes de e-mail:

A regra A permite a entrada do pacote com origem em 172.16.2.3 e destino 10.0.0.1.

A regra B permite que o servidor 10.0.0.1 responda ao cliente 172.16.2.3.

37

Agora considere o caso de alguém respondendo este e-mail. O cliente localizado na rede interna possui o IP 10.0.0.4 usando a porta 1245 vai responder para um usuário que possui conta no servidor 172.16.2.1 porta 25:

| **pacote** | **direção** | **ip_org.** | **ip_dst.** | **Proto.** | **porta_dst.** | **Ação** |
|---|---|---|---|---|---|---|
| **3** | out | 10.0.0.4 | 172.16.2.1 | TCP | 25 | permite (C) |
| **4** | in | 172.16.2.1 | 10.0.0.4 | TCP | >1245 | permite (D) |

Neste caso as regras do roteador permitem a saída dos pacotes de e-mail:

A regra C permite que o cliente 10.0.0.4 envie o e-mail para o servidor 172.16.2.1.

A regra D permite que o servidor 172.16.2.1 responda ao cliente 10.0.0.4.

Agora suponha que alguém localizado em uma rede externa, 172.16.2.3, usando a porta 4321 tente abrir uma conexão no servidor 10.0.0.1 na porta de x-windows, 6000:

| pacote | direção | ip_org. | ip_dst. | Proto. | porta_dst. | ação |
|---|---|---|---|---|---|---|
| **5** | in | 172.16.2.3 | 10.0.0.1 | TCP | 6000 | permite (D) |
| **6** | out | 10.0.0.1 | 172.16.2.3 | TCP | 4321 | permite (B) |

Neste caso as regras do roteador comportam-se da seguinte forma:

As regras A e B permitem a entrada de pacotes SMTP.

As regras C e D permitem a saída de pacotes SMTP.

Já as regras B e D permitem qualquer conexão que utilizem portas >1023.

É isso mesmo que quer?

NÃO! Para contornar esta situação deve agregar mais um elemento às regras: a porta de origem. Veja a seguir.

38

Veja como fica:

| regra | direção | ip_org. | ip_dst. | Proto. | porta_org. | porta_dst. | ação |
|---|---|---|---|---|---|---|---|
| **A** | in | externo | interno | TCP | >1023 | 25 | permite |
| **B** | out | interno | externo | TCP | 25 | >1023 | permite |
| **C** | out | interno | externo | TCP | >1023 | 25 | permite |
| **D** | in | externo | interno | TCP | 25 | >1023 | permite |
| **E** | ambas | qualquer | qualquer | qualquer | qualquer | qualquer | bloqueia |

Agora veja o comportamento das regras com este novo elemento:

| pacote | direção | ip_org. | ip_dst. | Proto. | porta_org. | porta_dst. | ação |
|---|---|---|---|---|---|---|---|
| **1** | in | 172.16.2.3 | 10.0.0.1 | TCP | 1234 | 25 | permite (A) |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **2** | out | 10.0.0.1 | 172.16.2.3 | TCP | 25 | 1234 | permite (B) |
| **3** | out | 10.0.0.4 | 172.16.2.1 | TCP | 1245 | 25 | permite (C) |
| **4** | in | 172.16.2.1 | 10.0.0.4 | TCP | 25 | 1245 | permite (D) |
| **5** | in | 172.16.2.3 | 10.0.0.1 | TCP | 4321 | 6000 | bloqueia (E) |
| **6** | out | 10.0.0.1 | 172.16.2.3 | TCP | 6000 | 4321 | bloqueia (F) |

Como se observa, após a inclusão deste novo elemento de filtragem foi possível bloquear o ataque à porta x-windows.

Mas o que impede de alguém tentar abrir uma conexão na porta x-windows, 6000, usando como origem a porta 25?

39

Analise o que acontece nesta situação:

| pacote | direção | ip_org. | ip_dst. | Proto. | porta_org. | porta_dst. | ação |
|---|---|---|---|---|---|---|---|
| **7** | in | 172.16.1.2 | 10.0.0.1 | TCP | 25 | 6000 | permite (D) |
| **8** | out | 10.0.0.1 | 172.16.1.2 | TCP | 6000 | 25 | permite (C) |

Como se nota, este pacote será permitido e a tentativa de abertura de conexão terá sucesso.

Para resolver este problema deve-se incluir mais um elemento nos filtros: a análise das flags dos pacotes TCP, especificamente a flag ACK.

| regra | direção | ip_org. | ip_dst. | Proto. | porta_org. | porta_dst. | flag | ação |
|---|---|---|---|---|---|---|---|---|
| **A** | in | externo | interno | TCP | >1023 | 25 | qualquer | permite |
| **B** | out | Interno | externo | TCP | 25 | >1023 | Só ACK | permite |
| **C** | out | Interno | externo | TCP | >1023 | 25 | qualquer | permite |
| **D** | in | Externo | interno | TCP | 25 | >1023 | Só ACK | permite |
| **E** | ambas | Qualquer | qualquer | qualquer | qualquer | qualquer | qualquer | bloqueia |

No processo de estabelecimento de conexão TCP, sempre o primeiro pacote possui a flag ACK setada como 0. Já os demais pacotes da conexão possuem a flag ACK setada em 1.

Agora analise o que ocorre com a inclusão deste novo elemento no filtro:

| pacote | direção | ip_orig. | ip_dest. | protocolo | porta_orig. | porta_dest. | flag | ação |
|---|---|---|---|---|---|---|---|---|
| **7** | in | 172.16.1.2 | 10.0.0.1 | TCP | 25 | 6000 | ACK=0 | bloqueia(E) |

Como pode notar agora as tentativas de abertura de conexão com origem em redes externas e destinadas a portas >1023 serão bloqueadas.

Com o exemplo dado, damos por encerrada esta etapa, sem exaurir o assunto que é bastante vasto. No próximo módulo será abordado o assunto DMZ que emprega o NAT, PAT e a ACL estudados até então.

40

## Resumo

O NAT (Network Address Translation) é um protocolo tradutor de endereços de camada-3 (rede) que visa:

1) minimizar os efeitos da escassez de endereços ipv4;

2) aumentar a segurança da rede interna das empresas.

3) conectar redes privadas à internet, pois traduzem IPs privados para ips públicos.

É um mecanismo para conectar redes privadas à Internet (rede externa, desconhecida e totalmente insegura), pois serve como ponto de tradução de IPs privados, não roteáveis na Internet, para IPs públicos, roteáveis na Internet.

Há dois tipos básicos de NAT: Estático, com estabelecimento de uma relação entre endereços locais e endereços públicos (da Internet) de maneira fixa. Sempre um IP interno será traduzido para um mesmo IP externo. O segundo tipo é o NAT Dinâmico que mapeia endereços locais e endereços da Internet de maneira fixa.

Alguns termos técnicos mais importantes a saber são:

a) Endereço local interno (Inside local address): endereço privado pertencente a rede interna. É o endereço a ser traduzido.

b) Endereço global interno (Inside global address): endereço válido na Internet pertencente ao roteador que está com o NAT configurado.

c) Endereço local externo (Outside local address): Endereço do host remoto pertencente à Internet.

d) Endereço global externo (Outside global address): Endereço da rede remota

**41**

O PAT – Port Address Translation assim como o NAT o PAT é um tradutor de endereços de camada-3 (rede) que tem o mesmo objetivo que o NAT, ou seja, visa:

1) minimizar os efeitos da escassez de endereços ipv4;

2) aumentar a segurança da rede interna das empresas.

3) conectar redes privadas à internet, pois traduzem IPs privados para ips públicos.

O PAT traduz o IP de origem e utiliza números de porta TCP e UDP de origem para distinguir cada uma das traduções que justifica o nome, ou seja, tradução de porta e endereço.

ACLs: Access Control Lists ou, Listas de Controle de Acesso de acesso de pacotes IP, também conhecidas como “access-lists”, são úteis para a manipulação do tráfego, podendo ser empregadas como métodos de packet filtering (ou filtro de pacotes), policy-based routing, route-maps, class-maps, NAT/PAT, entre outras aplicações. A forma mais comum de utilização das ACLs é o filtro de pacotes padrão, o que seria um firewall básico filtrando pacotes utilizando-se do contexto de endereços de origem e destino, assim como portas de origem e destino. As access-lists podem ser configuradas para todos os protocolos roteáveis, como o TCP/IP, IPX, AppleTalk, e isso nos permite controlar o tráfego de entrada ou saída em um roteador Cisco.

Pacotes IP transportam qualquer tipo de informação em uma rede, as ACLs controlam o acesso de TUDO e de TODOS! É um conjunto de instruções que diz ao roteador para aceitar ou rejeitar determinados pacotes vindos de redes IP especificadas. Esse filtro atua até na camada “4”, onde é possível especificar portes TCP ou UDP que se deseja filtrar.

São utilizados apenas dois parâmetros ao configurar uma ACL: PERMIT ou DENY. Estes parâmetros são seguidos das definições DO QUE se deve permitir (PERMIT) ou negar (DENY).

TODA ACL criada em um roteador Cisco termina com um DENY ANY implícito, negando TUDO, a todos, portanto MUITO CUIDADO.

Foram estudados dois tipos de ACL: ACL Padrão (standard) e ACL estendida (extended). Existe também a variação, a ACL nomeada, que ao invés de números usa nomes para identificá-la. A diferença básica entre os dois tipos de ACL é o grau de inspeção do pacote IP, antes de permitir ou negar seu acesso.

## UNIDADE 4 – CONCEITOS INTRODUTÓRIOS DE SEGURANÇA DE REDES: NAT, PAT, ACL E DMZ

### MÓDULO 3 – DMZ (ZONA DESMILITARIZADA)

**01**

## 1 – Conceito, função e características da DMZ

Atualmente estamos na era da **internet das coisas**. Assim como ocorreu um enorme avanço na comunicação entre redes, tornando possível o compartilhamento globalizado de seus recursos e informações, a segurança destas redes passou a ser crítica.

Em consequência, a segurança é considerada essencial no projeto de uma rede, seja esta corporativa, acadêmica ou até mesmo pessoal. As razões dessa nova preocupação estão relacionadas diretamente com o valor dos dados armazenados e ainda com a necessidade de se garantir diferentes níveis de privacidade, integridade e autenticidade para cada tipo de dado.

Uma das formas de otimização da segurança é pela implementação da **DMZ – Zona Desmilitarizada**.

A Zona Desmilitarizada é um segmento de rede separado das demais redes. Ela serve como uma segurança adicional entre a sua rede (interna) corporativa e a Internet (externa) pública. A DMZ pode ser utilizada, também, para separar determinada máquina, colocando-a fora da proteção de um firewall.

A DMZ é um conceito e não um *software* ou *hardware*. Consiste em separar, por meio físico e lógico, os setores, departamentos ou estações de uma rede corporativa. Este conceito é largamente utilizado por grandes corporações, governos e bancos.

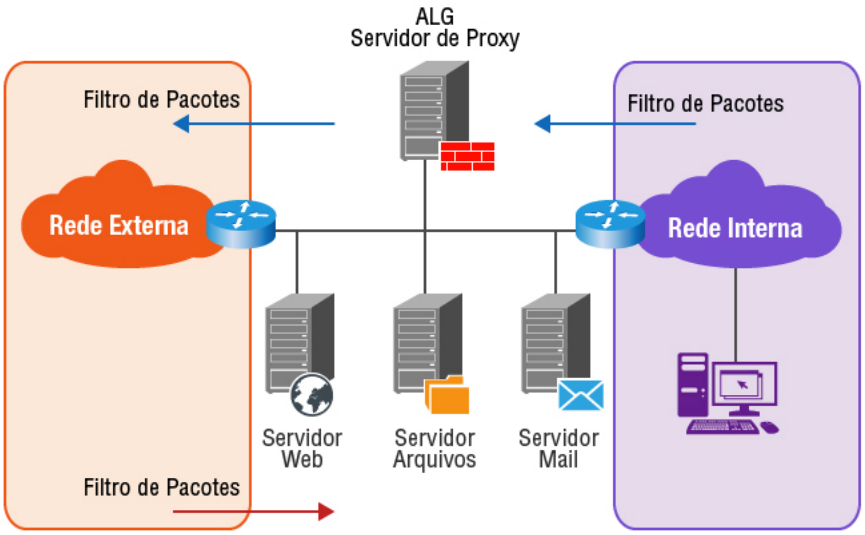
Geralmente essas companhias possuem como maior valor corporativo as **informações**, para elas é muito mais caro perder uma base de dados inteira do que um funcionário de renome, afinal, a informação é a alma da empresa.

02

### 1.1- Função de uma DMZ

A função de uma DMZ é separar os serviços externos, como http e ftp da rede local, com minimização dos danos de uma invasão à rede local. Para atingir este objetivo, os computadores presentes em uma DMZ não devem conter forma alguma de acesso à rede local.

Uma DMZ fica localizada entre uma rede interna e uma rede externa. Na criação de uma DMZ, acrescenta-se um segmento a mais de rede ou sub-rede que ainda faz parte do sistema por meio de uma terceira porta de interface no firewall. Esta configuração permite que o firewall troque dados com a rede geral e com a máquina isolada usando Network Address Translation (NAT). O firewall não costuma proteger o sistema isolado, permitindo que ele se conecte mais diretamente à Internet.




Uma DMZ pode ser implementada com filtros de rede configurados nas suas bordas, estes filtros são responsáveis por realizar o controle de acesso do que entra e do que sai da DMZ e podem ser do tipo filtro de pacotes, filtragem total de pacotes e de cache como servidores de proxy conhecidos como **ALG**s (Application Layer Gateway).

ALG

As ALGs - Application Layer Gateway, que são servidores de proxy, localizados em uma DMZ, servem como intermediários entre os hosts da rede interna e as redes externas como a Internet. É possível impor restrições de acesso com base no horário, login, endereço IP entre outros. Uma ALG serve também como cache de rede, armazenando as informações de páginas e arquivos já acessados.

As ALGs funcionam no nível da aplicação e interceptam e estabelecem conexões dos hosts da rede interna com a rede externa, autorizando ou não a conexão.

**03**

A filtragem de pacotes (Packet filtering) limita o tráfego dentro da rede, baseado no destino e na origem de endereços, IPs, portas e outras flags que podem ser utilizadas na implementação das regras de filtro.


A filtragem total de pacotes filtra o tráfego baseado no destino e na origem dos endereços IPs, portas, flags além de realizar "stateful inspection", uma inspeção de pacotes que permite o armazenamento de dados de cada conexão em uma **tabela de sessão**.

As DMZs podem possuir a capacidade de conter um ataque e limitar os danos na rede.

Uma das arquiteturas mais utilizadas são as DMZs que utilizam uma solução de **defesa em camadas**.

As múltiplas camadas de segurança que uma DMZ oferece são distribuídas entre pontos de serviços e de filtragem. Os pontos de filtragem inicialmente servem para proteger os serviços. Se os serviços da rede são comprometidos, a capacidade de um ataque prosseguir fica limitada. Tanto o tráfego que entra e sai da DMZ é filtrado, seja por roteadores ou por meio de firewalls.

Nesta disciplina vamos nos concentrar na **filtragem nos roteadores**.

Packet Filtering

Um firewall com filtragem de pacotes (packet filtering) é essencialmente um router com software de filtragem de pacotes. A filtragem de pacotes trabalha ao nível de rede do modelo OSI; cada pacote de dados é examinado quando a transferência de dados é feita de uma rede para a outra. Os pacotes de dados compatíveis com as regras de controle de acesso são autorizados a passar, aqueles que não obedecerem às regras serão barrados.

Stateful inspection

Os firewalls baseados no estado (stateful inspection firewalls) analisam todo o tráfego de dados para encontrar estados, ou seja, padrões aceitáveis por suas regras e que, a princípio, serão usados para manter a comunicação. Estas informações são então mantidas pelo firewall e usadas como parâmetro para o tráfego subsequente. Por exemplo, suponha que um aplicativo iniciou um acesso para transferência de arquivos entre um cliente e um servidor. Os pacotes de dados iniciais informam quais portas TCP serão usadas para esta tarefa. Se, de repente, o tráfego começar a fluir por uma porta não mencionada, o firewall pode então detectar esta ocorrência como uma anormalidade e efetuar o bloqueio.

Tabela de sessão

Esta tabela armazena o estado do fluxo de pacotes e serve como ponto de referência para determinar se os pacotes pertencem a uma conexão existente ou se são pacotes de uma fonte não autorizada.

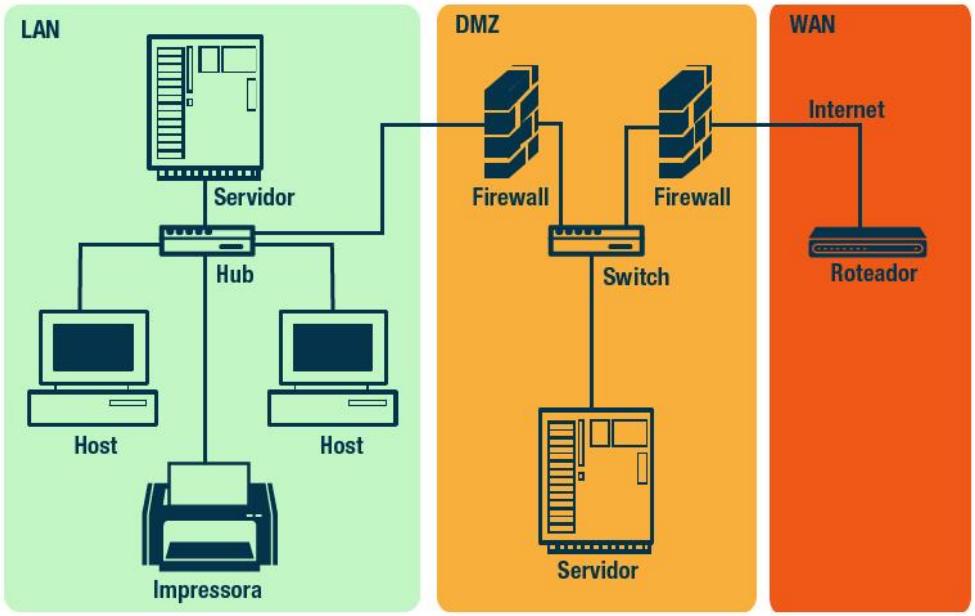
Camadas

Para montar uma DMZ que utilize múltiplas camadas de segurança, você precisa reunir diversas funcionalidades como packet filtering, stateful packet filtering e um servidor de proxy.

04

Os servidores públicos que ficam localizados na DMZ exigem medidas de segurança adequadas. Os serviços são protegidos, aumentando a dificuldade de um invasor comprometer os serviços disponíveis dentro do perímetro da DMZ.

Quando um ataque consegue entrar na DMZ, o ataque não é capaz de passar para a rede interna devido aos pontos de filtragem que oferecem uma defesa adicional. A implementação de funcionalidades, tais como VLANs (redes virtuais), podem ajudar a combater estes ataques.




**Exemplo de rede com DMZ**

Perímetro

O termo rede de perímetro refere-se a um segmento de rede isolado no ponto em que uma rede corporativa alcança a Internet. As redes de perímetro destinam-se a criar um limite que permite a separação do tráfego entre redes internas e externas. Com este limite, é possível categorizar, colocar em quarentena e controlar o tráfego da rede de uma empresa. A segurança de perímetro é proporcionada por um dispositivo de perímetro, como um firewall, por exemplo, que inspeciona os pacotes e as sessões para determinar se devem ser transmitidos para a rede protegida ou a partir dela ou ser abandonados.

05

**1.2– Características da DMZ**

As quatro características mais importantes de uma DMZ são:

1) Servidores que precisam ser acessados externamente são posicionados dentro de uma DMZ;
2) é estabelecida entre as zonas insegura e segura;
3) realiza o controle do tráfego do que entra e do que sai da rede;
4) pode conter um ataque sem que o mesmo passe para a rede interna.

Sabe-se que a rede possui algumas vulnerabilidades, tais como:

1) **Exposição da rede interna à internet**: disponibilizar serviços da rede interna (e-mail e outros) na mesma máquina que provê os serviços externos (web, por exemplo) deixa a rede interna exposta a ações da rede externa (Internet), pois deixarão os dados do usuário expostos em caso de uma invasão.
2) **Vulnerabilidades conhecidas:** concentrar muitos serviços em uma única máquina gera maior fragilidade a vulnerabilidades conhecidas, pois quanto mais serviços disponíveis, mais vulnerabilidades podem ser exploradas e, consequentemente, maior grau de exposição e risco de invasão.

A **solução** para os problemas acima citados seria:

**a)** a **divisão dos serviços críticos.**

**b) adoção de um *firewall*.**

divisão dos serviços críticos.

Separar os diversos servidores: Internet, E-mail, DNS2 e outros. Se um dos servidores for afetado por

algum ataque, apenas o serviço será parado e o restante funcionará normalmente.

adoção de um *firewall*

Seu objetivo é permitir somente a transmissão e a recepção de dados autorizados. Existem firewalls baseados na combinação de *hardware* e *software* e firewalls baseados somente em *software*. Este último é o tipo recomendado ao uso doméstico e também é o mais comum. O firewall é um mecanismo que atua como "defesa" de um computador ou de uma rede, controlando o acesso ao sistema por meio de regras e a filtragem de dados. A vantagem do uso de firewalls em redes, é que somente um computador pode atuar como firewall, não sendo necessário instalá-lo em cada máquina conectada.

06

**1.3- Implantando a DMZ**

O projeto lógico de uma rede que visa conexões com a Internet deve envolver a criação de uma DMZ. Esta DMZ será protegida por um sistema de defesa no qual os usuários de Internet podem entrar livremente para acessar os servidores web públicos, enquanto que os dispositivos localizados nos pontos de acesso filtram todo o tráfego não permitido, como por exemplo, pacotes de dados que tentam prejudicar o funcionamento do sistema.

A zona desmilitarizada comporta-se como uma outra sub-rede, atrás de um firewall, onde temos uma máquina segura na rede externa que não executa nenhum serviço, mas apenas avalia as requisições feitas a ela e encaminha cada serviço para a máquina destino na rede interna.

No caso de uma invasão de primeiro nível, o atacante terá acesso apenas ao firewall, não causando problema algum para a rede da empresa. Já em invasões de segundo nível, o atacante conseguirá passar do firewall para a sub-rede interna, mas ficará preso na máquina do serviço que ele explorar.


Para implementar uma DMZ podemos utilizar diversos tipos de dispositivos, sendo que o nível de segurança pode ser variado dependendo das funcionalidades disponíveis em cada dispositivo.

Em roteadores SOHO é possível criar uma DMZ rapidamente, porém este tipo de DMZ somente libera o acesso de um dispositivo da rede interna para a rede externa sem adicionar funcionalidades avançadas de segurança. Mas se você quer montar uma DMZ que utilize múltiplas camadas de segurança, você precisa reunir diversas funcionalidades como *packet filtering*, *stateful packet filtering* e um servidor de proxy.

Quanto aos **equipamentos** para implementação de uma DMZ, podemos utilizar roteadores com sistema operacional, que permita funções avançadas de segurança ou servidores utilizando Linux. Como dito acima, na nossa disciplina vamos concentrar nos roteadores.

07

## 2 – Acessos Externos à DMZ

Frequentemente máquinas da rede precisam receber acessos externos (servidores SMTP e servidores Web). Como já vimos, a função de uma DMZ é manter todos os serviços que possuem acesso externo (tais como servidores HTTP, FTP, de correio eletrônico etc) juntos em uma rede local, limitando, dessa forma, eventual dano em caso de comprometimento de algum destes serviços por um invasor. Para isso, os computadores presentes em uma DMZ não devem conter nenhuma forma de acesso à rede local.

Para permitir que as máquinas da rede possam desempenhar suas funções, mas que ao mesmo tempo o restante da rede continue protegido, muitos firewalls oferecem a opção de criar uma zona para essa vigilância, a DMZ. Nesse caso, o controle de acesso à internet pode ser feito através de um **projeto de DMZ**, permitindo que todo o tráfego entre os servidores da empresa, a rede interna e a internet passe por um firewall e pelas regras de segurança criadas para a proteção da rede interna.

Os firewalls se tornam único ponto de acesso à rede em que o tráfego pode ser analisado e controlado, por meio de scripts de firewall que definem o aplicativo, o endereço e os parâmetros de usuário. Esses scripts ajudam a proteger os caminhos de conectividade para redes e centros de dados externos.

08

### 2.1 - Como os serviços são filtrados

Segundo Nemeth et all (2004) a maioria dos serviços conhecidos está associada a uma porta de rede, no Linux esta associação está no arquivo */etc/services* e em outros fabricantes em um arquivo equivalente. Os aplicativos que fornecem os serviços vinculam os serviços às portas e ficam aguardando conexões remotas a estas portas. A maioria das portas de serviços mais conhecidas são chamadas de **privilegiadas** e os seus números estão entre 1 a 1023. As portas com numeração de 1024 acima são conhecidas como **portas não privilegiadas**.

As **portas privilegiadas** podem ser usadas por processos que estão sendo executados como root, assim a filtragem de serviços específicos baseia-se na suposição de que o cliente que iniciará a conversação através de TCP ou UDP utilizará uma porta não privilegiada para conectar-se a uma porta privilegiada no servidor.

Segundo o mesmo autor, para permitir o uso de serviços SMTP, por exemplo, seria necessário instalar um filtro, que permita que pacotes TCP endereçados à porta 25, saiam da rede com destino a qualquer endereço externo.

O autor afirma ainda que a maneira mais segura de usar um filtro de pacotes é iniciar a configuração que não permita nada a não ser SMTP que chega. Em seguida seriam liberadas as portas para serviços necessários e úteis para a rede e que não estariam em funcionamento.

Segundo Kurose (2006) a **filtragem de pacotes** normalmente é baseada em:

1) Endereço IP de origem e destino,

2) Porta TCP ou UDP de origem e destino,

3) Tipo de mensagem ICMP,

4) Datagramas de inicialização de conexão usando bits TCP SYN ou ACK.

09

## 3 - Arquitetura e configuração de DMZ

Como dito anteriormente, nossa implementação da DMZ contemplará o roteador que terá o NAT e ACLs para compor a mesma.

A configuração final do roteador da DMZ está listada abaixo:

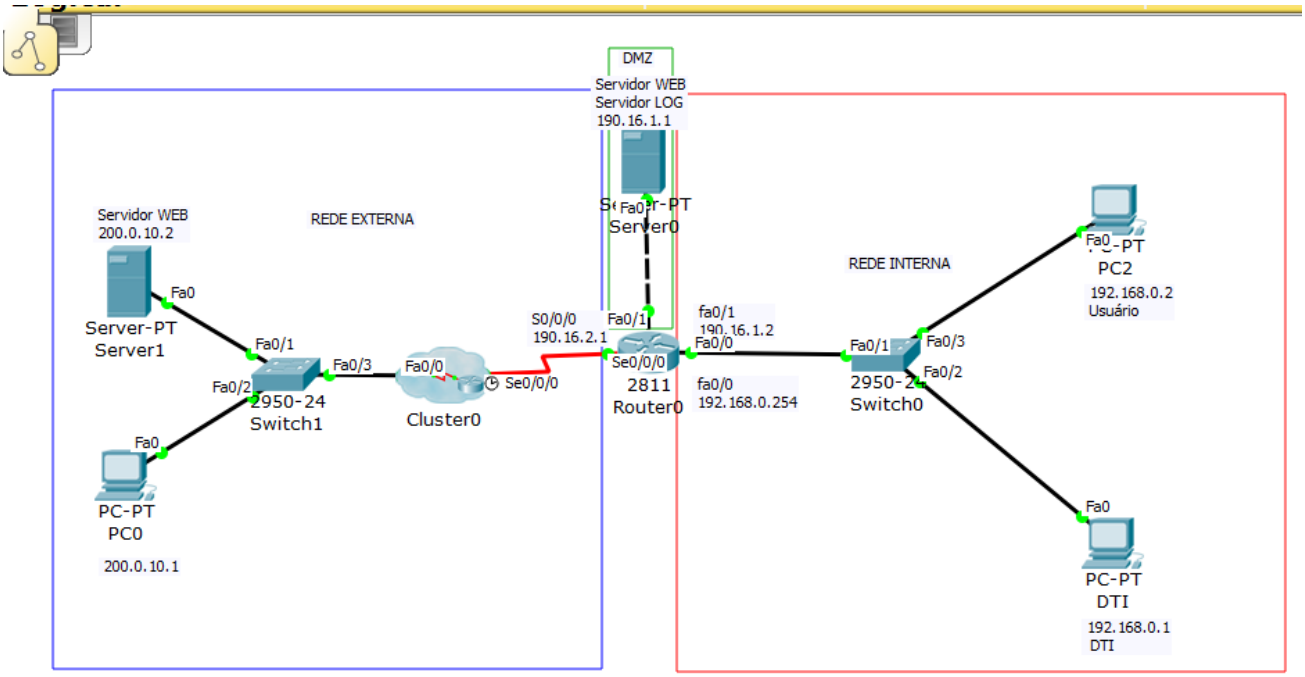
```
rt_dmz#show run
Building configuration...
Current configuration : 1344 bytes
version 12.4
........  omitida ......
hostname rt_dmz
ip inspect name dmz http audit-trail on
interface FastEthernet0/0
ip address 192.168.0.254 255.255.255.0
ip access-group rede_interna in
ip inspect dmz in
interface FastEthernet0/1
```

```
ip address 190.16.1.2 255.255.255.252
ip access-group dmz in
interface Serial0/0/0
ip address 190.16.2.1 255.255.255.252
ip access-group rede_externa in
ip inspect dmz in
clock rate 2000000
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
ip access-list extended rede_interna
permit tcp any any eq www
permit icmp any any
deny ip any any
ip access-list extended dmz
permit icmp any host 192.168.0.1
deny ip any any
ip access-list extended rede_externa
permit tcp any host 190.16.1.1 eq www
permit icmp any host 192.168.0.1 echo-reply
logging 190.16.1.1
end
rt_dmz#
```

Um exemplo simples de DMZ será demonstrado na figura que veremos a seguir.

**10**

A figura abaixo ilustra um **cenário típico de DMZ simples**.




**Cenário de uma DMZ Simples**

**Fonte: O autor, 2015.**

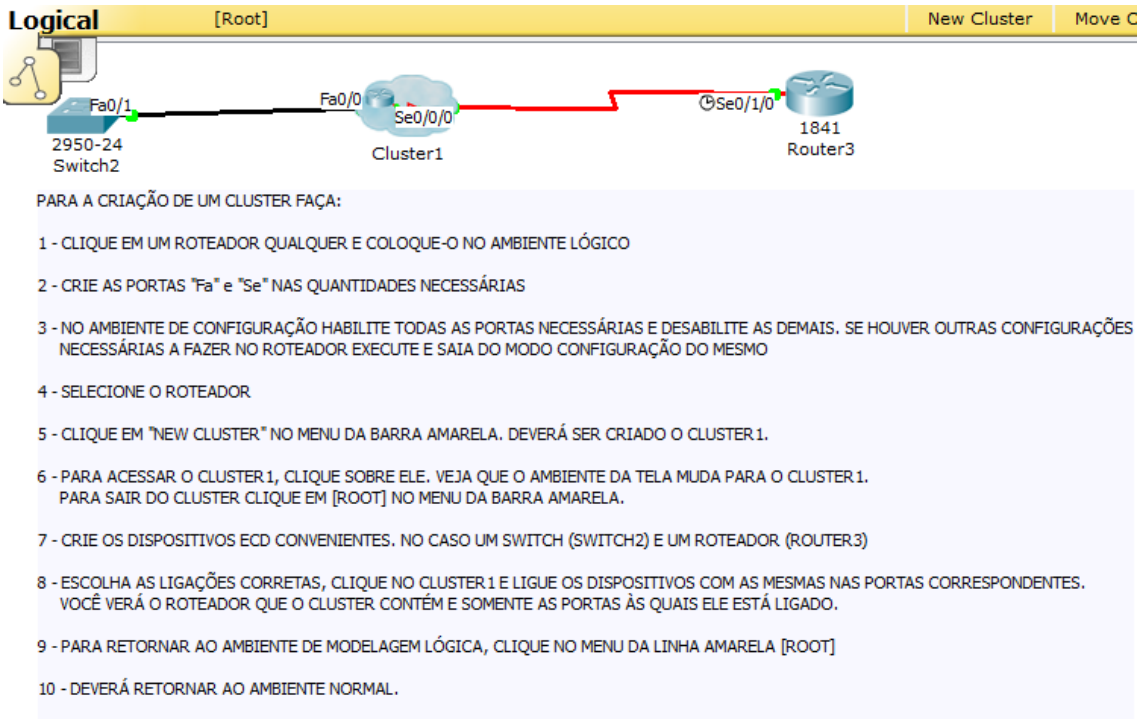
Para o resultado da listagem apresentada, conforme cenário dado, a **configuração da rede** deve seguir os passos abaixo:

1) Nomeie o servidor WEB externo como server1;
2) Nomeie o servidor WEB e LOG interno como Server0;
3) Nomeie o Router0 (2811) com hostname rt_dmz;
4) Nomeie o host DTI;
5) Configure os IPs, portas e gateways de acordo com a topologia dada.

As redes da família 190.16.0.0 têm máscara /30 e as demais têm máscara /24.

11

Para a **criação de um Cluster** faça:




**Criação de um cluster no Packet Tracer 6.2.0.**

**Fonte: O autor, 2015.**

Após a aplicação do plano de endereçamento IP, teste a conectivadade da rede com PING normal de todos para todos os vizinhos. Caso haja insucesso, retifique a configuração adequadamente para que haja conectividade com todos.

12

### 3.1– Configuração da DMZ Simples

Para a configuração da DMZ, o primeiro passo é a definição da **política de segurança da DMZ**:

1) Os dispositivos da rede externa só poderão realizar acesso HTTP no servidor WEB localizado na DMZ;

2) Os dispositivos da rede interna poderão realizar acesso HTTP no servidor WEB localizado na DMZ e em dispositivos da rede externa;

3) A estação de trabalho DTI poderá realizar ICMP e HTTP para o servidor WEB localizado na DMZ e para dispositivos da rede externa;

4) Qualquer outro tipo de tráfego deverá ser bloqueado;

5) Todo o tráfego HTTP que entrar no roteador deverá ser inspecionado;

6) Todos os logs de inspeção de pacotes deverão ser encaminhados para o servidor de LOG.

Vamos utilizar para a configuração da DMZ o processo **Stateful Packet Filtering** em roteadores Cisco. Siga a sequência lógica de implementação dos comandos de ACL e de inspeção de pacotes, de acordo com as etapas a seguir:

Etapa 01 - Identificar as interfaces internas e externas;

Etapa 02 - Definir as regras de ACLs nas interfaces;

Etapa 03 - Definir as regras de inspeção de pacotes;

Etapa 04 - Aplicar as regras de inspeção de pacotes e as ACLs nas interfaces;

Etapa 05 - Configurar o servidor que receberá as mensagens de auditoria;

Etapa 06 - Testar e verificar as configurações aplicadas.

**Etapa 01 - Identificar as interfaces internas e externas**

Router0 - porta fa0/0: Será a porta interna

Router0 - porta s0/0/0: Será a porta externa

Router0 - porta fa0/1: Será a porta da DMZ que contem o Servidor WEB e de LOG

**Etapa 02 - Definir as regras de ACLs das interfaces**

Entre no modo configuração com o comando “conf t” e digite (todo texto após o sinal de exclamação (!) é considerado como comentário e não será processado pelo roteador).

**(config)# ip access-list extended rede_interna** ! cria uma ACL estendida com nome rede_interna

**(config-ext-nacl)# permit tcp any any eq www** ! permite todo tráfego tcp de qualquer origem para qualquer destino que tenha a porta 80

**(config-ext-nacl)# permit icmp any any** ! permite todo tráfego icmp de qualquer origem para qualquer destino

**(config-ext-nacl)# deny ip any any** ! nega todo o tráfego ip de qualquer origem para qualquer destino. Comando implícito em qualquer ACL

**(config-ext-nacl)# ip access-list extended dmz** ! cria uma ACL estendida com nome dmz

**(config-ext-nacl)# permit icmp any host 192.168.0.1** ! permite todo tráfego icmp de qualquer origem para o host 192.168.0.1

**(config-ext-nacl)#deny ip any any** ! nega todo o tráfego ip de qualquer origem para qualquer destino

**(config)# ip access-list extended rede_externa** ! cria uma ACL estendida com nome rede_externa

**(config-ext-nacl)# permit tcp any host 190.16.1.1 eq www** ! permite todo tráfego tcp de qualquer origem para o host 190.16.1.1 que tenha a porta 80

**(config-ext-nacl)# permit icmp any host 192.168.0.1 echo-reply** ! permite todo tráfego icmp de resposta de qualquer origem para o host 192.168.0.1

Saia do modo global.

**Etapa 03 - Definir as regras de inspeção de pacotes**

Comande "conf t" se necessário para entrar no modo (config).

**(config)# ip inspect name DMZ http audit-trail on !** define uma regra de inspeção de pacotes, com o nome DMZ onde todo o tráfego http será inspecionado e logado. A inspeção de pacotes http permite automaticamente o retorno do tráfego de todas as sessões http, mesmo que haja uma regra de bloqueio por uma ACL.

Veja a definição do comando de inspeção separadamente:

**ip inspect**: Habilita a inspeção de pacotes;

**name**: Define que a regra de inspeção terá um nome;

**DMZ**: Nome da inspeção (define um nome para a regra de inspeção, pode ser qualquer nome);

**http**: Somente os pacotes http serão inspecionados;

**audit-trail on**: Habilita o rastreamento dos pacotes para fins de auditoria, neste caso vamos mandar os logs para um servidor de log.

**Etapa 04 - Aplicar as regras de inspeção de pacotes e as ACLs nas interfaces**

**(config)# interface FastEthernet0/0** ! entra no modo da interface

**(config-if)# ip access-group rede_interna in** ! aplica a ACL rede_interna para pacotes que entram na interface

**(config-if)# ip inspect dmz in** ! aplica a inspeção de pacotes DMZ para pacotes que entram na interface

**(config)# interface FastEthernet0/1** ! entra no modo da interface

**(config-if)ip access-group dmz in** ! aplica a ACL dmz para pacotes que entram na interface

**(config)# interface serial0/0/0** ! entra no modo da interface

**(config-if)#ip access-group rede_externa in** ! aplica a ACL rede_externa para pacotes que entram na interface

**(config-if)#ip inspect dmz in** ! aplica a inspeção de pacotes DMZ para pacotes que entram na interface

**Etapa 05 - Configurar o servidor que receberá as mensagens de auditoria**

**(config)# logging on** ! habilita os logs

**(config)# logging 190.16.1.1** ! configura o endereço IP do servidor que receberá os logs

**Etapa 06 - Testar e verificar as configurações aplicadas**

**#show ip access-lists** ! mostra as listas de acessos configuradas e o número de pacotes que foram associados

**#show ip inspect name DMZ** ! mostra as regras de inspeção de pacotes DMZ

**#show ip inspect interfaces** ! mostra as regras de inspeção de pacotes configuradas nas interfaces

**#show ip inspect sessions** ! mostra informações das sessões que estão sendo inspecionadas

**#show ip inspect statistics** ! mostra estatísticas das regras de inspeção de pacotes

Confira todas as informações e estatísticas mostradas pelo roteador e verifique se as regras estabelecidas estão consistentes (as do 1º passo – Definição da política de segurança da DMZ).

13

### 3.2- Falhas na Segurança

Segundo Stallings (2010) alguns ataques são realizados em roteadores de filtragem de pacotes com o objetivo de quebrar a segurança devido à vulnerabilidade de não se ter uma checagem dos dados das camadas superiores.

Os principais **ataques** são:

**1) Falsificação de endereço IP (spoofing)**

Segundo Stallings (2010) esse ataque utiliza de um endereço de IP falsificado para invadir uma rede privada. A ideia é modificar os cabeçalhos dos pacotes vindos de fora, utilizando o mesmo endereço IP de um host interno. Esse procedimento pode invadir sistemas pouco seguros, onde é verificado apenas se o endereço de destinos enviados por hosts internos para ser aceitos. Uma medida segura seria descartar todos os endereços internos que contem interface externa.

**2) Ataque de roteamento da origem (Souce Rounting)**

Segundo Stallings (2010) o ataque faz com que o pacote se desloque da rota correta, fugindo das medidas de segurança, percorrendo outro caminho até chegar ao destino. Apenas na eliminação dos pacotes que usam essa opção seria a medida para solucionar o problema. Segundo Carneiro e Junior (1999) neste tipo de ataque a estação de origem determina a rota que o pacote deve seguir ao ser transmitido pela internet, e tem a finalidade de enviar o pacote por uma rota não esperada até o seu destino fugindo das medidas de segurança. Este tipo de ataque pode ser evitado descartando todos os pacotes que contenham no cabeçalho a opção source route.

**3) Ataque de fragmento pequeno (tyne Fragment)**

Segundo Stallins (2010) “O intruso usa a opção de fragmentação IP para criar fragmentos extremamente pequenos e forçar as informações de cabeçalho TCP em um fragmento em um pacote separado.” A ideia principal é que o roteador permita o acesso do primeiro fragmento e que de permissão para o restante dos fragmentos. Segundo Carneiro e Junior (1999) este tipo de ataque pode ser neutralizado definindo uma regra que o primeiro fragmento de um pacote deve ter uma quantidade mínima predefinida do cabeçalho de transporte.

14

**3.3- Recomendações**

Toda rede possui um acesso para a Internet. Esse acesso deve ser **protegido**. Uma única exposição não reconhecida, como um acesso não protegido, pode comprometer toda a rede corporativa. As necessidades do negócio e o valor da informação mantida na rede da empresa são os fatores que devem determinar a arquitetura da rede e qual solução será implantada.

Vimos aqui como projetar e implementar uma nova topologia para uma rede, de maneira que nela seja incluída uma zona desmilitarizada.


O uso de uma zona desmilitarizada pode melhorar a segurança da rede, mas ela também pode ser restritiva, pois para acessos de fora da rede, nenhum serviço, em teoria, pode ser acessado a não ser aqueles disponibilizados na própria zona.

15

## Resumo

DMZ - Zona Desmilitarizada é um segmento de rede separado das demais redes. Ela serve como uma segurança adicional entre a sua rede (interna) corporativa e a Internet (externa) pública. A DMZ pode ser utilizada, também, para separar determinada máquina, colocando-a fora da proteção de um firewall.

A DMZ é um conceito e não um *software* ou hardware. Consiste em separar, por meio físico e lógico, os setores, departamentos ou estações de uma rede corporativa. Este conceito é largamente utilizado por grandes corporações, governos e bancos.

Geralmente essas companhias possuem como maior valor corporativo as informações, para elas é muito mais caro perder uma base de dados inteira do que um funcionário de renome, afinal, a informação é a alma da empresa.

A função de uma DMZ é separar os serviços externos, como http e ftp da rede local, com minimização dos danos de uma invasão à rede local. Para atingir este objetivo os computadores presentes em uma DMZ não devem conter forma alguma de acesso à rede local.

Uma DMZ fica localizada entre uma rede interna e uma rede externa. Na criação de uma DMZ, acrescenta-se um segmento a mais de rede ou sub-rede que ainda faz parte do sistema por meio de uma terceira porta de interface no firewall. Esta configuração permite que o firewall troque dados com a rede geral e com a máquina isolada usando Network Address Translation (NAT). O firewall não costuma proteger o sistema isolado, permitindo que ele se conecte mais diretamente à Internet.

Uma DMZ pode ser implementada com filtros de rede configurados nas suas bordas, estes filtros são responsáveis por realizar o controle de acesso do que entra e do que sai da DMZ e podem ser do tipo filtro de pacotes, filtragem total de pacotes e de cache como servidores de proxy conhecidos como ALGs (Application Layer Gateway).

16

A filtragem total de pacotes limita o tráfego baseado no destino e na origem dos endereços IPs, portas, flags além de realizar “stateful inspection” uma inspeção de pacotes que permite o armazenamento de dados de cada conexão em uma tabela de sessão, a qual armazena o estado do fluxo de pacotes e serve como ponto de referência para determinar se os pacotes pertencem a uma conexão existente ou se são pacotes de uma fonte não autorizada.

Uma das arquiteturas mais utilizadas são as DMZs que utilizam uma solução de defesa em camadas.

Quanto aos equipamentos para implementação de uma DMZ, podemos utilizar roteadores com sistema operacional que permita funções avançadas de segurança ou servidores utilizando Linux.

As quatro características mais importantes de uma DMZ são:

1 )servidores que precisam ser acessados externamente são posicionados dentro de uma DMZ;

2) é estabelecida entre as zonas insegura e segura;

3) realiza o controle do tráfego do que entra e do que sai da rede;

4) pode conter um ataque sem que o mesmo passe para a rede interna.

Para a configuração da DMZ siga os passos abaixo:

Etapa 01 - Identificar as interfaces internas e externas;

Etapa 02 - Definir as regras de ACLs nas interfaces;

Etapa 03 - Definir as regras de inspeção de pacotes;

Etapa 04 - Aplicar as regras de inspeção de pacotes e as ACLs nas interfaces;

Etapa 05 - Configurar o servidor que receberá as mensagens de auditoria;

Etapa 06 - Testar e verificar as configurações aplicadas.

O uso de uma zona desmilitarizada pode melhorar a segurança da rede, mas ela também pode ser restritiva, pois para acessos de fora da rede, nenhum serviço, em teoria, pode ser acessado senão aqueles disponibilizados na própria zona.

# UNIDADE 4 – CONCEITOS INTRODUTÓRIOS DE SEGURANÇA DE REDES: NAT, PAT, ACL E DMZ

## MÓDULO 4 – BOAS PRÁTICAS EM SEGURANÇA DE REDES

01

## 1 – SEGURANÇA BÁSICA DO ROTEADOR

Sabe-se que o assunto **segurança** é muito amplo e a cada dia surge uma nova maneira de explorar uma vulnerabilidade em uma infinidade de dispositivos. Os autores consagrados e gerentes experientes recomendam como boas práticas em termos de segurança de redes, **nos roteadores**, as ações a seguir.

### 1.1 - Desabilite os serviços desnecessários

Desabilite, no modo de configuração global dos roteadores, os serviços abaixo listados:

*CDP (Cisco Discovery Protocol) - no cdp run*

*Remote configuration - no service config*

*Source Routing - no ip source-route*

*Finger - no service finger*

*Web Server - no ip http server*

*SNMP - no snmp-server*

*BOOTP - no ip boot server*

*TCP services - no service tcp-small-servers*

*UDP services - no service udp-small-servers*

02

**1.2 – Interfaces de roteadores não utilizadas**

Se o roteador tiver interface não utilizada, desative-a administrativamente com o comando *shutdown*. Para **interfaces em uso** configure na forma abaixo:

```
no ip direct-broadcast

no ip mask-reply

no ip proxy-arp
```

**1.3 – Filtre o tráfego**

Filtre todo tráfego, log denials e evitar spoofing.

Bloqueie todo o tráfego desnecessário.

Configure o roteador para que não receba tráfego de rede com IPs privados (RFC 1918). Por exemplo:

```
Access-list 101 deny ip 10.0.0.0 0.255.255.255 any log

Access-list 101 deny ip 172.16.0 0.15.255.255 any log
```

```
Access-list 101 deny ip 192.168.0 0.0.0.255 any log

Interface s0/0

! Aplicação na interface WAN Internet

Ip access-group 101 in
```

03

**1.4 – Registro dos Logs**

Armazene os logs do roteador e utilize uma fonte confiável de hora. Todas ACLs do tipo deny que estão sendo negadas no passo anterior precisam ir para um arquivo de log. Esse arquivo de log conterá todas as alterações de configurações feitas no seu roteador e qualquer erro gerado. Para habilitar e guardar no roteador faça no ambiente de configuração global:

```
Logging on

!Concede ao roteador um buffer de 16KB buffer para armazenar logging

Logging buffered 16384
```

No caso do roteador reinicializar ou ser atacado perderá todos os logs então envie esses logs para um servidor de log. Para tanto, faça:

```
!Endereço IP do servidor Syslog

Logging 1.1.1.1

!Habilita o tempo para exibição dos logs

Service timestamps log datetime localtime show-timezone msec
```

Para assegurar que a hora nesses logs estará sempre atualizada, configure seu roteador de modo que utilize como fonte de tempo o protocolo Network Time Protocol (NTP):

```
!Este é um servidor NTP free baseado em Internet

Ntp server gpstime.trimble.com
```

04

**1.5 - Aplique as senhas no modo privilegiado e nas linhas vty.**

Existem três modos básicos para acessar um roteador:

1. console,
2. aux e
3. vty,

Assegure-se de que todos os três modos tenham senhas aplicadas a eles, conforme abaixo:

```
line con 0
login
password MinhaSenhaComplexa
Exec-timeout 0 0
line aux 0
login
password MinhaSenhaComplexa
Exec-timeout 0 0
!Verifique para ter certeza que você não tem mais do que 4 vty's, pois
!alguns roteadores possuem mais de quatro!
line vty 0 4
login
password MinhaSenhaComplexa
```

Para acessar os modos privilegiados dos roteadores, configure uma senha "*enable password*". Sempre use a "*enable secret*" para encriptar a senha com encriptação MD5, ao invés da "*enable password*". Exemplo: *Enable secret MinhaEnableSecretComplexa.*

05

**1.6 - Utilize senhas complexas, senhas encriptadas e evite ataques a dicionário**

Assegure-se de utilizar senhas longas no seu roteador, porque diminui as chances do roteador aceitar. Para fazer isto, use o comando:

```
!Configura um comprimento mínimo de senha para 6 caracteres
```

```
Security passwords min-length 6
```

Assegure-se que todas as senhas do seu roteador estão encriptadas com, pelo menos, a encriptação básica. Para fazer isto, use o comando:

```
Service password-encryption
```

Evite ataques de dicionário ao dizer ao roteador para aceitar logins a cada segundo somente e bloquear todos os logins para o roteador por 120 segundos se existirem 3 falhas consecutivas dentro de 60 segundos. Para fazer isto, use o comando:

```
login block-for 120 attempts 3 within 60
```

06

**1.7 - Controle o acesso ao seu roteador**

Restrinja os usuários que podem gerenciar seu roteador baseado no seu endereço IP e qual protocolo eles podem usar para fazer isso por acesso remoto. Para restringir o acesso gerenciado pelo endereço IP, faça:

```
!Isto é apenas uma LAN local; você pode fechá-la para um único ip
Access-list 1 permit 192.168.1.0 0.0.0.255
Line vty 0 4
Access-class 1 in
```

**1.8 - Use o SSH para acessar remotamente seus dispositivos**

Não é aconselhável a utilização do Telnet ou do HTTP para gerenciar seus roteadores. **OBRIGATORIAMENTE** mude para o Secure Shell (SSH) todos os gerenciamentos remotos dos seus dispositivos, pois o SSH é encriptado e os outros não.

Para habilitar o SSH faça:

```
!O hostname do  roteador é exigido
Hostname myroteador
!Um nome de domínio é exigido
Ip domain-name mydomain.com
!Geração de chaves de encriptação
Crypto key generate rsa
```

```
Ip ssh timeout 60
Line vty 0 4
Transport input ssh Page 3
```

07

**1.9 - Protocolos de roteamento seguros e serviços opcionais**

Utilize somente protocolo de roteamento que suporte senha encriptada para troca de atualizações de roteamento. Por exemplo, configurar o OSPF para usar senhas encriptadas com segurança:

```
!Em cada interface
ip ospf message-digest-key key# md5 MinhaSenha$OSPF
!No modo de configuração roteador OSPF para cada área
area X authentication message-digest
```

Se usar serviços opcionais, como gerenciamento HTTP baseado em Web ou SNMP, configure o método mais seguro para utilizá-los. Exemplo

**1.10 - Evitar ataques DoS (Denial of Service)**

Um dos comandos auxiliares para evitar ataques DoS é o comando ***no ip directed-broadcast***. IP directed-broadcasts são raramente necessários e são tipicamente explorados para refletir os ataques DoS.

Outra maneira simples de evitar ataques DoS é limitar as taxas de pacotes ICMP. O ICMP pode ser usado para fazer floods na sua rede, causando negação de serviço. Para evitar os floods, aplique os comandos a seguir em **cada interface** do seu roteador.

O exemplo abaixo limita todo ICMP a 20 kb. Aplique os comandos, abaixo listados, em cada interface que está na Internet:

```
access-list 100 permit icmp any any echo-reply
access-list 100 permit icmp any any echo
interface Serial 0/0
rate-limit input access-group 100 20000 8000 8000 conform-action transmit
exceed-action drop
```

Exemplo

Por exemplo, se você está usando o gerenciamento HTTP baseado em Web, altere o HTTP para usar somente senhas encriptadas. Se você for usar o SNMP, use uma senha complexa e a versão 3 do SNMP, que pode encriptar estas senhas.

08

**1.11 - Mantenha seu IOS atualizado**

Similarmente à Microsoft, que disponibiliza patches de atualização de *software*, a Cisco também o faz. Mantenha-se atualizado com os últimos anúncios de segurança da Cisco e aplique os patches em seus roteadores de forma regular quanto possível.

Para visualizar os últimos patches da Cisco para seu dispositivo, acesse o site da **Cisco Security Advisories**.


**SEMPRE EXECUTE** a versão "GD - General Deployment" do Cisco IOS. A versão GD é considerada a mais estável. Ele deverá ter menos bugs e vulnerabilidades de segurança.

09

## 2- Comandos de segurança ACLs

Abaixo estão listados os comandos de segurança ACLs (listas de controle de acesso), mais comuns, que servem de exemplo:

**2.1 - Negar tráfego FTP a partir de uma rede alvo a outra:**

```
Access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
Access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20
Access-list 101 permit ip any any
Interface Ethernet 0
Ip access-group 101 out
```

**2.2 - Negar o tráfego Telnet de uma sub-rede específica:**

```
Access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 23
Access-list 101 permit ip any any
Interface Ethernet 0
Ip access-group 101 out
```

**2.3 – Utilização das ACLs**

Utilize as ACLs:

1) em roteadores de firewall colocados entre as suas redes interna e externa, como a Internet e

2) em um roteador colocado entre duas partes da sua rede para controlar o tráfego que entra ou sai de uma determinada parte da sua rede interna.

Configure as ACLs em roteadores de borda (roteadores situados nas extremidades das suas redes). Isso fornece um buffer muito básico da rede externa ou entre uma área menos controlada da sua própria rede e uma área mais confidencial da sua rede.

10

**2.4 - Configure as ACLs para cada protocolo de rede configurado nas interfaces do roteador de borda**

Os roteadores de borda são os roteadores situados nas extremidades das suas redes.

Você pode configurar as ACLs em uma interface para filtrar o tráfego de entrada, o tráfego de saída ou ambos, dos serviços TCP e UDP, conforme tabela abaixo:

**Serviços, Protocolos e Portas respectivas**

| SERVIÇO | TIPO DA PORTA | Nº DA PORTA |
|---|---|---|
| **FTP**-DATA | TCP | 20 |
| **FTP**-CMDOS | TCP | 21 |
| **TELNET** | TCP | 23 |
| **S**imple **M**ail **T**ransfer **P**rotocol | TCP | 25 |
| **T**erminal **A**ccess **C**ontroller **A**ccess | UDP | 49 |
| **DNS** | TCP e UDP | 53 |
| **T**rivial **FTP** | UDP | 69 |
| **F**inger | TCP | 79 |
| SUN Remote Procedure Call (**RPC**) | UDP | 111 |
| **N**etwork **N**ews **T**ransfer **P**rotocol | TCP | 119 |
| Network Time Protocol | TCP e UDP | 123 |
| **N**ews**S** | TCP | 144 |
| **SNMP** | UDP | 162 |
| **BGP** | TCP | 179 |

| | | |
|---|---|---|
| **RL**ogin | TCP | 513 |
| **RE**xec | TCP | 514 |
| Talk | TCP e UDP | 517 |
| NTalk | TCP e UDP | 518 |
| **O**pen **W**indows | UDP | 2049 |
| **NFS** | UDP | 2049 |
| **X11** | TCP e UDP | 6000 |

**Fonte: CCNA, 2005.**

O Computer Emergency Response Team (**CERT**) recomenda filtrar os serviços listados na tabela abaixo:

**Filtros recomendados pelo CERT.**

| SERVIÇO | TIPO DA PORTA | Nº DA PORTA |
|---|---|---|
| DNS Zone Transfer | TCP e UDP | 53 |
| TFTP Daemon (TFTPD) | UDP | 69 |
| **L**ink - **C**ommonly **U**sed **B**y **I**ntruders | TCP | 87 |
| SUN RPC | TCP e UDP | 111* |
| NFS | UDP | 2049 |
| **BSD** UNIX r commands (rsh, rlogin, and so forth) | TCP | 512 - 514 |
| **L**ine **P**rinter **D**aemon (**LPD**) | TCP | 515 |
| **UNIX-to-UNIX c**opy **p**rogram **d**aemon (uucpd) | TCP | 540 |
| **O**pen **W**indows | TCP e UDP | 2000 |
| **X W**indows | TCP e UDP | 6000+ |

**Fonte: CERT, 2015.**

## 3 – Boas Práticas Recomendadas para Segurança em Roteadores Cisco

O primeiro passo é evitar serviços desnecessários no seu roteador, assim você diminui as possíveis falhas e portas de entrada para usuários maliciosos.

A seguir, os **comandos** para desligar os serviços desnecessários e uma breve explicação de cada comando ou série de comandos:

**a)** Desliga os chamados 'pequenos' serviços (*small services*) de tcp e udp, que apesar de simples, não são necessários na maioria dos roteadores. Esses serviços incluem *echo*, *discard* e *chargen*, entre outros.

```
Roteador# no service tcp-small-servers
Roteador# no service udp-small-servers
```

**b)** Desabilita o servidor *bootp*, que pode ser usado para dar IPs para Workstations através do protocolo bootp. Não é usado na maioria dos roteadores e é recomendável usar um servidor somente para isso.

```
Roteador# no ip bootp server
```

**c)** Desabilita o serviço *finger*, que permite que usuários remotos vejam quem está logado no roteador.

```
Roteador# no service finger
```

**d)** Desativa o servidor de HTTP para configuração do roteador. É recomendável você usar o console para fazer as alterações, evitando possíveis falhas no servidor HTTP comprometer sua rede.

```
Roteador# no ip http server
```



**e)** Desativa o serviço de ident, pouquíssimo confiável hoje na internet, com a proliferação de sistemas pessoais.

```
Roteador# no ip identd
```

**f)** Desativa o servidor de SNMP (Simple Network Management Protocol).

```
Roteador# no snmp-server
```

**g)** Se precisar usar o SNMP, habilite as strings da comunidade (community strings) para palavras difíceis de serem adivinhadas por força bruta com os comandos:

```
Roteador# no snmp community public [Desativa str public]
Roteador# no snmp community private [Desativa str private]
Roteador# snmp community String_Dificil
```

**h)** Desativa o serviço CDP (Cisco Discovery Protocol – Visualiza tudo de todos os equipamentos da marca Cisco).

```
Roteador# no cdp run
```

**i)** Não permite configuração remota da config do root.

```
Roteador# no service config
```

13

**j)** Não permite pacotes com source route habilitado, essencial para evitar ataques do tipo, onde usuários maliciosos mandam pacotes especiais a fim de sniffar a rede.

```
Roteador# no ip source-route
```

**k)** Para cada interface não usada, desabilite a mesma.

```
Roteador# config t
Roteador# int Nome_da_Interface
Roteador# shutdown
```

**l)** Para evitar ataques do tipo 'Smurf'.

```
Roteador# no ip directed-broadcast
```

**m)** Evitar proxy arp, usados em redes Ad-hoc.

```
Roteador# no ip proxy-arp
```

**n)** Permitem login pelo console e execuções de comandos através desse meio.

```
Roteador# line con 0
Roteador# exec-timeout 5 0
Roteador# login
Roteador# transport input telnet
```

14

**o)** Para evitar acessos indevidos habilite as opções abaixo.

```
Roteador# line aux 0
Roteador# no exec
Roteador# exec-timeout 0 10
Roteador# transport input none
```

**p)** Se não usar a linha AUX (Auxiliar), desative-as.

```
Roteador# line vty 0 4
Roteador# exec-timeout 5 0
Roteador# login
Roteador# transport input telnet
```

NOTA: VTY se refere a Virtual TTY, ou seja, a conexão via telnet ao roteador.

**q)** Ative a criptografia MD5 das senhas, para estas não serem gravadas em texto pleno na configuração.

```
Roteador# service password-encryption
```

**r)** Crie e mantenha as senhas bem difíceis de serem abertas.

```
Roteador# enable secret 0 y0uh4v33m4il [Para a senha de enable]
Roteador# line con 0 [Para o console]
Roteador# password r0ut3r-s3cur1ty
Roteador# line aux 0 [Para a AUX]
Roteador# password n0-4c3ss-f0r-y0u!
Roteador# line vty 0 4 [Para acesso via telnet]
Roteador# password 1q2w3e4r5t!Q@W#E$R%T
```

15

**s)** Configura um servidor interno (exemplo: 1.2.3.4) para ser servidor de syslog e habilitar o log para o console de mensagens críticas.

```
Roteador# logging on
Roteador# logging 1.2.3.4
Roteador# logging console critical
Roteador# logging buffered
Roteador# logging trap debugging
Roteador# logging facility local1
```

**t)** Para ter logs consistentes em data, configure o roteador para usar servidores NTP (exemplos: 1.2.3.5 e 1.2.3.6):

```
Roteador# service timestamps log datetime localtime show-timezone
Roteador# clock timezone EST - 3 [Para o Brasil]
Roteador# ntp source Ethernet0/1 [Qualquer int. ethernet]
Roteador# ntp server 1.2.3.5
Roteador# ntp server 1.2.3.6
```

16

## 4 – Exemplos genéricos de controle

Os exemplos a seguir são genéricos, portanto trate-os com prudência, pois para o seu caso particular, pode haver alguma diferença. Os comandos são sempre inseridos no ambiente de configuração global do roteador e interfaces.

**a)** Permitir somente a entrada de pacotes com origem na rede 172.16.0.0:

```
access-list 1 permit 172.16.0.0 0.0.255
```

**b)** Bloquear um host específico com origem na rede 172.16.0.0:

```
access-list 1 deny 172.16.1.30 0.255.255.255
```

**c)** Bloquear a sub-rede 172.16.1.0/24:

```
access-list 1 deny 172.16.1.0 0.0.0.255
```

**d)** Bloquear FTP para a interface Eth0:

```
access-list 101 deny tcp 172.16.1.0 0.0.0.255 192.168.0.0 0.0.255.255 eq 21
access-list 101 deny tcp 172.16.1.0 0.0.0.255 192.168.0.0 0.0.255.255 eq 20
```

**e)** Bloquear tentativas de telnet para fora da rede 192.168.1.0 e permitir os demais tráfegos:

```
access-list 101 deny tcp 192.168.1.0 0.0.0.255 any eq 23
access-list 101 permit ip any any
```

17

**f)** Permitir tráfego da rede externa 172.16.0.0/16:

```
Access-list 1 permit 172.16.0.0 0.0.255.255
Interface Ethernet 0
```

```
Ip access-group 1 out
Interface Ethernet 1
Ip access-group 1 out
```

**g)** Bloquear o tráfego do host 172.16.4.13:

```
Access-list 1 deny 172.16.4.13 0.0.0.0
Access-list 1 permit 0.0.0.0 255.255.255.255
Interface Ethernet 0
Ip access-group 1 out
```

**h)** Bloquear um tráfego da sub-rede 172.16.4.0/24:

```
Access-list 1 deny 172.16.4.0 0.0.0.255
Access-list 1 permit any
Interface Ethernet 0
Ip access-group 1 out
```

**i)** Permitir estabelecer sessões Telnet da rede 192.89.55.0:

```
Access-list 2 permit 192.89.55.0 0.0.0.255
Line vty 0 4
Access-class 2 in
```

18

**j)** Negar tráfego FTP a partir da rede 172.16.4.0/24 para a rede 172.16.3.0/24:

```
Access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
Access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20
Access-list 101 permit ip any any
Interface Ethernet 0
Ip access-group 101 out
```

**k)** Negar o tráfego Telnet da sub-rede 172.16.4.0/24 para a rede 172.16.3.0/24:

```
Access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 23
Access-list 101 permit ip any any
Interface Ethernet 0
Ip access-group 101 out
```

**l)** Limpar a lista 101 para permitir atualização:

```
no access-list 101
```

**m)** Restrições aos endereços de origem dos pacotes que proíbe endereços iguais ao IP interno (spoofing):

```
access-list 101 deny ip <Classe_C_Interno> 0.0.0.255 any log
```

**n)** Proíbe endereços das interfaces do roteador (land attack)

```
access-list 101 deny ip <Endereço_IP_da_S0> 0.0.0.0<Endereço_IP_da_S0>
0.0.0.0 log
access-list 101 deny ip <Endereço_IP_da_S1> 0.0.0.0 <Endereço_IP_da_S1>
0.0.0.0 log
access-list 101 deny ip <Endereço_IP_da_Eth0> 0.0.0.0 <Endereço_IP_da_Eth0>
0.0.0.0 log
```



**o)** Proíbe endereços reservados das redes privativas (RFC-1918):

```
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
```

**p)** Proíbe o endereço de loopback:

```
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
```

**q)** Proíbe o broadcasting (evita ping amplifying - solicitação de mensagem broadcasting):

```
access-list 101 deny ip host 255.255.255.255 any log
```

**r)** Permite conexões iniciadas internamente (TCP ACK=1):

```
access-list 101 permit tcp any any established
```

**s)** Proíbe acesso ao TFTP:

```
access-list 101 deny udp any any eq 69 log
```

**t)** Proíbe acesso ao X-Windows:

```
access-list 101 deny tcp any any range 6000 6005 log
access-list 101 deny udp any any range 6000 6005 log
```

20

**u)** Proíbe o acesso ao SNMP:

```
access-list 101 deny udp any any eq snmp log
access-list 101 deny udp any any eq snmptrap log
```

**v)** Permite o acesso à porta 113/tcp e 113/udp (identd e auth) e faz log. Essas portas são usadas em ataques winoob/winnuke:

```
access-list 101 permit tcp any any eq 113 log
access-list 101 permit udp any any eq 113 log
```

**x)** Permite HTTP apenas para o servidor HTTP:

```
access-list 101 permit tcp any host <Endereco_IP_Serv_WWW> eq www
access-list 101 permit udp any host <Endereco_IP_Serv_WWW> eq 80
```

**y)** Permite SMTP apenas para o servidor de mail:

```
access-list 101 permit tcp any host <Endereco_IP_Serv_SMTP> eq smtp
```

**z)** Permite POP3 apenas para o servidor de POP3, para pedido externo:

```
access-list 101 permit tcp any host <Endereco_IP_Serv_POP3> eq pop3
```

Com essas práticas citadas, encerramos o nosso estudo e os assuntos tratados ao longo do semestre da disciplina Redes de Computadores, em que foi dada ênfase nas configurações dos dispositivos de redes, especificamente os roteadores.

21

## Resumo

Os autores consagrados e gerentes experientes recomendam como boas práticas em termos de segurança de redes, nos roteadores, as ações a seguir:

1 - Desabilite os serviços desnecessários.

CDP (Cisco Discovery Protocol) - no cdp run

Remote configuration - no service config

Source Routing - no ip source-route

Finger - no service finger

Web Server - no ip http server

SNMP - no snmp-server

BOOTP - no ip boot server

TCP services - no service tcp-small-servers

UDP services - no service udp-small-servers

2 – Interfaces de roteadores não utilizadas.

no ip direct-broadcast

no ip mask-reply

no ip proxy-arp

3 – Filtre todo tráfego, log denials e evite spoofing. Bloqueie todo o tráfego desnecessário.

22

4 – Registro dos Logs: armazene os logs do roteador e utilize uma fonte confiável de hora.

5 - Aplique as senhas no modo privilegiado e nas linhas vty.

6 - Utilize senhas complexas e assegure-se que todas as senhas do seu roteador estão encriptadas com, pelo menos, a encriptação básica.

7 - Controle o acesso ao seu roteador.

8 - Use o SSH para acessar remotamente seus dispositivos.

9 - Protocolos de roteamento seguros e serviços opcionais.

!Em cada interface

ip ospf message-digest-key key# md5 MinhaSenha$OSPF

!No modo de configuração roteador OSPF para cada área

area X authentication message-digest

10 - Evite ataques DoS (Denial of Service).

11 - Mantenha seu IOS atualizado.