Captura de pantalla de un celular con letras

Descripción generada automáticamente

**RELATÓRIO DO PROJETO DE SEGURANÇA INFORMÁTICA**

**Miguel Peñaranda Nº2019122**

**Curso Técnico Superior Profissional em Tecnologias e Programação de Sistemas de Informação**

**UNIDADE CURRICULAR:**

Segurança Informática

**DOCENTE:**

Lisandro Marote

**DATA:**

20 de janeiro de 2024

# ÍNDICE

[1. INTRODUÇÃO 5](#_Toc156686427)

[2. DESENVOLVIMENTO 6](#_Toc156686428)

[ Etapa 1 6](#_Toc156686429)

[ Etapa 2 6](#_Toc156686430)

[ Etapa 3 7](#_Toc156686431)

[**Tabela de Endereçamento da Rede** 7](#_Toc156686432)

[ Etapa 4 8](#_Toc156686433)

[ Etapa 5 9](#_Toc156686434)

[ Etapa 6 10](#_Toc156686435)

[ Etapa 7 10](#_Toc156686436)

[ Etapa 8 11](#_Toc156686437)

[ Etapa 9 12](#_Toc156686438)

[ Etapa 10 12](#_Toc156686439)

[ Etapa 11 14](#_Toc156686440)

[**Criar uma ACL que negue todo o tráfego entre as LANs do R1 e do R3** 14](#_Toc156686441)

[**Todo o tráfego da rede local do R3 com destino à porta TCP 80, 443 e DNS deve ser permitido** 15](#_Toc156686442)

[**A Rede do R3 deverá poderá comunicar em FTP para as LAN dos R4 e R6** 15](#_Toc156686443)

[**Qualquer tráfego não especificado deve ser negado** 16](#_Toc156686444)

[ Etapa 12 16](#_Toc156686445)

[**Zona Outside:** 16](#_Toc156686446)

[**Zona Inside:** 17](#_Toc156686447)

[**Zona DMZ:** 17](#_Toc156686448)

[ Etapa 13 19](#_Toc156686449)

[ Etapa 14 19](#_Toc156686450)

[3. CONCLUSÃO 21](#_Toc156686451)

[Ilustração 1 - Topologia da Rede 6](#_Toc156686388)

[Ilustração 2 - Banner Configurado em Todos os Dispositivos de Rede 7](#_Toc156686389)

[Ilustração 3 - Verificação do Funcionamento das Rotas Estáticas 9](#_Toc156686390)

[Ilustração 4 - Verificação do Mínimo de Caracteres nas Senhas 10](#_Toc156686391)

[Ilustração 5 - Enable Secret "cisco12345" 10](#_Toc156686392)

[Ilustração 6 - Utilizador Criado em Todos os Routers e Switchs 10](#_Toc156686393)

[Ilustração 7 - Ligação a um Router desde o PC-A 11](#_Toc156686394)

[Ilustração 8 - Tentativa de Ligação a um Router desde outro PC 11](#_Toc156686395)

[Ilustração 9 - Criação do Servidor RADIUS 12](#_Toc156686396)

[Ilustração 10 - Autenticação através do Servidor RADIUS no R1 13](#_Toc156686397)

[Ilustração 11 - Autenticação através do Servidor RADIUS no R3 13](#_Toc156686398)

[Ilustração 12 - Verificação de que a ACL foi Implementada com Sucesso I 14](#_Toc156686399)

[Ilustração 13 - Verificação de que a ACL foi Implementada com Sucesso II 14](#_Toc156686400)

[Ilustração 14 - Verificação do Tráfego Permitido através da porta TCP 80, 443 e DNS 15](#_Toc156686401)

[Ilustração 15 - Ligação ao Servidor da LAN R4 através de FTP com Sucesso 15](#_Toc156686402)

[Ilustração 16 - Negação de Tráfego não Especificado 16](#_Toc156686403)

[Ilustração 17 - Nenhum Tráfego Iniciado na Zona Outside é Permitido para a Rede Interna 17](#_Toc156686404)

[Ilustração 18 - Ligação do PC-B ao PC-D através de HTTP 18](#_Toc156686405)

[Ilustração 19 - Ligação desde o PC-F ao PC-B através de HTTP 18](#_Toc156686406)

[Ilustração 20 - Nenhum Tráfego é Permitido Entre a Rede Interna e a DMZ 19](#_Toc156686407)

[Ilustração 21 - Verificação do Encaminhamento de Pacotes através do Túnel IPsec desde o R4 20](#_Toc156686408)

[Ilustração 22 - Verificação do Encaminhamento de Pacotes através do Túnel IPsec desde o R6 20](#_Toc156686409)

# AGRADECIMENTOS

Para iniciar, quero agradecer ao docente Lisandro Marote, que fez um grande esforço em nos ensinar o conteúdo necessário para nos adentrar no mundo da segurança informática, sempre estive disposto para esclarecer as nossas dúvidas e para motivar-nos a desenvolver os conhecimentos adquiridos durante as aulas.

# INTRODUÇÃO

No relatório a seguir, será apresentado o nosso projeto proposto pelo professor Lisandro Marote para a disciplina de “Segurança Informática”, que consiste na criação uma topologia de uma rede com 7 routers, 4 switches, 3 servidores e 3 PC’s.

Para dar um breve conceito, a segurança informática é uma peça fundamental na preservação da integridade, confidencialidade e disponibilidade dos dados em ambientes tecnológicos.

Desde modo, o presente relatório aborda uma série de etapas cruciais para fortalecer a segurança de uma infraestrutura de rede, garantindo a proteção dos sistemas e dados envolvidos. Isto é através de etapas como a atribuição de nomes aos equipamentos até a ativação de serviços de segurança avançados, cada etapa contribui para a criação de uma rede robusta e resiliente. Enfim ao abordar aspetos como configuração de IPs, implementação de firewalls e protocolos de segurança, o relatório visa fornecer uma visão abrangente das medidas tomadas para mitigar possíveis ameaças e ataques.

# DESENVOLVIMENTO

## Etapa 1

Na primeira etapa a prioridade foi a atribuição adequada de nomes aos equipamentos. A nomenclatura consistente é uma prática essencial para facilitar a identificação e a manutenção dos dispositivos em uma rede. Nesta etapa, cada dispositivo foi nomeado de forma a refletir sua função e localização na topologia de rede.

Uma imagem com diagrama, file, mapa

Descrição gerada automaticamente

Ilustração 1 - Topologia da Rede

## Etapa 2

A segunda envolveu a configuração de banners nos dispositivos da rede. Por tanto, os banners são mensagens informativas exibidas ao acessar num dispositivo, servindo como uma medida adicional para comunicar políticas de segurança ou informações importantes aos utilizadores.

Esta etapa é muito importante porque promove a transparência ao informar aos utilizadores sobre as políticas de segurança em vigor e atuam como uma camada adicional de dissuasão contra acessos não autorizados.

Uma imagem com texto, captura de ecrã, software, Página web

Descrição gerada automaticamente

Ilustração 2 - Banner Configurado em Todos os Dispositivos de Rede

## Etapa 3

A terceira etapa concentrou-se na configuração dos endereços IP nos dispositivos da rede. Desta forma a atribuição adequada de IPs é essencial para garantir a conectividade e a comunicação eficiente entre os dispositivos.

### **Tabela de Endereçamento da Rede**

| Dispositivo | Interface | Endereço IP | Máscara de Sub-Rede | Gateway padrão |
| --- | --- | --- | --- | --- |
| R1 | Fa0/0 | 192.28.1.1 | 255.255.255.0 | N/D |
| R1 | S0/0/0 | 10.1.1.1 | 255.255.255.252 | N/D |
| R2 | Fa0/0 | 10.3.3.1 | 255.255.255.252 | N/D |
|  | Fa0/1 | 10.6.6.2 | 255.255.255.252 | N/D |
| S0/0/0 | 10.1.1.2 | 255.255.255.252 | N/D |
| S0/0/1 | 10.2.2.2 | 255.255.255.252 | N/D |
| Loopback 0 | 62.48.16.12 | 255.255.255.0 | N/D |
| R3 | Fa0/0 | 192.28.2.1 | 255.255.255.0 | N/D |
| R3 | S0/0/1 | 10.2.2.1 | 255.255.255.252 | N/D |
| R4 | Fa0/0 | 192.28.3.1 | 255.255.255.0 | N/D |
| S0/0/0 | 10.4.4.1 | 255.255.255.252 | N/D |
| R5 | Fa0/0 | 10.3.3.2 | 255.255.255.252 | N/D |
| S0/0/0 | 10.4.4.2 | 255.255.255.252 | N/D |
| S0/0/1 | 10.5.5.2 | 255.255.255.252 | N/D |
| R6 | Fa0/0 | 192.28.4.1 | 255.255.255.0 | N/D |
| S0/0/1 | 10.5.5.1 | 255.255.255.252 | N/D |
| R7 | G0/0 | 172.16.1.1 | 255.255.255.0 | N/D |
| G0/1 | 10.6.6.1 | 255.255.255.252 | N/D |
| G0/2 | 192.28.5.1 | 255.255.255.0 | N/D |
| PC-A | Fa0 | 192.28.1.10 | 255.255.255.0 | 192.28.1.1 |
| PC-B | Fa0 | 172.16.1.10 | 255.255.255.0 | 172.16.1.1 |
| PC-C | Fa0 | 192.28.2.10 | 255.255.255.0 | 192.28.2.1 |
| PC-D | Fa0 | 192.28.3.10 | 255.255.255.0 | 192.28.3.1 |
| PC-E | Fa0 | 192.28.4.10 | 255.255.255.0 | 192.28.4.1 |
| PC-F | Fa0 | 192.28.5.10 | 255.255.255.0 | 192.28.5.1 |

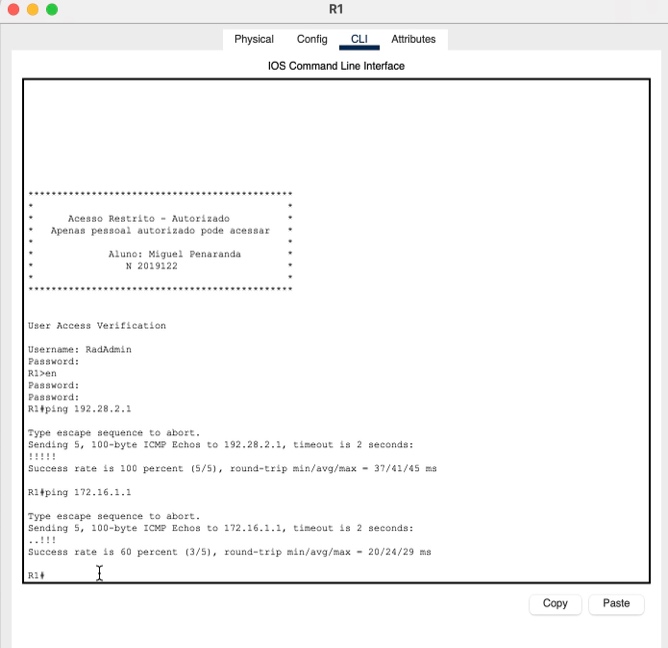
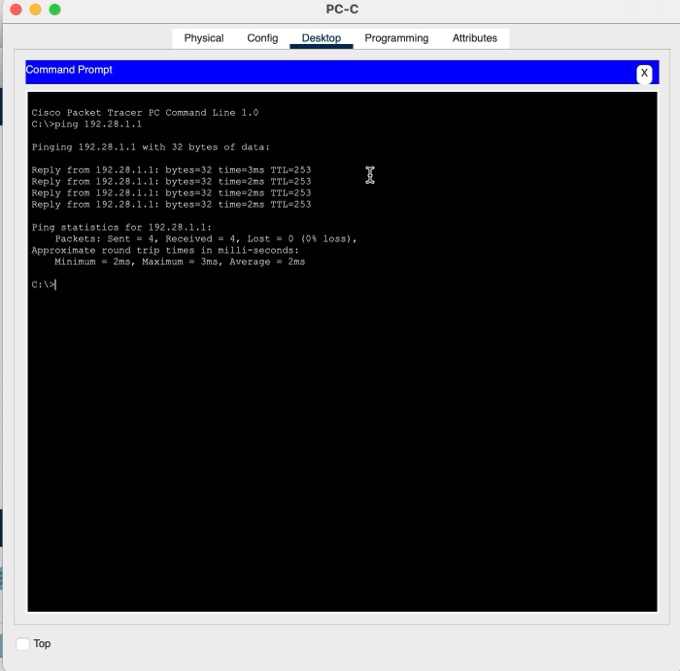
## Etapa 4

Na quarta etapa do projeto de segurança informática, o foco foi na configuração de rotas estáticas nos dispositivos para permitir a comunicação entre eles. Desde modo as rotas estáticas são essenciais para direcionar o tráfego de maneira eficiente, especialmente em redes pequenas ou em cenários específicos.

As razões para a configuração de rotas estáticas são:

* **Direcionamento de Tráfego**: As rotas estáticas indicam aos dispositivos por qual interface ou gateway enviar pacotes de dados para alcançar redes específicas.
* **Estabelecimento de Conectividade**: Permitem a comunicação eficiente entre redes, direcionando o tráfego para o destino apropriado.

Por tanto a configuração de rotas estáticas é crucial para garantir que os dispositivos na rede possam se comunicar eficientemente. Visto que, ao direcionar o tráfego por meio de rotas específicas, estabelecem uma base sólida para futuras implementações de segurança e gerenciamento de rede.



Uma imagem com texto, captura de ecrã, software, Página web

Descrição gerada automaticamente

Ilustração 3 - Verificação do Funcionamento das Rotas Estáticas

## Etapa 5

Na quinta etapa estabeleceu-se a configuração de senhas com um tamanho mínimo de 10 caracteres nos dispositivos da rede. Essa prática é fundamental para fortalecer a segurança, tornando mais difícil para usuários não autorizados comprometerem as credenciais.

Uma imagem com texto, captura de ecrã, documento, Tipo de letra

Descrição gerada automaticamente

Ilustração 4 - Verificação do Mínimo de Caracteres nas Senhas

## Etapa 6

Na sexta etapa realizei a configuração da senha de enable nos dispositivos da rede. A senha de enable é crucial para acessar os modos privilegiados de configuração, garantindo a segurança e o controle de acesso aos recursos críticos do dispositivo.



Ilustração 5 - Enable Secret "cisco12345"

## Etapa 7

Na sétima etapa configurei um utilizador com privilégios 15 em todos os roteadores e switches. Além disso, estabeleci a configuração na linha VTY para permitir acesso remoto via SSH.

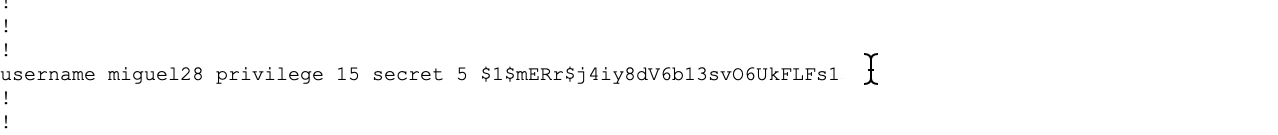


Ilustração 6 - Utilizador Criado em Todos os Routers e Switchs

## Etapa 8

Na oitava etapa do projeto de segurança informática, configurei ACL’s em todos os roteadores para permitir o acesso remoto apenas pelo PC-A. Assim sendo restringido o accesso através do protocolo ssh aos routers apenas para um dispositivo.

Uma imagem com texto, captura de ecrã, software, computador

Descrição gerada automaticamente

Ilustração 7 - Ligação a um Router desde o PC-A

Uma imagem com texto, captura de ecrã, software, Retângulo

Descrição gerada automaticamente

Ilustração 8 - Tentativa de Ligação a um Router desde outro PC

## Etapa 9

Na nona etapa configurei um servidor RADIUS no PC-A e criei um utilizador chamado "RadAdmin" com a senha "RadAdminpa55". O RADIUS (Remote Authentication Dial-In User Service) é um protocolo comumente usado para autenticação, autorização e contabilidade em redes.

Uma imagem com texto, captura de ecrã, software, Ícone de computador

Descrição gerada automaticamente

Ilustração 9 - Criação do Servidor RADIUS

## Etapa 10

Na décima etapa criei um modelo AAA (Autenticação, Autorização e Contabilidade) nos roteadores R1 e R3. Desde modo, o modelo AAA foi configurado com dois métodos de autenticação: o primeiro utilizando o servidor RADIUS no PC-A e o segundo utilizando a base de dados local do roteador.

Por tanto ao criar um modelo AAA nos roteadores R1 e R3 com dois métodos de autenticação, fornecemos redundância e garantimos a disponibilidade contínua da autenticação, mesmo em cenários de falha do servidor RADIUS.

Uma imagem com texto, captura de ecrã, software, Página web

Descrição gerada automaticamente

Ilustração 10 - Autenticação através do Servidor RADIUS no R1

Uma imagem com texto, software, Página web, Ícone de computador

Descrição gerada automaticamente

Ilustração 11 - Autenticação através do Servidor RADIUS no R3

## Etapa 11

Na décima primeira etapa implementei ACL’s para cumprir com as premissas especificadas:

### **Criar uma ACL que negue todo o tráfego entre as LANs do R1 e do R3**

Uma imagem com captura de ecrã, texto, software, Software de multimédia

Descrição gerada automaticamente

Ilustração 12 - Verificação de que a ACL foi Implementada com Sucesso I

Uma imagem com texto, captura de ecrã, software, Software de multimédia

Descrição gerada automaticamente

Ilustração 13 - Verificação de que a ACL foi Implementada com Sucesso II

### **Todo o tráfego da rede local do R3 com destino à porta TCP 80, 443 e DNS deve ser permitido**

Uma imagem com texto, captura de ecrã, software, Página web

Descrição gerada automaticamente

Ilustração 14 - Verificação do Tráfego Permitido através da porta TCP 80, 443 e DNS

### **A Rede do R3 deverá poderá comunicar em FTP para as LAN dos R4 e R6**

Uma imagem com texto, captura de ecrã, software, Página web

Descrição gerada automaticamente

Ilustração 15 - Ligação ao Servidor da LAN R4 através de FTP com Sucesso

### **Qualquer tráfego não especificado deve ser negado**

Uma imagem com texto, eletrónica, captura de ecrã, software

Descrição gerada automaticamente

Ilustração 16 - Negação de Tráfego não Especificado

## Etapa 12

Na décima segunda etapa implementei uma Zone-Based Firewall no roteador R7, dividindo a rede em três zonas distintas: Outside, DMZ e Inside. Deste modo a configuração visa atender a premissas especificadas para garantir a segurança e controlar o tráfego entre as zonas.

### **Zona Outside:**

* Todo tráfego iniciado na zona Outside com destino à rede interna é negado, reforçando a segurança da rede interna.
* Permite o tráfego de retorno da zona Outside para o R7, essencial para receber respostas de solicitações originadas de qualquer rede do R7.

### **Zona Inside:**

* Computadores na rede interna (Inside) têm permissão para iniciar qualquer tipo de tráfego, seja TCP, UDP ou ICMP, reconhecendo-os como confiáveis.
* Implementa uma política rigorosa de segurança ao negar qualquer tráfego direto entre a rede interna e a DMZ.

### **Zona DMZ:**

* Servidores na DMZ têm permissão para iniciar apenas tráfego da Web, limitando-se a HTTP ou HTTPS, contribuindo para um ambiente mais seguro.
* Apenas permite que servidores na DMZ recebam tráfego da Web (HTTP ou HTTPS) proveniente da zona Outside.

Estas configurações de Zone-Based Firewall criam um perímetro robusto de segurança, controlando estritamente o tráfego entre zonas e permitindo apenas as comunicações necessárias para as operações da rede. Por tanto esta abordagem reforça a proteção contra ameaças externas e contribui para um ambiente de rede mais seguro e controlado.

Uma imagem com texto, captura de ecrã, software, Software de multimédia

Descrição gerada automaticamente

Ilustração 17 - Nenhum Tráfego Iniciado na Zona Outside é Permitido para a Rede Interna

Uma imagem com texto, captura de ecrã, software, Página web

Descrição gerada automaticamente

Ilustração 18 - Ligação do PC-B ao PC-D através de HTTP

Uma imagem com texto, captura de ecrã, software, Página web

Descrição gerada automaticamente

Ilustração 19 - Ligação desde o PC-F ao PC-B através de HTTP

Uma imagem com texto, captura de ecrã, software, Página web

Descrição gerada automaticamente

Ilustração 20 - Nenhum Tráfego é Permitido Entre a Rede Interna e a DMZ

## Etapa 13

Na décima terceira etapa implementei a ativação da IPS no Roteador R2 com assinaturas básicas para a rede 10.3.3.0/30 que contribui para a segurança proativa, detectando e mitigando intrusões em tempo real. Além disso, o encaminhamento de logs para o PC-A permite uma análise eficiente das atividades da IPS.

## Etapa 14

Na décima quarta etapa configurei um túnel IPSec entre os roteadores R4 e R6 para estabelecer uma comunicação segura entre as LANs associadas a esses dispositivos.

Por tanto a configuração bem-sucedida do túnel IPSec entre R4 e R6 estabelece uma conexão segura entre as respectivas LANs, garantindo a confidencialidade e integridade dos dados transmitidos.

Uma imagem com texto, captura de ecrã, software, Página web

Descrição gerada automaticamente

Ilustração 21 - Verificação do Encaminhamento de Pacotes através do Túnel IPsec desde o R4

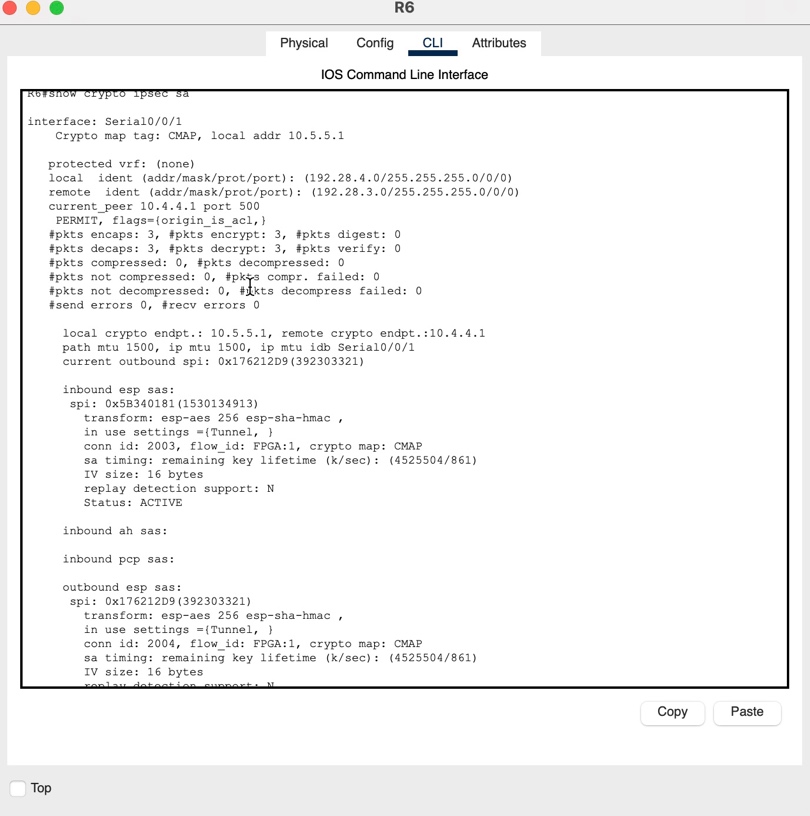


Ilustração 22 - Verificação do Encaminhamento de Pacotes através do Túnel IPsec desde o R6

# CONCLUSÃO

Em suma, durante o processo de desenvolvimento da topologia especificada, tive a oportunidade de me questionar e tomar decisões fundamentadas nos conhecimentos adquiridos na disciplina de Segurança Informática, melhorando assim as minhas habilidades neste âmbito. Deste modo, durante este projeto, consegui aplicar os conceitos e princípios aprendidos na disciplina, utilizando medidas organizadas e eficientes para a proteção dos sistemas de informação.

Para concluir, o propósito de todas estas etapas foi estabelecer uma infraestrutura de rede robusta e segura. Desde a configuração inicial dos equipamentos, a implementação de práticas de segurança em diversos níveis até a ativação de serviços específicos, cada etapa visa fortalecer a integridade, confidencialidade e disponibilidade da rede. Isto é através da implementação de tecnologias como VPNs, firewalls, IPSec, autenticação segura e serviços de segurança do IOS que visam mitigar ameaças potenciais, proteger dados sensíveis e proporcionar uma comunicação eficaz e segura entre os dispositivos da rede. Por fim ao integrar medidas de segurança em todos os níveis, o resultado é um ambiente de rede resiliente que é capaz de enfrentar desafios de segurança de forma proativa.