

Relatório de Suporte Técnico

Nº do Chamado: 005

Data: 06/09/2025

Cliente: Universidade Federal

Tipo de Cliente: Externo

Problema Relatado: Laboratório não acessa sistema acadêmico local

Técnico Responsável: Arthur Gimax

Diagnóstico

O laboratório não conseguia acessar o sistema acadêmico local, provavelmente devido a problemas de rede ou firewall bloqueando a comunicação.

Solução Aplicada

1. Situação Inicial

Durante os testes de conectividade na rede interna do laboratório, foi identificado que os computadores não conseguiam acessar o sistema acadêmico, mesmo estando fisicamente conectados corretamente à rede. A análise inicial indicou que a infraestrutura de rede (cabos, switches, roteadores) estava funcionando adequadamente, mas o problema persistia na comunicação entre os terminais e o servidor responsável pelo sistema acadêmico.

2. Diagnóstico Inicial

2.1 Identificação da Causa

Após a inspeção preliminar, constatamos que o problema não estava na rede física, mas sim na **comunicação entre os computadores e o servidor**. Realizamos uma série de testes de conectividade, como o uso do comando **ping** para verificar se o servidor estava acessível na rede. Os testes indicaram que o servidor estava respondendo ao **ping**, mas o sistema acadêmico não estava disponível.

2.2 Investigação no Firewall do Servidor

Diante dos resultados, focamos nossa investigação nas configurações do **firewall do servidor**, que pode bloquear ou permitir o tráfego de rede com base em regras de segurança. Descobrimos que o **firewall estava configurado para bloquear as portas específicas** utilizadas pelo sistema acadêmico, impedindo que os dados trafegassem corretamente entre os computadores e o servidor.

O firewall do Windows, que é utilizado no servidor, é uma ferramenta de segurança responsável por gerenciar as conexões de entrada e saída de dados, podendo restringir ou permitir o tráfego com base em **regras definidas**. Nesse caso, as regras de segurança estavam mal configuradas, o que causava o bloqueio de portas essenciais para a operação do sistema acadêmico.

3. Resolução do Problema

3.1 Acesso ao Painel de Configuração do Firewall

Para corrigir o problema, acessamos a configuração avançada do **Firewall do Windows Defender**. O procedimento para isso foi o seguinte:

1. Acesso ao Painel de Controle:

- No servidor, abrimos o **Painel de Controle**.
- Navegamos até **Sistema e Segurança > Firewall do Windows Defender**.

2. Configurações Avançadas:

- Dentro da interface do firewall, selecionamos a opção “**Configurações Avançadas**”.
- Nessa seção, é possível configurar as **regras de entrada e saída**, que controlam o tráfego de dados entre o servidor e outros dispositivos da rede.

3.2 Ajuste das Regras de Firewall

● Identificação das Portas do Sistema Acadêmico:

- O sistema acadêmico utiliza **portas específicas** para a comunicação. Essas portas geralmente são informadas pelo fornecedor do sistema ou pela equipe de TI responsável.
- Identificamos as **portas de rede necessárias** para a operação do sistema acadêmico.

● Criação de Exceções no Firewall:

- Ajustamos as **regras de entrada e saída**, criando exceções para **liberar as portas utilizadas** pelo sistema acadêmico.
- Adicionamos regras específicas permitindo o tráfego de dados através dessas portas essenciais.

3.3 Aplicação das Alterações

Após ajustar as regras do firewall, aplicamos as alterações e reiniciamos os **serviços de rede** no servidor para garantir que as novas configurações fossem aplicadas corretamente e que o tráfego de dados fosse liberado sem restrições.

4. Testes de Conectividade e Verificação de Funcionamento

4.1 Testes Realizados

Com as portas liberadas e as regras corrigidas, realizamos uma série de testes para garantir que a solução estivesse funcionando adequadamente:

1. Acesso Direto ao Sistema Acadêmico:

- Verificamos se os computadores conseguiam acessar o sistema acadêmico de maneira normal, sem interrupções ou falhas.

2. Verificação de Resposta do Servidor:

- Utilizamos o comando **ping** para testar a comunicação entre os computadores e o servidor, garantindo que o servidor estivesse acessível e respondendo sem falhas.

3. Simulações de Uso Real:

- Simulamos o uso do sistema acadêmico nas máquinas para verificar se o sistema estava funcionando sem interrupções.
- Verificamos o tráfego de rede e a comunicação com o servidor, para garantir que todos os dados estavam trafegando corretamente.

4.2 Resultados dos Testes

Os testes indicaram que o sistema acadêmico estava **totalmente acessível** e funcional em todas as estações de trabalho do laboratório. A comunicação com o servidor foi restabelecida sem falhas, e o ambiente voltou a operar de forma estável.

- **Acesso ao sistema acadêmico** foi totalmente restabelecido.
- **Comunicação com o servidor** foi verificada e estava sem interrupções.
- Nenhuma **falha de rede** ou bloqueio foi detectado durante os testes.

Recomendações:

- **Revisar periodicamente as configurações do firewall**, para garantir que as portas necessárias para o funcionamento dos sistemas internos estejam sempre liberadas.
- **Manter a documentação** das configurações do firewall atualizada, para facilitar ajustes futuros, caso necessário.
- **Monitorar o tráfego de rede**, para garantir que não haja novas configurações incorretas ou problemas de conectividade.

Resultado Final

As regras de firewall foram corrigidas e as portas necessárias liberadas, restabelecendo a comunicação entre o laboratório e o servidor do sistema acadêmico. Foram feitos testes em todas as máquinas, confirmando acesso pleno ao sistema e funcionamento estável da rede sem bloqueios.

Feedback do Cliente

Avaliação: ★★★★★

Comentário: [sem registro]

Tempo de Resolução

1h e 10min

Situação Final

Resolvido

PROBLEMA DE ACESSO – SISTEMA ACADÊMICO

DIAGNÓSTICO



Laboratório
sem acesso



Firewall
suspeito

SOLUÇÃO APLICADA



Acesso ao firewall



Liberar
portas

TESTES DE VERIFICAÇÃO



Ping



Simulação
de uso real

RUSTUDES OBTIDOS



Semulação
de uso real



Tráfego
estável

RESULTADOS OBTIDOS



Sistema acessível
em todas as máquinas
Rede estável

CAUSA PROVÁVEL



Regras incorretas
do firewall
bloqueando portas



Monitorar
rede

CONCLUSÃO

