Guia de Orientação: Como Abrir Chamados para a Equipe de Firewall

1. Objetivo

Este guia foi criado para auxiliar todos os colaboradores, mesmo aqueles sem conhecimento técnico profundo em redes, a solicitar acessos ou bloqueios através do nosso Firewall de maneira rápida e eficiente.

2. O que é um Firewall?

Imagine o firewall como um segurança na porta de um prédio corporativo. Para permitir que alguém entre (ou saia), o segurança precisa saber exatamente quem está tentando entrar, para onde essa pessoa vai dentro do prédio e por qual porta ela deve passar. Se faltar alguma dessas informações, a entrada será negada por precaução. Na rede da empresa, o processo é o mesmo.

3. Informações Obrigatórias para Abrir um Chamado

Para que a equipe de Firewall possa atender sua solicitação no menor tempo possível e sem precisar devolver o chamado pedindo mais informações, você sempre deve fornecer os itens abaixo. A ausência destas informações poderá resultar na devolução do chamado.

- Endereço de Origem (Quem está tentando acessar?): De onde o acesso está saindo? Pode ser o endereço IP do seu computador, de um servidor ou de uma rede inteira. (Exemplo: Meu computador no IP 192.168.1.50).
- Endereço de Destino (Onde você quer chegar?): Para onde o acesso precisa ir? Onde está o sistema, site ou serviço que você quer acessar? (Exemplo: Servidor da Aplicação no IP 10.0.0.100 ou o site www.exemplo.com).
- Portas Necessárias (Por qual porta vai passar?): Qual o "canal" técnico de comunicação que será utilizado para esse acesso? Sem essa informação, o firewall não sabe qual

serviço autorizar. Veja nosso glossário abaixo para referência.
- Motivo da Solicitação / Justificativa do Negócio (Por que o acesso é necessário?): É obrigatório descrever o motivo. Por que esse acesso é necessário para o seu trabalho? (Exemplo: Necessidade de acessar o sistema do RH para liberação da folha de pagamento).
- Print / Captura de Tela do Erro: Você deve anexar ao chamado uma imagem (print) mostrando exatamente o erro que está aparecendo na sua tela ao tentar o acesso. Isso ajuda a equipe a confirmar se é um bloqueio de rede ou erro na própria aplicação.

3.1. Como testar a liberação usando o comando TNC no PowerShell (Validação Prévia)

Antes de abrir o chamado, você deve testar se o firewall realmente está bloqueando a comunicação. No Windows, usamos a ferramenta Test-NetConnection (TNC) via PowerShell. Siga o passo a passo:

1. Abra o Menu Iniciar do Windows, digite powershell e clique no aplicativo "Windows PowerShell" (uma tela azul irá se abrir).
2. Digite o comando seguindo esta estrutura: tnc [IP_DE_DESTINO] -port [PORTA] e aperte Enter.
3. Exemplo prático: Se você quer testar a porta 3306 para o IP 10.0.0.50, digite: tnc 10.0.0.50 -port 3306
4. Aguarde alguns segundos enquanto o Windows realiza o teste de comunicação.
5. Observe o resultado na última linha, chamada TcpTestSucceeded:

- Se aparecer True: O firewall não está bloqueando essa porta. A rede está livre. Se você não consegue acessar o sistema, o problema provavelmente é senha incorreta, o serviço lá no destino está travado/desligado, ou falta de permissão no próprio sistema.
- Se aparecer False: A comunicação não está chegando lá. O firewall pode estar bloqueando, ou o servidor destino pode estar completamente fora do ar. Tire um print dessa tela preta com o erro "False" e anexe no seu chamado de firewall!

4. Glossário de Portas de Comunicação Mais Comuns

Abaixo estão as portas mais comuns que você pode precisar mencionar em seu chamado:

Número da Porta	Nome / Protocolo	Para que serve (Exemplo prático de uso)

80	HTTP	Acessar páginas de internet comuns ou sistemas web internos (sem criptografia).
443	HTTPS	Acessar sites seguros na internet ou sistemas (páginas com o cadeado de segurança).
445	SMB / CIFS	Acesso a Servidores de Arquivos: pastas e arquivos compartilhados na rede do Windows.
3389	RDP	Acesso Remoto do Windows (usado para ver e controlar a tela de outro computador à distância).
22	SSH	Acesso remoto seguro a servidores (geralmente tela preta/terminal usado em Linux).
1433	SQL Server	Conexão direta com Banco de Dados Microsoft SQL (muito usado por sistemas de gestão/ERP).
1521	Oracle DB	Conexão com Banco de Dados Oracle.
3306	MySQL / MariaDB	Conexão com Banco de Dados MySQL ou MariaDB (muito usado em aplicações web e sites).
21	FTP	Transferência de arquivos tradicionais pela rede.

5. Exemplos Práticos de Chamados

? Exemplo Ruim (O que NÃO fazer)

"Oi, o sistema de notas não está funcionando na minha máquina, acho que é o firewall bloqueando. Por favor, liberem para mim o mais rápido possível."

Por que está ruim? Falta o IP de origem, IP de destino, porta necessária, motivo detalhado, e nenhum print do erro ou validação do TNC foi enviada. O chamado será devolvido.

? Exemplo Bom (O modelo ideal)

"Olá equipe, preciso de liberação no firewall para que eu consiga acessar o novo banco de dados. Seguem os dados:

Origem:
- Servidor Web (IP 192.168.1.150)

Destino:
- Servidor de Banco de Dados (IP 10.0.0.50)

Portas:
- 3306 (MySQL), ICMP (ping)

- Motivo da Solicitação: O servidor web precisa conectar ao novo banco de dados para que o portal de clientes possa listar as faturas recentes."

- Anexo: Segue o print da tela do sistema com o erro e o print do PowerShell (TNC) retornando 'TcpTestSucceeded: False'."

6. Dicas Úteis

- Como descubro meu IP (Origem)? Se estiver usando Windows, digite cmd no Menu Iniciar para abrir o Prompt de Comando. Digite o comando ipconfig e pressione Enter. Procure pela linha "Endereço IPv4". Se precisar de ajuda, acione o Suporte Local / Help Desk.
- Como descubro o IP e Porta do sistema (Destino)? Se for um sistema novo ou desconhecido, consulte o fornecedor do software ou a equipe de desenvolvimento/infraestrutura que gerencia esse sistema. Eles são obrigados a fornecer os requisitos de rede (IPs e portas) para o funcionamento.

Documentação para Usuários Finais - Equipe de Segurança e Redes

---

Revision #5
Created 28 April 2026 11:49:01 by Marcos Luciano Carrilho
Updated 30 April 2026 19:21:56 by Marcos Luciano Carrilho