

Boas práticas de segurança em redes para o uso de TR-069 através de HTTP

1. **Termos definidos.** As palavras, expressões e abreviações com as letras iniciais maiúsculas, não definidas em outras partes deste documento, no singular ou no plural, terão o significado atribuído a elas nesta cláusula, exceto se expressamente indicado de outra forma:
 - 1.1. *Provedor:* É a beneficiária dos *softwares* oferecidos como serviço pela Anlix, que necessariamente será uma pessoa jurídica de fornecimento de Serviço de Valor Adicionado de Internet, conforme art. 61, parágrafo 1º da Lei Geral de Telecomunicações.
 - 1.2. *Rede Local:* É a rede de computadores e equipamentos sob responsabilidade e controle do Provedor.
 - 1.3. *IP:* Identificador único de um equipamento eletrônico ao conectar-se em uma rede de computadores, como a Rede Local a internet.
 - 1.4. *Usuário:* Pessoa natural ou jurídica que contrata, do Provedor, os serviços providos por ele.
 - 1.5. *CPE:* Equipamento eletrônico localizado nas residências ou estabelecimentos de Usuários do Provedor e responsáveis pelo fornecimento de internet banda larga ao Usuário.
 - 1.6. *TR-069:* Protocolo de comunicação entre equipamentos capazes de conexão à Rede Local, destinado a emissão de comandos remotos para CPEs com o objetivo de controlar funcionalidades e configurações das CPEs.
 - 1.7. *ACS:* *Software* responsável por enviar e receber comandos remotamente para CPEs através do protocolo TR-069.
 - 1.8. *PPPoE:* Protocolo de comunicação entre equipamentos capazes de conexão à Rede Local ou internet, destinado a autenticar o acesso desses equipamentos à Rede Local do Provedor.
 - 1.9. *VLAN:* Conceito bem estabelecido em redes de computadores que consiste na possibilidade de criar Redes Locais virtuais, compartilhando a mesma Rede Local real.
 - 1.10. *HTTP:* Protocolo de comunicação entre dois computadores conectados a uma Rede Local ou conectados à internet, com o objetivo de estruturar o envio e recebimento de documentos de hipertexto.

- 1.11. *Porta*: Conceito bem estabelecido em redes de computadores que consiste em identificadores com numeração de 0 a 65535 e destinados a organizar o recebimento e envio de dados para *softwares* em execução em computadores.
2. **Objeto.** Este documento tem por objeto recomendar ações necessárias para garantir a segurança cibernética relacionada ao uso do protocolo TR-069 em equipamentos eletrônicos conectados à rede do Provedor.
 - 2.1. As recomendações indicadas neste documento não garantem a segurança cibernética irrestrita e ilimitada de equipamentos eletrônicos conectados à rede do Provedor.
 - 2.2. As recomendações indicadas neste documento garantem somente a segurança cibernética decorrente de possíveis vulnerabilidades de segurança cibernética relacionadas ao uso do protocolo TR-069 através do protocolo HTTP por equipamentos eletrônicos conectados à rede do Provedor.
3. **Recomendações.** As recomendações expostas nesta cláusula referem-se à Rede Local e IPs sob o controle e/ou utilização do Provedor.
 - 3.1. Toda a comunicação entre CPEs e o ACS deve estar contida na Rede Local do Provedor.
 - 3.1.1. Motivo: Prevenir toda e qualquer tentativa de comunicação utilizando o protocolo TR-069 oriunda ou destinada à IPs não pertencentes à Rede Local do Provedor. Este bloqueio previne situações de tentativa de injeção de comandos no CPE através do protocolo TR-069 e tentativas de redirecionamento ou redefinição do servidor ACS configurado em cada CPE do Provedor.
 - 3.2. A comunicação entre CPEs através dos IPs da Rede Local do Provedor deve ser bloqueada.
 - 3.2.1. Motivo: Prevenir o envio de comandos através do protocolo TR-069 originados a partir de IPs da Rede Local do Provedor e destinados para CPEs da mesma Rede Local.
4. **Sugestões de abordagem para recomendações indicadas.** As sugestões expostas nesta cláusula não são exaustivas. Determinadas situações e cenários de cada Provedor podem sugerir abordagens não expostas aqui.
 - 4.1. Uso do PPPoE como protocolo de acesso para as CPEs do Provedor.
 - 4.1.1. O uso de conexões ponto-a-ponto por PPPoE irá isolar o tráfego de pacotes entre a CPE e o servidor autenticador PPPoE, impossibilitando o envio de comandos entre IPs locais, conforme recomendado no item 3.2.
 - 4.2. Uso de VLAN exclusiva para a comunicação entre CPEs e ACS através do protocolo TR-069 (VLAN de gerência).
 - 4.2.1. Atende ao recomendado no item 3.2.
 - 4.3. Uso de filtro de pacotes em equipamentos do Provedor responsáveis por concentrar o fluxo de dados de cada CPE. Os filtros devem ser capazes de remover pacotes destinados a IPs da Rede Local de cada CPE.

- 4.3.1. Atende ao recomendado no item 3.2.
- 4.4. Criação de redes virtuais privadas (VPN) ponto-a-ponto entre Redes Locais separadas.
 - 4.4.1. Para Provedores que utilizam múltiplas Redes Locais é indicado a criação de redes virtuais privadas (VPN) interconectando as Redes Locais e evitando o envio de dados relativos ao TR-069 através da internet. Atende ao recomendado no item 3.1.
- 4.5. Criação de filtro de saída da Rede Local pertencente ao Provedor para a internet, filtrando pacotes destinados à Porta de comunicação utilizada pelo ACS.
 - 4.5.1. Porta utilizada para comunicação por HTTP: 57547
 - 4.5.2. Atende ao recomendado no item 3.1.
- 4.6. Criação de filtro de entrada para Portas efêmeras da Rede Local pertencente ao Provedor com pacotes destinados a IPs públicos do mesmo.
 - 4.6.1. As Portas efêmeras são Portas com numeração acima de 1024 e até 65535.
 - 4.6.2. Atende ao recomendado no item 3.1.