APÊNDICE VII – Arquitetura de Integração com a Companhia de Processamento de Dados de Porto Alegre - PROCEMPA

REDUTOR ELETRÔNICO DE VELOCIDADE (REV)

LOMBADA ELETRÔNICA

Documento de especificação técnica

1. Introdução

Esse documento descreve a especificação técnica de integração entre o sistema de monitoramento da contratada e a Companhia de Processamento de dados da Prefeitura de Porto Alegre - Procempa. São cobertos nesse documento requisitos de segurança das informações, especificações de comunicação (rede) e câmeras, bem como as formas possíveis de integração com os serviços disponíveis no sistema.

2. Premissas de Projeto

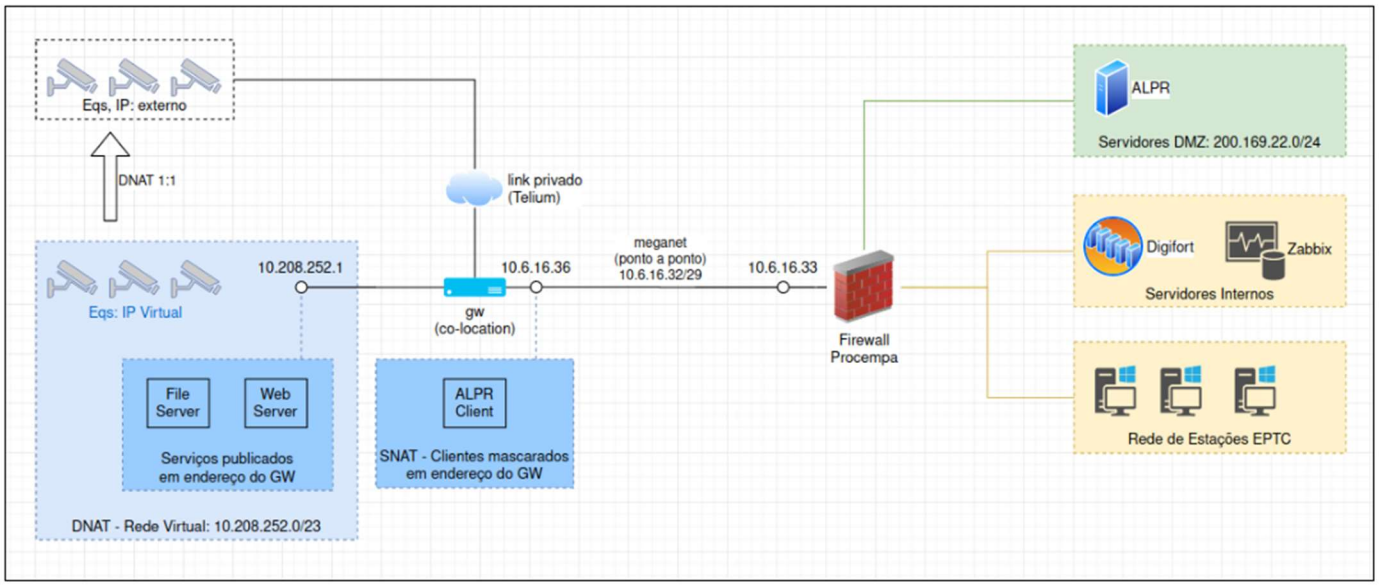
A organização utilizada nesse provisionamento tem por base as seguintes premissas:

a) que a CONTRATADA tenha completa autonomia sobre a tecnologia empregada para conectividade das câmeras dentro de sua infraestrutura, respeitados os parâmetros de disponibilidade e segurança definidos em contrato com a EPTC, não estando, em particular, obrigada a utilizar serviços da PROCEMPA para essa finalidade;
b) que a CONTRATADA deve, para finalidade de integração aos sistemas da PMPA, possuir ponto de presença dentro do Datacenter da Procempa, na forma de um gateway (lógico) que mediará a integração entre os equipamentos dentro de sua infraestrutura (recursos remotos) e os serviços da PMPA, hospedados no Datacenter da Procempa;
c) que o tráfego dessa integração CONTRATADA-PMPA deverá ocorrer através de link dedicado e com dimensionamento apropriado, provisionado dentro do Datacenter para essa finalidade pela PROCEMPA e às custas da CONTRATADA, não podendo, em particular, ocorrer essa integração através do link de Internet padrão da PMPA;
d) assegurar a integridade e disponibilidade do ambiente de rede da PMPA e dos serviços hospedados no datacenter da Procempa, mitigando o risco de incidentes propagados a partir da rede da CONTRATADA.

3. Arquitetura da Implantação

A figura a seguir apresenta o diagrama de arquitetura de implantação existente, podendo ser utilizada como referência para implantações futuras de outros fornecedores do mesmo tipo de

serviço, salvo pelas faixas de endereço IP utilizadas, que precisarão serem ajustadas, pois são particulares à cada implantação.



Os principais elementos dessa arquitetura, de suas dinâmicas de implantação e funcionamento, em linhas gerais, são os seguintes:

a) O elemento **gw** corresponde ao equipamento gateway da CONTRATADA, provisionado fisicamente em regime de co-location no datacenter da PROCEMPA. O equipamento a ser utilizado deve possuir ao menos duas interfaces físicas, uma para conexão com o link privado da CONTRATADA e outra para integração via MEGANET à PROCEMPA. Em termos de funcionalidade, ele deve possuir capacidade de firewall/roteamento e de implementação de políticas de tradução de endereços via DNAT/SNAT. A título de referência, uma possível implementação para esse equipamento consiste em usar um servidor de rack rodando o **pfSense**, mas outros tipos de appliance também podem ser utilizados. Havendo interesse em aproveitar o mesmo equipamento para hospedar outros componentes (ex. Web Server, File Server, ALPR Client), pode ser conveniente utilizar-se um servidor físico com máquinas virtuais para cada um dos demais serviços.
b) A integração lógica à rede da PROCEMPA ocorre através de uma VLAN ponto a ponto UNTAGGED entre o equipamento da CONTRATADA e um firewall dentro da infraestrutura da PROCEMPA (link **MEGANET**). Para esse link é alocado um range de IPs no padrão

10.6.X.Y/29, sendo que os 3 endereços mais baixos desse range são reservados para o firewall da PROCEMPA, destes o IP mais baixo é o VIP do cluster de firewall (no caso da figura, o VIP é 10.6.16.33). Os 3 endereços IP seguintes estão alocados para uso pela CONTRATADA, sendo, novamente, o endereço mais baixo definido como VIP (no caso 10.6.16.36). Quaisquer outros endereços estão reservados e não devem ser utilizados sem alinhamento prévio com a PROCEMPA.

c) Os dispositivos e serviços disponibilizados pela CONTRATADA são acessados sempre através de IPs virtuais, e nunca através de seu endereço IP real. Para isso é alocado pela PROCEMPA um range de IPs no padrão 10.208.X.0/23, sendo que o IP mais baixo dessa faixa deve ser reservado para o gateway (gw) da CONTRATADA. É responsabilidade do gateway implementar regras de tradução de endereço via DNAT para viabilizar acesso às cameras e demais serviços dos IPs virtuais.
d) Referente às câmeras, deve ser utilizada obrigatoriamente uma estratégia de tradução DNAT 1:1, ou seja, um endereço virtual por dispositivo físico. Os demais serviços, tais como File Server e Web Server, quando oferecidos pela CONTRATADA, devem ser multiplexados via DNAT de porta todos sobre mesmo o VIP do GW na rede virtual, independente de estarem hospedados no mesmo equipamento do gateway, ou em algum outro servidor interno ou VM da na infraestrutura da CONTRATADA. No caso da figura, os serviços de File Server e Web Server estão publicados no IP 10.208.252.1.
e) Caso exista a previsão de integração com a API do sistema ALPR, a CONTRATADA poderá redirecionar o tráfego destinado à rede 200.169.22.0/24 (DMZ) através do link MEGANET dessa instalação, usando o VIP do Firewall da Procempa como gateway, e realizando tradução da origem (SNAT) antes que tal tráfego entre no link MEGANET. Não há necessidade de configuração de outras rotas e nenhum outro tráfego iniciado do lado da CONTRATADA será permitido através desse link.
f) Os acessos realizados a partir da PMPA para recursos na rede de IPs Virtuais da CONTRATADA terão a origem mascarada no firewall da PROCEMPA utilizando o endereço VIP do firewall no link MEGANET. Ou seja, não deve ser esperado que o equipamento da CONTRATADA tenha visibilidade sobre o IP de origem dos acessos para implementação de controle de acesso. A CONTRATADA deve, para isso, empregar controles na camada de aplicação (ex. autenticação por usuário). Por exemplo, no caso ilustrado na figura, é utilizado o endereço 10.6.16.33 para todos os acessos provenientes de clientes na rede da PMPA (sejam estações de trabalho ou servidores do DIGIFORT). Sugere-se liberar no firewall da CONTRATADA os endereços do /29 por simplicidade.
g) Em particular, destaca-se que a CONTRATADA não terá visibilidade direta nem dos IPs do Digifort e nem dos IPs da rede da EPTC. O controle das redes PMPA autorizadas a chegarem até gateway e IPs virtuais de cameras é implementado no firewall da PROCEMPA.

h) Após definir o mapeamento 1:1 entre IPs virtuais e câmeras, a CONTRATADA deverá informar este mapeamento à EPTC, vinculando o endereço IP virtual à identificação do equipamento e localidade onde encontra-se instalado, para finalidade de cadastro dos equipamentos no DIGIFORT através dos endereços virtuais. As portas liberadas para integração das câmeras ao DIGIFORT são 80, 443 e 554, para os protocolos de transporte TCP e UDP. Uma limitação do componente do lado do DIGIFORT não permite utilizar outras portas, sendo que, em particular, não é possível multiplexar câmeras em um ínico IP virtual usando-se portas distintas.
i) A gateway deve responder a ICMP direcionado tanto para seu IP no link MEGANET (10.6.16.36 no caso da figura) quanto para para seu IP no range de endereços virtuais (10.208.252.1 no caso da figura) para pacotes originados a partir do IP MEGANET do firewall da PROCEMPA, de forma a permitir a monitoria de disponibilidade do gateway e facilitar a depuração de problemas de rede.
j) O gerenciamento do gateway pela CONTRATADA ocorrerá através do link privado por ela contratado, não havendo, em nenhuma hipótese atribuição de IP público (roteável) no range da PROCEMPA ao equipamento da CONTRATADA no link MEGANET ou em qualquer outra interface. Em casos excepcionais, e mediante alinhamento prévio com a PROCEMPA, poderá ser disponibilizada credencial para acesso via VPN.

Responsabilidades das Partes

É de responsabilidade da CONTRATADA:

a) definir se utilizará, ou não, equipamentos redundantes para o gateway e para conectividade deste para com sua infraestrutura remota;
b) garantir a conectividade entre o gateway e as câmeras através do link privado contratado;
c) empregar estratégias de conectividade às câmeras que sejam adequadas aos níveis de proteção de dados definidos pela EPTC, de forma a mitigar o risco de interceptação por quaisquer agentes não autorizados;
d) zelar pela proteção das imagens e implementar controles de segurança apropriados de forma a prevenir risco de acesso direto às câmeras por pessoas não autorizadas, em consonância com política de acesso às imagens estabelecida pela EPTC, em particular no que se refere ao acesso a partir da Internet; e
e) implementar controle de acesso na camada de aplicação para os serviços expostos através do gateway para clientes na rede da PMPA autorizados pela EPTC, mantendo os logs de auditoria de acesso pertinentes.

É de responsabilidade da EPTC:

a) estabelecer os níveis de proteção de dados aceitáveis para o transporte de imagens na infraestrutura da CONTRATADA, assim como definir a política de acesso às imagens das câmeras (quem poderá ter acesso, quando e através de quais meios);
b) exigir evidências, no momento da homologação da contratação, de que as estratégias adotadas pela CONTRATADA dentro de sua infraestrutura são adequadas em termos de privacidade e segurança, assim como auditar posteriormente estas evidências para garantir a manutenção do nível de serviço acordado, podendo, onde considerar oportuno, demandar à PROCEMPA, na forma de horas de consultoria, auxílio na revisão de evidências e definição de parâmetros de tecnologia;
c) formalizar à PROCEMPA, através deste SEI, a política de acesso ao gateway da CONTRATADA a partir de clientes na rede da PMPA, assim como alterações futuras dessa política, para parametrização do firewall de borda; e
d) definir um fluxo de resposta a incidentes de segurança da informação nesta infraestrutura, comunicando-o à CONTRATADA e à PROCEMPA, que contemple ao menos a definição de um contato formal para notificação/acionamento em caso de suspeita de incidente detectado por alguma das partes.

É de responsabilidade da PROCEMPA:

a) garantir a conectividade interna no datacenter, entre os serviços na rede da PMPA e o gateway da CONTRATADA;
b) implementar políticas de firewall para controle de acesso, em camada 3 (rede/IP), ao gateway da CONTRATADA a partir da rede interna da PMPA, conforme diretrizes definidas pela EPTC, bloqueando o acesso a partir de quaisquer redes origem que não tenham sido estritamente autorizadas pela EPTC; e
c) notificar a EPTC sobre quaisquer anomalias que por ventura venham a ser detectadas entre a rede interna e o gateway da CONTRATADA.