金融城域网网络替代方案

项目背景与需求目标

背景:

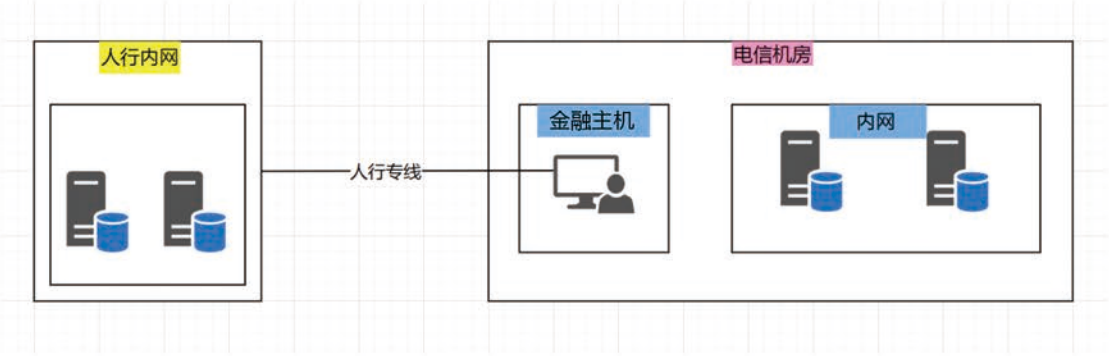
金融业务场景下，在保障安全和合规的前提下，实现指定主机到银行专线网络互联互通

目标

实现稳定安全高效的网络连接，以满足业务需要

当前网络拓扑

当前网络拓扑为，金融主机使用 easyconnect 通过专线拨号连接到人行内网，其他主机无法连接，该主机操作系统为 windows 10.



需求分析

链路层

当前人行至电信机房的专线链路已就绪，负责连接人行内网到电信机房.

专线应当满足不同主机的访问需求，尤其是网关及其下属设备.

网关架设

1. 部署专用的核心网关，以替代金融主机
2. 网关应当满足并配置相关的路由规则，以确保下联主机能通过 SNAT 通过专线访问人行内网.
3. 网关应当采用冗余或热备部署，确保在极端情况下宕机后，在可接受的时间内自动切换.

安全策略

1. 链路层通过 vlan 来实现逻辑隔离，只允许指定的主机到人行网络的链路层可达.
2. 网关上配置 ACL 及 NAT 策略，确保只允许指定的主机到人行网络在网络层可达.

流量审计

1. 在网关上开启流量日志记录，以保存每个终端到人行内网的访问日志.
2. 部署监控系统，以实时分析监控终端到人行内网的访问情况.
3. 定期报表生成，以供运维及安全团队进行分析和审查.

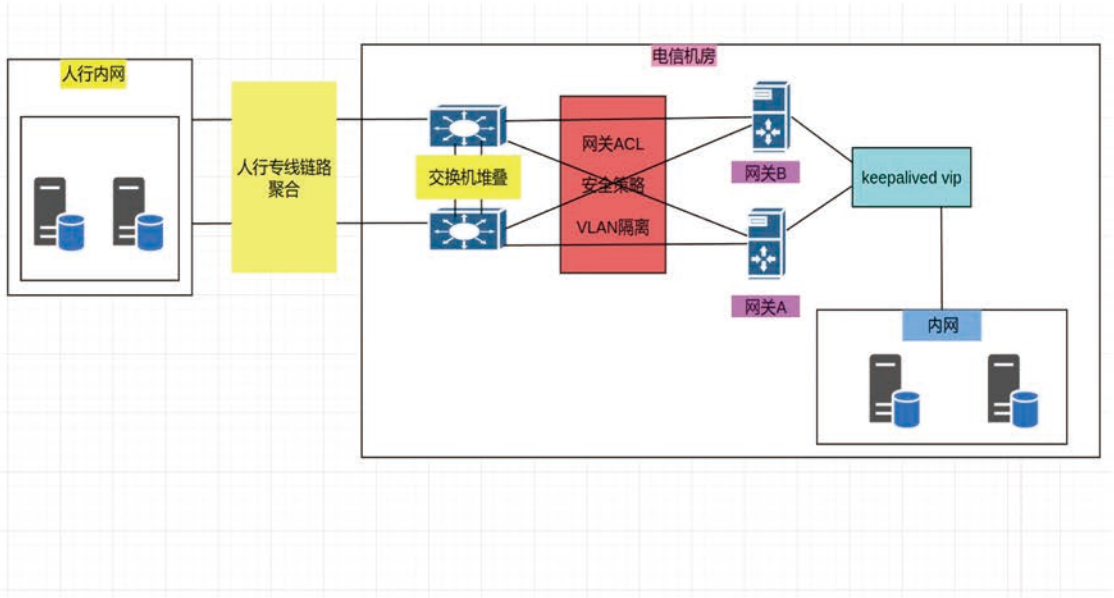
高可用设计

1. 链路冗余，从人行过来的光纤，下联网络设备，及网关到下联主机，应当采用堆叠及链路聚合来保证链路层的高可用.
2. 设备冗余，网关及关键设备使用双机热备或负载均衡，尽可能的防止和避免单点故障.
3. 网关采用 keeplived vip 来实现故障时, ip 自动漂移，保证业务的高可用.

容灾演练

1. 定期进行容灾演练，检查和考验网络架构在极端情况下的可靠性

方案网络拓扑



实施阶段

1. 物理链路及网络设备部署
2. 网关及安全策略部署
3. 流量审计部署
4. 高可用性测试