MONDRIAN: Comprehensive Inter-domain Network Zoning Architecture

NDSS ‘21

背景：企业网络管理

大型企业分布在不同地域，同一地域可能还有众多分支机构（银行）

- 区域内功能相似
- 共享同一安全级别
- 进入区域有统一的入口点

每个区域都关联一定的安全级别

- 为了实现基于安全级别的访问控制，需要FW、UTM等
- 网络的建模和管理还是麻烦，这么多中间设备配置得过来吗

通过Internet进行跨部门、跨区域通信

- 可以用IPSec、TLS-VPN确保机密性完整性
- 但是如何管理成规模的VPN？要知道四个机构互联就需要6条VPN
- VPN与其他安全设施的兼容性
- 如何与其他（公司外的）合作伙伴共享VPN？

MONDRIAN*的提出

Mondrian是一种全新的网络分区架构

- 可以确保第三层上运行的区域间通信的安全
- 支持异构第二层体系结构（以太网、Wireless WAN、PPP、ATM等）
- 可扩展的加密密钥管理和灵活的安全策略实施

主要思路

- Mondrian讲当前分层复杂的网络区域拓扑扁平化为一组水平区域。这些区域连接到一个一的安全网关，称为区域转换点（TP，(Zone) Translation Point），简化网络拓扑
- 通过TPs互连区域，TP通过充当网络区域的安全入口/出口点
- TPs的控制器逻辑上集中

*听起来像个德意志名字，其实人家是个荷兰画家

调研：典型企业网络存在的问题

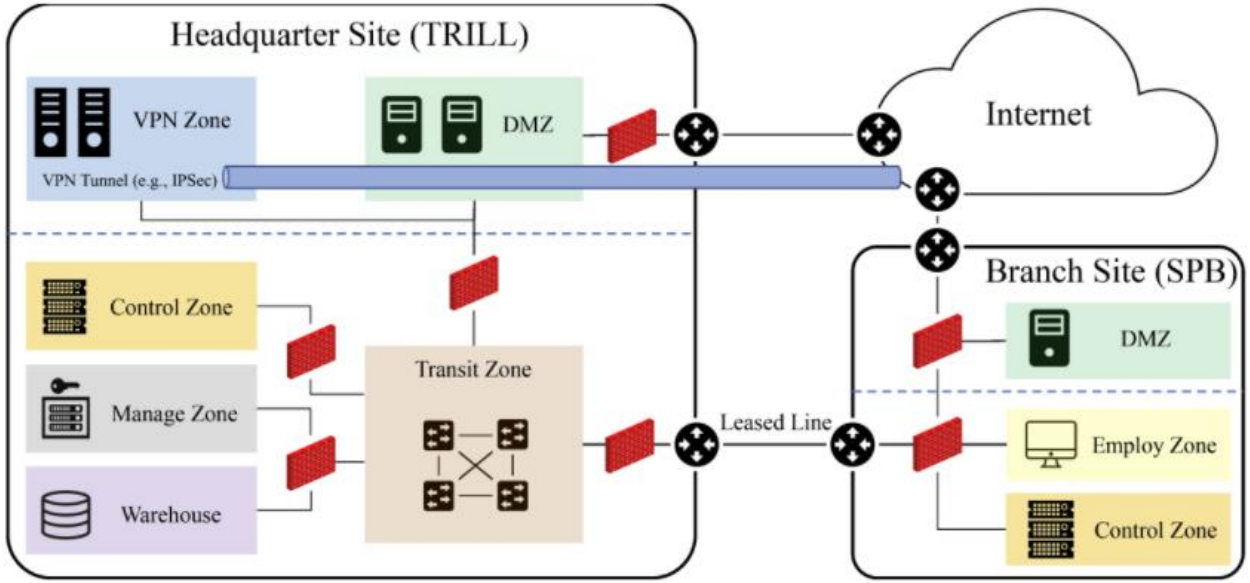


Fig. 1: Network zoning use case for large enterprises. Network zones are realized with heavy use of security middleboxes (e.g., Firewalls).

到处都是防火墙 还有IPS IDS.jpg

调研：典型企业网络存在的问题

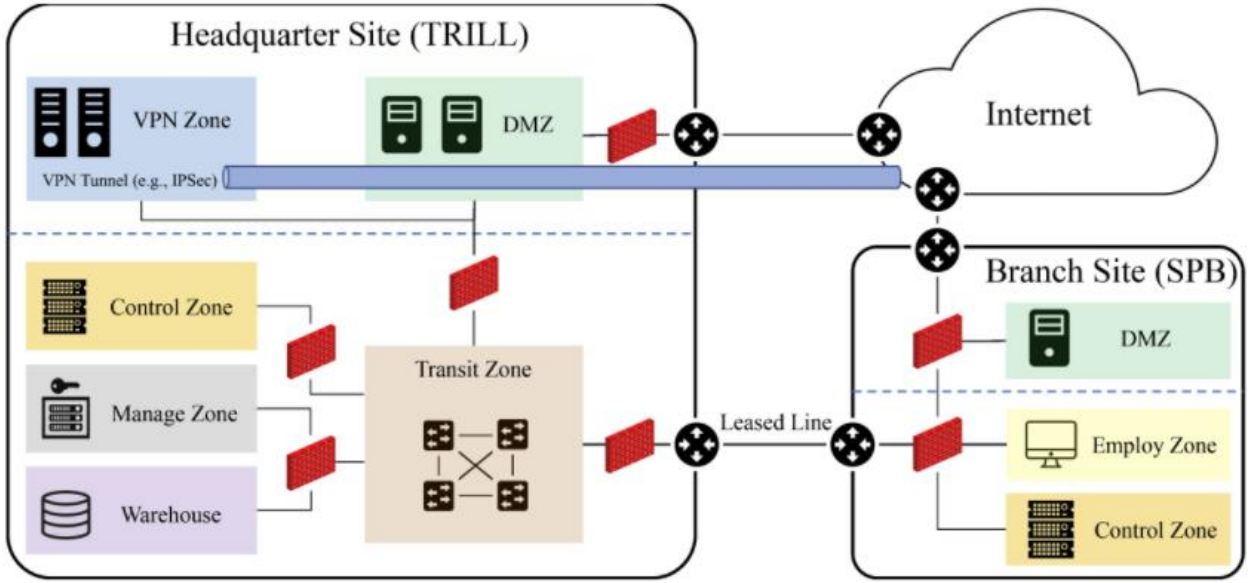


Fig. 1: Network zoning use case for large enterprises. Network zones are realized with heavy use of security middleboxes (e.g., Firewalls).

到处都是防火墙 还有IPS IDS.jpg

调研：典型企业网络存在的问题

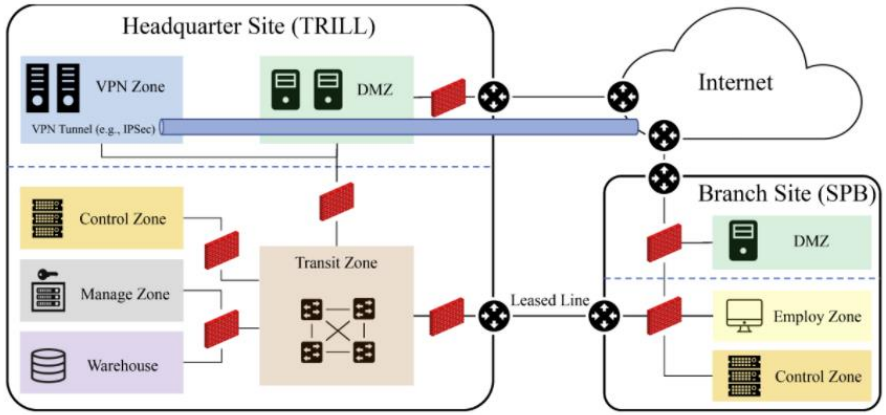


Fig. 1: Network zoning use case for large enterprises. Network zones are realized with heavy use of security middleboxes (e.g., Firewalls).

挑战1：安全区域间的数据传输

挑战2：区域之间的互操作性

挑战3：管理可扩展性

MONDRIAN 架构

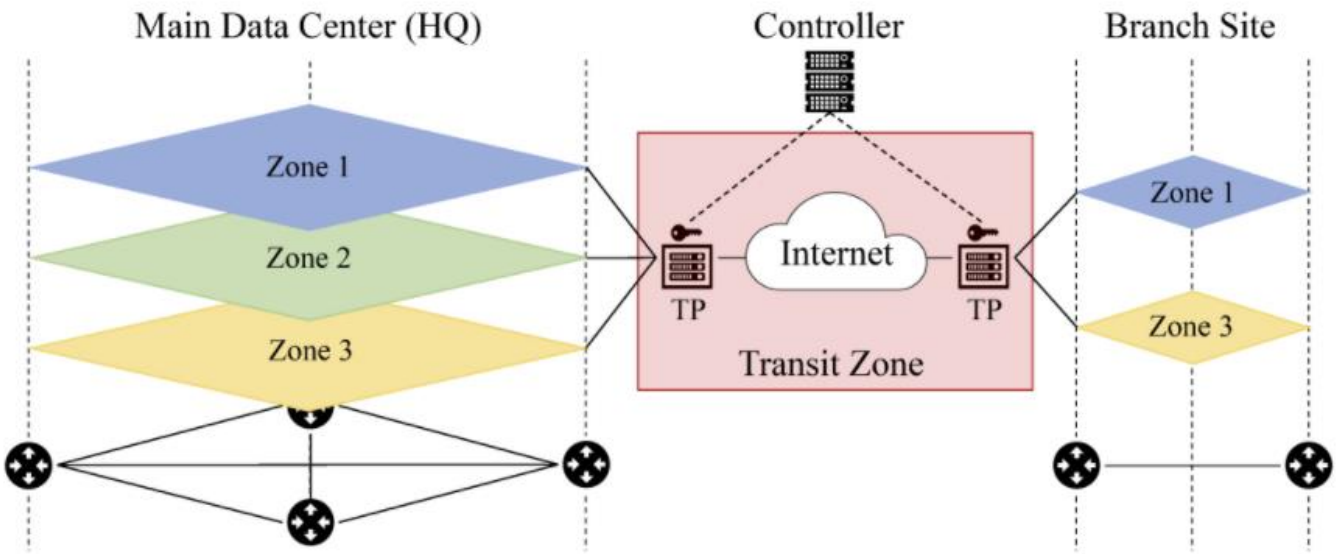
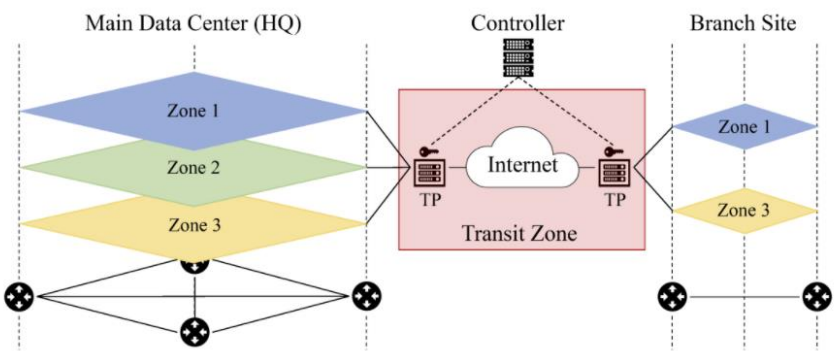


Fig. 2: An overview of the MONDRIAN architecture. The inter-domain transit zone interconnects physically and logically distributed network zones with unified security policy enforcement.

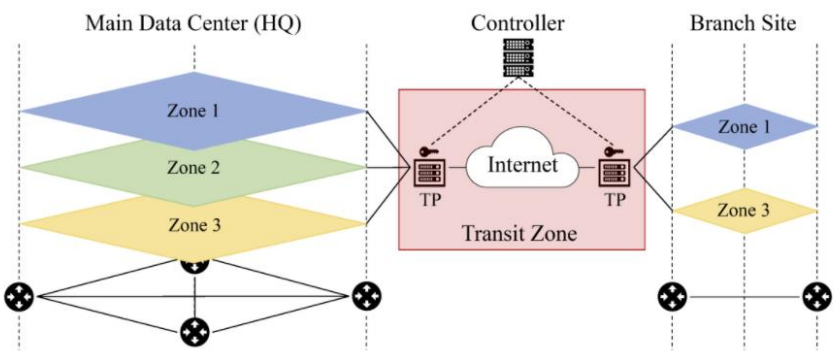
- 目标：数据机密性、管理可扩展、效率、可部署性

MONDRIAN 架构



- 企业的不同分支站点通过广域网（如互联网）互连
- 每个站点包含多个逻辑上分离的区域，这些区域连接到相应站点的单区域转换点
- TP是区域转换的指定网关，在第3层上运行并将企业网络给定站点的所有区域互连
- TPs是MONDRIAN体系结构的端点，这意味着需要对内部网络进行最小的更改，以确保与现代企业环境的兼容性

区域转换点 TP

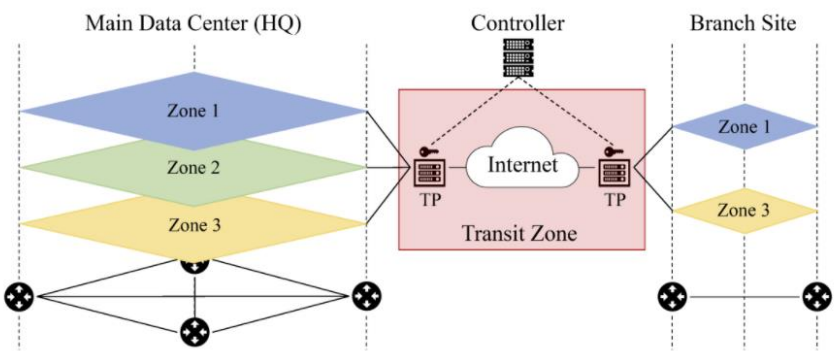


- 企业的不同分支站点通过广域网（如互联网）互连
- 每个站点包含多个逻辑上分离的区域，这些区域连接到相应站点的单区域转换点
- TP是区域转换的指定网关，在第3层上运行并将企业网络给定站点的所有区域互连
- TPs是MONDRIAN体系结构的端点，这意味着需要对内部网络进行最小的更改，以确保与现代企业环境的兼容性

TP沟通流程：

- 管理员建立网络拓扑及域间转换策略，上传到控制器
- 每对TPs交换对称密钥以建立安全通道，密钥定期更新
- 发送数据包时，数据包与相应的区域转换信息一起加密，并通过WAN转发
- 远程站点TP解密数据包，并根据封闭的区域转移信息转发数据包（前提是符合转发策略）

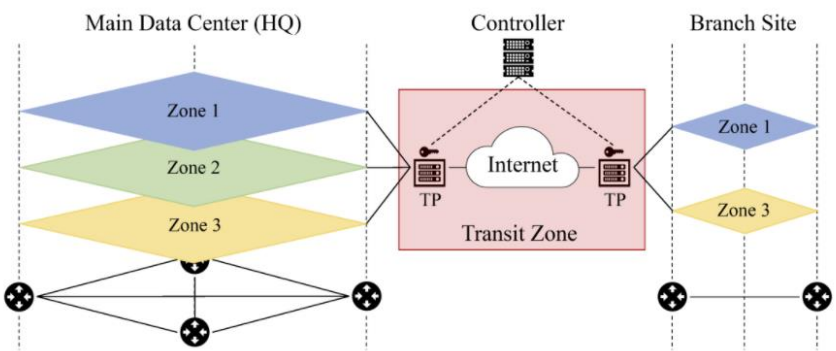
密钥管理



TP使用层级化密钥管理

- 0级密钥：每个TP单独生成一个S_tp
- 1级密钥：从S_tp派生出其他TP的不同的对称密钥
- 2级密钥：为同一TP后的每个Zone派生不同的密钥

安全性分析



- 渗透
  - 防止交换密钥时的中间人攻击：TPs使用相互信任的CA颁发的证书交换密钥
  - 数据包重放：一旦有效载荷发生变化，重复使用的数据包报头的有效性就会丢失，因为会检查MAC
  - 暴力破解加密密钥：256位AES暂时是够了，还能防量子计算机

- DDoS
  - 部署多台TPs并做好负载均衡；甚至可以上之前讲过的Ripple系统防止链路阻塞（分号后面我自己想的）
  - 甚至还能加上端口隐藏（SPA），在需要的时候才放对应的TP流量进来，平时根本扫描不到开放的端口（也是我自己想的）

Ideas

- 粒度
  - 现在的粒度是网络区域
  - 现在市面上零信任产品的粒度是啥？用户（大概）？粒度非常细，当然也有分组管理
- 基线
  - 怎么判断一整个网络区域的安全程度？不止根据密级，还要根据动态的区域威胁程度来调整——这不就是把网络区域当成零信任里的用户了吗！
  - 怎么做好网络内部态势感知与中心控制器的协调

只要能写出来原型，感觉排列组合以后能写好几篇，当然咱还不知道有没有人做过这方面的工作