文章编号：2096-1618(2017)增-0079-03

基于安全区的气象业务局域网规划设计探讨

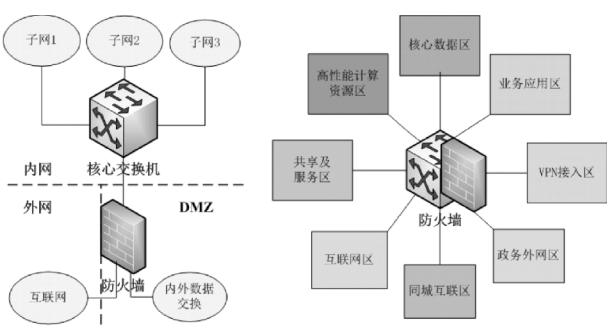
杨　东
(成都市气象局，四川 成都 610072)

摘要：为解决日益迫切的网络安全和管理问题，以成都市气象局核心局域网的规划设计为例，探讨了核心局域网的构建思路，就基于防火墙和安全区的局域网设计进行了阐述，为构建数据交换和安全防护高度一体化的局域网提供参考。

关　键　词：局域网；安全区；防火墙；安全策略

局域网通常以核心交换机为核心，用于局域网内的数据交换，防火墙布设在局域网的边界上，用于隔离内外网络，防火墙通过区域划分的概念将网络划分成不同的逻辑区域，即安全域，针对不同的安全域采用不同的域间策略控制各域间访问控制，从而实现内部网络、外部网络和 DMZ 间可控的信息交互。网络规模的扩大使得此方式在内部网络安全防护、网络扩展性和易管理性方面的不足逐步显见。将防火墙引入局域网的核心是行之有效的办法，以核心交换机加防火墙为核心，通过在局域网中加入防火墙，引入安全域的概念，对局域网进行区域划分，由核心交换机负责网络数据流的转发，防火墙负责网络数据流的安全过滤，实现网络和安全防护一体化的同时，将网络业务管理和安全业务管理分离，满足局域网安全扩展性和易管理需求。以成都市气象局局域网重构为例，阐述以交换机和防火墙为核心的局域网规划设计过程，探讨网络结构规划、技术实现等核心问题，为组建高效、安全、灵活的气象业务局域网提供参考借鉴。

1　网络结构



(a) 传统局域网结构　　(b)基于安全区的局域网结构

图 1　局域网结构对比

如图 1(a)所示，传统的局域网设计是以核心交换机为核心，由它实现子网及 VLAN 的划分及数据流交换，防火墙一般都部署在网络的边界上，用以实现内外网的隔离和数据流安全过滤，而内部网络中各子网间的安全防护一般不考虑，即使有需求一般也采用应用策略实现，安全过滤效果不佳，实施和管理都不够方便灵活。

基于安全区的局域网在网络结构上将防火墙移至局域网核心，通过防火墙将安全过滤功能引入至网络的核心。配合核心交换机实现数据流的过滤交互，其中交换机负责数据流转发，而防火墙负责数据流的安全过滤。如图 1(b)所示，逻辑上网络不再是单一的内网、外网和 DMZ，而是将网络按照不同的应用需求和安全需求划分为多个安全区。通过防火墙定义每个安全区对应的安全域(数据流入域和数据流出域)，设置每个安全域的优先级和域间访问控制策略实现多个安全区之间的数据流过滤交互，根据策略的不同将网络逻辑划分为若干个内网、外网和 DMZ。此结构不仅实现高效的局域网安全访问控制，而且实现了网络业务和安全业务的分离。如果后续网络结构或安全防护需求发生变化，只需根据需求单独调整安全区结构或安全策略，不仅以低维护成本实现了高效灵活的安全策略，同时组网更加灵活，网络管理更加高效。同时在局域网的边界上，还可以根据需要布设专用于隔离内外网的防火墙或行为管理等安全防护管理设备。

所谓安全区，在这里是针对局域网而言，由一组具有相同安全保护需求、并相互信任的系统组成的逻辑区域。一般根据不同的业务布局、工作区分布、应用需求将网络进行人为划分定义区域。一般情况下，一个安全区包括一个或多个子网。所谓安全域，是针对防火墙而言，是通过防火墙将网络划分成不同的逻辑区域。

2　硬件构架

根据高可靠性、高扩展性和兼顾集约化的规划设

计原则,核心交换机加防火墙插卡的构架是业内主流的解决方案。通过防火墙插卡,灵活、迅速地在核心交换机中整合防火墙、VPN 等安全功能,可实现网络和安全防护的高度一体化。

(1)高可靠性

防火墙插卡嵌入核心交换机中,不仅实现了交换机与防火墙之间的高线速交换能力,而且可有效降低单点故障,保证了网络的高可靠性。

(2)功能扩展

核心交换机配合防火墙插卡使用,可实现将核心交换机的每个物理接口作为防火墙接口使用,从而将核心交换变为具有强大接入能力的“核心防火墙”,摆脱了防火墙物理接口有限的束缚,组网更加灵活可控,网络的扩展能力也大大提高了。可进一步结合虚拟化技术,通过在“核心防火墙”设备上划分多个逻辑的防火墙实例来实现对多个业务独立安全策略部署的需求。当业务划分发生变化或者产生新的业务需求时,可以通过添加或者减少防火墙实例的方式十分灵活地解决后续网络扩展问题,简化了网络管理的复杂度。

(3)集约化

在实现交换机设备高性能数据转发的同时,能够根据实际需求处理安全业务,实现安全防护和监控,将核心交换机的转发和安全业务处理有机融合在一起。

3 转发方式

针对核心交换机加防火墙插卡的构架,可选择的转发方式有:跨 VLAN 二层转发、三层子接口转发和跨 VLAN 三层转发。要实现网络业务和安全业务的分离,就防火墙插卡而言,采用跨 VLAN 二层转发方式可以保证网络结构的纯粹性和灵活性。将三层接口都设置在核心交换机上,由核心交换机负责各安全区、各子网、各 VLAN 间网络数据流的转发,而防火墙插卡只以二层数据流方式负责网络数据流的安全过滤。

跨 VLAN 二层转发,就是由数据链路层来完成不同 VLAN 间的通信。防火墙插卡和交换机配合使用,经过交换机的二层网络数据流由防火墙插卡过滤后再由三层接口进行转发。跨 VLAN 二层转发需注意:流量在交换机上的入接口和出接口分别属于不同的 VLAN;交换机与防火墙插卡相连的链路两端的以太网口均配置为 Trunk 类型;防火墙插卡连接交换机的以太网口下配置多个子接口,每个子接口的编号和交换机上的 VLAN 一一对应;将各子接口加入相应的安全域,通过安全域策略实现安全过滤。

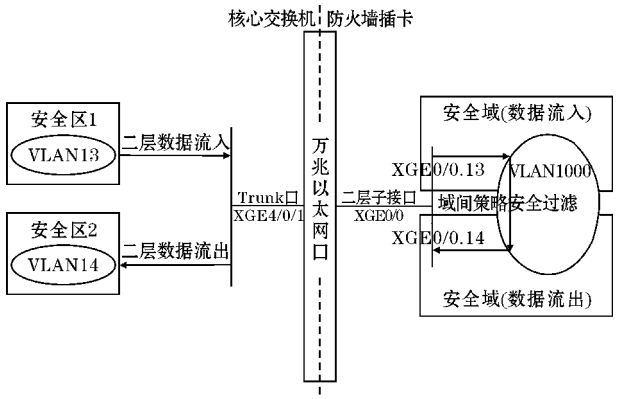


图 2 同网段安全过滤

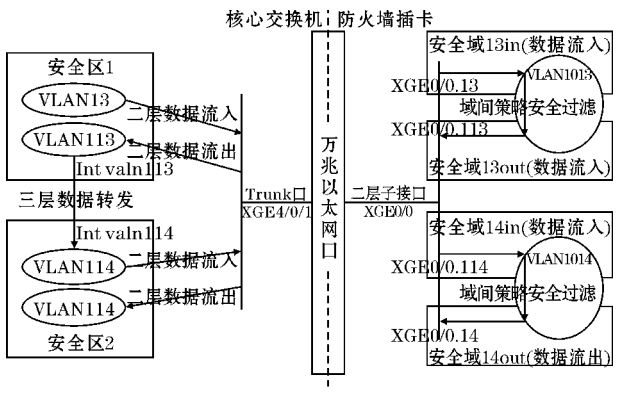


图 3 不同网段安全过滤

图 2 和图 3 描述了从安全区 1 至安全区 2 的单向数据流安全过滤过程,反向数据流与此类似。其中图 2描述了两个安全区同属一个子网(网段)的情况下,数据流安全过滤过程,图 3 描述了两个安全区分属不同子网(网段)的情况下,数据流安全过滤过程。如图 2所示,安全区 1 划分为 VLAN13、安全区 2 划分为 VLAN14,两个安全区在同一网段,此情况下的跨 VLAN 二层转发的具体过程为:(1)报文进入交换机,交换机对报文加上 Tag 标签(图 2 中 VLAN13)。因为报文目的属于另一个 VLAN(图 2 中 VLAN14),所以不能直接从交换机的另一个接口发送出去,报文由 Trunk 口发送至防火墙插卡。(2)防火墙插卡去掉报文中的 Tag 标签,加上防火墙 VLAN 的 Tag 标签(图 2 中 VLAN1000),之后对报文进行相关处理(防火墙的各种安全功能,主要是基于安全域的数据流安全检测和过滤)。(3)防火墙插卡去掉报文中防火墙 VLAN 的 Tag 标签,加上出方向子接口的编号对应 VLAN 的 Tag 标签(图 2 中 VLAN 14)(出方向子接口可以通过查 MAC 地址表确定)后把报文发送至交换机。(4)交换机在对应的 VLAN(图 2 中 VLAN 14)中转发报文。

实际应用中,各安全区各自占用一个子网,要实现跨网段数据转发与安全过滤的分离,更多的情况是如

图3所示的采用不同网段安全过滤的方式,具体过程与上述过程类似。需要注意的是:每一个安全区的出入数据流分别属于两个不同的VLAN(图3中的VLAN13、VLAN113和VLAN14、VLAN114,其中安全区1中的网口都划为VLAN13,安全区2中的网口都划为VLAN14);两个VLAN分别对应防火墙插卡的两个不同的二层子接口(图3中的XGE0/0.13、XGE0/0.113和XGE0/0.14、XGE0/0.114);两个二层子接口分别属于防火墙的两个安全域(图3中的安全域13in、13out和安全域14in、14out);安全过滤由对应的安全域策略完成;转发由出数据流VLAN对应的三层虚接口(图3中的Int VLAN113和Int VLAN114,其中安全区1中的设备以Int VLAN113为网关,安全区2中的设备以Int VLAN114为网关)在交换机上完成。

由此可见,不同安全区的数据流不是采用传统的核心交换机二三层转发,而是经过跨VLAN二层转发,以二层数据流引入的方式由防火墙安全域过滤后再通过核心交换机转发。

4　安全区及VLAN规划

安全区是根据业务布局、工作区分布、应用需求、安全需求进行划分的。考虑到气象部门的实际情况和需求,根据业务布局,可分为服务器区、实时业务区、一般业务区、视频会商区、行政办公区、普通用户区等。根据工作区分布可分为气象台、信息中心、服务中心等。根据应用和安全需求可分为高性能计算资源区、核心数据区、服务区、共享区等。同时由于对外互联的网络并非单一,不能简单地将对外互联网络都定义为外部网络,而是根据业务和安全需求定义为相应的安全区,如政务外网区、同城互联区、互联网区、VPN接入区等。

便于网络结构的清晰,一般情况下一个安全区占用一个子网。跨VLAN二层转发需要在核心交换机上为每个安全区规划两个VLAN,同时在防火墙上规划三个VLAN,其中两个分别与交换机上的VLAN一致,第三个VLAN用于转发从交换机接收到的报文。需要规划定义的VLAN较多,并且具有一定的对应关系,所以需特别注意VLAN的命名规范和对应关系,以免出现混乱;注意在适当位置预留VLAN,用于网络扩展和变动。另外一种情况是,可将数据交换效率需求高、相互之间安全隐患小的安全区部署在交换机上,各自只划分一个VLAN,不将二层数据流引入至防火墙,而通过VLAN虚接口直接实现数据高速转发,如高性能计算区与核心数据区、视频会商区等。

5　安全域及策略规划

要实现安全过滤,需要在防火墙插卡上规划每个需要安全过滤安全区相应的安全域及过滤策略。这里我们采用二层物理子接口加VLAN,及结合IP地址的方式定义安全域。为每个安全区数据流入和数据流出分别定义安全域,并将相应的子接口和VLAN加入至安全域中。

域间策略是基于访问控制列表(ACL),在安全域之间实现流识别功能的。域间策略在一对源安全域和目的安全域之间维护一个ACL,该ACL中可以配置一系列的匹配规则,以识别出特定的报文,然后根据预先的设定允许或禁止该报文通过。

根据各安全区的需求,通过部署安全域间的安全策略实现数据流的过滤和交互。基于以上方式,通过创建或引用ACL,可以根据报文的源IP地址、目的IP地址、源MAC地址、目的MAC地址、IP承载的协议类型和协议特性(例如TCP或UDP的源端口/目的端口、ICMP协议的消息类型/消息码)、时间段、HTTP/SMTP报文中携带的内容等信息制定匹配规则,并指定是否允许匹配的报文通过。从而实现精确的数据流的安全过滤。

安全域策略设计的原则是满足需要的前提下尽量简单,易于匹配,便于提高报文过滤的效率。如果访问控制需求过于复杂,建议进一步细化安全域划分,而不是设计过于复杂的安全域策略,以使得网络结构清晰,便于网络管理。

6　结束语

通过在局域网的核心部署防火墙,将安全区这一概念作为局域网规划设计的核心,摆脱了传统设计中内外网划分的单一概念,转而由安全区的需求决定各区域在网络中的位置,提高了组网规划的灵活性。通过合理部署安全区访问策略,灵活细致地控制各种数据流的过滤及交互,提高了局域网的安全性。核心交换机和防火墙插卡的集约化结构更是提高了网络的可靠性和扩展性。同时也应该注意到,采用此方式的局域网组建,在初期网络规划和实施时都相对繁复一些,但后期在适应性和管理性方面的优势却是其他方式不能比拟的。