商业轻骑兵解决方案

政府行业电子政务外网安全加固方案

开局指导

新华三技术有限公司

http://www.h3c.com

目录

官网介绍

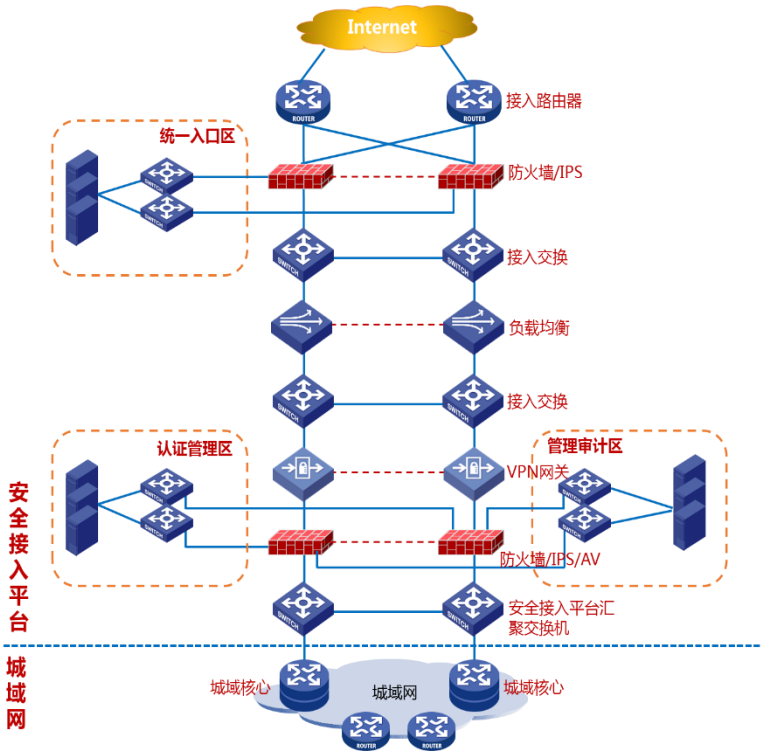
电子政务外网安全加固解决方案-https://www.h3c.com/business/zf2.htm

参考设备配置清单

根据需求做防火墙选型：F1000-AI-15/25/55/75、F5000-AI-15/20/40 等，在此以 F1000-AI-25 为例做配置。

方案名称	类型	组网应用定位	产品选型建议
电子政务外网安全加固解决方案	设备	乡镇延伸安全边界	H3C SecPath F1000-AI-25
			NS-SSD-480G-SATA-SFF
			PSR150-A1-B
	相关软件产品	乡镇延伸安全边界	H3C SecPath F1000,SSL VPN 25个用户
			H3C iMC-SSL VPN认证客户端-F1000-25 License
		终端准入管理	H3C iMC-智能管理平台标准版-25 License
			H3C iMC-EAD终端准入控制组件
			EAD-工程实施服务(管理2000安全认证用户端远程技术支持服务及5个客户端样板点安装费用)
			EAD-工程实施服务(必配)
			H3C iMC-EAD终端准入控制组件-2000 License
			H3C iMC-智能管理平台标准版
		终端数据管理、终端行为管理	H3C iMC-智能管理平台标准版-25 License
			H3C iMC-EBM终端行为管理组件
			H3C iMC-EBM终端行为管理组件-500 License
			H3C iMC-EDM终端数据管理组件
			H3C iMC-EDM终端数据管理组件-500 License
			H3C iMC-智能管理平台标准版

参考组网及关键技术



方案名称	关键技术点	作用	涉及产品
电子政务外网安全加固解决方案	XXX VPN	建设VPN隧道，网络准入，安全访问电子政务外网	防火墙等安全设备
	入侵防御	阻断外部发起对内部的攻击事件	防火墙等安全设备
	终端准入	对接入终端进行认证，确保网络的安全性	IMC-EAD
	用户行为监控	对网络数据采集、分析和识别，可以实时监测终端行为、网络行为及网络流量	IMC-EBM
	数据监控	有针对性地进行数据管控，防止核心信息资产外泄	IMC-EDM
	…		

开局相关资料

1. 安全策略是根据报文的属性信息对报文进行转发控制和 DPI（Deep Packet Inspection，深度报文检测）深度安全检测的防控策略。技术介绍及典型配置可参考下述链接。

F1000/F5000 系列防火墙

http://www.h3c.com/cn/d_202203/1561659_30005_0.htm#_Toc96721881

2. SSL VPN 以 SSL（Secure Sockets Layer，安全套接字层）为基础提供远程的安全连接服务。用户可通过互联网，使用内嵌 SSL 协议的浏览器与远端的 Web 服务器建立安全的连接，访问内部资源。技术介绍及典型配置可参考下述链接。

   F1000/F5000 系列防火墙

   http://www.h3c.com/cn/d_202203/1561710_30005_0.htm#_Toc96724746

3. IPS（Intrusion Prevention System，入侵防御系统）是一种可以对应用层攻击进行检测并防御的安全防御技术。技术介绍及典型配置可参考下述链接。

   F1000/F5000 系列防火墙

   http://www.h3c.com/cn/d_202203/1561692_30005_0.htm#_Toc96723941

4. iMC EDM 终端数据管理是基于 iMC 平台开发的业务组件，支持有针对性地对数据进行管控。技术介绍及典型配置可参考下述链接。

   http://www.h3c.com/cn/d_202111/1490264_30005_0.htm#_Toc86997105

5. 终端行为管理（EBM，Endpoint Behavior Manager）是基于 iMC 平台开发的业务组件，是一款结合终端行为审计和监控、用于加强信息安全建设的综合性产品，主要用于解决各企事业单位终端用户行为管理的问题。技术介绍及典型配置可参考下述链接。

   http://www.h3c.com/cn/d_202111/1490261_30005_0.htm#_Toc86940482

6. EAD 安全策略组件通过对接入网络的用户终端强制实施企业安全策略，加强网络用户终端的主动防御能力，并严格控制终端用户的网络使用行为，保护网络安全。技术介绍及典型配置可参考下述链接。

   http://www.h3c.com/cn/Service/Document_Software/Document_Center/IP_Management/H3C_intelligentize/H3C_intelligentize/Configure/Online_Help/iMC_EAD_Online_Help-7.3-5PW103/?CHID=175758

   http://www.h3c.com/cn/Service/Document_Software/Document_Center/IP_Management/

H3C_intelligentize/H3C_intelligentize/Configure/Typical_Configuration_Example/iMC_EAD_Typical_CE-5PW101/?CHID=181880