



ADDC5.3方案防火墙添加自定义的IPS策略

ADDC解决方案

李猛

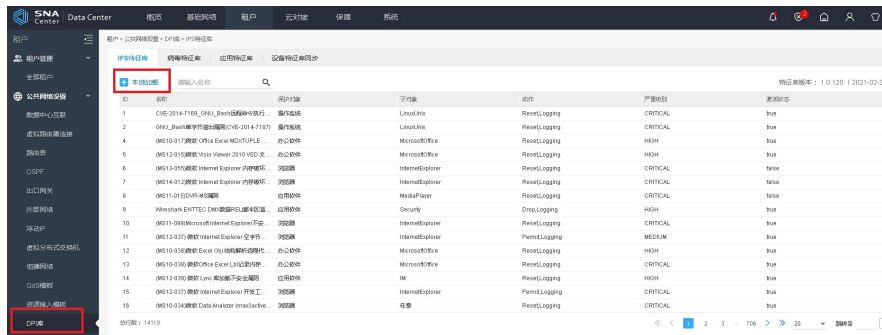
2021-03-12 发表

问题描述

ADDC5.3方案防火墙如何添加自定义的IPS策略?

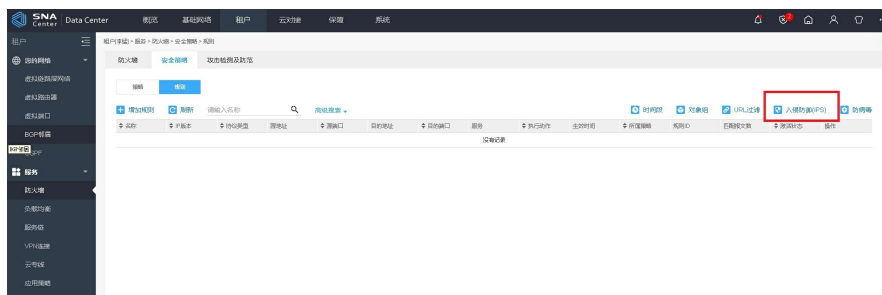
解决方法

1.加载DPI特征库

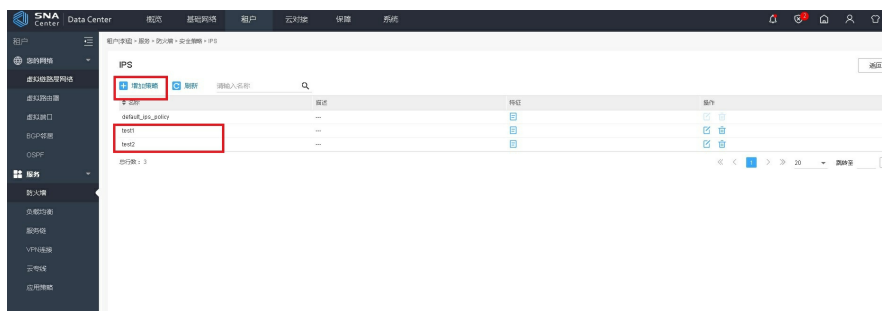


ID	名称	保护对象	子项值	动作	严重级别	启用标志
1	CVE-2018-7109_OVAL_漏洞扫描引擎漏洞	漏洞扫描	Linux/Win	ResetLogging	CRITICAL	true
2	OWASP_BurpSuite漏洞扫描引擎漏洞	漏洞扫描	Linux/Win	ResetLogging	CRITICAL	true
4	MS10-017微软Excel宏漏洞	办公软件	MicrosoftOffice	ResetLogging	HIGH	true
5	MS13-016微软Visio Viewer 2010 VSD文件	办公软件	MicrosoftOffice	ResetLogging	HIGH	true
6	MS13-015微软Internet Explorer的漏洞	浏览器	InternetExplorer	ResetLogging	CRITICAL	false
7	MS14-012微软Internet Explorer的漏洞	浏览器	InternetExplorer	ResetLogging	CRITICAL	false
8	MS11-015微软Windows Defender	杀毒软件	WindowsDefender	ResetLogging	CRITICAL	false
9	Windows EXTERNAL_CANT_CONNECT漏洞	应用软件	Security	ResetLogging	HIGH	true
10	MS11-009微软Internet Explorer的漏洞	浏览器	InternetExplorer	ResetLogging	CRITICAL	true
11	MS13-017微软Excel宏漏洞	办公软件	MicrosoftOffice	ResetLogging	HIGH	true
12	MS10-030微软Excel宏漏洞	办公软件	MicrosoftOffice	ResetLogging	HIGH	true
13	MS10-030微软Excel宏漏洞	办公软件	MicrosoftOffice	ResetLogging	CRITICAL	true
14	MS13-016微软Excel宏漏洞	办公软件	MicrosoftOffice	ResetLogging	HIGH	true
15	MS13-017微软Internet Explorer的漏洞	浏览器	InternetExplorer	ResetLogging	CRITICAL	true
16	MS10-030微软Data Analyzer (malicious)	浏览器	Security	ResetLogging	CRITICAL	true

2.增加IPS策略



3.根据default策略自定义IPS策略



名称	描述	动作
test1	测试策略	ResetLogging
test2	测试策略	ResetLogging

4.成功增加IPS策略后，在防火墙页面增加规则

