Supernova 测试仪 防火墙恶意代码检测配置手册

网测科技 2021/01/22





1.	文档说明	3
2.	网络拓扑图	3
3.	设置防火墙	4
	3.1 设置接口 ip 地址	4
	3.2 配置防火墙病毒检测	5
	3.3 配置防火墙策略	6
4.	设置 Supernova 测试仪	7
	4.1 防火墙恶意代码检测用例配置	7
	4.2 启动测试用例	8
	4.3 运行用例	8
	4.4 查看运行报告	9



1. 文档说明

本文档介绍配置防火墙恶意代码检测的配置过程,此文档使用一台简网防火 墙配置举例,不同品牌的防火墙操作配置存在差异性,而且随着系统版本升级和 接口变化,需要不断对配置用例进行修改和升级,所以有任何问题,请联系我们 的售前或售后支持人员。

2. 网络拓扑图

本次测试的网络拓扑图如下



判断方法:

通过 HTTP 协议,Get 一个病毒文件或者恶意程序,通过响应的成功与否,判断防火墙对恶意代码的检查结果。



3. 设置防火墙

3.1 设置接口 ip 地址

进入防火墙系统网络接口配置页面

KFW 监控-	系统管理-	路由▼	防火墙•	病毒与攻击+	上网行为管理•	VPN-	设置用户▼	日志与报告
系统管理 / 控制面板 / 状态	控制面板	•						
9 控件	网络	L ·	接口					
 系统信息 客户名称 序列号 主机名 持续运行时间 	 DHCP服务器 配置 管理员设置 证书 维护 	* * * *	区 选项 DNS 服务 网络代理 7 小时 1 分钟				(更)	x]
系统日期 AV特征值		Mon Ja 33.15	an 6 13:01:54 6 (升级 2017-1	2020 1-08)] [刊]	政]
IPS特征值		7.156	(升级 2017-11	-08)			[升]	级]
警告信息窗口							0000	00
◎ 2020-01-06 12:59:23 失败的管	管理员登录尝试 admi	n						×
② 2019-12-30 20:00:29 系统重原	3							×
◎ 2019-12-24 12:16:31 系统重原	3							×
◎ 2019-12-04 19:19:57 系统重局								×
◎ 2019-11-26 16:45:58 失败的管	管理员登录尝试 APW	1KMB00	1000004 login	t.				×
◎ 2019-11-26 16:45:55 失败的智	管理员登录尝试 APW	1KMB00:	1000004 login	8				×

我这里用的是 m1/1 和 m1/2 端口

KFW	监控▼	系统管理-	路由▼	防火墙-	病毒与攻击,	上网行为管理•	VPN+	设置用户▼	日志与报告・
系统管理 / 网络 /	接口								
0创建 / 编辑	會删除								
	名称				IP/子阿掩码				
	m1/1			81.1	.1.1 / 255.255.0.0	0			
	m1/2			82.1	.1.1 / 255.255.0.0	0			
	m1/3			117.:	1.1.1 / 255.255.0.	.0			
	m1/4			118.:	1.1.1 / 255.255.0.	.0			
	port1			192.168.	16.244 / 255.255.	.255.0			
	port2			8.8.8	.8 / 255.255.255	.0			
	port3			9.9.9	.9 / 255.255.255	.0			
	port4			10.20.9	92.1 / 255.255.25	5.0			
	port5			10.20.8	81.1 / 255.255.25	5. <mark>0</mark>			
	port6			10.20.9	91.1 / 255.255.25	5.0			
	port7			77.1	.1.1 / 255.255.0.0	0			
	port8			78.1	.1.1 / 255.255.0.0	0			



3.2 配置防火墙病毒检测

3.2.1 配置防火墙病毒文件过滤器

进入防火墙病毒文件过滤器配置界面



点击文件过滤器模板进行编辑

KFW	1 -	盆腔・	系统管理-	器由-	防火墙+	病毒与攻击。	上用行为管理。	VPN-	设置用户。	日志与报告	i•		🛓 admin	۵
病毒与攻击/	病毒检查 /	文件过滤	8											
0 sitt 🖊	编辑 合创	除												
						部	*				#条目	DLP规则	出释	
						builtin-p	atterns				19			

文件过滤器中,启动对 .exe 文件模板的屏蔽

KE	N	盖拉• 系统管理	• 路由•	防火墙-	病毒与攻击-	上网行为管理。	VPN-	设置用户。	日志与最告。		🛔 admin 🛛 😁
的粤与攻击	/ 病毒检查/	文件过速器									
22 100	n national										
注释	repacteris			1							
				100.0000000							
-		G		(最大63个学	符)						
		ок									
O sile	/编辑 含于		isable 11 ¥	\$2b9l							
-	H1428									后作	E3)
	▼ 文件模板	(18)									
	*.exe									算器	0
	*.bat									屏蔽	0
	=.com									屏蔽	0
	".dl									深痕	0
	*.doc									屏蔽	0
	*.gz									屏蔽	0
	".hta									##	0
	*.ppt									屏蔽	0
	".rar									用在	0
	*.scr									屏蔽	0
	".tar									##	0
	*.tgz									屏蔽	0
	=.vb7									屏蔽	0
	".wps									屏蔽	0
	*.xl?									屏蔽	0
	".zip									屏蔽	0
	⁼.p#									屏蔽	0
	".cpl									屏蔽	0
	> 文件类型	(0)									

3.2.2 配置防火墙病毒检测配置模板

KFW ***	系统管理-	路由- 8	防火墙- 病毒	与攻击・	上两行为管理。	VPN -	设置用户;	日志与报告。							🛔 admin	۵
病毒与攻击 / 病毒检查 / 配置模	板		的肉	秘密	▶ 配置模板	1										
			入侵	助护	 文件过滤 	2										
				名称	隔离								注释			
点击创建	新增	配置	置模核	汳												
KFW ≝#₹-	系统管理-	28曲・ 18	防火墙- 病毒	与攻击•	上网行为管理。	VPN-	设置用户。	日志与报告・							🛓 admin	
病毒与攻击 / 病毒检查 / 配置模	板															
								新的反差急软件和	CT18866							
名称 test-exe 注释	模板名称															
			(最大63个字符)			_										
	HTTP	FTP	ІМАР	POP3	SMTP	IM	NNTP	нтте	PS	IMAPS	POP3S	SMTPS	日志记录	选项		
反於憲政件均值 文件过渡									1					builtin-patterns		
隔离发送者(至被禁止的用户列表)		测过滤协议	v .			5				0	0			3448 上二	(1)(2)(2)(2)(2)(2)(2)(2)(2)(2)(2)(2)(2)(2)	
方法	源IP地址		^											应注工——外部面加	卫际部便似	
过期	◎无限期 ○:	2后 5	分钟(s) ~													
								ок	IRSA							

进入防火墙病毒检测配置模板界面



3.3 配置防火墙策略

进入到防火墙策略配置界面:

KFW	监控▼	系统管理・	路由▼	防火墙▼	病毒与攻击	 	VPN+	设置用户→	日志与报告
系统管理 / 控制面板	反/ 状态			策略		策略	1		
◎ 控件				地址	Þ	显式NAT表			
系统信息				服务时刻表	*	DDoS策略 探测策略		00	00
客户名称			SN not	流量整形器	<u>к</u>	IPv6策略			
序列号			APW1K	나이TD		林沙海市			
主机名			APW1K	AEPAIR		WILL LEAN		更	改]
持续运行时间			6 天 17	负载均衡	•				
系统日期			Mon Jai	IPMAC绑定	≞ ▶			[更]	改]
AV特征值			33.156	(升级 2017-11	-08)			[升]	级]
IPS特征值			7.156 (升级 2017-11-	08)			[升]	级]

点击创建增加策略:

KFW	监控▼	系统管理▼	路由▼	防火墙→	病毒与攻击▼	上网行为管理・	VPN -	设置用户▼	日志与报告・
防火墙 / 策略 / 策略									
0创建 → /编辑 →	會删除	11 移动到 +	0 插入						
配置策略内氡	芩:								

KFW	监控• 系统管理• ·	8由- 防火場- 前4	§与攻击→ 上間行为管理→ VI	PN- 设置用户-	日志与服告。				🛔 admin
助火場/ 領轄/ 領轄									
					Sector Se				
源接口/区	m1/1		等略源端口						
源地址	al	• B se	5						
目的接口/区	m1/2		策略目的端口						
目的地址	al	· (18)	5						
时刻表	always	~							
服务	ANY	 (語多2) 	1						
动作	ACCEPT	v							
□ 记录允许流量									
NAT									
④ 不使用 NAT									
〇 启用 NAT	□ 动态IP地址地								
○ 使用中央NAT表									
□ 启用基于BYOD用户认	正的策略								
自用基于用户认证的集	₩E :								
日上房行为管理	default	17							
	test-exe	2 R	deconstruction (and ()) advanta	1 dimetation					
	[请选择]		后用策略上网行 为 管理	中启用病毒检	澳				
□ 扇用Web过滤器	[書店译]		升选择刚才配置的两再	位则使权					
🗌 启用email过读器	[清访挥]								
□ 雇用安全审计	[请选择]								
□ 雇用应用控制	[清西垣]								
山 <u>鹿</u> 用VoIP	[青改祥]								
前展空制 反向流量控制	[清达年]								
最后的	效果如	下:							
KFW	监控→ 系统管理- 器	油- 防火培- 病毒	占攻击• 上两行为管理• VP	N• 设置用户•	日志与报告・				🛔 admin 🕞
防火墙/策略/策略									
○创建 / 编辑 - 日	自删除 11 移动到 电插入	副检查						[列设建]	→ 基于接口查看 ④ 清单式查看
	序列号 7	(序号) 【	7 2 Y EM	¥ 291	ent Timent	▼ 財剣表	T IBS	▼ 动作	হ ম হ
	1	2 m	1/1 m1/2	o all	o all	always	o ANY	ACCEPT	



4. 设置 Supernova 测试仪

4.1 防火墙恶意代码检测用例配置

新增防火墙恶意代码检测测试用例,点击用例→系统安全测试→防火墙策略检测 →恶意代码检测→增加,创建测试用例,受测设备工作模式选择 NAT 模式。



设置填写用例配置中 IP 地址(此处 ip 地址与拓扑中一致):

网络参数限退	客户端	服务器 记述	5					
保持网络设置 客户端 port1				服务端 选择与防j port3	火墙连通的测试口			
◎ 類用調口			MAC 90:e2:ba:ee:92:50	◎ 競用跳口				MAC 90:e2:bared:b5:74
CPU核绑定			-	CPU核绑定				•
报文捕获			-	报文捕获				•
速率与MAC			-	速率与MAC				-
QinQ (部用)			•	QinQ (盆用)				•
子网 😡			+ 添加子网	子网 🛛				+ 版加子网
第1个子网			倉 移除子内 ◎ 禁用子内	第1个子网				自移除子网 ② 禁用子网
測成化調用]IP地址或范围 17.1.2.2-1	7.1.2.201] 测试仪充当客户端的测试 IP	•	测试仪端口IP地址或范围	18.1.1.100	0	测试仪充当服务器端的测
Mitt	Q號口子阿獲码 16	0			测试仪端口子网掩码	16	0	试IP
	应 拟路由器 17.1,254	0			虚拟路由器	17,1.254.2	0	
1	制武仪第口网关 17.1.1.1	20	客户端port口与防火墙连接	的端口IP	测试仪端口网关	18.1.1.1	0	服务器端port口与防火墙
	VLAN ID 1	0			VLAN ID		0	连接的端口IP
	子网機拟 只懷以書	戸講			子网模拟	只模拟服务请	~	
.8	B拆满所在主机 192.168.	16.237						
8	服务编所在第日 port3	~						
8	路號所在子网 篇1个子	号 ~						

配置请求的病毒文件:

◎ 网测科 netitest.	技	Image: State Image: State<	V20.12.06	Supernova-88D
■ 网关设备测试 Q	16	基本信息(恶意代码绘图)		
@ 代理设备测试 O	0	用語(学校 11-1		
■ 应用服务测试 Θ	0	Home and Marchald Control (1) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2	0	
□ 终端客户测试 Θ		2046 AND 1938 ACTIV 2017 131		
♥系統安全測試 Θ				
由 安全检测评估	0	提號[[1]范囲] 10000-65335		
● DDoS咬击		范囲 1,000-65,335		
C 攻击流量重放		输户确关问题式 Reset 🛩		
1 防火機策略控制		TCPP将随脑的方式,可以用一层度手,也可以通接致reset能交换时 TCPP将随脑的方式,可以用一层度手,也可以通接致reset能交换时		
▶转发策略检测		HI Irgitika. User vigenit, niedower, o		
▶ 思意代码检测				
★ 約天場日30H24238				
₩ 网络流星分析 0	0			
		* 如果POSTB的数据是pon格式,语在语文共中语和Content-Type: application/json * 如果POSTB数据是简单的文本,语在语文头中语如Content-Type: application/s-www-form-untercoded		
		文件功能 EUX#8521年 図 GF 日 HTP常常短35132 114355-1568-5737 307+03114855418538		



4.2 启动测试用例

用例配置后,可点击【启动】直接运行测试用例:

网络 报文捕获 速率与MAC QinQ (美用)	限速(客户	端 服务器	记录	报文捕获		
速率与MAC QinQ (禁用)			•	取义佣砍		
速率与MAC QinQ (禁用)						
QinQ (禁用)			•	速率与MAC		
			•	QinQ (鮮用)		
子网 😧			+ 添加子网 🔺	子网 😡		+ 添加子网
1 个子网			會 移除子网 ◎ 禁用子网	第1个子网		自移除子网 ◎ 祭用子
	测试仪端口IP地址或范围	17.1.2.2-17.1.2.201	0	测试仪端口IP地址或范围	18.1.1.100	
	测试仪确口子网掩码	16	0	测试仪端口子网掩码	16	
	虚拟路由	17.1.254.1		虚拟路由	17.1.254.2	
	测试仪端口网关	17.1.1.1	20	测试仪端口网关	18.1.1.1	
	VERNIE -	-		VERITE		
	子阿模拟	只機以僅戶調	*	子网模拟	只模拟能务调	
	服务端所在主机	192.168.16.228				
	服务端所在端口	port5	~			
	服务端所在子网	第1个子网	~			

4.3 运行用例

用例启动后,正常运行界面如下:

2: 認意代码检测 测试用户: admin	用例名称: Maliciou	usCodeCheck_TP_admin_20210122-14:34:12					۲
(建结果	^	状态 用的用道			网络层		
192.168.16.228 - Port3	90	(Commission of the Commission of the Commissiono			息和 単損 多損 广播		
HTTP 建汞滤素	12.040	应用层		-			
HTTP 建束接时	0	总和 port3 port7		^	192.168.16.228 - Port3	1941	8
92.168.16.228 - Port7	200				被又勝权	830,790	14,654,3
TTP 请求速率	0		砂值	总数	10,7,2,2	445,497	7,858,2
TTP 通常超时	0	HTTP_请求遮率	12,040	212,380	192.168.16.228 - Port7	1910	8
		HTTP_国应码2xx	12,040	212,380	REXERC	445,491	7,858,1
		HTTP_国应码3xx	0	0	般文发送	830,784	14,654,3
		HTTP_国应码4xx	0	0			
		HTTP_国应码5xx	0	0			
		HTTP_请求中断	0	0			
◇ /###		HTTP_请求超时	0	0	6428 E		
		HTTP_平均时延 (微秒)		28			
92.168.16.228 - Port3	88	HTTP_最小时延 (微秒)		11	速率		
研設蛋白数量	D	HTTP_最大时廷 (微秒)		200,059 🗸			
较字节数量	0	Concerned in the second se			192.108.10.228 * PORS		0.006
L文编程	(重雪)已经停止	佐榆辰 ♥		^	AND DECK AND		9,990.
22 168 16 228 - Port7	0.00	總和 port3 port7		^	102 168 16 228 8++2		300
					(TBAR)		209
	0		砂值	总数	(TERMON		0.006
10162	Leber 1 Eddamate	TCP_主动新建连接	12,041	212,381	And BLOCKS		9,990.
COND	THE CASADIT	TCP_主动建成连接	12,040	212,380			
		TCP_被动蹦成连接	12,040	212,380			
		TCP_当前主动并发数量		4			
抗资源	^	TCP_当前被动并发数量		6	用例管理		
		TCP_主动FIN关闭成功		0			
3称 占用	总数	TCP_被动FIN关闭成功		0	用例名称		用户
統内存 53345 46 66%	64322 MB	TCP_主动Reset关闭连接		212,377	MaliciousCodeCheck_TP_ad	min_20210122-14	:34:12 adm
(页内存 3) 03.81%	30656 MB	TCP_被动Reset关闭连接		212,375			
93,0110			0	6 8			



Supernova 测试仪防火墙恶意代码检测配置手册

用例运行中,可点击【报文捕获】进行抓包查看运行报文:



查看报文捕获到的交互报文,可以看到防火墙对此病毒文件进行了访问阻断:

He.	Time	Saurce	Destination	Frotecal	Length	Seclert	DatFort Info		
+	2 0.000002	18.1.1.100	17.1.2.197	TCP	62	80	11993 80 + 11993 [SYN, ACK] Seq-0 Ack-1 Win-5840 Len-0 M	55-1460 SA	ICK_PERM-1
-+-	7 0.000013	17.1.2.197	18.1.1.100	HTTP	155	11993	80 GET /TrojanVirus.exe HTTP/1.1		
	12 0.000035	18.1.1.100	17.1.2.197	TCP	60	80	11993 80 → 11993 [ACK] Seq=1 Ack=102 Win=5840 Len=0		
-	19 0.000257	18.1.1.100	17.1.2.197	HTTP	336	80	11993 HTTP/1.1 200 OK (text/html)		
	20 0.000260	17.1.2.197					80 11993 + 80 [RST, ACK] Seq=102 Ack=283 Win=65535 [Ti	CHECKSU	M INCORRECT] Len=0
1L	22 0.000264	18.1.1.100	17.1.2.197	TCP	60	80	11993 80 → 11993 [FIN, ACK] Seq=283 Ack=102 Win=5840 Len-	-0	
< > Fr > Et > Tr > Hy	ume 7: 155 bytes on wire hervet 11, 5+c; IntelCor, annmässion Control Proto ppertext Transfer Protocol	Wireshark · ﷺ GET /Trojank Host: 1.0.1 Gennection: User-Agent User-Agent HTTP/1.1 286 Content-Type Content Content-Type Content-Type Content-Typ	<pre>AF TCP It (prastream eq 1) - tester_192.162.1 (inc) case (hTTP/L.1) Meteopolity Exter(x).1.0 () () () () () () () () () () () () ()</pre>	1277_pont.poop	: not permitted 抓包查	to dow 活此3	- weload the file "TrojanVirus.exe" (p) (p)URL = 18.1.1.100, 文件被阻塞访问		

4.4 查看运行报告

用例运行结束可以生成报告数据及 HTML/PDF/Word 报告,报告生成后,可以下载 HTML/PDF/Word 格式测试报告。

思意代码检测 测试用户: admin 用例名称: Malco	ousCodeCheck_TP_admin_20210122-14:34:12 运行结果: ● 成功	(臺臺历史) [獨成文件]				*
総規果・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	状态 用例释道	童春报音		网络层		
12 168 16 228 - Port3	for some state of the source o			息和 単損 多損 广摄		
TTP (#12)(#2)	应用层		<u> </u>	Berner von service of the service of		
TTP 建浓超时 0	MHD port3 port7		^	192.168.16.228 - Port3	640	4
12.168.16.228 - Port7 #90				报文播收	90	48,415
TTP 请求读本 0		砂道	er	报文发送	39	25,962
TTP 请求提时 0	HTTP_请求速率	1	701,678	192.168.16.228 - Port7	1910	
	HTTP_国应码2xx	1	701,678	後文張仪	59	25,961
	HTTP_园应码3xx	0	0	微义观击	90	48,415
	HTTP_园应码4xx	0	0			
	HTTP_园应码5xx	0	0			
	HTTP_请求中断	0	0			
(捕获 🔺	HTTP_请求超时	0	0	链路层		
	HTTP_平均时延(微秒)		30			
12.168.16.228 - Port3 总数	HTTP_最小时延 (微秒)		11	24		
存款通知数量 0	HTTP_最大时延(微秒)		200,074 👻	107 169 16 229 Port2		14
(東京市設備) 0	Contra de			济县建立		
文編获 (圖應) 已经停止	15個层 0		^	注意分子		
12.168.16.228 - Port7 总数	●和 port3 port7		^	192 168 16 228 - Port7		м
(2) (2) (2) (2) (2) (2) (2) (2) (2) (2)				济县地位		
(2) (2) (2) (2) (2) (2) (2) (2) (2) (2)		砂塘	总数	流量发送		
文捕获 (国際) 已经停止	TCP_主动新建造接	0	701,678			
	TCP_主动跳动油接	1	701,678			
	TCP_被动建成连接	1	701,678			
	TCP_当前主动并发数量		4			
£资源 🔺	TCP_当前被动并发数量		10	用例管理		
	TCP_主动FIN关闭成功		0			
称 占用 总数	TCP_被助FIN关闭成功		0	用例名称用	户名称	运行和
統内存 53.32% 46.68% 64322 MB	TCP_主动Reset关闭连接		701,678			
页内存 引 93.81% 30656 MB	TCP_被动Reset关闭连接		701,668			



Supernova 测试仪防火墙恶意代码检测配置手册

信息					
MaliclousCodeCheck_TP_admin_2021012	2-14:34:12		用例类型 恶意代码检测		
刪户 admin			开始时间 2021-01-22 14:34:30		
吉果 💿 测试运行正常结束			结束时间 2021-01-22 14:35:44		
数据					
\$次运行 📄 生成报告 📄 生成文档	THE THE THE	皺Word			會 删除此记
应用层 (应用统计)	24/07		传输层(会游航计		
如此 大地和木 多3 应用层 (应用统计)	妙值	总数	传输层(会选统计)	砂疽	感急
2014 ススピロホー 545 应用层 (仮用約):// HTTP_請求達率	砂值 11,694	总数 701,678	传输层 (会选统计) TCP_主动新建选接	砂値 11,694	总数 701,678
www、スタンロホー、あり 应用层 (企用約5分 HTTP:消去注意年 HTTP:回答明2xx	砂信 11,694 11,694	総数 701,678 701,678	传输层 (余/556) TCP_主动新维选报 TCP_主动建成选择	移植 11,694 11,694	总政 701,678 701,678
www.xmu xmum 数3 应用层 (@用時計) HTTP,请未送年 HTTP,自時用2xx HTTP,目時用3xx	砂道 11,694 11,694 0	起数 701,678 701,678 701,678 0	传输层 (金////////////////////////////////////	砂油 11,694 11,694 11,694	总数 701,678 701,678 701,678 701,678
2010年 2014年 2020日本 第3 应用层 (②用時計) 1117 清末送単 1117 月前時32xx 1117 月前時32xx 1117 月前時32xx	946 11,694 11,694 0 0	458 701,678 701,678 0 0	传输层 (小350))) 107.主动脉络连接 107.主动脉络连接 107.主动脉络连接 107.当前声动外发发镜	9 % 11,694 11,694 11,694	830 701,678 701,678 701,678 4
2012 2014 スジロロボ 2013 広用屋 (道)用約1/1 1117: 3月25年 1117: 月回時35xx 1117: 月回時35xx 1117: 月回時35xx	86 11,694 11,694 0 0 0	200 701,678 701,678 0 0 0 0	信結层 (金派時/) TCP 主动師使徒様 TCP 主动師使徒様 TCP 主动使成法様 TCP 生动使成法様 TCP 当前後の形式数量 TCP 当前後の形式数量	86 11,694 11,694 11,694	830 701,678 701,678 701,678 4 4 10
2012 2014 スジロロボ 及5 应用度 ((の用除け) 417P)通用度なx 417P 回用長5xx 417P 回用長5xx 417P 回用長5xx 417P 回用長5xx 417P 回用長5xx	6/6 11,694 11,694 0 0 0 0	880 701,678 701,678 0 0 0 0	(传输展 (分成時計) TCF 主动振荡法策 TCF 主动振荡法策 TCF 振动振荡法策 TCF 振动振荡法策数量 TCF 当新振志动并发数量 TCF 当新振动开关数量	96 11,694 11,694 11,694	8500 701,678 701,678 701,678 4 10 0 0
	800 11,694 11,694 0 0 0 0 0 0 0 0 0 0 0 0 0	888 701,678 701,678 0 0 0 0 0 0 0) 11,694 11,694 11,694	250 701,678 701,678 701,678 4 10 0 0 0
	80 11,694 11,694 0 0 0 0 0 0 0 0 0	88 701,678 701,678 0 0 0 0 0 0 0 0 0 0 0 0 0	【信稿层 (金/500///) TCP 主动師使法様 TCP 主动師使法様 TCP 当前使法功者发展量 TCP 当前使动力发展量 TCP 当前使动力发展量 TCP 主动和以关闭成功 TCP 提向IN关闭成功 TCP 主动和exe天们刻根	84 11,694 11,694 11,694	688 701,678 701,678 4 10 0 0 701,678
	900 11,694 11,694 0 0 0 0 0 0 0 0	838 701,678 0 0 0 0 0 0 0 1 1	传输层 (+):389:11) 1707 主动脉络振振 1707 生动脉络振振 1707 当前走动升发数量 1707 当前走动升发数量 1707 当前走动升发数量 1707 生动的运动的 1707 生动的运动的 1707 生动的主动在长利动振	908 11,694 11,694 11,694	2015 701,678 701,678 4 10 0 0 701,678 701,668
	800 11,694 11,694 0 0 0 0 0 0 0 0 0	88 701,678 701,678 0 0 0 0 30 0 11 200,074		998 11,694 11,694 11,694 11,694	6300 701,678 701,678 701,678 4 10 0 701,678 701,668 4 1
	800 11,694 11,694 0 0 0 0 0 0 0 0	800 701,678 701,678 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		01 11,694 11,694 11,694 11,694	888 701,678 701,678 4 10 0 0 701,678 701,678 41 701,668 41 36

例信息							
田紀名 MaliciousCodeCheck_TP_admin_20210122-1 解成用户 admin 宣行結果 ● 政治宣行正常结束	14:34:12			用例类型 恶意代码检测 开始时间 2021-01-22 14:34:30 结束时间 2021-01-22 14:35:44			
			报告	生成进度			
行数据							
🛪 再次运行 📄 生成报告 📄 生成	······································				100%	已完成	會 删除此证
状态 第日 关键结果 男	*				100%	已完成	
					100%	已完成	
四田辰(亚相皖市) P	DE				1009	日完成	220 C
HTTP_请求速率					100,	0.00	701,678
HTTP_回应码2xx	Vord				1009	已完成	701,678
HTTP_回应码3xx							701,678
HTTP_回应码4xx							4
HTTP_回应码5xx						_	10
HTTP_请求中断		关闭	下载HTML	下載PDF 下載Wa	rd		0
HTTP_请求超时	U		0	TCP 被动FIN天网成功		_	0
HTTP_平均时延 (微秒)			30	TCP_主动Reset关闭连接			701,678
HTTP_最小时延 (微秒)			11	TCP_被动Reset关闭连接			701,668
HTTP_最大时延 (微秒)			200,074	TCP_重传报文数量		0	41
				TCP_主动新建平均时延 (微秒)			36
				TCP 主动新建最小时延 (微秒)			7