应用审计 **刘嘉炜** 2016-06-21 发表

۰

客户购买F100-X-G的防火墙,内网用户为192.168.1.0网段。想要部分用户禁止访问迅雷和QQ等应用



1、分别设置外网接口和内网接口的IP地址(x.x.x.x为外网IP地址、192.168.1.1为内网网关)。

H3C [Root]	R	名称 >	查询 高级查询			
一设备截览	名称*	IPtété	网络掩码	安全域	状态	操作
	GigabitEthernet0/0			-	0	æ 1
1 其大部門	GigabitEthernet0/1	XXXX	255.255.255.0	Untrust	0	1
日期和时间	GigabitEthernet0/2	192.168.1.1	255.255.255.0	Trust	0	1
一接口管理	GigabitEthernet0/3			-	0	B 1
一安全域	GigabitEthernet0/4			-	0	æ 1
─□ 虚拟设备管理	GigabitEthernet0/5				0	1
一配置管理	NULLO				0	191

2、接口加入对应的安全区域

设备管理 > 安全域						保存 帮助 退
 → 设备管理 → 基本電法 → 日期和如封间 → 換口管理 支全括 → 直点拟设备管理 → 配接设备管理 	安全域に	安全域名	优先级	共享	虚拟设备	操作
	0	Management	100	no	Root	û 1
	1	Local	100	no	Root	ø 1
	2	Trust	85	no	Root	p 1
	3	DMZ	50	no	Root	p 1
	4	Untrust	5	no	Root	1

将0/1口加入到"untrust"区域,将0/2口加入到"trust"区域。

3、配置用于NAT的ACL

(墙 > ACL							
➡ 防火墙		_					
	新建AGL						
- CANAT	2012Hedd Tol		_			2000-2999 基本	\$访问控制列
一应用层协议检测	ID:	2000		•		3000-3999 高級	及访问控制系 2.访问控制系
ACL ARP管理	(元表249m):	用户商	2罟	×			491-11191/
- ARP防政击	Ellevert.	107 H	10 III.	-			
- QoS	描述:					^	
□ 流量监管						> 字符	(0-127)
────会话管理	星号(*)为	必须填写项			-	_	
🖬 攻击防范	~				确	定 取消	
Ē > kī.							保存」帮助
防火樓					ACL加速状态	國标描述:●已加速	◎未加速
		访问控制列表	(ID V 查询	高級查询			
-B NAT	访问控制列法D	类型	规则数型	匹数顺序	編述	ACL加速管理	操作
应用层协议检测	2000	基本	0	用户配置		⊘ toi∉	@1
-ACL							
ARP管理			2039	100032-A	10000.02		
ARP防攻击			利油	開始。日本	關防主动		
镐 > ACL							
Desista.							
	ACI -2000 568	H-t-Loni					
-III NAT	NOC-2000 \$131	102-0-202/1					
一应用层协议检测	□规则ID:				(0-65534。如果不報	认规则ID,系统将	会自动指定
- ACL	操作:	[允许	~	时间段	:	无限制 🗸
ARP管理	□分片报文				日记	相志	
a namb of the							
ARP防攻击	□源IP地址:				源地址	通配符:	
- 12 ARP防攻击 - 12 QoS - 12 法軍営管	□源IP地址: VPN实例:	1	无 🗸		源地址	通配符:	

4、配置NAT



-静态:	地址转换	地址转换方式:	Easy IP	\sim	
一应用层的	服为奋 办议检测	地址池索引:		(0-31)	
ACL		□ 外部VPN实例:	~		
- ARP	四里	□开启VRRP关联	关联的VRRP组:		(1-255)
ARPB)	- □ ARP防攻击 - □ QoS - □ 流쮤监管	端口保持:	NO 🗸		
- ¹ Qos - ¹ 流量:		* 星号(*)为必须填写项		确定	取消

选择外网接口、ACL调用之前设置的ACL 2000、地址转换方式设置为Easy ip。

5、配置默认路由

□ 路由管理 - 路由信息	^	静态路由创建		
静心路出 		目的IP地址:	0.0.00	•
- OSPF		撞码:	0.0.0.0	~.
— BGP — {8 #892 cb		下—跳:	X.X.X.X	
一策略路由		出接口:		~
IGMP PIM PIM 		优先级:		(1-25
	~	星号(*)为必须填写项		确定取

x.x.x.x为外网网关

- 二、限制策略的使用
- 6、配置前需要注意
- 1) 设备是否购买特征库licence,如果没有特征库相应的流量无法识别。
- 2) 设备是否购买CF卡,需要设备携带CF卡运行深度检测模块应用。
- 3)防火墙需要运行在UTM模式,单独的防火墙模式下没有深度检测。
- 7、切换防火墙为"UTM"模式

□ 设备管理 □ 基本配置	^	设备运行模式			
一设备基本信息		设备当前运行模式	UTM		
运行模式		下次启动时设备运行模式	UTM	~	
— 日期和时间 — 接口管理		星号(*)为必须填写项			确定

设备当前运行模式必须选择为"UTM"模式。

8、注意在自动升级特征库前一定要设置设备的域名解析。

网络管理 > DNS > 动态	或名解析	
- DHCP	▲ 动态域名解析	
─■ DNS 一静态域名解析 → 动态域名解析	动态域名解析 DNS代理	 ● 启动 ○ 关闭 ○ 关闭
- DDNS	□ 清空动态域名缓存区	
□□□ 流里统计 □诊断工具		NRIAE.
	114.114.114.114	DNS服务器IP地址

■ 攻击防范 ■ 深度安全防御	IPS库 当前版本	2.1.330 2016-05-21			
一时间表 一 License	☑ 自动升级 每星期	- ♥ _在 03:00 ♥			立即升级
─ 特征库升级 — IDC	+1411/2		White	11/m	

H3C [Root]			
一设备觀览	License信息		
- 配置向导	特征库		
₩ 设备管理	IPS	2016-07-18	
→■ 资源管理	APP	2016-07-18	
网络管理	AV_SS	2016-07-18	
11月户管理		Hard and a second	
🖴 防火墙			
🖬 攻击防范			
🖬 深度安全防御	License⇔∧		
一时间表	License文件	浏览	
Licence			

9、在"深度安全防御"中"带宽管理策略应用"中"新建"。

ミ度安全防御 > 帯宽管理					
 入侵检测统计 菜度安全防御 时间表 口(cense 特征库升级 口PS 防病毒 内容监控 带壳管理 协议审计 URU送差 内容过差 过差条目 过透液端 消热电传机 (cense) 	^	新建带克管理策略应用 源域 目的域	Trust V Untrust V		
		市交會運用船 源IP地址列表 (最多10个)	192.168.1.0/24	添加	192.168.1.0/24
		目的IP地址列表 (最多10个)		添加	

设置源域为"trust"目的域为"untrust"源IP地址为192.168.1.0网段。

10、设置过滤QQ

宝度安全防御 > 带宽管理				
→入侵检测统计 ■ 深度安全防御	▲ 新建市汽管理制度			
一时间表	名称	test (1-63字符,1个汉字占2个字符)		
一特征库升级	策略工作模式			
- IPS	本组织则总流量的上行带宽	kbps (8 - 1,000,000) kbps (8 - 1,000,000)		
一防病毒	本组织则总流量的下行带宽			
带宽管理		揮勵势		
一份议审计 一URL过渡	□ 服务名称		劫作	
四月空制	□ 所有服务		允许	
一过透泉目	□选择服务	○///9 〒○ 淘宝旺旺	允许	
— 过滤策略 一 策略模板 一 统计信息	• 上、下行带宽取值范围为8-1,000,000,单位为kcps-	● ● <u>■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■</u>		

11、设置过滤迅雷

□ 入侵检测统计 一型 采度安全防御					
一时间表 一 License	名称	test * (1-63字符-	1个汉字占2个字符)		
一特征摩升级	策略工作模式	○組模式 ●用户模式	○組模式 ◎用户模式		
- IPS	本组织则总流量的上行带宽	kbps (8-1,00	0,000)		
一防病毒	本组规则总流量的下行带宽	kbps (8-1.00	0.000)		
带宽管理		前选择服务	opogiaseoopus		
一時效率计 一URL过渡	日期労名称	— ① 天阿Maze	^	幼作	
一型広用控制	□ 所有服务			允许	
一过港条目	20所通 □	● ○ 0.0000 ○ 移动平台资源下载		允许	
一 过渡第昭 一 第昭模板 一 统计值意	•上、下行带资助值范围为8-1,000,000,单位为ibps-	 □ 107000 □ 0½股软件 □ 防病物支付 □ 1000000000000000000000000000000000000			

12、设置禁止动作并记录日志

深度安全防御 > 带宽管理													
	^	發達環境管理解釋											
一时间表 — License		名称		test	• (1-63字符,1个汉:	与占2个字符)							
一特征库升级		解職工作模式		○組模式 ●	用户模式								
- IPS		本组织则总流量的上行带宽											
一内容溫控		本组规则总流量的下行带宽		kbps (8-1,000,000)									
- 带宽管理													
URL过渡		- 服务	名称		生效时间		劫作						
		□ 所有服务		所有时间		V.	允许 🗸						
一过建杂目		- (28)	3	所有时间		Vel	館虧+日志 ∨						
一过透镜路		DDF器 D	3	所有时间		v .	阻断+日志 ✔						

实验结果:

1、测试QQ无法登陆



2、在日志报表中带宽管理日志中查看阻断日志。

- 一帯売業理	~ ~	P	1141	30.00	- 86	日 作					
一物议审计		Sector Bill Sector	100 M	1 19.02	3914	0224	30	BANP	540	EISTARCE.	広用协议
URLigit		2016-06-16 23:11:23	活業	DBAE	Trust	Untrust	192.168.1.2	119.189.1.9	49636	80	Thunder Kankan HTTP Stream 3
- 22 広用控制		2016-06-16 23:10:45	Mil.00	19.45	Trust	Untrust	192.168.1.2	111.161.52.148	49610	443	Tencent QQ Login Request(TCP)
- CA VPN		2016-06-16 23:10:45	Mil.OO	10.45	Trust	Untrust	192.168.1.2	111.101.52.148	49609	80	Tencent QQ Login Request(TCP)
·····································		2016-06-16 23:10:45	. DO.5M .	1945	Trust .	Untrust .	192.168.1.2		49613	80	Tencent QQ Login Request(TCP)
B志覚標		2016-06-16 23:10:45	勝利の口	198.65	Trust	Untrust	192.168.1.2	183 232 94 212	49607	80	Tencent QQ Login Request(TCP)
- Systec Filt		2016-06-16 23:10:45	(100) (100)	1845	Trust	Untrust :	192.168.1.2	119.147.32.229	49616	443	Tencent QQ Login Request(TCP)
UsericoFLIX		2016-06-16 23:10:45	酸洗の口	IBAS	Trust	Untrust	192.168.1.2	119.147.32.229	49615	80	Tencent QQ Login Request(TCP)
CARD &		2016-06-16 23:10.45	Bil.00	10.61	Trust	Untrust	192.168.1.2	183.60.49.183	49614	443	Tencent QQ Login Request(TCP)
1801-G	90°	2016-06-16 23:10:45	読えのの	19.65	Trust	Untrust	192.168.1.2	111.161.52.177	4027	8000	Tencent QQ Login Request(UDP)
CI-C001+		2016-05-16 23:10:45	読えのの	19.65	Trust	Untrust	192.168.1.2	220 249 246 124	4026	8000	Tencent QQ Login Request(UDP)
- HARE		2016-06-16 23:10:45	100 Billioo	TRAS	Trust	Untrust	192.168.1.2	119.147.45.203	4025	8000	Tencent QQ Login Request(UDP)
日志新工業局		2016-06-16 23:10.45	第3,00	18.65	Trust	Untrust	192.168.1.2	183.60.48.234	4024	8000	Tencent QQ Login Request(UDP)
一全間设置		2016-06-16 23:10:45	勝法の口	18.65	Trust	Untrust	192 168 1.2	183 232 93 25	4013	8000	Tencent QQ Login Request(UDP)
日志服表		2016-06-16 23:10:43	酸洗の口	19.65	Trust	Unbrust	192.168.1.2	183.60.49.182	49605	80	Tencent QQ Login Request(TCP)
一系統日志		2016-06-16 23:10:43	脱退のの	19.65	Trust	Untrust	192.168.1.2	125.39.205.34	49600	80	Tencent QQ Login Request(TCP)
一连接封印制日志		2016-06-16 23:10:43	Milloo	REE	Trust	Untrust	192.168.1.2	183.232.127.166	49601	443	Tencent QQ Login Request(TCP)
一次击路百日志		2016-06-16 23:10:43	験法のロ	四根	Trust	Untrust	192.168.1.2	183 232 94 217	49599	80	Tencent QQ Login Request(TCP)
一篇名单曰志		2016-06-16 23:10:43	Billoo	隐断	Trust	Untrust	192.168.1.2	183.60.50.26	49603	443	Tencent QQ Login Request(TCP)
-160700012		2016-06-16 23:10:43	100.00	FREE	Trust	Untrust	192.168.1.2	163.177.90.147	49604	80	Tencent QQ Login Request(TCP)
- TOCIDITE		2016-06-16 23:10:43	勝利の口	TBRE -	Trust	Untrust	192.168.1.2	163.177.93.213	49602	443	Tencent QQ Login Request(TCP)
PARG		2016-06-16 23:10:43	勝讯のロ	PERF	Trust	Untrust	192.168.1.2	125.39.205.55	49598	443	Tencent QQ Login Request(TCP)
10004016		2016-06-16 23:10.43	Billoo	PERE .	Trust	Untrust	192.168.1.2	123.151.40.24	49595	443	Tencent QQ Login Request(TCP)
Preatents		2016-06-16 23:10:43	勝沢の口	78.65	Trust	Untrust	192.168.1.2	123.151.40.179	49594	80	Tencent QQ Login Request(TCP)
EBSE STREET		2016-06-16 23:10:43		TERE	Trust	Untrust	192.168.1.2	183.232.127.247	4023	8000	Tencent GQ Login Request(UDP)
一切以过费日志	~	2016-06-16 23:10:43	勝讯00	PERF	Trust	Untrust	192.168.1.2	123.151.13.168	4022	8000	Tencent QQ Login Request(UOP)
一Userlog日志		2016-06-16 23:10:43	Billoo	FERE	Trust	Untrust	192.168.1.2	111.30.131.101	4021	8000	Tencent OQ Login Request(UDP)

3、测试迅雷无法登陆



4、在日志报表中带宽管理日志中查看阻断日志。

一带宽管理		R	时间	一重印	「夏の日	1.					
一份议审计		封用	服务	ihit	- 355	目的城	₩P	BMP	1. A	目的第日	使用协议
LURL过去		2016-06-16 23:19:40	記書	胞紙	Trust	Untrust	192.168.1.2	119.188.48.83	51549	80	Thunder Get Resource
		2016-06-16 23:19:35	记言	阳断	Trust	Untrust	192.168.1.2	123.129.242.226	51542	80	Thunder Get Resource
- 😫 VPN		2016-06-16 23:19:31	活雷	阳新	Trust	Untrust	192.168.1.2	123.129.242.226	51517	80	Thunder Get Resource
		2016-06-16 23:19:14	活言	阳断	Trust	Untrust	192.168.1.2	119.188.48.83	51469	80	Thunder Get Resource
日志管理		2016-06-16 23:19:07	35	阳桥	Trust	Untrust	192.168.1.2	119.188.48.83	51441	80	Thunder Get Resource
-SalarR#		2016-06-16 23:18:28	記書	阳断	Trust	Untrust	192.168.1.2	123.129.242.179	51277	80	Thunder Get Resource
- Under Dit		2016-06-16 23:18:24	活雷	阳断	Trust	Untrust	192.168.1.2	123.129.242.140	51027	80	Thunder Get Resource
Useriog(CLS)		2016-06-16 23:18:23	记言	開新	Trust	Untrust	192.168.1.2	123.129.242.140	50988	80	Thunder Get Resource
常田志		2016-06-16 23:18:23	活雷	阳断	Trust	Untrust	192.168.1.2	121.10.120.61	50987	80	Thunder Get Resource
一日志創件		2016-06-16 23:18:23	記書	阳断	Trust	Untrust	192.168.1.2	163.177.79.152	50986	80	Thunder Get Resource
		2016-06-16 23:17:32	32	阳桥	Trust	Untrust	192.168.1.2	60.217.235.169	50682	80	Thunder KanKan HTTP Stream 3
一日志輸出策略		2016-06-16 23:17:28	通言	阳断	Trust	Untrust	192.168.1.2	60.217.235.158	50669	80	Thunder KanKan HTTP Stream 3
一全局设置		2016-06-16 23:17:12	活雷	阳断	Trust	Untrust	192.168.1.2	60.217.235.158	50606	80	Thunder KanKan HTTP Stream 3
日志探表		2016-06-16 23:17:05	记言	阳断	Trust	Untrust	192.168.1.2	163.177.79.183	50583	80	Thunder KanKan HTTP Stream 3
- Eiter#		2016-06-16 23:17:05	话言	阳新	Trust	Untrust	192.168.1.2	60.217.235.158	50581	80	Thunder KanKan HTTP Stream 3
		2016-06-16 23:17:02	记言	阳断	Trust	Untrust	192.168.1.2	60.217.235.158	50553	80	Thunder KanKan HTTP Stream 3
日田田田町		2016-06-16 23:17:02	100.后器	阳断	Trust	Untrust	192.168.1.2	183 232 94 212	50526	80	Tencent QQ Login Request(TCP)
"现当防范日志		2016-06-16 23:17:02	四月月	阳断	Trust	Untrust	192.168.1.2	111.161.52.148	50528	80	Tencent QQ Login Request(TCP)
一黑名甲日志		2016-06-16 23:17:02	新讯00	跑新	Trust	Untrust	192.168.1.2	111.161.52.148	50529	443	Tencent QQ Login Request(TCP)
一城间第閏日志		2016-06-16 23:17:02	新元00	阳断	Trust	Untrust	192.168.1.2	183.60.49.183	50533	443	Tencent QQ Login Request(TCP)
- IPS日志		2016-06-16 23:17:02	勝讯00	阳断	Trust	Untrust	192.168.1.2	119.147.32.229	50535	443	Tencent OQ Login Request(TCP)
一防病毒日志		2016-06-16 23:17:02	10万元报	REAL	Trust	Untrust	192.168.1.2	183.60.49.183	50532	80	Tencent QQ Login Request(TCP)
一府容温控日志		2016-06-16 23:17:02	展示00	阳断	Trust	Untrust	192,168,1,2	119.147.32.229	50534	80	Tencent OQ Login Request TCF
-ESA GREAT		2016-06-16 23:17:02	105.5番	同新	Trust	Untrust	192.168.1.2	111.161.52.177	4031	8000	Tencent QQ Login Request(UD
-URLH#RE	100	2016-06-16 23:17:02	勝元00	陶新	Trust	Untrust	192.168.1.2	220.249.245.124	4030	8000	Tencent QQ Login Request(UDP)
- Userlog日ま	×	2016-06-16 23:17:02	四万元隆	阳断	Trust	Untrust	192.168.1.2	119.147.45.203	4029	8000	Tencent QQ Login Request(UDP)

1、策略在做上去后,对于已经登录的QQ、已经下载的是没有作用的。

COLUMN CO	20	语: 发起为事iP地址	▼ P#1:		重调				(474-1-1623) 1
NAZIS III OVERS III	0	家庭方面中地址	827039984	RE5 VPN/VLANI PKINE	-	RETERMEN	RETS VPN/VLANJ INUNE	39 KR	●qq õ [©] =
1.朱國	0.	92,168.1,1:00	192 168 1 2 50371	-	192 168 1 2 50371	192.168.1.1.80	-	TOP	HIC 9 T ms
安全知暇	01	92.168.1.2.50235	112.90.83.23.80	-	112.90.83.23.80	192.168.124.6.3318		TOP	13C Differ TRANK
TARI I CALER		92 168 1 2 50236	112 90 83 23 80	- 1	EAST-		-	*	ACC-188
APPENDER .	01	25.39.240.113.443	192.168.124.6.3179	420000					RE-REA. STOR. P. 25
APPER	01	12.65.192.34.80	192 168 124 6 3243						0.000000000
ARPESIE	0,	92.168.1.2.50372	112.65 192.34.80	-		0 00			1
QoS	n ,	92 168 1 2 50373	192,168,1,1,80	_		1 3 QC)		I H M M M L
1222	0.	92 168 1 2 50334	112 65 192 34 80			45			> \$8294246 1/2
CALL .									~ \$\$\$\$167.5% LIS1/243
11110750 111508				1				1	Lane Lane
2007							-		HBC NL BRO TERES
ANDER					Har	2/18805385			A CONTRACTOR DE LA CONTRACTÓRIA DE LA CONTRACTÍRIA DE LA CONTRACTÓRIA DE LA CONTRACTÓRIA DE LA CONTRACTÓRIA
di@leit					STREET, ST.		CD MORE	813	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1673					0	2 纪在常時 ()	日の設定		
T.S. S. THE						STREET, STREET, ST. ST.			🗶 सरम 🚥
网络					1.				2016-06-13:季机直接上面可以用
CERTIFIC AND					-	的网络成者本机动大律说	п.		STA STATE
NUM 7THR					数据G-2000000001				/vp/SHETHERENAS ALMOTA
									0.9.0.2.8
m daim.									The state of the second

- 2、防火墙在过滤迅雷、QQ等应用时,需要将防火墙设置在UTM模式。
- 3、如果发现无法过滤相关应用时请及时更新特征库。
- 4、使用自动升级的时候需要保证您的设备开启了DNS代理,并设置了DNS服务器地址。
- 5、特征库是需要维护的,我们会在定时更新特征库。如果发现自动更新请等待一段时间后再去更新。