陈斌A 2007-03-23 发表

XLog F0204和SecPath1800F配合接收Flow日志的典型配置 一 组网需求: XLog V2.10-F0204, SecPath1800F XLog和SecPath1800F路由可达,用户能和外网互通。 二 组网图: SecPath1800F WAN LAN 202.1.2.22 XLog 192.168.0.16 SecPath1800F Comware, V3.40-R0357.02(08) XLog V2.10-F0204 三 配置步骤: 3.1 配置设备 # 置防火墙域间记录Session的ACL acl number 2000 rule 0 permit source 192.168.0.0 0.0.0.255 #配置日志类型和XLog的地址、端口 firewall session log-type binary host 192.168.0.16 9020 #将内网接口加入信任域,将外网接口加入不信任域 firewall zone trust add interface Ethernet1/0/1 firewall zone untrust add interface Ethernet1/0/0 # 将域间的session进行日志记录 firewall interzone trust untrust session log enable acl-number 2000 inbound session log enable acl-number 2000 outbound #确认设备时间 dis clock \\查看设备当前时间是否正确,若不正确请修改 3.2 配置XLog 3.2.1 请先确认Windows系统的时间和时区正确。 3.2.2 在Windows的服务管理中停止XLog的两个服务: H3C Xlog Server ; H3C XLog Web Server 用记事本打开配置文件:\H3C\XLog\conf\sysreceiver.xml,修改该文件 3.2.3 的如下参数由0改为2: <BinaryLogProcessMode>0</BinaryLogProcessMode> 3.2.4 启动XLog的两个服务。 登陆到XLog配置管理平台: <u>http://192.168.0.16/xlog</u> 3.2.5 3.2.6 点击左侧菜单中的<日志服务管理> <服务配置>,出现如下的配置界面:

	Distributer htt		-1 84 million
19 ft	告: ADMIN (127.011) 登録的号: 2007年3月21日 星球三 アキ02年35分の形		帮助 关于 1
	日志服兵管理 服兵動重		
PERSONAL PROPERTY AND INCOME.			
- HUNHE	服务配置		
DOM DE	公共位意		
INCOME VILLE	* 抗療薬F1621 192100.0.10 * 系統含要:	新年史 1998年 1998年年年年 1998年	
	FTPEH: FTPEH: [
IN THREE IS	FTPEB#:		
HITOSSES.	oRea		
	世界内内NK(内内の子内構成)		
1000	1982 168 0.0/266 366 366 0		
S B S B C B			
NACT SALET ALLET ALLET ALLET DALEN SALEN SALEN SALEN SALEN			
NACT SAUN AGESTIN CATENI CATENI CATENI SALANTISE SALANTISE	Refat		
NARCE SILVE ANDER MADE MAD MAD MAD MAD MADE MADE MADE MAD	Refits If All Honology Metter FLOWER Dotte	NetStraw	e vida
RANCE RAISE ADDET	Reas B Structure ville write FLowite Dodde	NetStreet	- Mille
	RASE If BRHOTHANNINES WITH FLOWER DOOLS RASE RASE	Nilliter	with a second
		NiChea	wda
B ments Start Machan B dogarth Machan B dogarth D dogarth D dogarth B salasta B dogarth B dogarth B dogarth B dogarth B dogarth B dogarth B dogarth	RASE BANNENNINIES NOTE LOODE RASE	Nettree	nvitit#

3.2.7 点击<修改>后配置相关参数,配置处理器地址(XLog 服务器的地址),添加内网网端,选择Flow日志菜单,增加接收器。

	'al-g/wein jef						-) 23 HM
# 11 2	1 ADMIN (127.0.0.1)	放射的词:2007年3 月	21日 麗観三 万中028	1359-018			帮助 关于
	日志振奏管理 新兵委道 服务修订						1.011100000
maasa	40						
LONTE				NAME:			
DOMPLE	2 848			- Aller			
A DRAWNING	* 他想新FIB社: 1921682.10			> 系统音響:	秘密不统击型	-	
N B N C	FTPRP:			FTPERA:			
NUMBER	(TPERM)						
H/10553	-						
CONTRACTOR OF STREET	ERARNE (ARD) FREE		#HEATS				
THE R. S.							
			P1612 : [112	168.0.21			
			FORMEN: 255.	266 265 1			
			100	RTN BEFK			
0.000	a dia seconda di second						
E SHORE	MAGE .						
A CONTRACTOR	F BRNetSteam VIES						
0.00000	NATES	FLOWE	ε	DIOBE	1	NetDream VSBE	
BARR.	* 漱山黄晦: 不进行聚业						
	RCBAR			Projector.			
	101 B 11 B		desirable and the second	and the second second			
	101038-0135						



10 Mig 200	CREW IAD MRS					2
14 (1) (1) herty //127 0 0 1	/slog/wwin.jsf					
	1 ADMIN (127.0.0.1)	数录时间: 2007年3月3	218 ##E YY02#350018			植物 关于 证明
	11回脚头管理 副兵動道 副兵利	107 1010 MILLION 754				
A NATES ANALESE A LOWER A COMPTON A NATIVAL A NATIVAL A NATIVAL	 一般の描字地址: 120月期日: 20月期日: 第人注意: 	 不进行过渡 	増加技会器			
B NUTERIT B HOUSES DEMANT B TONE D CONE D CONE D CONE D CONE	an a There a	858	NG 210	80×169	8554	
3.2.9	输入设备名称	r, IP地址,	选择设备时间处	理方式。		

ThepHPG Swith S = Biccouft Internet Repl 2002 Million 8600 CR () IAC Million			
ORE . O . O NE ORE C	0.42		
HENE (D) (here //127 0 0 1/sleg/wein jef			- 21 ten um -
# 作 热: ADMIN (127.0.0.1)	董泰纳词: 2007年3月21日	星観王 77年02時35分01世	和助 关于 证明
Prediction Monthle Monthle	- 说是态称: - 说是不知的日本向数: - 说是中地址: - 说是有地址: - 说是句明时间如何是想方式:	境施設各 [BecPark 1838 (
OLNASS OLNASS OLNAS OLNAS OLNAS OLNAS		RC ER	



1 IL	INE ORRA C D						
812 (2) (112T 0 0 L	aleg/main jef					· • • • • •	95.78
# 11 5	ADMIN (127.0.0.1)	放卵时间 = 2007年3	肉21日 単規三 アキ02月35分01世			相助 天日	7 0.1
U	日田副長智慧 副兵動道 副兵会注					191200	10
			增加接收器				
rumtiz	· ########	192 188.0.16					
DOMESS	·)222746 :	Territia	3				
MILEAN VILLE	+ geiegt :	9020.8621	多个确口用来文谱号分开				
1076	* 願入设备:						
D TOXALS	8.6	8858	被暴火的的狂怒思想	60744	4850		
10731470F	GF BecPatv1808	1	FLOWEI	202.1.2.22	Factorial		
21.7%	MILLION &						
			in the second second second second				

3.2.11 返回服务配置窗口,点击<下发>

ADMIN (127.0.0.1)	the second se				
and a second	董康的间1 2007年3月21日	建筑 世 予举02时35份01世			帮助 关于 住地
18日本管理 副兵制度 利助					-
		服务配置			
SREE • 2.9889612 : [192100.0.10 FTHEP : FTHEP :		• 2489 FT/EN	[2	
- 内門建業 日本内門均衡(内門小子門連絡) 192 100 0 0/256 256 256 0					
190 X 8					
R Behetbean Vills					
NATE:	FLOWBE	040B8	1	Netiliteen VSB&	
8748 • Rome: (Torrag	×				
建立模仿明					
	SHELE - SHELE - SHELE - SHELE - SHELE - SHELE - TYPE - TYPE - State - TYPE	BRSE • REBENSE • STREE • REBENSE • STREE • STREE • PRESE • STREE • STREE • PRESE • STREE • STREE • REBENSE • STREE • STREE • REBENSE • STREE • STREE • REBENSE • STREE • STREE	RSACT ARRE KRACT ARREFIGE: 112 (10.216 TYTAGE: YTTESH TYTESH: TYTESH TYTESH: TYTESH: TYTESH: TYTESH:	BASE Eght2 2 REB * XMR® : IF U (12:0) 179288 : * 779281 : * 779281 : 179288 : * 779281 : * 779281 : 179298 : * 779281 : * 779281 : 179298 : * 779281 : * 779281 : 179298 : * 779281 : * 779281 : 179298 : * 70928 : * 60928 : 180 : # 60948 : * 60928 : 180 : * 60948 : * 60948 :	BANK BANK 2.952 BANK 2.952 SAR# 1.952 Partial 1.952

3.2.12 接下来会弹出下发的情况。

200 mig 200	O CORD IAO MINO			
S	S . RE CORR C	• U G		
12 (1) Attp://127 0.0	1/slog/wwin.jef			- C] ++21 48.00
	# 1 ADMIN (127.0.0.1)	新新和6号: 2007年3月21日 MA	E 740201359018	税助 关于 凹
2 C C C C C C C C C C C C C C C C C C C	1 DEMANS MANE	847x	e son de la companya en com	
			处理器配置下发情况	
ILONGE	and the second second	BE BPILL	73	14.9
Dout Ba	192 188.0.18	Constant Constant	Testa	
			接收器配置下发情况	
nevento		服装置の構築	75	ISB IF
a mressis	192160.016		78.63	
TITES ILLERS			各書配置下发情况	
		BABPINE	75	15.8
C MILDING	192188.0.18		TRAD	
			8.2	

3.2.13 确定后再通过<检测>确认处理器和接收器的运行情况:

· 根約: 未干 行状态
行铁态
行状态
20X8 2000
2018
行状态
8086 7868
注任法 集
1

3.2.14 点击<详细信息>可以查看具体情况:

200 880 880	CREW IAU MRO					
0.88 - 0 - 0.2 1	NE CREA C					
雑葉(型) 副 1449 //127 0 0 1/	alog/wain. jaf					· 2 PR 48
# 11.5	ADMIN (127.0.0.1)	意味が同: 2007年3	月21日 副規定 アギウ2町35分01			세하 关于 년부
87. E • •	·····································	(M)				
			处理器》	行状态		
C FLOORE		4.00-16.16	10000	2028	245 <u>8</u>	
COLUMN	192180.018		政行正常		ERR	
			放牧器 3	行状态		
NOVEMENT		15 ID # 14 12		800A	ance	
D HANANT	392 188 0 18		RUER		建建筑	
			100			

3.2.15 (此步不是必需)通过抓包确认设备已经正常发送UDP的日志报文到指定端口(9020)。



3.2.16 (此步不是必需)经过一段时间后,在Vreceiver_data又件来下能发现Flow 日志报文。

NALS -

 Note:
 Construct Also

 Strip:
 Stri

3.2.17 正常情况下再经过10分钟后就能在XLog的控制台上查询到Flow日志: (请注意查询的结束时间需要比当前时间晚):

7 0 0 1/slog/wwis. jsf									2 HDI 44 W
# # # # ADMIN (127.0	(£1)	新建##5号: 2007年3月21日 MA	RE 774058(28)278						相助 关于 迂转
Platewit	++ FLOWER	201051300007940525105	eest an week w			_			
415			医 间的脉管 从	2007-03-19:00:00 🖽 2007-	03-21 17 69	- #4	10.0 10.0		20.00
36278	1.8L 11.#IZP+.M	। ज					50	10. W	
	ITRACE	SLOPPH	EPIL V	B.BPRAN.M.S.	10094600	6160)	-	1112	25944
2007-03-2	1 88 45 (54	2007-03-21 80 45:24	182108.016	2021221	23	4391	TOP	E R.M.	192168.01
3007-03-2	1.00.45.30	2007-03-21 08:45:32	192 160 0 16	202.1.2.23	612	2048	KWP 1	利利间 春秋道 己筆	192166.01
3007-03-2	1 0645/04	2007-03-21 00:45:00	192100.016	202.1.2.23	23	4301	TCP	日町间 今夜流 己筆	192.168.0.1
2007-03-2	1 00:45:30	2007-03-21 08:54:24	192 100 0 16	202.1.2.23	612	2048	ICMP .	同門主	102168.01
2007-03-2	1 00:09:44	2007-03-21 09:09:50	192160.0.18	202.1.2.23	22	4443	TCP	に対対 手度注 と見	192168.01
2007-03-2	1 08:07:28	2007-03-21 89:09:58	192.160.0.18	202.1.2.23	22	4442	TOP	FRA	192168.01
2007-03-2	1.09.09.44	2007-03-21 09:09:58	192168.0.16	202.1.2.23	22	4449	TCP.	EXIA .	192.168.0.1
2007-03-2	1 081001	2007-03-21 0910.08	192.168.0.16	202.1.2.23	012	2048	CMP 1		192.156.01
3007-03-2	1 09:10:01	2007-03-21 08:10:31	192.168.0.16	2021223	612	2048	KMP	ante -	192.168.0.1
2007-03-2	1 99:07 28	2007-03-21 89:07:31	192 168.0 18	202 1 2 21	23	844))	TOP	日田田	192 168.0 1
2007-03-2	1 0011:50	2007-03-21 09 12 22	182168.016	2021223	612	2048	ICMP 3	(intell	192168.01

3.3 配置聚合和过滤策略

为了减少日志占用空间,需要配置聚合和过滤,具体步骤如下:

3.3.1 点击<日志服务管理> <聚合策略>,进入如下窗口,点击左上侧的<增加> 创建聚合策略:

国11+6月戸行力率计系統一日	Siccord Internet Inglanat				
大师田 建酸田 建氟田	ORU IAU HRO				
0.88 . 0 . 0 . 2 .	RE CREA C	V 7			
總建築) (1/127 0.0.1/	falogfaain jef				· 2 Prill 48/8
# fl 25	1 ADMIN (127.0.0.1)	登録時间: 2007年3月21日 業業三 下午02月25分01世			Mith (4.7 U)
A	日本部委官僚 東山市場				
	1010 4120				
			2658:	*	重度 新花板市 重重
COMPLE COMPLE	*5310/122			15 . AKENS 🕡 🕻	00000
BREVIEW VERE	2528	116.9.8	7858	84	-
3 HERE				00	00000
A THE REAL					00000

3.3.2 输入聚合策略名称、日志类型,聚合粒度等。

	Alatiania ist	e			- 63 80 80
	1 ADMIN (127.0.0.1)	登録的第三 2007年3月21日	##E 74020359018		위하 유주 대체
87. E • •	日本部条管理 王:	1996			
			增加聚合策略		
Compliant Compliant Compliant Contract	- ##Qž	• 26658 : (TENT • ROLLE ROLLE • HARD		· B8用数: FLOWER	в
	R:: 67	F 8P82 F 80782 F 90782	다 Banks 및 다 Banks		
	Runz	- #1673 - 62978	的第名方式:「取用每日方项平的的最小值 的第名方式:「取用每日方项平的的最小值	2	

3.3.3 点击<日志服务管理> <过滤策略>,进入如下窗口,点击左上侧的<增加> 创建过滤策略:

1144日PG力率計系列 二 文件(2) 瞬間(2) 登号(2)	CRU IAD MRG				10
0.62 - 0 - 5 2 3	NE OREA C D.	4.9			
18 12 (2) ANTO //127 0 0 1	alog/sein jef				· · · · · · · · · · · · · · · · · · ·
***	1 ADMIN (127.0 0.1)	重要約6日: 2007年3月21日 単規三 アキ02873556018			帮助 关于 进入
	日本副兵管理 江北軍馬				
	NT ND				- e - e e - e
			3965B		查注 BUER 重要
DOMBIE	\$2RDBRR			15 . AURIT	000000
MILEN AVIE	3568	• B658	amta		82
1076					000000

3.3.4 输入策略名称、日志类型、对不满足过滤条件的日志的处理方式,再点击

注意: 这里的过滤策略必须慎重配置, 不要丢弃了有用的日志。



3.3.5 配置相关参数:

14 4 10 14 1/11 0 0	L/sl-g/eein jif					- 87 aut mit
10 M	B1 ADMIN(127.0.0.1)	國防國主 2007年3月21日 麗城世	740201359018			帮助 关于 注
	1日市部各管理	増加过成品作				
- mailgait			增加过滤条件			
FLOWTH	8148					
DOM NO.	* 洗燈方式: 損収	-				
	tidan .					
	9 APRULE	@F1812	192168.0.21	用户地址规则	258.255.255.0	
A NUME	F decide	2980				
0 0/10 3555	F HOPHEWICH	000Pittate		自动中枢征用导	[5
BERATE	E BORDIDE	IT answer:				
10ATE	E MAYLE	ME				
			DCMD			
C MILDING	S monthly	10200	TEP			
A NUMBER	- overalle		VOP			
21470			14 A.			
CHICKNE			M2 2.0			

3.3.6 确定,返回。

		BRANK - CONTRACT OF BRANK STRATCOURSE				
	日志服务管理 过度发展	1002436				440 AT
Rallswit wittle ricette boatte		增加过滤液略				
	- 35628: TT	T-Flow • Bas	R: FLOWER	Э		
INCOME VILLE	1000417	MERTER		2000		
NUNK NUNK	He.	10070620 1 102 160 0.0255 255 255 0 1002020 1 TCP		(1858.	-	RF4
ELMANT					N#7010	14419
1 TATE	* NT#EXIdeHold	erffra: « sa C me				

3.3.7 点击<日志服务管理>, <服务配置>, <修改>, 在Flow日志的聚合策略中选择刚创建的策略。

	L ADMINISTER N	BRANK : MATRIARIA B	THE TRACTORNER		
4 	1288497 84872 8466 425				
e de Nos			服务配置		
	公共成員 * 気度毎F時後注: [192100.0.10 FTF規則 P: FTF更直要: 	=	* \$155 FTPg	19: [#45K89] H: [-
14 14 12 12 15 15 15 15 15 15 15 15 15 15 15 15 15	2307008(00077083)		197571 192100021 1925250021 192525050 1926	1	
1.5 malle	IT BENetibean Vills				
0110	NATES	FLOWEIS	Billion	the	Eliterative State
1918	· 是非准备 • 附注附称: 「不进行相乐 · 按约路信息 - 还经行和乐 · 按约路信息 - 还经过	I HAT	6	1214-1420 服入语言	6 8.0 BN
	192 188 0 10	Feblue	9020,9	021 DecFabil0007	1532 Mile
	增加接收器				

3.3.8 在接收器选项中点击<修改>, <过滤策略>, 选择刚建立的策略:

0 82 · 0 · 0 2 ·	NE CORR C	17				- 21 10 40
# n 5	ADMIN (127.0.0.1)	10.0000 H 200	7年3月21日 麗城三 77年02月25分01世			Alb (17 12)
11 2 4	· · · · · · · · · · · · · · · · · · ·	的汉 师汉册代数				
NUTER NUTER NUMBE DURATES DURATES DURATES DURATES NUTER	· 陳の臣が地址: 12月7時日: - 出外地口:	[1923188.0] 不进行法』 不进行法』 百日元4月11日	●改臣牧器 1 5 5 (第22年555 5 (第22年555)			
NORMET	1.5		建备实件的目表类型	KOPIAN		
DIAMANT	12 BecPath10	1007	FLOWER	2021222	Fermat	
B TOTAL	a featar					

3.3.9 确定后返回服务配置页面,点击<下发>重新下发服务:

	/slog/weik.jst						- 51 HBI
# 11.7	1 ADMIN (127.0.0.1)	整要的词: 2007年3月211	日 麗観世 下学02时	359/018			税助 共行
	日本服务管理 服务配置						
IS NOT		118 56)		股外配置 • X ian参: FTPEH:	The survey	2	
HATEPEN HATEPEN DATEM CARDANE MATER MATE SUCCESS SUCCE	勝の回意 副 記号varitinaam V9日本 1941日本 - R会演編(1922	n.owBg		CecHig	Ŧ	Netiltean VSB\$	
	and the second se				E440	82.68	





- 四 配置关键点:
- 1. 正确配置设备和Windows系统的时间。
- 2. 修改sysreceiver.xml文件
- 3. 正确配置过滤条件。