Содержание

Конфигурация NAT Flow	3
Настройка получения отдельного потока NAT Flow с DPI или NETSTREAM	3
Включение импорта событий NAT из FullFlow	4
Агрегация NAT Flow	5

Конфигурация NAT Flow

Есть 2 способа формирования NAT лога в QoE Stor (сервере статистики) 1. Получать NAT Flow отдельным потоком с DPI. Для этого на устройстве DPI необходимо настроить экспорт трансляций на внешние коллекторы

2. Получить NAT Flow из Netstream сторонних систем (не DPI)

3. Формировать NAT Flow из FullFlow средствами QoE Stor

Настройка получения отдельного потока NAT Flow с DPI или NETSTREAM

- Перейти: Главное меню \rightarrow Администратор \rightarrow Конфигурация сервера QoE Stor \rightarrow Конфигурация сервера QoE Stor

Experts D	PI : SSG_Station -	
 BPI CONTROL SETURCES CONTROL 	RDIWARE MANAGEMENT / EQUIPMENT	
@ GOE ANALYTICS	· •	
W48 CLOUD SERVICES	Equipment	
ADMINISTRATOR	* E SOUPMENT	Host
>_ HARDWARE SSH TERMINAL	W USERS	- Q. Titler
-1-	6 & ROLES	192.165.2.200
(GUR) update	CPILI2 (GUI) SERVER CONFIGURATION	127.0.0.1
or (feator) server configuration	C D GOE STOR (FASTOR) SERVER CONFISURATION	R (FASTOR) SERVER CONFIGURATION
or (fastor) logs	I PAST PORF (PASTPORF) SERVER COMPIGURATION + & QOE STO	R (FASTOR) LOGS
:RF (lastport) server configuration		
CRP (Instport) loga		

- Перейти в раздел "Ресиверы"; добавить новый рессивер; выбрать "Тип ресивера" - NAT Флоу; дозаполнить форму добавления ресивера и нажать кнопку "Применить"

Адиинистратор Э конфигурации дос stor																			0-0	0		
Конфигурация																				>		
🖞 Coxponents tà 🕀 🕲		e											форна			Ф Редактор						
Рь Настройки	0	© Ресмери																				
Ресиверы	+	_	ц D	2	12																	
бильтроция	1	Tien p	ecveep	a			Тип пор	710				Парт				Cydi	() Ten	() Serv	⊙ Ho			
Общие		NAT @noy ~		v S top			~	® 1500			0		top			0						
Настройки Uir	11	иотоция в минутох 10 Зодержка в секундах					и стоция в минутох	0	Ротация в секундах				٢	Potouxe no @noy			0		tcp			Ð
Настрайки журнала FULLFLOW							адержка в секундах Разнер с					число процессов вставки					top			0		
Hoctpołke wypeono PULLPLOW AGG		0				0	10				٢	0			0		top		9	D		
Настрайки журнала СЫСКЕТВЕАМ АЗВ		Okonopt 10.0.0.2/9920/tep.10.0.0.3/3440/			Околорт Идентнерика 10.0.0.2/9920/top;0.0.0.3/3440/ Ф -1 Субресиверы болонсира Тип субприек				фикатор	» ОРІ еков балансир		٢	болонсир Отключено ч					tcp			0	
Настрайки журнала NAT		Субреснееры болонсира							приенна		энсира	~	Балонсир авто				top			0		
настрайки журнала СМ.IMEPLOW		10.0.0.2/9920.10.0.0.3/3440				10.0.0.2/992030.0.0.3/5440 0 top					0	D 0110/10/10/10/10		, 0		tcp			Ď			
Настрайки журнала DNS АGG		0	ip napro	001000	npu	۲											tep			0		
Настрайки OpenCellD										OTHE				Coverence of the			top			0		
настройки сервиса обора ананалый в ОЛР																	tcp			0		
Настрайки сервиса обора статистики UPLINK LOAD RA	n 2	0	Клинст	η tep	15013	2	0	0	400	10		0		30			top			0		
Список зараженных востов Косперского	2	ø	NAT ¢	v top	1900	10	0	0	0	10		0		10			top			0		
Настрайки кластера	8	0	DNS d	w tep	15014	1	0	0	0	10		0	100.134	30			top			0.		

- Перейти в раздел формы "Настройки журнала NAT";
- Включить заполнение привязки IP-LOGIN из fullflow (FILL IP LOGIN BINDING FROM FULLFLOW);
- Включить добавление LOGIN в журнал NAT из привязки IP-LOGIN

(NAT_ADD_LOGIN_FROM_IP_LOGIN_BINDING)

конфигурация												
m Coxponents ta @ 19	С 🖬 форма 🚸 Редактор											
9 ₆ Ностройки	В Настройки журнало NAT											
Росиверы	Инпорт событий NAT на fulfiow (NAT_IMPORT_FROM_FULLFLOW)											
Фильтрация	Включено											
Общие	Tions gus coxponences non or pervecences systems NAT (NAT_ADD_LOD_FELDS_TO_SAVE_BITMASK)											
Настройки Uir	Ох1 - Ю протокола, 0x2 - Тип события, 0x4 - IPv4 адрес источенка, 0x8 - Порт источенка, 0x10 - IPv4 адрес палучателя, 0x20 - Порт	`										
Настрайки журнала FULLFLOW	Интервал вретени для огранирования логов NAT (NAT_AGG_LOG_GROUP_TIME_INTERVAL)											
Настройки журнала PULLPLOW AGG	ar menyi çina yinan wennoy	_										
Настрайки журнала СЫСКВТЯБАМ АЭВ	Bickovertu sononeevee npizekskii IP-LOGIN va fulffow (FILL_IP_LOGIN_BINONG_FROM_FULLFLOW) Bickoveno											
Настрайки журнала NAT	BK/MOVETINE JOŠGISINENE LOGIN IS XXXXHON NAT WS TOMBROSKI IP-LOGIN (WAT_ADD_LOGIN_FROM_IP_LOGIN_BINDING)											
настройки журнала ОМ.INEPLOW	Включено											
Настрайки журнала DNS AGG	Использовать роспределенную таблицу привезки IP-LOGIN (NAT_USE_DISTR_IP_LOGIN_BINDING)	_										
Настройки OpenCellD												
настройки сервиса обора аноналий в 87Р												
настрайки сереиса обора статистики UPLINK LOAD RATE												

Включение импорта событий NAT из FullFlow

Для включения импорта событий из FullFlow, передаваемого с DPI в QoE Stor: - Перейти: Главное меню → Администратор → Конфигурация сервера QoE Stor → Конфигурация сервера QoE Stor

 BPICONTROL SERVICES CONTROL 	WOWARE WANAGEMENT / EQUIPMENT	
GOE ANALYTICS		
ADMINISTRATOR	E COURMENT	Host
> HARDWARE SSH TERMINAL	W USERS -	Q, Filter
IUI) update	A ROLES DPUI2 (GUI) SERVER CONFIGURATION SERVER CONFIGURATION	192.168.2.200
(festor) server configuration	GOE STOR (FASTOR) SERVER CONFIGURATION	SERVER CONFIGURATIO
(fastor) loga	IN PAST PORF (PASTPORP) SERVER COMPIGURATION · & QUE STOR (FASTOR)	1008
r (fastor) server configuration r (fastor) logs	OOE STOR (FASTOR) SERVER CONFIGURATION OOE STOR (FASTOR) OOE STOR (FASTOR) A QOE STOR (FASTOR)	SERVER CONFIGUR

- Импорт событий NAT из fullflow (NAT_IMPORT_FROM_FULLFLOW) - Включить

банфигурация		
D Cooperans ti @ 19	12 🖬 форма — 🚸 Редактор	
ь настройол	В Настройки журнало NAT	
Ресиверы	Инперт событий NAT из fullflow (NAT_IMPORT_FROM_FULLFLOW)	
бильтрация	Включено	×
общие	Tions give coxponences now orpervepeedness scyphions NAT (NAT_AGG_LOG_FELDS_TO_SAVE_BITMASK)	
ностройки Ulr	0s1 - ID протокола, 0x2 - Тип события, 0s4 - IPv4 адрес источника, 0x8 - Порт источника, 0x10 - IPs4 адрес получателя, 0x20 - Порт	×
іастрайки журнала FULLFLOW	Mintepean aperionic dure or perioposonice INAT (INAT_AGG_LOG_GROUP_TIME_INTERNAL) 15 Minutr (To ymoneseno)	
tectpolikik журнеле PULLPLOW AGG		
астрайки журнала СЦСХЕТВЕАМ АЭВ	Biotenems sonaneeree привежи IP-LOGIN из fulfflow (ITLL_IP_LOGIN_BINDING_PROM_FULLFLOW) Включено	
Кастрайки журнала NAT	Bicnoverts goficeneeve LOGIN a xyphon NAT из привлам IP-LOGIN (NAT_ADD_LOGIN_FROM_IP_LOGIN_BINDING)	
астройки журнала ONLINEPLOW	BK/IIOVIEHO	v
астрайки журнала DNS AGG	Использовать роспряделенную таблицу привяжи IP-LOGIN (NAT_USE_DISTR_IP_LOGIN_BINDING)	
юстройки OpenCellD		¥
астройки сервиса обора аноналый в 87Р		ħ
іостройки сервиса обора статистики UPLINK LOAD RATI		
писок зараженных востов Косперского		

Агрегация NAT Flow

Перейти: Главное меню \rightarrow Администратор \rightarrow Конфигурация сервера QoE Stor \rightarrow Конфигурация сервера QoE Stor

-	WAS Experts D	PI :	SSG_Station -			
	E DPICONTROL C SERVICES CONTROL	;	VROWARE WANAGEMENT / EQUIPMENT			
	COR ANALYTICS		+			
	WAS CLOUD SERVICES	-	F Equipment			
	ADMINISTRATOR		III EQUIPMENT			Host
PIU	> HARDWARE SSH TERMINAL		48F USERS		~	Q, Titler
PIU.			& ROLES			192.168.2.200
PIUQ	(GUI) update		E DPUI2 (GUI) SERVER CONFIGURATION	300		127.0.0.1
oE 59	or (fastor) server configuration		GOE STOR (FASTOR) SERVER CONFISURATION		QUE STOR (FASTOR) 5	ERVER CONFIGURATION
oE Sa	or (Eastor) loga		RAST PORF (PASTPORP) SERVER COMPIGURATION >		QOE STOR (FASTOR) L	008
int PC	CRF (lastport) server configuration					
nt PC	CRP (Isolperf) lags					

Выбрать "Настройки журнала NAT" → Выбрать поля для сохранения при агрегации журнала NAT, Интервал времени заполнения лога (по умолчанию 15 минут), включить заполнения привязки IP-LOGIN

📧 John Smith 🗸 🗰 EN 🖌 🖉 🖉 🖉 💿 🛛 🛛 V2-17.17 Big VAS Experts DPI : SSG_Station -ADMINISTRATOR / GOE STOR (WSTOR) SERVER CONFIGURATION II Epipment 2 G Belen B fave 15 4 Edu er Users INT log sellings 40 Settings A Roles Import NAT events from fulfilese (NAT_MPORT_PROIL_PULLPLON) Enabled Receivers III 0PU2 (SU) server configuration , Ø Filtration a crockings Common Fields to save inten appropring NAT log (NAT_AGG_LOG_PELDS_TO_SAVE_BITMASK) Bit1 : Protocol ID, Stid - Boarce PrvI, Se130 - Secolar ID, Bid30 - DPI ID . O Un settings 8 DPL82 (0.0) update Coli Stor (betor) server configuration PULL/PLOW log settings Time interval for appropring NAT logs (NAT_AGG_LOG_SROLP_TIME_NTERNAL) 15 minutes (5) default) , Ø at GoE Stor (faster) lega CLICKSTREAM log-settings Enable filling IP-LOGIN bind from fullfore (FEL_JP_LOGIN_BINDING_FROM_FULLFLOW) Toubled III Fast PCRF (tastport) server config-NAT log settings . O & PastPOTP (Indpot) logs Evaluation of the State of the , ©

Сохранить изменения и перезапустить сервис.