ITSF XII ВСЕРОССИЙСКАЯ КОНФЕРЕНЦИЯ

Техническая диагностика межсетевых экранов Check Point

Роман Жерихов
ICL Системные технологии

Программа

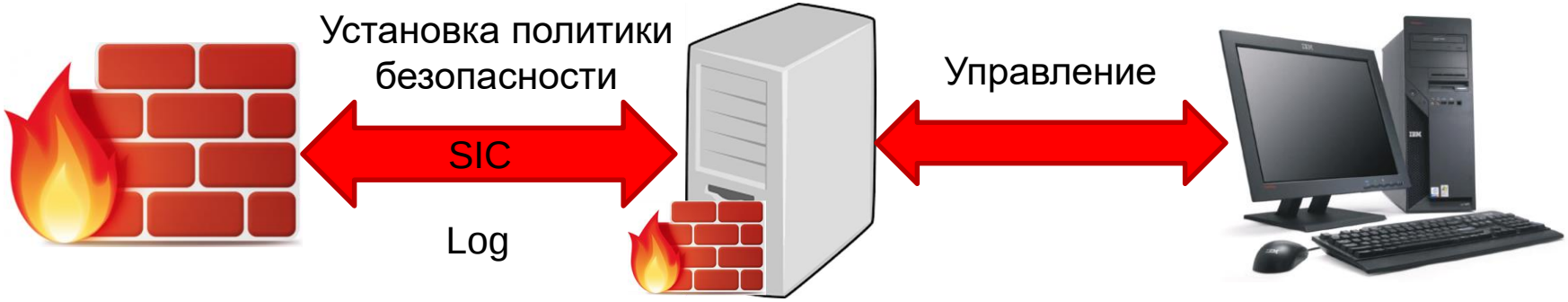
1. Процессы и файлы диагностики
2. Kernel Debug
3. Kernel Tables

Check Point
SOFTWARE TECHNOLOGIES LTD

Программа

1. Процессы и файлы диагностики
2. Kernel Debug
3. Kernel Tables

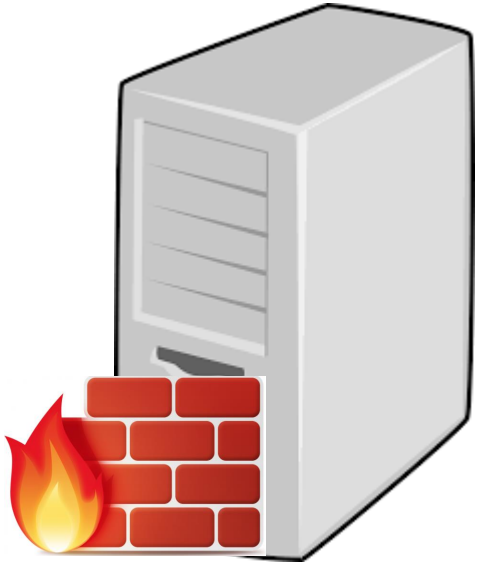
Процессы и файлы диагностики



Основные процессы МЭ

fwd	Модуль Firewall: Логирование и вызов дочерних процессов МЭ
vpnd	Модуль IPSec VPN
cvpnd	Модуль Mobile Access Blade
dlpu	Модуль DLP: Получение данных
rad	Application Control, URL Filtering
ted	Модуль Thread Emulation : эмуляция файлов и взаимодействие с облаком

Основные процессы сервера управления



fwm	Подключение Smart Console (CPMI), взаимодействие с БД, компиляция политики безопасности
fwd	Отправка и получение логов
cpd	Установка политики безопасности, проверка SIC, информация о состоянии устройств
cpca	Взаимодействие с Internal CA
cpwd	Мониторинг состояния процессов

Запущен ли процесс?

```
# cpwd_admin list
```

Имя процесса | PID | Состояние (E-enabled) | Количество запусков | Время запуска процесса | Команда для запуска

```
APP          PID    STAT  #START  START_TIME                MON  COMMAND
CPVIEWD      314    E     1       [07:48:45] 18/8/2017      N    cpviewd
CPD          317    E     1       [07:48:45] 18/8/2017      Y    cpd
FWD          406    E     1       [07:48:47] 18/8/2017      N    fwd -n
FWM          21308  E     1       [17:27:53] 16/4/2018      N    fwm
STPR         411    E     1       [07:48:47] 18/8/2017      N    status_proxy
SVR          534    E     1       [07:48:47] 18/8/2017      N    SVRServer
CPSEAD       2103   E     1       [13:39:45] 23/4/2018      N    cpsead
```

Диагностика работы процессов

Файлы диагностики (<имя процесса>.elg) процессов Check Point обычно расположены в директориях $FWDIR/log и $CPDIR/log.

1. Запустить дебаг:
fw debug fwm on TDERROR_ALL_ALL=5

2. Воспроизвести проблему

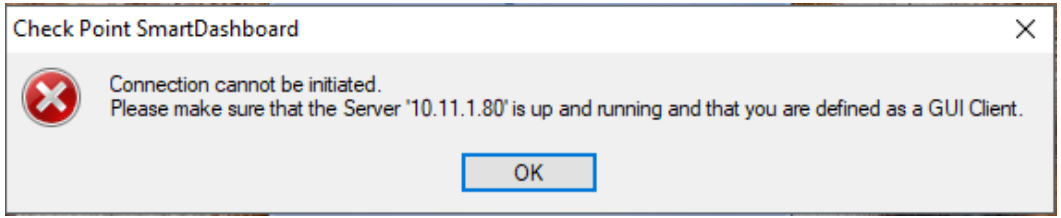
3. Остановить дебаг:
fw debug fwm off TDERROR_ALL_ALL=0

$FWDIR/log/fwm.elg

sk97638 – Check Point Processes and Daemons

Пример

При запуске Smart Dashboard возникает следующая ошибка:



Шаг 1

Разрешено ли подключение с рабочей станции:

- добавлен ли адрес рабочей станции в список для подключения клиентов (GUI Clients);
- Не блокируется ли подключение с рабочей станции до сервера управления по порту 18190 (CPMI).

Пример

Шаг 2

Проверить запущен ли процесс fwm:
#cpwd_admin list

Процесс fwm запущен

Процесс fwm не запущен

Шаг 3.1

Проверить сертификат на сервере управления:
cpca_client lscert –dn ‘cn=cp_mgmt’

Шаг 4.1

Собрать дебаг процесса fwm:
fw debug fwm on TDERROR_ALL_ALL=5

Шаг 3.2

Удалить файлы
$FWDIR/conf/CPMIL*
$FWDIR/conf/applications.C*

Шаг 4.2

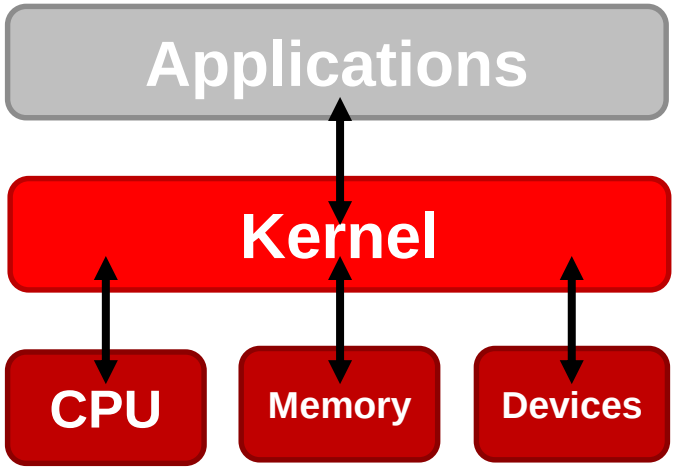
Запустить fwm в режиме дебага
#Export TDERROR_All_ALL=5
#fwm –d &> <название файла>

Программа

1. Процессы и файлы диагностики
2. Kernel Debug
3. Kernel Tables

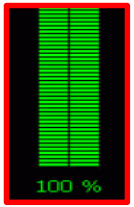
Kernel Debug

Определяет как операционная система и программное обеспечение взаимодействует с аппаратными компонентами.



Kernel Debug. С чего начать?

Учитывать влияние на производительность



CPU Usage

Установить параметры дебага по умолчанию

fw ctl debug 0

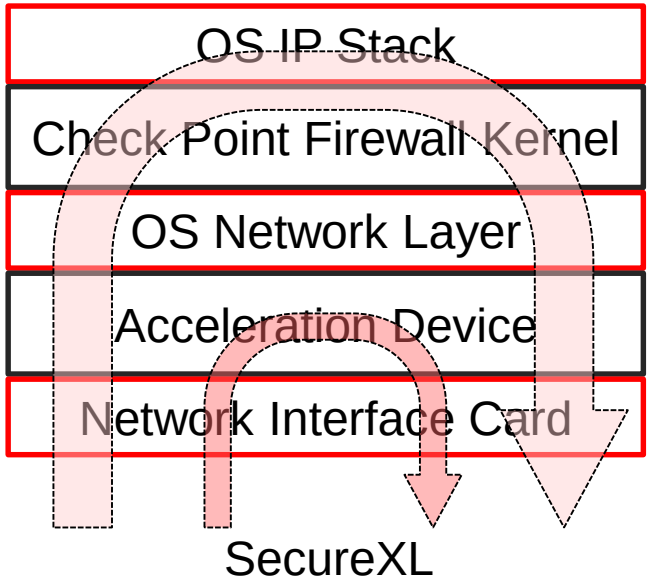
Увеличение размера буфера дебага

fw ctl debug –buf 32768

Kernel Debug. С чего начать?

Выключение SecureXL

```
# fwaccel off
```



Kernel Debug

```
# fw ctl debug -m <module name> + flag1 flag2 flag3
```

Активные модули на межсетевом экране:

```
# fw ctl debug -m
```

Запуск Kernel debug

```
# fw ctl kdebug -T -f > <имя файла>.dbg
```

sk98799 – Kernel Debug

Kernel Debug. Программные модули

Модуль	Описание
fw	Модуль Firewall
Multik	Модуль CoreXL
Dlpk	Модуль DLP (Data Loss Prevention)
cluster	Модуль ClusterXL
cmi_loader	Сигнатуры IPS
RAD_KERNEL	Категоризация ресурсов
APPI	Модуль Application Control
VPN	Модуль VPN

Kernel Debug. Флаги

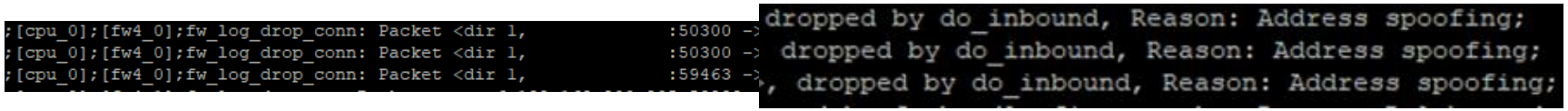
Флаг	Описание
drop	Заблокированные соединения, причина блокировки
conn	Информация о соединениях (направление пакетов, ip-адреса, порты)
xlate	Основная информация по NAT
xltsrc	Расширенная информация по NAT (включая информацию о политике NAT)
aspii	IPS

fw ctl zdebug drop

Запуск дебаг с автоматическими параметрами (с использованием одного флага)

fw ctl zdebug –m <modulename>+ flag

fw ctl zdebug + drop



Kernel Debug. Пример

Пример запроса:
Не устанавливается политика на межсетевой экран с ошибкой
Load on module failed – no memory

Шаг 1

```
[Expert@FW]# df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/sda6             1004M  214M  740M  23% /
/dev/sda1              145M   11M  126M   8% /boot
/dev/sda5              3.4G  1.1G  2.2G  33% /opt
/dev/sda2              1.5G  569M  862M  40% /sysimg
/dev/sda7               52G  1.5G   48G   3% /var
```

Kernel Debug. Пример

Шаг 2

cat /proc/meminfo | grep Vmalloc

```
[Expert@FW]# cat /proc/meminfo | grep Vmalloc
VmallocTotal:   116728 kB
VmallocUsed:     47448 kB
VmallocChunk:    54324 kB
[Expert@FW-P01]#
```

Kernel Debug. Пример

Шаг 3

fw ctl debug -m fw + filter

«;[cpu_3];fw_rules_uid_handle_uid: couldn't allocate dictionary string id for rule no. 40»

Программа

1. Процессы и файлы диагностики
2. Kernel Debug
3. Kernel Tables

Kernel tables

Check Point kernel tables содержат различную информацию о текущих соединениях, о узлах сети, о пользователях и т.д.

Список всех таблиц доступен в выводе команды

```
# fw tab
```

Для просмотра таблицы:

```
# fw tab -t <table name/table ID>
```

connections

fwx_alloc
fwx_cache

string_dictionary_table

Таблица соединений

Просмотр таблицы соединений

fw tab -t connections

fw tab –t 8158

```
[Expert@gw-940120:0]# fw tab -t connections
localhost:
-------- connections --------
dynamic, id 8158, attributes: keep, sync, aggressive aging, kbufs 17 18 19 20 21
 22 23 24 25 26 27 28 29 30 31 32 33 34, expires 60, refresh, , hashsize 32768,
limit 25000
<00000001, 0a0b0292, 00000a70, 0a0b0201, 00000000, 00000001, 00020001, 00006000,
 00000000, 0000001e, 00000000, 5b852c7e, 00000000, 92010b0a, c0000000, ffffffff,
 ffffffff, 00000002, 00000002, 00000000, 00000000, 00008004, 00000000, 00000000,
 00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000,
 00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000; 27/30>
<00000000, 0a0b0201, 00000000, 0a0b0292, 00000a70, 00000001> -> <00000001, 0a0b0
292, 00000a70, 0a0b0201, 00000000, 00000001> (00000006)
```

Переполнение таблиц

Пример запроса:
После очередной установки политики стала пропадать связь с сетями, которые терминируются на кластере Check Point, в том числе доступ в сеть Интернет

В логах МЭ:

;[cpu_3];[fw4_0];fw_log_drop_ex: Packet proto=17 xxx.xxx.xxx.xxx:62529 -> xxx.xxx.xxx.xxx:53 dropped by fwconn_memory_check Reason: full connections table;)

Переполнение таблиц

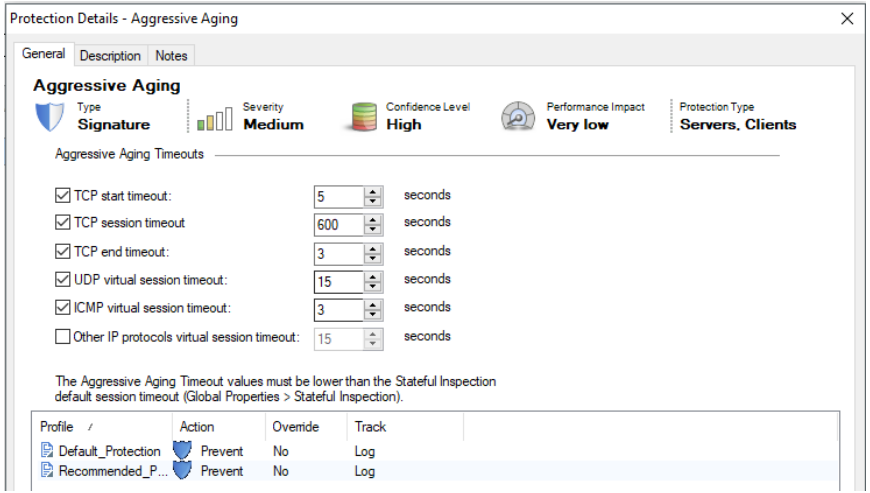
Просмотр количества соединений

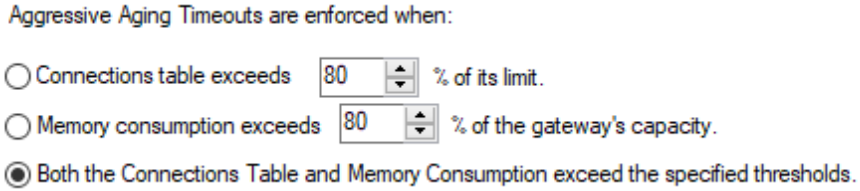
[Expert@fw]# **fw tab -t connections -s**
HOST NAME ID #VALS #PEAK #SLINKS
localhost connections 8158 **29493 30000** 107742

Проверка максимального количества соединений

[Expert@fw]# **fw tab -t connections | grep limit**
dynamic, id 8158, attributes: keep, sync, aggressive aging, kbufs 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34, expires 50, refresh, , hashsize 131072, **limit 30000**

Aggressive Aging





[Expert@fw]# fw ctl pstat | grep Aggressive
Aggressive Aging is not active

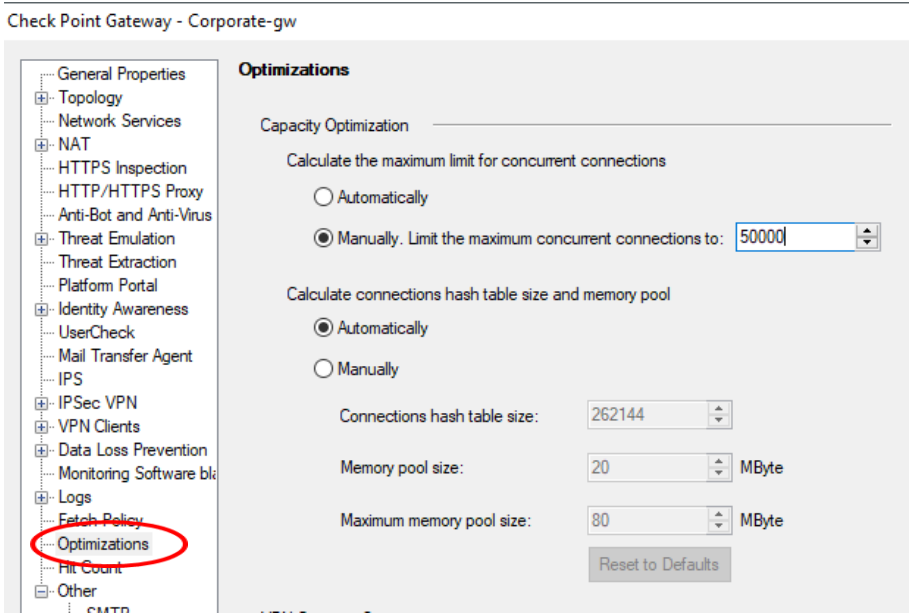
[Expert@fw]# fw ctl pstat | grep Aggressive
Aggressive Aging is active

[Expert@fw]# fw ctl pstat | grep Aggressive
Aggressive Aging is disabled

[Expert@fw]# fw ctl pstat | grep Aggressive
Aggressive Aging is in monitor only

Количество соединений

Установка максимального количества соединений



Как очистить таблицу?

Для удаления всех записей в таблице соединений:

[Expert@fw]# **fw tab -t fwx_alloc -x**
[Expert@fw]# **fw tab -t fwx_cache -x -y**

Kernel Debug. Пример

Шаг 3

fw ctl debug -m fw + filter

«;[cpu_3];fw_rules_uid_handle_uid: couldn't allocate dictionary string id for rule no. 40»

```
[Expert@FW]# fw tab -t string_dictionary_table -s
HOST                 NAME                          ID #VALS #PEAK #SLINKS
localhost            string_dictionary_table         8135 32768 32768       0

[Expert@FW]# fw tab -t string_dictionary_table |grep limit
dynamic, id 8135, attributes: keep level 2, kbuf 1, expires never, limit 32768
```

Программа

1. Процессы и файлы диагностики
2. Kernel Debug
3. Kernel Tables

Check Point
SOFTWARE TECHNOLOGIES LTD

Спасибо за внимание!