s•terra®

Ваш ориентир в мире безопасности

Версия 4.3

С-Терра Шлюз, С-Терра Шлюз DP

Дмитрий Махоткин,
пресейл инженер,
dmahotkin@s-terra.ru
+7 (499) 940 9001 доб. 181

Москва, 2021

План вебинара

s•terra®

Функциональные возможности С-Терра Шлюз/С-Терра Шлюз DP

- Преимущества архитектуры IPsec VPN;
- Навязываемые мифы о IPsec VPN.

Основные изменения в версии 4.3

- **Дешевле.** Новая продуктовая линейка;
- **Производительнее.** Новая продуктовая линейка, **40 Гбит/с** ГОСТ шифрования на паре шлюзов;
- **Функциональнее.** Новые сценарии для С-Терра L2: full-mesh l2vpn, отказоустойчивость и Active/Active кластеризация;
- **Удобнее.** Все функции «из коробки», без установки дополнительных пакетов. Новые команды в Cisco-like консоли. Упрощения в настройке мониторинга. И другие приятные мелочи.

Архитектура С-Терра Шлюз

IPsec VPN с поддержкой **ГОСТ алгоритмов** шифрования и западных алгоритмов:

- ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012;
- ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015.

IPsec – “Mature standard” для создания криптографически защищенных сетей
“Default choice” для построения сетей любых топологий и защиты удаленного доступа

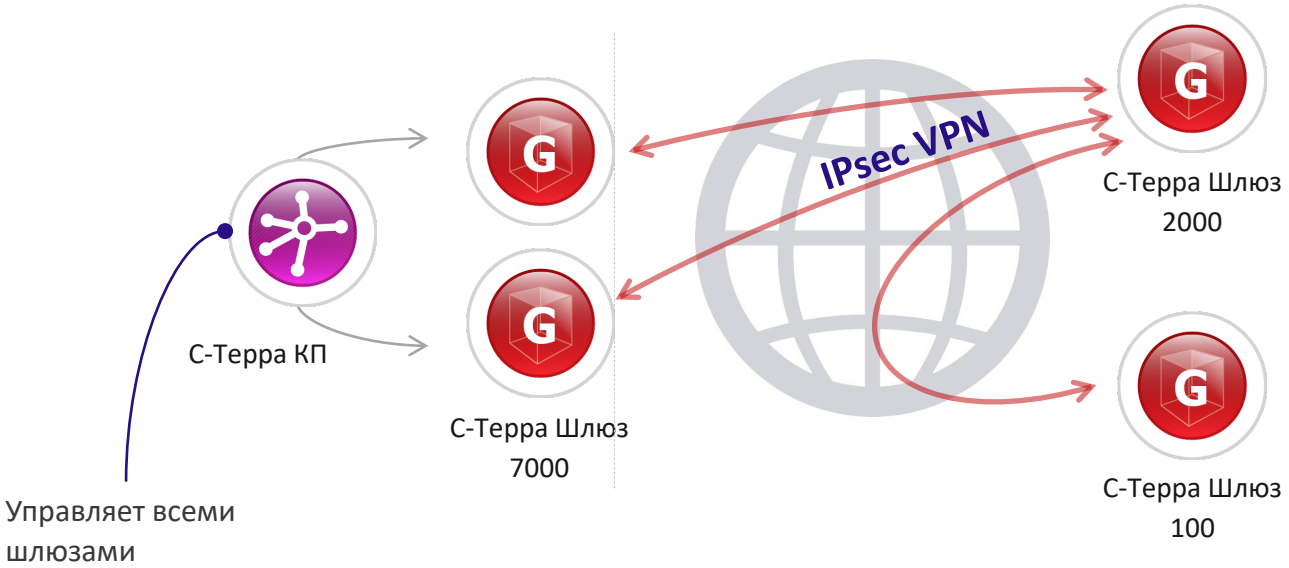
Gartner

С-Терра Шлюз совместим:

- Cisco, CheckPoint, Fortinet на западных алгоритмах шифрования;
- Любой другой вендор, реализующий IPsec по RFC2401-2412.

С-Терра Шлюз

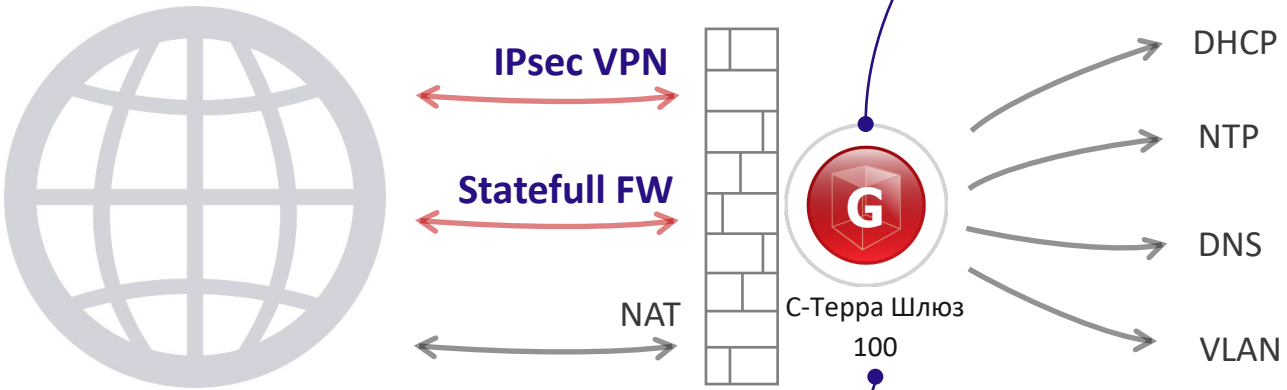
Миф №1: IPsec VPN – это всегда точка-точка



Реальность:
Можно строить любые IPsec туннели.

Поддерживается полносвязная топология, аналог DMVPN

С-Терра Шлюз в малом филиале I



Даже младший
С-Терра Шлюз поддерживает сетевые сервисы для LAN

Управление трафиком:

— Из LAN доступны Интернет и корпоративная сеть;

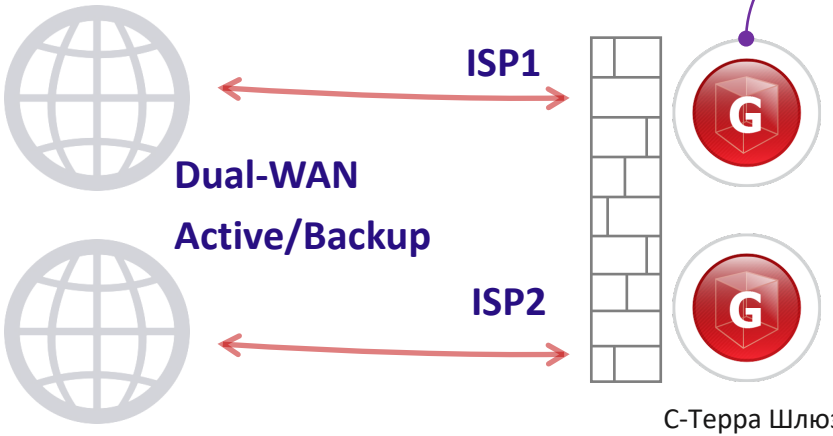
— Можно запретить все, кроме VPN;

— Весь трафик в центр внутри VPN.

Все модели С-Терра Шлюз **одинаково функциональны**

С-Терра Шлюз в малом филиале II

Даже младший
С-Терра Шлюз поддерживает все механизмы отказоустойчивости



Dual-WAN
Active/Backup

VRRP кластеризация
Active/Backup

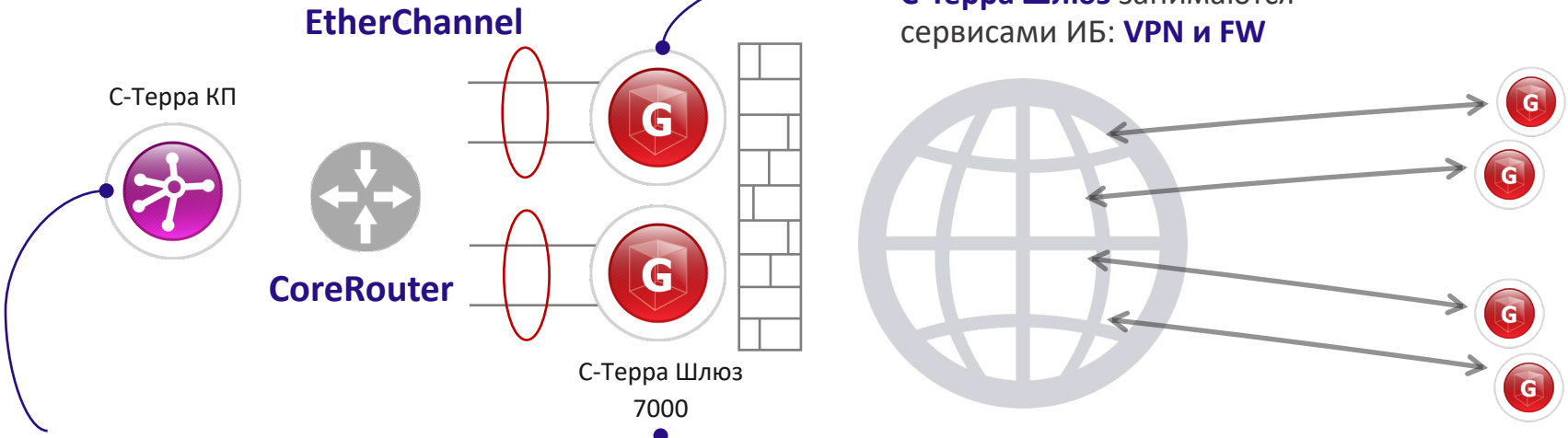
С-Терра Шлюз 100

Dual-WAN –
резервирование провайдеров ISP1 и ISP2

С-Терра Шлюз в центре

s•terra®

Подключений множество. Функции организации сети лучше отдать на **CoreRouter.** **С-Терра Шлюз** занимаются сервисами ИБ: **VPN и FW**

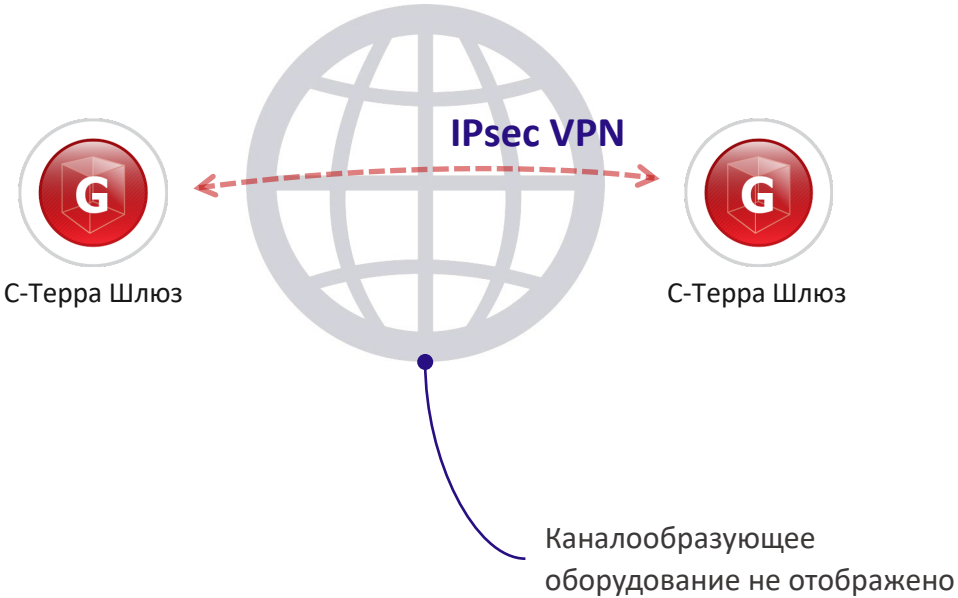


С-Терра КП управляет всеми С-Терра Шлюз или доступен **SSH**

Филиальные подключения балансируются на шлюзы в центре, поддерживаются BGP, OSPF, RIPv2

IPsec VPN на спутниковых каналах связи

Миф №2: IPsec VPN нестабилен на спутниковых каналах связи



Реальность:

Подтверждена стабильная работа на спутниковом канале

Latency – 500 мс, Jitter – 20 мс, PacketLoss – < 1%

Тестировали трафик:

- ICMP
- TCP 1 поток
- TCP 30 потоков
- UDP

С-Терра Шлюз DP

Миф №3: IPsec VPN ограничен в производительности

L2-over-L3
Канал между шлюзами может быть любым, даже Интернет
VPN туннель связывает единый broadcast домен

Изменения продуктовой линейки I

Модель	С-Терра Шлюз 100	С-Терра Шлюз 1000	С-Терра Шлюз 2000
Что изменилось?	Увеличена производительность **90 Мбит/с IMIX** (было 40)	Увеличена производительность **270 Мбит/с IMIX** (было 120)	Увеличена производительность **690 Мбит/с IMIX** (было 250)
Финансы (Условия сравнения: СКЗИ класса КС3, курс $: 75 руб)	**Раньше:** С-Терра Шлюз 1000 256 850 руб. **Сейчас:** 111 360 руб.	**Раньше:** С-Терра Шлюз 2000 360 910 руб. **Сейчас:** 256 850 руб.	**Раньше:** С-Терра Шлюз 3000 484 400 руб. **Сейчас:** 360 910 руб.

Изменения продуктовой линейки II

Модель	С-Терра Шлюз 7000 HE	С-Терра Шлюз 8000 HE
Что изменилось?	Оптимизирована производительность на двух и более сессиях: Одна сессия: **2039 Мбит/с IMIX** **Две+ сессии: 3460 Мбит/с IMIX**	Оптимизирована производительность на двух и более сессиях для «больших» пакетов: Две сессии: **5 264 Мбит/с UDP 558** Две сессии: **9 290 Мбит/с UDP 1446**
Финансы (Условия сравнения: СКЗИ класса КС3, курс $: 75 руб)	**Раньше:** 1 374 000 руб. **Сейчас:** 1 418 000руб.	

Чем больше сессий, тем лучше балансируется нагрузка. Обновление с 4.2 до 4.3 увеличит производительность.

Изменения продуктовой линейки III

s•terra®

Тип трафика	С-Терра Шлюз 10G	С-Терра Шлюз 25G	С-Терра Шлюз 40G
UDP 1446 mono	9 523	23 717	37 691
UDP 110 mono	6 073	13 310	9 580
UDP IMIX mono	8 406	21 008	27 784
UDP 1446 dual	18 969 (в 4.2 было 12 644)	27 479	45 008
UDP 110 dual	7 738 (в 4.2 было 5 355)	14 907	15 629
UDP IMIX dual	16 731 (в 4.2 было 9 964)	22 913	32 066

Обновление с 4.2 до 4.3 увеличит производительность

Исправлены недостатки версии 4.2

БЫЛО В 4.2:	СТАЛО В 4.3:
С-Терра Шлюз DP не поддерживал фрагментацию трафика средствами шлюза	С-Терра Шлюз DP поддерживает фрагментацию трафика средствами шлюза Просадка в производительности ~15%
FRR (динамическая маршрутизация OSPF, BGP, RIP), MultiWAN (резервирование провайдеров) – только в КС1, КС2 с установкой дополнительных пакетов	FRR, MultiWAN – во всех исполнениях без установки дополнительных пакетов
Поддержка USB модемов после установки дополнительных пакетов	Поддержка USB модемов, их резервирование без установки дополнительных пакетов

Новые команды Cisco-like консоли I

Новые команды облегчают настройку и диагностику сетевых интерфейсов в Cisco-like консоли:

sterragate#show interfaces

```
GigabitEthernet0/0 is up, line protocol is up
  Hardware address is 000c.292a.2a90
  Description: WAN
  Internet address is 10.10.10.251/24
  MTU 1500 bytes
GigabitEthernet0/1 is up, line protocol is up
  Hardware address is 000c.292a.2a9a
  Description: LAN
  Internet address is 192.168.100.251/24
  MTU 1500 bytes
```

Description на интерфейсе тоже мини-новинка

sterragate#show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	10.10.10.251	YES	NVRAM	up	up
GigabitEthernet0/1	192.168.100.251	YES	NVRAM	up	up
GigabitEthernet0/2	unassigned	YES	NVRAM	down	down
GigabitEthernet0/3	unassigned	YES	NVRAM	down	down
GigabitEthernet0/4	unassigned	YES	NVRAM	down	down
GigabitEthernet0/5	10.0.199.11	YES	NVRAM	up	up

sterragate(config)#interface range gi0/0 - 2

```
sterragate(config)#interface range gi0/0 - 2
sterragate(config-if-range)#
```

Особенно актуально для С-Терра Шлюз DP

Новые команды Cisco-like консоли II

Команды диагностики VRRP кластера:

sterragate#show vrrp

```
Interface                          VRID   State
-----------------------------------------------
GigabitEthernet0/0                 70     Master
GigabitEthernet0/1                 50     Master
```

В примере – шлюз ~~MASTER~~ PRIMARY нода.

sterragate#show vrrp statistics

```
Interface GigabitEthernet0/0 (VRID is 70):
  Advertisements:
    Received: 0
    Sent: 238
  Became master: 1
  Released master: 0
  Packet Errors:
    Length: 0
    TTL: 0
    Invalid Type: 0
    Advertisement Interval: 0
    Address List: 0
  Authentication Errors:
    Invalid Type: 0
    Type Mismatch: 0
    Failure: 0
  Priority Zero:
    Received: 0
    Sent: 0
```

Быстро растущий счетчик «Became ~~master~~ primary» говорит о «флапах» кластера

Новые команды Cisco-like консоли III

Команда просмотра списков доступа:

sterragate#show access-lists

```
Extended IP access list GOST_VPN
    10 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
Extended IP access list DENY_SSH
    10 deny   tcp any host 10.0.0.1 eq 22
```

Команда настройки VPN:

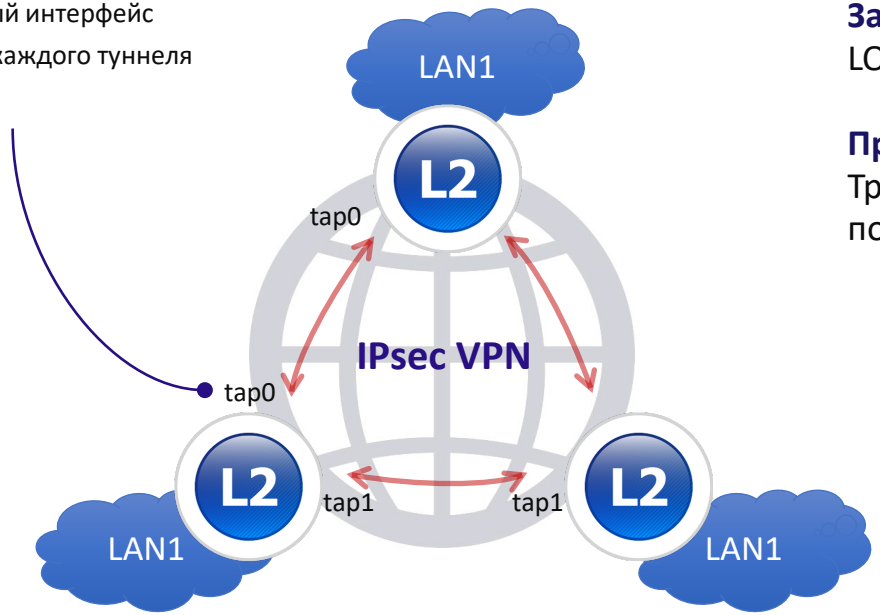
sterragate(config-crypto-map)#set certificate local credential

```
sterragate(config)#cr map CMAP 1
sterragate(config-crypto-map)#set certificate local credential "CN=sterra03MSK"
```

Позволяет выбрать конкретный локальный сертификат по DN имени для определенного пира. Для каждого пира свой сертификат

Новый сценарий для L2: full-mesh L2VPN

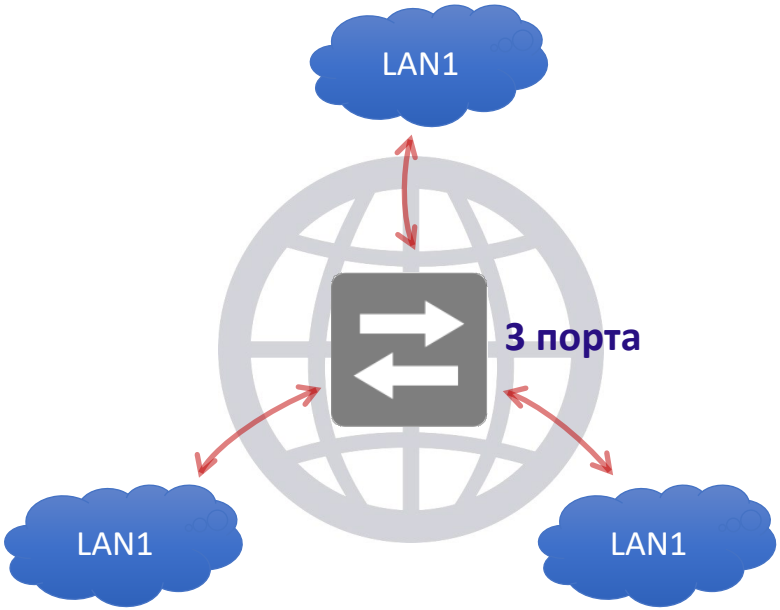
tapN – виртуальный интерфейс в С-Терра L2. Для каждого туннеля отдельный



Защита от петель:
LOOP PROTECTION SPLITHORIZON

Принцип работы:
Трафик с одного tap интерфейса не попадет на другой tap интерфейс

Новый сценарий для L2: full-mesh L2VPN



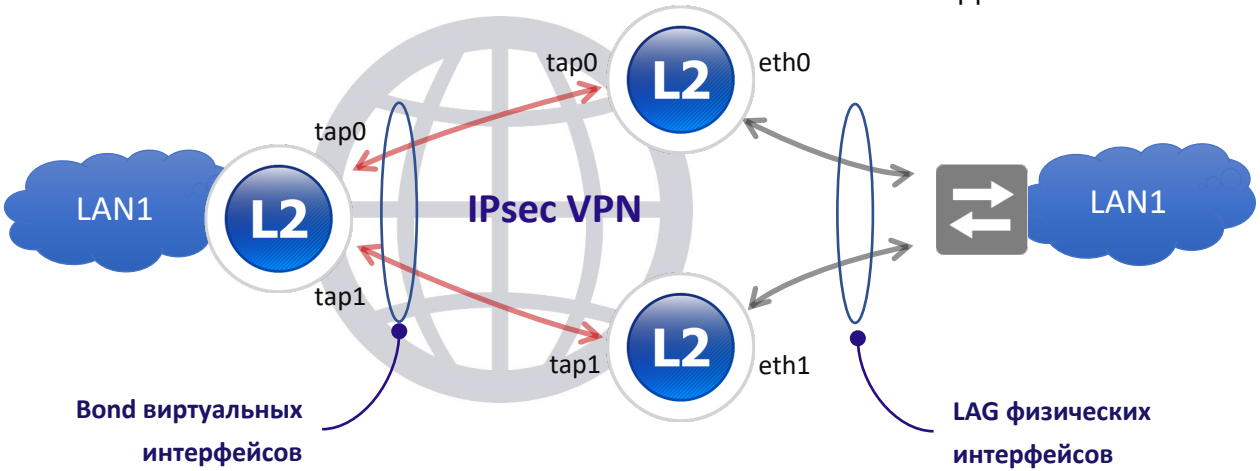
Ограничения:
Количество broadcast и multicast трафика

«Криптокоммутатор»:
Масштабируется до 50 узлов в full-mesh L2VPN или
до 50 портов «криптокоммутатора» на С-Терра Шлюз 7000

Новый сценарий для L2: балансировка Active/Active

Задача:
Обеспечить отказоустойчивость
и Active/Active балансировку

Проблема ассиметрии:
Keepalive отслеживает состояние VPN.
Если туннеля нет, физический интерфейс
выводится из LAG



Приятные мелочи для Зумеров

Текстовый редактор nano
(можно работать почти как в Word):

Карта интерфейсов создается автоматически

Изменения в мониторинге I

s•terra®

- Добавлены Zabbix-агент, NetFlow, IPFIX
- Добавлен мониторинг:
  - Температуры компонентов АП
  - Загрузки процессора
  - Состояния жестких дисков
- Упрощена настройка (*скрипты предустановлены, файлы предзаполнены*)

Изменения в мониторинге II. Утилита top

s•terra®

Ядра процессора

Графическое отображение загрузки процессора

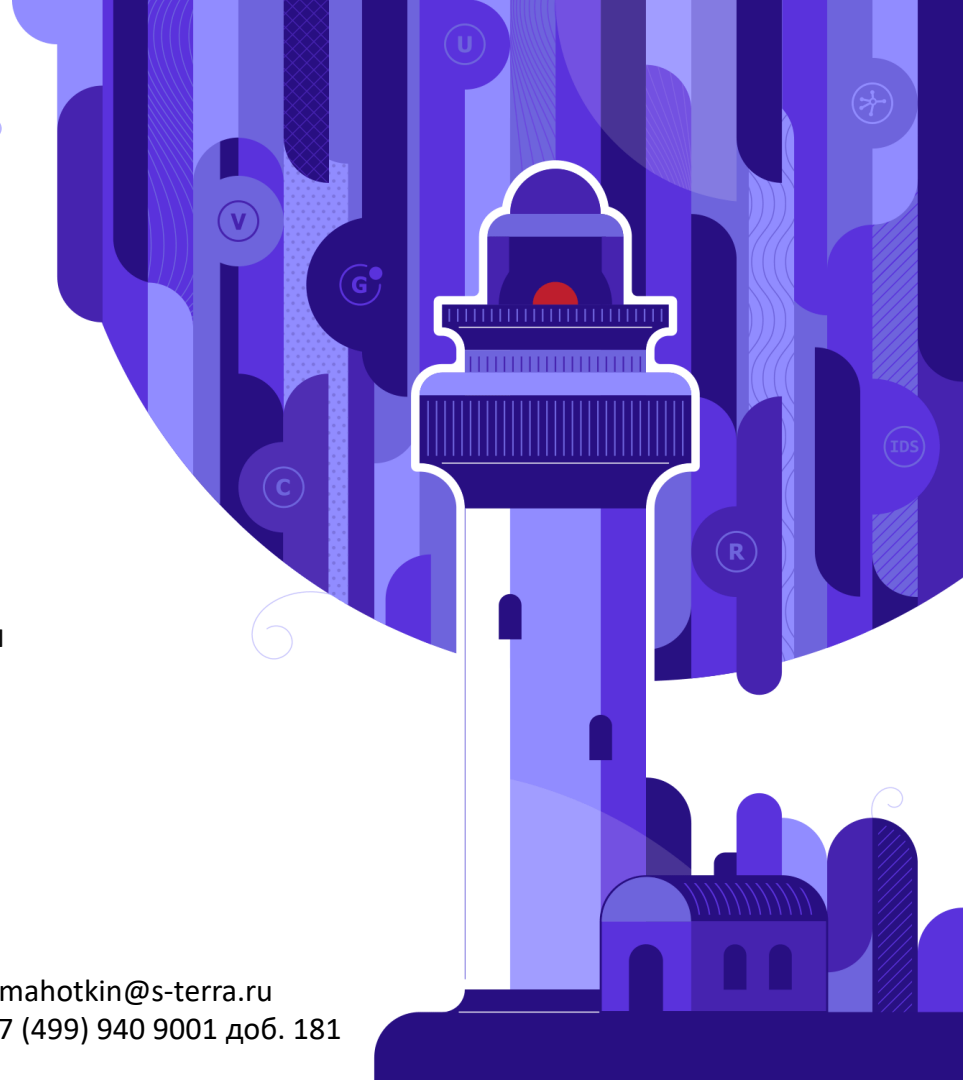
```
top - 16:55:13 up 2 days, 13:46,  8 users,  load average: 0.10, 0.14, 0.16
Tasks: 152 total,   1 running, 151 sleeping,   0 stopped,   0 zombie
%Cpu0  :   0.0/0.0     0[
%Cpu1  :   0.0/7.0     7[|||||||
%Cpu2  :   0.0/6.7     7[|||||||
%Cpu3  :   0.0/7.6     8[|||||||
%Cpu4  :   0.3/0.3     1[
%Cpu5  :   0.3/0.3     1[
%Cpu6  :   0.0/0.0     0[
%Cpu7  :   0.0/0.0     0[
KiB Mem :  3775064 total,  3288172 free,   252544 used,   234348 buff/cache
KiB Swap:        0 total,        0 free,        0 used.  3258388 avail Mem
```

Загрузка ядра в процентах

Спасибо за внимание

Основные изменения в версии 4.3

- **Дешевле.** Новая продуктовая линейка;
- **Производительнее.** Новая продуктовая линейка, **40 Гбит/с** ГОСТ шифрования на паре шлюзов;
- **Функциональнее.** Новые сценарии для С-Терра L2: full-mesh l2vpn, отказоустойчивость и Active/Active кластеризация;
- **Удобнее.** Все функции «из коробки», без установки дополнительных пакетов. Новые команды в Cisco-like консоли. Упрощения в настройке мониторинга. И другие приятные мелочи.



dmahotkin@s-terra.ru
+7 (499) 940 9001 доб. 181