Тестирование решений Эс-Терра Си Эс Пи для построения VPN с использованием модулей RVPN компании Cisco Systems

Докладчик:
Ильин Роман Владимирович , Главный специалист ЗАО «Компания ТрансТелеКом»

Наша Компания традиционно уделяет повышенное внимание вопросам безопасности при передаче данных. Причины этого очевидны – проекты, которые выполняет наша компания связаны:

- С ежедневной безопасностью тысяч граждан России, ведь ТТК обеспечивает работу сети передачи данных ОАО РЖД;
- с безопасностью бизнеса наших клиентов. Так, например, от «Единой информационно-аналитической системы по надзору в сфере транспорта», строящейся нашей компанией для Ространснадзора, будет зависеть бизнес сотен компаний;
- со строительством СОИБ ЕМЦСС ОАО РЖД;
- с созданием интегральной мультисервисной телекоммуникационной сети МВД РФ.

Именно по этому мы согласились на любезное предложение компании **Cisco Systems** и **Эс-Терра** на тестирование данного продукта – модуля RVPN

Технология тестирования

В процессе тестирования учитывались требования к оборудованию используемому Компанией при оказании услуг по обеспечению информационной безопасности;

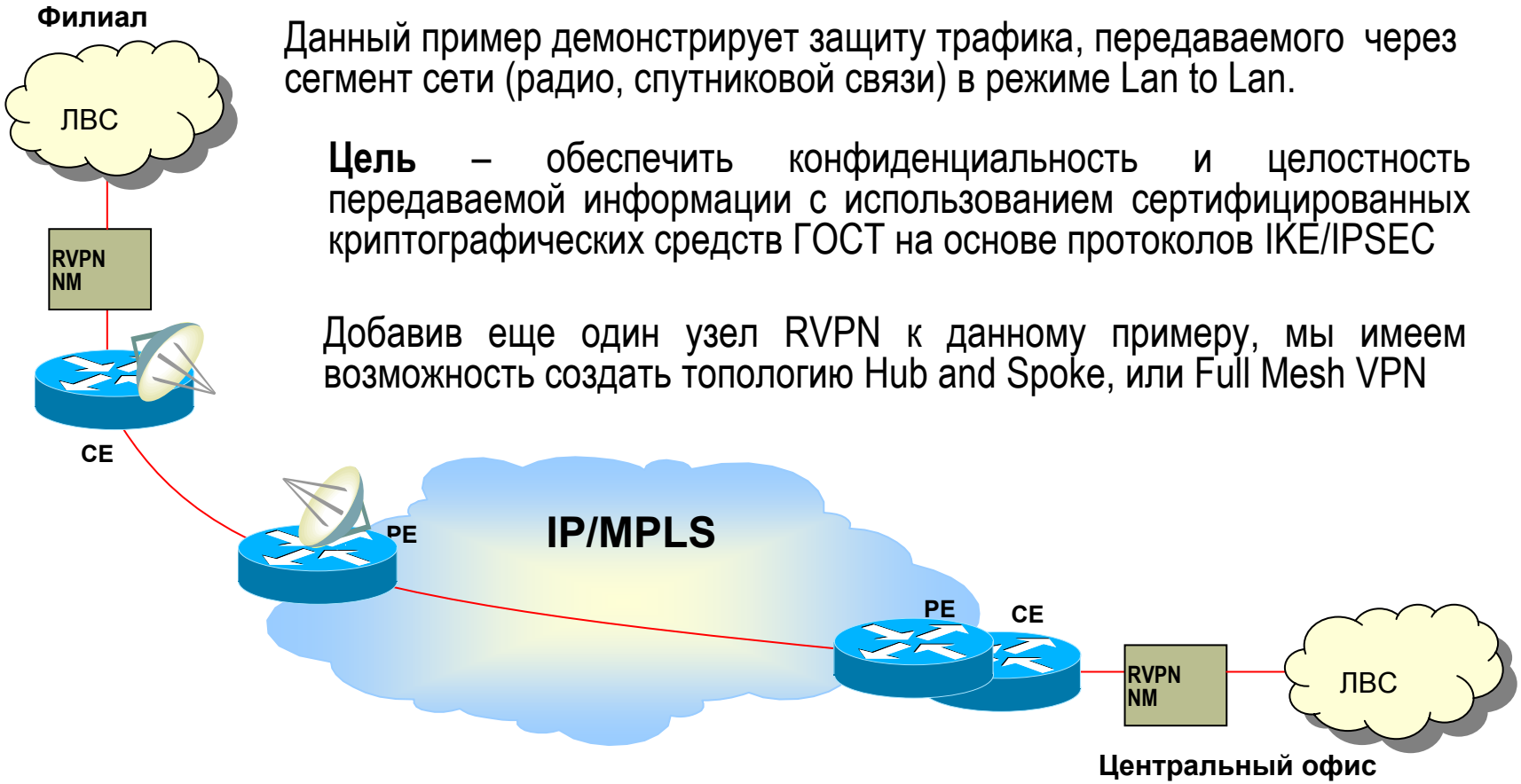
В тестах участвовало следующее оборудование:

- 2 маршрутизатора Cisco 2851 с установленными в NME слоты модулями RVPN*;
- 2 ПК размещенные в защищенных сетях.
- 1 VPN Gate 3000.

*RPVN модуль с инсталлированным ПО на базе криптографического ядра “Сигнал-КОМ”

В рамках тестирования были собраны тестовые схемы, приведенные ниже, также была оттестирована пропускная способность модуля при различных видах шифрования ГОСТ. Для тестирования использовалось Open Source ПО iperf “http://dast.nlanr.net/Projects/Iperf/” что дало некоторую погрешность при выполнении тестирования не более 5% - 10 %

Lan to Lan шифрование



Данный пример демонстрирует защиту трафика, передаваемого через сегмент сети (радио, спутниковой связи) в режиме Lan to Lan.

Цель – обеспечить конфиденциальность и целостность передаваемой информации с использованием сертифицированных криптографических средств ГОСТ на основе протоколов IKE/IPSEC

Добавив еще один узел RVPN к данному примеру, мы имеем возможность создать топологию Hub and Spoke, или Full Mesh VPN

Тестирование производительности Lan to Lan

Без crypto map на интерфейсе IP - без шифрования				
Datagramm Length	**64**	**300**	**1400**	
Mbits/sec	**16.9**	**46.7**	**93.4**	
Jitter	**0.030 ms**	**0.050 ms**	**0.136 ms**	
PPS	**33273**	**19607**	**8403**	
загрузка CPU модуль RVPN	**23.8%**	**17.5%**	**9.5%**	
загрузка CPU cisco 2851	**25%m**	**19%m**	**11%m**	
TCP Window size	**8K**	**16K**	**32K**	**64K**
Mbits/sec	**40.6**	**85.5**	**90.3**	**91.1**
загрузка CPU модуль RVPN	**6.4%**	**13.9%**	**14.3%**	**14.0%**
загрузка CPU cisco 2851	**7%m**	**16%m**	**17%m**	**17%m**

Тестирование производительности Lan to Lan

ESP - с проверкой целостности ESP + HMAC ГОСТ 28147-89, ГОСТ Р34.11-94				
Datagramm Length	**64**	**300**	**1400**	
Mbits/sec	**6.97**	**21.9**	**39.9**	
Jitter	**0.125 ms**	**0.553 ms**	**0.448 ms**	
PPS	**13698**	**9174**	**3571**	
загрузка CPU модуль RVPN	**78.8%**	**89.0%**	**98.3%**	
загрузка CPU cisco 2851	**15%m**	**12%m**	**5%m**	
TCP Window size	**8K**	**16K**	**32K**	**64K**
Mbits/sec	**22.2**	**32.7**	**34.5**	**34.8**
загрузка CPU модуль RVPN	**58.0%**	**93.9%**	**98.2%**	**99.2%**
загрузка CPU cisco 2851	**4%m**	**6%m**	**6%m**	**7%m**

Тестирование производительности Lan to Lan

ESP - без проверки целостности ESP ГОСТ 28147-89				
Datagramm Length	**64**	**300**	**1400**	
Mbits/sec	**14.9**	**27.0**	**92.4**	
Jitter	**0.035 ms**	**0.091 ms**	**0.625 ms**	
PPS	**29389**	**11363**	**8333**	
загрузка CPU модуль RVPN	**46.5%**	**37.6%**	**86%**	
загрузка CPU cisco 2851	**23%m**	**13%m**	**12%m**	
TCP Window size	**8K**	**16K**	**32K**	**64K**
Mbits/sec	**35.9**	**68.2**	**88.4**	**89.1**
загрузка CPU модуль RVPN	**37.2%**	**71.0%**	**92.7%**	**93.3%**
загрузка CPU cisco 2851	**7%m**	**13%m**	**17%m**	**17%m**

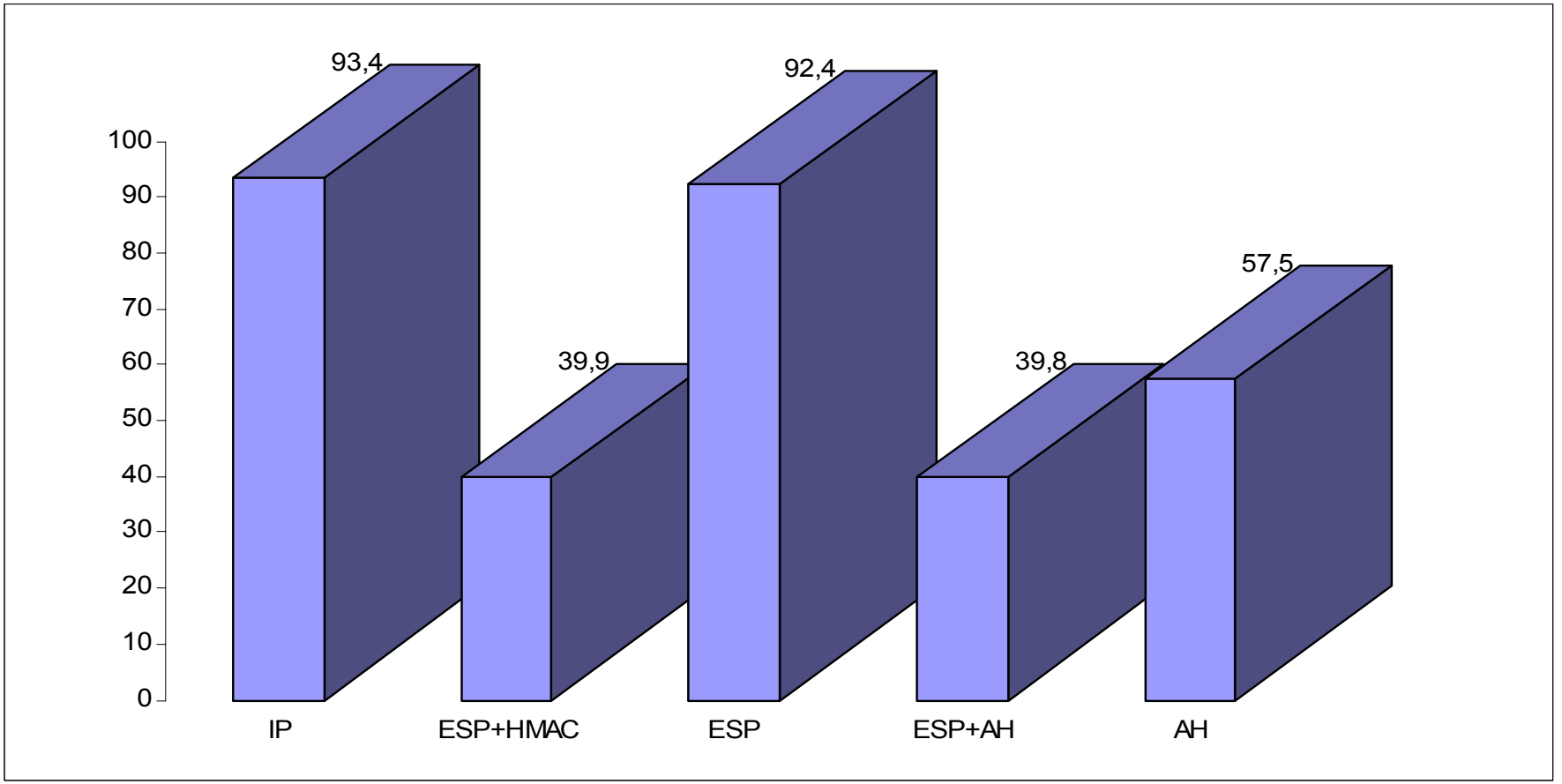
Тестирование производительности Lan to Lan

ESP - с проверкой целостности AH ESP + AH ГОСТ 28147-89, ГОСТ Р34.11-94				
Datagramm Length	**64**	**300**	**1400**	
Mbits/sec	**6.95**	**20.9**	**39.8**	
Jitter	**0.075 ms**	**0.123 ms**	**0.446 ms**	
PPS	**13698**	**8772**	**3571**	
загрузка CPU модуль RVPN	**84.8%**	**90.3%**	**99.2%**	
загрузка CPU cisco 2851	**15%m**	**12%m**	**5%m**	
TCP Window size	**8K**	**16K**	**32K**	**64K**
Mbits/sec	**21.7**	**32.0**	**33.5**	**33.6**
загрузка CPU модуль RVPN	**61.4%**	**94.0%**	**97.8%**	**98.4%**
загрузка CPU cisco 2851	**4%m**	**6%m**	**6%m**	**6%m**

Тестирование производительности Lan to Lan

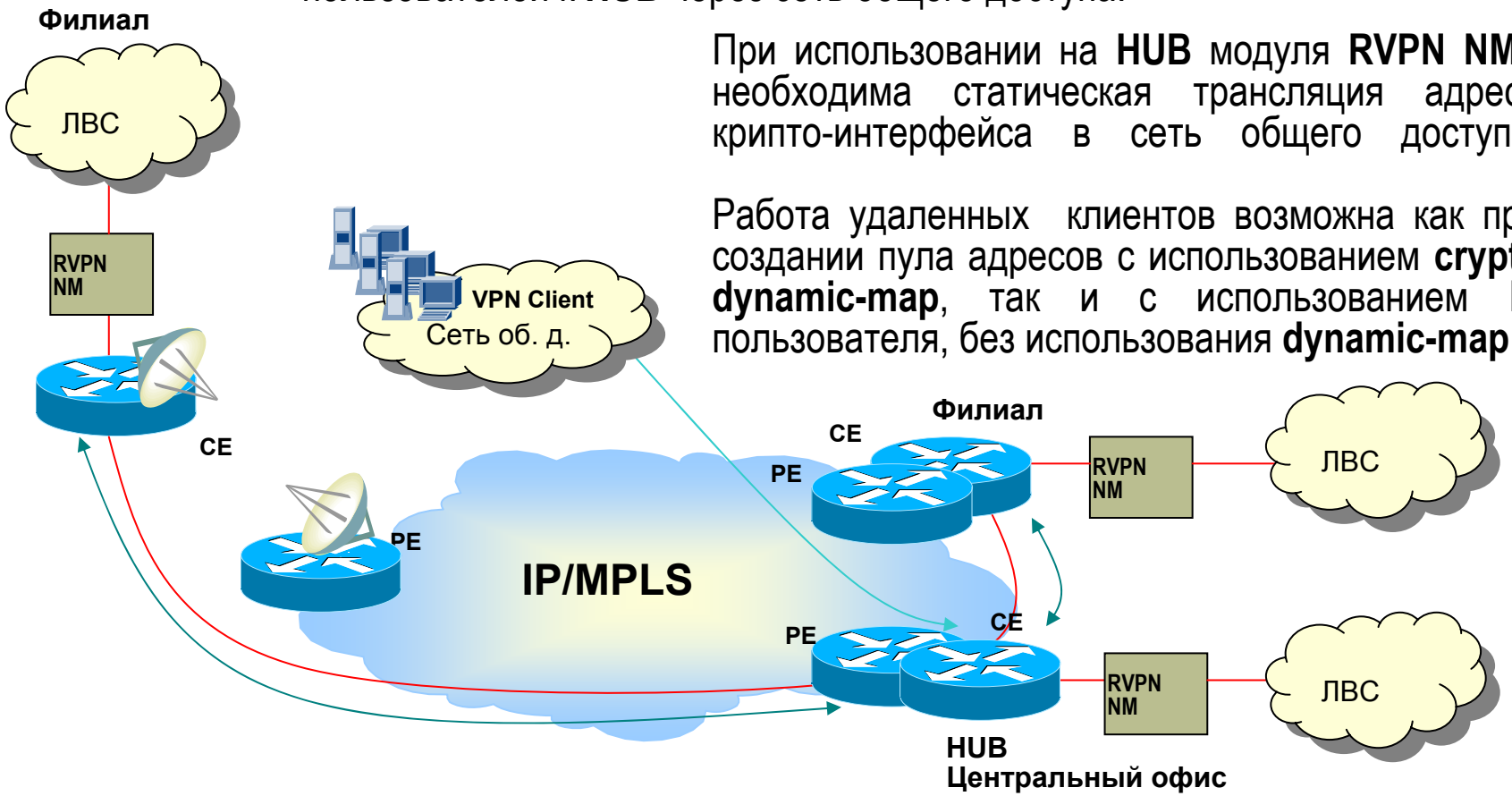
AH - только проверка целостности AH ГОСТ Р34.11-94				
Datagramm Length	**64**	**300**	**1400**	
Mbits/sec	**7.96**	**27.0**	**57.5**	
Jitter	**0.084 ms**	**0.346 ms**	**0.240 ms**	
PPS	**15625**	**11363**	**5181**	
загрузка CPU модуль RVPN	**83.7%**	**85.1%**	**99.2%**	
загрузка CPU cisco 2851	**16%m**	**14%m**	**8%m**	
TCP Window size	**8K**	**16K**	**32K**	**64K**
Mbits/sec	**27.3**	**44.0**	**47.4**	**47.9**
загрузка CPU модуль RVPN	**54.3%**	**91.8%**	**98.1%**	**98.8%**
загрузка CPU cisco 2851	**5%m**	**8%m**	**9%m**	**9%m**

Тестирование производительности Lan to Lan



Hub and Spoke RVPN (Remote)

Данный пример демонстрирует защиту трафика, передаваемого между тремя сегментами сети в в режиме hub and spoke, и подключение удаленных пользователей к **HUB** через сеть общего доступа.



При использовании на **HUB** модуля **RVPN NME** необходима статическая трансляция адреса крипто-интерфейса в сеть общего доступа.

Работа удаленных клиентов возможна как при создании пула адресов с использованием **crypto dynamic-map**, так и с использованием IP пользователя, без использования **dynamic-map**

Особенности применения

Модуль не поддерживает дополнительные сервисы такие как NAT, DHCP, динамические протоколы маршрутизации.

Для того чтобы использовать DHCP, NAT, динамическую маршрутизацию или другие сервисы, необходимо сконфигурировать данные сервисы на любом свободном интерфейсе маршрутизатора смотрящем в ЛВС.

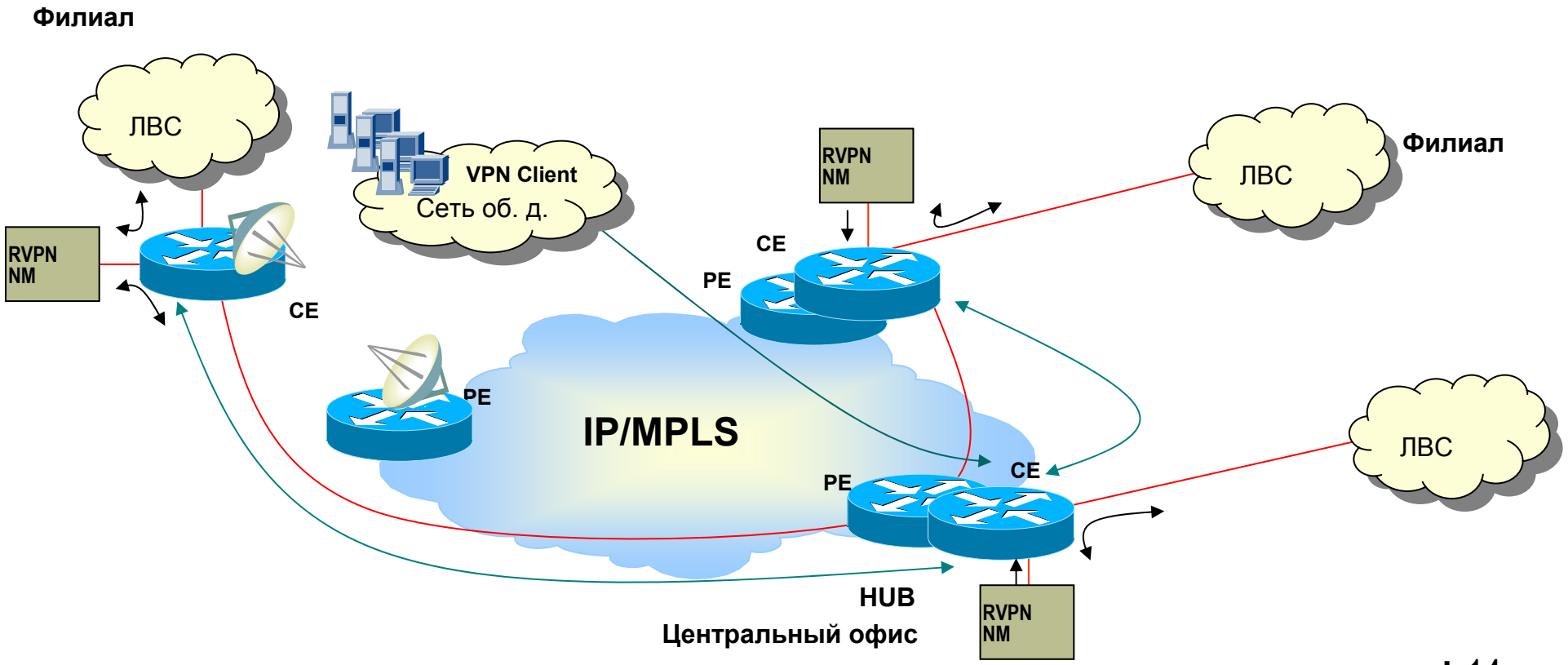
На маршрутизаторе настроить GRE тунель в который будет входить ЛВС трафик и после этого перенаправляться на модуль RVPN, шифроваться IPSEC и отправляться обратно маршрутизатору в формате IPSEC(GRE[IP]).

(для этих целей можно использовать также route map).

Шифрование GRE туннеля через RVPN NME модуль (Lan to Lan)

Hub and Spoke RVPN (Remote) & GRE

При шифровании трафика по ГОСТ из ЛВС в ЛВС, необходимо создать GRE туннель или route map для прохождения трафика через модули RVPN.



Тестирование Lan to Lan производительности GRE

ESP - с проверкой целостности ESP + HMAC ГОСТ 28147-89, ГОСТ Р34.11-94				
Datagramm Length	**64**	**300**	**1400**	
Mbits/sec	**4.99**	**16.9**	**34.0**	
Jitter	**0.158 ms**	**0.660 ms**	**0.396 ms**	
PPS	**9804**	**7092**	**3039**	
загрузка CPU модуль	**70.8%**	**80.0%**	**90.1%**	
загрузка CPU cisco	**21%m**	**17%m**	**9%m**	
TCP Window size	**8K**	**16K**	**32K**	**64K**
Mbits/sec	**15.9**	**25.6**	**30.6**	**31.4**
загрузка CPU модуль	**47.5%**	**80.4%**	**95.3%**	**98.7%**
загрузка CPU cisco	**6%m**	**10%m**	**12%m**	**12%m**

Тестирование Lan to Lan производительности GRE

ESP - без проверки целостности ESP ГОСТ 28147-89				
Datagramm Length	**64**	**300**	**1400**	
Mbits/sec	**11.1**	**21.9**	**81.1**	
Jitter	**0.046 ms**	**0.327 ms**	**0.082 ms**	
PPS	**21738**	**9174**	**3178**	
загрузка CPU модуль	**54.3%**	**36.0%**	**89.3%**	
загрузка CPU cisco	**39%m**	**20%m**	**17%m**	
TCP Window size	**8K**	**16K**	**32K**	**64K**
Mbits/sec	**22.7**	**43.6**	**64.9**	**74.4**
загрузка CPU модуль	**28.1%**	**50.7%**	**83.3%**	**97.8%**
загрузка CPU cisco	**9%m**	**16%m**	**23%m**	**27%m**

компания ТрансТелеКом™

Тестирование Lan to Lan производительности GRE

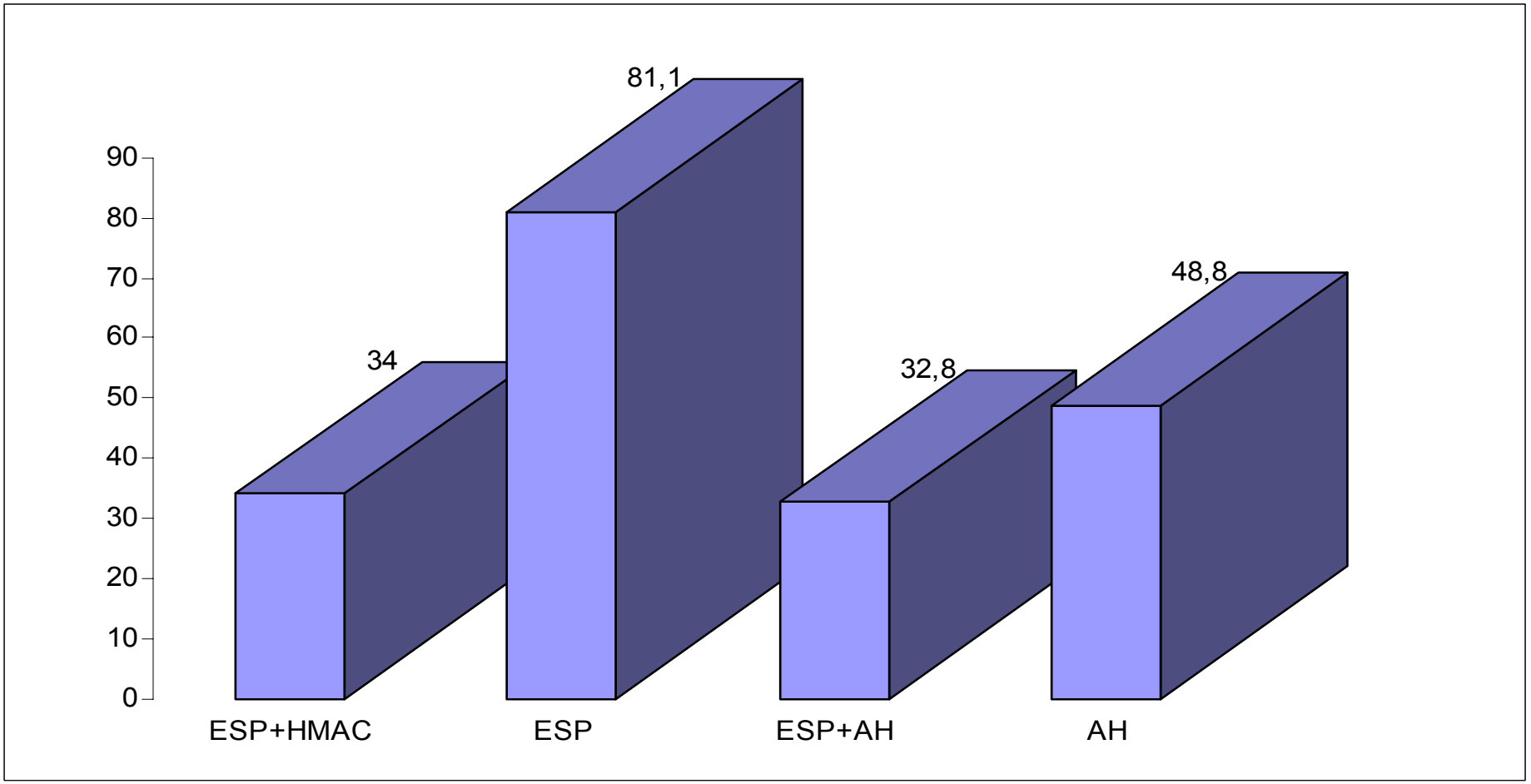
ESP - с проверкой целостности AH ESP + AH ГОСТ 28147-89, ГОСТ Р34.11-94				
Datagramm Length	**64**	**300**	**1400**	
Mbits/sec	**5.00**	**15.9**	**32.8**	
Jitter	**0.102 ms**	**0.383 ms**	**0.425 ms**	
PPS	**9801**	**6666**	**2950**	
загрузка CPU модуль	**73.6%**	**78.0%**	**91.1%**	
загрузка CPU cisco	**21%m**	**16%m**	**9%m**	
TCP Window size	**8K**	**16K**	**32K**	**64K**
Mbits/sec	**15.8**	**24.6**	**29.1**	**30.1**
загрузка CPU модуль	**49.0%**	**78.6%**	**95.7%**	**98.1%**
загрузка CPU cisco	**6%m**	**10%m**	**11%m**	**11%m**

компания ТрансТелеКом™

Тестирование Lan to Lan производительности GRE

AH - только проверка целостности AH ГОСТ Р34.11-94				
Datagramm Length	**64**	**300**	**1400**	
Mbits/sec	**5.98**	**19.9**	**48.8**	
Jitter	**0.109 ms**	**0.657 ms**	**0.687 ms**	
PPS	**11764**	**8333**	**4386**	
загрузка CPU модуль	**73.5%**	**77.3%**	**93.5%**	
загрузка CPU cisco	**24%m**	**19%m**	**11%m**	
TCP Window size	**8K**	**16K**	**32K**	**64K**
Mbits/sec	**18.5**	**32.0**	**40.0**	**41.2**
загрузка CPU модуль	**38.8%**	**71.4%**	**92.8%**	**96.5%**
загрузка CPU cisco	**8%m**	**11%m**	**14%m**	**15%m**

Тестирование Lan to Lan производительности GRE



Выводы

Управление данным продуктом довольно простое и интуитивно понятное, самый главный плюс это совместимость с CLI IOS, в том числе есть возможность осуществлять администрирование через WEB (GUI) интерфейс, и централизованное управление с платформы Cisco Works

Данное решение позволяет интегрировать в существующую телекоммуникационную инфраструктуру, развернутую на базе оборудования Cisco Systems, сертифицированные средства криптографической защиты.

Что позволяет удовлетворить потребности государственных и ряда коммерческих структур связанных с передачей данных по незащищенным сетям с использованием сертифицированных криптографических средств.

Контакты

Ильин Роман Владимирович, Главный специалист

ЗАО «Компания ТрансТелеКом»

Дирекция информационной безопасности

127006 г. Москва, ул. Долгоруковская, д.7.

тел. : (095) 784 6670

факс: (095) 784 6671

e-mail: r.ilin@transtk.ru