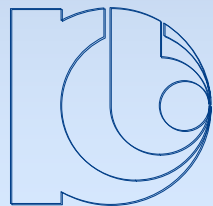


Архитектура на сигурна и интегрирана компјутерска мрежа за финансиски трансакции



Душко Серчевски
Оливер Стефановски
Александар Моновски



Архитектура на сигурна и интегрирана компјутерска мрежа за финансиски трансакции

Вовед

Два проекти

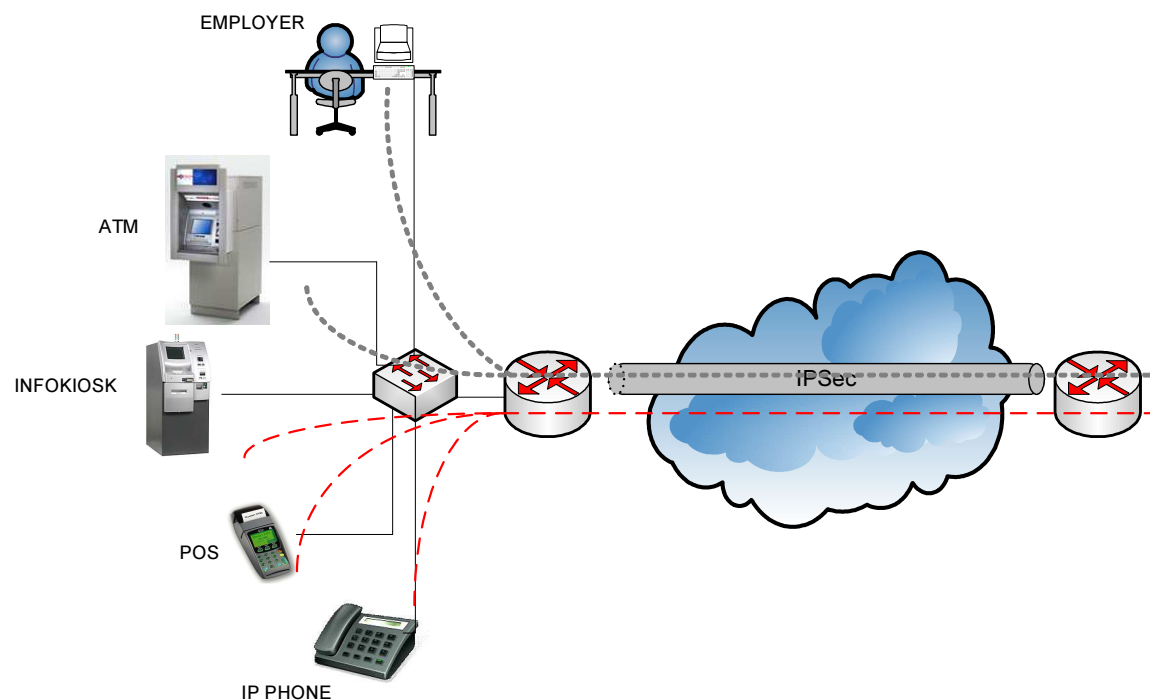
- Надградба на WAN комуникациска опрема во филијалите/експозирутите
- Сигурна Wireless LAN мрежа во зградата на Банката



Архитектура на сигурна и интегрирана компјутерска мрежа за финансиски трансакции

Цел

- Сигурна и интегрирана компјутерска мрежа за поддршка на деловните процеси на Банката.



Cisco Expo
2008



Архитектура на сигурна и интегрирана компјутерска мрежа за финансиски трансакции

Се раководеме од следниве главни задачи:

- Подобрување на перформансите на ИТ системот во поглед на зголемување на брзината на работата на апликациите, а со тоа и зголемување на ефикасноста на работењето во филијалите и експозитурите
- Зголемување на сигурноста на ИТ системот со енкрипција на мрежниот сообраќај согласно препораките
- Интегрирање на корпоративната компјутерската мрежа на Банката и мрежата за видео надзор што значи и помали трошоци за одржување на опремата.
- Менаџмент на мрежната опрема преку сигурен канал (SSH) согласно препораките
- Зголемување на скалабилноста на компјутерската мрежа во поглед на вововедување на нови сервиси преку зголемување на процесорската моќ и типот на хардверските модули во мрежната опрема
- Сигурна, оптимална и практична безжична мрежа за ИТ поддршка на состаноци на менаџментот на Банката



Фази на проектите

- **Имплементација и тестирање на првобитната идеја во демо околина**
- **Прилагодување согласно ограничувањата од опремата и ИТ околината**
- **Имплементација на решенијата**
- **Пилот продукција на неколку локации**
8 локации, 1 VPN Offload рутер на централна локација
- **Продукција**
55 локации, 2 VPN Offload рутери на централна локација



Користени опрема и сервиси

- Рутери CISCO 2811 (Sec Bundle)
- Access point-и CISCO AP 1130 AG
- CISCO ACS (Access Control Server)
- Microsoft Active Directory
- Microsoft CA
- Microsoft Share Point



Надградба на WAN комуникациската опрема во филијалите/експозитурите

Технички опис на користена опрема

Router Cisco 2811 (Sec Bundle)

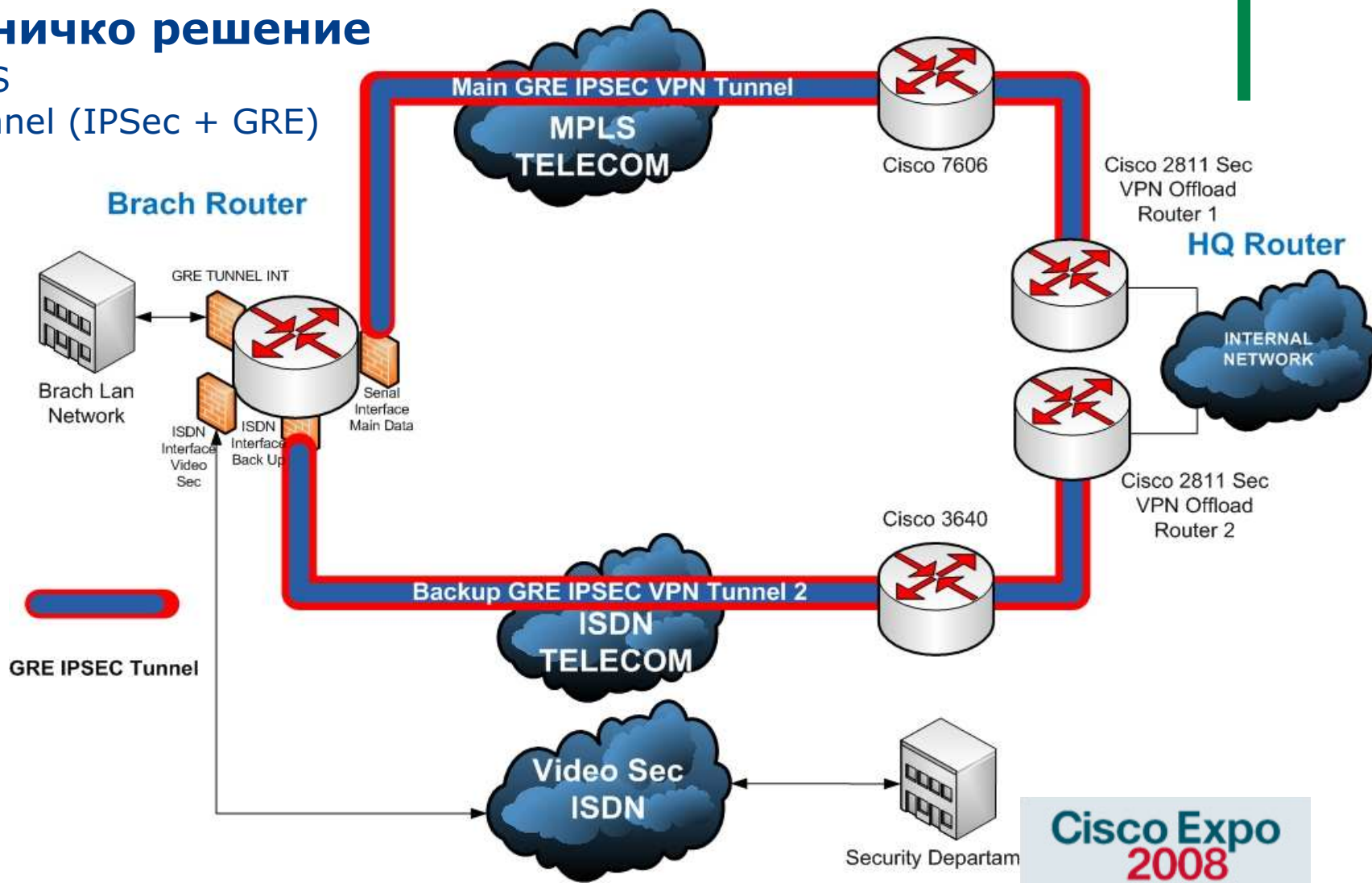
- RAM: 256MB
- Flash: 64MB
- Interfaces: integrated 2FE, WIC-1T, WIC-1B-S/T-V3
- Modules: integrated hardware VPN accelerator
- Cisco IOS: Sec Bundle



Надградба на WAN комуникациската опрема во филијалите/експозитурите

Техничко решение

- QoS
- Tunnel (IPSec + GRE)

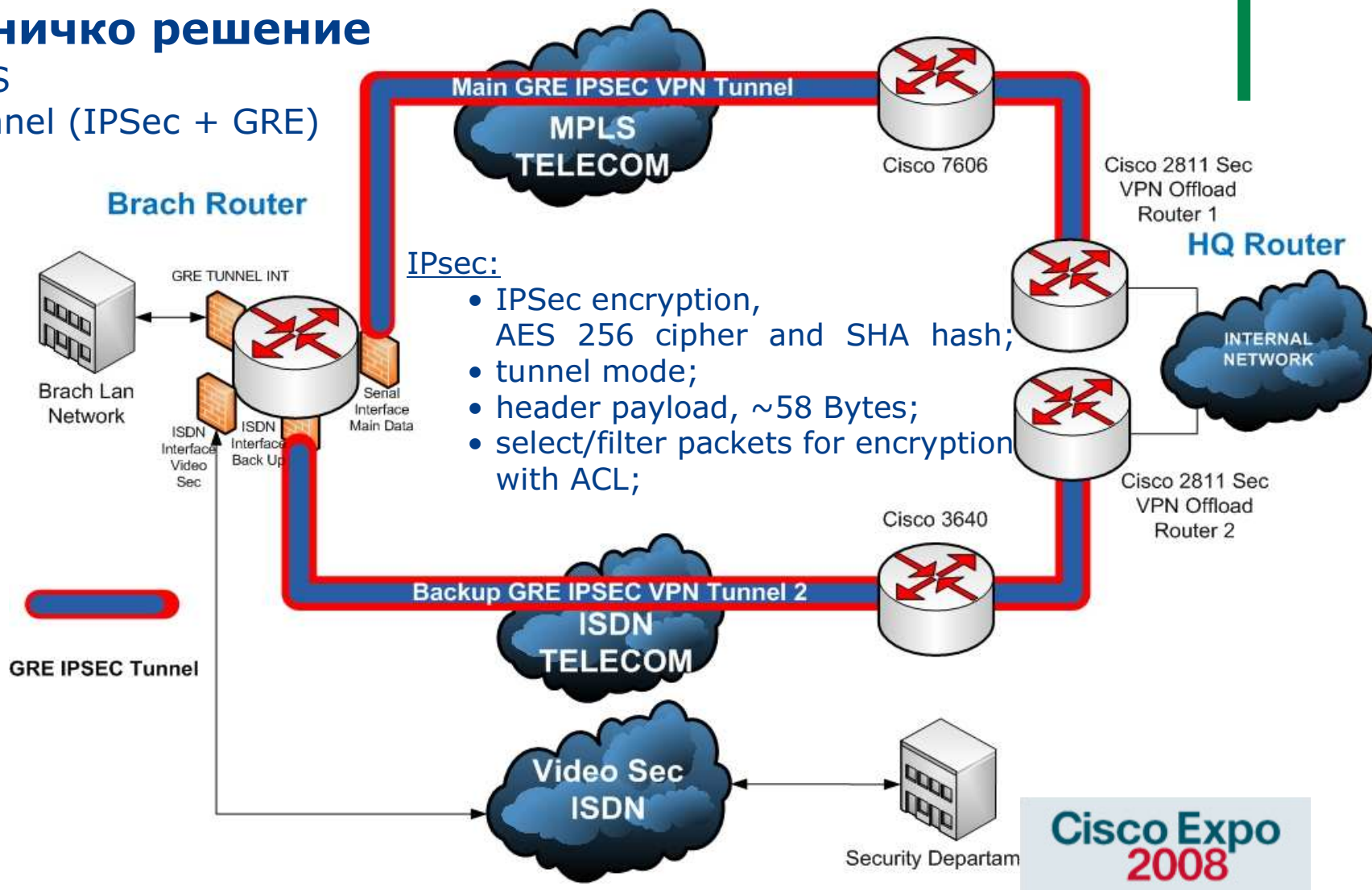




Надградба на WAN комуникациската опрема во филијалите/експозитурите

Техничко решение

- QoS
- Tunnel (IPSec + GRE)

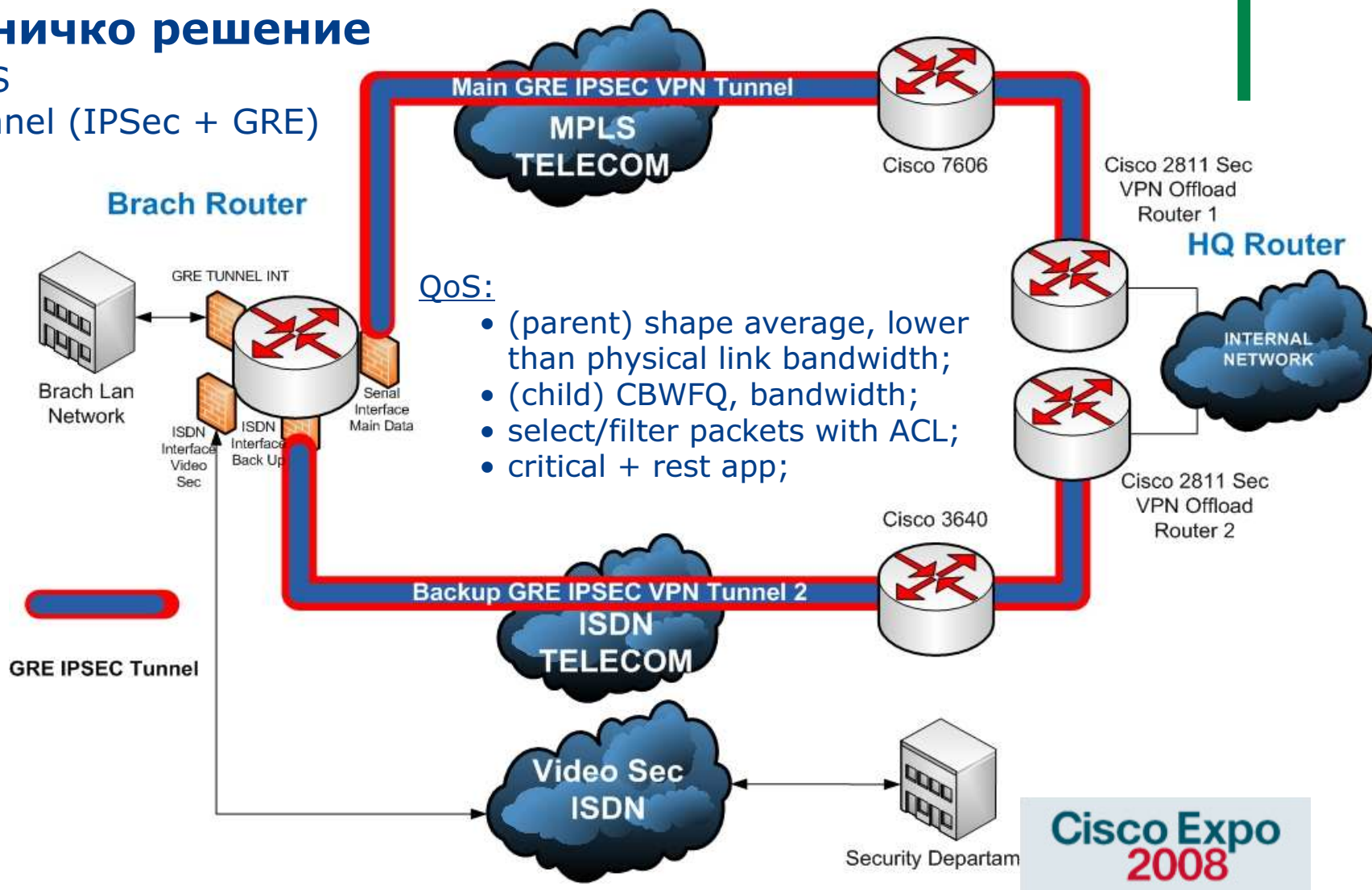




Надградба на WAN комуникациската опрема во филијалите/експозитурите

Техничко решение

- QoS
- Tunnel (IPSec + GRE)

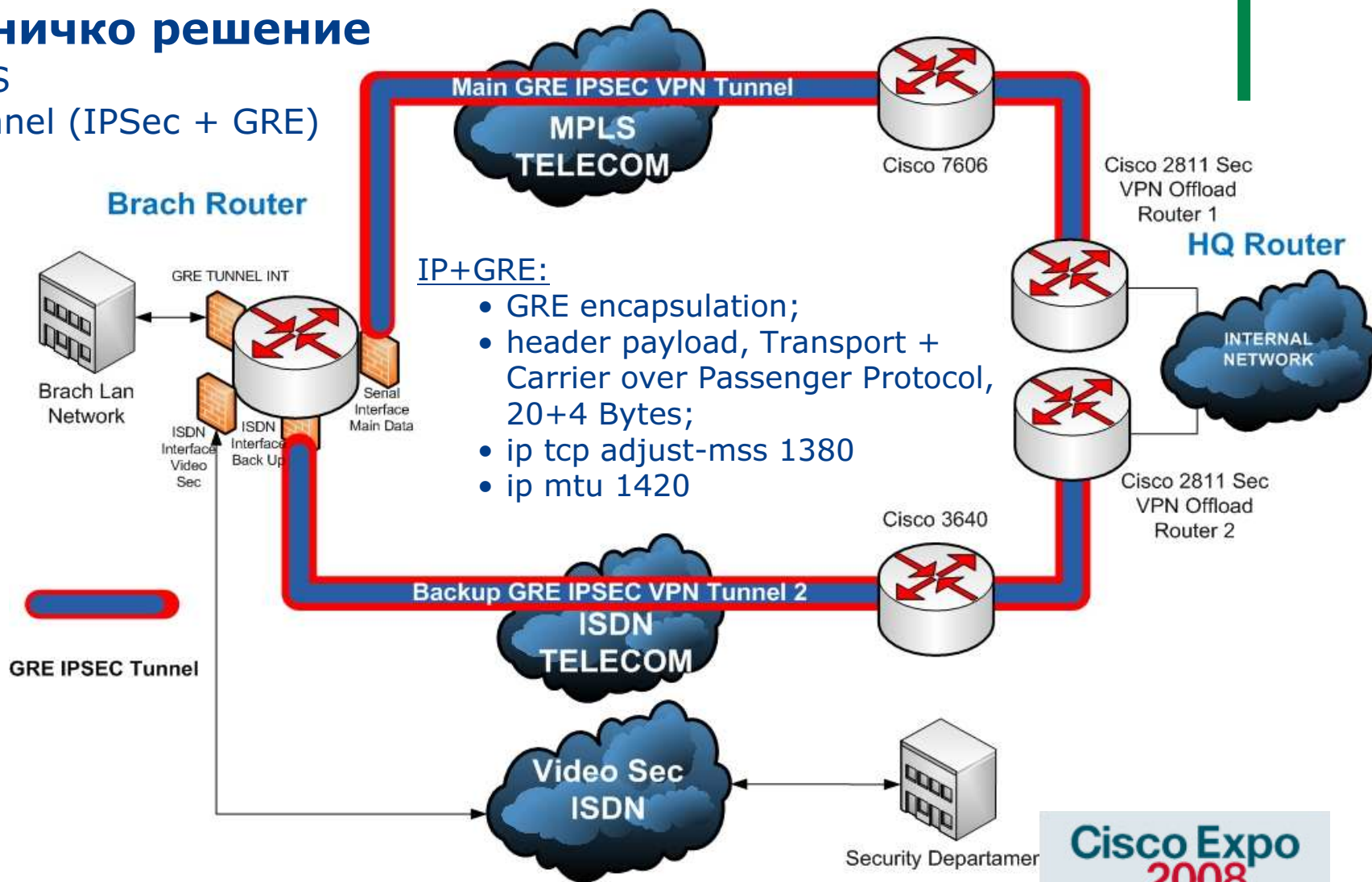




Надградба на WAN комуникациската опрема во филијалите/експозитурите

Техничко решение

- QoS
- Tunnel (IPSec + GRE)

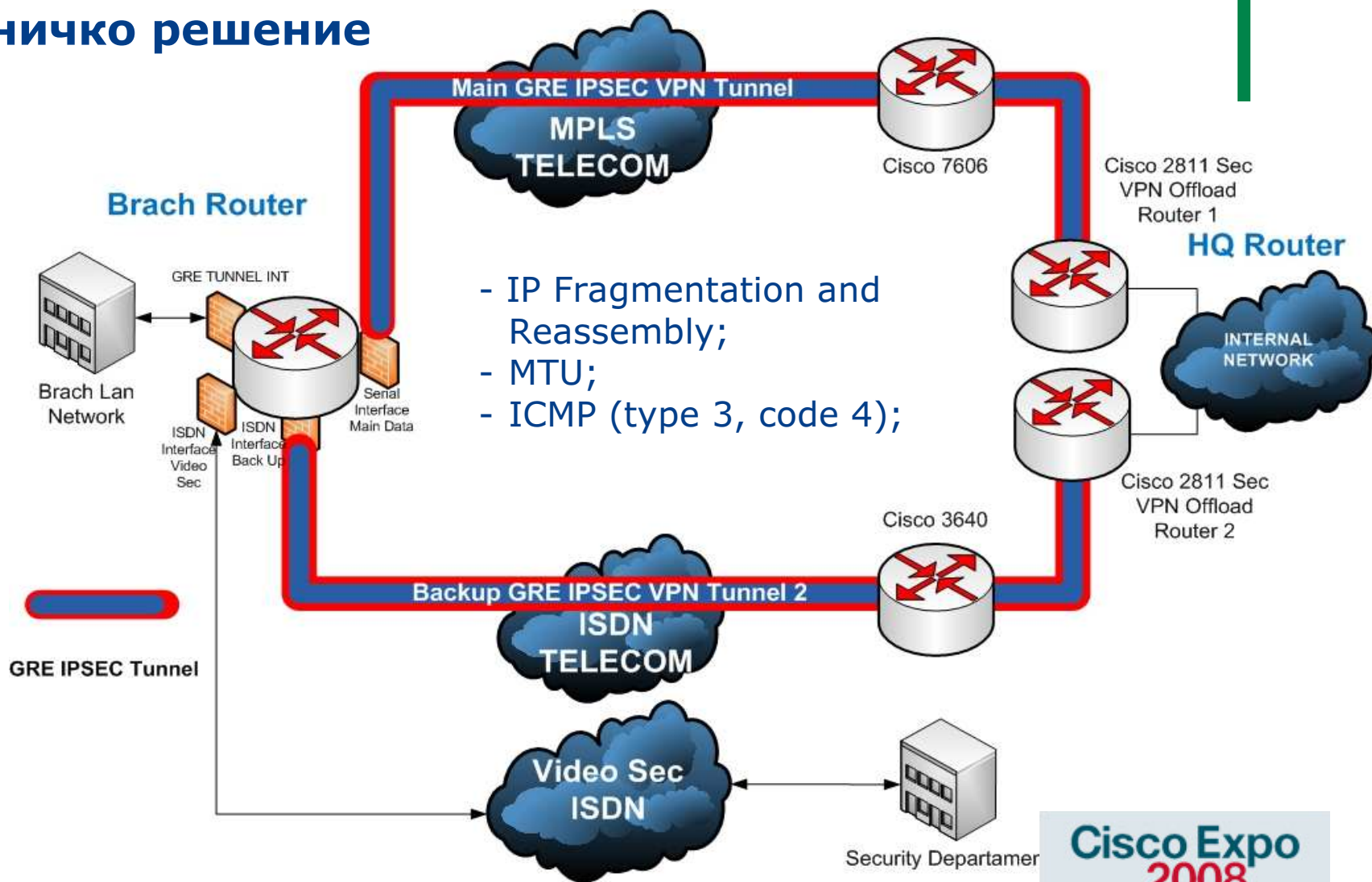


Cisco Expo
2008



Надградба на WAN комуникациската опрема во филијалите/експозитурите

Техничко решение



Cisco Expo
2008



Техничко решение

IP Fragmentation and Reassembly:

- MTU (Maximum Transmission Unit)
- MSS (TCP Maximum Segment Size)
- PMTUD (Path Maximum Transmission Unit Discovery)
- DF bit in IP header
- ICMP (type 3, code 4) "fragmentation needed and DF set"

Problems:

- A router can drop a packet and not send an ICMP message.
- A router can generate and send an ICMP message but the ICMP message gets blocked by a router or firewall between this router and the sender.
- A router can generate and send an ICMP message, but the sender ignores the message.



Надградба на WAN комуникациската опрема во филијалите/експозитурите

Техничко решение

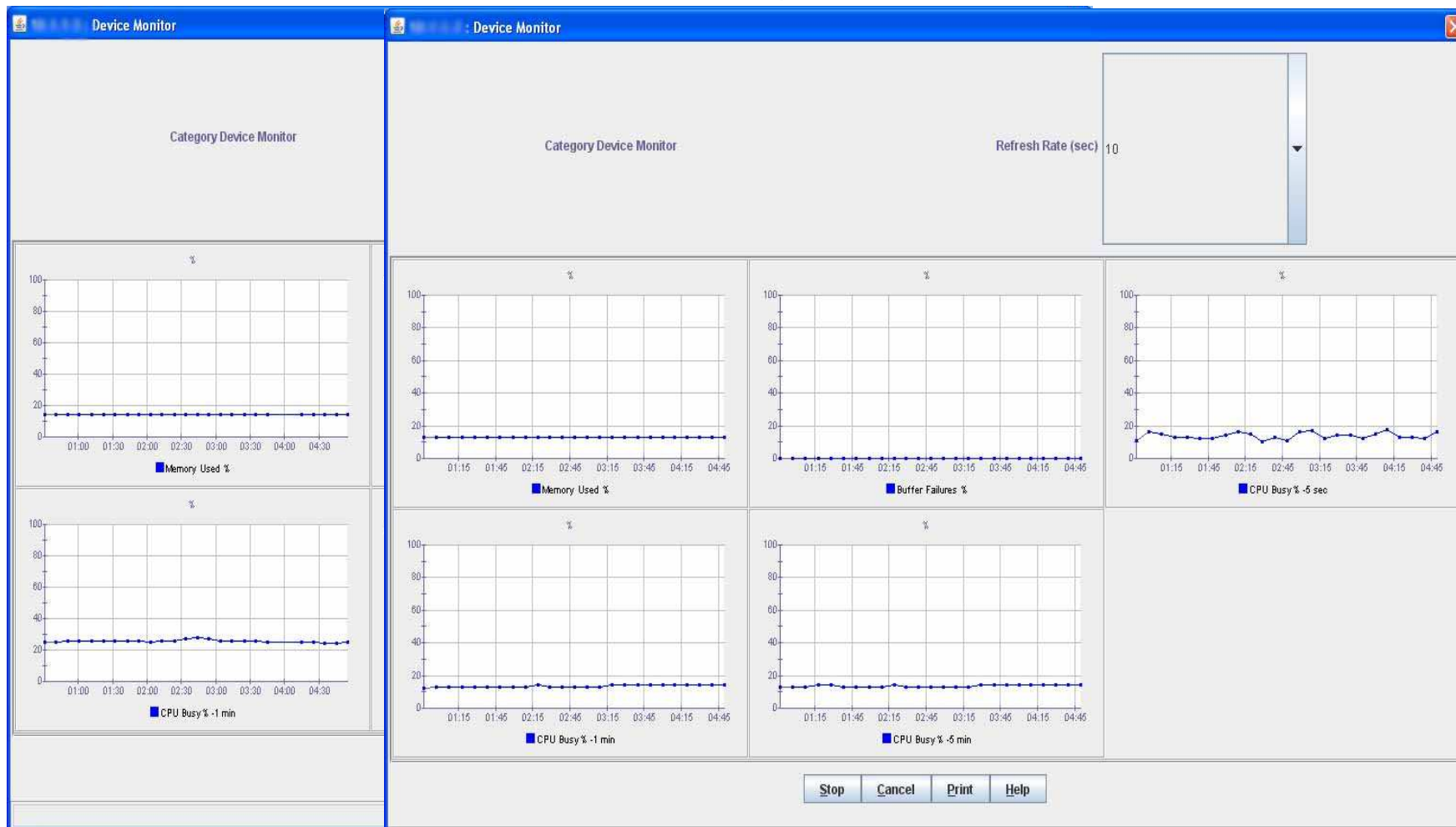
Router Security:

- remote access with SSHv2
- access only from IT administrator workstations
- login block feature - enabled
- potentially unsecure services - disabled
- password encryption service - enabled
- syslog time stamping – enabled



Надградба на WAN комуникациската опрема во филијалите/експозитурите

Перформанси на VPN offload рутерите на централна локација





Надградба на WAN комуникациската опрема во филијалите/експозитурите

Техничко решение - реализирани планови

NBAR (Network based Application Recognition) - NBAR, an important component of the Cisco Content Networking architecture, is a new classification engine in Cisco IOS® Software that can recognize a wide variety of applications, including Web-based applications and client/server applications that dynamically assign TCP or User Datagram Protocol (UDP) port numbers. After the application is recognized, the network can invoke specific services for that particular application. NBAR currently works with quality-of-service (QoS) features to help ensure that the network bandwidth is best used to fulfill your business objectives.

CBAC (Context-based access control) – intelligently filters TCP and UDP packets based on application-layer protocol session information and can be used for intranets, extranets and internets. You can configure CBAC to permit specified TCP and UDP traffic through a firewall only when the connection is initiated from within the network you want to protect. (In other words, CBAC can inspect traffic for sessions that originate from the external network.) However, while this example discusses inspecting traffic for sessions that originate from the external network, CBAC can inspect traffic for sessions that originate from either side of the firewall.



Планови



3G Wireless High-Speed WAN



Cisco WAAS Network Module

... CISCO VMSS Network module

**Cisco Expo
2008**



Техничко решение за Сигурна Wireless LAN мрежа во зградата на Банката

Технички опис на користена опрема

CISCO AIRONET 1130AG Authentication

Security Standards

- WPA
- WPA2 (802.11i)
- Cisco TKIP
- Cisco message integrity check (MIC)
- IEEE 802.11 WEP keys of 40 bits and 128 bits

802.1X EAP types:

- EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)
- Protected EAP-Generic Token Card (PEAP-GTC)
- PEAP-Microsoft Challenge Authentication Protocol Version 2 (PEAP-MSCHAP)
- EAP-Transport Layer Security (EAP-TLS)
- EAP-Tunneled TLS (EAP-TTLS)
- EAP-Subscriber Identity Module (EAP-SIM)
- Cisco LEAP

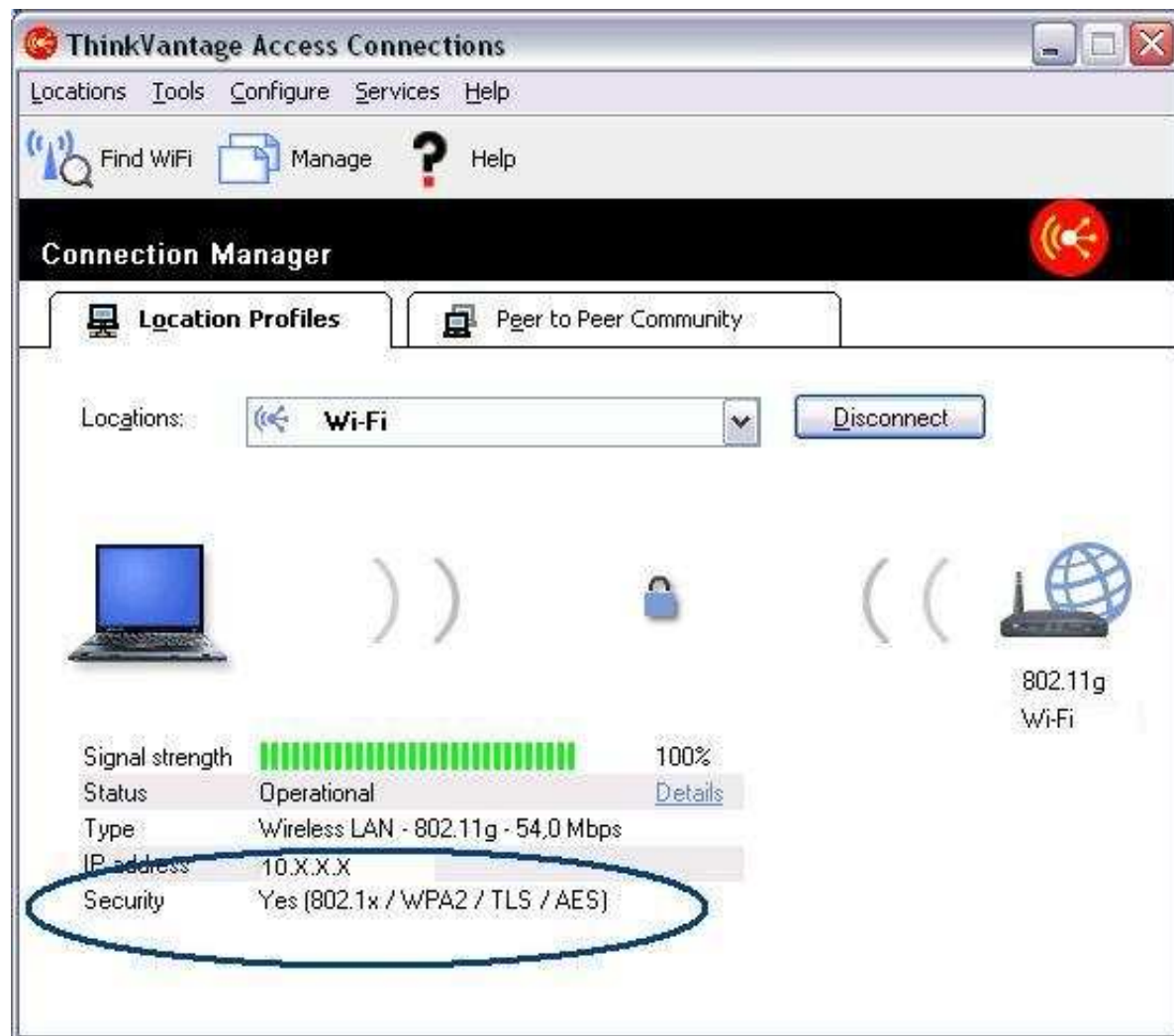
Encryption

- AES-CCMP encryption (WPA2)
- TKIP (WPA)
- Cisco TKIP
- WPA TKIP
- IEEE 802.11 WEP keys of 40 bits and 128 bits



Техничко решение за Сигурна Wireless LAN мрежа во зградата на Банката

Технички опис на користена опрема

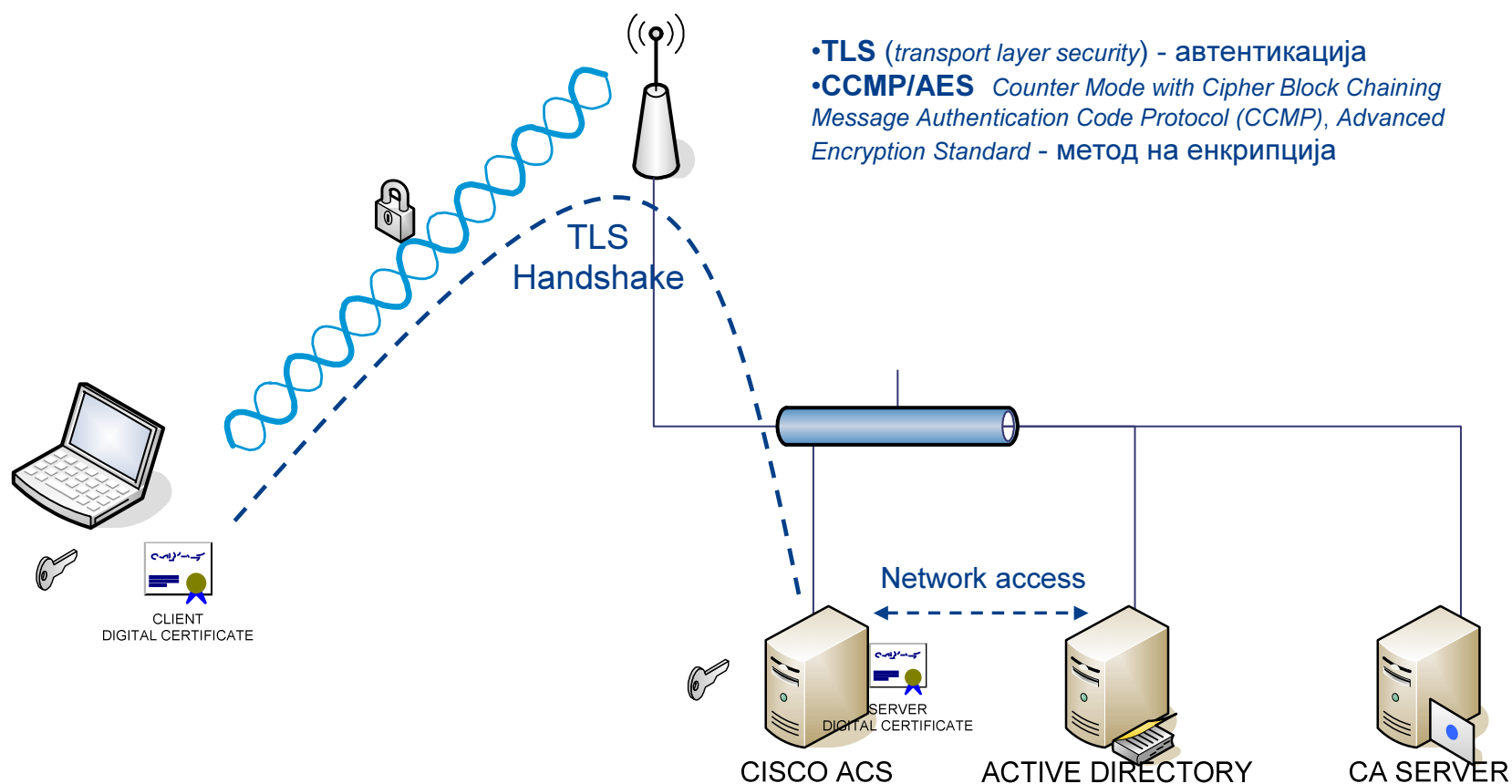




Техничко решение за Сигурна Wireless LAN мрежа во зградата на Банката

Техничко решение

802.1X / EAP (*Extensible Authentication Protocol*)

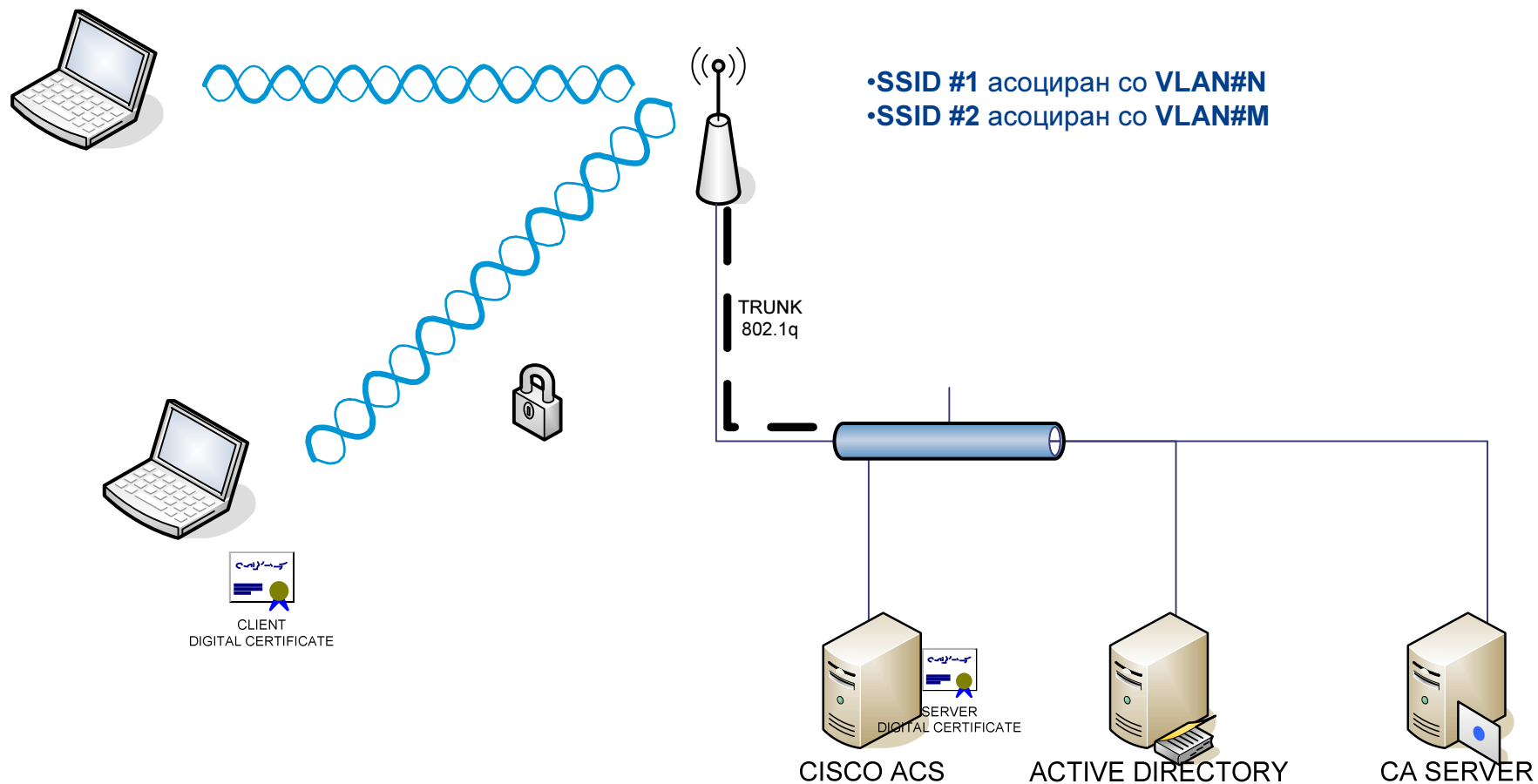




Техничко решение за Сигурна Wireless LAN мрежа во зградата на Банката

Техничко решение

СЕГМЕНТАЦИЈА





ПРАШАЊА



Душко Серчевски
dusko@kb.com.mk

Оливер Стефановски
olis@kb.com.mk

Александар Монеvски
ace@kb.com.mk