Загрози безпеки UC & VoIP і способи захисту. Основні види атак і способи захисту Cisco UCM.

Андрій Шип

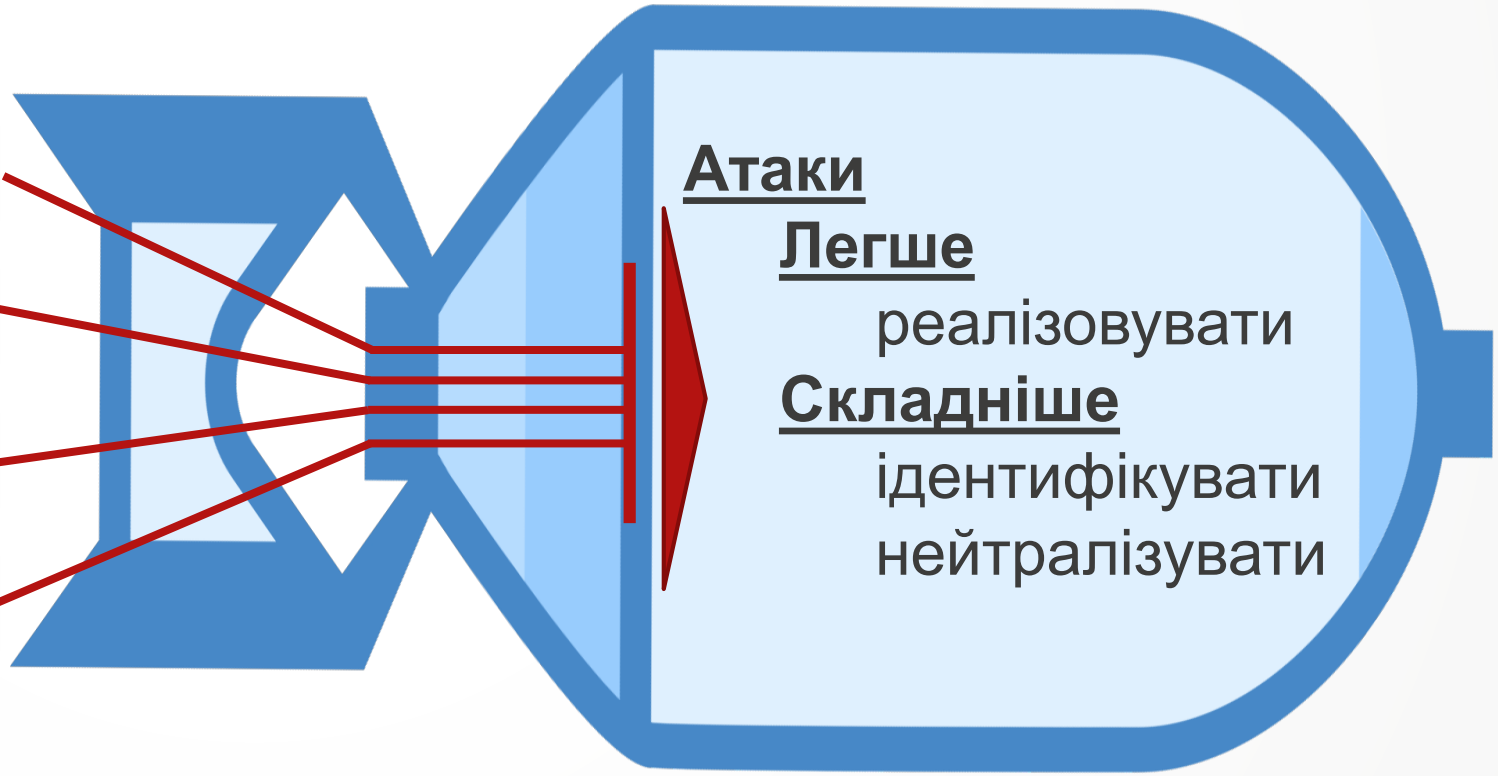
18 листопада 2017

Види загроз UC

UC Application	TDoS, Toll fraud, Vishing
UC Protocols	Call\message hijacking, eavesdropping, modification
OS	Buffer overflow, worms, DoS
Supporting services	SQL injection, DHCP resource exhaustion, XSS
Network	Flooding, Spoofing, DDoS
Physical security	Reboot, Crash, Destroy

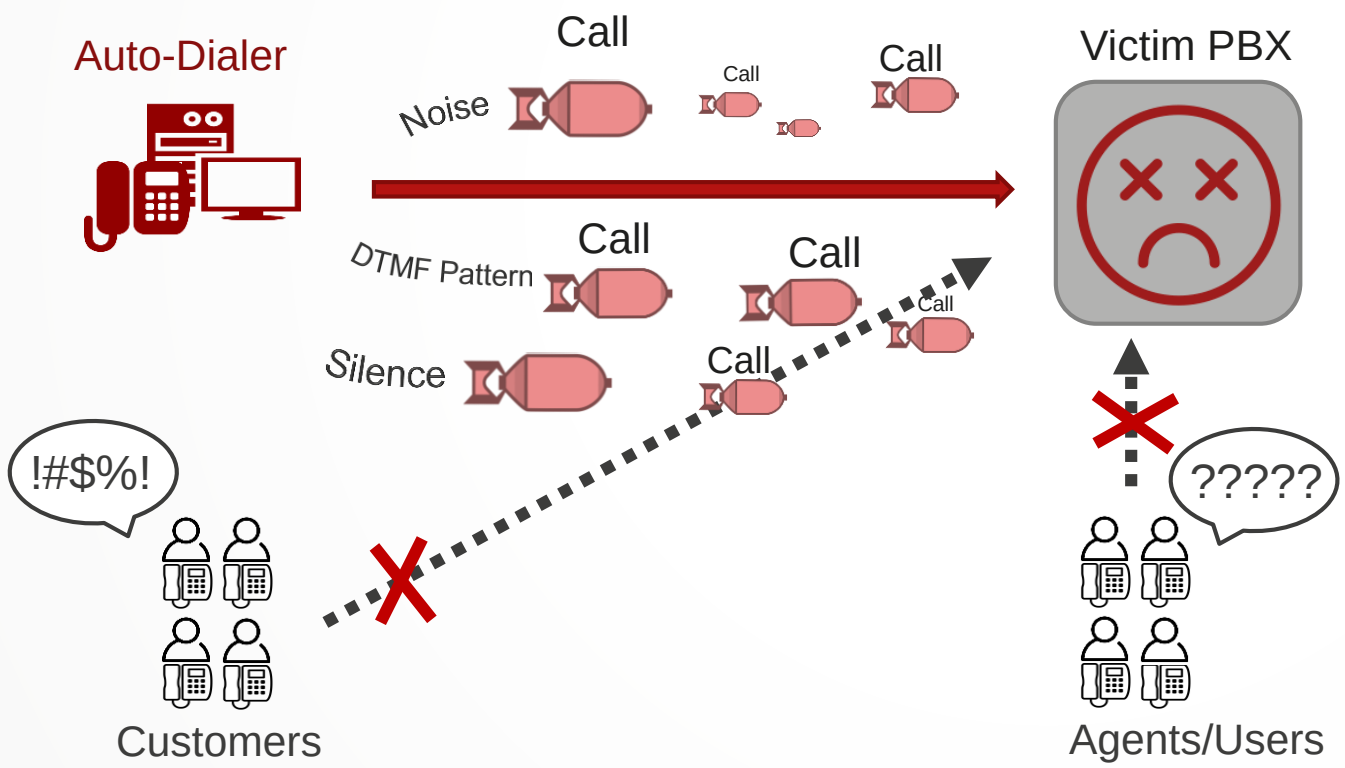
Ситуація на сьогодні

- PSTN ≈ Internet
- Міграція до SIP транків
- Free PBX, SIP підключення
- Спуфінг номеру



Telephony DoS (TDoS)

Automated TDoS

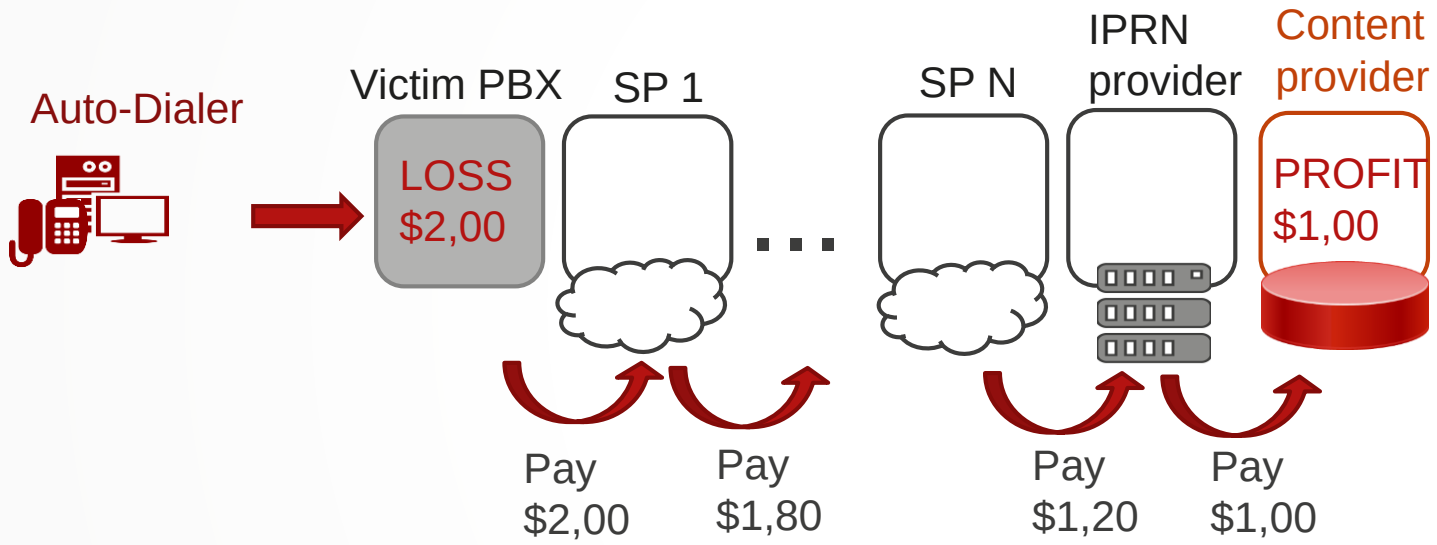


Контрзаходи

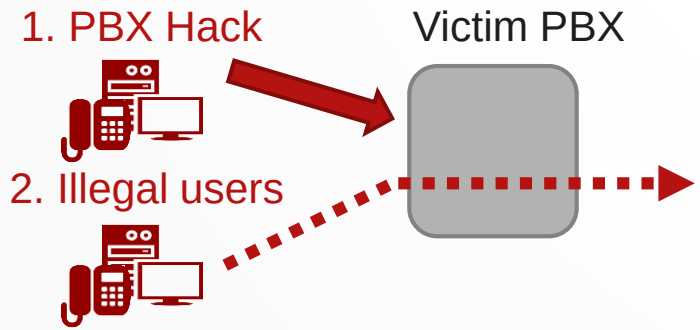
- Блокування дзвінків на основі аналізу calling number.
- Application firewall, який аналізує медіа-трафік

Toll Fraud – IRSF, DTF

IRSF



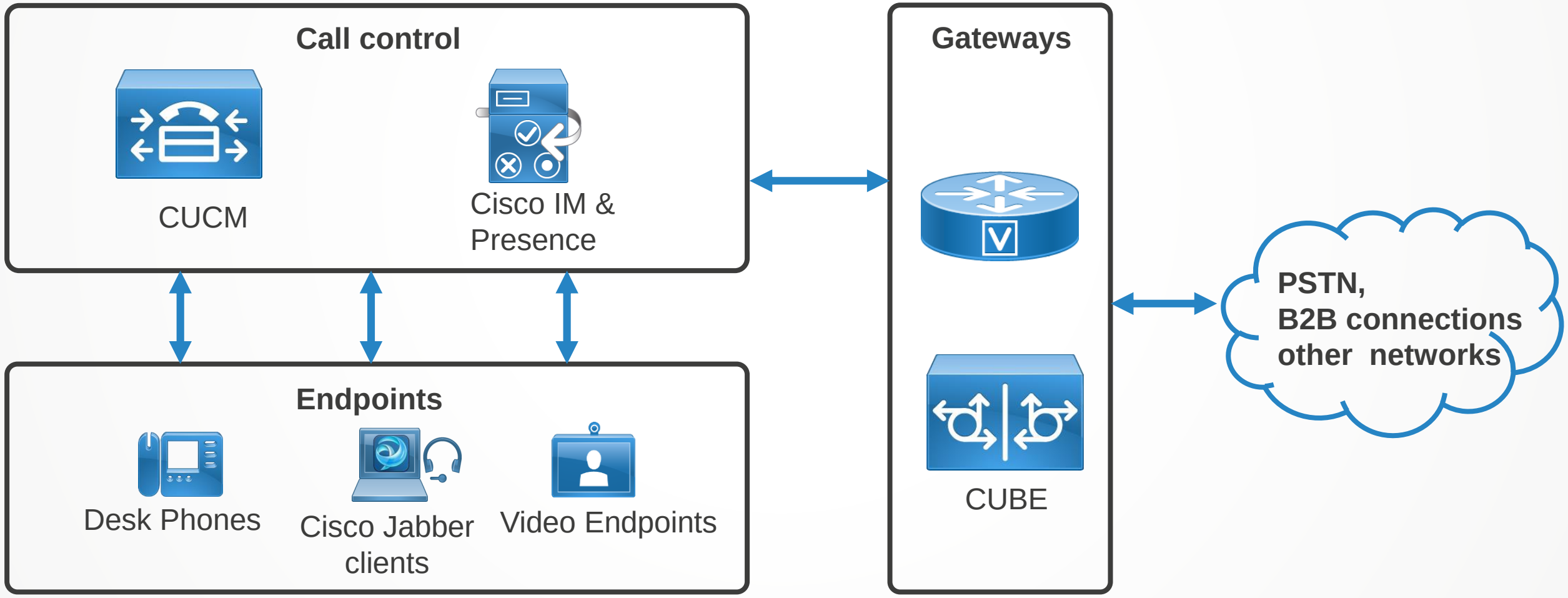
DTF



Контрзаходи

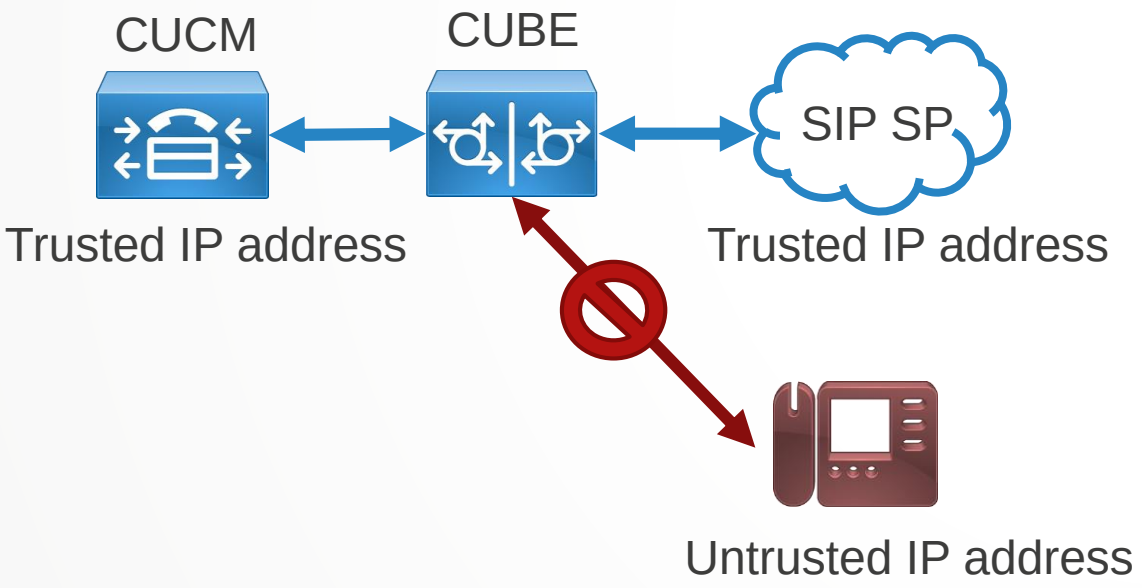
- Розмежування доступу по напрямках
- Закриття доступу до напрямків: Куба, Сомалі, Сьєрра-Леоне, Зімбабве, Сербія, Латвія і т. д.
- Аналіз CDR.

Компоненти Cisco Unified Communications Manager



Захист Gateway

IP Address Trusted Authentication

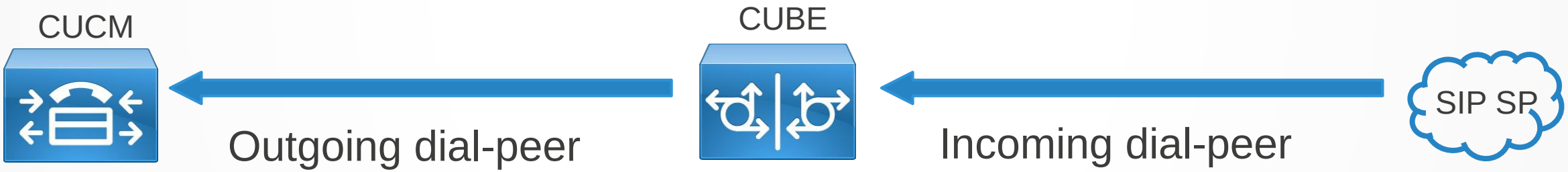


- Cisco IOS Release 15.1(2)T and later
- IP address trusted list automatic creation
- Unauthorized calls blocking
- Generate syslog messages when blocked

Захист Gateway

Dial-peer configuration

- Don’t use default destination-pattern .T
- Use explicit incoming dial-peer



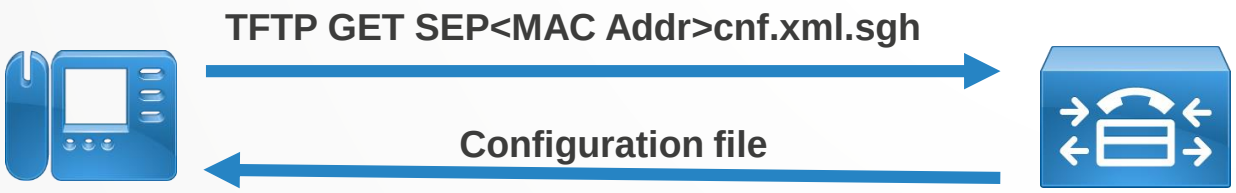

```
dial-peer voice 101 voip
description –outbound to CUCM
destination-pattern 032222334.
session protocol sipv2
session target ipv4:172.16.10.1
codec g711alaw
```

```
dial-peer voice 100 voip
description ---inbound from PSTN
incoming called-number 032222334.
session protocol sipv2
codec g711alaw
```

Захист Phones

Security By Default

- Initial Trust List (ITL) for phones
- Signed configuration files
- Configuration file encryption
- TVS+HTTPS with Web services



Disable-Disable-Disable

- PC Port
- PC Voice VLAN Access
- Span to PC Port
- Settings Access
- Web access
- Speakerphone

COMPAREX Software · Consulting · Services

Захист CUCM

- Blocking inbound calls based on Caller ID
- Signaling, media encryption: TLS, SRTP
- Do not use <*None*> CSS, partition
- Time of Day Routing
- Block Off-Net to Off-net Transfers
- Disable Auto-registration
- New Features (CUCM ver 12.0) - SIP Trunk – Trusted/Untrusted CallerID in SIP header : From, RPID, PPI, PAI
- New Feature (CUCM ver 12.0) – TLS minimum version

Дякую за увагу!