
NET
SYSTEM

Příklady fraud útoků

Jiří Novák, j.novak@netsystem.cz

NET-SYSTEM s.r.o.

CISCO SYSTEMS

NET SYSTEM

Agenda

- Úvod
- Tři případy
  - popis prostředí
  - popis útoku a jeho dopad
  - návrh obrany
- Závěr

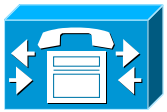
Úvod

- Nebudou jmenováni zákazníci, operátoři apod.
- Net-System je zaměřen na Cisco technologie
  - dokumentované případy jsou důsledkem špatné konfigurace nikoliv použité technologie

Úvod

- Terminologie
  - Hlasová brána

    - IOS – firmware řídící Cisco routery/brány
  - CCM = CUCM – Cisco Unified CallManager



    - SW ústředna pro firemní prostředí
  - CCME = CUCME – Cisco Unified CallManager Express
    - jednodušší verze CCM přímo na hlasové bráně
    - vlastnosti konfigurace jsou shodné jako pro bránu
  - Firewall

Úvod

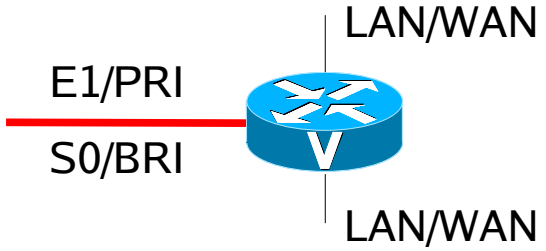
- Analogové rozhraní = FXS/FXO – rozhraní pro připojení analogového přístroje, faxu nebo analogové státní linky
- Digitální/TDM rozhraní = BRI/ISDN2, PRI/ISDN30/E1 – rozhraní pro připojení digitálního přístroje nebo digitální státní linky
- VoIP rozhraní – IP rozhraní schopné přijmout VoIP provoz
- IP trunk/VoIP trunk – VoIP propoj mezi dvěma ústřednami (H.323 trunk, SIP trunk)

Úvod

- Signalizace – řízení hovoru
  - navázání a ukončení hovoru, služby během hovoru
  - protokoly H.323, SIP, MGCP, MEGACO, SKINNY, IAX a další
- RTP – vlastní přenos hlasu
  - signalizace určuje, odkud a kam „poteče“ RTP

Úvod

- Hlasová brána
  - router doplněný „hlasovými“ kartami
  - převádí VoIP do TDM a zpět
    - průchozí VoIP hovory vidí jako data a směruje jako router (výjimkou je IP2IP gateway = CUBE)
    - signalizace může být H.323, SIP, MGCP
  - může dělat firewall, NAT, PAT apod.
    - firewall a NAT/PAT rozumí mnoha aplikačním protokolům včetně H.323 a SIP
      - prostupy pro RTP se odvozují dynamicky ze signalizace



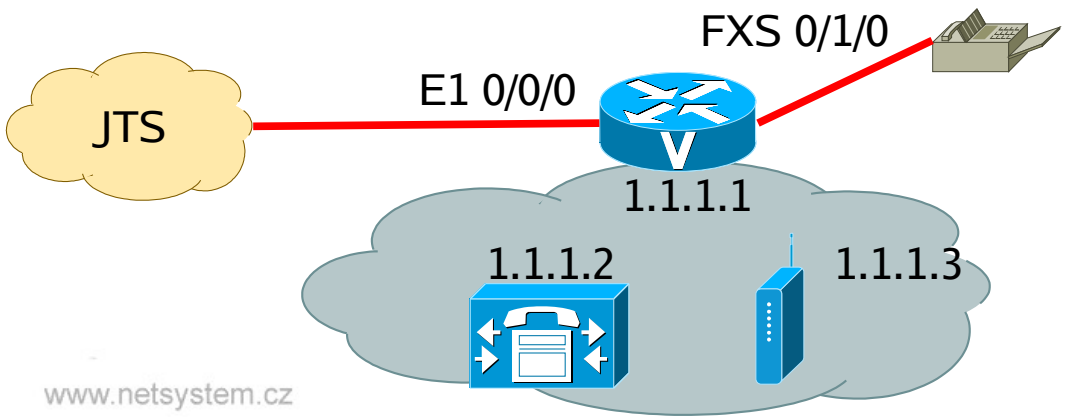
Úvod

- Směrování hovorů na bráně
  - brána „vidí“ hovor jen pokud je cílen na některé VoIP rozhraní brány – při přechodu média TDM<->VoIP
  - směrování hovoru pomocí tzv. dial-peeru
    - shoda čísla se vzorem (např. 0T, 123.., 38[1-5])
    - převážně na základě volaného čísla
    - co není popsáno, je nedovolatelné
  - mnoho možností přepisu čísel

Úvod

```
dial-peer voice 1 pots
 description Odchozi vnitrostatni
 destination-pattern 0[2-9].......
 no digit-strip
 port 0/0/0:15
!
dial-peer voice 2 pots
 description Odchozi mezistatni
 destination-pattern 000T
 no digit-strip
 port 0/0/0:15
!
dial-peer voice 20 pots
 description Analogovy fax
 destination-pattern 196
 port 0/1/0
```

```
dial-peer voice 150 voip
 description Volani na GSM branu
 destination-pattern 060[1267]......
 session protocol sipv2
 session target ipv4:1.1.1.3
 codec g711alaw
!
dial-peer voice 154 voip
 description Volani na CCM
 destination-pattern ...
 session target ipv4:1.1.1.2
 codec g711alaw
```



Úvod

- Zvláštní vlastnosti Cisco hlasových bran
  - podpora analogových i TDM rozhraní
    - z důvodu kompatibility je výchozí stav ignorování čísel uvedených v TDM signalizaci (ignoruje volané číslo v SETUP zprávě)
    - důsledkem je two stage dialing a mnoho zmatků
  - brána s H.323/SIP směruje hovory „sama“
    - brána nezkoumá, odkud hovor přichází (IP adresa, volající číslo, protokol)
    - VoIP hovor akceptuje na jakémkoliv IP rozhraní (kterékoliv má IP adresu), jakýmkoliv protokolem (SIP/H.323)

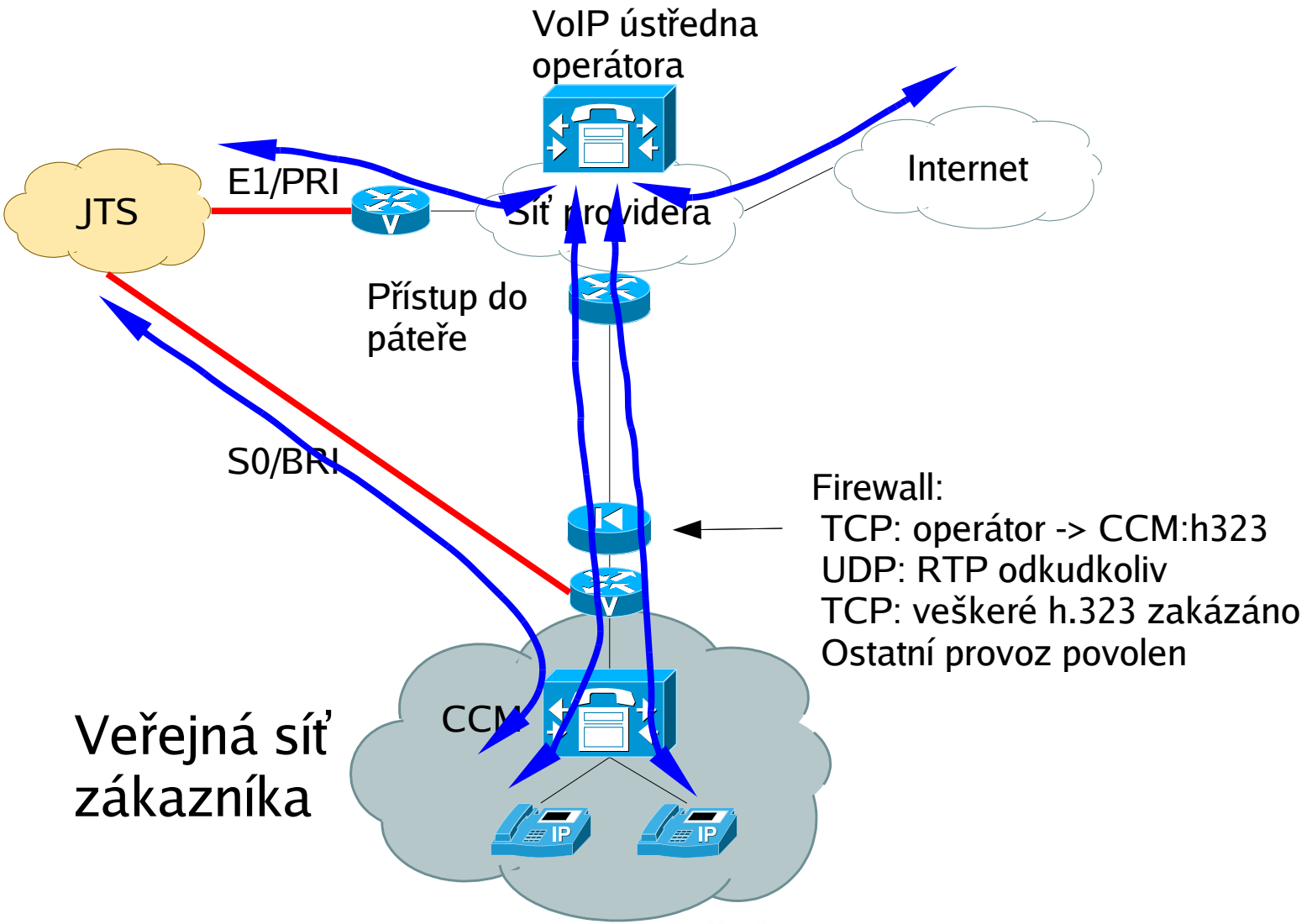
Úvod

- CCM
  - pobočková VoIP ústředna
  - zajišťuje překlad signalizace mezi koncovými telefony, VoIP trunky a hlasovými bránami
  - management/monitoring/billing

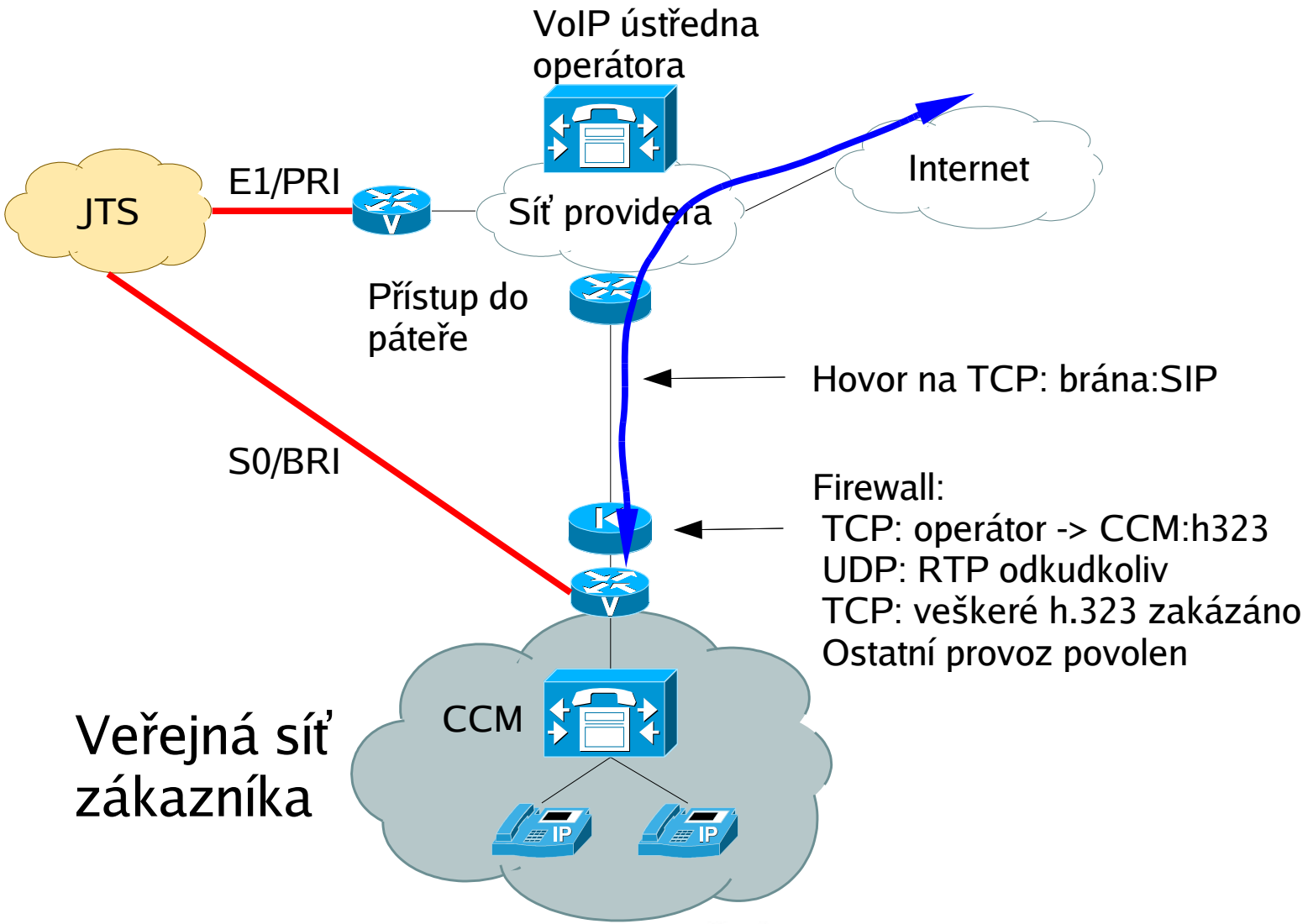
Případ 1

- Scénář – vánoce 2007/2008
  - zákazník připojen pomocí H.323 trunku k operátorovi
  - zákazník zajišťoval bezpečnost pomocí vlastního firewallu
  - lokální záloha spojení do JTS
  - vnitřní VoIP infrastruktura na veřejném IP rozsahu
  - směrování hovorů řídil CCM

Případ 1 – zapojení



Případ 1 – útok



Případ 1 – útok

- Nevěděli jsme, že IOS defaultně akceptuje i SIP hovory – nebylo bráněno firewallem
- Na útok zareagoval fraud protect systém operátora na základě měsíční faktury
  - bohužel upozornil jen zodpovědného obchodníka, který měl dovolenou
- Ztráta 160 000
- Po zjištění, že útok přišel ze zahraničí se dál neřešilo

Případ 1 – útok

- Útoky byly asi dva
- Hlasová brána vůbec negenerovala CDR, protože nebyly třeba – dlouho se proto hledalo, co se vlastně děje
  - „skutečná“ ústředna (CCM) říkala, že se nic neděje, ale operátor viděl hovory
    - na základě předchozí zkušenosti byl problém původně odložen jako chyba na straně operátora

Případ 1 – útok

- První útok – nejsou CDR z brány
  - z výpisů operátora víme, že vše byly hovory jen na Kubu
  - čísla nebyla žádným způsobem zvláštní
    - asi šlo o náhodně generovaná čísla – nevíme, kolik hovorů bylo neúspěšných
    - délky hovoru byly převážně do 30 vteřin
    - hovor každou 1-2 minuty – intenzivní
  - operátor nebyl schopen dodat nic jiného než scan papírových výtisků CDR, které bylo třeba ještě zaplatit!

Případ 1 – útok

- Druhý útok – jsou CDR z brány
  - byl veden skrz bota na PC v Izraeli
    - kontaktován správce tamní sítě, ale dál to k ničemu nevedlo
  - útok byl vlastně začátek útoku – vyhledávání prefixu

Případ 1 – útok

- šlo o sekvenci volání z `519936283264` (možná Peru) na `xxxxxx21222741082` (možná Maroko) a `xxxxxx` se průběžně měnilo i když ne zcela náhodně, ale ani v sekvenční řadě
- útok prošel rozsah `112xxx`, `150xxx`, pak přešel k `2xxxxx` a zastaven/objeven byl v řadě `6xxxxx`
  - úspěšných hovorů bylo kolem 30 denně – asi obrana proti „nalezení“
  - hovory byly bez 00 – byly národní, takže to vyšlo docela „levně“

Případ 1 – útok

- za zaznamenané 4 dny
  - uskutečnilo se 130 hovorů (většina skončila na timer 20 vteřin => ISDN kód 66h)
  - pokus o dalších 8295 hovorů
    - 7300 => 7Fh – chyba v síti, blíže nespecifikováno
    - 333 => 22h – není volný kanál pro uskutečnění hovoru
    - 660 => 01h – nepřidělené číslo

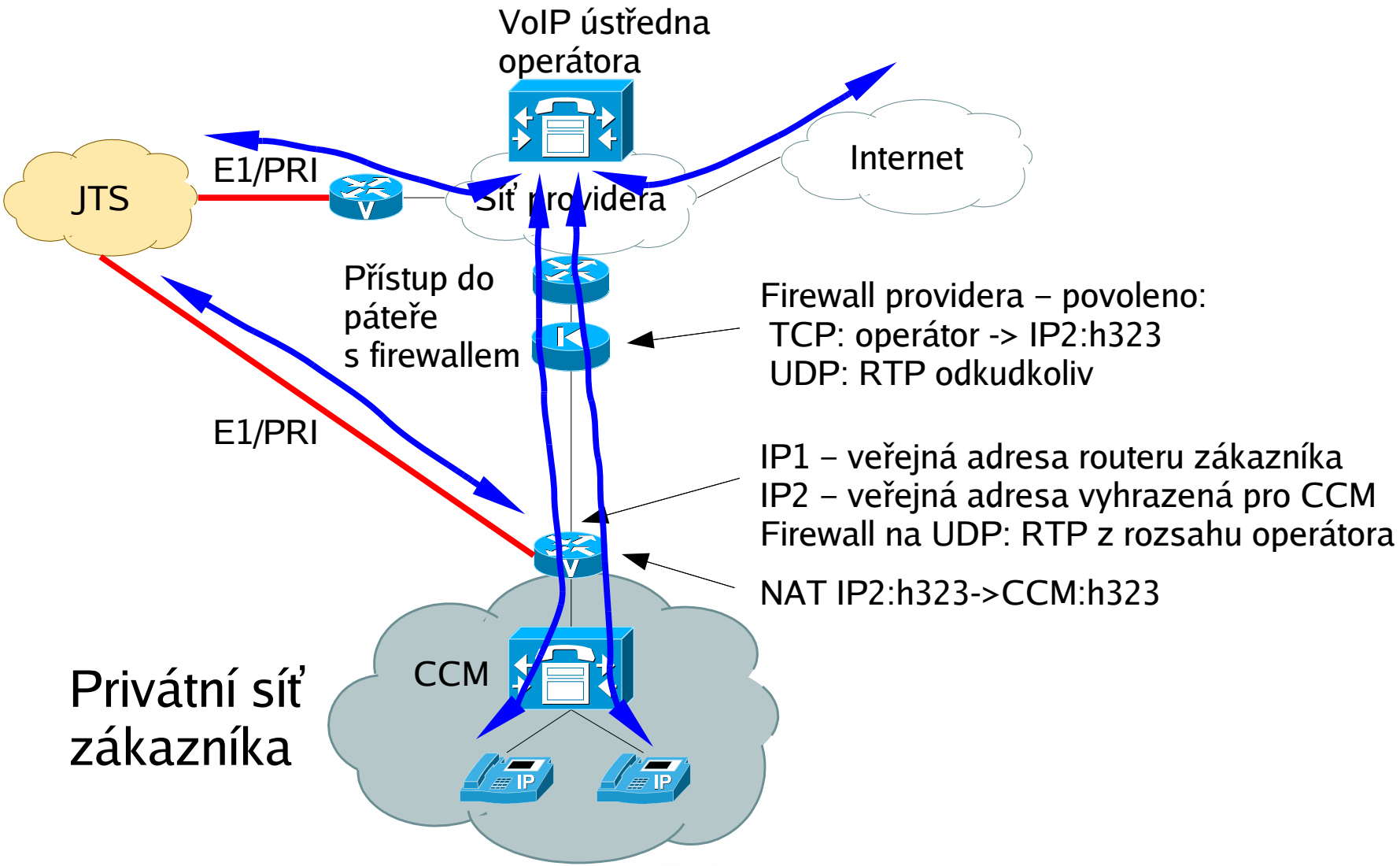
Případ 1 – obrana

- Při obraně bránit všechny hlasové prvky i proti věcem, které nepoužíváte
- Seznamovat se s vlastnostmi firmware
- Vypínat nepotřebné vlastnosti
  - zapnutým nevyužívaným a nebráněným SIPem v té době trpěla velká část instalaci v CZ (a asi i ve světě)
- Vždy generovat CDR, i když jsou na první pohled zbytečné

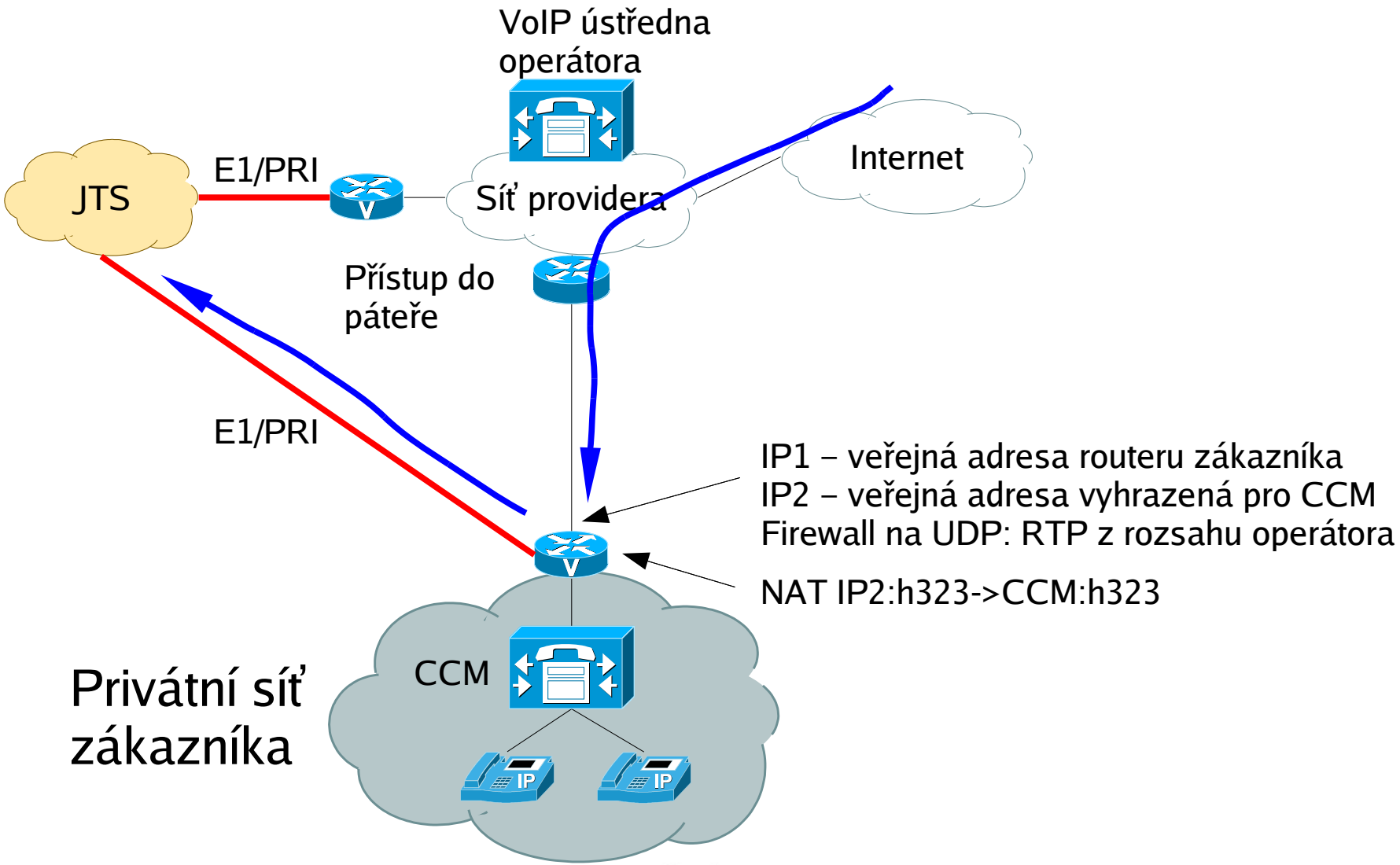
Případ 2

- Scénář – půlka roku 2008
  - zákazník připojen pomocí H.323 trunku k operátorovi
  - operátor zajišťoval bezpečnost pomocí firewallu
  - lokální záloha spojení do JTS
  - vnitřní VoIP infrastruktura na privátním IP rozsahu – překlad pomocí PATu
  - směrování hovorů řídí CCM

Případ 2 – zapojení



Případ 2 – útok



Případ 2 – útok

- Operátor bez varování odstranil firewall
  - útok probíhal na IP1 i IP2
- Na útok se přišlo až při faktuře od operátora
  - v půlce dalšího měsíce
  - nejsou CDR záznamy
- Ztráta 300 000 Kč
- Podáno trestní oznámení na neznámého pachatele – bez výsledku

Případ 2 – útok

- IP1 je VoIP/TDM brána a tudíž hovory zpracovávala
  - interní FW blokoval RTP pakety a tudíž se nepřenášel hlas/zvuk
  - CDR nebyly zapnuté, neměly být třeba
- CCM/IP2 hovory ignoroval/nespojoval, protože byly vedeny na špatná čísla
  - hovory tarifikace ignorovala, protože se „nestaly“

Případ 2 – útok

- Útok byl veden automatem
  - nejdříve automat hledal provolbu, skrz kterou projde – začínal USA provolbami
    - nalezení provolby trvalo několik hodin
  - následně se volalo na barevné linky ve vzdálených lokacích
  - hovory trvaly lehce přes minutu a byly ukončovány
  - neprocházel hlas!

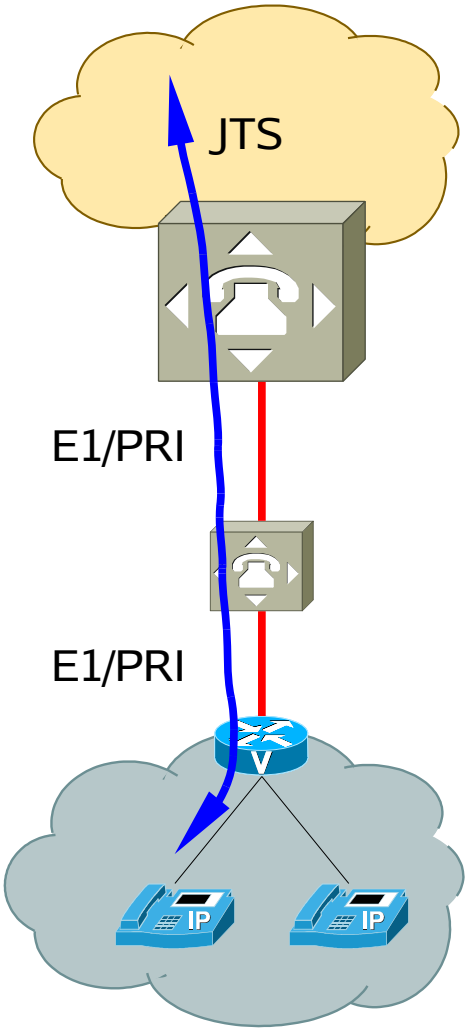
Případ 2 – obrana

- Nevěřit při obraně „nikomu“
  - firewall na bráně:
    - propouštět VoIP signalizaci jen z vnitřních ústředen na vnitřní rozhraní brány
    - propouštět VoIP provoz z Internetu na CCM – třeba kvůli H.323 trunku
  - obecně limitovat VoIP provoz jen na to, co nutně potřebujeme pro provoz
    - obrana proti nakažení vnitřních strojů viry/boty
  - zpracování CDR ze všech zdrojů, které jsou k dispozici

Případ 3

- Scénář – konec roku 2009
  - zákazník připojen pomocí TDM, VoIP používá jen pro připojení telefonů k ústředně
  - zákazník připojen k mezioperátorovi
  - směrování hovorů řídí CCME
  - CCME včetně konfigurace dodán jako služba zákazníkovi mezioperátorem
    - konfiguraci dodala mezioperátorovi externí firma

Případ 3 – zapojení



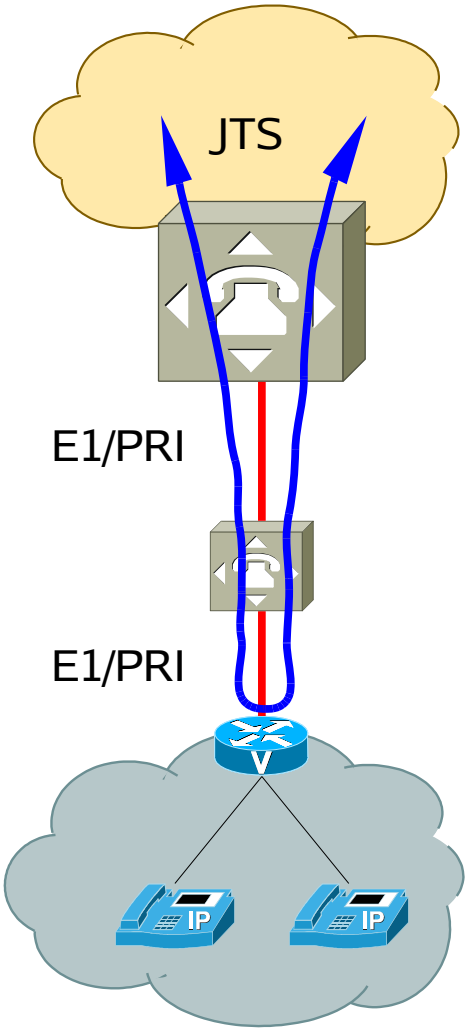
Ústředna velkého operátora

Ústředna „mezioperátora“

CCME připojený do JTS pomocí TDM

LAN zákazníka

Případ 3 – útok



Ústředna velkého operátora

Ústředna „mezioperátora“

CCME připojený do JTS pomocí TDM

LAN zákazníka

Případ 3 – útok

- Na útoku není nic „VoIP“
  - CCME byl nakonfigurován nevhodně a umožnil „otočit“ volání zpět do JTS
  - mezioperátor nelimituje délku volaného čísla
- Na útok se přišlo až při faktuře od operátora
- Ztráta 700 000 Kč
- Právníci řeší, kdo za to může

Případ 3 – útok

- Brána byla nevhodně konfigurována
  - konfigurace vycházela z předpokladu, že volané číslo odpovídá jen rozsahu zákazníka (1xx-9xx)
  - pro ostatní čísla ignorovala volané číslo v SETUP zprávě a následně očekávala pokračování volby – two stage dialing
    - při útoku stačilo poslat jen prefix zákazníka (6 místo 9 číslic) nebo jako vnitřní linku uvést 000
  - průběh útoku sledován/ověřen během probíhajícího útoku

Případ 3 – útok

- O rozsahu útoku nevíme mnoho
  - CDR nejsou a výpisy jsou nyní jsou v režimu „zatloukání“
  - CCME u zákazníka negeneruje CDR
  - mezioperátor neměl žádný nástroj na kontrolu/obranu proti fraudu

Případ 3 – útok

Ukázka z původní konfigurace

```
dial-peer voice 1 pots
 description Prichozi hovory
 incoming called-number [1-9]..
 direct-inward-dial <- Zajišťuje to, že se uvažuje číslo v SETUPu
!
dial-peer voice 2 pots
 description Odchozi mezistatni hovory
 destination-pattern 000T
 no digit-strip
 port 0/0/0:15
```

Případ 3 – obrana

- Vždy zajistit převzetí čísla ze signalizace
  - uvažovat i o „nesmyslných“ kombinacích
  - zajistit blokování neznámých čísel
- V případě Cisco použít buď přepisovací pravidla a blokování nebo cor listy
  - přepisovací pravidla jsou jednodušší a dostatečné

Případ 3 – obrana

Návrh úpravy

```
! Přepsat neznámá čísla na nějaké nepoužívané, např. na 999
voice translation-rule 1
 rule 1 /^211111\([1-9]..\)$/ /\1/
 rule 2 /^.*/ /999/
voice translation-profile jts_dovnitr
 translate called 1

! Vytvořit profil pro zablokování hovorů
voice translation-rule 6
 rule 1 reject /^.*/
voice translation-profile zablokuj
 translate called 6
```

Případ 3 – obrana

```
! Aplikovat přepisy na příchozí hovory
voice-port 0/0/0:15
 translation-profile incoming jts_dovnitr

! Zablokovat neznámá čísla (která byla přeložena na 999)
dial-peer voice 101 pots
 call-block translation-profile incoming zablokuj
 call-block disconnect-cause incoming call-reject
 incoming called-number 999$
```

Závěry

- Není pochyb o tom, že útoky budou pokračovat
- Útoky jsou/mohou být vysoce automatizované
- Existují seznamy známých děravých instalací
  - ještě měsíce po odstranění problému jsme viděli v CDR a logu firewallu pokusy o útoky

Závěry

- Znát své ústředny/brány
  - možnosti i podivné vlastnosti
  - hned od začátku využívat všech možností omezení volání
    - oprávnění – blokovat neobvyklé směry
    - přepisy čísel – přepsat vše neznámé na spojovatelku apod.
    - vypnout možnost přepojení příchozího hovoru směrem ven
  - sledovat aktualizace SW a změny výchozích hodnot

Závěry

- Vypnout nepotřebné služby/protokoly
  - úplné vypnutí hlasových služeb

```
voice service voip
 shutdown
```

  - vypnutí H.323

```
voice service voip
 h323
  call service stop
```

  - vypnutí SIP

```
voice service voip
 sip
  call service stop forced
```

Závěry

- Bránit infrastrukturu firewally
  - výchozí nastaveni firewallu – vše zakázáno
  - povolit jen signalizaci mezi ústřednami/bránami
  - pro útok po VoIP je třeba signalizace
    - pokud prochází RTP, může dojít „jen“ k DOS útoku
    - mnoha VoIP řešením nevadí, že RTP k hovoru chybí
  - bránit i proti vnitřním prvkům, např. PC
    - komplikací jsou SW telefony

Závěry

- Vždy generovat CDR
  - třeba je jen ukládat a pravidelně kontrolovat, že se tak děje
  - třeba pro dokazování, co se stalo
- Používat aktivní kontroly
  - revize konfigurací
  - kontroly konzultačních firem (nejlépe jiných, než řešení prodaly/dodaly)
  - „generátory“ útoků

Závěry

- Ve smlouvách řešit vlastnictví/odpovědnost
  - za prvky
  - za konfigurace
    - i s firmami, které poskytují subdodávky
  - za sběr/ztráty CDR
    - i s firmami, které poskytují subdodávky
  - za následky
    - jak z pohledu odběratele, tak z pohledu poskytovatele

Děkuji za pozornost

Prostor pro dotazy