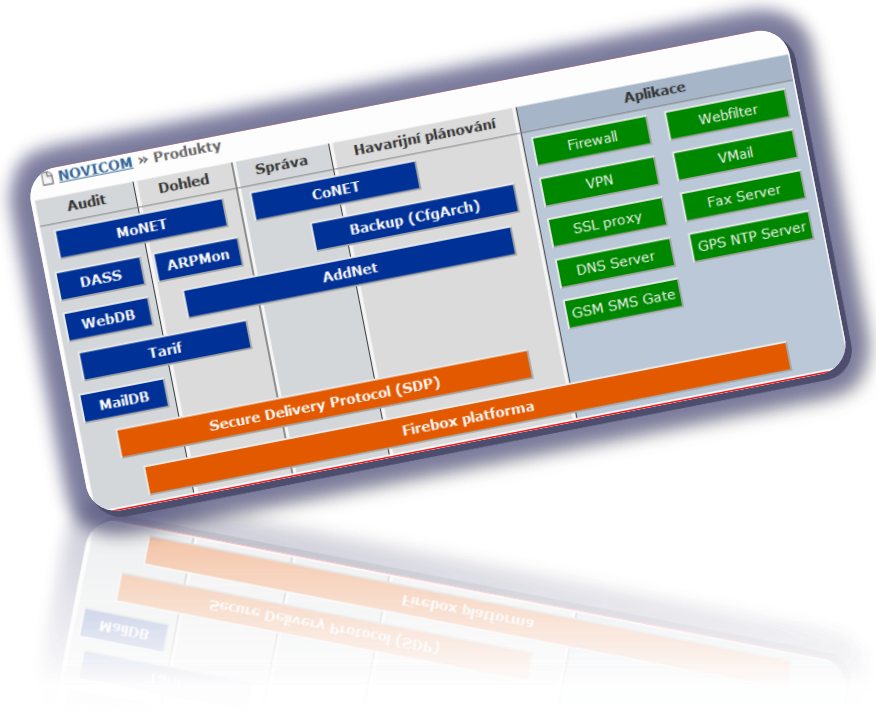
Zabezpečení mobilní komunikace.



Novicom MTN
Mobile Trusted Network

Petr Linke
ředitel společnosti

4.4.2012

Obsah prezentace

Situace na trhu

- **Obrovský nárůst využití mobilních zařízení**
  - mobilní telefony
  - tablety
- **Požadavky na bezpečnost podceňovány**
  - jsou realizovány maximálně základní bezpečnostní opatření, pouze partikulárně
  - požadavek na univerzální a snadnou použitelnost je v rozporu s bezpečností
- **Požadavky firemních zákazníků a institucí**
  - přístup k datům a aplikacím odkudkoliv
  - zabezpečené terminály

Mobilní zařízení

- **Nový fenomén – každý má svoje „mobilní PC"**
  - postaveno zpravidla na UNIX based OS
    - Android
    - iOS
- **Použití mobilních zařízení**
  - klasické GSM služby
    - hlas a SMS
  - datové služby
    - mail, aplikace
    - internet banking

- **Každý si instaluje své aplikace**
  - Google Play (Android Market)
  - App Store

  - **bez centrální správy!**
  - **bez znalostí bezpečnostních aspektů!**
  - filozofie „Potvrď nebo neinstaluj“
    - bez možnosti ovlivnění dílčích parametrů

Typické hrozby pro mobilní zařízení

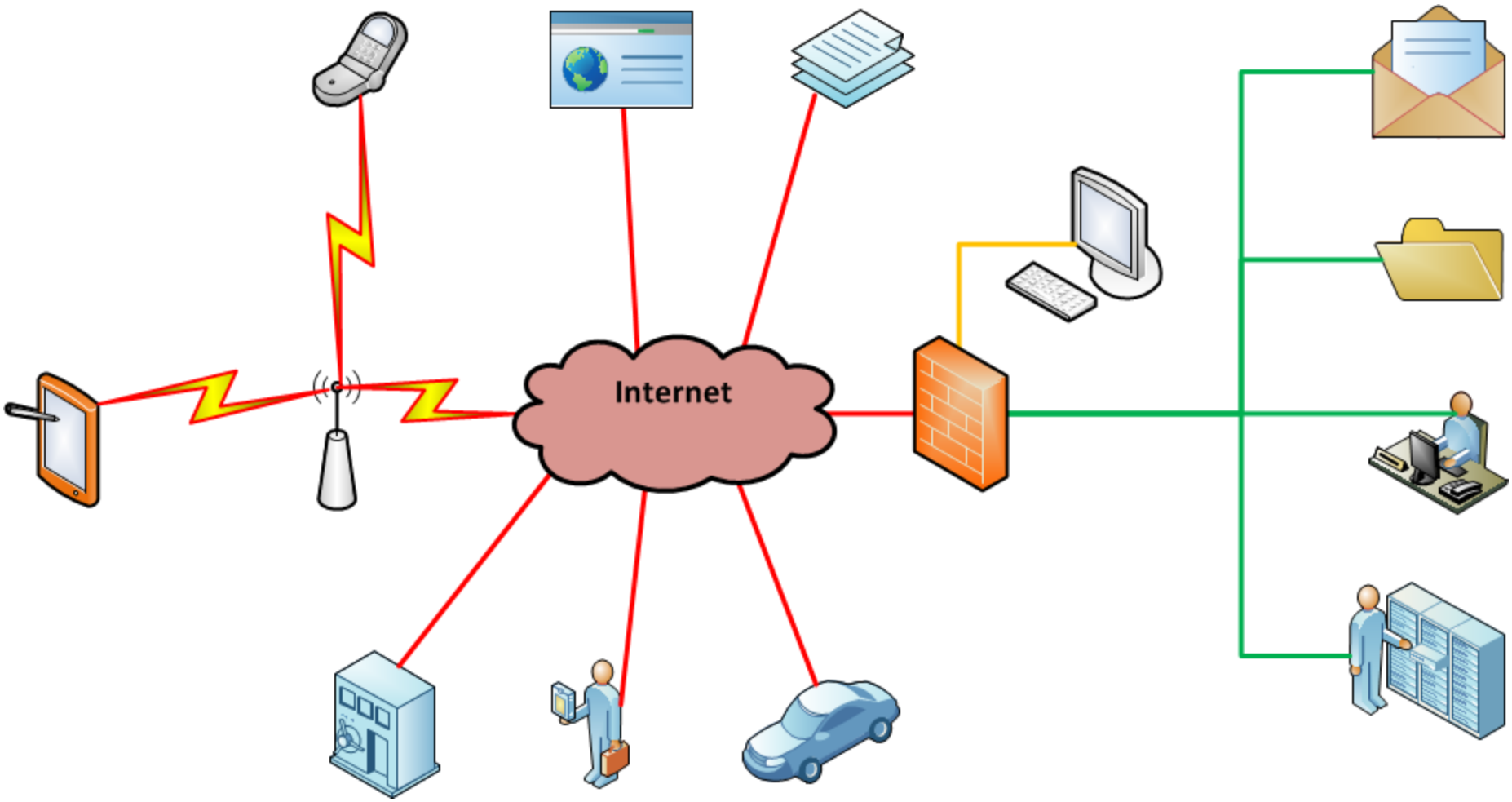
- **Neoprávněná komunikace na Premium čísla**
  - odchozí hovory
  - SMS
- **Utajené shromažďování informací**
  - informace o chování uživatele (čas, lokalita, prováděné akce)
- **Bezproblémový odposlech**
  - hovory
  - datový provoz
  - softwarová štěnice

Typické hrozby pro mobilní zařízení

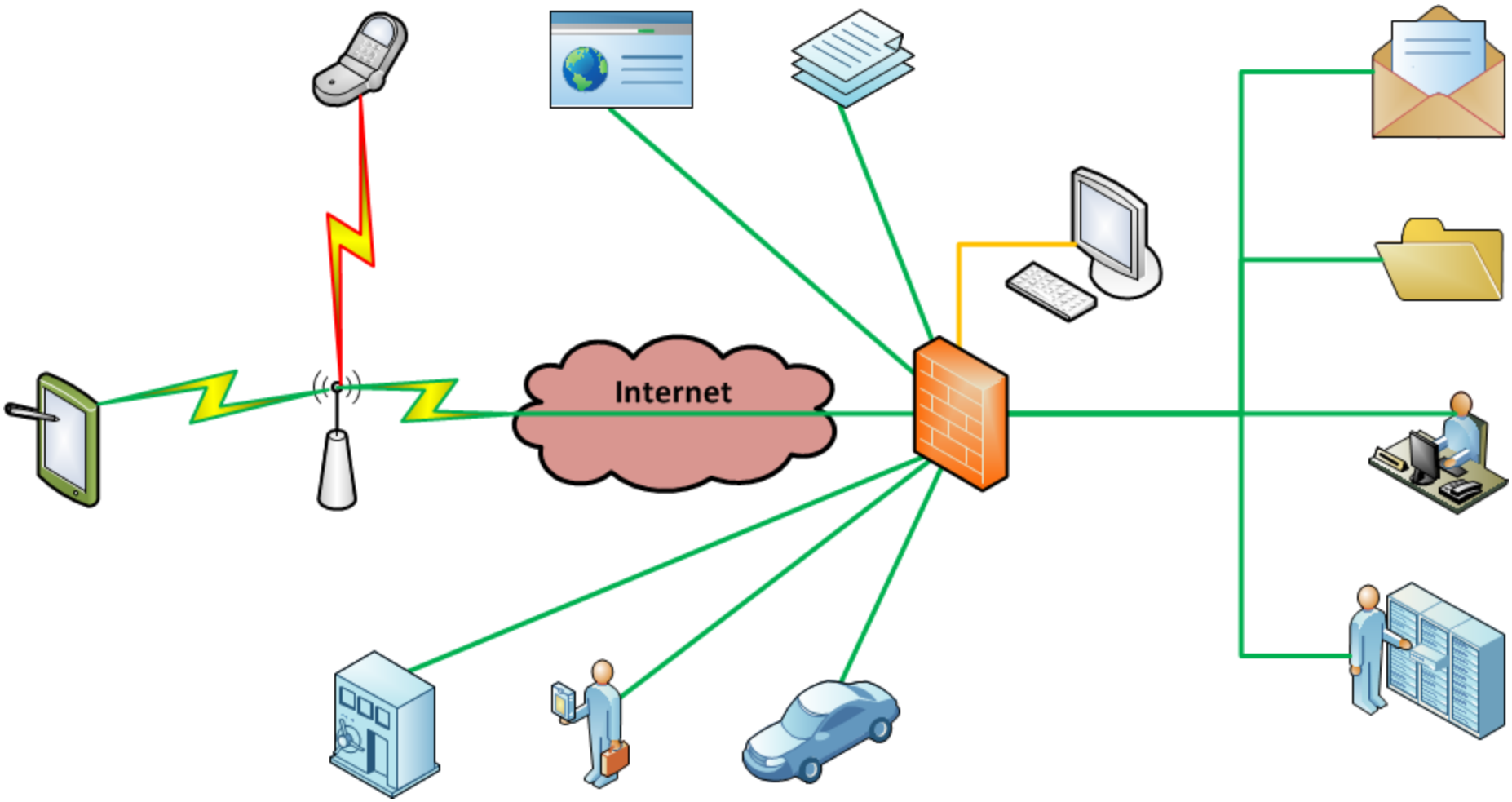
- **Zcizení přístupů a identit**
  - mailové služby
  - internetové bankovnictví
  - …

- **Možnost cíleného blokování provozu zařízení**
  - hrubou silou - DoS útok
  - selektivně (blokování vybraných služeb, adres, hovorů apod.)
- **Neoprávněné sledování pohybu (lokality) zařízení**
- **Využití mobilního zařízení pro trestnou činnost**

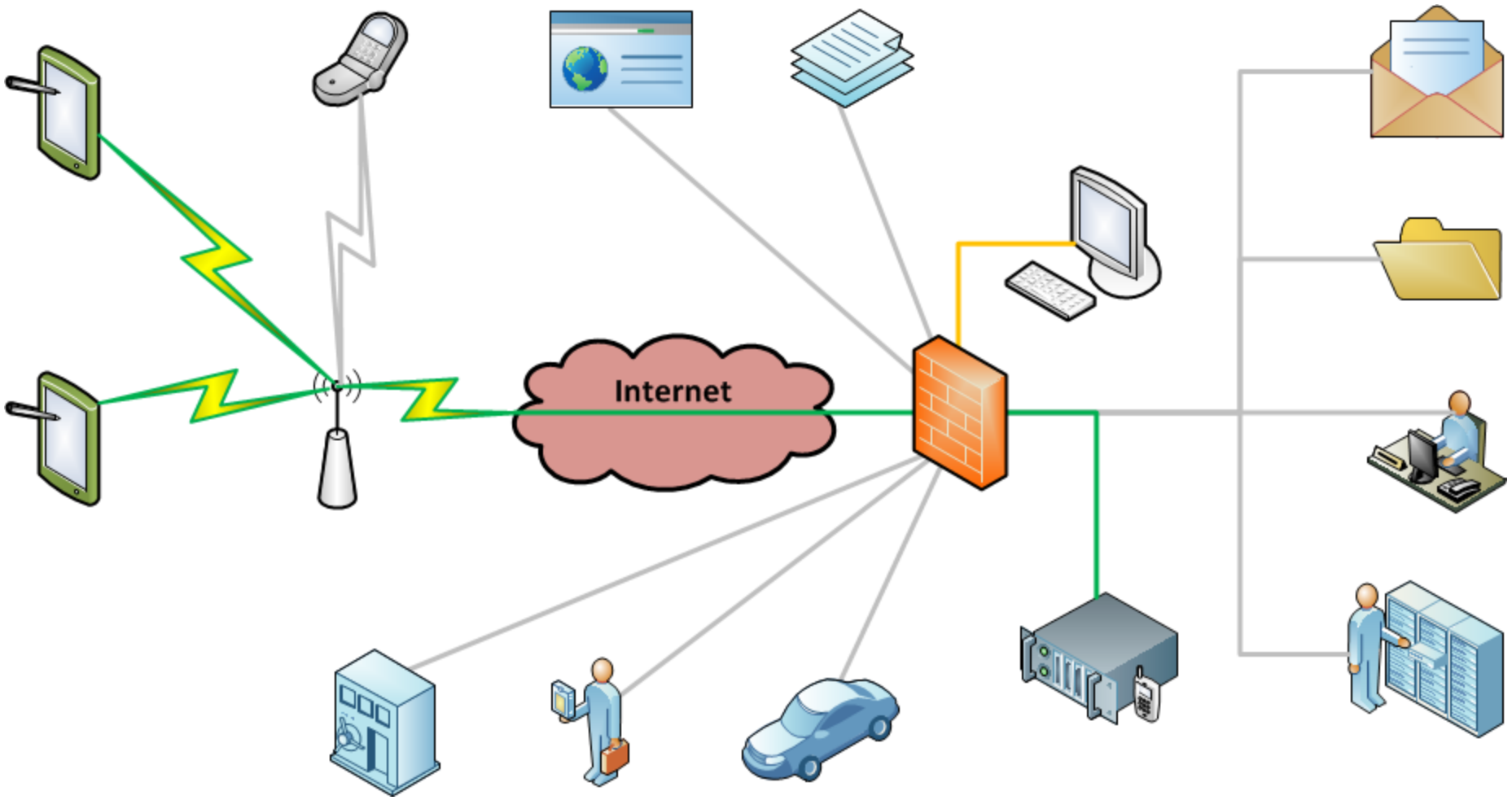
Schéma dnešního připojení



Požadavek na bezpečné datové připojení



Požadavek na zabezpečenou hlasovou komunikaci



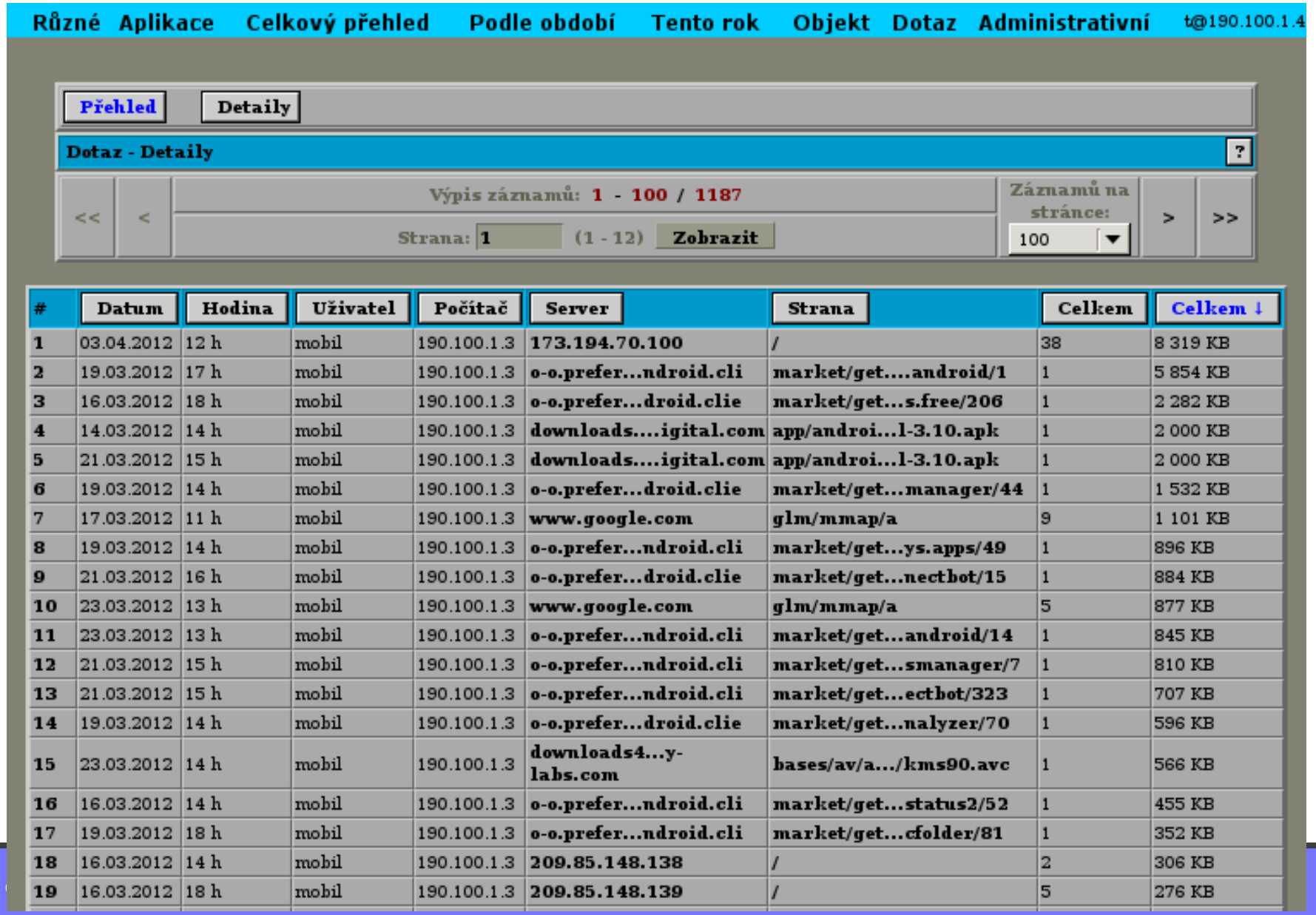
Definice produktu Novicom MTN

- **Soubor nástrojů pro**
  - zajištění mobilních zařízení Android před neoprávněnou komunikací na internetu
  - monitoring síťového provozu těchto zařízení
- **Cíl Novicom MTN**
  - dodat zákazníkům platformu pro zabezpečený mobilní přístup odkudkoliv na platformě mobilních telefonů a tabletů
- **Základní principy**
  - bezpečně
  - bez uživatelských omezení
  - s centrální správou a monitoringem

Praktická ukázka řešení

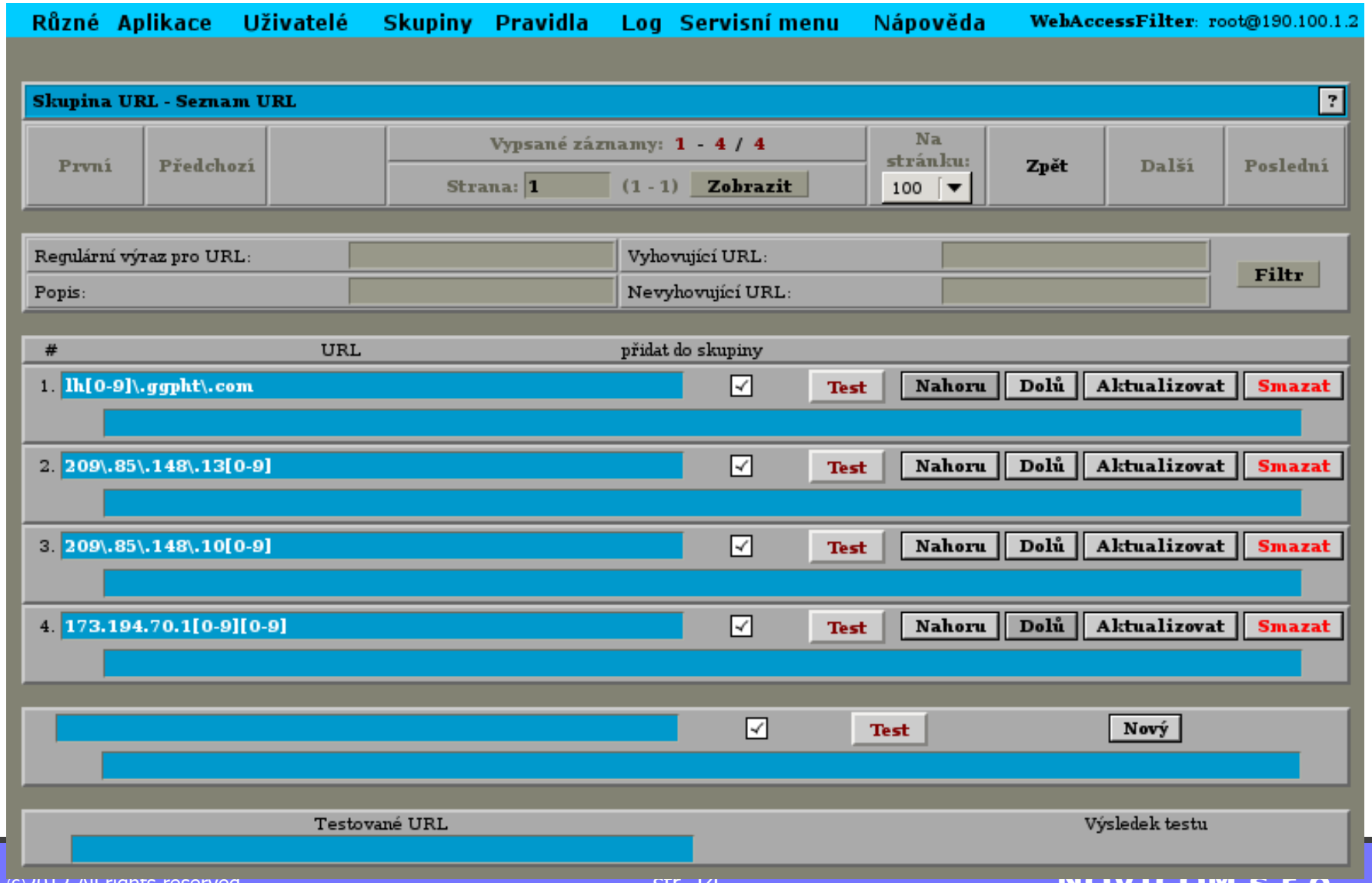
- **Novicom MTN**
  Mobile Trusted Network
  - Monitoring
  - Konfigurace pravidel

Monitoring uživatele mobilního zařízení



#	Datum	Hodina	Uživatel	Počítač	Server	Strana	Celkem	Celkem ↓
1	03.04.2012	12 h	mobil	190.100.1.3	173.194.70.100	/	38	8 319 KB
2	19.03.2012	17 h	mobil	190.100.1.3	o-o.prefer...ndroid.cli	market/get....android/1	1	5 854 KB
3	16.03.2012	18 h	mobil	190.100.1.3	o-o.prefer...droid.clie	market/get...s.free/206	1	2 282 KB
4	14.03.2012	14 h	mobil	190.100.1.3	downloads....igital.com	app/androi...l-3.10.apk	1	2 000 KB
5	21.03.2012	15 h	mobil	190.100.1.3	downloads....igital.com	app/androi...l-3.10.apk	1	2 000 KB
6	19.03.2012	14 h	mobil	190.100.1.3	o-o.prefer...droid.clie	market/get...manager/44	1	1 532 KB
7	17.03.2012	11 h	mobil	190.100.1.3	www.google.com	glm/mmap/a	9	1 101 KB
8	19.03.2012	14 h	mobil	190.100.1.3	o-o.prefer...ndroid.cli	market/get...ys.apps/49	1	896 KB
9	21.03.2012	16 h	mobil	190.100.1.3	o-o.prefer...droid.clie	market/get...nectbot/15	1	884 KB
10	23.03.2012	13 h	mobil	190.100.1.3	www.google.com	glm/mmap/a	5	877 KB
11	23.03.2012	13 h	mobil	190.100.1.3	o-o.prefer...ndroid.cli	market/get...android/14	1	845 KB
12	21.03.2012	15 h	mobil	190.100.1.3	o-o.prefer...ndroid.cli	market/get...smanager/7	1	810 KB
13	21.03.2012	15 h	mobil	190.100.1.3	o-o.prefer...ndroid.cli	market/get...ectbot/323	1	707 KB
14	19.03.2012	14 h	mobil	190.100.1.3	o-o.prefer...droid.clie	market/get...nalyzer/70	1	596 KB
15	23.03.2012	14 h	mobil	190.100.1.3	downloads4...y-labs.com	bases/av/a.../kms90.avc	1	566 KB
16	16.03.2012	14 h	mobil	190.100.1.3	o-o.prefer...ndroid.cli	market/get...status2/52	1	455 KB
17	19.03.2012	18 h	mobil	190.100.1.3	o-o.prefer...ndroid.cli	market/get...cfolder/81	1	352 KB
18	16.03.2012	14 h	mobil	190.100.1.3	209.85.148.138	/	2	306 KB
19	16.03.2012	18 h	mobil	190.100.1.3	209.85.148.139	/	5	276 KB

Definice filtrovacího pravidla



Přehled filtrovacích pravidel

Různé Aplikace Uživatelé Skupiny Pravidla Log Servisní menu Nápověda **WebAccessFilter**: root@190.100.1.2

Filtrovací pravidla - Seznam ?

První	Předchozí	Nový	Vypsané záznamy: 1 - 11 / 11 Strana: 1 (1 - 1) Zobrazit	Na stránku: 100		Další	Poslední

#	Časové okno	Skupina uživatelů	Skupina URL	Skupina IP	Povolit přístup				
1.	Všechna	G: Mobil users	G: No android market	I: 190.100.1.3	Ne	Nahoru	Dolů	Editace	Smazat
2.	Všechna	G: Mobil users	G: No meteor servis	I: 190.100.1.3	Ne	Nahoru	Dolů	Editace	Smazat
3.	Všechna	U: mobil	G: No android market	I: 190.100.1.3	Ne	Nahoru	Dolů	Editace	Smazat
4.	Všechna	G: Mobil users	Všechny	I: 190.100.1.3	Ano	Nahoru	Dolů	Editace	Smazat
5.	WORK TIME	Všichni	G: WORK DENIED URLs	Všechny	Ne	Nahoru	Dolů	Editace	Smazat
6.	Všechna	Všichni	G: DENIED URLs	Všechny	Ne	Nahoru	Dolů	Editace	Smazat
7.	WORK TIME	G: VALID USERS	G: WORK TIME URLs	G: VALID WORKSTATIONS	Ano	Nahoru	Dolů	Editace	Smazat
8.	Všechna	Všichni	G: AVP SERVERS	G: DOWNLOAD SERVERS	Ano	Nahoru	Dolů	Editace	Smazat
9.	FREE TIME	G: VALID USERS	Všechny	G: VALID WORKSTATIONS	Ano	Nahoru	Dolů	Editace	Smazat
10.	WEEKEND	G: VALID USERS	Všechny	G: VALID WORKSTATIONS	Ano	Nahoru	Dolů	Editace	Smazat
11.	Všechna	U: petr	Všechny	Všechny	Ano	Nahoru	Dolů	Editace	Smazat

Jak to funguje

- **Nastavení systému**
  - modifikace systému mobilního zařízení
    - kombinace zařízení a verze OS
    - finální provoz bez nutnosti mít privilegovaný přístup
  - nastavení přístupu na centrální FW
  - nastavení setu povolených služeb
  - nastavení monitoringu

Jak to funguje - Provoz

- **Administrace přístupů zařízení**
- **Průběžný monitoring**
  - sledování dostupnosti mobilních zařízení
  - možnost sledování síťového provozu na úrovni vyhodnocení síťových logů
    - Novicom SquidDB
  - možnost rozšíření o sledování vybraných systémových parametrů
    - GPS souřadnice/BTS lokace apod.
- **Možnost kontroly konzistence zařízení**

Shrnutí vlastností produktu MTN (Mobile Trusted Net)

- **Stejný režim práce bez ohledu na připojení**
  - Wifi i mobilní datové připojení
- **Neomezuje uživatelskou správu zařízení**
  - možnost instalace aplikací uživatelů
- **Centrální robustní řešení**
  - firewall, monitoring (MoNET), squidDB
  - redundantnost a škálovatelnost (clusterové řešení - active-active)
  - interní cache mechanismy
- **Zabezpečený klient – mobilní zařízení**
  - systémová VPN – nativní prostředí

Komu je určen a Typické využití

- **Pro koho**
  - Top managementu firem a institucí, kteří chtějí mít jistotu, že mají **pod kontrolou datové toky** svého mobilního zařízení a/nebo hledají **alternativu zabezpečené mobilní hlasové komunikace**
- **Možnosti nasazení**
  - Zabezpečení mobilního zařízení
  - Bezpečný kanál do vlastní sítě
  - Monitoring využívání a provozu
  - Centrální řízení přístupu
  - Neodposlouchávatelný datový i hlasový kanál
  - Lokalizace pohybu zařízení pro interní použití

Kontakt

Adresa

- Koněvova 67a
- Praha 3
- 130 00

Spojení

- Telefon
  - 271777231
- Email
  - sales@novicom.cz
- Web
  - www.novicom.cz