



FoxStat

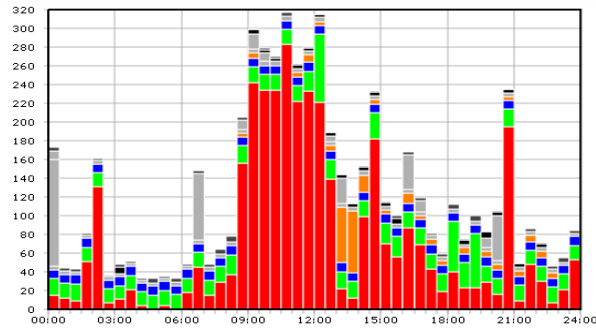
Change the **Net**.Work

Nástroj pro **záznam a analýzu**
datového provozu

LinuxBox.cz

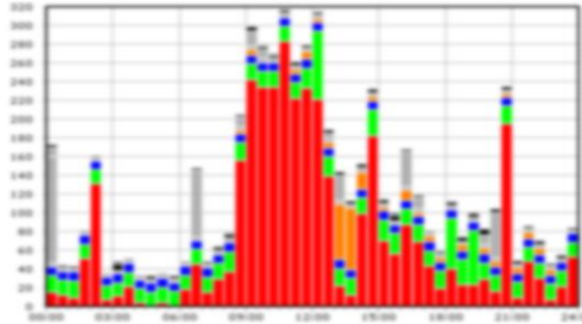
Problémy síťového administrátora

- Zátěž linky



Problémy síťového administrátora

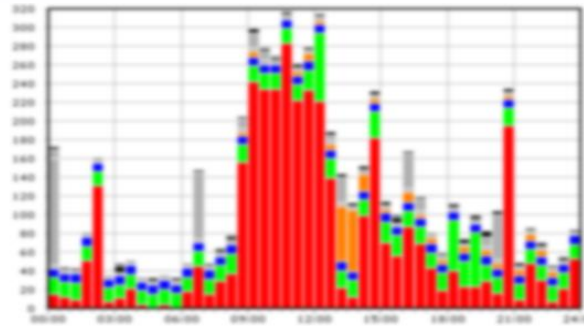
- Zátěž linky
- Obsah a debug komunikace až na úroveň paketů



Čas ▲	Délka ▾	Zdrojová MAC adresa ▾	Cílová MAC adresa ▾	Vlan Id ▾	Celková Délka ▾	Protokol (IP) ▾	Zdrojová IP ▾	Cílová IP ▾
30.02.2010 01:45:00.023274	60	00:05:dc:c7:0c:81	01:80:c2:00:00:00		0			
30.02.2010 01:45:00.137212	130	00:e0:4d:9a:b6:b8	00:30:48:91:31:90		116	6	10.76.66.32	62.245.111.135
30.02.2010 01:45:00.138590	98	00:30:48:91:31:90	00:e0:4d:9a:b6:b8		84	6	62.245.111.135	10.76.66.32

Problémy síťového administrátora

- Zátěž linky
- Obsah a debug komunikace až na úroveň paketů
- Dohledání bezpečnostních incidentů, dokazování



Čas	Délka	Zdrojová MAC adresa	Cílová MAC adresa	Vlan ID	Celková Délka	Protokol (IP)	Zdrojová IP	Cílová IP
30.02.2010 01:45:00.023274	60	00:05:40:c7:0c:81	01:90:c2:00:00:00			0		
30.02.2010 01:45:00.137212	130	00:e0:48:9a:36:38	00:30:48:91:31:90		116	6	10.76.66.32	62.245.111.135
30.02.2010 01:45:00.138590	98	00:30:48:91:31:90	00:e0:48:9a:36:38		84	6	62.245.111.135	10.76.66.32

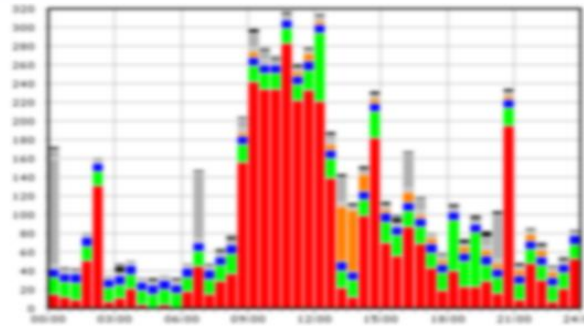
62.77.89.187:61317 < 62.245.111.135:smtp

vyvojari@foxstat.com > kolacek@random.cz : DOKLADY

```
vyvojari@foxstat.com > kolacek@random.cz : DOKLADY
inline text/plain 359B
inline text/html 527B
```

Problémy síťového administrátora

- Zátěž linky
- Obsah a debug komunikace až na úroveň paketů
- Dohledání bezpečnostních incidentů, dokazování
- Flashback problému



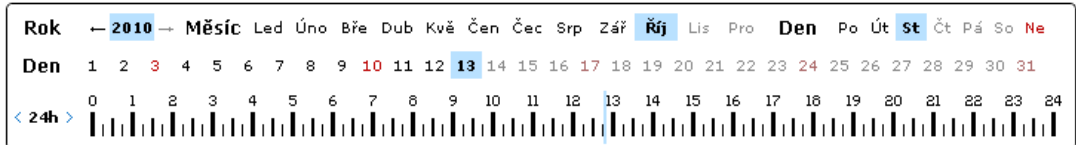
Čas	Délka	Zdrojová MAC adresa	Cílová MAC adresa	Vlan ID	Celková Délka	Protokol (IP)	Zdrojová IP	Cílová IP
30.02.2010 01:45:00.023274	60	00:05:40:c7:0c:81	01:90:c2:00:00:00			0		
30.02.2010 01:45:00.137212	130	00:e0:48:9a:36:38	00:30:48:91:31:90		116	6	10.76.66.32	62.245.111.135
30.02.2010 01:45:00.138590	98	00:30:48:91:31:90	00:e0:48:9a:36:38		84	6	62.245.111.135	10.76.66.32

62.77.89.187:61317 < 62.245.111.135:smtp vyvojar@foxstat.com > kolacek@random.cz : DOKLADY

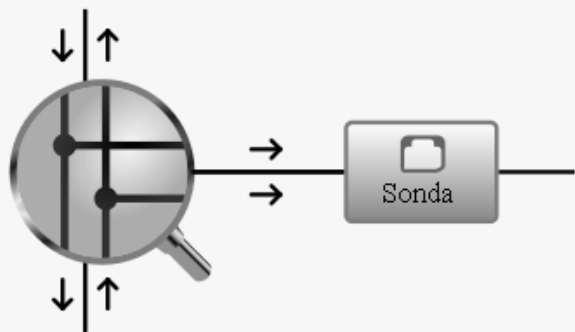
vyvojar@foxstat.com > kolacek@random.cz : DOKLADY
 inline text/plain 359B
 inline text/html 527B

Čas od - do: 13.10.2010 12:48:23 - 13.10.2010 12:53:22

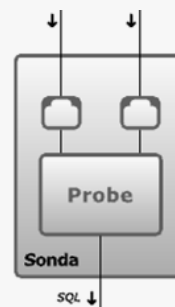
AND Rozhraní alix eth1 - eth2 in



FoxStat hlavní cíle



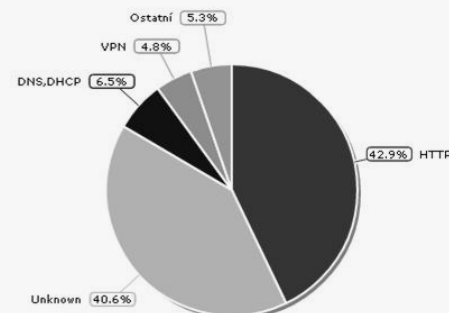
Snímání



Dekódování



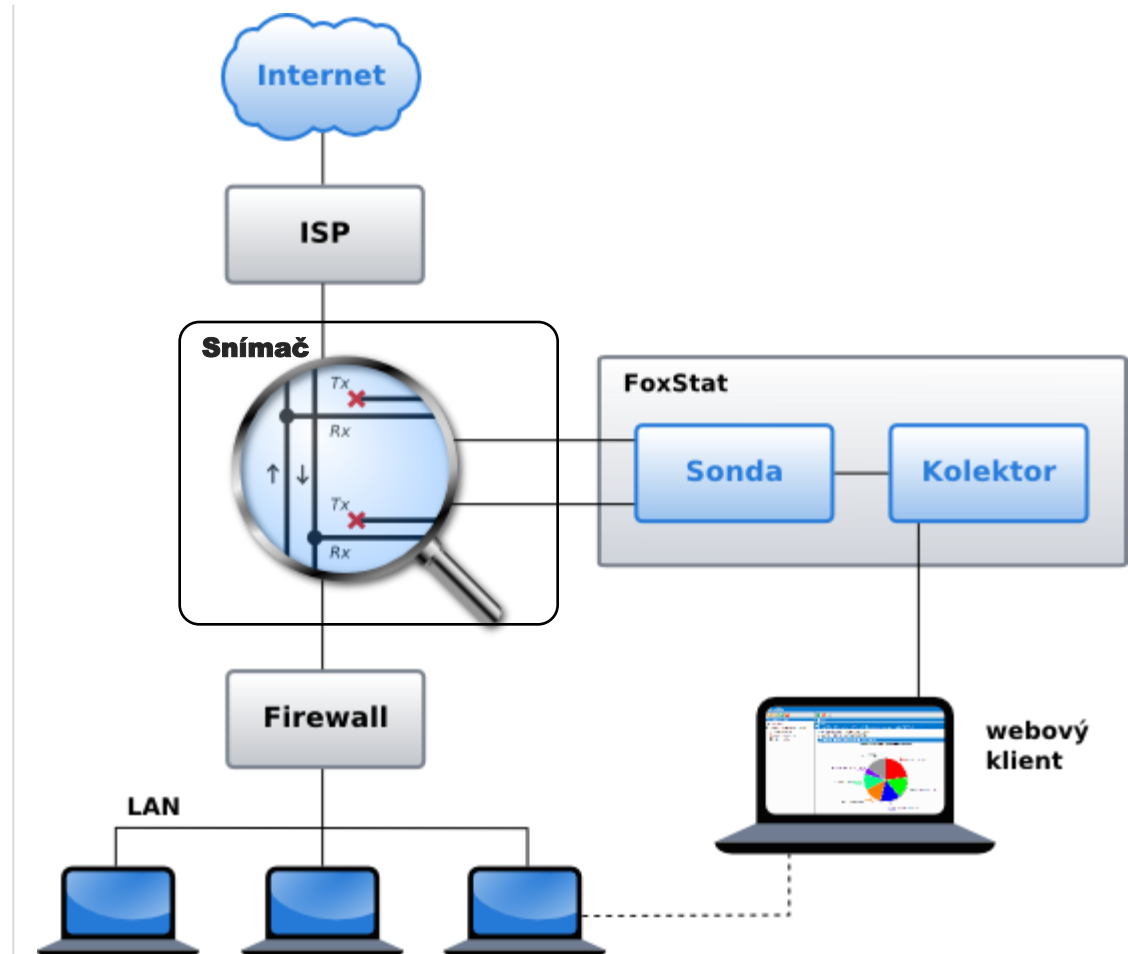
Ukládání



Analýza

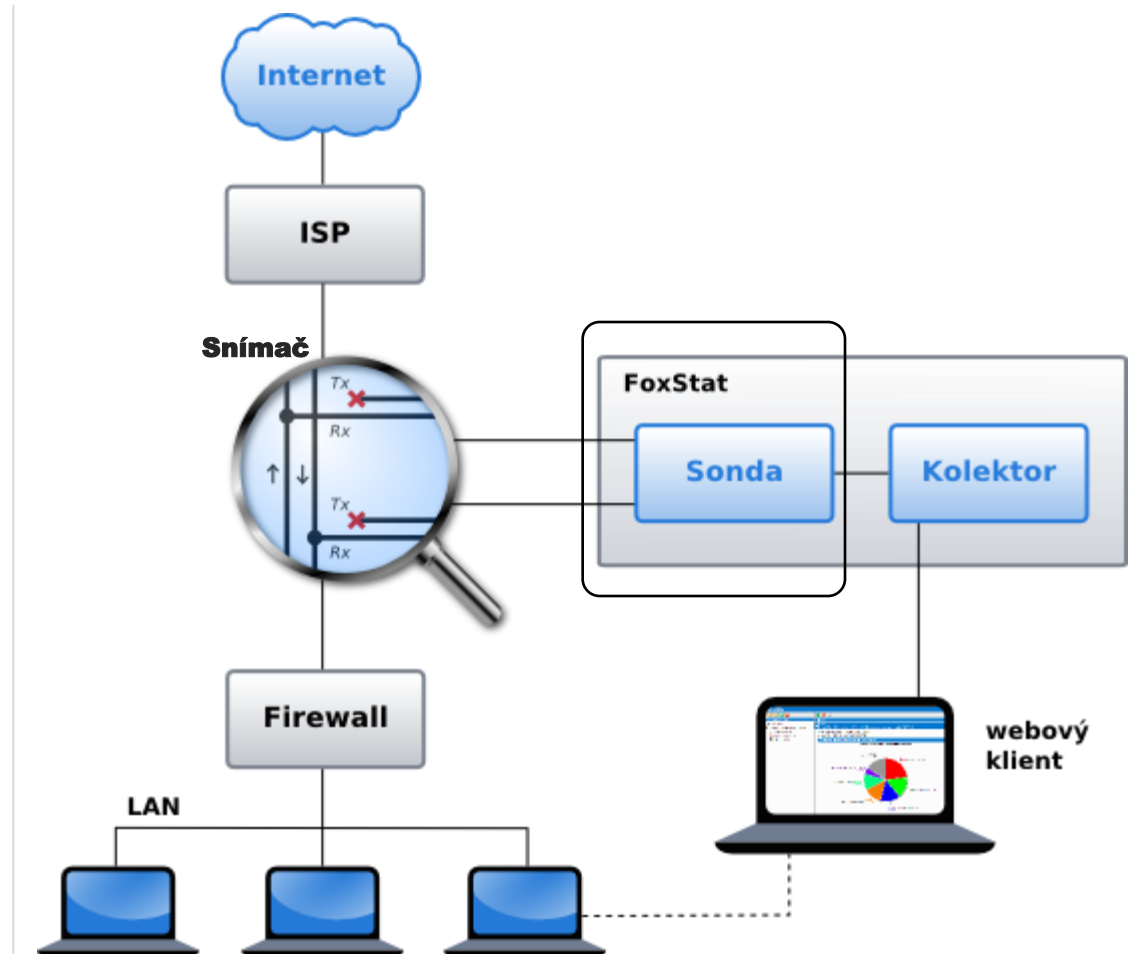
Zapojení ve Vaší síti

- Snímač - pasivně sleduje provoz na lince mezi providerem a Vaší sítí



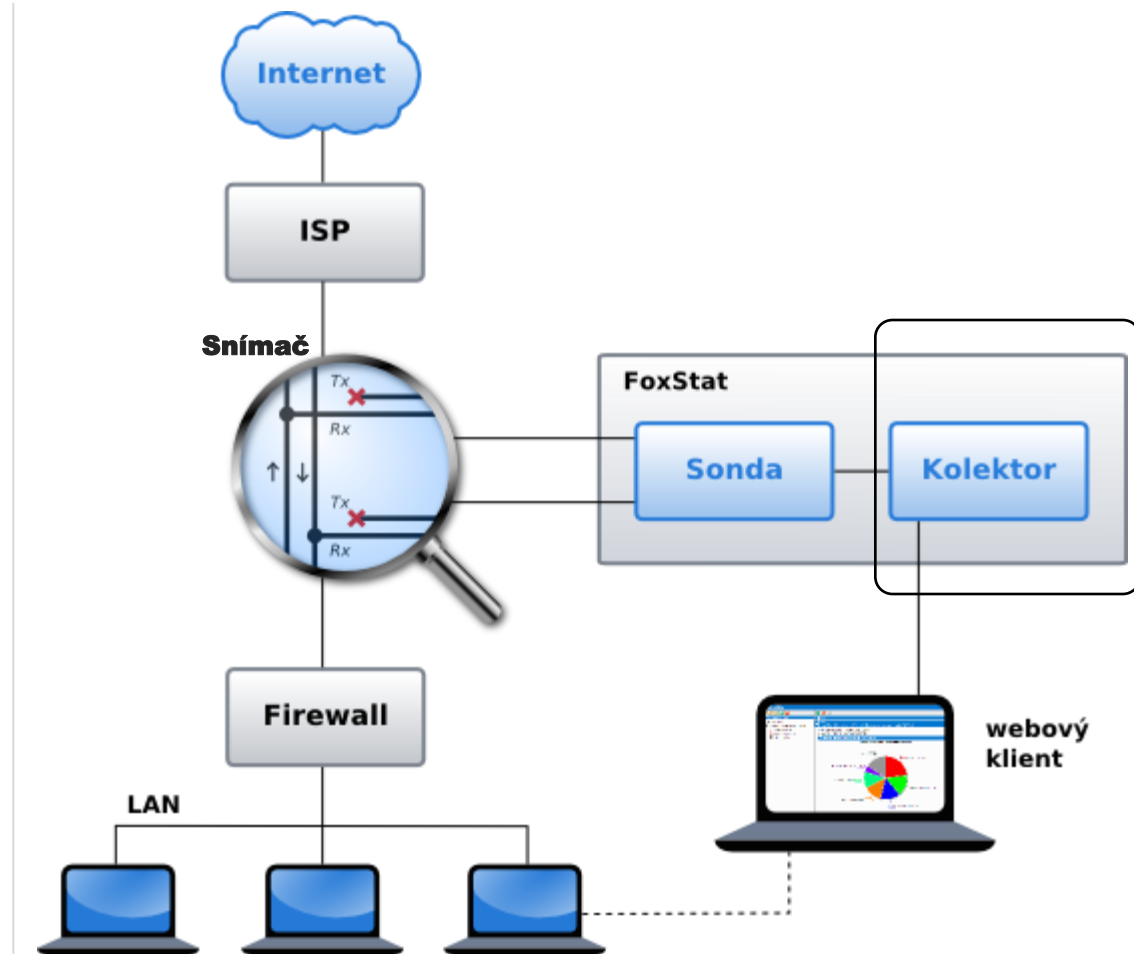
Zapojení ve Vaší síti

- Snímač - pasivně sleduje provoz na lince mezi providerem a Vaší sítí
- FoxStat sonda - dekóduje data



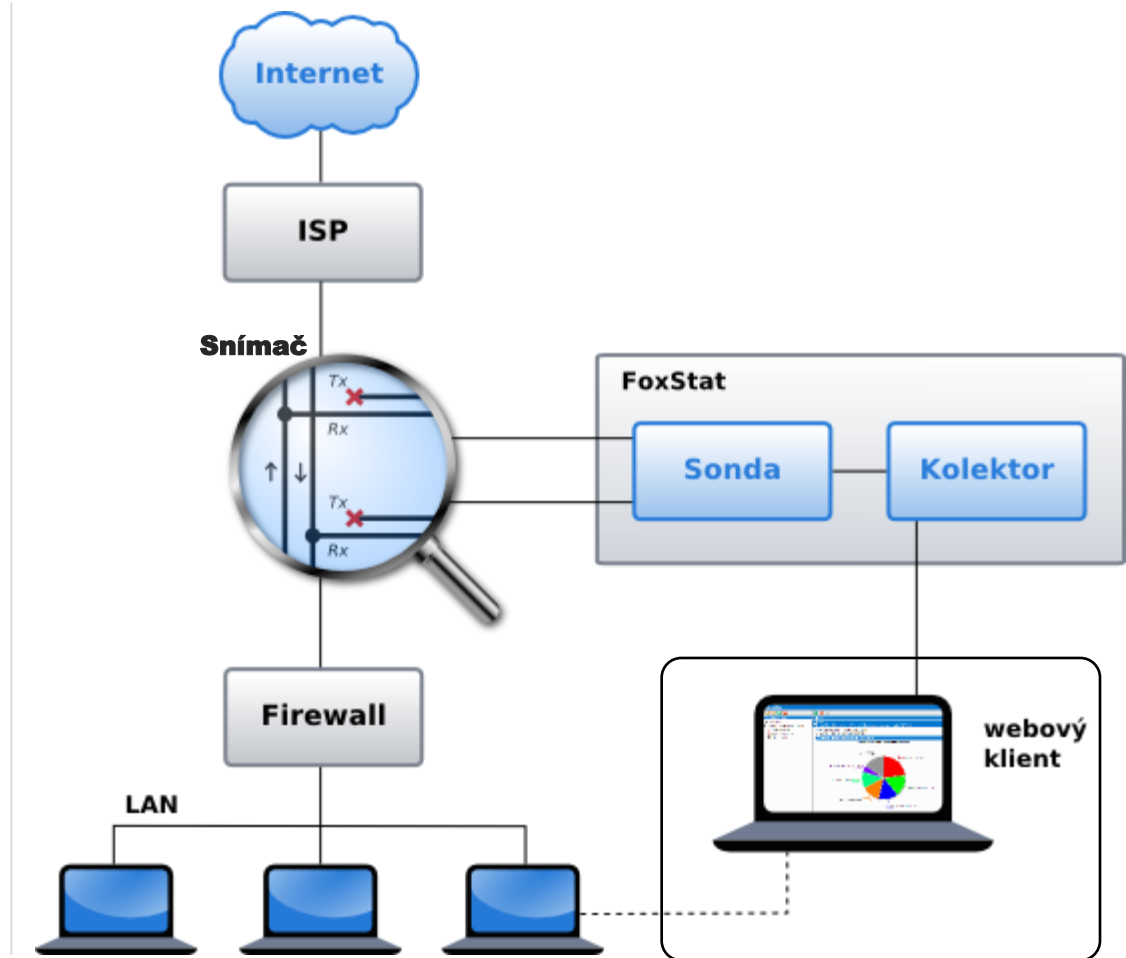
Zapojení ve Vaší síti

- Snímač - pasivně sleduje provoz na lince mezi providerem a Vaší sítí
- FoxStat sonda - dekóduje data
- FoxStat kolektor - ukládá data do databáze



Zapojení ve Vaší síti

- Snímač - pasivně sleduje provoz na lince mezi providerem a Vaší sítí
- FoxStat sonda - dekoduje data
- FoxStat kolektor - ukládá data do databáze
- Aplikace - zpřístupnění analýz přes webové rozhraní



FoxStat příklad - dotaz

Vytvoříme dotaz

- pojmenujeme dotaz

The screenshot shows the FoxStat web interface. The top bar displays the user 'lbstat@SERVER'. The main area is divided into several sections:

- NetStat analýzy:** A sidebar menu with various analysis options like 'aktuálních 5 min', 'aktuální hodina', 'koláčový graf', 'čárový graf', 'křížová tabulka', 'výpis spojení', 'http', 'výpis paketů', 'radia online', 'DEN', 'podle názvů', and 'ukázka'. The 'Cil' option is highlighted.
- Dotaz:** A configuration panel for the selected query. It includes:
 - Sloupce:** A list of columns: 'Zdroj', 'Cil', 'Požadavek-odpověď', 'Proto class', 'Proto detail', 'Detail', and 'Skupiny'.
 - Vybrané sloupce:** A dropdown menu showing 'Cil' as the selected column.
 - Hodnoty:** A list of values: 'Počet bajtů' and 'Počet paketů'.
 - Vybrané hodnoty:** A dropdown menu showing 'Počet bajtů' as the selected value.
 - Podmínky:** A section for defining conditions with logical operators (AND, OR, NOT) and a search icon.
- Footer:** Shows the query name 'Čas 5 minut' and the condition 'AND Rozhraní internet in'. There is an 'Obnovovat' button with a checkmark.

Představení

FoxStat příklad - dotaz

Vytvoříme dotaz

- pojmenujeme dotaz

Vybereme formu dotazu

- ze 7 možných variant

The screenshot shows the FoxStat application interface. The top bar displays the user 'lbstat@SERVER'. The main window is titled 'NetStat analýzy' and contains a sidebar with various analysis options. The 'Dotaz' (Query) section is active, showing a list of columns and a selected column 'Cil'. The 'Hodnoty' (Values) section shows 'Počet bajtů' and 'Počet paketů'. The 'Podmínky' (Conditions) section shows a query: 'Čas 5 minut' AND 'Rozhraní internet' in 'in'. The 'Obnovovat' (Refresh) button is checked.

NetStat analýzy

- cíl
- aktuálních 5 min
- aktuální hodina
- koláčový graf
- čárový graf
- křížová tabulka
- výpis spojení
- http
- výpis paketů
- radia online
- DEN
- podle názvů
- ukázka

Dotaz

Sloupce

- Zdroj
- Cil
- Požadavek-odpověď
- Proto class
- Proto detail
- Detail
- Skupiny

Vybrané sloupce

Cil

Hodnoty

Počet bajtů
Počet paketů

Vybrané hodnoty

Počet bajtů

Podmínky

AND OR () NOT ←

Čas 5 minut
AND Rozhraní internet in

Obnovovat

Představení

FoxStat příklad - dotaz

Vytvoříme dotaz

- pojmenujeme dotaz

Vybereme formu dotazu

- ze 7 možných variant

Uřídíme hodnoty

- sloupce, hodnoty přenosu

The screenshot shows the FoxStat interface with a query configuration window. The window is titled "FoxStat" and shows a user "lbstat@SERVER". The main area is divided into several sections:

- Popis** (Description)
- Dotaz** (Query) - expanded, showing a list of columns and values.
- Sloupce** (Columns) - list of available columns: Zdroj, Cil, Požadavek-odpověď, Proto class, Proto detail, Detail, Skupiny.
- Vybrané sloupce** (Selected columns) - list of selected columns: Cil.
- Hodnoty** (Values) - list of available values: Počet bajtů, Počet paketů.
- Vybrané hodnoty** (Selected values) - list of selected values: Počet bajtů.
- Podmínky** (Conditions) - list of conditions: Čas 5 minut, AND, Rozhraní internet in.

At the bottom, there are buttons for logical operators: AND, OR, (,), NOT, and a refresh button "Obnovovat".

Představení

FoxStat příklad - dotaz

Vytvoříme dotaz

- pojmenujeme dotaz

Vybereme formu dotazu

- ze 7 možných variant

Uřídíme hodnoty

- sloupce, hodnoty přenosu

Navolíme podmínky

- čas, rozhraní, protokoly,...

The screenshot shows the FoxStat web interface. The top bar displays the user 'lbstat@SERVER'. The left sidebar is titled 'NetStat analýzy' and lists various analysis options like 'aktuálních 5 min', 'aktuální hodina', 'koláčový graf', 'čárový graf', 'křížová tabulka', 'výpis spojení', 'http', 'výpis paketů', 'radia online', 'DEN', 'podle názvů', and 'ukázka'. The main content area is titled 'Dotaz' and is divided into several sections: 'Sloupce' (Columns) with a list of fields including 'Zdroj', 'Cil', 'Požadavek-odpověď', 'Proto class', 'Proto detail', 'Detail', and 'Skupiny'; 'Hodnoty' (Values) with 'Počet bajtů' and 'Počet paketů'; and 'Podmínky' (Conditions) with a logical operator 'AND' and two conditions: 'Čas 5 minut' and 'AND Rozhraní internet in'. A 'Představení' (Preview) button is located on the right side of the interface.

Představení

FoxStat příklad - dotaz

Vytvoříme dotaz

- pojmenujeme dotaz

Vybereme formu dotazu

- ze 7 možných variant

Uřídíme hodnoty

- sloupce, hodnoty přenosu

Navolíme podmínky

- čas, rozhraní, protokoly,...

Spustíme dotaz

The screenshot shows the FoxStat web interface. The top bar includes the FoxStat logo and the user 'lbstat@SERVER'. The main area is divided into several sections:

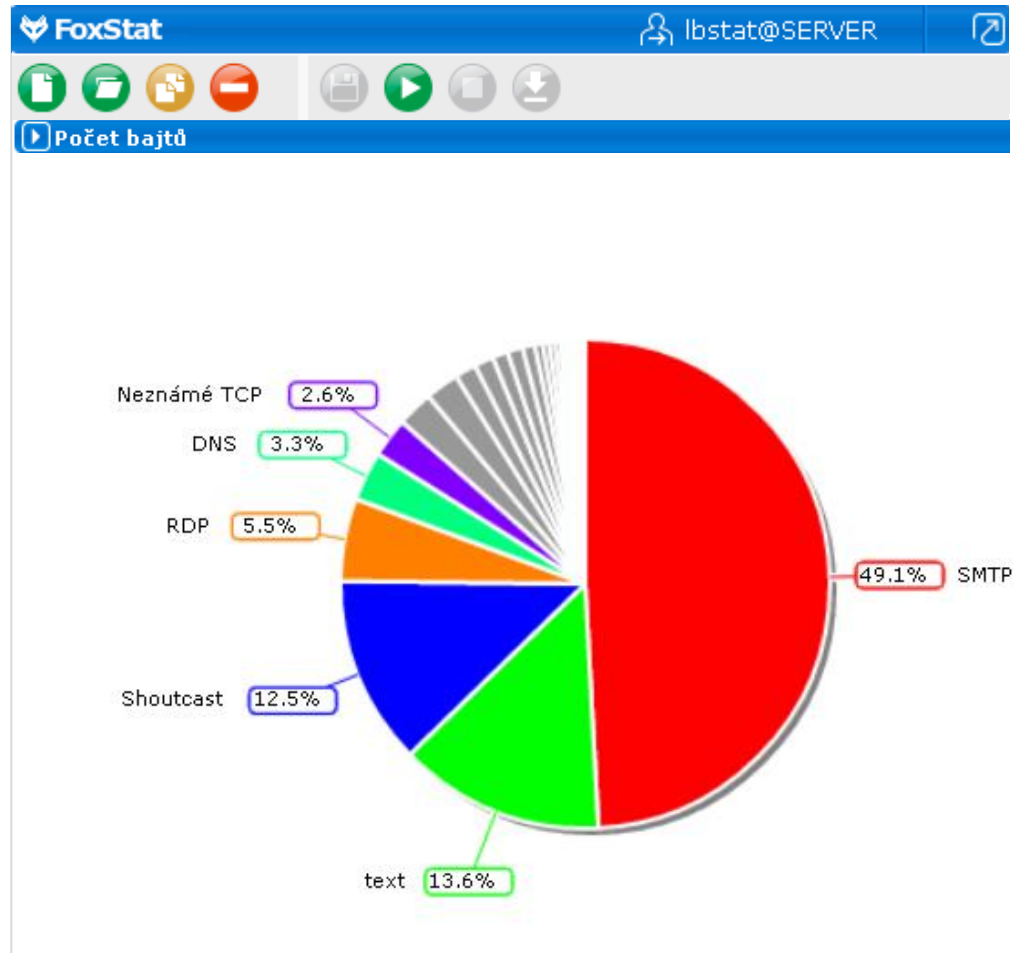
- NetStat analýzy** (left sidebar): A list of analysis options including 'cil', 'aktuálních 5 min', 'aktuální hodina', 'koláčový graf', 'čárový graf', 'křížová tabulka', 'výpis spojení', 'http', 'výpis paketů', 'radia online', 'DEN', 'podle názvů', and 'ukázka'.
- Dotaz** (main configuration area):
 - Sloupce** (Columns): A list of available columns: 'Zdroj', 'Cil', 'Požadavek-odpověď', 'Proto class', 'Proto detail', 'Detail', and 'Skupiny'.
 - Vybrané sloupce** (Selected columns): 'Cil' is selected.
 - Hodnoty** (Values): A list of available values: 'Počet bajtů' and 'Počet paketů'.
 - Vybrané hodnoty** (Selected values): 'Počet bajtů' is selected.
 - Podmínky** (Conditions): A section for defining query conditions with logical operators (AND, OR, NOT) and a list of conditions: 'Čas 5 minut', 'AND Rozhraní internet in'.
- Obnovovat** (Refresh): A checkbox that is checked.

FoxStat příklad - graf

Výsledky:

Graf

- poměr jednotlivých protokolů



Představení

FoxStat příklad - tabulka

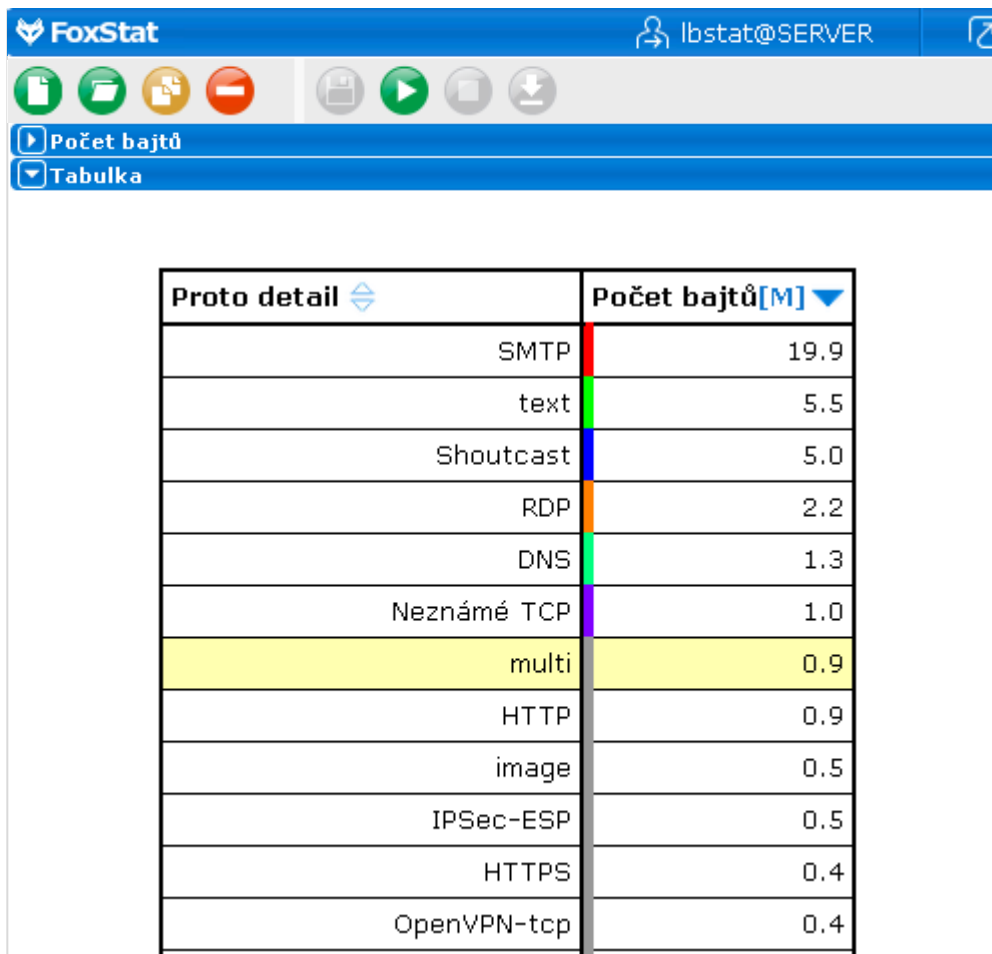
Výsledky:

Graf

- poměr jednotlivých protokolů

Tabulka

- hodnoty zvolené do sloupců



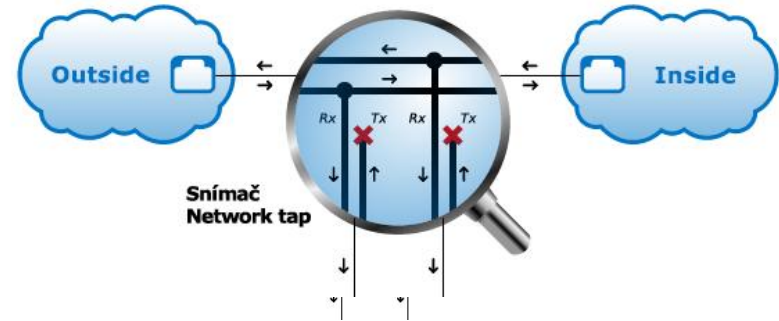
The screenshot shows the FoxStat application window. The title bar reads 'FoxStat' and the user is logged in as 'lbstat@SERVER'. Below the title bar is a toolbar with icons for file operations and playback. A menu bar shows 'Počet bajtů' (selected) and 'Tabulka'. The main content area displays a table with two columns: 'Proto detail' and 'Počet bajtů[M]'. The table lists various protocols and their corresponding byte counts in megabytes. The 'multi' row is highlighted in yellow.

Proto detail	Počet bajtů[M]
SMTP	19.9
text	5.5
Shoutcast	5.0
RDP	2.2
DNS	1.3
Neznámé TCP	1.0
multi	0.9
HTTP	0.9
image	0.5
IPSec-ESP	0.5
HTTPS	0.4
OpenVPN-tcp	0.4

Představení

KLÍČOVÉ VLASTNOSTI

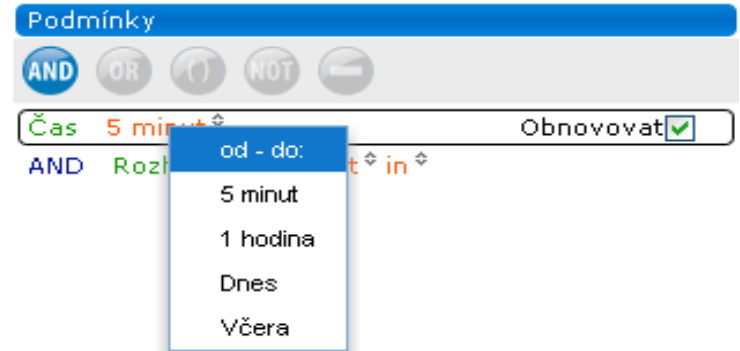
1. pasivní odposlech



KLÍČOVÉ VLASTNOSTI

1. pasivní odposlech

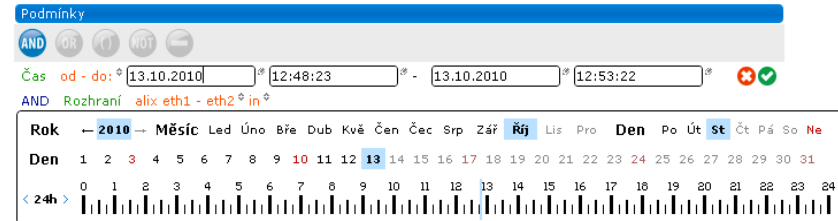
2. analýza v reálném čase



KLÍČOVÉ VLASTNOSTI

1. pasivní odposlech
2. analýza v reálném čase

3. pohled do historie



KLÍČOVÉ VLASTNOSTI

1. pasivní odposlech
2. analýza v reálném čase
3. pohled do historie

4. detekce protokolů

AND ▾ Proto detail ▾ IN ▾



P2P : Napster , GNUTella , Fastrack kazaa/morpheus , BitTorrent , eDonkey
Skype , Joltid PeerEnabler , Direct Connect

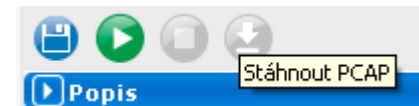
VoIP : SIP , SIP-TLS , SIP-data , Asterisk , H.323 , STUN

MultiMedia : RTSP-udp , RTSP-tcp , MMS-udp , MMS-tcp , Shoutcast

Games : World of Warcraft

KLÍČOVÉ VLASTNOSTI

1. pasivní odposlech
2. analýza v reálném čase
3. pohled do historie
4. detekce protokolů
5. záznam síťového provozu

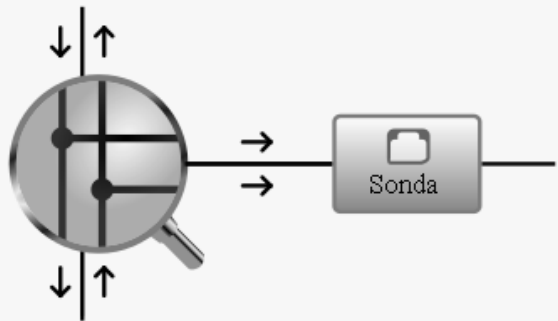


KLÍČOVÉ VLASTNOSTI

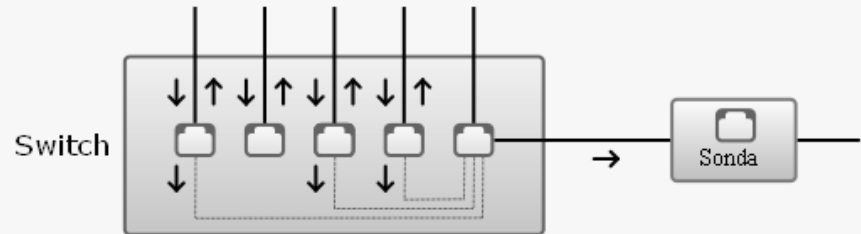
1. pasivní odposlech
2. analýza v reálném čase
3. pohled do historie
4. detekce protokolů
5. záznam síťového provozu
6. dekódování NAT adres

Tabulka		
Velikost	Služba	Detaily spojení
	HTTP	poz-3.gb-sh.vol.cz:irdmi < pclin9:49687
	TCP:1034	live-reflector.infomaniak.ch:80 > r2av175.net.upc.cz:activesync
	HTTP flash	81.30.226.135:http < gwu.lbox.cz:46040
	HTTP text	www-03.ahe.boulder.ibm.com:http < gwu.lbox.cz:52201
	OpenVPN-tcp	93.90.166.6:46614 > r2av81.net.upc.cz:openvpn
	OpenVPN-tcp	93.90.166.10:60650 > r2av81.net.upc.cz:openvpn
	ICQ	bos-d095c-rdr3.blue.aol.com:aol < 10.76.66.113:1091
	OpenVPN-tcp	93.90.166.5:38224 > r2av81.net.upc.cz:openvpn
	OpenVPN-tcp	93.90.166.11:50848 > r2av81.net.upc.cz:openvpn
	ICMP	hlas.802.cz > r2av87.net.upc.cz
	TCP:15717	ryvs-be05129305.e21-3.tg10.gathering.org:15717 < pcrnz:41857
	SMTP	mail.snyze.com:48295 > gwu.lbox.cz:smtp
	SMTP	ivd178.internetdsl.tpnet.pl:10165 > gwu.lbox.cz:smtp

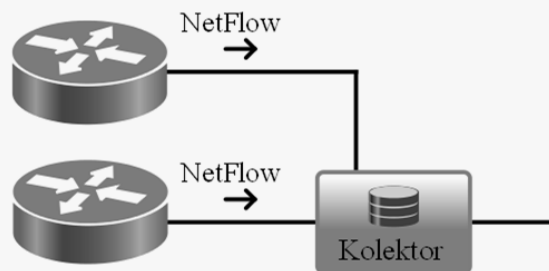
MOŽNOSTI SNÍMAČE



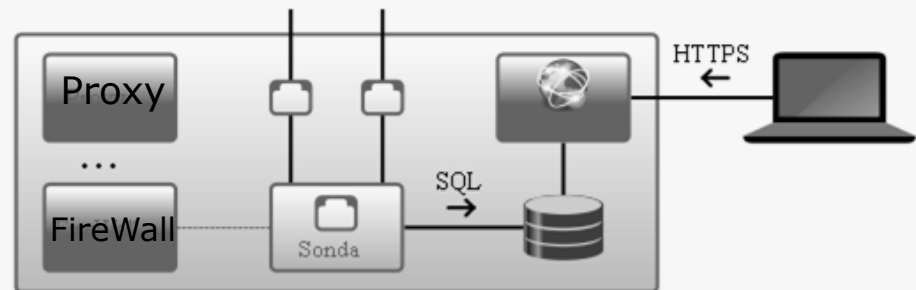
Network Tap



Port mirror / SPAN

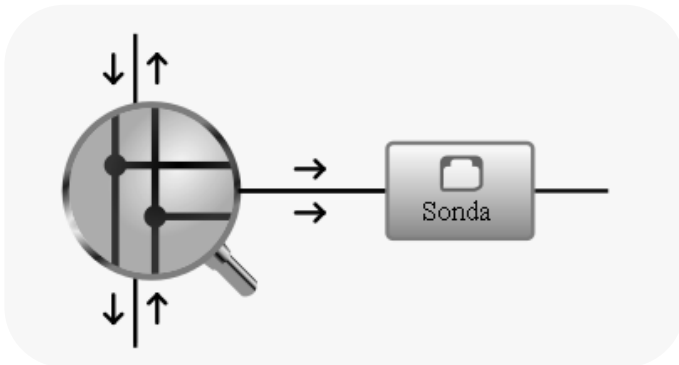


NetFlow

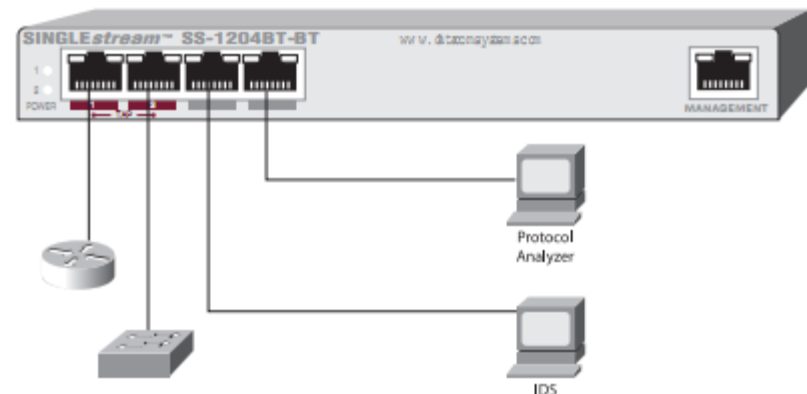
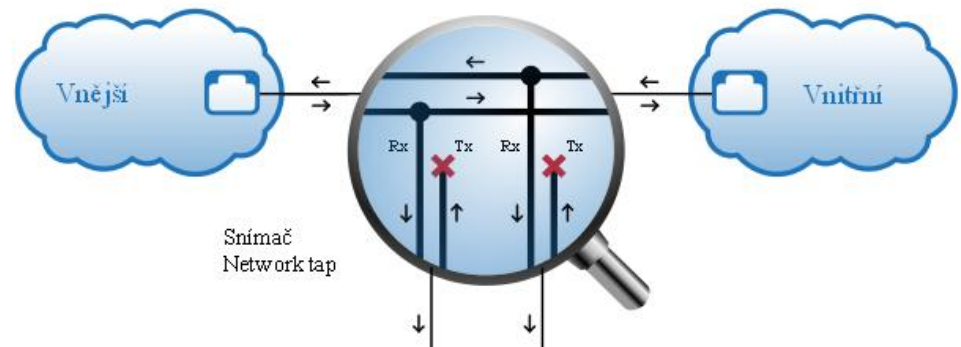


LinuxBox / SecureBox

Network Tap



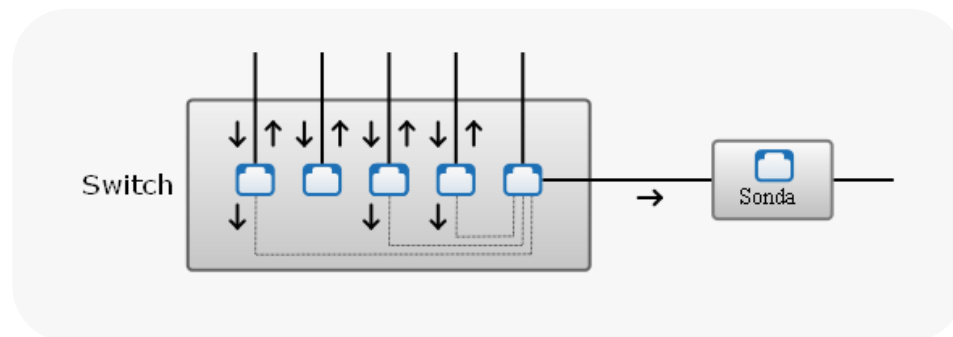
- pasivní snímání
- přesnost bez ztrát či zpoždění
- metalické i optické linky
- současné sledování více linek
- potřeba dvou portů pro každý směr přenosu



Možnosti snímače

SPAN / Port Mirror

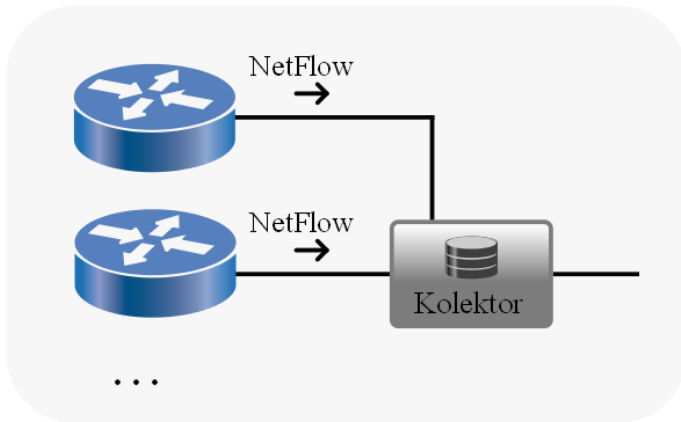
- stávající switche
- velké množství portů
- otagování VLAN
- rychlé změny
- minimální kabeláž
- posoudit možnosti switche



NetFlow

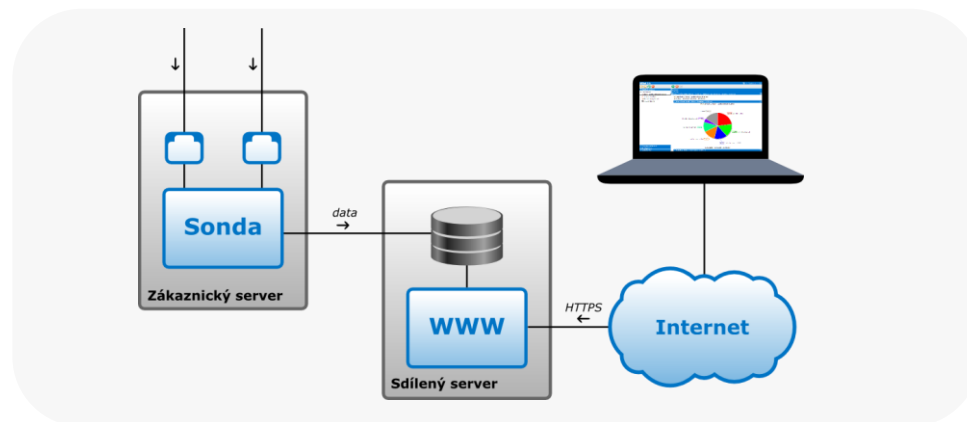


- stávající routery
- velké množství rozhraní
- rychlé změny
- minimální kabeláž
- **NEOBSAHUJE** rozšířené detekce, dekódování ani detaily komunikace



LinuxBox / SecureBox

- stávající servery
- sonda přímo na serveru
- vhodnější umístění kolektoru
- NAT, proxy, FW
- minimální kabeláž
- více sond na jeden kolektor



Možnosti snímače

FoxStat je...

Nástroj

optimalizovaný pro:

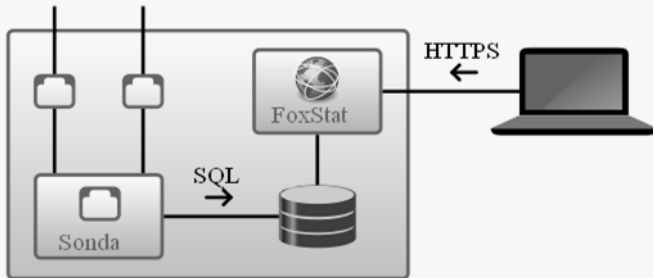
- velmi rychlý návrh dotazu
- velmi rychlou úpravu dotazu
- velmi rychlé zjištění zdroje problému
- zpětný debug

The screenshot shows the FoxStat web interface. The top bar includes the logo and the user 'lbstat@SERVER'. The main interface is divided into several sections:

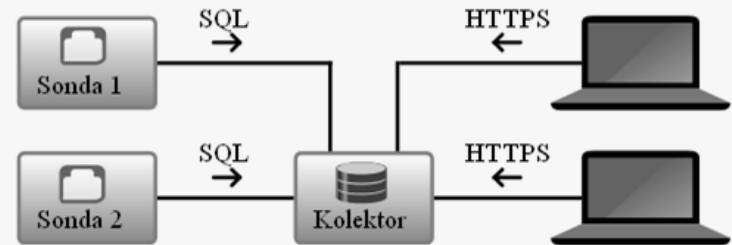
- NetStat analýzy:** A sidebar with various analysis options like 'aktuálních 5 min', 'aktuální hodina', 'koláčový graf', 'čárový graf', 'křížová tabulka', 'výpis spojení', 'http', 'výpis paketů', 'radia online', 'DEN', 'podle názvů', and 'ukázka'.
- Popis:** A section for describing the query.
- Dotaz:** A section for defining the query structure, including columns and values.
- Podmínky:** A section for defining query conditions using logical operators (AND, OR, NOT) and search criteria.
- Search Criteria:** A list of search criteria including IM (IRC, IRCS, ICQ, Jabber-client, Jabber-ebuddy.com), P2P (Napster, GNUTella, Fastrack kazaa/morpl, Skype, Joltid PeerEnabler, Direct Connect), and VoIP (SIP, SIP-TLS, SIP-data, Asterisk, H.323).

Představení

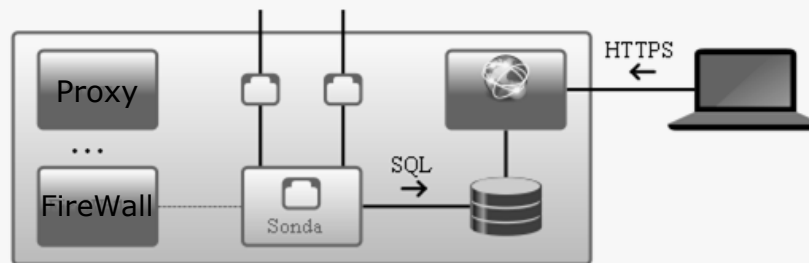
DISTRIBUCE



Bundle



Sdílený kolektor

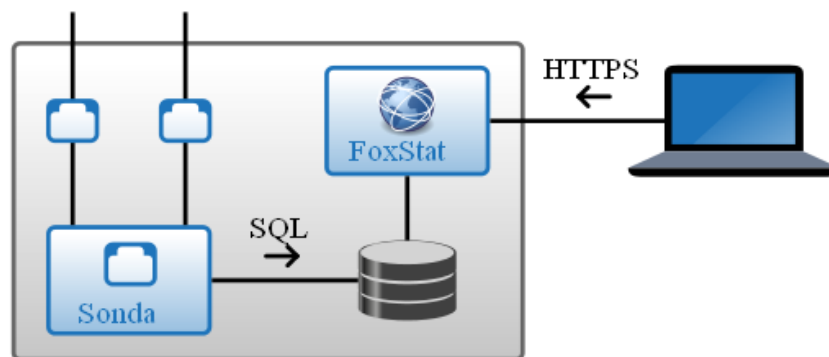


LinuxBox / SecureBox

distribuce - Bundle

sonda + kolektor

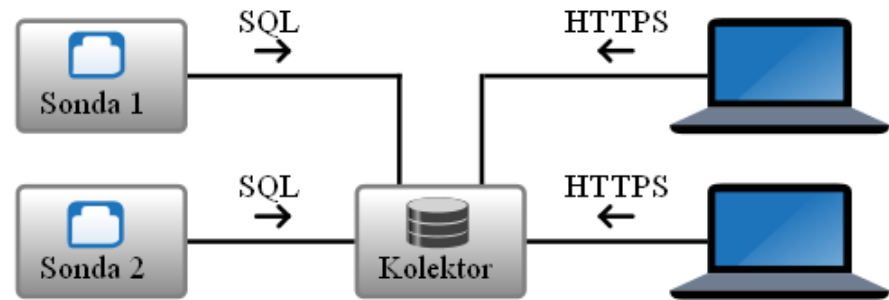
- střední síť či samostatné pobočky
- nižší náklady na jednoduchá řešení
- celé řešení v 1U
- možnost více sond



Distribuce

distribuce – sdílený kolektor

- rozsáhlé sítě
- srovnání dat z různých sond
- nižší náklady rozsáhlých řešení
- providerům umožňuje provozovat samostatnou instanci pro zákazníka

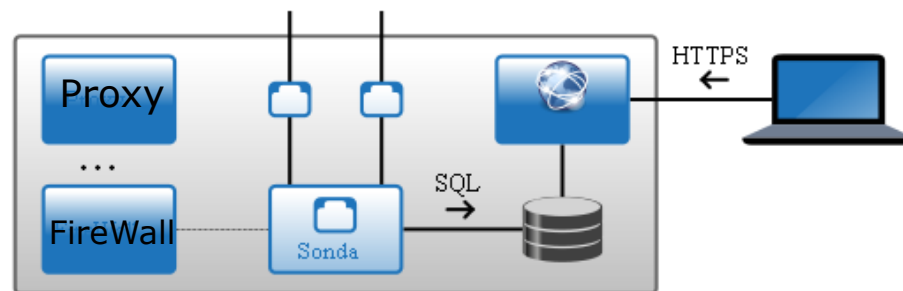


Distribuce



distribuce – LinuxBox / SecureBox

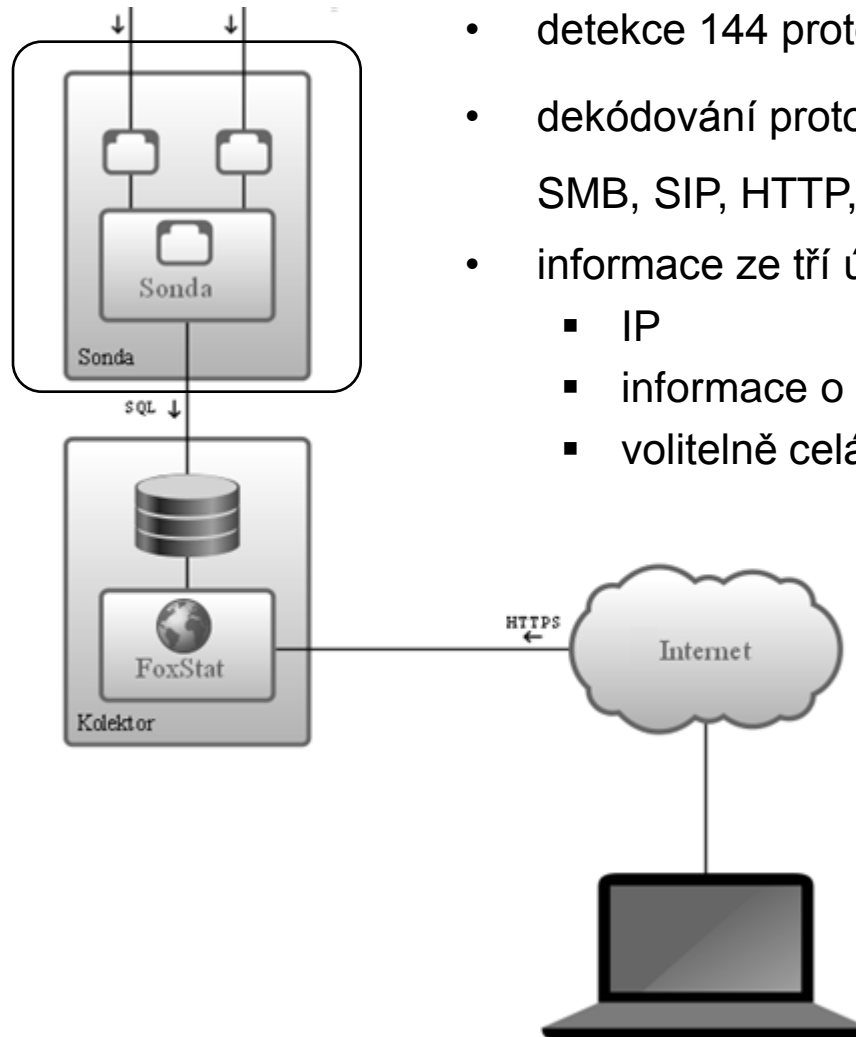
- stávající uživatelé LinuxBox / SecureBox serveru
- řeší NAT, proxy, FW,...
- analyzuje provoz VPN linek
- nejjednodušší řešení (sleduje se síťové rozhraní serveru)



Distribuce

PARAMETRY ZAŘÍZENÍ

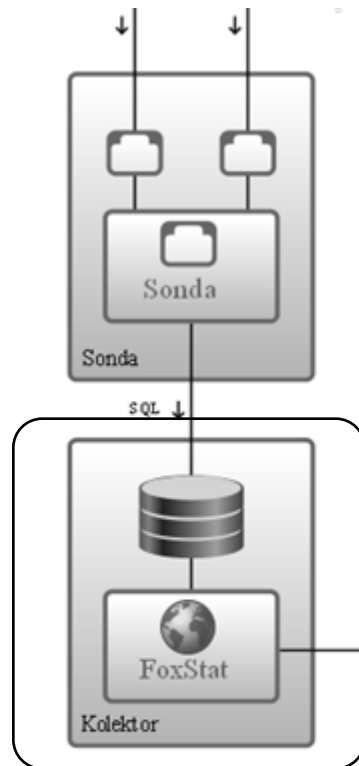
sonda



- detekce 144 protokolů v 19 skupinách
- dekódování protokolů a subprotokolů (FTP, SMB, SIP, HTTP, SMTP,...)
- informace ze tří úrovní
 - IP
 - informace o obsahu
 - volitelně celá komunikace

PARAMETRY ZAŘÍZENÍ

sonda

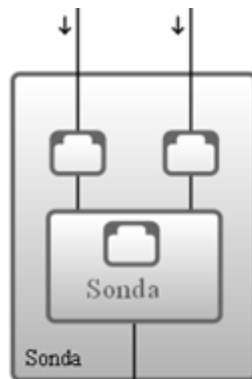


kolektor

- standardně od 500GB do 12TB
- RAID1 nebo RAID5 či jiné
- PostgreSQL – bez nákladů
- vteřinové vzorky, data za několik měsíců
- překlad IP na DNS, GeoIP
- FoxStat – HTTPS, neomezený počet klientů

PARAMETRY ZAŘÍZENÍ

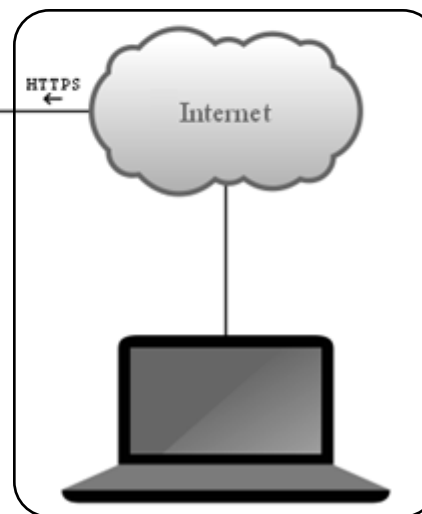
sonda



kolektor

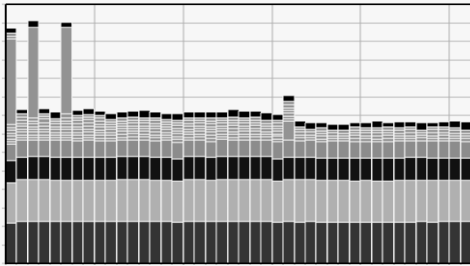


- IE, FireFox, Opera, Chrome, Safari
- žádný plugin či SW
- 7 základních typů analýzy
- komplexní reporty s integrovaným editorem
- export výpisu jako .pcap (WireShark)
- nové záložky bez ztráty dat

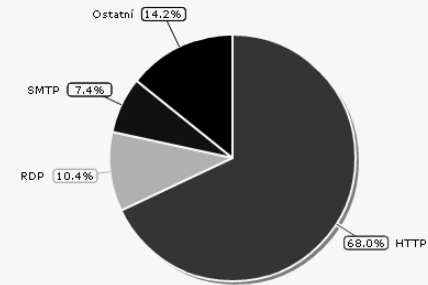


webový
klient

PŘÍNOSY & FINANCE



Vytížení linky



Analýza provozu

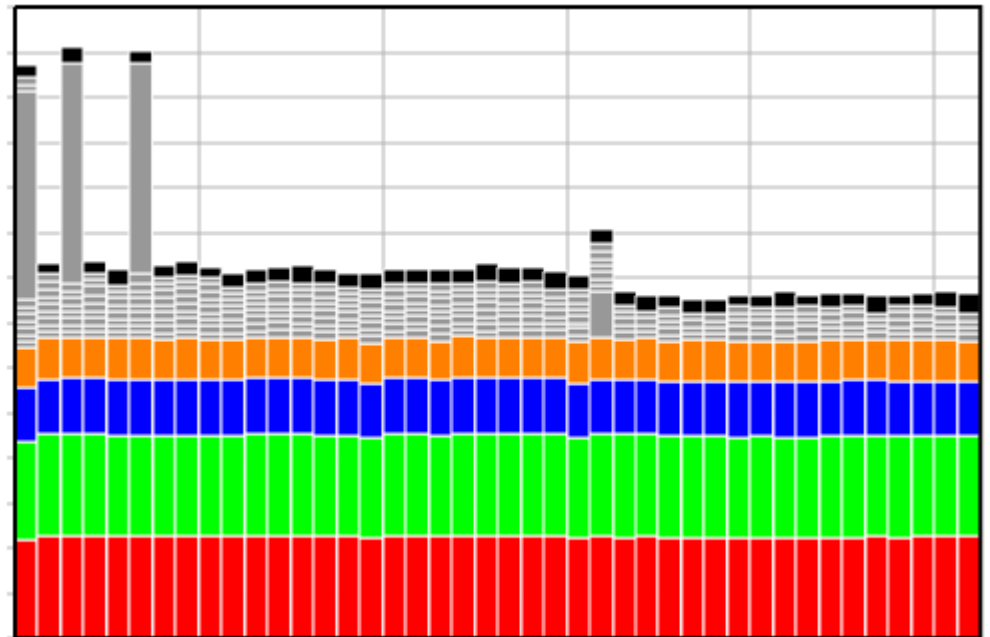


Úniky informací

FoxStat & přínosy

Vytížení linky

- přímoúměrná souvislost mezi zahlcením linky a ztrátami financí z výpadku
- analyzuje vytížení linky jako prevenci před zahlcením

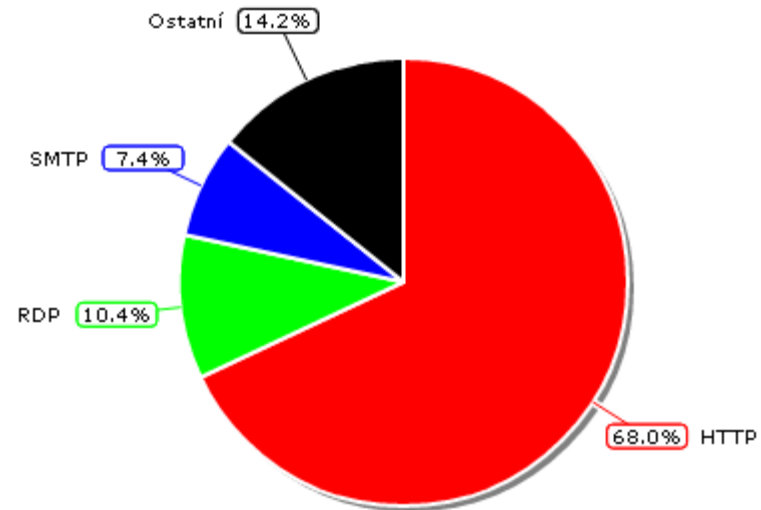


Přínosy

FoxStat & přínosy

Analýza provozu

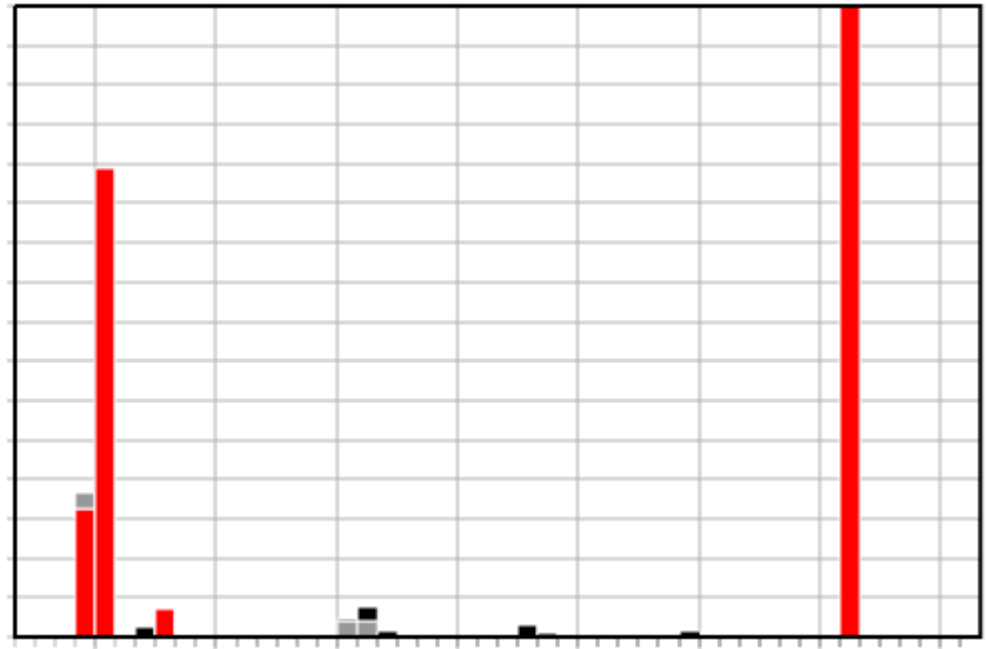
- vytížení linky na placených kanálech (garantovaná linka)
- analyzuje vytížení linky v souvislosti s jednotlivými protokoly



FoxStat & přínosy

Úniky informací

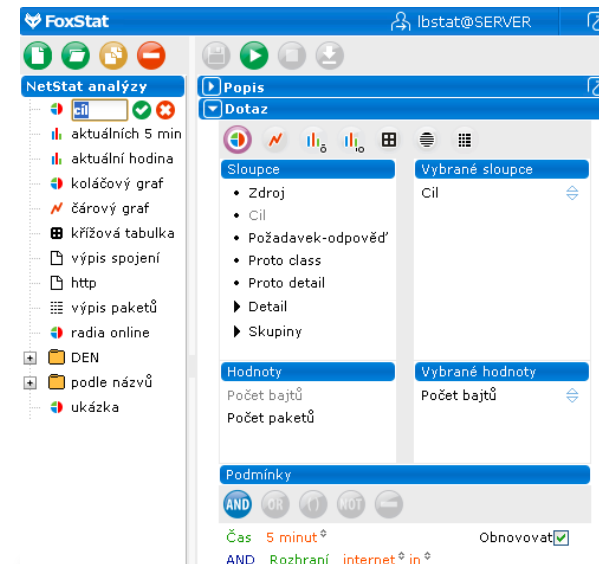
- odhalení a zamezení úniku informací z podnikové sítě
- analyzuje provoz linky a odchozí firemní data
- kontroluje VPN – síťové tunelování



Přínosy

FoxStat výhody

- rychlé dohledání zátěže a problému v síti
- zpětné dohledání v historii uložených dat
- zjištění zdroje úniku citlivých informací
- detekce používání nestandardních portů
- možnost záznamu kompletní komunikace
- optimalizace využití pásma datových linek
- snadná instalace



Výhody

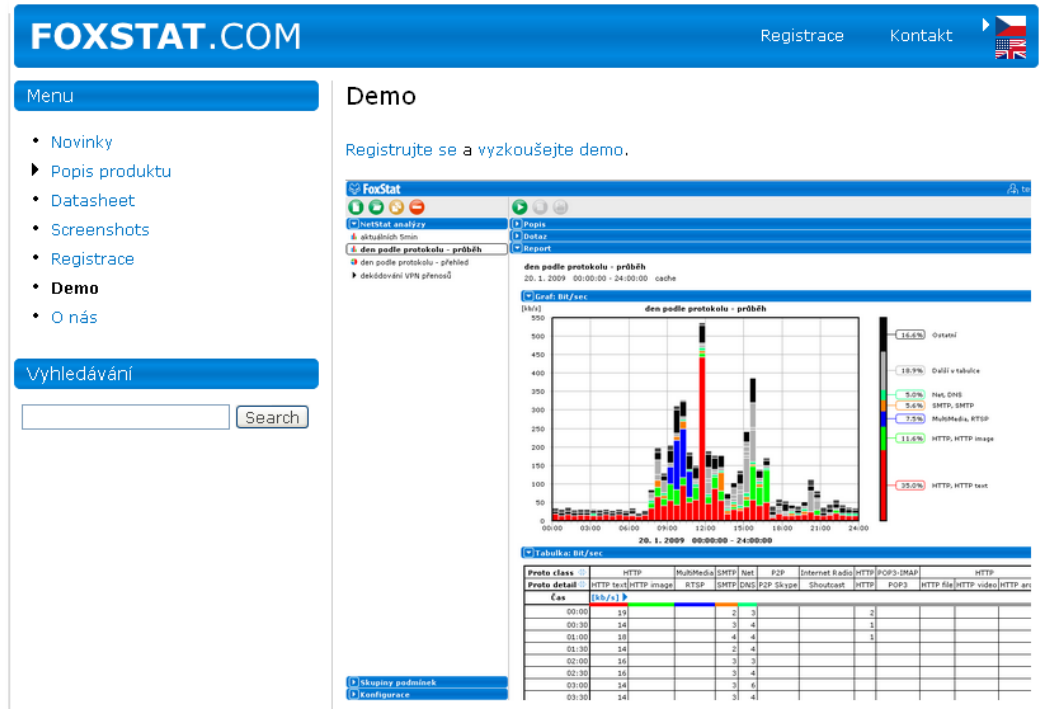
demoverze & zápůjčky

Na www.foxstat.com

- demoverze
- datasheet
- prezentace
- screencast
- školení
- servis

Zapůjčení

- individuálně, viz. ceník
- ukázková analýza u Vás



Demoverze

LinuxBox.cz



FoxStat
Change the **Net**.Work

FoxStat produkt manažer

Radoslav Dubný
radoslav.dubny@foxstat.com

+420 737 238 332