Jak vybrat správný firewall

Martin Šimek
Západočeská univerzita

EurOpen.CZ, Měřín, 5. října 2015

Obsah prezentace

- K čemu je firewall?
- Co je to firewall?
- Kam svět spěje?
- Nová generace firewallů?
- Jak vypadá trh?
- Společný management?
- Jaký je výkon?
- Co lze virtualizovat?
- SDN

Jaká jsou rizika?

- Krádež nebo zveřejnění interních dat
- Neoprávněný přístup k interním uzlům
- Zachycování nebo pozměňování dat
- Odmítnutí služby
- Záporná publicita, veřejné mínění, právní aspekty
- …

Co musí být zabezpečeno?

- Byznys: know-how, patenty, zdrojové kódy, informační agendy, …
- Jakýkoli přístup do vaší sítě
- Jakákoliv cesta z vaší sítě
- Informace o vaší síti
- …

Co je to firewall?

- Síťový prvek k řízení provozu mezi sítěmi s různou úrovní důvěryhodnosti či zabezpečení
- Definuje pravidla pro komunikaci mezi sítěmi
- Imunní vůči průnikům
- Zachycuje a reportuje dostatek informací pro sledování provozu

Paketový filtr

- Filtrování na L3 a částečně L4
- Posuzuje jednotlivé pakety
- Bez souvislostí
- Bez znalosti vyšších vrstev
- Bezestavový
- Pravidla pro každý směr
- Jednoduchý, rychlý

Stavový firewall

- Rozhoduje na základě kontextu
- Bere v úvahu vzájemné stavy mezi pakety
- Pamatuje si vnitřní stavy spojení
- Realizuje konečný automat
- Pravidla nejsou pouze jednosměrná
- Minimální zatížení pro existující spojení

Společné vlastnosti

- Zdroj a cíl komunikace zadán IP adresou
- Zdrojový anebo cílový port
- Použitý protokol
- Stav spojení

- Stačí to?

Web 2.0

- Číslo portu nestačí k identifikaci aplikace
- Komunikace probíhá přes aplikační vrstvu
- Většina provozu cloudových aplikací je zabalena v HTTP(S) protokolech

- Nové typy útoků cílí na aplikační vrstvu

Tradiční firewall

- Nemá kontrolu nad povolenou komunikací
- Nerozpozná tunelovaný provoz
- Nerozlišuje aplikace
- Nerozpozná aplikační útoky

IDS/IPS

- IDS – detekce útoků
  - Podá informaci jinému zařízení
  - Signatury útoků – automatický update
  - Heuristika
  - Detekce neobvyklého chování sítě
- IPS – prevence útoků
  - Aktivně reaguje

Nová generace firewallů

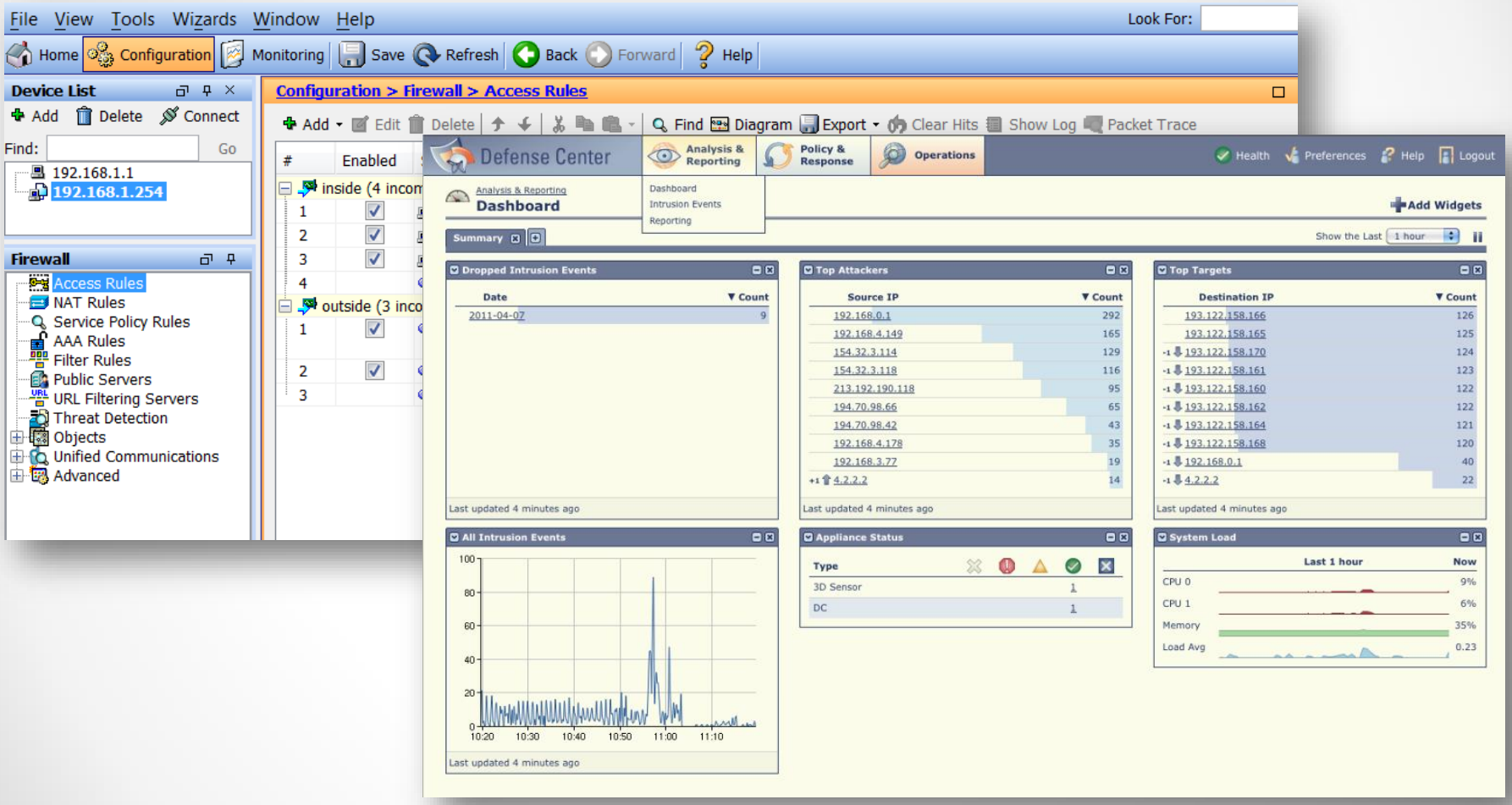
- Schopnost práce v L2 i L3 režimu
- Integrace s IPS
  - Zpracování paketu v jednom průchodu
  - Automatická aktualizace signatur
- Rozpoznávání aplikací
  - Definice aplikačních pravidel
  - Nahlížení do šifrovaného SSL provozu
- Standardní funkce firewallu (SPI, NAT, VPN, …)
- Integrace s externími ověřovacími službami

Jak vypadá trh s NGFW?

- Poradenské firmy
  - Gartner
  - Frost & Sullivan
  - …

Jak vypadá trh s NGFW?

Co na to management?



Co na to management?

	Source			Destination						
Name	Zone	Address	User	Zone	Address	Application	URL Category	Service	Action	Profile
LogAll	Tap	any	any	Tap	any	any	CustomerURLCategory	any	✓	
IT Allow Override	trust	any	pancademo\administrators	untrust	any	Custom-app	any	any	✓	
Read Only Facebook	trust	any	pancademo\administrators	untrust	any	facebook-base	any	any	✓	
Allow facebook posting	trust	any	pancademo\marketing	untrust	any	facebook-posting	any	any	✓	
Block Peer to Peer	trust	any	any	untrust	any	Peer to Peer	any	any	✗	none
Webmail file blocking	trust	any	any	untrust	any	Webmail	any	any	✓	
Sharepoint	Untrust-L3	any	any	DMZ	Sharepoint Server	sharepoint-base sharepoint-documents	any	application-default	✓	
Allow SSL and SSH	trust	any	pancademo\domain admins	untrust	any	ssh ssl	any	any	✓	
Allow Web-browsing	trust	Sharepoint Server	any	untrust	any	web-browsing	any	any	✓	
Block encrypted tunnel	trust	any	any	untrust	any	Encrypted Tunnel	any	any	✗	none
Block Proxies and Anonymizers	trust	any	any	untrust	any	Proxies	any	any	✗	none
Mail server	Untrust-L3	any	any	DMZ	Mail Server FQDN	outlook-web smtp	any	application-default	✓	
Web server	Untrust-L3	any	any	DMZ	Web-server	ssl web-browsing	any	application-default	✓	

Add | Delete | Clone | Enable | Disable | Move Top | Move Up | Move Down | Move Bottom | Highlight Unused Rules | 13 rule(s)

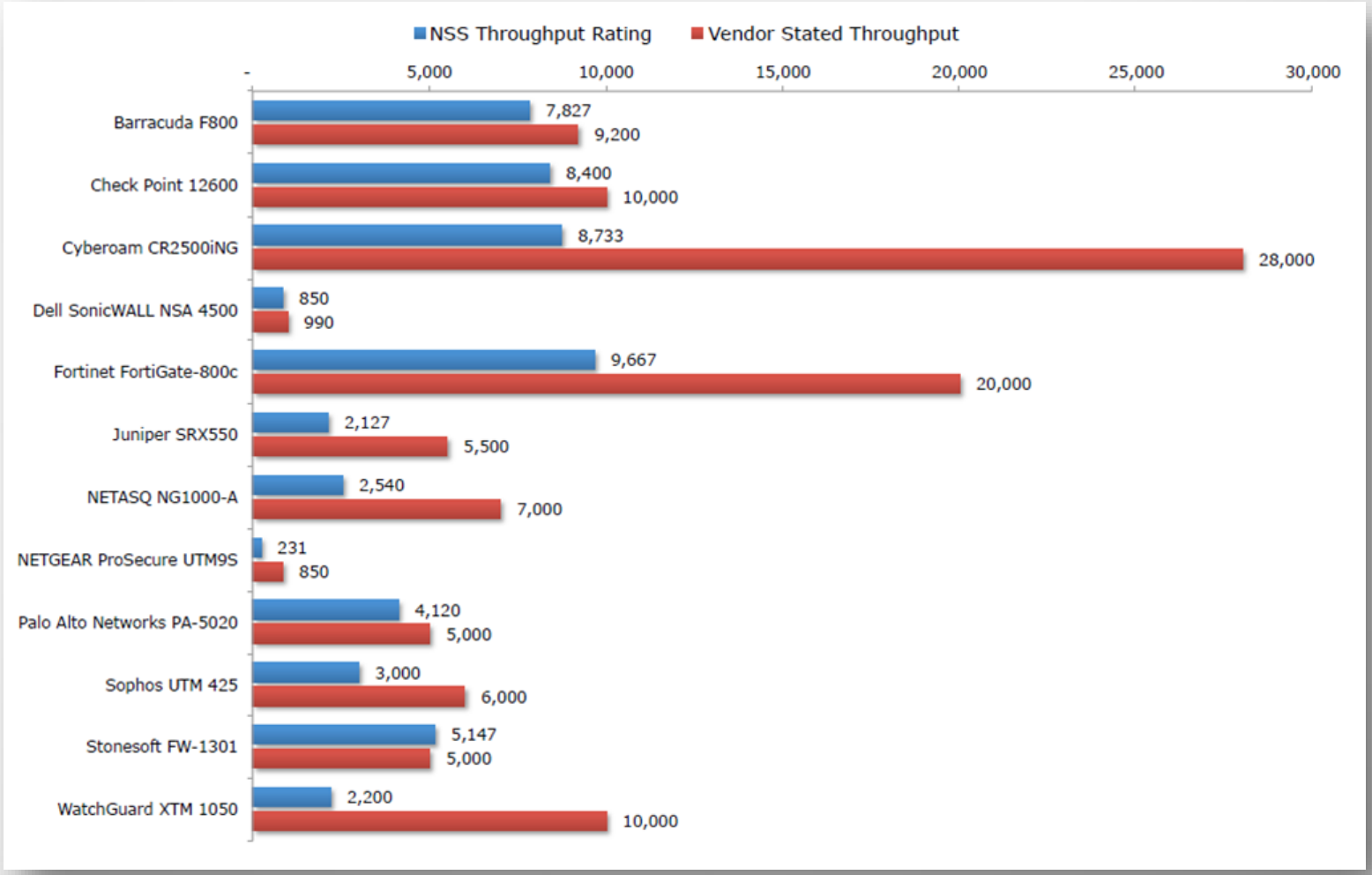
Pohodlí něco stojí

- Je paket zpracován v jednom průchodu?
- Používá se standardní hardware?
- Probíhá stavová inspekce na firewallu?
- Je integrace IPS a firewallu bezešvá?
- Jaká je propustnost firewallu?
- Jaká je propustnost po aktivaci ostatních modulů?
- Kolik je k dispozici portů a jakých?
- Kolik je možno vytvořit VPN tunelů?
- Nabízí podporu IPsec/SSL VPN?
- Obsahuje antivirus, antispyware (antimalware)?
- Blokuje nežádoucí e-maily (antispam, phishing)?
- Umožňuje webfiltering (URL filtering vs. content filtering)?
- Je možné nastavit časová omezení, šířku pásma (traffic shaping)?
- Umožňuje správu uživatelů (integrace s AD, LDAP/Radius)?
- Umožňuje vynutit politiky na základě identity uživatele nebo IP adresy?
- Nabízí nějakou použitelnou formu reportingu?
- Lze pomocí regulárních výrazů detekovat únik informací (DLP)?
- Jaká je provázanost a spolupráce mezi jednotlivými moduly?
- Je k dispozici jednotné a intuitivní uživatelské rozhraní?
- Jak je to s licencemi?
- Lze používat zařízení v režimu failover nebo load balancing?

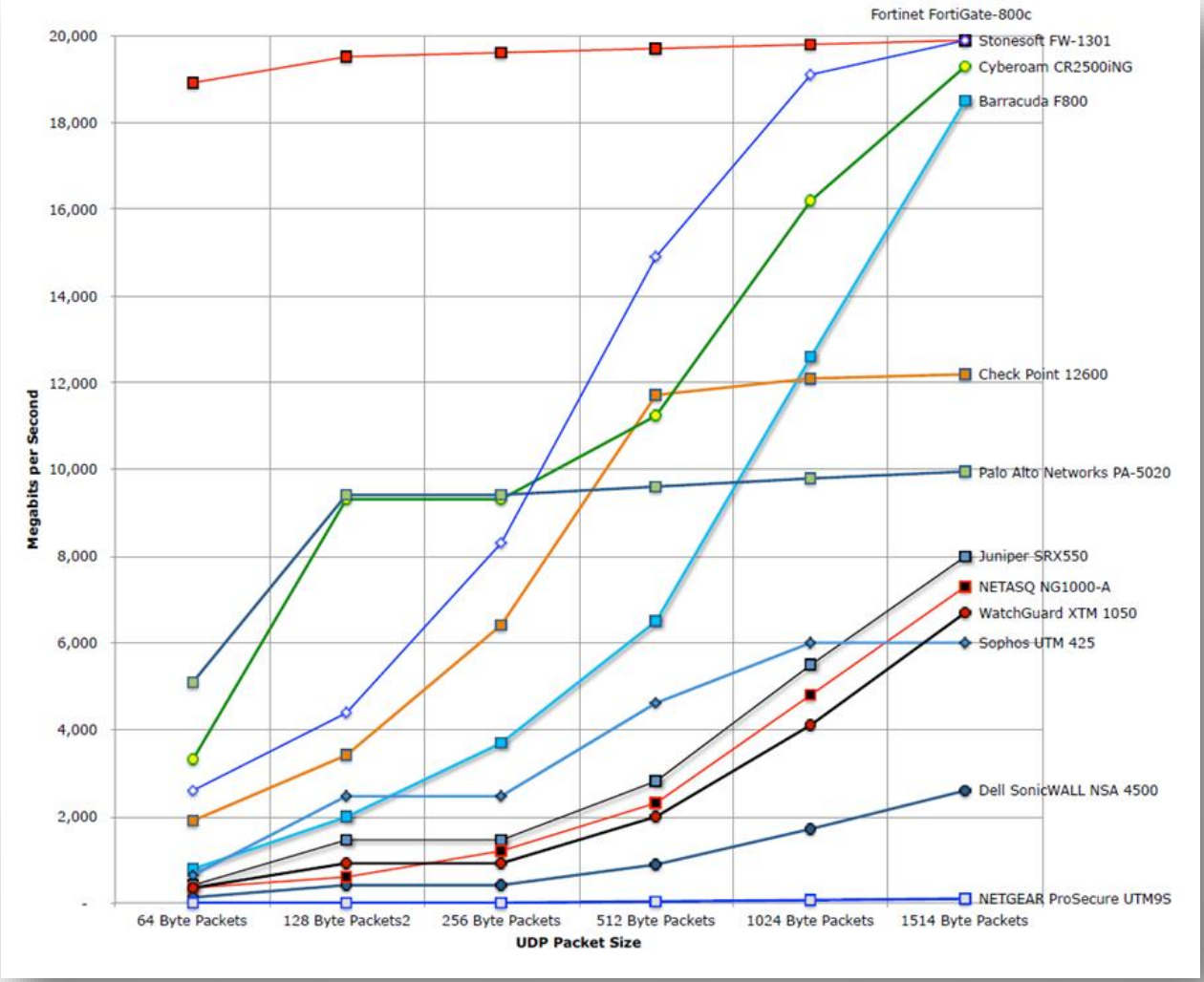
Výkon je výkon

- Testování stojí čas
- Nezávislé testovací laboratoře
  - NSS Labs
  - …

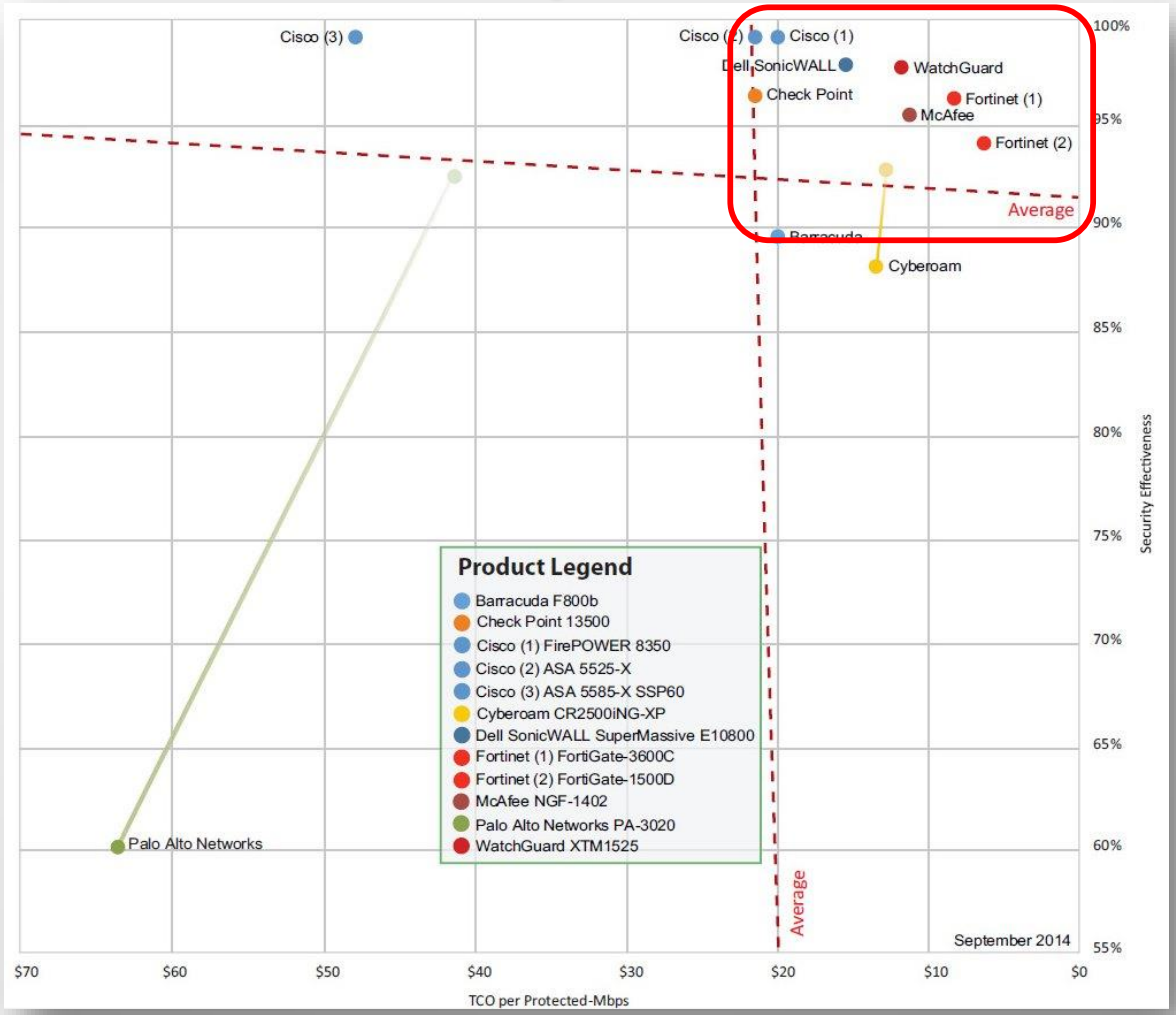
Výkon je výkon



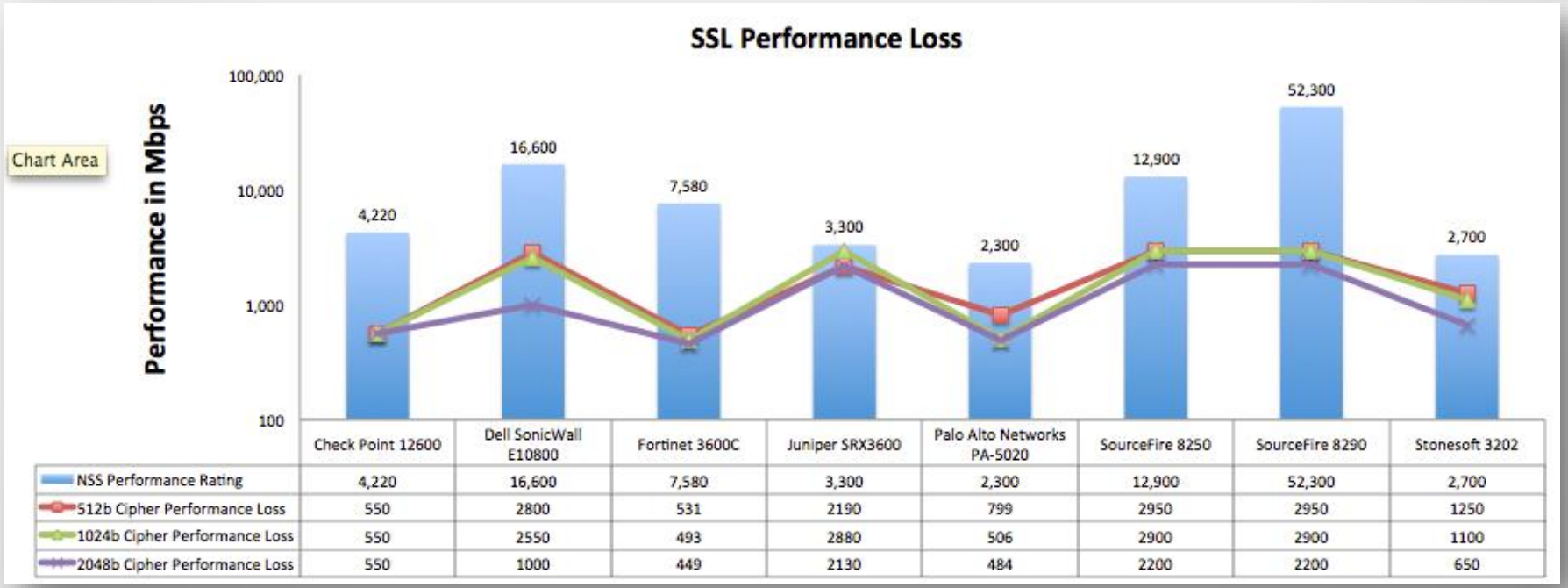
Reálná průchodnost



Je to výhodné?



A co šifrovaný provoz?



	Check Point 12600	Dell SonicWall E10800	Fortinet 3600C	Juniper SRX3600	Palo Alto Networks PA-5020	SourceFire 8250	SourceFire 8290	Stonesoft 3202
NSS Performance Rating	4,220	16,600	7,580	3,300	2,300	12,900	52,300	2,700
512b Cipher Performance Loss	550	2800	531	2190	799	2950	2950	1250
1024b Cipher Performance Loss	550	2550	493	2880	506	2900	2900	1100
2048b Cipher Performance Loss	550	1000	449	2130	484	2200	2200	650

Certifikace řešení

Co lze virtualizovat?

- Filtrace provozu mezi instancemi
  - V rámci datového centra
  - Mezi datovými centry
- Filtrace provozu zvenčí fyzické sítě
- VPN koncentrátor
- Loadbalancer

SDN FW

- Veškerá logika zpracování je na straně řadiče
  - Latence při zpracování nového spojení
  - Výměna dalších zpráv
- Ve stádiu výzkumu
  - Upřednostnění požadavků na blokování
  - Stavové tabulky

- Prakticky
  - Firewall ovládaný REST API
  - Součást platformy

Závěr

- Sledování trendů
- Cyklus obnovy zařízení
- Požadované vlastnosti
- Nezávislé testy výkonu
- Virtuální vs. Hardwarový

Děkuji za pozornost

Dotazy?